

**КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА**

Костюк Ю.В., Складанний П.М.

**ЗАХИСТ ІНФОРМАЦІЇ
В КОМП'ЮТЕРНИХ СИСТЕМАХ
ТА МЕРЕЖАХ**

Підручник

*Частина II. Прикладні аспекти та сучасні
технології захисту інформації в комп'ютерних
системах та мережах*

Київ 2026

УДК 004.056:004.7(075.8)

*Рекомендовано Вченою радою Факультету інформаційних технологій та математики
(протокол №1 від 14 січня 2026 року)*

Автори:

Костюк Ю.В., Складанний П.М.

Рецензенти: В. Л. Шевченко, д-р техн. наук, професор, заступник директора з наукової роботи Інституту програмних систем Національної академії наук України;
О. А. Смірнов, д-р техн. наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Костюк Ю. В., Складанний П.М.

Захист інформації в комп'ютерних системах та мережах. Частина II: підручник / Ю.В. Костюк, П.М. Складанний. – Київ : Київський столичний університет імені Бориса Грінченка, 2026. – 386 с.

У підручнику висвітлено сучасні прикладні аспекти забезпечення безпеки комп'ютерних систем та мереж у спеціалізованих середовищах. Розглянуто питання захисту мобільних і безпроводових технологій, Інтернету речей, хмарних сервісів і систем критичної інфраструктури, а також конфіденційності та захисту персональних даних відповідно до міжнародних і національних нормативних вимог. Подано цілісний підхід до побудови комплексних систем захисту інформації на підприємстві, що охоплює архітектуру безпеки, політики захисту, інтеграцію засобів моніторингу й реагування на інциденти (SIEM, SOC, SOAR) та управління ризиками з використанням сучасних методів і інтелектуальних технологій. Висвітлено технології моніторингу та реагування на інциденти, автоматизацію захисту, використання штучного інтелекту й пояснюваної аналітики, а також сучасні підходи до побудови адаптивних систем кіберзахисту, зокрема на основі концепції Zero Trust. Окрему увагу приділено практичним аспектам захисту корпоративних мереж і систем, забезпеченню безперервності бізнес-процесів, резервному копіюванню даних, цифровій стійкості та впровадженню вимог Регламенту DORA. Матеріал поєднує теоретичні положення з практичними прикладами та орієнтований на студентів, фахівців і дослідників у сфері кібербезпеки. Підручник стане корисним для фахівців з кібербезпеки, студентів і всіх, хто прагнуть системно оволодіти сучасними знаннями та практиками у сфері кіберзахисту.

УДК 004.056:004.7(075.8)

© Костюк Ю. В., Складанний П.М. 2026
© Київський столичний університет імені
Бориса Грінченка, 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	6
ВСТУП.....	9
РОЗДІЛ 1	12
ЗАХИСТ СПЕЦІАЛІЗОВАНИХ СЕРЕДОВИЩ: МОБІЛЬНІ ТА БЕЗДРОТОВІ МЕРЕЖІ, ХМАРНІ СЕРВІСИ, КРИТИЧНА ІНФРАСТРУКТУРА ТА КОНФІДЕНЦІЙНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ.....	12
1.1. Особливості захисту безпроводових технологій (Wi-Fi, ZigBee, Bluetooth, NFC, 5G/6G).....	13
1.2. Загрози для Інтернету речей (IoT) і сенсорних мереж (WSN).....	29
1.3. Хмарна безпека: IaaS, PaaS, SaaS, DevSecOps у хмарних середовищах	45
1.4. Безпека ICS/SCADA-систем та критичної інфраструктури ...	58
1.5. Конфіденційність і захист персональних даних (GDPR, ССРА, УКРАЇНСЬКЕ ЗАКОНОДАВСТВО)	68
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 1.....	75
Контрольні питання	79
РОЗДІЛ 2	81
АРХІТЕКТУРА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ (КСЗІ) ТА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.....	81
2.1. Моделювання архітектури КСЗІ на підприємстві	82
2.2. Організаційний, технічний та політичний рівні захисту	93
2.3. Інтеграція SIEM, SOC та засобів моніторингу	99
2.4. Методи оцінки ефективності та тестування КСЗІ	106
2.5. Розробка та впровадження політики безпеки	110
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 2	114
Контрольні питання	117
РОЗДІЛ 3	119
УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: МОДЕЛІ, МЕТОДИ ТА ІНСТРУМЕНТИ ОЦІНКИ.....	119
3.1. Методології ризик-менеджменту: ISO/IEC 27005, NIST SP 800-30, FAIR	120
3.2. Методи кількісної та якісної оцінки ризиків	132
3.3. GAP-аналіз, SWOT, FMEA, Delphi-метод, Метод матриці ризиків (Risk Matrix) як якісні підходи до оцінки вразливостей	149
3.4. Моделі загроз і векторів атак у ризик-орієнтованому управлінні	162
3.5. Адаптивне управління ризиками на основі машинного навчання.....	171

3.6. Автоматизований моніторинг, візуалізація та аудит ризиків у системах управління інформаційною безпекою	175
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 3.....	178
Контрольні питання	183
РОЗДІЛ 4	185
ТЕХНОЛОГІЇ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ.....	185
4.1. Центри оперативного реагування (SOC) і їх роль у захисті	186
4.2. Життєвий цикл інциденту: виявлення, аналіз, реагування, відновлення	191
4.3. Автоматизація реагування за допомогою SOAR.....	195
4.4. Використання штучного інтелекту для інтелектуального моніторингу подій безпеки	200
4.5. Технології предиктивного моніторингу та прогнозного реагування на інциденти	204
4.6. Постінцидентний аналіз і lessons learned	206
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 4.....	211
РОЗДІЛ 5	218
СИНЕРГІЯ ШТУЧНОГО ІНТЕЛЕКТУ, БЛОКЧЕЙНУ ТА КВАНТОВИХ ОБЧИСЛЕНЬ У ПОБУДОВІ СИСТЕМ КІБЕРЗАХИСТУ	218
5.1. Використання штучного інтелекту та машинного навчання у виявленні кіберзагроз і аномалій поведінки.....	220
5.2. Пояснюваний штучний інтелект (EXPLAINABLE AI, XAI) у ЗАБЕЗПЕЧЕННІ ПРОЗОРОСТІ ТА ДОВІРИ ДО РІШЕНЬ СИСТЕМ КІБЕРЗАХИСТУ	225
5.3. Блокчейн-технології як основа довіри, цілісності та невідмовності в інформаційних системах	229
5.4. Квантові обчислення та виклики для сучасної криптографії і безпеки даних	233
5.5. Актуальні підходи до концепції Zero Trust та побудови адаптивних систем захисту інформації.....	237
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 5	241
Контрольні питання	250
РОЗДІЛ 6.....	252
ПРАКТИЧНІ АСПЕКТИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ І СИСТЕМ.....	252
6.1. Архітектура корпоративної мережі з урахуванням безпеки	253
6.2. Використання VLAN, VPN і тунелювання	259
6.3. Контроль доступу та багаторівнева аутентифікація.....	265
6.4. Захист електронної пошти та веб-сервісів	274
6.5. Безпека DevOps і DevSecOps-процесів	283

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 6	293
Контрольні питання	302
РОЗДІЛ 7.....	304
МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ ТА РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ	304
7.1. Планування безперервності бізнес-процесів (Business Continuity Planning, BCP) і стратегії відновлення після катастроф (Disaster Recovery Planning, DRP) у комп'ютерних системах та мережах.....	306
7.2. Резервне копіювання даних у системах інформаційної безпеки: сучасні технології, типи (повне, інкрементне, диференційне) та стратегії збереження інформаційних ресурсів...	316
7.3. Використання хмарних сервісів і гібридних інфраструктур для забезпечення цифрової безперервності функціонування підприємства.....	327
7.4. Автоматизовані системи тестування та перевірки готовності до відновлення: симуляції інцидентів, моніторинг і оцінка ефективності планів DRP.....	335
7.5. Впровадження вимог Регламенту DORA (Digital Operational Resilience Act) у процеси управління цифровою стійкістю та безперервністю комп'ютерних систем і мереж	338
СПИСОК ДЖЕРЕЛ РОЗДІЛУ 7	349
Контрольні питання	358
СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ	360

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT	– Advanced Persistent Threat (тривала цілеспрямована загроза)
AES	– Advanced Encryption Standard (стандарт симетричного шифрування)
ABAC	– Attribute-Based Access Control (керування доступом на основі атрибутів)
ACL	– Access Control List (список контролю доступу)
API	– Application Programming Interface (програмний інтерфейс взаємодії)
BCP	– Business Continuity Plan (план безперервності бізнесу)
BIOS	– Basic Input/Output System (базова система введення-виведення)
BOTNET	– мережа заражених комп'ютерів, керованих зловмисником
VPN	– Virtual Private Network (віртуальна приватна мережа)
VoIP	– Voice over IP (передача голосу через IP-мережі)
GDPR	– General Data Protection Regulation (загальний регламент ЄС про захист даних)
GUI	– Graphical User Interface (графічний інтерфейс користувача)
DDoS	– Distributed Denial of Service (розподілена атака на відмову в обслуговуванні)
DNS	– Domain Name System (система доменних імен)
DLP	– Data Loss Prevention (запобігання витоку даних)
DORA	– Digital Operational Resilience Act (акт про цифрову операційну стійкість)
ECDSA	– Elliptic Curve Digital Signature Algorithm (алгоритм цифрового підпису на еліптичних кривих)
EDR	– Endpoint Detection and Response (виявлення та реагування на кінцевих точках)
EMV	– електромагнітне випромінювання
Zero Trust	– архітектура «нульової довіри»
ІБ	– інформаційна безпека
ІКС	– інформаційно-комунікаційна система
ІС	– інформаційна система
ІТ	– інформаційні технології
ІоТ	– Інтернет речей (Internet of Things)
ІоЕ	– Інтернет усього (Internet of Everything)

КСЗІ	– комплексна система захисту інформації
КІД	– конфіденційність, цілісність, доступність (CIA)
КЦІАН	– розширена модель безпеки (Confidentiality, Integrity, Availability, Authentication, Non-repudiation)
MAC (address)	– Media Access Control (унікальний апаратний ідентифікатор мережевого інтерфейсу)
MAC (control)	– Mandatory Access Control (примусовий контроль доступу)
MITM	– Man-in-the-Middle (атака «людина посередині»)
MITRE ATT&CK	– база тактик і технік кіберзагроз
NDR	– Network Detection and Response (виявлення та реагування в мережі)
NIST CSF	– National Institute of Standards and Technology Cybersecurity Framework (рамкова модель кібербезпеки NIST)
НСД	– несанкціонований доступ
OSINT	– Open Source Intelligence (розвідка з відкритих джерел)
ОС	– операційна система
ПБ	– політика безпеки
ПЕМВ	– побічне електромагнітне випромінювання
ПЗ	– програмне забезпечення
PKI	– Public Key Infrastructure (інфраструктура відкритих ключів)
RBAC	– Role-Based Access Control (керування доступом на основі ролей)
RaaS	– Ransomware-as-a-Service (програми-вимагачі як сервіс)
RSA	– Rivest–Shamir–Adleman (алгоритм асиметричного шифрування)
SCADA	– Supervisory Control and Data Acquisition (системи диспетчерського керування і збору даних)
SIEM	– Security Information and Event Management (керування інформацією й подіями безпеки)
SOAR	– Security Orchestration, Automation and Response (автоматизація реагування на інциденти безпеки)
SQLi	– SQL Injection (ін'єкція SQL-коду)
TLS	– Transport Layer Security (захист транспортного рівня)
TCP/IP	– Transmission Control Protocol / Internet Protocol (основний стек мережевих протоколів)

ТЗР ПЕМВН	– технічні засоби розвідки побічних електромагнітних випромінювань і наведень
FTP	– File Transfer Protocol (протокол передавання файлів)
FIPS	– Federal Information Processing Standards (федеральні стандарти обробки інформації)
Firewall	– міжмережевий екран
HTTP/HTTPS	– HyperText Transfer Protocol (Secure) (протокол передавання гіпертексту (захищений))
XML	– Extensible Markup Language (розширювана мова розмітки)
ЦОД	– центр обробки даних (data center)
ЦП	– центральний процесор (CPU)
SHA	– Secure Hash Algorithm (алгоритм хешування)
SSH	– Secure Shell (захищене з'єднання)
LAN	– Local Area Network (локальна мережа)
WAN	– Wide Area Network (глобальна мережа)
Wi-Fi	– Wireless Fidelity (бездротова локальна мережа)
XSS	– Cross-Site Scripting (міжсайтове виконання скриптів)

ВСТУП

Проблематика захисту інформації в комп'ютерних системах та мережах є однією з ключових у сучасному інформаційному суспільстві. Зростаюча складність архітектури обчислювальних систем, інтеграція локальних і глобальних мереж, розвиток хмарних технологій та поява нових класів кіберзагроз вимагають від фахівців ґрунтовного розуміння теоретичних і методологічних основ побудови систем безпеки. Саме ці питання розглядаються у підручнику «Захист інформації в комп'ютерних системах та мережах», який має на меті надати читачеві цілісну картину сучасних концепцій, принципів та засобів забезпечення інформаційної безпеки.

Частина II. «Прикладні аспекти та сучасні технології захисту інформації в комп'ютерних системах та мережах» є продовженням підручника «Захист інформації в комп'ютерних системах та мережах» і присвячена практичній реалізації сучасних методів і технологій кіберзахисту у спеціалізованих середовищах. У ній розглянуто питання безпеки мобільних і бездротових мереж, хмарних платформ, систем критичної інфраструктури, а також захисту персональних даних відповідно до міжнародних і національних нормативів.

Послідовна структура частини спрямована на формування цілісного уявлення про побудову комплексних систем захисту інформації (КСЗІ), управління ризиками, моніторинг інцидентів, забезпечення безперервності діяльності та впровадження новітніх підходів — від DevSecOps і Zero Trust до блокчейн-технологій, квантової криптографії та штучного інтелекту в системах кіберзахисту. Матеріал орієнтований на підготовку фахівців із кібербезпеки, інформаційної безпеки, адміністрування комп'ютерних систем і мереж, а також аспірантів і дослідників, які працюють над створенням інтелектуальних, стійких і прозорих систем захисту в умовах цифрової трансформації та розвитку технологій Industry 4.0/5.0.

У другій частині також подано розгорнуті приклади практичних рішень, що ілюструють застосування теоретичних положень на реальних об'єктах інформаційної інфраструктури. Зокрема, наведено моделі архітектури корпоративних мереж із вбудованими засобами безпеки, приклади побудови сегментованих VLAN-систем, VPN-тунелів і механізмів багаторівневої аутентифікації, а також сценарії впровадження політик безпеки та управління ризиками відповідно до стандартів ISO/IEC 27001, 27005, NIST SP 800-30 і DORA. Особливу увагу приділено інтеграції інтелектуальних технологій моніторингу та реагування (SIEM, SOC, SOAR), використанню штучного інтелекту та пояснюваної аналітики (XAI) у

процесах виявлення аномалій, а також розробці практичних рекомендацій із побудови цифрово стійких і адаптивних систем кіберзахисту. Кожен розділ містить методичні пояснення, контрольні питання, приклади лабораторних і проєктних завдань, що спрямовані на закріплення знань і розвиток навичок практичного застосування сучасних засобів захисту інформації у комп'ютерних системах та мережах.

Матеріали підручника будуть корисними не лише для студентів спеціальностей «Комп'ютерна інженерія», «Кібербезпека та захист інформації», «Інженерія програмного забезпечення», й для здобувачів інших спеціальностей, таких як, «Системний аналіз», «Комп'ютерні науки» та ін. Крім того, підручник стане у пригоді аспірантам і здобувачам ступеня доктор філософії з технічних наук, які досліджують методи захисту інформації, що базуються на аналізі ризиків, управлінні безпекою інформаційних, комунікаційних та комп'ютерних систем, а також комп'ютерних мереж.

Головною метою посібника є надання студентам базових знань і методологічних засад у сфері захисту інформації в комп'ютерних системах та мережах, формування розуміння ключових принципів побудови багаторівневих систем безпеки, а також оволодіння практичними навичками застосування сучасних технологій кіберзахисту. Особливу увагу приділено поєднанню теоретичних положень із прикладними аспектами, що дозволяє майбутнім фахівцям не лише засвоїти фундаментальні концепції, а й навчитися впроваджувати їх у реальних умовах функціонування інформаційних та комунікаційних систем.

Для зміцнення національної безпеки України питання кіберзахисту набувають особливої ваги, адже стійкість державних інституцій, критичної інфраструктури та бізнес-сектору безпосередньо залежить від ефективності системи захисту інформації. Підручник «Захист інформації в комп'ютерних системах та мережах» покликаний сприяти підготовці висококваліфікованих фахівців, здатних аналізувати й нейтралізувати загрози, розробляти та впроваджувати комплексні заходи інформаційної безпеки, забезпечуючи як інтереси конкретних підприємств, так і загальнодержавні пріоритети.

Таким чином, видання орієнтоване на формування у студентів і слухачів цілісного уявлення про сучасні підходи до кіберзахисту, що є необхідною умовою не лише професійного розвитку майбутніх спеціалістів, а й укріплення цифрового суверенітету та національної безпеки України.

Дослідження проведено в рамках реалізації науково-дослідної теми «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних

комплексів управління критичної інфраструктури» (реєстраційний номер 0122U200483 від 06.07.2022).

РОЗДІЛ 1

ЗАХИСТ СПЕЦІАЛІЗОВАНИХ СЕРЕДОВИЩ: МОБІЛЬНІ ТА БЕЗДРОТОВІ МЕРЕЖІ, ХМАРНІ СЕРВІСИ, КРИТИЧНА ІНФРАСТРУКТУРА ТА КОНФІДЕНЦІЙНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ



- 1.1. Особливості захисту безпроводових технологій (Wi-Fi, ZigBee, Bluetooth, NFC, 5G/6G)***
- 1.2. Загрози для Інтернету речей (IoT) і сенсорних мереж (WSN)***
- 1.3. Хмарна безпека: IaaS, PaaS, SaaS, DevSecOps у хмарних середовищах***
- 1.4. Безпека ICS/SCADA-систем та критичної інфраструктури***
- 1.5. Конфіденційність і захист персональних даних (GDPR, CCPA, українське законодавство)***

Розділ «Захист спеціалізованих середовищ: мобільні та бездротові мережі, хмарні сервіси, критична інфраструктура та конфіденційність персональних даних» присвячено комплексному аналізу сучасних підходів до забезпечення безпеки інформації в середовищах, які мають специфічні архітектурні, технологічні та функціональні особливості. У цих середовищах традиційні засоби захисту потребують адаптації до нових умов, пов'язаних із мобільністю, розподіленістю, використанням хмарних технологій, зростанням обсягу персональних даних та підвищенням значущості критичної інфраструктури для національної безпеки.

У контексті мобільних та бездротових мереж розглядаються питання автентифікації користувачів, захисту каналів зв'язку, протидії атакам типу «людина посередині» (MITM), спуфінгу, перехоплення трафіку та

несанкціонованого доступу. Особлива увага приділяється стандартам захисту Wi-Fi (WPA3), безпеці мобільних операційних систем і пристроїв, а також методам контролю ризиків у середовищі Інтернету речей (IoT), де обмеженість ресурсів створює додаткові виклики для криптографічного захисту.

Хмарні сервіси розглядаються як середовище із підвищеними вимогами до довіри, контролю доступу та забезпечення цілісності даних у спільній інфраструктурі. У межах розділу аналізуються моделі безпеки IaaS, PaaS і SaaS, методи багаторівневої ідентифікації, шифрування даних на стороні клієнта, журналювання дій користувачів та інтеграція з системами моніторингу і реагування на інциденти. Розглядаються питання дотримання вимог DORA і GDPR під час оброблення даних у хмарі, а також методи побудови довірених обчислювальних середовищ із використанням контейнеризації та Zero Trust-архітектури.

Значна частина розділу присвячена захисту критичної інфраструктури, де забезпечення безперервності функціонування інформаційних систем є питанням державної безпеки. Описуються принципи побудови систем кіберзахисту промислових мереж (ICS/SCADA), застосування сегментації, ізоляції каналів управління, резервування та засобів моніторингу в реальному часі. Пояснюється роль національних кризових і ситуаційних центрів, інтегрованих із системами SIEM/SOAR для автоматизованого виявлення, аналізу й реагування на інциденти.

Окремий підрозділ розкриває аспекти конфіденційності персональних даних, де розглядаються нормативно-правові вимоги щодо їх оброблення, методи мінімізації, псевдонімізації та анонімізації даних, а також застосування диференційно-приватних і федеративних механізмів навчання, що дають змогу здійснювати аналіз без розкриття вихідної інформації. Важливою складовою є також впровадження політик доступу, аудиту й моніторингу з урахуванням принципів прозорості, підзвітності та контролю прав суб'єктів даних.

Загалом, розділ формує системне бачення безпеки спеціалізованих середовищ, що охоплює технічні, організаційні й правові аспекти. Він демонструє взаємозв'язок між рівнями захисту мобільних і хмарних технологій, кіберстійкістю критичної інфраструктури та дотриманням конфіденційності персональної інформації. Такий підхід забезпечує цілісне розуміння сучасних викликів інформаційної безпеки й формує компетентності для розроблення та впровадження ефективних механізмів захисту в умовах динамічних кіберзагроз.

1.1. ОСОБЛИВОСТІ ЗАХИСТУ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ (Wi-Fi, ZIGBEE, BLUETOOTH, NFC, 5G/6G)

Особливості захисту безпроводових технологій (Wi-Fi, ZigBee, Bluetooth, NFC, 5G/6G) полягають у необхідності врахування специфічних характеристик цих мереж, зокрема відкритості ефірного середовища, обмежених обчислювальних ресурсів пристроїв, динамічності топології та широкої варіативності протоколів обміну даними. На відміну від дротових мереж, де фізичний доступ до середовища передачі є контрольованим, у бездротових системах будь-який сторонній користувач потенційно може перехопити або модифікувати трафік, що створює додаткові вимоги до автентифікації, шифрування та цілісності переданої інформації.

Загальними особливостями захисту безпроводових технологій є необхідність забезпечення конфіденційності даних у відкритому радіоканалі, що досягається шляхом застосування стійких криптографічних алгоритмів і динамічного оновлення ключів шифрування. Важливою умовою є реалізація багаторівневої автентифікації користувачів і пристроїв, яка унеможливорює підміну вузлів та несанкціонований доступ до мережі. Через обмежені ресурси багатьох пристроїв (сенсорів, контролерів, IoT-модулів) застосовуються полегшені протоколи безпеки, що балансують між продуктивністю й рівнем захисту. Особливу увагу приділяють стійкості до атак відмови в обслуговуванні (DoS) і забезпеченню безперервності зв'язку в умовах радіоперешкод чи змін топології мережі. Не менш важливими є механізми сегментації та моніторингу трафіку, які дозволяють виявляти аномалії та ізолювати скомпрометовані вузли. Комплексний підхід до захисту безпроводових технологій має включати криптографічні, організаційні та інтелектуальні методи, здатні адаптуватися до динамічних умов сучасного бездротового середовища.

Захист мереж Wi-Fi

Для мереж Wi-Fi ключовими є протоколи безпеки WPA2 і WPA3, що забезпечують шифрування на основі стандарту AES і захист від атак типу перехоплення ключів та підміни точок доступу. Застосування механізму Simultaneous Authentication of Equals (SAE) у WPA3 дозволяє протидіяти атакам грубої сили на паролі, а сегментація мережі за VLAN і впровадження контролю доступу 802.1X підвищують рівень ізоляції користувачів. Водночас залишаються актуальними загрози фальшивих точок доступу, спуфінгу MAC-адрес і атак деаутентифікації, що потребують постійного моніторингу трафіку та використання систем виявлення вторгнень (WIDS/WIPS).

Архітектурні та процедурні заходи. У корпоративних розгортаннях доцільно використовувати WPA3-Enterprise з EAP-TLS і власним центром сертифікації, що забезпечує взаємну аутентифікацію клієнта і точки доступу та усуває залежність від паролів. Для гостьових підключень варто впровадити Opportunistic Wireless Encryption, який шифрує трафік навіть без спільного секрету, а гостьовий сегмент ізолювати від виробничих ресурсів за допомогою

окремого SSID і динамічних VLAN через RADIUS. Обов'язково вмикають Protected Management Frames за 802.11w, оскільки це блокує деаутентифікаційні та частину керувальних атак, у діапазоні 6 ГГц цей захист є вимогою за замовчуванням. Слід повністю відмовитися від WEP і TKIP, використовувати AES-CCMP для WPA2 і GCMP у режимах WPA3, налаштувати періодичну ротацію групових ключів і вимикати WPS, який часто є точкою компрометації. Для безперервного роумінгу без втрати захисту застосовують 802.11r Fast Transition разом із 802.11k і 802.11v, при цьому необхідно перевірити сумісність клієнтів і правильність роботи кешування PMK.

Сегментація мережі має бути багаторівневою. Окремі SSID виділяють для офісних, гостьових та IoT-пристроїв, причому для IoT доцільно застосовувати клієнтську ізоляцію на рівні другого рівня і політики міжмережевих екранів з принципом мінімальних прав. Для пристроїв, що не підтримують 802.1X, корисні технології унікальних передспільних ключів на пристрій, які спрощують відкликання доступу та знижують ризики повторного використання паролів. Доступ адміністратора до точок і контролерів переносять у виділений керувальний VLAN, дозволяють тільки захищені протоколи на кшталт HTTPS і SSH, вмикають SNMPv3, встановлюють списки контролю доступу та зберігають журнали подій на централізованому сервері. Резервне копіювання конфігурацій та контроль цілісності прошивок зменшують ризики прихованих змін налаштувань.

Моніторинг і виявлення вторгнень реалізують через WIDS/WIPS з інтеграцією до SIEM. Потрібно відстежувати показники рівня деаутентифікаційних кадрів, помилок EAP, стрибків у кількості асоціацій, появи неавторизованих SSID і точок доступу та аномалій у розподілі каналів. У разі виявлення фальшивої точки доступу система може автоматично ізолювати підозрілих клієнтів або перейти в режим підвищеної настороженості, але заходи активного придушення слід застосовувати з урахуванням правових обмежень. Регулярні обстеження ефірного середовища, планування каналів і керування потужністю передавачів допомагають уникнути співканальних завад і прихованих вузлів, що підвищує як якість зв'язку, так і точність виявлення атак.

Захист клієнтів є не менш критичним. Потрібно вимикати автоприєднання до відкритих мереж, використовувати профілі з перевіркою сертифікатів і регулярно оновлювати прошивки клієнтських адаптерів для усунення відомих вразливостей на кшталт повторної інсталяції ключів. Для доступу з недовірених мереж рекомендують тунелювання через VPN, обмеження служб локального спільного доступу та фільтрацію службових протоколів в межах бездротового сегмента. Для чутливих застосунків варто застосовувати додаткове шифрування на рівні застосунку і перевірку цілісності трафіку.

Фізичні та радіочастотні аспекти також впливають на безпеку. Доцільно планувати розміщення точок доступу так, щоб мінімізувати вихід сигналу за межі

контрольованої зони, використовувати спрямовані антени в складних середовищах і за потреби екранувати приміщення з підвищеною чутливістю. Контроль доступу до самих точок і комутаційного обладнання, герметизація портів і відеоспостереження перешкоджають підключенню сторонніх пристроїв або заміні обладнання.

На рис. 1.1 показано загальну схему взаємодії компонентів у процесі аутентифікації користувача в захищеній Wi-Fi мережі. Модель складається з трьох основних частин: Supplicant (клієнтський пристрій), Authenticator (точка доступу) та Authentication Server (RADIUS), який є частиною інфраструктури AAA (Authentication, Authorization, Accounting). Процес починається з ініціації з'єднання клієнтом, який передає свої облікові дані через протокол EAP (Extensible Authentication Protocol). Точка доступу виступає посередником і перенаправляє ці дані до сервера RADIUS для перевірки достовірності. Після успішної автентифікації між клієнтом і точкою доступу встановлюється спільний сеансовий ключ (Session Key, SK) і формується ключ шифрування (Master Key, MK) для захисту переданих кадрів WEP/TKIP або 802.11i (AES/CCMP). Схема демонструє також використання PKI (Public Key Infrastructure) або AuC (Authentication Center) для генерації та управління сертифікатами і ключами, що забезпечує високий рівень безпеки, контроль доступу та цілісність трафіку у корпоративних бездротових мережах.

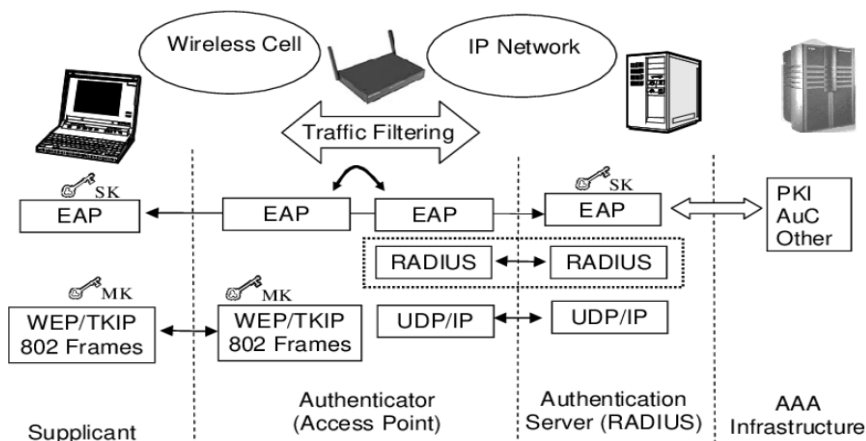


Рис. 1.1. Архітектура аутентифікації та захисту Wi-Fi з використанням протоколу 802.1X і сервера RADIUS

Джерело: [1-10, 18-23, 45-56]

Окрему увагу приділяють забезпеченню безпеки в діапазонах п'ятого та шостого покоління стандартів Wi-Fi. У 6 ГГц немає зворотної сумісності із застарілими алгоритмами, тому за замовчуванням використовуються сучасні механізми аутентифікації і шифрування, що знижує ризики, пов'язані зі спадщиною попередніх стандартів. Це поєднується з більш чистим ефіром і точнішим керуванням спектром, але вимагає оновлення клієнтських пристроїв і

ретельного управління політиками доступу. Сукупність наведених заходів створює цілісний контур безпеки, який охоплює криптографію, керування доступом, сегментацію, моніторинг і фізичний рівень, та дає змогу підтримувати високий рівень довіри у бездротових мережах різного масштабу.

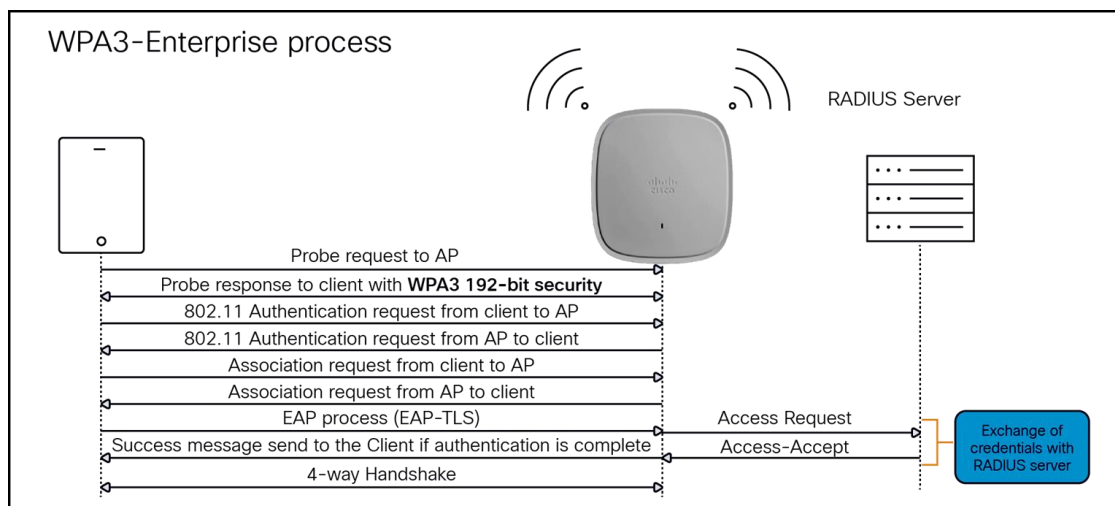


Рис. 1.2. Процес автентифікації в мережі Wi-Fi за протоколом WPA3-Enterprise
Джерело: [1-10, 18-23, 45-56, 68-78]

На рис. 1.2 показано послідовність етапів встановлення захищеного з'єднання між клієнтським пристроєм, точкою доступу (Access Point, AP) та сервером автентифікації RADIUS у корпоративній мережі Wi-Fi, що використовує стандарт WPA3-Enterprise. Процес розпочинається з Probe Request клієнта до точки доступу з метою виявлення доступної мережі. Точка доступу відповідає Probe Response із зазначенням підтримки WPA3 і 192-бітного рівня безпеки. Далі відбувається двосторонній обмін запитами 802.11 Authentication і Association, що формує базове логічне з'єднання між клієнтом і точкою доступу. Основний етап — це процес EAP (Extensible Authentication Protocol), який у WPA3-Enterprise реалізується через метод EAP-TLS, тобто автентифікацію з використанням цифрових сертифікатів. У цей момент точка доступу виступає посередником між клієнтом і сервером RADIUS, передаючи облікові дані для перевірки у системі AAA (Authentication, Authorization, Accounting). Після успішної перевірки сервер RADIUS надсилає повідомлення Access-Accept, що підтверджує автентичність клієнта. Точка доступу ініціює обмін 4-way Handshake, у ході якого генерується спільний ключ сеансу для шифрування трафіку. Завдяки використанню WPA3-Enterprise забезпечується взаємна автентифікація, захист від MITM-атак, стійке шифрування AES-256 і динамічна генерація ключів, що робить процес з'єднання безпечним навіть у масштабних корпоративних або хмарних інфраструктурах.

Захист мереж ZigBee

Технологія ZigBee, що використовується в системах розумного дому, сенсорних мережах і промисловому Інтернеті речей, характеризується низьким енергоспоживанням і спрощеною криптографією. Захист у ZigBee базується на використанні симетричного алгоритму AES-128, а ключі шифрування можуть бути мережевими або унікальними для кожного вузла. Основними загрозами є атаки повторного відтворення (replay), підміна вузлів та несанкціоноване підключення нових пристроїв до мережі. Ефективний захист забезпечується за рахунок автентифікації вузлів, регулярного оновлення ключів і обмеження дальності радіосигналу.

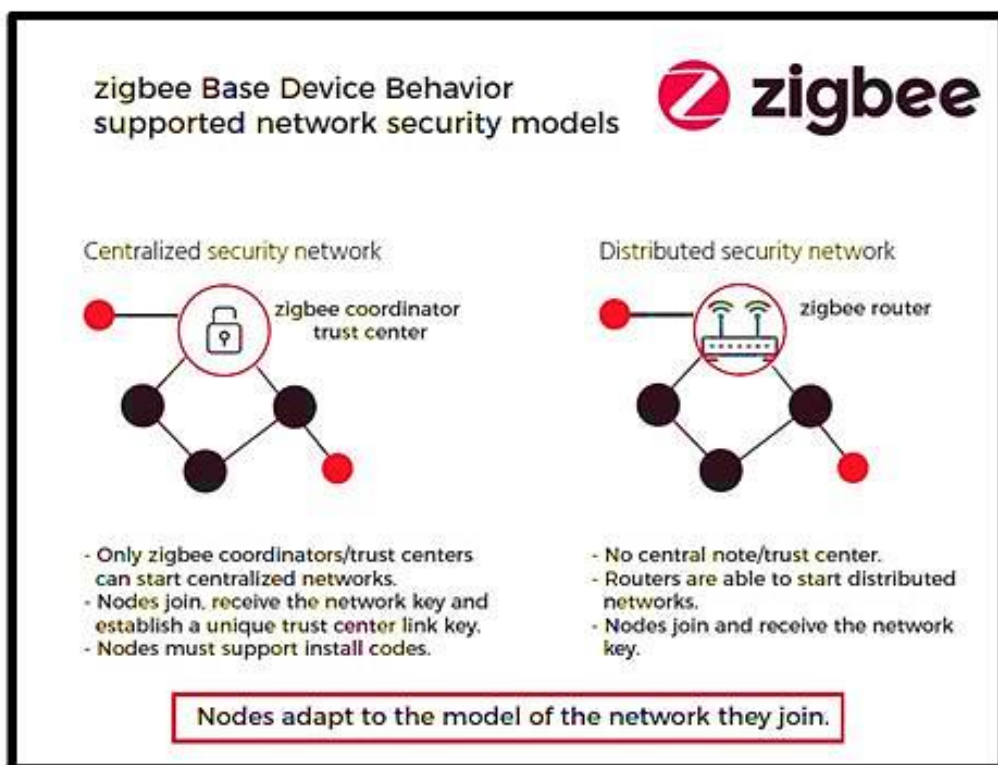


Рис. 1.3. Система керування безпекою ZigBee: Trust Center, обмін ключами та рівні захисту

Джерело: [1-10, 18-23, 45-56, 68-78]

На рис. 1.3 показано архітектуру механізмів безпеки ZigBee, яка включає Trust Center, вузли мережі (координатор, маршрутизатори, кінцеві пристрої) та канали обміну ключами. Центральним елементом виступає Trust Center, що виконує функції генерації, розподілу й оновлення ключів — Network Key, Master Key і Link Key. У верхній частині схеми позначено рівні, на яких реалізовано захист: NWK (Network) — відповідає за шифрування маршрутизаційних повідомлень, APS (Application Support) — за цілісність і автентифікацію прикладних даних. Процес автентифікації передбачає, що приєднання нового

вузла до мережі можливе лише через Trust Center, який перевіряє його справжність і видає тимчасовий Trust Center Link Key. Потім цей ключ використовується для створення унікального Application Link Key для кожної пари пристроїв. Таким чином, на схемі відображено повний цикл безпеки ZigBee — від формування ключів і автентифікації до шифрування кадрів і контролю довіри між пристроями, що гарантує захист комунікацій навіть у ресурсно обмежених середовищах IoT.

У мережах ZigBee система безпеки реалізована на рівнях мережевого й прикладного шарів, що дозволяє захищати як маршрутизаційні кадри, так і дані користувачів. Координатор мережі (Trust Center) виконує роль головного елемента управління ключами, а також контролює приєднання нових пристроїв і розподілення прав доступу. Для автентифікації вузлів застосовується процес обміну ключами через заздалегідь встановлений ключ Trust Center Link Key, який далі використовується для генерування унікальних Network Key та Application Link Key. Такі механізми дозволяють формувати захищені пари з'єднань між пристроями та уникати повторного використання компрометованих ключів.

Для запобігання атакам повторного відтворення ZigBee використовує лічильники кадрів (Frame Counters) і верифікацію цілісності повідомлень за допомогою кодів автентифікації (Message Integrity Code — MIC). Усі пакети шифруються з урахуванням номерів кадрів, що унеможливує відтворення старих повідомлень навіть за умови перехоплення трафіку. Пристрої з обмеженими ресурсами повинні мати алгоритмічно оптимізовані реалізації AES, щоб уникнути перевантаження енергоспоживання та затримок у маршрутизації.

Вразливими залишаються сценарії, пов'язані з несанкціонованим приєднанням пристроїв, особливо коли мережа функціонує в режимі відкритого доступу (Permit Join). У таких випадках необхідно обмежувати тривалість цього режиму, а після формування стабільної топології — відключати можливість автоматичного підключення. Також слід регулярно оновлювати ключі безпеки через процедури rekeying, що ініціюються Trust Center, аби зменшити ризики компрометації.

Особливу роль відіграє контроль фізичного рівня, адже обмеження радіусу дії передавачів і використання спрямованих антен зменшує ймовірність перехоплення сигналу сторонніми пристроями. Додатково застосовують механізми захисту від глушіння сигналу (jamming), резервування каналів і динамічне перемикавання частот, що підвищує стійкість мережі до перешкод і навмисних атак.

Для промислових застосувань ZigBee PRO передбачає розширені політики контролю доступу, підтримку численних таблиць зв'язків і резервування маршрутів для забезпечення надійності передачі в умовах критичної інфраструктури. Інтеграція ZigBee з шлюзами IoT вимагає додаткового

шифрування трафіку на транспортному рівні (TLS) між шлюзом і хмарними сервісами, щоб запобігти втраті довіри між сегментами системи.

Ключовими заходами комплексного захисту є впровадження сегментації мережі за призначенням пристроїв, автентифікація на основі сертифікатів або унікальних ідентифікаторів IEEE 64-bit, а також моніторинг стану вузлів і мережевих подій для виявлення аномальної активності. Постійне оновлення прошивок, контроль цілісності програмного забезпечення пристроїв та обмеження доступу до фізичних компонентів системи дозволяють мінімізувати ризики компрометації.

Таким чином, захист ZigBee базується на поєднанні криптографічних методів, централізованого управління довірою, контролю фізичного середовища та постійного моніторингу, що забезпечує прийнятний рівень безпеки навіть у середовищах із жорсткими обмеженнями енергоспоживання й обчислювальних ресурсів.

Захист Bluetooth

Bluetooth широко застосовується в мобільних пристроях, носимій електроніці та автомобільних системах. Його безпека залежить від версії протоколу: сучасні реалізації Bluetooth 5.0 і вище підтримують шифрування на основі AES-CCM, процедури Secure Simple Pairing та численні механізми уникнення MITM-атак. Разом із тим Bluetooth залишається вразливим до атак BlueBorne, KNOB і прослуховування зв'язку у відкритому режимі, тому необхідним є вимкнення непотрібних служб, регулярне оновлення прошивок і використання режимів з підтвердженням автентичності пристроїв.

Архітектура безпеки Bluetooth базується на багаторівневій моделі, яка включає процедури автентифікації, авторизації, шифрування трафіку та керування ключами. Основу становить процес *парування* (pairing), під час якого пристрої обмінюються ключами зв'язку (Link Keys), що надалі використовуються для формування сесійних ключів шифрування. У сучасних реалізаціях Bluetooth 5.0+ застосовується механізм Secure Simple Pairing (SSP), який підтримує чотири режими взаємодії — Just Works, Numeric Comparison, Passkey Entry та Out-of-Band (OOB) — з метою мінімізації ризику атак “людина посередині” (MITM). Найвищий рівень безпеки забезпечує метод OOB, оскільки він передбачає передавання аутентифікаційних даних поза радіоканалом, наприклад через NFC.

На схемі (рис. 1.4) показано типову стекову архітектуру Bluetooth із виділенням ключових компонентів безпеки: шар Link Manager / Link Controller, L2CAP, RFCOMM і модуль Security Manager (який координує автентифікацію, шифрування, керування ключами). Пристрої взаємодіють через HCI (Host Controller Interface) та відповідні сервіси. Чітко видно, що Security Manager є центральним компонентом, який приймає рішення щодо доступу, обробляє запити на автентифікацію, і підтримує зв'язок із базовими шарами стеку. Модуль Security

Manager виконує ключові функції — ініціює автентифікацію, генерує та зберігає Link Keys, забезпечує шифрування трафіку за допомогою AES-CCM, а також контролює політику доступу до сервісів. На верхньому рівні стеку працюють прикладні профілі (наприклад, HID, HFP, OBEX), які використовують встановлені безпечні канали зв'язку. На нижніх рівнях — Baseband і Radio Layer, що реалізують фізичну передачу сигналу та базову логіку обміну кадрами. Така архітектура забезпечує багаторівневий захист Bluetooth-з'єднання, включаючи автентифікацію пристроїв, керування ключами, авторизацію сервісів і шифрування даних під час передачі.

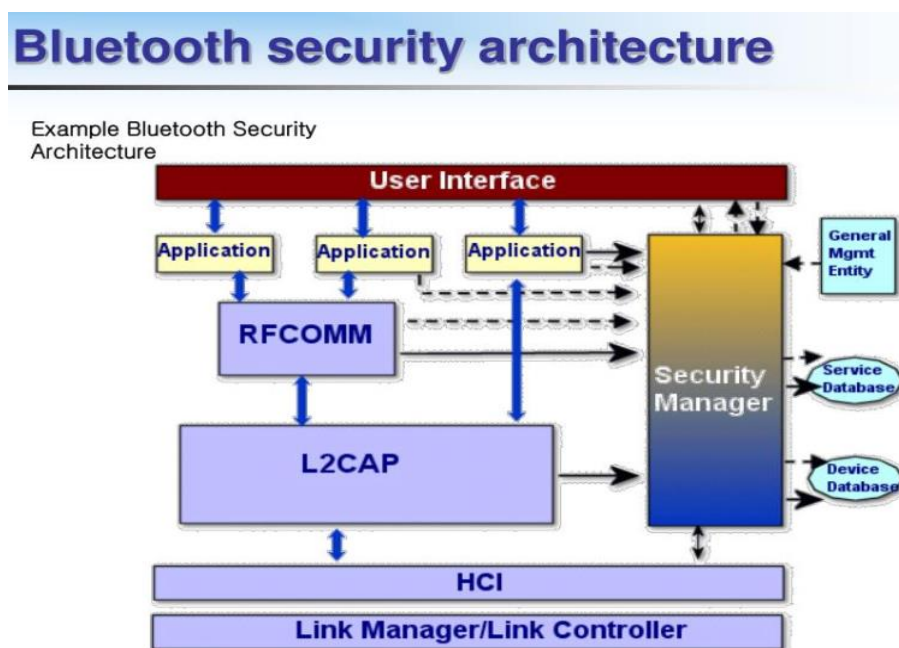


Рис. 1.4. Архітектура безпеки Bluetooth із менеджером безпеки (Security Manager) та стеком протоколів

Джерело: [1-10, 18-23, 45-56, 68-78]

Процес шифрування у Bluetooth здійснюється за допомогою алгоритму AES-CCM, що забезпечує як конфіденційність, так і цілісність даних, а для генерації випадкових чисел і ключів застосовується спеціалізований апаратний генератор, який зменшує ризики повторного використання ключів. Для уникнення компрометації ключів кожна нова сесія створюється на основі унікальних параметрів, включаючи ідентифікатори пристроїв (BD_ADDR) та випадкові числа (RAND). У версіях Bluetooth Low Energy (BLE) безпека додатково підсилюється процедурою LE Secure Connections, що використовує обмін ключами на основі еліптичних кривих (Elliptic Curve Diffie-Hellman, ECDH). Це забезпечує криптографічну стійкість навіть у випадку перехоплення трафіку під час первинного з'єднання.

Попри вдосконалення протоколу, Bluetooth залишається вразливим до низки специфічних атак. До них належать BlueBorne — дистанційне виконання коду через уразливості в реалізації стеку Bluetooth; KNOB (Key Negotiation of Bluetooth) — зниження ентропії ключів шифрування до одного байта під час обміну параметрами; BIAS (Bluetooth Impersonation AttackS) — відтворення автентифікаційних сесій без повторного парування. Для запобігання таким загрозам слід регулярно оновлювати прошивки контролерів і стеків Bluetooth, вимикати непотрібні профілі (OBEX, HFP, HID) і встановлювати мінімально необхідний рівень видимості пристрою (non-discoverable mode).

Захист Bluetooth-пристроїв у мобільних і автомобільних системах передбачає впровадження політик автентифікації з двостороннім підтвердженням, обмеження часу активності відкритого каналу і фільтрацію MAC-адрес у білому списку. Для носимих пристроїв (фітнес-трекерів, розумних годинників) важливо застосовувати процедури автоматичного роз'єднання при втраті зв'язку та очищення пам'яті від ключів після розриву пари. Автомобільні мультимедійні системи мають бути ізольовані від внутрішніх шин управління (CAN, LIN), аби запобігти перехопленню команд через Bluetooth-з'єднання.

Для підвищення захисту на рівні користувача доцільно використовувати параметри *trusted devices*, блокування автоматичного прийому файлів через OBEX і шифрування трафіку додатковими програмними засобами, особливо під час обміну конфіденційними даними. Рекомендовано також періодично очищувати список з'єднаних пристроїв і вимикати Bluetooth у разі невикористання, що знижує ймовірність атак типу *sniffing* і *tracking*.

Важливу роль відіграє моніторинг активності Bluetooth у межах корпоративних або публічних середовищ. Для цього застосовуються системи аналізу спектру та інструменти IDS/IPS, які дозволяють виявляти несанкціоновані пристрої, підозрілі сигнали або повторювані спроби підключення. У поєднанні з журналюванням подій це забезпечує можливість оперативного реагування на інциденти безпеки.

Загалом, ефективний захист Bluetooth базується на поєднанні криптографічних протоколів, регулярного оновлення стеків, обмеження видимості пристроїв і поведінкових політик безпеки, які разом формують багаторівневу систему протидії сучасним загрозам у безпроводовому середовищі.

Захист NFC (Near Field Communication)

NFC (Near Field Communication) відрізняється малим радіусом дії (до 10 см), що частково знижує ризик несанкціонованого доступу, однак не виключає можливості атак перехоплення, ретрансляції або підміни пристрою. Для забезпечення конфіденційності транзакцій використовуються криптографічні протоколи з короткочасними сесіями та обмін ключами Diffie–Hellman, а також

додаткові механізми шифрування на рівні застосунків (наприклад, у мобільних платіжних системах).

Безпека технології NFC ґрунтується на поєднанні фізичних обмежень радіоканалу, криптографічних механізмів шифрування та процедур автентифікації між пристроями. Хоча мала відстань зв'язку (до 10 см) істотно знижує ймовірність несанкціонованого перехоплення даних, вона не гарантує повного захисту, адже злоумисник із спеціалізованою антеною може зчитувати сигнал на відстані до кількох метрів. Тому фізичний бар'єр у NFC лише доповнює, але не замінює криптографічний захист.

Архітектура безпеки NFC включає три рівні: фізичний, протокольний і прикладний. На фізичному рівні передбачено низьку потужність передавача, індукційне з'єднання та обмежений час активності сеансу, що знижує ймовірність глушіння або підміни сигналу. На протокольному рівні реалізуються механізми взаємної автентифікації між пристроями, які можуть працювати в режимах Reader/Writer, Peer-to-Peer або Card Emulation. Для обміну ключами та формування короткочасних сесій використовуються алгоритми на основі еліптичних кривих Diffie–Hellman (ECDH), що забезпечують високий рівень стійкості при мінімальних обчислювальних витратах.

У платіжних та ідентифікаційних системах NFC застосовуються захищені елементи (Secure Element, SE) — апаратні модулі, які ізолювано зберігають криптографічні ключі та сертифікати. Вони можуть бути реалізовані у вигляді вбудованого чипа (eSE), SIM-карти або спеціального контролера в смартфоні. Така ізоляція гарантує, що навіть у разі компрометації операційної системи доступ до ключів неможливий. Сеанси обміну між SE та зовнішнім терміналом додатково захищаються протоколами APDU із використанням цифрових підписів і кодів автентифікації повідомлень (MAC).

Серед типових загроз для NFC виділяють relay-атаки (ретрансляція сигналу між справжнім користувачем і шахрайським пристроєм), skimming (пасивне зчитування даних картки), spoofing (імітація легітимного пристрою) та data corruption (навмисне внесення шуму у сигнал). Для протидії relay-атакам застосовується time-of-flight validation — контроль затримки сигналу, який дає змогу виявити невідповідність фізичної відстані. Крім того, сучасні платіжні системи (Google Pay, Apple Pay) реалізують динамічні токени та одноразові ідентифікатори транзакцій, що робить повторне використання перехоплених даних безглуздом.

Важливим аспектом є захист на рівні застосунків, де використовуються додаткові криптографічні протоколи — TLS або спеціалізовані токенізаційні схеми, що шифрують усі критичні дані (номери карток, біометричні параметри, цифрові підписи). Багато сучасних рішень реалізують багаторівневу

автентифікацію: поєднання PIN-коду, біометричних параметрів і підтвердження на рівні сервера емітента картки.

У промислових і логістичних системах, де NFC використовується для ідентифікації об'єктів або доступу до обладнання, безпека забезпечується через використання унікальних сертифікатів UID, обмеження часу сесії та контроль цілісності даних у тегах. Теги з підтримкою криптографії (MIFARE DESFire, NTAG 424 DNA) дозволяють генерувати динамічні автентифікаційні коди при кожному зчитуванні, що унеможливорює їх клонування.

Для користувачів важливо дотримуватися поведінкових правил безпеки — не залишати ввімкнену функцію NFC у публічних місцях без потреби, підтверджувати транзакції лише після перевірки легітимності терміналу та використовувати офіційні додатки з цифровими підписами. Адміністраторам систем рекомендується проводити періодичний аудит сертифікатів, тестування на relay-атаки й перевірку наявності оновлень безпеки у драйверах і прошивках NFC-контролерів.

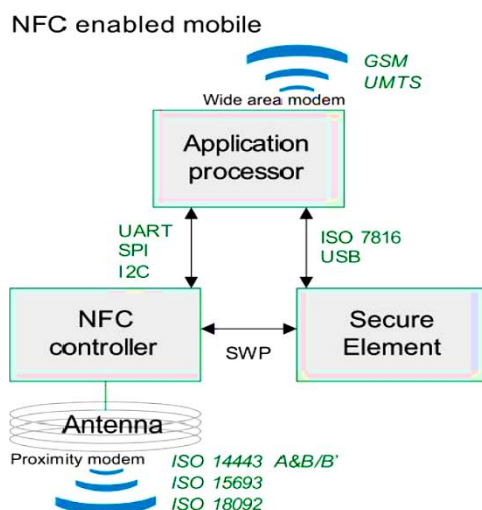


Рис. 1.5. Архітектура NFC у мобільному пристрої з Secure Element (SE)
Джерело: [1-10, 18-23, 45-56, 68-78]

На схемі (рис. 1.5) показано компоненти мобільного пристрою з підтримкою NFC: NFC controller, Secure Element (SE), Application Processor і Antenna. Контролер займається обробкою радіосигнального інтерфейсу (RF), а Secure Element відповідає за надійне зберігання криптографічних ключів та виконання конфіденційних операцій, ізольовано від основної ОС. Комунікація між контролером і SE може здійснюватися через інтерфейси типу SWP (Single Wire Protocol) або інші апаратні канали.

У підсумку, захист NFC забезпечується комплексом технічних, криптографічних та організаційних заходів: ізоляцією Secure Element, динамічною генерацією ключів і токенів, контролем часу сеансу, перевіркою достовірності

пристроїв та багаторівневою автентифікацією користувача. Такий підхід гарантує високий рівень безпеки як у платіжних ідентифікаційних системах, так і в промислових або побутових сценаріях використання.

На схемі (рис. 1.6) показано три компоненти: Reader (термінал читання), Proxy (проксі-пристрій), і Smart-Mole (молекс-пристрій). Proxy перехоплює або ретранслює APDU-команди між Reader та справжньою міткою (тегом / смарт-картою). Smart-Mole, розташований поблизу картки або NFC-тега, виконує роль локального інтермедіара, який передає дані від карти через інтернет або канал зв'язку до Proxy, що потім взаємодіє з Reader як ніби це легітимна карта. Таким чином атака "...relay" дозволяє зловмиснику дистанційно "розтягнути" дію NFC-каналу, обманюючи систему, що карта справді поруч.

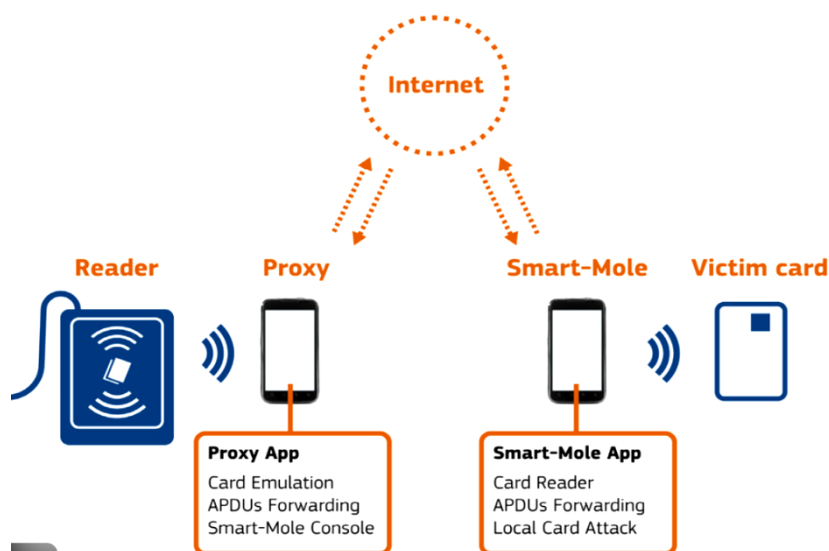


Рис. 1.6. Архітектура NFC у мобільному пристрої з Secure Element (SE)
Джерело: [1-10, 18-23, 45-56, 68-78]

Захист 5G/6G

Мережі п'ятого і шостого поколінь (5G/6G) реалізують принципово нову архітектуру безпеки, орієнтовану на віртуалізацію, сегментацію мережі (network slicing) і концепцію Zero Trust. Захист базується на обов'язковому шифруванні користувацького та сигнального трафіку, аутентифікації з подвійним фактором (EAP-AKA'), динамічному керуванні ключами та постійному моніторингу стану мережевих вузлів. Важливим аспектом є також протидія DDoS-атакам, захист від компрометації базових станцій та використання методів штучного інтелекту для виявлення аномалій у трафіку.

На рис. 1.7 представлено узагальнену архітектуру захисту мереж п'ятого покоління, яка реалізує багаторівневу ізоляцію сегментів (slices) відповідно до типу галузі або сервісу — *Industrial IoT*, *Critical Infrastructure* та *Autonomous*

Vehicles. У центрі схеми зображено ядро мережі 5G (5G Core Network), що включає функціональні модулі AMF (Access and Mobility Management Function), SMF (Session Management Function) і UPF (User Plane Function), які керують автентифікацією користувачів, маршрутизацією трафіку й реалізацією політик безпеки. Сегментація мережі забезпечує логічну ізоляцію потоків даних і дозволяє призначати індивідуальні ключі, алгоритми шифрування та політики контролю для кожного зрізу. Механізм *learning of context* формує контекст автентифікації за параметрами *Subscriber ID*, *Equipment ID* і *Network Slice ID*, а модуль UPF здійснює інспекцію трафіку та застосовує модулі запобігання загрозам (*threat prevention*) для кожного зрізу або групи зрізів. Дані після обробки в ядрі мережі спрямовуються до відповідних хмарних сегментів — *Industrial IoT Cloud*, *Critical Infrastructure Cloud* або *Data Networks / Internet*, що дає змогу інтегрувати політики безпеки на рівні додатків і сервісів. Така архітектура відображає принципи Zero Trust, Network Slicing Security Policies і динамічного моніторингу, що забезпечують високий рівень захисту й кіберстійкості мереж 5G/6G у критичних і промислових середовищах.

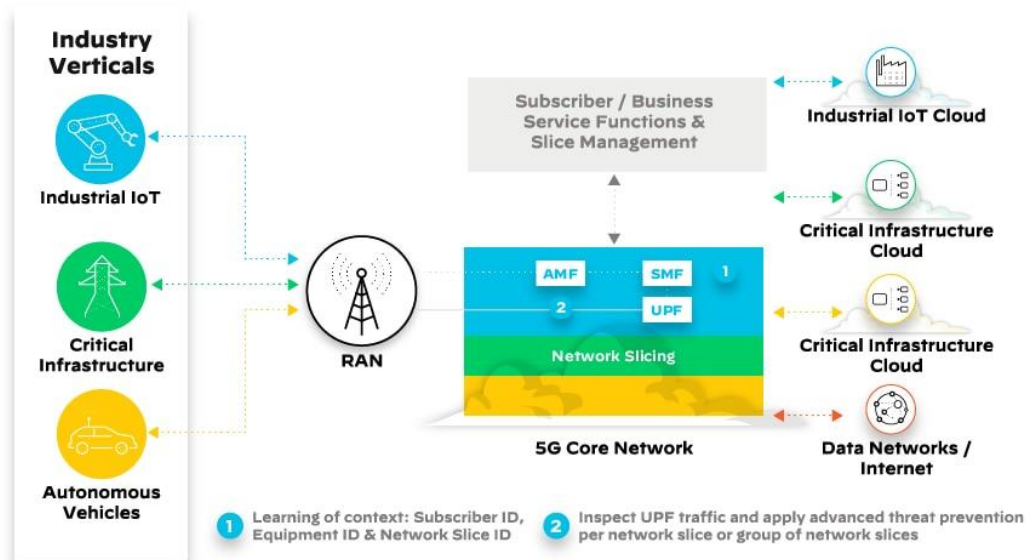


Рис. 1.7. Архітектура безпеки мереж 5G із сегментацією (*network slicing*)
Джерело: [1-10, 18-23]

Архітектура безпеки 5G базується на багаторівневій моделі, у якій функції мережі реалізовані у вигляді віртуалізованих сервісів (NFV – Network Function Virtualization) і контейнеризованих компонентів, що керуються через SDN (Software-Defined Networking). Це дозволяє динамічно розподіляти ресурси, але водночас потребує суворої ізоляції між логічними сегментами — *network slices*, кожен з яких має власні політики безпеки, ключі, засоби моніторингу та рівень довіри. Механізм *slice isolation* гарантує, що порушення в одному сегменті не

призведе до компрометації інших частин мережі, що особливо важливо для критичних застосувань (транспорт, медицина, оборона).

У 5G усунуто низку вразливостей попередніх поколінь. Зокрема, відмовлено від статичних ідентифікаторів абонентів (IMSI), які могли бути перехоплені через псевдобазові станції (*IMSI catchers*). Натомість впроваджено механізм SUCI (Subscription Concealed Identifier), який шифрує ідентифікатор абонента за допомогою асиметричної криптографії, що унеможлиблює відстеження користувачів. Автентифікація здійснюється за допомогою вдосконаленого протоколу EAP-AKA' (Extensible Authentication Protocol – Authentication and Key Agreement Prime), який реалізує двосторонню перевірку справжності як абонента, так і мережі, запобігаючи підміні базових станцій.

Шифрування трафіку у 5G реалізується на рівнях NDS/IP (Network Domain Security), RRC (Radio Resource Control) і NAS (Non-Access Stratum), що забезпечує захист як сигнальних, так і користувацьких даних. Алгоритми 128-NEA і 128-NIA (New Encryption/Integrity Algorithms), засновані на AES і ZUC, гарантують цілісність і конфіденційність передавання. Ключі формуються й оновлюються за допомогою Key Derivation Function (KDF), яка створює унікальні ключі для кожного рівня протоколу й для кожної сесії. Динамічне керування ключами (Key Lifetime Management) дозволяє обмежити час дії криптографічного матеріалу та мінімізувати наслідки компрометації.

Особливістю безпеки 5G є віртуалізоване ядро (5GC), де кожна мережева функція має власні інтерфейси REST API для взаємодії. Це створює нові ризики, пов'язані з атаками на API, тому застосовується шифрування TLS 1.3, автентифікація токенів OAuth2.0, контроль запитів і сегментація доступу. Компоненти управління оркестрацією (MANO – Management and Orchestration) повинні працювати в ізольованих контейнерах із перевіреними образами та контролем цілісності (Trusted Platform Module – TPM).

Протидія DDoS-атакам у 5G реалізується через розподілені системи виявлення та фільтрації трафіку на базі штучного інтелекту. Механізми AI/ML-based Traffic Analytics дозволяють ідентифікувати аномальні шаблони запитів у реальному часі, розрізняючи легітимний трафік від зловмисного. У поєднанні з Network Slicing Security Policies оператор може динамічно обмежувати пропускну здатність підозрілих потоків або перенаправляти їх до ізольованих середовищ аналізу.

У шостому поколінні (6G) рівень безпеки підвищено за рахунок інтеграції Quantum-Resistant Cryptography (криптографія, стійка до квантових атак), а також Physical Layer Security, яка використовує фізичні характеристики сигналу (наприклад, фазові зсуви та шум каналу) для генерації унікальних ключів між пристроями. Важливу роль відіграє Blockchain-based Identity Management, що дозволяє децентралізовано перевіряти справжність пристроїв і керувати

сертифікатами довіри без єдиного центру. 6G також впроваджує AI-native Security, де системи машинного навчання не лише виявляють аномалії, а й адаптивно змінюють політики захисту, прогнозуючи ймовірні атаки за історією поведінки трафіку.

Критичним напрямом у 5G/6G є захист периферійних вузлів (Edge Computing). Оскільки обробка даних дедалі більше переноситься на край мережі, важливо забезпечити автентичність edge-вузлів, шифрування даних при передачі до хмари, а також сегментацію обчислювальних ресурсів між різними користувачами. Для цього використовуються механізми Trusted Execution Environment (TEE) і Secure Boot, які перевіряють цифрові підписи компонентів ще до запуску системи.

З огляду на зростання кількості IoT-пристроїв у 5G-екосистемі, велика увага приділяється захисту mMTC (massive Machine-Type Communications) і URLLC (Ultra-Reliable Low-Latency Communications). Для IoT-вузлів застосовуються полегшені криптографічні схеми, зокрема Elliptic Curve Lightweight Cryptography, а також групове керування ключами для одночасної аутентифікації великої кількості сенсорів.

Управління довірою в 5G/6G реалізовано через концепцію Zero Trust Architecture (ZTA), згідно з якою жоден компонент або користувач не вважається надійним за замовчуванням. Кожен запит, незалежно від його походження, підлягає перевірці, автентифікації та авторизації. Таке управління підтримується централізованими консолями Security Orchestration, Automation and Response (SOAR), що дозволяють координувати реакції на інциденти та автоматично блокувати компрометовані сегменти мережі.

Ключовими напрямками розвитку безпеки в 6G є інтеграція цифрових близнюків (Digital Twins) для моделювання атак, використання Federated Learning для колективного навчання моделей виявлення аномалій без передачі даних, а також застосування Zero-knowledge proofs (ZKP) для анонімної автентифікації користувачів. Ці механізми сприяють формуванню глибоко інтегрованої системи кіберзахисту, де інтелектуальні алгоритми прогнозують загрози, а система самостійно перебудовує політику безпеки у відповідь на зміни середовища.

Отже, захист мереж 5G/6G — це комплексна система, яка об'єднує віртуалізацію, сегментацію, динамічне шифрування, інтелектуальне виявлення атак, квантово-стійку криптографію та концепцію Zero Trust. Вона формує самонавчальну екосистему безпеки, здатну забезпечувати конфіденційність, цілісність, доступність і стійкість зв'язку у масштабних розподілених інфраструктурах майбутнього.

Отже, захист безпроводових технологій потребує багаторівневого підходу, що поєднує криптографічні методи, механізми автентифікації, контроль доступу, сегментацію мереж і постійний моніторинг безпеки. Особливості кожного

стандарту зумовлюють необхідність використання спеціалізованих рішень, спрямованих на мінімізацію ризиків, збереження цілісності та забезпечення довіри у бездротовому середовищі передачі даних.

1.2. ЗАГРОЗИ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ (IoT) І СЕНСОРНИХ МЕРЕЖ (WSN)

Інтернет речей (IoT) і бездротові сенсорні мережі (WSN) підпадають під широкий спектр загроз, які охоплюють усі елементи їхнього життєвого циклу — від виробництва й постачання апаратних компонентів до експлуатації, оновлення й утилізації пристроїв; ці загрози можна розглядати через призму конфіденційності, цілісності, доступності та довіри. На рівні пристроїв найбільш поширеними є проблеми дефолтних або слабких облікових даних і незмінюваних заводських паролів, що дають змогу зловмисникам отримати первинний доступ; відсутність або некоректна реалізація механізмів secure boot і перевірки підписів прошивки дозволяє завантажити підроблене ПЗ або бекдору, а брак апаратного кореня довіри (TPM/SE/TEE) робить неможливим надійне зберігання ключів і генерацію ентропії. Фізичне захоплення вузлів у польових умовах (node capture) призводить до екстракції секретів, зворотного інжинірингу й подальшого використання пристроїв як плацдарму для атак у мережі. Через енергетичні обмеження багато сенсорних вузлів використовують полегшені криптопротоколи або зовсім їх уникають, що створює вразливість до криптографічних атак, replay-атак і підміни повідомлень.

На рівні мережі IoT/WSN існує набір специфічних атак на протоколи і маршрутизацію: sinkhole (приховане приваблення трафіку через зловмисний вузол), wormhole (створення тунелю між віддаленими точками для спотворення топології), HELLO-flood і selective forwarding, що підривають коректну доставку пакетів і дозволяють перехоплювати або втрачати дані. Sybil-атаки, коли один пристрій представляє кілька ідентичностей, підривають механізми голосування, маршрутизації на основі репутації і розподілу навантаження. Перешкоди на фізичному рівні (jamming) і енергетичні атаки (sleep-deprivation, battery draining) спрямовані на доступність мережі й можуть вивести з ладу цілі сегменти мережі або вимусити повторні підключення, що відкриває додаткові вектори атак.

Шлюзи й краєві вузли (edge gateways) — критична зона ризику: вони з'єднують локальні сенсорні мережі з корпоративними мережами й хмарними сервісами, тож компрометація шлюзу дає зловмисникам доступ до широкого набору даних і команд. Типові загрози тут — MITM між вузлом і шлюзом, компрометація облікових даних для API, використання незашифрованих або слабо захищених протоколів (наприклад, небезпечні конфігурації MQTT/CoAP), а також уразливості в контейнеризованих сервісах і оркестрації.

У хмарному шарі атаки на облікові записи, витік сертифікатів і неправильно налаштовані політики доступу дозволяють маніпулювати конфігурацією пристроїв, масово оновлювати їх під шкідливі прошивки або витягувати чутливі дані.

Життєвий цикл пристрою додає власні ризики на етапах виробництва та постачання: шкідливі компоненти, вбудовані бекдори або модифікації прошивок постачальниками в ланцюзі поставок (supply-chain compromise). Відсутність прозорості й відсутність SBOM (software bill of materials) для вбудованого ПО ускладнює виявлення таких проблем. На етапі decommissioning некоректне видалення секретів і даних робить можливим їх відновлення і повторне використання пристроїв у злочинних цілях.

Наслідки атак на IoT/WSN можуть бути надзвичайно серйозними: від витоку персональних і медичних даних до фізичних наслідків — порушення роботи промислового обладнання, збої в енергетичних мережах, аварії транспортних систем. Пристрої, інфіковані ботнетами (Mirai та аналогічні), використовуються для масштабних DDoS-кампаній, що паралізує критичну інфраструктуру і знижує довіру до сервісу. Правові і регуляторні наслідки (штрафи за недотримання GDPR чи локальних норм) та репутаційні втрати також є суттєвим ризиком для власників рішень IoT.

Для ефективного зниження ризиків необхідний багаторівневий підхід, що поєднує технічні, процесні та організаційні заходи. На рівні пристрою обов'язкові: унікальна ідентифікація пристроїв і відмова від заводських паролів, апаратний root of trust (TPM/SE/TEE), secure boot і підписання прошивок, механізми tamper-detection, можливість віддаленого стирання секретів і безпечні OTA-оновлення з rollback-захистом. Криптографія має бути правильно підбраною: використання ECC/ECDH для ключового обміну, AES (або його полегшених варіантів для низькоресурсних пристроїв) для симетричного шифрування, використання nonce/лічильників кадрів і MIC для захисту від replay-атак, а також регулярна ротація ключів і політики відкликання. Для пристроїв з обмеженими ресурсами застосовують стандартизовані lightweight-протоколи та апаратні прискорювачі криптографії.

На мережевому рівні ключові заходи — сегментація мережі (VLAN/VRF/SDN-політики) з чітким розділенням IoT-сегментів від критичних IT-систем, застосування захищених каналів (DTLS/TLS/mTLS) до шлюзів і хмари, а також контроль доступу на основі мінімальних привілеїв. Протоколи маршрутизації повинні включати автентифікацію вузлів та валідацію оновлень маршруту, захист від wormhole і sinkhole через часові перевірки, геолокаційні співставлення або latency-based detection. Для захисту від DoS слід впровадити rate-limiting, edge-фільтрацію і можливість «blackholing» підозрілих потоків.

На рівні шлюзів і хмари важливо реалізувати жорстку гартовану конфігурацію (hardened images), mTLS для взаємної автентифікації, менеджмент секретів (vault), клієнтське і серверне логування з кореляцією подій у SIEM/SOAR, а також обмеження API через WAF, rate limiting і OAuth2/mTLS. Моніторинг телеметрії і поведінки пристроїв повинен включати збір heartbeat, метрик використання ресурсів, частоти повторних підключень і відхилень від типової поведінки; для виявлення аномалій корисні ML/AI-моделі, але їх треба навчати на правильних і контрольованих наборах даних та застосовувати з урахуванням ризику фальшивих позитивів.

Організаційні заходи охоплюють threat modeling (STRIDE/PASTA), вимоги до постачальників (SCRM), впровадження життєвого циклу пристрою з визначенням процедур provisioning, оновлення, моніторингу і decommissioning, регулярне тестування (penetration testing, fuzzing, firmware analysis) і наявність плану реагування на інциденти з playbook-ами для IoT. Важливим є вимагати від постачальників SBOM, прозорості щодо криптографічних компонентів і підтвердження практик secure manufacturing.

Практичні контрзаходи проти конкретних атак включають: для replay — механізми nonce/лічильників кадрів і короткі сесії; проти wormhole — time/latency checks і локальна валідація сусідства; проти sinkhole і Sybil — authenticated routing, reputation scoring і обмеження ролей пристроїв; проти relay/relay-like атак — distance-bounding, time-of-flight validation і challenge-response з лічильниками. Для мінімізації впливу компрометації пристрою необхідно впровадити механізми швидкого відкликання сертифікатів і ключів та автоматичної ізоляції вузла мережею при виявленні аномалій.

Загрози для Інтернету речей (IoT)

Загрози для Інтернету речей (IoT) охоплюють як технічні, так і організаційні аспекти безпеки, оскільки екосистема IoT складається з великої кількості взаємопов'язаних пристроїв, сенсорів, шлюзів і хмарних сервісів. Кожен компонент може стати точкою входу для атаки, що робить IoT особливо вразливим у порівнянні з традиційними IT-системами.

На рис. 1.8 представлено ключові ризики, які загрожують безпеці екосистеми Інтернету речей. У центрі схеми зображено хмару, що символізує ядро IoT-інфраструктури — середовище, де відбувається обробка, передавання та зберігання даних між пристроями, шлюзами і хмарними сервісами. Навколо неї розміщені основні категорії загроз, що формують комплексну картину ризиків. До першої групи належать небезпечні мережеві сервіси (Insecure Network Services), які виникають через відсутність захищених протоколів, відкриті порти, слабкі налаштування маршрутизаторів або некоректну фільтрацію трафіку. Такі вразливості створюють умови для перехоплення даних, атак типу DDoS і несанкціонованого доступу. Другий ризик пов'язаний

із відсутністю безпечних оновлень (Lack of Secure Updates). Багато IoT-пристроїв не підтримують регулярне оновлення прошивок або мають механізми оновлення без цифрового підпису, що дозволяє зловмисникам впроваджувати шкідливе ПЗ. Третім аспектом є використання ненадійних компонентів (Use of Insecure Components), коли у систему інтегруються сторонні модулі, бібліотеки чи мікроконтролери без належної перевірки безпеки. Це створює потенційні бекдори й точки компрометації системи. Четвертим ризиком виступає небезпечна передача даних (Insecure Data Transfer). Відсутність шифрування або автентифікації під час обміну інформацією між пристроями, шлюзами чи хмарними платформами може призвести до втрати конфіденційності, підміни пакетів або їхнього перехоплення.

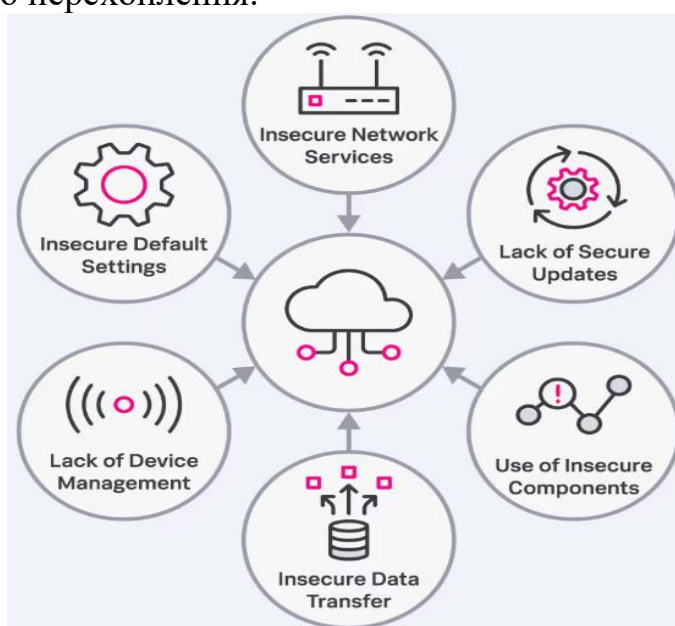


Рис. 1.8. Основні ризики безпеки Інтернету речей (IoT Security Risks)
Джерело: [1-10, 18-23, 45-72, 85-93]

П'ятий фактор стосується недостатнього управління пристроями (Lack of Device Management). У великих IoT-середовищах без централізованих засобів моніторингу й оновлення виникає складність виявлення заражених або несанкціоновано підключених пристроїв, що сприяє поширенню ботнетів. Останньою загрозою є небезпечні налаштування за замовчуванням (Insecure Default Settings), коли виробники залишають стандартні паролі або відкриті сервіси, які користувачі не змінюють після інсталяції. Це робить пристрої легкою мішенню для автоматизованих атак. Таким чином, рисунок відображає взаємопов'язану структуру вразливостей IoT-середовища, де порушення безпеки на будь-якому рівні — від пристрою до хмарної інфраструктури — може призвести до компрометації всієї системи. Комплексне усунення

перелічених ризиків є ключовою умовою створення надійної та стійкої екосистеми Інтернету речей.

Найпоширенішими є загрози конфіденційності, які виникають через несанкціонований збір і передачу даних користувачів. Пристрої розумних домів або носимі гаджети можуть передавати інформацію про місцезнаходження, біометричні показники або поведінкові шаблони без згоди власника. У промислових системах це може призвести до витоку технологічних даних і комерційних таємниць.

Загрози цілісності пов'язані зі спотворенням або підміною даних. У сенсорних мережах підроблення телеметричних показників може викликати неправильні рішення систем керування, наприклад, хибну реакцію автоматизованих систем безпеки або аварію обладнання. Маніпуляції з даними часто супроводжуються атаками типу *man-in-the-middle (MITM)* або підміною вузлів (*spoofing*), коли злоумисник перехоплює або модифікує інформацію між сенсором і сервером.

Загрози доступності (DoS/DDoS) є одними з найсерйозніших для IoT. Через обмеженість ресурсів пристрої легко перевантажити запитами або примусити до безперервних обчислень, що виснажує їхні батареї. Масове зараження IoT-пристроїв шкідливими кодами формує ботнети, такі як Mirai, які використовуються для масштабних DDoS-атак на вебсервери, інфраструктуру або хмарні сервіси.

Компрометація автентичності та довіри відбувається, коли злоумисник видає себе за легітимний пристрій. Типові приклади — *Sybil-атаки*, коли один вузол створює кілька фіктивних ідентичностей, або *sinkhole-атаки*, коли атакуювальний пристрій приваблює трафік, перенаправляючи його через себе для перехоплення або модифікації. Без належної взаємної аутентифікації та контролю сертифікатів такі атаки можуть повністю порушити логіку маршрутизації та розподіл довіри.

Фізичні загрози для IoT і сенсорних мереж пов'язані з прямим доступом до пристроїв. Злоумисник може вилучити мікроконтролер, зчитати флеш-пам'ять і отримати криптографічні ключі. Атаки побічних каналів (*side-channel*) дозволяють відновити секретні дані через аналіз часу виконання, споживання енергії або електромагнітного випромінювання.

Загрози ланцюга постачання (*supply chain*) проявляються у випадках, коли в пристрій ще на етапі виробництва або оновлення прошивки вбудовується шкідливий код чи бекдор. Компрометація вендора або використання неперевіраних компонентів ставить під загрозу всю систему.

Окрему групу становлять загрози хмарних платформ IoT, де відбувається збирання та обробка даних. Атаки на API, слабкі токени авторизації або відкриті

порти управління дозволяють зловмисникам отримати доступ до конфігурацій пристроїв, витягнути журнали або видалено керувати вузлами.

До поведінкових і соціоінженерних загроз належать фішингові атаки на адміністраторів IoT-платформ, несанкціоноване підключення до публічних мереж Wi-Fi або підміна мобільних застосунків для керування пристроями. Через необізнаність користувачів чи відсутність політик безпеки зловмисники можуть використати відкриті Bluetooth-з'єднання, відкриті NFC-інтерфейси або стандартні паролі для доступу до пристроїв.

Вразливість IoT поглиблюється через відсутність централізованого оновлення програмного забезпечення. Багато пристроїв мають обмеження на встановлення патчів, тому залишаються з відомими уразливостями, що активно експлуатуються.

На рис. 1.9 подано класифікацію основних загроз безпеці в екосистемі Інтернету речей (IoT) за рівнями архітектури: рівень сприйняття (Perception Layer), мережевий рівень (Network Layer), рівень підтримки (Support Layer) та рівень застосунків (Application Layer). Такий підхід дозволяє зрозуміти, які типи атак характерні для кожного рівня системи IoT і яким чином вони впливають на цілісність, доступність і конфіденційність даних.

На рівні сприйняття (Perception Layer), який охоплює сенсори, RFID-мітки та інші пристрої збору даних, основними загрозами є підміна пристроїв (Spoofing), глушіння сигналу (Signal jamming / Radio jamming) та захоплення вузлів (Node capturing / Node outage). Ці атаки спрямовані на фізичний доступ або порушення роботи сенсорів, що може призвести до викривлення чи втрати критичних даних.

На мережевому рівні (Network Layer) зосереджуються загрози, пов'язані з передаванням інформації між пристроями та шлюзами. До них належать атаки на протоколи маршрутизації та адресації (Threats to NDP protocol), атаки під час передавання даних (Data transit attacks) та атаки типу відмова в обслуговуванні (Routing and DoS Attacks). Такі дії можуть блокувати комунікацію між вузлами, перехоплювати пакети або створювати затори в мережі.

Рівень підтримки (Support Layer), що включає сервери, шлюзи та хмарні сервіси, є вразливим до підміни або модифікації даних (Data Tempering) та несанкціонованого доступу (Unauthorized access). Ці загрози часто пов'язані з відсутністю контролю автентифікації або недостатнім шифруванням, що дозволяє зловмисникам маніпулювати переданою інформацією чи отримувати доступ до систем управління.

На рівні застосунків (Application Layer), який відповідає за користувацьку взаємодію, аналітику та керування пристроями, поширеними є ін'єкція шкідливого коду (Malicious code injection), порушення цілісності даних та мультикористувацького доступу (Integrity, Multi-user access) і перехоплення

сесій (Session Hijacking). Ці атаки можуть призвести до втрати довіри користувачів, крадіжки конфіденційної інформації або повного компрометування системи. Таким чином, рисунок відображає багаторівневу структуру загроз для IoT, підкреслюючи необхідність комплексного підходу до захисту — від фізичного рівня сенсорів до програмних застосунків. Кожен рівень потребує власних механізмів безпеки, а їхня інтеграція забезпечує цілісність, стійкість і надійність інтелектуальних систем.

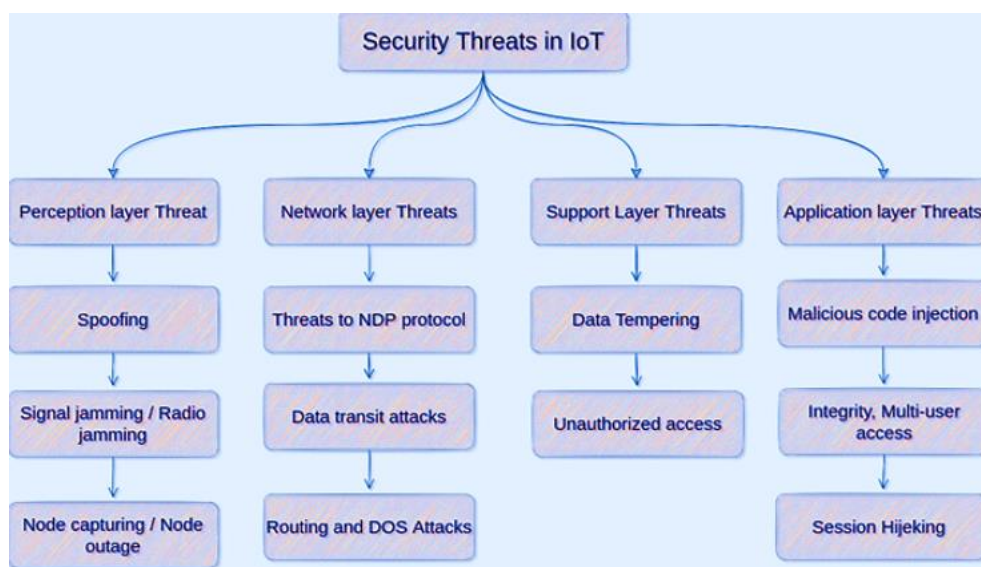


Рис. 1.9. Загрози безпеці в Інтернеті речей (Security Threats in IoT)
Джерело: [1-10, 18-23, 45-72, 85-93]

Загалом загрози для Інтернету речей формують складну багаторівневу картину, де кожен рівень — від фізичного до хмарного — може бути джерелом ризику. Для ефективного захисту необхідно впроваджувати комплексну стратегію: шифрування трафіку на всіх рівнях, багатофакторну автентифікацію, сегментацію мереж, контроль цілісності прошивок, моніторинг подій, регулярні оновлення безпеки й аудит ланцюгів постачання. Такий підхід забезпечує цілісність, конфіденційність і доступність систем IoT, що є критично важливими для стійкості сучасних інформаційно-комунікаційних середовищ.

Захист Інтернету речей (IoT)

Захист Інтернету речей (Internet of Things, IoT) — це комплексна система технічних, криптографічних, мережових і організаційних заходів, спрямованих на забезпечення конфіденційності, цілісності, доступності та довіри в екосистемі взаємопов'язаних пристроїв. Особливість IoT полягає у великій кількості гетерогенних вузлів — від сенсорів і мікроконтролерів до шлюзів і хмарних платформ, — які взаємодіють у реальному часі через бездротові або дротові мережі. Водночас більшість пристроїв мають обмежені ресурси

обчислень, енергоспоживання та пам'яті, що ускладнює впровадження традиційних механізмів кіберзахисту.

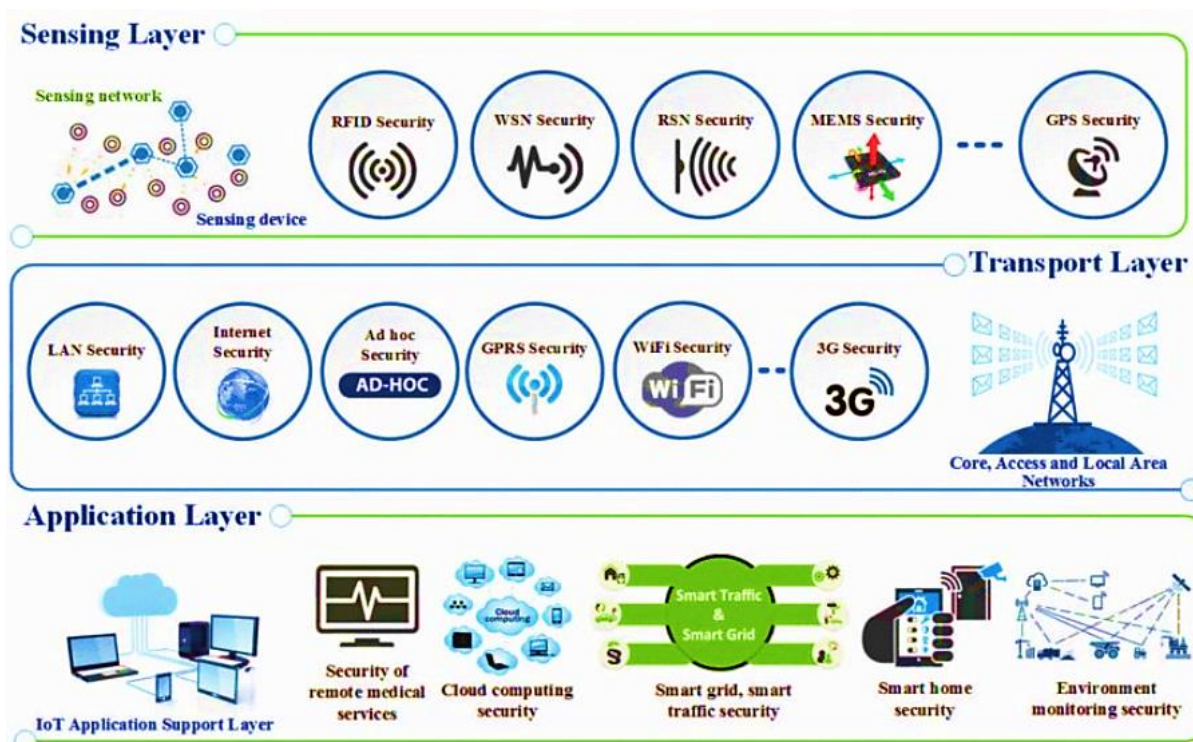


Рис. 1.10. Багаторівнева архітектура безпеки Інтернету речей (IoT)
Джерело: [1-10, 18-23]

На рис. 1.10 подано узагальнену архітектуру безпеки IoT, що складається з трьох взаємопов'язаних рівнів: сенсорного, транспортного та прикладного. Сенсорний рівень охоплює захист пристроїв збору даних — RFID-міток, сенсорних вузлів, мікромеханічних систем і GPS-модулів. Його мета полягає у запобіганні підміні пристроїв, перехопленню сигналів і несанкціонованому доступу до сенсорів. Транспортний рівень забезпечує безпечне передавання інформації між вузлами, шлюзами та хмарними сервісами за допомогою технологій LAN, Wi-Fi, GPRS, 3G і VPN-тунелів, використовуючи шифрування та автентифікацію для захисту від атак типу «людина посередині». Прикладний рівень відповідає за захист даних і сервісів у розумних системах — транспорті, енергомережах, медицині, «розумному домі» та екологічному моніторингу. Тут реалізуються політики контролю доступу, шифрування з кінця в кінець, токенизація даних і захист хмарних платформ. У сукупності ці три рівні формують комплексну модель безпеки IoT, у якій захист інтегровано від сенсора до хмарної аналітики.

Захист IoT-середовища починається з фізичного рівня, де необхідно запобігати несанкціонованому доступу до пристроїв. Пристрої повинні мати

захищені корпуси, сенсори втручання (tamper detection), а їхні мікроконтролери — підтримку функцій Secure Boot, Trusted Execution Environment (TEE) або Hardware Security Module (HSM) для зберігання ключів. Цифрові підписи прошивок забезпечують перевірку цілісності під час завантаження, що унеможливорює підміну програмного коду. Важливо також фізично обмежувати доступ до портів (USB, UART, JTAG), щоб запобігти перепрограмуванню пристрою або зчитуванню даних з пам'яті.

На мережевому рівні безпека реалізується через шифрування каналів зв'язку (TLS, DTLS, IPsec, VPN), автентифікацію пристроїв і сегментацію трафіку. Мережа IoT поділяється на ізольовані підмережі VLAN або SDN-сегменти, що мінімізує наслідки компрометації одного вузла. Для управління трафіком використовуються файрволи, IDS/IPS та SIEM-системи, які виявляють аномалії або підозрілі з'єднання. Важливим елементом є Zero Trust Architecture, яка передбачає, що жоден пристрій не вважається надійним за замовчуванням — кожен запит проходить перевірку автентичності, авторизації та контекстного аналізу.

Криптографічний захист у IoT ґрунтується на використанні легковагових алгоритмів (Lightweight Cryptography), адаптованих для пристроїв з низькими ресурсами. Найпоширенішими є AES-CCM, ChaCha20-Poly1305, Elliptic Curve Cryptography (ECC), PRESENT, SPECK і SIMON. Для обміну ключами використовуються протоколи ECDH (Elliptic Curve Diffie–Hellman) або PSK (Pre-Shared Keys). Важливою тенденцією є впровадження квантово-стійких алгоритмів (Post-Quantum Cryptography) у промислових IoT-системах, щоб забезпечити довготривалу безпеку. Управління ключами здійснюється через централізовані PKI-інфраструктури, де сертифікати видаються і перевіряються автоматично, або за допомогою blockchain-рішень для децентралізованої ідентифікації пристроїв.

На рівні застосунків безпека передбачає автентифікацію користувачів і сервісів, контроль доступу та захист даних під час їхньої обробки. Для цього застосовуються політики Role-Based Access Control (RBAC) або Attribute-Based Access Control (ABAC), які враховують контекст запиту (місце, час, тип пристрою). Дані шифруються end-to-end між сенсорними вузлами, шлюзами та хмарними сервісами. Для хмарних платформ важливими є механізми multi-tenant isolation, моніторинг API-запитів, виявлення DDoS-атак і контроль цілісності контейнеризованих сервісів (Docker, Kubernetes).

Захист шлюзів і хмарної інфраструктури є критично важливим, адже вони виступають центральними вузлами агрегації трафіку. Шлюзи мають підтримувати двофакторну автентифікацію, обмеження адміністративного доступу, журналювання подій і регулярне оновлення безпеки. У хмарних IoT-платформах (AWS IoT, Azure IoT Hub, Google Cloud IoT Core) обов'язково

впроваджується багаторівневе шифрування даних, контроль політик доступу IAM (Identity and Access Management) і системи моніторингу безпеки (Cloud SIEM, Security Center).

Особливу увагу приділяють виявленню аномалій і реагуванню на інциденти. Алгоритми машинного навчання (ML) аналізують поведінку пристроїв, виявляючи нетипові шаблони комунікації, які можуть свідчити про зараження ботнетом (Mirai, Mozi, Hajime). Сучасні IDS/IPS-системи для IoT здатні динамічно оновлювати правила виявлення та автоматично ізолювати підозрілі пристрої. Для промислового IoT (IIoT) використовуються спеціалізовані рішення OT Security (Nozomi Networks, Claroty, Dragos), що контролюють SCADA- і PLC-компоненти.

Важливою складовою є захист даних і приватності користувачів. IoT-пристрої повинні відповідати вимогам GDPR, ISO/IEC 27001 та ISO/IEC 27400, що визначають принципи безпечного зберігання, мінімізації та шифрування персональних даних. Для забезпечення прозорості використовується токенизація або псевдонімізація ідентифікаторів користувачів.

Не менш важливими є організаційні та процедурні заходи: регулярне оновлення прошивок, проведення аудитів безпеки, застосування Secure Development Lifecycle (SDL) у розробці IoT-програм, використання перевірених бібліотек і тестування на проникнення. Адміністратори повинні впроваджувати системи централізованого управління IoT-пристроями (IoT Device Management), що дозволяють контролювати конфігурацію, оновлення, журналювання та відкликання сертифікатів.

На рис. 1.11 представлено шість основних принципів кібербезпеки IoT, які охоплюють увесь технологічний стек — від фізичних пристроїв до хмарних сервісів і прикладних застосунків. Перший принцип, Secure Device (Hardware), передбачає захист на рівні пристрою шляхом використання апаратної ідентифікації, захищеного завантаження (Secure Boot), модулів довіреного виконання (TEE) та інтелектуального керування на рівні краю мережі (Edge Processing). Другий принцип, Secure Communications, забезпечує безпечну взаємодію між пристроями, шлюзами та хмарою завдяки автентифікації, ініціації з'єднання лише з перевірених вузлів і контролю обміну повідомленнями через зашифровані канали (TLS, DTLS, VPN). Третій принцип, Secure Cloud, охоплює захист даних під час їхнього зберігання та обробки у хмарних платформах, включно з автентифікацією, авторизацією, шифруванням і багаторівневим контролем доступу. Четвертий принцип, Secure Lifecycle Management, передбачає безпечне керування життєвим циклом IoT-пристроїв — від оновлень прошивок до віддаленого моніторингу та відкликання сертифікатів. П'ятий і шостий принципи пов'язані з ідентифікацією, управлінням довірою та аналітикою безпеки, що дозволяють контролювати всі

елементи екосистеми IoT — користувача, пристрій, шлюз, з'єднання, хмару й застосунки. Сукупність цих принципів формує цілісну систему кіберзахисту, у якій безпека інтегрована на кожному етапі функціонування IoT-рішень — від апаратного рівня до корпоративних інформаційних систем.

Six principles of IoT Cyber Security across the stack

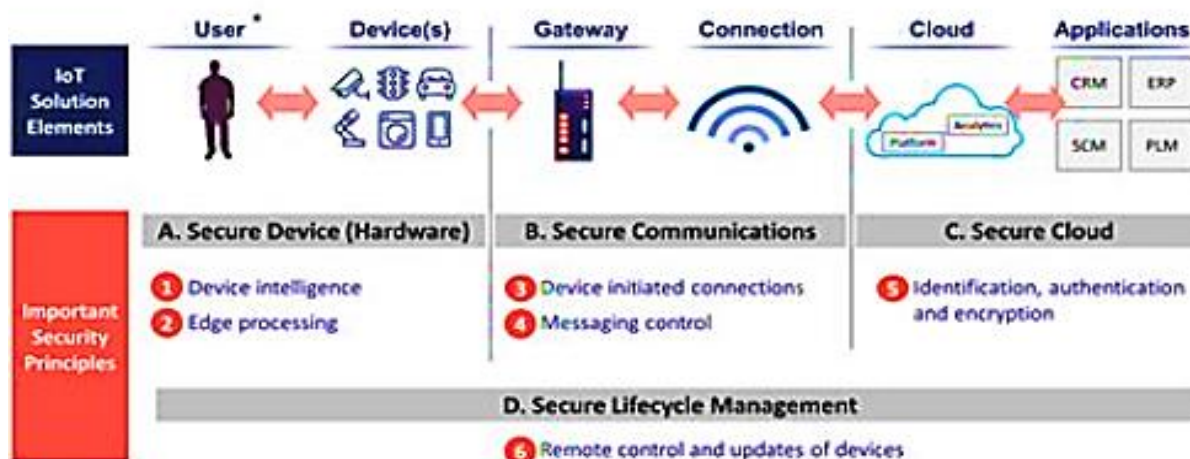


Рис. 1.11. Шість принципів кібербезпеки Інтернету речей (IoT) на всіх рівнях архітектури

Джерело: [1-10, 18-23]

Таким чином, ефективний захист IoT-систем базується на принципах багаторівневості, довіри за нульовим припущенням (Zero Trust), шифрування, поведінкового аналізу та автоматизації реагування. Поєднання технічних і організаційних засобів дозволяє створити стійку до кіберзагроз екосистему, у якій безпека інтегрована на кожному етапі — від сенсора до хмарної аналітики, забезпечуючи стабільність, надійність і захист критичних даних у цифровому середовищі.

Загрози для сенсорних мереж (WSN)

Сенсорні мережі (Wireless Sensor Networks, WSN) є однією з найвразливіших складових Інтернету речей, оскільки вони складаються з великої кількості малопотужних вузлів, що працюють у розподіленому середовищі з обмеженими ресурсами енергії, пам'яті та обчислювальної потужності. Ці особливості зумовлюють специфічний набір загроз, які впливають на конфіденційність, цілісність, доступність та достовірність переданих даних, а також на стабільність і надійність самої мережі.

Однією з головних проблем WSN є відсутність централізованого контролю, що відкриває простір для атак на маршрутизацію. Типовими є

sinkhole-атаки, коли зловмисний вузол рекламує себе як найкоротший або найнадійніший маршрут для трафіку, змушуючи інші вузли передавати через нього пакети. У результаті зловмисник може перехоплювати, змінювати або знищувати дані. Іншим поширеним видом є wormhole-атака, коли два зловмисники створюють тунель між різними частинами мережі, спотворюючи її топологію та викликаючи перенаправлення даних через контрольований канал. Такі атаки призводять до порушення синхронізації та розриву мережевої маршрутизації.

Selective forwarding (вибіркове пересилання) — ще одна небезпечна загроза, за якої вузол-зловмисник вибірково передає лише частину отриманих пакетів, блокуючи інші. Це ускладнює виявлення інцидентів, оскільки мережа продовжує функціонувати, але дані спотворюються. Схожим за природою є blackhole-атака, коли всі пакети, що потрапляють до певного вузла, безслідно відкидаються. У свою чергу, Sybil-атака дозволяє одному вузлу створити декілька фіктивних ідентичностей, порушуючи принципи автентифікації та унеможливаючи достовірне голосування при виборі маршрутів або кластерних голів.

Окрему категорію становлять атаки на рівні енергоспоживання, які спрямовані на виснаження ресурсів вузлів. Наприклад, sleep deprivation змушує пристрій залишатися активним і обробляти безперервні запити, що призводить до швидкого розрядження батареї. HELLO flood-атака використовує фальшиві широкомовні повідомлення “hello” для створення перевантаження каналів і заповнення таблиць сусідів неправдивими записами. Такі атаки ефективно виводять із ладу частину мережі, зменшуючи її покриття та ефективність.

Не менш небезпечними є фізичні загрози, оскільки сенсорні вузли часто розташовуються у відкритих або важкодоступних місцях. Зловмисник може отримати фізичний доступ до вузла, зчитати вміст пам'яті, змінити прошивку або навіть замінити пристрій власним. Фізичне захоплення одного вузла може поставити під загрозу всю мережу, якщо у ньому зберігаються спільні ключі шифрування чи маркери автентифікації. Такі атаки доповнюються атаками побічних каналів (side-channel attacks) — зчитуванням інформації через електромагнітне випромінювання, часові затримки або коливання споживання енергії.

Додатковим чинником є обмеженість криптографічних механізмів. Через обмежені ресурси WSN часто використовують спрощені або застарілі алгоритми, що не забезпечують належного рівня захисту. Відсутність надійного управління ключами робить можливим replay-атаки, коли зловмисник повторно надсилає старі дійсні пакети, видаючи їх за нові. Унаслідок цього система може повторно виконати команди або сприйняти застарілі дані як актуальні.

Атаки на цілісність даних часто супроводжуються підміною або спотворенням інформації, що може мати критичні наслідки у системах моніторингу. Наприклад, у промислових або екологічних мережах спотворення показників температури, тиску чи вологості може викликати неправильну реакцію системи керування або подання хибних звітів. Такі маніпуляції особливо небезпечні у критичних системах, пов'язаних із охороною здоров'я чи безпекою.

Загрози доступності виявляються у вигляді DoS- або DDoS-атак, що можуть бути реалізовані як через перевантаження вузлів фальшивими пакетами, так і через навмисне створення колізій у радіоканалі (jamming). У результаті справжні пакети втрачаються, мережа розпадається на ізольовані сегменти, а час доставки повідомлень різко зростає.

Для мінімізації цих загроз застосовуються комплексні заходи безпеки: автентифікація вузлів при приєднанні до мережі, використання криптографічного захисту з легкими алгоритмами (наприклад, ECC або AES з короткими сесіями), регулярна ротація ключів, обмеження кількості сусідніх з'єднань і контроль маршрутизації. Важливим є впровадження механізмів виявлення вторгнень (IDS), які аналізують поведінку вузлів і виявляють аномалії, наприклад, нетипові частоти передачі даних або спроби змінити маршрути.

Загалом, сенсорні мережі потребують багаторівневого підходу до безпеки, який поєднує криптографічні засоби, моніторинг активності, захист фізичних пристроїв і правильну архітектуру мережевої взаємодії. Тільки інтегрований підхід — від проектування до експлуатації — дозволяє забезпечити цілісність, конфіденційність і доступність даних у середовищах WSN, які часто є основою сучасних систем автоматизації, екологічного моніторингу, "розумних міст" і промислових IoT-рішень.

Захист сенсорних мереж (WSN)

Захист сенсорних мереж (Wireless Sensor Networks, WSN) є одним із ключових напрямів забезпечення кібербезпеки сучасних розподілених систем, адже сенсорні вузли часто працюють у ворожому або неконтрольованому середовищі, збираючи важливі дані для систем моніторингу, автоматизації чи критичної інфраструктури. Основною особливістю WSN є обмеженість енергетичних, обчислювальних і пам'яттєвих ресурсів вузлів, що ускладнює впровадження класичних механізмів захисту. Тому безпека сенсорних мереж повинна будуватися як багаторівнева система, яка поєднує криптографічні, архітектурні, поведінкові та фізичні методи захисту.

На фізичному рівні головна мета полягає у запобіганні несанкціонованому доступу до вузлів і зменшенні ризику перехоплення сигналів. Для цього застосовують захищені корпуси з сенсорами розтину, що автоматично

видаляють криптографічні ключі при спробі фізичного втручання. Потужність передавача обмежується для мінімізації зони випромінювання, а динамічне перемикання частот або резервні канали зв'язку дозволяють протидіяти глушінню сигналу. Виявлення сторонніх джерел здійснюється шляхом аналізу рівня потужності сигналу та часових характеристик передавання, що дозволяє ідентифікувати потенційних порушників.

На каналному рівні реалізується захист від підробки кадрів, повторного відтворення пакетів і атак типу “відмова в обслуговуванні”. Для цього використовують симетричне шифрування (AES-CCM, Speck, Skipjack) та лічильники кадрів, які запобігають replay-атакам. Джерело даних підтверджується шляхом автентифікації, а частотний аналіз і контроль кількості передач дозволяють виявити спроби навмисного перевантаження вузла.

На мережевому рівні основна увага зосереджується на захисті маршрутів від атак типу sinkhole, wormhole, Sybil і selective forwarding. Для цього впроваджується обов'язкова автентифікація вузлів при приєднанні до мережі, цифрові підписи, криптографічна перевірка маршрутів і репутаційні механізми, які дозволяють ідентифікувати вузли з підозрілою поведінкою. Розподіл ключів може здійснюватися за допомогою попереднього розгортання (key predistribution) або протоколів на основі еліптичних кривих (ECDH), що забезпечують стійкість навіть за обмежених обчислювальних можливостей. Сегментація мережі й кластеризація вузлів дозволяють ізолювати скомпрометовані ділянки без порушення роботи всієї системи.

На транспортному рівні захист спрямований на запобігання несанкціонованим з'єднанням і збереження цілісності даних під час обміну між сенсорними вузлами та шлюзами. Для цього використовується шифрування транспортних пакетів із кодами перевірки достовірності (HMAC), обмежується тривалість сеансів і кількість одночасних з'єднань, а довготривалі сеанси супроводжуються повторною автентифікацією.

Прикладний рівень зосереджений на перевірці достовірності джерел інформації, контролі цілісності даних і запобіганні підміні сенсорів. Дані шифруються end-to-end перед передаванням, застосовуються цифрові підписи, а системи виявлення аномалій з використанням методів машинного навчання або нечіткої логіки аналізують поведінкові відхилення у трафіку, що дозволяє виявляти скомпрометовані вузли. Репутаційні механізми дають змогу оцінювати довіру до вузлів і фільтрувати потенційно недостовірні повідомлення.

Ключовим компонентом безпеки є управління криптографічними ключами. Через обмежені ресурси вузлів у WSN використовуються легковагові алгоритми (ECC, PRESENT, SIMON, SPECK), що забезпечують достатній рівень стійкості при низькому споживанні енергії. Регулярна ротація ключів і

використання апаратних генераторів випадкових чисел запобігають повторному використанню ключів і підвищують стійкість системи до криптоаналітичних атак.

Оскільки сенсорні мережі часто розгортаються у середовищах із підвищеним ризиком, важливу роль відіграють системи моніторингу та реагування. Системи виявлення вторгнень (IDS) аналізують структуру трафіку, час передачі, рівень сигналу та кількість пересилань, виявляючи відхилення, характерні для атак або збоїв. Журнали подій регулярно відправляються на центральний сервер або хмарну платформу для подальшого аналізу, а скомпрометовані вузли автоматично ізолюються з мережі.

Додатково застосовуються організаційно-технічні заходи, такі як регулярне оновлення прошивок і перевірка їх цифрових підписів, аудит безпеки, тестування на проникнення, використання сертифікованих алгоритмів за стандартами ISO/IEC 29192 та IEEE 802.15.4, а також розмежування повноважень між адміністраторами.

На рис. 1.12 зображено архітектуру захищеної сенсорної мережі (WSN), у якій реалізовано комплексний підхід до безпеки через використання технологій тунелювання, VLAN-сегментації та кластеризації серверів. Така архітектура забезпечує як стійкість до кіберзагроз, так і високу доступність системи під час оброблення, передавання та зберігання даних, що надходять від сенсорних вузлів.

У нижній частині схеми показано два незалежні кластери сенсорних мереж — WSN1 та WSN2, які складаються з численних вузлів збору даних. Ці вузли взаємодіють між собою через дротові або бездротові канали з надлишковістю (redundancy), що гарантує безперервність передачі навіть у разі відмови окремого елемента. Кожен кластер під'єднано до шлюзу (Gateway), який працює у резервному режимі для запобігання єдиній точці відмови. Далі дані передаються до локальних серверів у кластерному режимі (Local Servers in cluster mode), розміщених у межах окремих VLAN-сегментів. VLAN-сегментація дозволяє ізолювати мережеві потоки різних підсистем, запобігаючи несанкціонованому доступу та розповсюдженню атак усередині інфраструктури.

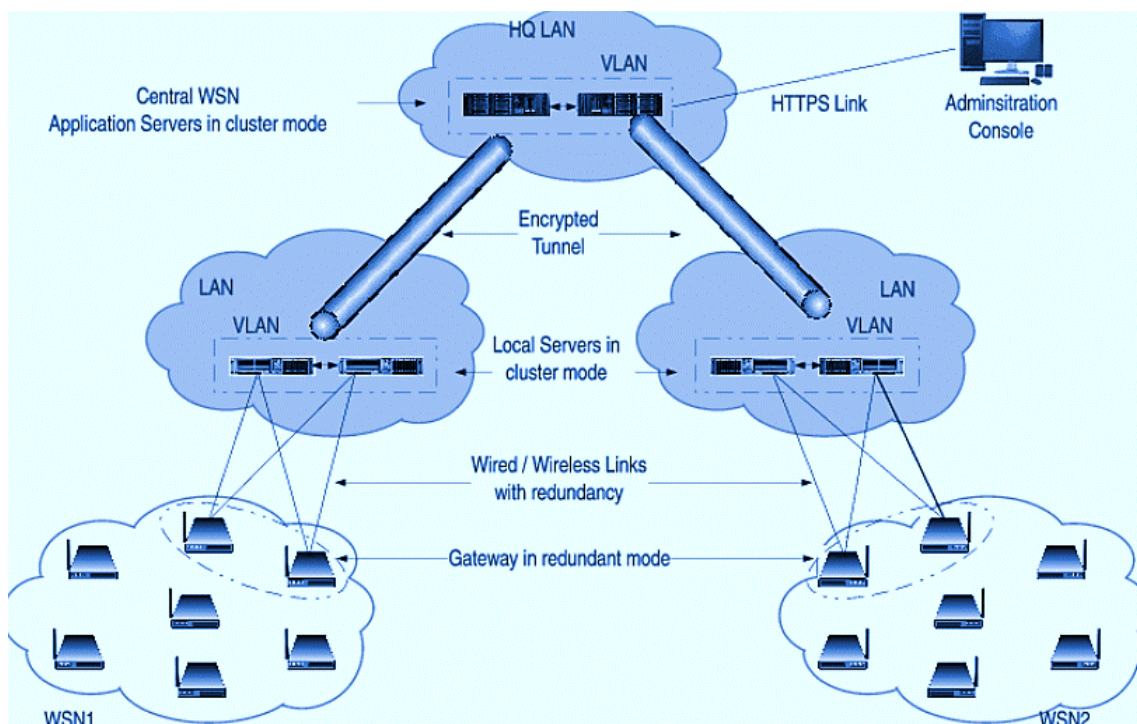


*Рис. 1.12. Архітектура захищеної сенсорної мережі (WSN) з тунелюванням, VLAN-сегментацією та кластеризацією серверів
Джерело: [1-10, 18-23]*

Між локальними серверами та центральним сервером (Central WSN Application Servers in cluster mode), що розташований у головному офісі (HQ LAN), організовано захищений тунель (Encrypted Tunnel). Він забезпечує конфіденційність і цілісність трафіку під час передавання через зовнішні мережі, використовуючи протоколи VPN або IPsec. Центральний сервер виконує функції оброблення даних, керування політиками безпеки, синхронізації та централізованого адміністрування. Доступ до системи здійснюється через адміністративну консоль (Administration Console) за захищеним каналом HTTPS, що гарантує аутентифікацію користувачів і шифрування управлінських команд. Така побудова дозволяє здійснювати моніторинг стану вузлів, оновлення конфігурацій і віддалене керування сенсорними мережами без ризику перехоплення даних. Загалом представлена архітектура поєднує переваги кластеризації серверів, VLAN-ізоляції та тунельного шифрування, створюючи багаторівневу модель безпеки для WSN. Вона забезпечує високу відмовостійкість, масштабованість і захист від типових атак на мережеву інфраструктуру, що робить її придатною для критичних застосувань — промислового моніторингу, розумних міст або систем безпеки.

Отже, ефективний захист сенсорних мереж базується на поєднанні багаторівневого шифрування, автентифікації вузлів, контролю маршрутів,

моніторингу поведінки, фізичного захисту пристроїв і регулярного оновлення безпеки. Такий комплексний підхід дозволяє протидіяти типовим атакам — sinkhole, Sybil, wormhole, replay, DoS — і забезпечує надійність, цілісність і конфіденційність даних у WSN, що є критично важливим для застосування у промислових, екологічних, медичних і розумних інфраструктурах.

Впровадження ефективного захисту IoT/WSN вимагає також створення практичних процедур: забезпечити унікальність і змінність облікових даних, підписувати й верифікувати прошивки, застосовувати апаратні засоби захисту секретів, шифрувати трафік і логічно сегментувати мережу, вести централізоване логування й аналіз, мати процеси supply-chain assessment і регулярні перевірки безпеки. Комбінація технічних заходів з політиками життєвого циклу й організаційними практиками дає змогу зменшити ймовірність успішних атак і пом'якшити їхні наслідки, забезпечуючи стійкість і надійність IoT/WSN-рішень у довгостроковій перспективі.

1.3. ХМАРНА БЕЗПЕКА: IAAS, PAAS, SAAS, DEVSECOPS у ХМАРНИХ СЕРЕДОВИЩАХ

Хмара — це віртуалізоване обчислювальне середовище, у якому ресурси (сервери, мережі, сховища, платформи та програми) надаються користувачу через Інтернет. Така архітектура дає змогу гнучко масштабувати обчислювальні потужності, зменшувати витрати на фізичне обладнання та забезпечувати безперервність бізнес-процесів. Хмарні середовища працюють за моделлю спільного використання ресурсів, що дозволяє ефективно розподіляти навантаження між користувачами та оптимізувати енергоспоживання. Вони підтримують різні формати розгортання — публічні, приватні, гібридні та мультихмарні, що забезпечує гнучкість і контроль над даними залежно від потреб підприємства. Завдяки централізованому адмініструванню й автоматизації процесів хмара забезпечує високу відмовостійкість, резервне копіювання та швидке відновлення після збоїв. У контексті кібербезпеки хмарна інфраструктура потребує впровадження багаторівневого захисту, що охоплює апаратний, мережевий, прикладний і організаційний рівні.

Залежно від рівня надання послуг розрізняють три основні моделі:

- IaaS (Infrastructure as a Service) — інфраструктура як послуга;
- PaaS (Platform as a Service) — платформа як послуга;
- SaaS (Software as a Service) — програмне забезпечення як послуга.

Хмарна безпека є комплексом заходів, спрямованих на захист даних, користувачів і сервісів, що функціонують у віртуалізованих середовищах. Її основна мета полягає у забезпеченні конфіденційності, цілісності, доступності

та довіри в цифрових екосистемах, у яких ресурси надаються за моделями IaaS, PaaS і SaaS. Для реалізації цих цілей застосовуються багаторівневі технології, стандартизовані політики доступу, а також сучасні методи інтегрованої розробки безпеки, зокрема DevSecOps.

На рис. 1.13 представлено концепцію розподілу відповідальності за безпеку між користувачем (Customer Responsibility) та хмарним провайдером Amazon Web Services (AWS Responsibility) у різних моделях хмарних сервісів — Infrastructure as a Service (IaaS), Platform as a Service (PaaS) і Software as a Service (SaaS). У моделі IaaS (Amazon EC2) користувач несе найбільшу відповідальність за безпеку, оскільки контролює керування операційною системою, конфігурацію мережі й файрволів, шифрування даних та моніторинг трафіку. AWS, у свою чергу, відповідає за фізичну інфраструктуру — апаратне забезпечення, мережеві компоненти, центри обробки даних і глобальну інфраструктуру. У PaaS (Amazon RDS) відповідальність частково розділяється: користувач забезпечує захист даних і контроль мережевих підключень, тоді як AWS бере на себе керування операційною системою, платформою виконання, резервуванням і оновленнями. У SaaS або керованих сервісах (AWS S3, AWS KMS, DynamoDB) майже вся безпека делегується провайдеру, який відповідає за зберігання, доступ, шифрування та цілісність даних. Користувач залишається відповідальним лише за захист власних облікових даних, політики доступу та управління шифруванням на стороні клієнта. Таким чином, рисунок демонструє баланс між гнучкістю (customizability) і зоною відповідальності користувача: чим більше користувач може налаштовувати систему під свої потреби (IaaS), тим більшу частку безпеки він має забезпечити самостійно. У міру переходу до керованих сервісів (PaaS, SaaS) рівень відповідальності користувача зменшується, а роль провайдера зростає.

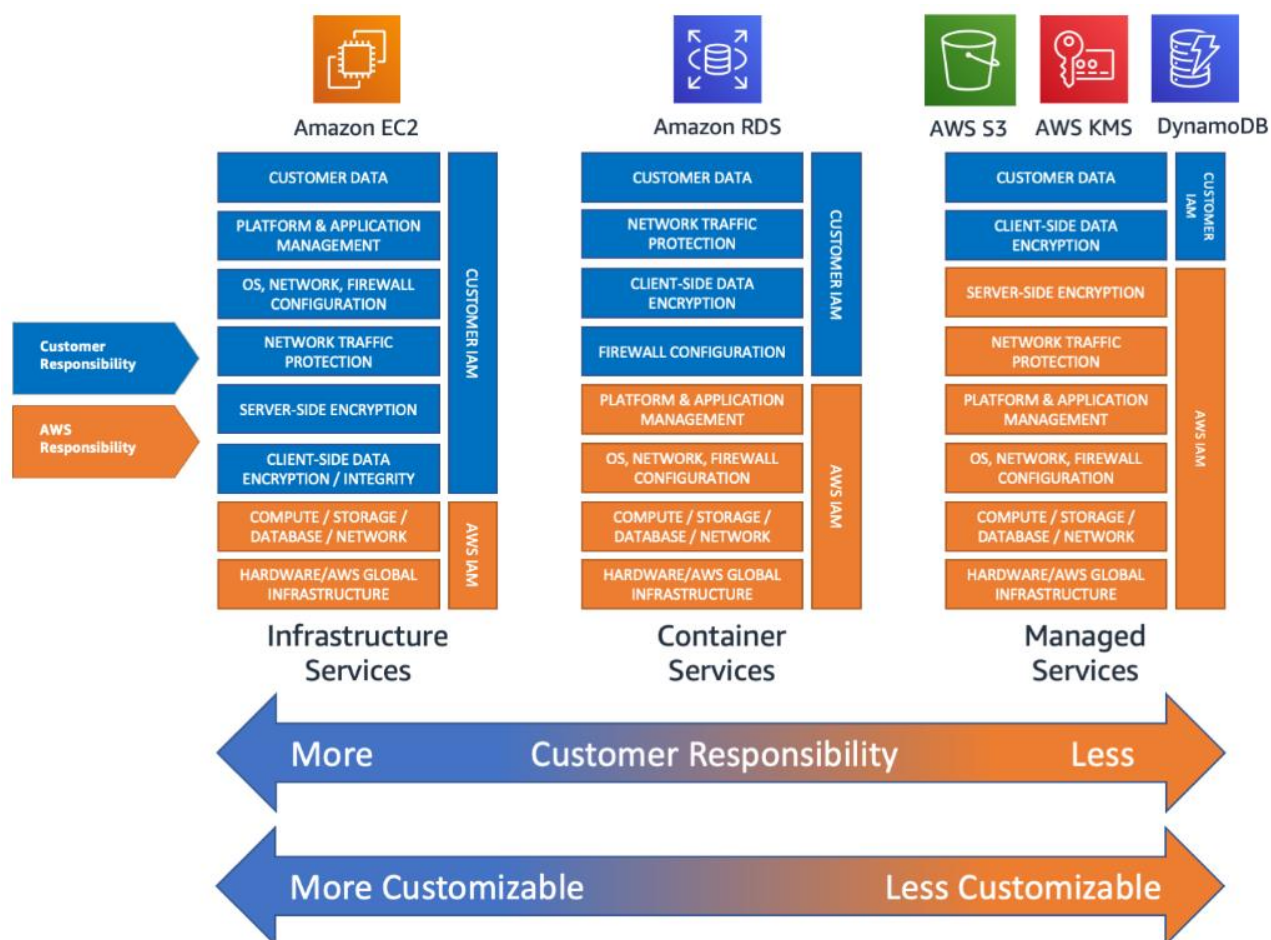


Рис. 1.13. Модель розподілу відповідальності між користувачем і провайдером у хмарних сервісах AWS (IaaS, PaaS, SaaS)

Джерело: [1-10, 18-23]

Хмарна безпека охоплює не лише технічні, а й організаційні аспекти, включаючи управління ризиками, аудит і моніторинг відповідності стандартам безпеки. Вона передбачає розподіл відповідальності між постачальником хмарних послуг і користувачем, де перший відповідає за інфраструктуру, а другий — за конфігурацію та захист даних. У хмарних середовищах особливе значення мають механізми автентифікації, шифрування, виявлення аномалій і реагування на інциденти безпеки. Ефективна хмарна безпека також спирається на автоматизацію процесів, що дозволяє своєчасно виявляти вразливості та запобігати витокам інформації. Важливим чинником є використання міжнародних стандартів, таких як ISO/IEC 27017, NIST SP 800-144 та CSA Cloud Controls Matrix, які формують основу політик безпеки. У результаті хмарна безпека забезпечує не лише захист інформаційних ресурсів, але й стабільність, довіру та безперервність бізнес-процесів у цифровій інфраструктурі.

Безпека IaaS (Infrastructure as a Service)

У моделі IaaS (Infrastructure as a Service) користувачу надається доступ до базової інфраструктури — віртуальних серверів, мереж, сховищ і систем зберігання даних, розміщених у хмарі провайдера. Безпека на цьому рівні зосереджена на контролі віртуального середовища, управлінні ідентифікацією користувачів і захисті каналів передавання інформації. Основними складовими є сегментація мережі, яка забезпечує ізоляцію віртуальних середовищ через VLAN або SDN і мінімізує ризик внутрішнього поширення атак; захист трафіку за допомогою міжмережевих екранів, VPN, IPsec-тунелів та IDS/IPS-систем; криптографічне управління ключами через централізовані системи (KMS) для зберігання, ротації та відкликання сертифікатів; управління ідентифікацією та доступом (IAM), що реалізує принцип мінімальних привілеїв і багатофакторну автентифікацію; а також моніторинг і аудит подій із застосуванням SIEM/SOC для виявлення аномалій і реагування на інциденти. У межах IaaS користувач відповідає за безпечну конфігурацію віртуальних машин, тоді як провайдер забезпечує фізичний захист серверів, гіпервізорів і центрів обробки даних.

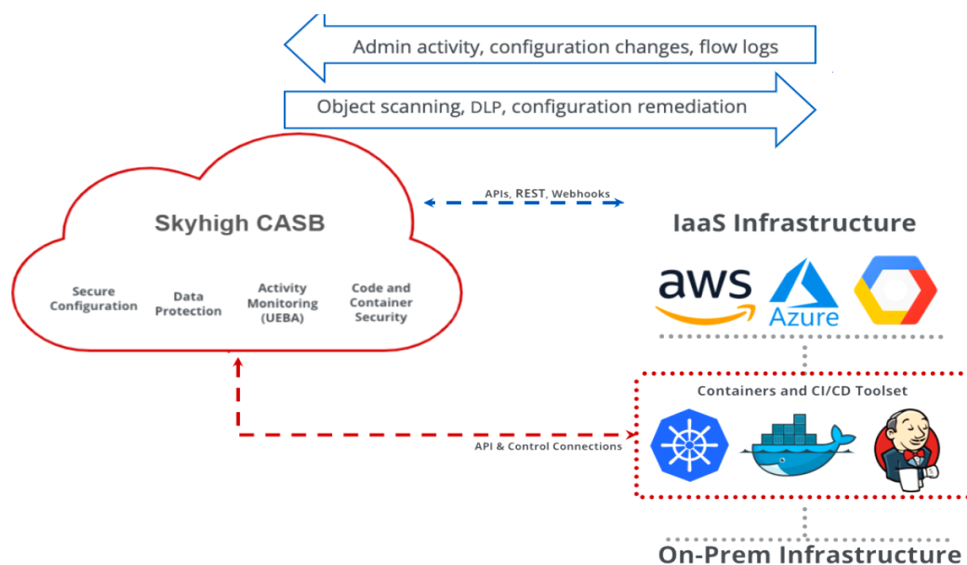


Рис. 1.14. Архітектура безпеки моделі IaaS із використанням Skyhigh CASB
Джерело: [1-10, 18-23]

На рис. 1.14 представлено інтегровану архітектуру хмарної безпеки моделі IaaS (Infrastructure as a Service), у якій поєднано сервіси інфраструктури (AWS, Azure, Google Cloud), локальні інструменти розробки та хмарну платформу безпеки Skyhigh CASB (Cloud Access Security Broker) — брокера контролю доступу до хмарних сервісів.

Skyhigh CASB забезпечує Secure Configuration (захищену конфігурацію), Data Protection (захист даних), Activity Monitoring / UEBA (User and Entity

Behavior Analytics — аналітику поведінки користувачів і об'єктів) та Code and Container Security (захист коду і контейнерів). Взаємодія між CASB і інфраструктурою IaaS відбувається через API (Application Programming Interface — інтерфейс прикладного програмування), REST (Representational State Transfer — архітектурний стиль обміну даними) або Webhooks (механізми асинхронного сповіщення про події). У межах цієї взаємодії реалізується Object Scanning (сканування об'єктів), DLP (Data Loss Prevention — запобігання витоку даних), аудит змін конфігурацій і контроль активності адміністраторів. Хмарна інфраструктура інтегрується з локальними засобами CI/CD (Continuous Integration / Continuous Deployment — безперервна інтеграція та розгортання) і контейнерними платформами (Docker, Kubernetes, Jenkins), що забезпечує автоматизований контроль безпеки на всіх етапах розробки та експлуатації. Така архітектура формує багаторівневу систему захисту, у якій безпека інтегрована як у хмарне середовище, так і в локальні ресурси підприємства, забезпечуючи безперервний моніторинг, автоматичне виявлення загроз і централізоване управління політиками доступу.

У системах IaaS критично важливим є застосування концепції Zero Trust, яка передбачає перевірку кожної дії користувача або процесу незалежно від його розташування у мережі. Для підвищення рівня ізоляції даних використовуються технології віртуальних приватних підмереж, контроль міжмережевих з'єднань на основі політик доступу та обов'язкове шифрування даних як під час передавання, так і у стані зберігання. Адміністратори повинні впроваджувати процедури регулярного оновлення систем безпеки, контроль цілісності образів віртуальних машин і перевірку підписів гіпервізорів, що знижує ризик компрометації середовища. Також важливо здійснювати аудит привілеїв, відстежуючи доступ до критичних ресурсів і використовуючи журнали подій для розслідування інцидентів. Окрему роль відіграють механізми резервного копіювання та відновлення після збоїв (Backup & Disaster Recovery), які гарантують безперервність роботи навіть у разі порушення доступності інфраструктури. У комплексі такі заходи забезпечують глибоку багаторівневу оборону (defense in depth), що підвищує стійкість IaaS-середовища до внутрішніх і зовнішніх загроз.

Безпека PaaS (Platform as a Service)

Безпека PaaS (Platform as a Service) орієнтована на захист платформ, що забезпечують розробку, тестування й розгортання програмного забезпечення без управління апаратними ресурсами. Основними напрямками безпеки є ізоляція середовищ виконання через контейнери та віртуальні екземпляри для запобігання ескаляції привілеїв; захист API через шлюзи API Gateway із застосуванням OAuth 2.0, OpenID Connect або JWT; вбудований контроль безпеки в CI/CD-процеси, що включає автоматизований аналіз коду на

вразливості; керування секретами, де конфіденційні дані зберігаються у спеціалізованих сховищах, таких як HashiCorp Vault або AWS Secrets Manager; а також контроль доступу та аудит усіх дій користувачів і сервісів. PaaS вимагає особливої уваги до безпеки зовнішніх бібліотек і компонентів, оскільки їхня компрометація може призвести до системних уразливостей у всій платформі.

Крім базових механізмів, безпека PaaS також передбачає управління життєвим циклом додатків із включенням політик безпеки на кожному етапі — від створення коду до його розгортання у виробничому середовищі. Розробники мають використовувати принцип "Security by Design", коли вимоги до захисту інтегруються у процес проєктування архітектури програмного забезпечення. У хмарних платформах важливим є застосування сервісів управління вразливістю (Vulnerability Management Services), які автоматично сканують контейнери, залежності та середовище виконання на наявність ризиків і формують звіти для DevOps-команд.

Додаткову безпеку забезпечують механізми контролю ресурсів і політик середовища, які обмежують використання пам'яті, процесорного часу та доступу до мережових інтерфейсів для запобігання DoS- або privilege escalation-атакам. У межах PaaS активно застосовується контейнерна оркестрація (Kubernetes, OpenShift), де безпека підтримується через контроль RBAC, Network Policies, Pod Security Standards і секрети Kubernetes Secrets. Важливу роль відіграє захист журналів і телеметрії — усі події мають бути централізовано зібрані та аналізовані в системах типу Cloud SIEM для виявлення аномальної активності.

Не менш важливим є управління оновленнями та патчами платформи, яке має бути автоматизованим, щоб усувати вразливості до їх експлуатації зловмисниками. Провайдери PaaS повинні дотримуватися міжнародних стандартів, таких як ISO/IEC 27017, NIST SP 800-190 та CIS Controls, що визначають вимоги до безпеки контейнеризованих середовищ. Завдяки поєднанню архітектурних, процесних і технологічних рішень модель PaaS забезпечує високий рівень цілісності, прозорості та контролюваності програмних процесів, роблячи її ключовим компонентом сучасної хмарної безпеки.

На рис. 1.14 представлено модель безпеки PaaS (Platform as a Service), у якій ключову роль відіграють контейнеризація, керування API та політики доступу. У центрі архітектури розташований API Gateway — шлюз, який забезпечує єдину точку входу для зовнішніх запитів до мікросервісів і контролює аутентифікацію, авторизацію та обмеження трафіку. Через нього запити користувачів маршрутизуються до різних контейнеризованих компонентів, таких як Customer Service, Order Service чи Inventory Service,

кожен з яких ізольований у власному контейнері для запобігання ескалації привілеїв і компрометації суміжних модулів.

Контейнери розгортаються у хмарній платформі з підтримкою CI/CD-процесів (Continuous Integration / Continuous Deployment), що дозволяє автоматично перевіряти код, виконувати сканування вразливостей і застосовувати оновлення без зупинки роботи системи. Система керування контейнерами (наприклад, Kubernetes) відповідає за балансування навантаження, контроль мережових політик і моніторинг стану мікросервісів, що забезпечує високу доступність і захищеність середовища.

Безпека платформи підсилюється за рахунок застосування OAuth 2.0 та OpenID Connect для автентифікації користувачів, TLS 1.3 для шифрування трафіку, а також RBAC (Role-Based Access Control) для обмеження дій користувачів відповідно до їхніх ролей. Виявлення загроз здійснюється через централізовані журнали подій і системи моніторингу, інтегровані з платформою, що дає змогу оперативно реагувати на підозрілі дії. Таким чином, схема демонструє сучасний підхід до побудови захищеної архітектури PaaS, у якій безпека інтегрована на всіх рівнях — від коду й контейнерів до API-взаємодії та політик доступу, що забезпечує цілісність, гнучкість і стійкість хмарних платформ до кіберзагроз.

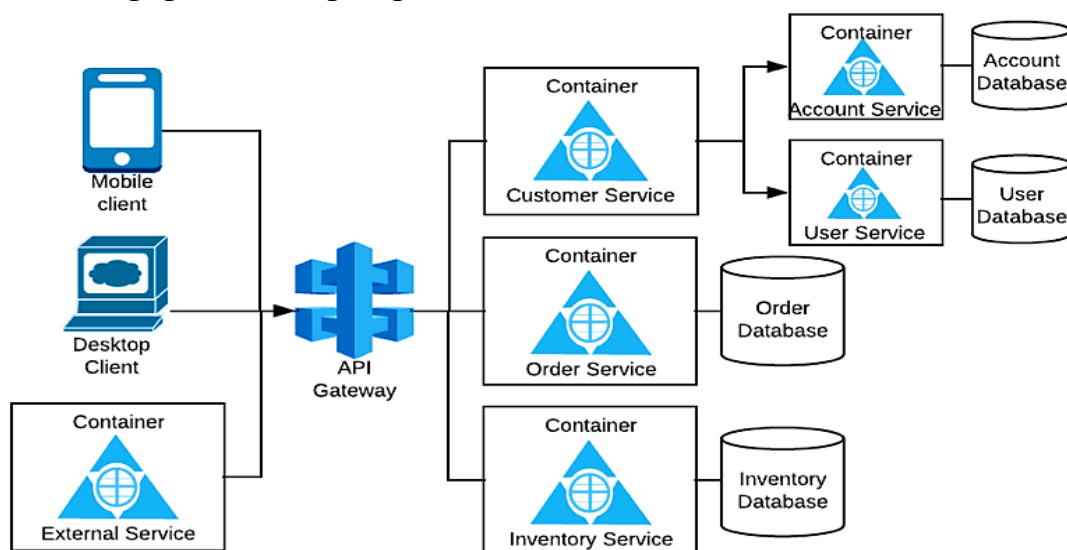


Рис. 1.15. Архітектура безпеки PaaS із контейнерами, API Gateway та мікросервісами

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Безпека SaaS (Software as a Service)

У моделі SaaS (Software as a Service) користувач отримує готові додатки, що розгортаються у хмарі провайдера й доступні через вебінтерфейс або API. Провайдер відповідає за захист інфраструктури та застосунків, тоді як

користувач забезпечує безпечну аутентифікацію та управління обліковими записами. Основними елементами безпеки є багатофакторна автентифікація (MFA), політики контролю доступу (RBAC, ABAC) і єдина система входу (SSO), що мінімізують ризики компрометації облікових даних; шифрування даних під час передавання (TLS 1.3) і зберігання (AES-256); контроль сесій для запобігання викраденню токенів і несанкціонованим підключенням; політики запобігання витоку даних (DLP), які контролюють завантаження, копіювання та обмін конфіденційними файлами; а також моніторинг API для запобігання ін'єкціям і надмірним дозволам. Важливою складовою є дотримання міжнародних стандартів — GDPR, ISO/IEC 27018, SOC 2, HIPAA, що регулюють захист персональних даних і прозорість хмарних сервісів.

Дотримання цих стандартів забезпечує відповідальне зберігання даних, захист приватності користувачів і прозорість процесів обробки інформації у хмарному середовищі. Провайдери SaaS впроваджують сертифікаційні механізми, регулярні аудити та оцінки відповідності, що гарантують надійність і довіру до сервісу. Також використовуються інструменти контролю доступу до даних на рівні політик і журналювання дій користувачів, що дозволяє запобігати порушенням і виявляти потенційні інциденти безпеки. У результаті забезпечується комплексний захист усіх етапів життєвого циклу даних — від їхнього створення і зберігання до передачі та видалення.

Безпека SaaS охоплює не лише захист даних користувачів, але й контроль над життєвим циклом інформації, включаючи створення, обробку, зберігання та видалення даних. Важливо, щоб провайдер реалізовував моделі ізоляції даних (data isolation) між клієнтами у багатокористувацькому середовищі (multi-tenancy), що запобігає доступу одного користувача до даних іншого. Для підвищення рівня довіри використовуються механізми прозорого шифрування (Transparent Data Encryption) і управління ключами клієнта (Customer Managed Keys, CMK), що дозволяють замовнику контролювати криптографічний захист своїх даних навіть у межах хмари провайдера.

Сучасні рішення SaaS впроваджують системи поведінкової аналітики (User and Entity Behavior Analytics, UEBA), які відстежують нетипову активність користувачів або сервісів, виявляючи підозрілі спроби доступу чи ексфільтрації даних. Для запобігання шкідливій активності у хмарних середовищах застосовуються Cloud Access Security Brokers (CASB) — спеціалізовані платформи, що забезпечують контроль видимості, політик безпеки, DLP-функцій та виявлення аномалій у трафіку SaaS-додатків.

Додатково велике значення має керування оновленнями та патчами програмного забезпечення, які повинні виконуватися автоматично та без переривання сервісів, аби усунути вразливості, що можуть бути використані зловмисниками. На рівні користувача важливо дотримуватись принципів

безпечного доступу, зокрема обмеження за IP-адресами, геолокацією, пристроєм чи часом сесії.

Провайдери SaaS також повинні забезпечувати аудит дій користувачів (User Activity Audit), централізоване журналювання подій і можливість проведення розслідувань у разі інцидентів. У критичних сценаріях застосовується резервне копіювання та політика відновлення після збоїв (Backup & Disaster Recovery), що гарантує доступність даних навіть у разі відмови інфраструктури або кібератак.

На рис. 1.16 зображено модель архітектури безпеки SaaS (Software as a Service), у якій головний акцент зроблено на управлінні політиками, ідентифікацією користувачів, контролем якості обслуговування (QoS) і дотриманням угод про рівень сервісу (SLA). У структурі SaaS-провайдера виділено три основні функціональні блоки: Identity and Access Management, SLA Management і Service Provisioning. Перший блок забезпечує автентифікацію, авторизацію та контроль політик доступу користувачів, що дозволяє підтримувати принципи мінімальних привілеїв і запобігати несанкціонованим діям. Policies Management і QoS Evaluation здійснюють управління наборами правил безпеки, визначають вимоги до якості послуг і контролюють відповідність заявленим параметрам продуктивності.

Блок SLA Management відповідає за формування, узгодження та моніторинг угод про рівень сервісу (Service Level Agreement), що гарантують користувачам прозорість і передбачуваність роботи хмарних сервісів. Тут виділяються три підпроцеси: SLA Negotiation, SLA Monitoring and Assessment, які спільно забезпечують як дотримання встановлених умов, так і виявлення відхилень у якості обслуговування. Service Provisioning охоплює процеси розгортання сервісів, публікацію доступних ресурсів і вибір серверів, на яких ці сервіси функціонують, що прямо впливає на їхню доступність і стійкість до перевантажень.

На нижньому рівні схеми показано сховище метаданих, що містить Policies, Profiles, SLA Templates, Committed SLAs та QoS Information — ці елементи забезпечують централізоване управління всіма аспектами безпеки та якості. У сукупності така архітектура гарантує узгоджене функціонування компонентів SaaS-провайдера, зберігаючи цілісність і конфіденційність даних, а також забезпечуючи контрольований, передбачуваний і безпечний рівень надання послуг користувачам. Ця структура дає змогу автоматизувати процеси моніторингу, оновлення політик і розподілу ресурсів між користувачами відповідно до встановлених рівнів сервісу. Метадані виступають основою для динамічної адаптації системи до змін навантаження, вимог безпеки та оновлень нормативних стандартів. Завдяки централізованому зберіганню конфігурацій і політик адміністратор може швидко реагувати на інциденти, змінювати

параметри доступу або пріоритети без втручання у роботу всієї платформи. Таким чином, архітектура на основі метаданих у SaaS-середовищах створює прозорий, масштабований і керований механізм забезпечення кібербезпеки, що підвищує довіру користувачів і стабільність хмарних сервісів.

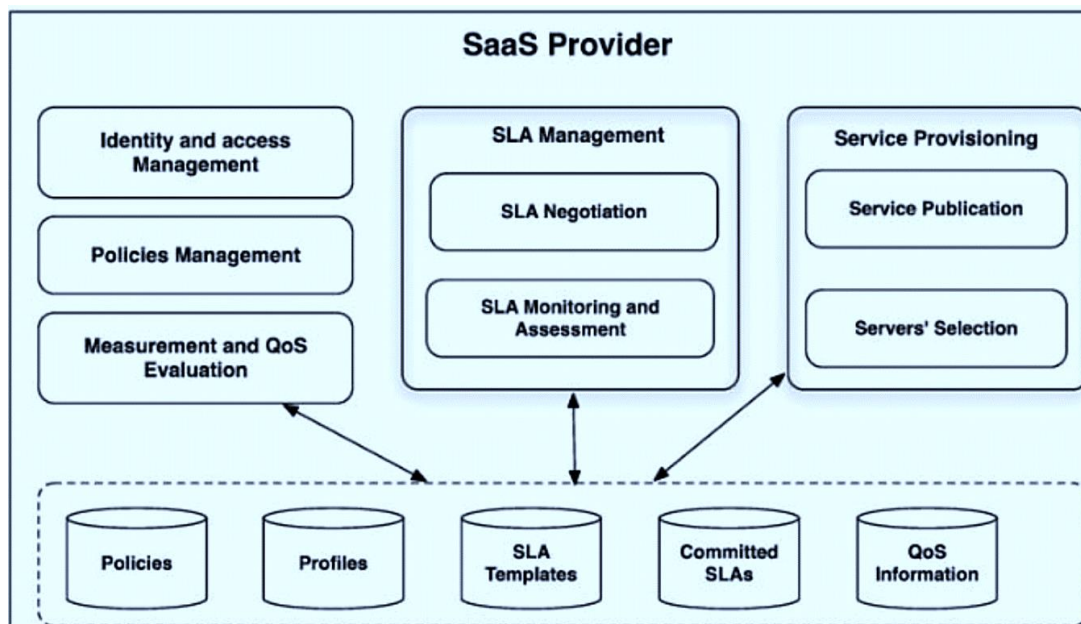


Рис. 1.16. Архітектура безпеки SaaS-провайдера з управлінням політиками, доступом і рівнем сервісу (SLA)

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Отже, ефективна безпека SaaS базується на поєднанні криптографічного захисту, поведінкового моніторингу, управління доступом і відповідності нормативним вимогам. Такий підхід забезпечує цілісність, довіру та надійність хмарних сервісів, роблячи їх придатними для критично важливих застосувань — від фінансових систем до охорони здоров'я й державного управління. Впровадження багаторівневої архітектури захисту дозволяє мінімізувати ризики витоку інформації та несанкціонованого доступу до корпоративних даних. Регулярний аудит безпеки, тестування на проникнення й моніторинг активності користувачів забезпечують своєчасне виявлення потенційних загроз і підтримку стабільної роботи сервісів. Інтеграція механізмів штучного інтелекту та аналітики поведінкових патернів підвищує здатність системи до самонавчання й автоматичного реагування на аномалії. У сукупності це створює гнучку та стійку екосистему SaaS, здатну протистояти сучасним кіберзагрозам у глобальному цифровому середовищі.

DevSecOps у хмарних середовищах

DevSecOps у хмарних середовищах — це сучасна концепція, що інтегрує безпеку в усі етапи життєвого циклу програмного забезпечення: від розробки до експлуатації. Вона передбачає автоматизацію перевірок безпеки, безперервний моніторинг середовища та швидке реагування на загрози. Основними принципами є автоматизоване тестування безпеки в CI/CD-конвеєрах через інструменти SAST, DAST і IAST, що виявляють уразливості ще до етапу розгортання; впровадження Infrastructure as Code (IaC), яке дозволяє створювати інфраструктуру програмно з вбудованими політиками безпеки та уникати людських помилок; постійний моніторинг хмарних систем через сервіси SIEM, CloudTrail, Azure Security Center для виявлення аномалій і вторгнень; захист контейнерів і мікросервісів через сканування Docker-образів і контроль Kubernetes-кластерів; а також реалізація принципів Zero Trust, де кожна взаємодія між користувачами, сервісами чи додатками перевіряється незалежно від їхнього розташування. DevSecOps формує динамічну модель безпеки, у якій контроль є безперервним і автоматизованим, а ризики мінімізуються ще на етапі розробки.

DevSecOps у хмарних середовищах також передбачає тісну взаємодію команд розробки (Dev), експлуатації (Ops) та безпеки (Sec) з метою формування єдиного циклу “Shift-Left Security”, коли перевірки безпеки переносяться якнайраніше у процес розроблення програмного забезпечення. Це дозволяє виявляти вразливості ще до інтеграційного або тестового етапу, що істотно зменшує витрати на їхнє усунення та підвищує якість кінцевого продукту. У межах DevSecOps активно використовуються репозиторії політик безпеки (Security Policy as Code), де всі правила, обмеження та шаблони конфігурацій зберігаються у вигляді коду, що забезпечує їхню повторюваність, версіонування та контроль змін.

Одним із ключових елементів DevSecOps є автоматизований аналіз залежностей (Dependency Scanning), який перевіряє сторонні бібліотеки та пакети на наявність відомих вразливостей за базами CVE. Додатково впроваджується динамічний контроль середовища виконання (Runtime Application Self-Protection, RASP), що дозволяє додаткам самостійно виявляти і блокувати підозрілі дії під час роботи. Для забезпечення надійності контейнеризованих сервісів використовуються інструменти оркестраційної безпеки (Kubernetes Security Benchmarks, OPA Gatekeeper, Falco), які контролюють мережеві політики, доступ до ресурсів і дотримання вимог конфігурації.

У хмарних платформах DevSecOps інтегрується з Cloud Native Security Frameworks, що поєднують функції безпеки, моніторингу, управління ідентичностями та реагування на інциденти. Це дозволяє забезпечити повний цикл безпеки — від розробки до автоматизованого відновлення після атак або

збоїв. Важливу роль відіграє контейнерна ізоляція та контроль цілісності образів за допомогою перевірених репозиторіїв (Docker Trusted Registry, Harbor), що мінімізує ризик впровадження шкідливого коду у процес розгортання.

Крім технічних аспектів, DevSecOps охоплює культурну трансформацію організації: безпека перестає бути окремою функцією й стає частиною спільної відповідальності всіх учасників життєвого циклу продукту. Постійні навчання, симуляції атак (Red Team/Blue Team Exercises) та аналіз інцидентів допомагають підтримувати готовність до нових кіберзагроз.

Завдяки поєднанню автоматизації, моніторингу, безперервного вдосконалення процесів і взаємодії команд DevSecOps створює адаптивну екосистему безпеки, у якій вразливості усуваються ще до їх експлуатації, а оновлення безпеки відбуваються без зупинки сервісів. Такий підхід забезпечує стійкість хмарних систем, високу швидкість реагування на інциденти й відповідність сучасним стандартам кіберзахисту, включаючи ISO/IEC 27034, NIST SP 800-190 та CSA Cloud Controls Matrix.

На рис. 1.17 подано архітектуру DevSecOps у хмарному середовищі, що демонструє комплексну взаємодію між етапами розроблення, тестування, розгортання та захисту програмного забезпечення. У центрі моделі розташовано CI/CD-конвеєр, який автоматизує процеси безперервної інтеграції та доставки (Continuous Integration / Continuous Deployment), до якого інтегровані елементи безпеки — SAST, DAST і IAST — для виявлення вразливостей ще на етапі кодування. Контейнерна інфраструктура, представлена системами Docker та Kubernetes, забезпечує ізольоване виконання сервісів, контроль доступу до ресурсів і безпечне оновлення компонентів через політику Policy-as-Code, що дозволяє централізовано визначати та застосовувати правила безпеки.

Важливою складовою архітектури є хмарні служби моніторингу, такі як SIEM, CloudTrail або Azure Security Center, які забезпечують постійне спостереження за поведінкою системи, виявлення аномалій і реагування на інциденти у режимі реального часу. Дані з CI/CD-конвеєра, контейнерів і хмарних платформ збираються у єдиному інформаційному потоці, що дозволяє DevSecOps-командам здійснювати аудит, оцінку ризиків і контроль відповідності вимогам стандартів ISO/IEC 27034 та NIST SP 800-190. Архітектура також включає компоненти Zero Trust, які гарантують, що кожна взаємодія між користувачами, сервісами чи додатками проходить перевірку незалежно від їхнього розташування в мережі.

Завдяки такій побудові DevSecOps у хмарі забезпечує безперервну безпеку — від розробки коду до його експлуатації, поєднуючи автоматизацію, аналітику, контроль політик і самооновлення систем. У результаті формується

адаптивне середовище, де вразливості виявляються й усуваються на ранніх етапах, а процеси розробки та захисту функціонують як єдина інтегрована екосистема.

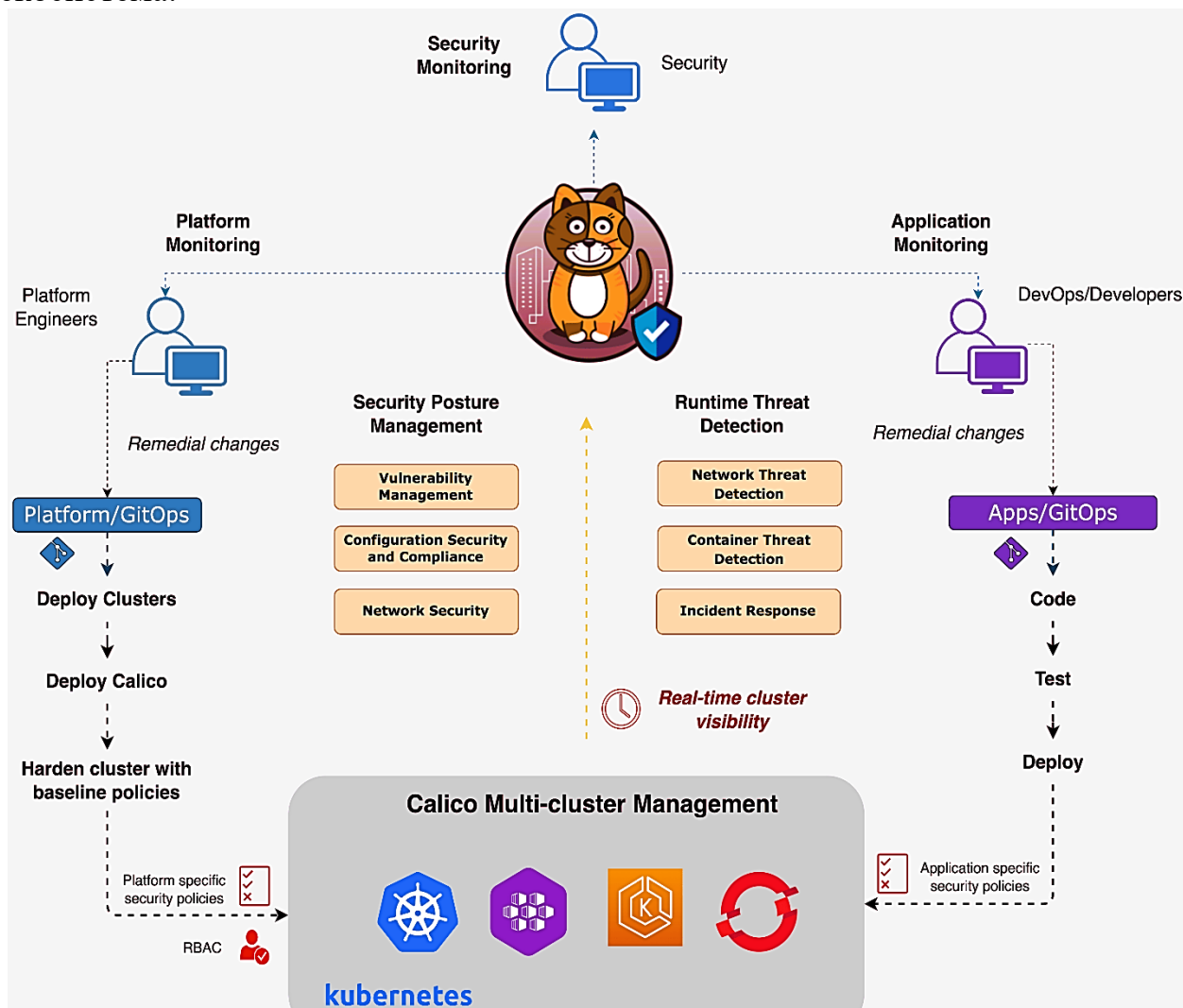


Рис. 1.17. Архітектура DevSecOps у хмарному середовищі з інтеграцією безпеки, контейнеризації та моніторингу

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Отже, кожен рівень хмарної архітектури — IaaS, PaaS і SaaS — має свої унікальні виклики та специфічні механізми захисту, тоді як DevSecOps об'єднує їх у єдиний контур хмарної безпеки. Такий підхід формує стійку, гнучку та керовану екосистему, у якій безпека інтегрована в кожен процес — від інфраструктури до прикладного коду. Це забезпечує стабільність, прозорість і відповідність сучасним міжнародним стандартам кіберзахисту, що є критично важливим для надійного функціонування цифрових сервісів у хмарних середовищах.

1.4. БЕЗПЕКА ICS/SCADA-СИСТЕМ ТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Безпека систем керування технологічними процесами (Industrial Control Systems — ICS) та диспетчерських систем збору й обробки даних (Supervisory Control and Data Acquisition — SCADA) є стратегічно важливим аспектом кіберзахисту критичної інфраструктури. Ці системи керують енергетичними мережами, водопостачанням, транспортом, виробничими підприємствами й іншими об'єктами, від яких залежить безперебійне функціонування держави. На відміну від традиційних IT-систем, ICS/SCADA мають унікальні особливості — тривалий життєвий цикл, використання застарілого обладнання, обмежену можливість оновлення та жорсткі вимоги до безперервності роботи. Тому головним викликом є поєднання кібербезпеки з безпекою технологічного процесу, без ризику зупинки виробництва чи втрати керованості системою.

На рис. 1.18 представлено типовий приклад архітектури ICS/SCADA-системи, побудованої за моделлю Purdue, яка поділяє виробниче середовище на шість рівнів безпеки — від фізичних процесів до корпоративних інформаційних систем. На нулевому рівні (Level 0) розташоване технологічне обладнання, яке безпосередньо виконує виробничі операції — сенсори, виконавчі механізми та промислові роботи. Над ним знаходиться перший рівень (Level 1), що включає програмовані логічні контролери (PLC) та інтелектуальні пристрої, які здійснюють збір даних і керування технологічними процесами. На другому рівні (Level 2) працюють системи SCADA та інтерфейси людино-машинної взаємодії (HMI), які забезпечують моніторинг і візуалізацію процесів у реальному часі.

Третій рівень (Level 3) відповідає за керування виробництвом — тут розміщуються системи управління продуктивністю підприємства (Plant Performance Management System), сервери історії даних (Historian) та модулі виявлення аномалій і моніторингу активів. Для ізоляції виробничого середовища від корпоративних мереж застосовується рівень 3.5 (Industrial DMZ) — демілітаризована зона, у якій розташовані шлюзи віддаленого доступу (Jump Host), системи управління журналами SCADA (Logs, Assets, Anomalies) та сервери безпечного підключення зовнішніх користувачів. Вище знаходиться четвертий рівень (Level 4), що включає бізнес-логістичні системи, ERP-рішення й корпоративні аналітичні сервіси, які взаємодіють із виробничими процесами через строго контрольовані канали. П'ятий рівень (Level 5) представляє корпоративну IT-мережу, у межах якої працюють співробітники, аналітики, а також зовнішні підрядники чи технічні фахівці (наприклад, Rockwell, Siemens, GE), які можуть здійснювати діагностику віддалено.

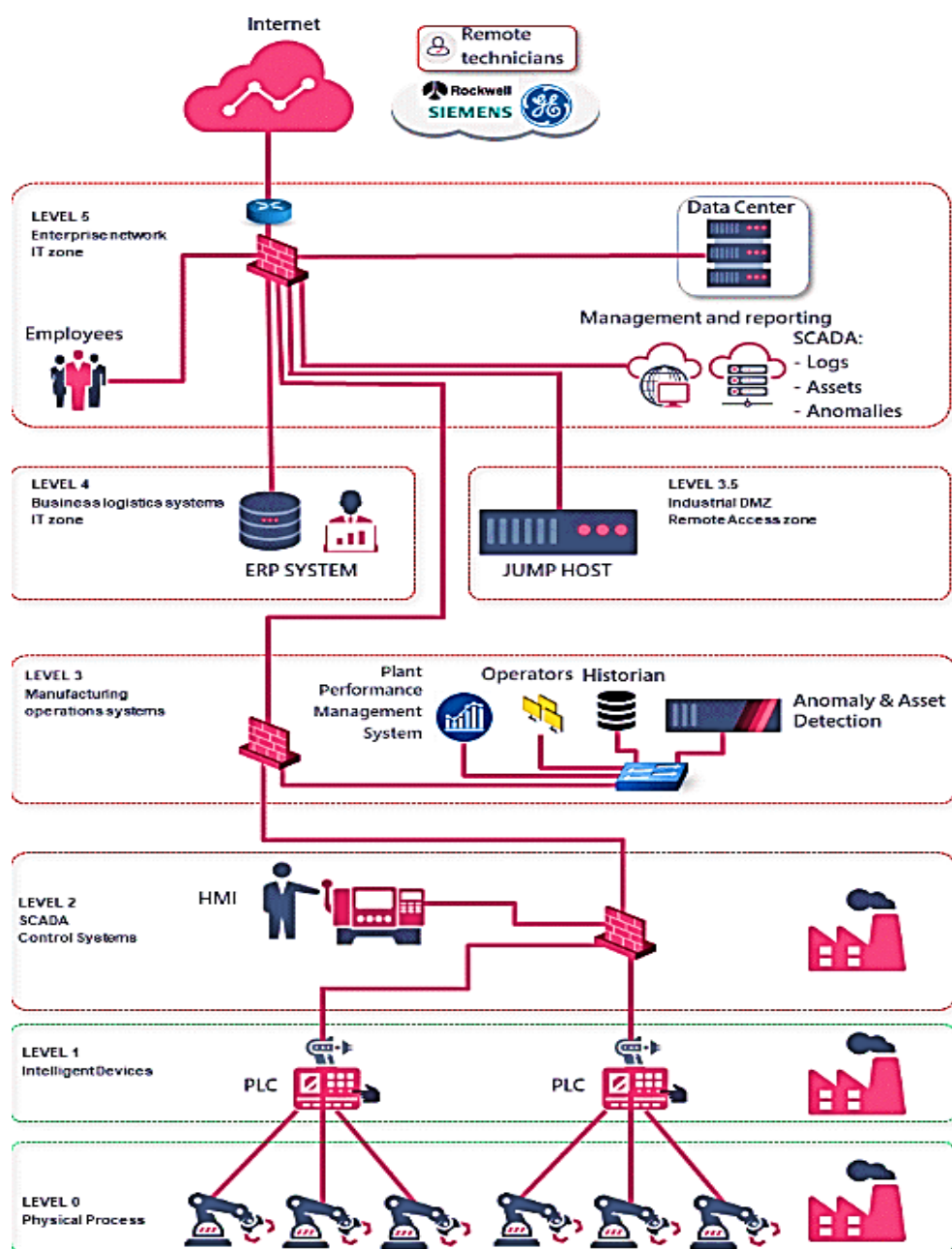


Рис. 1.18. Багаторівнева архітектура безпеки ICS/SCADA-систем відповідно до моделі Purdue

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Така архітектура забезпечує реалізацію принципів *Defense in Depth* — кожен рівень ізольований від інших, а доступ між ними здійснюється лише через перевірені шлюзи з контролем трафіку й автентифікацією користувачів. Завдяки цьому досягається багаторівневий захист виробничих процесів, знижується ризик проникнення шкідливого коду з ІТ-зони в ОТ-середовище, а також гарантується цілісність і стабільність критичної інфраструктури.

На фізичному рівні захист починається з контролю доступу до обладнання — програмованих логічних контролерів (PLC), сенсорів, комунікаційних модулів і серверів SCADA. Впроваджуються багаторівневі системи ідентифікації персоналу, відеоспостереження, контроль периметра й сигналізація, що унеможлиблює несанкціоноване підключення пристроїв або маніпуляції з апаратурою. Для підвищення стійкості до фізичних втручань застосовують захищені шафи, екранізовані канали передавання сигналу та ізольовані технічні приміщення.

Додатково на фізичному рівні реалізується контроль температурних, електромагнітних і вібраційних впливів, які можуть бути використані як непрямі вектори атак на обладнання. Всі критично важливі компоненти розміщуються у зонах з обмеженим доступом, де діє система допуску за біометричними параметрами або смарт-картками. Проводиться маркування обладнання та регулярна інвентаризація для запобігання підміні або несанкціонованому переміщенню пристроїв. Використовуються резервні джерела живлення (UPS) та системи контролю мікроклімату, що гарантують безперервність роботи навіть у разі аварій. Важливим аспектом є фізичне розділення комунікаційних ліній керування і моніторингу, що мінімізує ризик перехоплення сигналів. У сукупності ці заходи формують основу фізичного захисту ICS/SCADA, забезпечуючи стабільність, надійність і захист технологічного обладнання від цілеспрямованих деструктивних впливів.

На мережевому рівні реалізується сегментація на зони безпеки згідно зі стандартами ISA/IEC 62443, де кожна зона має власні політики доступу, а взаємодія між ними відбувається через демілітаризовану зону (DMZ) із контролем трафіку. Відокремлення IT-мереж від ОТ-середовища (Operational Technology) запобігає поширенню шкідливого коду з корпоративної інфраструктури у виробничу. Використовуються міжмережеві екрани промислового класу, VPN, а також системи виявлення та запобігання вторгненням (IDS/IPS), адаптовані для промислових протоколів, таких як Modbus, DNP3, Profibus, IEC 60870-5-104.

Для забезпечення цілісності та автентичності мережевих з'єднань застосовуються цифрові сертифікати, контроль списків доступу (ACL) та механізми глибокої перевірки пакетів (Deep Packet Inspection, DPI). Усі комунікаційні канали між зонами контролюються через шлюзи з політиками "allow list", що обмежують трафік лише необхідними напрямками. Впроваджується моніторинг мережевих потоків у реальному часі з використанням SIEM-систем для виявлення аномалій і несанкціонованих з'єднань. Для підвищення стійкості до атак типу DDoS застосовуються системи балансування навантаження та автоматичного фільтрування підозрілих запитів.

Адміністратори постійно оновлюють сигнатури IDS/IPS і ведуть журнали подій, що дає змогу своєчасно виявляти спроби вторгнення. У комплексі ці заходи створюють багаторівневу систему мережевої безпеки, яка мінімізує ризики кіберінцидентів та гарантує стабільність функціонування виробничої інфраструктури.

На рівні протоколів і комунікацій важливим є забезпечення автентичності та цілісності даних. Для цього застосовуються захищені варіанти промислових протоколів (наприклад, Secure Modbus/TCP, DNP3-SA) і шифрування каналів із використанням TLS 1.3 або IPsec. Синхронізація часу здійснюється через захищені механізми NTP/PTP, що запобігає маніпуляціям із часовими мітками, які можуть спотворити логіку управління.

Додатково впроваджується взаємна автентифікація вузлів за допомогою цифрових сертифікатів X.509, що унеможлиблює підключення неавторизованих пристроїв до мережі керування. Для контролю цілісності повідомлень використовуються коди автентифікації повідомлень (MAC) і криптографічні хеш-функції, які дозволяють виявляти будь-які зміни даних під час передавання. Застосовується механізм черговості пакетів і перевірка номерів кадрів для запобігання повторним атакам (replay attacks). Вузли обміну інформацією можуть використовувати адаптивні алгоритми вибору частоти передавання даних для зменшення ризику перехоплення сигналу. У критичних системах передбачено багатоканальне дублювання зв'язку з автоматичним перемиканням на резервний маршрут у разі виявлення аномалії. Сукупність цих заходів гарантує достовірність обміну даними, стійкість комунікацій до перехоплення й підвищує рівень кіберзахисту промислових протоколів.

На рівні контролерів і SCADA-додатків безпека реалізується через контроль цілісності програмного коду, багаторівневу автентифікацію користувачів і обмеження команд керування. Використовуються підписані конфігураційні файли, а оновлення прошивок проходять через перевірку цифрових підписів. У SCADA-системах запроваджуються журнали аудиту для кожної операції (дистанційного керування, зміни параметрів, аварійних сигналів), що дозволяє швидко ідентифікувати інциденти.

Додатково впроваджується рольова модель доступу (RBAC), яка чітко розмежовує повноваження операторів, інженерів і адміністраторів, запобігаючи виконанню критичних команд неавторизованими особами. Для підвищення надійності використовується механізм “dual control”, що передбачає підтвердження небезпечних дій двома користувачами одночасно. SCADA-сервери ізолюються у власному сегменті мережі та підключаються до корпоративних систем лише через шлюзи з контролем протоколів OPC UA або MQTT із шифруванням. Для зменшення ризику зараження шкідливим кодом

обмежується використання змінних носіїв і впроваджуються системи білого списку програм (Application Whitelisting). Контролери регулярно проходять верифікацію стану прошивки та перевірку хешів для виявлення змін у коді. У комплексі ці заходи забезпечують цілісність і стійкість SCADA-рівня, мінімізуючи ризики саботажу, помилкових команд та зовнішнього втручання в технологічні процеси.

На аналітичному рівні ефективним є застосування рішень класу SIEM (Security Information and Event Management), які збирають події з різних компонентів системи — PLC, шлюзів, операторських станцій, серверів SCADA — і формують централізовану картину безпеки. Використання IDS/IPS для OT (наприклад, Nozomi Networks, Claroty, Dragos) дозволяє виявляти аномалії в мережеских потоках та моделі поведінки пристроїв, що свідчать про спроби кібератак або порушення штатного режиму роботи.

SIEM-рішення інтегруються з аналітичними платформами, які застосовують машинне навчання для кореляції подій і виявлення складних багатоступеневих атак у реальному часі. Дані з систем моніторингу збагачуються контекстною інформацією з баз загроз (Threat Intelligence Feeds), що дає змогу розпізнавати нові шкідливі кампанії на ранніх етапах. Для оперативного реагування використовуються автоматизовані сценарії SOAR (Security Orchestration, Automation and Response), які виконують ізоляцію скомпрометованих вузлів або блокування підозрілих сесій без участі оператора. Аналітичний рівень також забезпечує створення звітів про стан кіберзахисту, виявлені інциденти та тенденції розвитку загроз, що полегшує аудит безпеки й планування оновлень політик. Постійне вдосконалення аналітичних моделей дозволяє підвищувати точність виявлення та зменшувати кількість хибних спрацювань. У результаті формується адаптивна система моніторингу, здатна самостійно виявляти, оцінювати та нейтралізувати ризики в ICS/SCADA-середовищах.

На організаційному рівні впроваджується політика управління ризиками та інцидентами згідно з вимогами NIST SP 800-82, ISO/IEC 27019 і IEC 62443-3-3. Вона включає навчання персоналу, регламентацію дій операторів, контроль змін конфігурацій і розмежування ролей. Регулярні тестування на проникнення, аудити безпеки та симуляції атак допомагають перевірити готовність системи до реальних загроз.

Також розробляються плани реагування на інциденти (Incident Response Plans) та відновлення після збоїв (Disaster Recovery Plans), що визначають послідовність дій у разі компрометації або виходу з ладу критичних компонентів. Проводяться навчальні тренування типу Red Team/Blue Team, які моделюють атаки на виробничі процеси для підвищення обізнаності персоналу

та злагодженості дій у кризових ситуаціях. На рівні управління ризиками застосовується методика оцінки критичності активів і пріоритизації захисних заходів за їхнім впливом на безперервність виробництва. Важливою складовою є створення внутрішнього Центру кібербезпеки підприємства (ICS-SOC), який координує моніторинг, аналіз та реагування на інциденти в режимі 24/7. Усі політики та процедури безпеки регулярно переглядаються відповідно до оновлених стандартів і загроз, що забезпечує актуальність системи захисту. Такий організаційний підхід формує культуру безпеки, у якій відповідальність за кіберзахист є колективною та підтримується на всіх рівнях управління підприємством.

Концепція “Defense in Depth”

Важливим напрямом є впровадження концепції “Defense in Depth” (глибокої безпеки), коли безпека забезпечується багатьма шарами — від фізичного доступу до аналітики подій. Додатково застосовується бекапування та аварійне відновлення (Disaster Recovery), що гарантує швидке відновлення роботи після інцидентів.

Кожен рівень захисту в межах “Defense in Depth” виконує власну функцію: фізичний бар'єр обмежує несанкціонований доступ до обладнання, мережевий — контролює трафік і сегментує зони безпеки, прикладний — забезпечує автентифікацію та цілісність даних, а аналітичний — виявляє відхилення та координує реагування. Такий підхід дозволяє знизити ймовірність одночасного компрометування кількох рівнів системи.

Важливу роль відіграє централізоване управління журналами подій, резервування каналів зв'язку та підтримка синхронних копій критичних даних. Упровадження багаторівневого шифрування, ізоляції сегментів і перевірених механізмів автентифікації формує надійну екосистему безпеки. Крім того, “Defense in Depth” забезпечує гнучкість і адаптивність системи — навіть у разі порушення одного з рівнів інші продовжують функціонувати, підтримуючи цілісність і стійкість інфраструктури. У комплексі це створює інтегровану модель захисту, орієнтовану на превентивне виявлення, локалізацію та мінімізацію наслідків кібератак на ICS/SCADA-системи та критичну інфраструктуру.

Реалізація концепції “Defense in Depth” у середовищі ICS/SCADA відбувається шляхом поетапного накладання взаємопов'язаних механізмів безпеки, що охоплюють як технічні, так і організаційні заходи. На початковому етапі впроваджується фізичний захист, який включає контроль доступу до виробничих приміщень, систем відеоспостереження, біометричну ідентифікацію персоналу та захищені шафи для контролерів і комунікаційного обладнання. Далі застосовується мережевий рівень безпеки, який реалізується через сегментацію мереж на ізольовані зони (згідно з ISA/IEC 62443),

встановлення промислових міжмережевих екранів, VPN, IDS/IPS і використання DMZ для безпечного обміну між IT- та OT-середовищами.

На рівні прикладних систем захист забезпечується за рахунок цифрового підпису конфігурацій і прошивок, контролю цілісності SCADA-додатків, а також застосування багатофакторної аутентифікації операторів і адміністраторів. Аналітичний рівень представлений SIEM- і SOAR-платформами, які збирають журнали подій, виконують кореляцію інцидентів і автоматично реагують на відхилення. Для забезпечення безперервності роботи впроваджуються політики резервного копіювання (Backup Policy), дублювання критичних вузлів і географічно розподілені центри обробки даних.

На рис. 1.19 показано узагальнену модель концепції *Defense in Depth* (глибокої оборони), яка передбачає створення кількох взаємопов'язаних рівнів безпеки — від політик і процедур до захисту даних і прикладних систем. Зовнішнє кільце відображає рівень політик і процедур (Policy and Procedures), що включає управління ризиками, реагування на інциденти, контроль постачальників, аудит безпеки, навчання персоналу та підвищення обізнаності. Наступний шар — фізична безпека (Physical Security), яка охоплює захист об'єктів і обладнання через системи ідентифікації, відеоспостереження (CCTV), обмеження доступу та периметрові бар'єри.

Далі йде мережевий рівень (Network Security), який охоплює корпоративні й промислові сегменти (ICS) та реалізує засоби міжмережевого екранування, VPN, IDS/IPS, ізоляцію трафіку, моніторинг і виявлення вторгнень. Вище розташований рівень безпеки хостів (Host Security), що забезпечує оновлення антивірусів, контроль служб, динамічні списки дозволів, а також захист від несанкціонованого читання чи запису. Центральним ядром є захист застосунків і даних (Application and Data Security) — тут реалізується шифрування конфіденційної інформації, вчасне оновлення програмного забезпечення, перевірка цілісності та контроль доступу до критичних ресурсів.

Така багатошарова структура забезпечує стійкість системи навіть у разі компрометації одного з рівнів, оскільки інші залишаються активними бар'єрами. У контексті ICS/SCADA-конфігурацій цей підхід гарантує, що як фізичні пристрої, так і цифрові компоненти працюють у єдиній захищеній екосистемі, здатній протистояти складним кіберзагрозам і зберігати безперервність технологічних процесів.

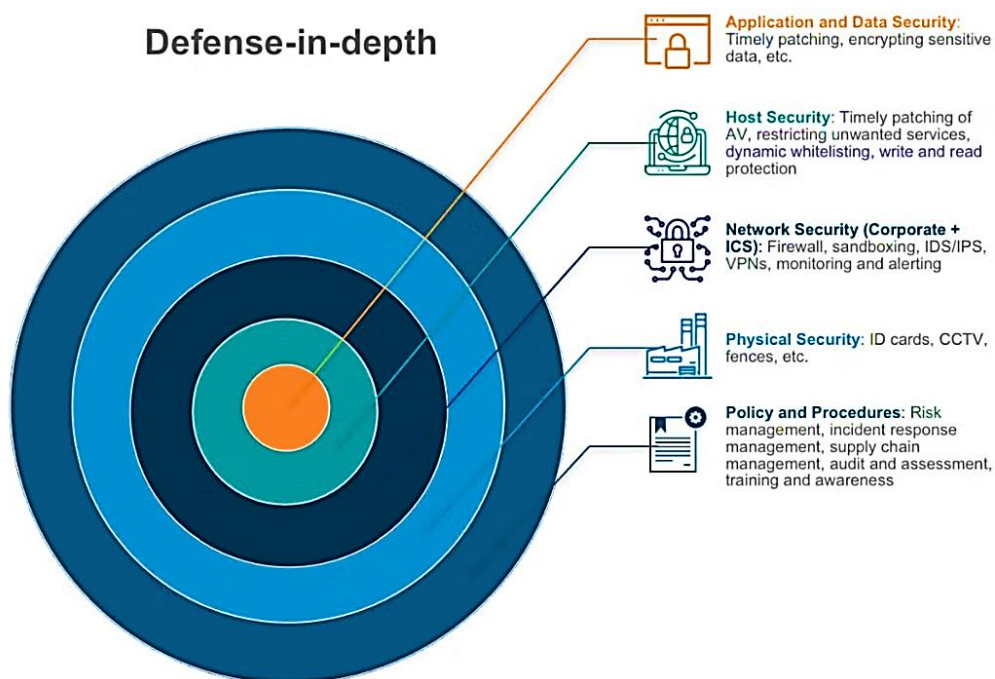


Рис. 1.19. Концепція багаторівневої безпеки (Defense in Depth) у системах кіберзахисту

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Крім того, концепція “Defense in Depth” реалізується через постійний моніторинг стану безпеки за допомогою засобів OT Threat Detection, аналіз поведінкових аномалій пристроїв і регулярне тестування на проникнення. Організаційно вона підтримується навчанням персоналу, оновленням політик реагування та періодичними аудитами відповідності вимогам NIST SP 800-82 і ISO/IEC 27019. Завдяки цьому формується багаторівнева архітектура захисту, у якій усі компоненти діють скоординовано, створюючи надійний бар’єр проти кіберзагроз і збоїв у критичних інфраструктурних системах.

Загрози для ICS/SCADA

Серед типових загроз для ICS/SCADA виділяють атаки типу Stuxnet, Havex, Industroyer, Triton, що націлені на зміну логіки контролерів, перехоплення управління або виведення з ладу технологічного обладнання. Для протидії цим атакам необхідні своєчасне оновлення прошивок, контроль мережових з’єднань, моніторинг аномалій і впровадження Zero Trust-архітектури у виробничих мережах.

На цьому рисунку представлені основні класи загроз, з якими стикаються системи керування технологічними процесами (ICS / SCADA). Показано, як шкідливе програмне забезпечення може розповсюджуватись через мережі, включно з атаками на протоколи зв’язку, перехопленням мережевого трафіку й модифікацією команд або даних. Також висвітлено сценарії впровадження

хибних даних (false data injection), replay-атаки та підміни повідомлень, які спотворюють показники сенсорів чи вводять неправильні команди на виконавчі вузли.

На рис. 1.20 звернено увагу на уразливості індустріальних протоколів (наприклад, Modbus без шифрування), недостатній захист комунікаційного обладнання та можливість відключення або порушення роботи окремих компонентів (unplanned shutdown). Це ілюструє, що атаки в ICS/SCADA охоплюють різні рівні — від фізичних пристроїв до мережевих протоколів і рівня даних. У сукупності цей рисунок підкреслює необхідність багаторівневого і глибокого захисту, який враховує всі можливі шляхи проникнення та компрометації.

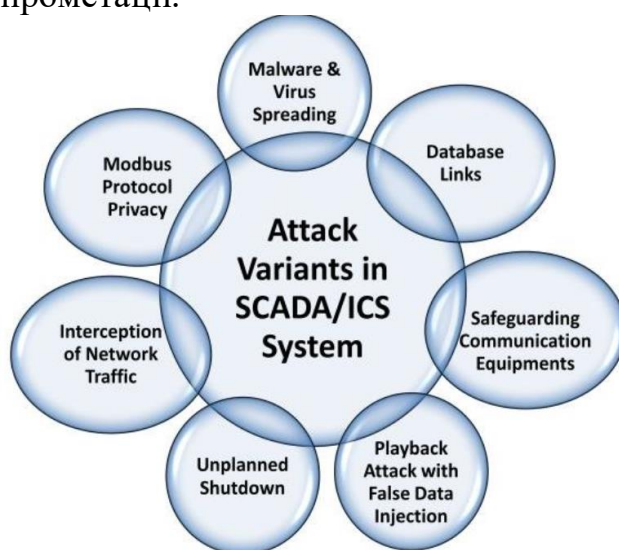


Рис. 1.20. Типові вектори атак у SCADA / ICS-системах (Attack Variants in SCADA/ICS)

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Крім цілеспрямованих шкідливих кампаній, загрози для ICS/SCADA охоплюють широкий спектр ризиків, пов'язаних із людським фактором, технічними збоями та вразливостями у промислових протоколах. Частими є атаки через віддалений доступ (Remote Access Exploits), коли зломисники використовують слабкі паролі або неконтрольовані VPN-з'єднання для проникнення у виробничу мережу. Значну небезпеку становлять атаки через ланцюг постачання (Supply Chain Attacks), під час яких компрометуються оновлення ПЗ або сторонні бібліотеки, що використовуються у SCADA-додатках. Фішингові кампанії проти операторів або інженерів можуть призвести до викрадення облікових даних, відкриття шкідливих вкладень і несанкціонованого доступу до панелей керування.

Окрему категорію складають вразливості промислових протоколів — таких як Modbus, DNP3, IEC 60870-5-104, OPC-UA — які часто не передбачають автентифікації або шифрування, що робить їх привабливими для атак типу *Man-in-the-Middle (MitM)* чи *Replay*. Унаслідок таких дій зловмисник може змінювати сигнали керування, підміняти показники сенсорів або створювати хибні аварійні події. Не менш небезпечними є атаки на Denial of Service (DoS/DDoS), які перевантажують контролери або шлюзи SCADA, блокуючи обмін даними між рівнями управління.

Важливим напрямом захисту від подібних загроз є впровадження архітектури Zero Trust у промислових середовищах, де жоден пристрій чи користувач не вважається безпечним за замовчуванням. Для цього реалізується багаторівнева аутентифікація, мікросегментація мереж, обмеження прав доступу до мінімально необхідних, а також моніторинг усіх транзакцій у режимі реального часу. Системи аномалійного виявлення (Anomaly Detection Systems) аналізують поведінку PLC, HMI, шлюзів і сенсорів, фіксуючи навіть мінімальні відхилення від нормального функціонування.

Додатково запроваджується моніторинг активів (Asset Inventory & Vulnerability Management), що дозволяє своєчасно виявляти нові пристрої, невідомі з'єднання чи застарілі прошивки. Регулярне оновлення сигнатур IDS/IPS, перевірка контрольних сум файлів і використання цифрових підписів гарантують, що будь-які спроби несанкціонованих змін будуть оперативно виявлені. У поєднанні з безперервним навчанням персоналу, симуляціями атак і політикою реагування на інциденти ці заходи створюють багатокомпонентну систему кіберзахисту, здатну ефективно протидіяти навіть складним багатовекторним загрозам у середовищі ICS/SCADA.

Отже, безпека ICS/SCADA-систем — це багаторівневий процес, що охоплює технічні, криптографічні, мережеві та організаційні заходи. Її ефективність залежить від інтеграції IT- і OT-безпеки, безперервного моніторингу та готовності до реагування на інциденти. Такий підхід забезпечує стійкість критичної інфраструктури до сучасних кіберзагроз і гарантує безперервність життєво важливих процесів держави.

Додатково важливим чинником є формування культури безпеки серед персоналу, адже людський фактор залишається одним із найвразливіших елементів промислових систем. Постійне навчання, проведення тренувань і симуляцій кіберінцидентів сприяють підвищенню готовності до реагування на реальні загрози. Використання концепції Zero Trust та принципу мінімально необхідних привілеїв дозволяє значно обмежити можливості зловмисників у разі компрометації окремого вузла. Також важливо впроваджувати політику резервного копіювання та аварійного відновлення, що гарантує збереження даних і швидке повернення до штатної роботи після інцидентів.

Централізований моніторинг подій безпеки, застосування SIEM- і SOAR-рішень, аналіз журналів подій і поведінкових відхилень створюють основу для превентивного виявлення атак. У сукупності це формує надійну систему захисту ICS/SCADA, орієнтовану на стійкість, контроль і безперервність технологічних процесів.

1.5. Конфіденційність і захист персональних даних (GDPR, ССРА, УКРАЇНСЬКЕ ЗАКОНОДАВСТВО)

Конфіденційність і захист персональних даних є одним із ключових аспектів сучасної інформаційної безпеки, адже у цифрову епоху дані стали стратегічним ресурсом, від якого залежать довіра, репутація й стабільність бізнесу та державних структур. Головна мета захисту персональних даних полягає у забезпеченні конфіденційності, цілісності, доступності й законності обробки інформації, що стосується ідентифікованих або потенційно ідентифікованих осіб. У світі діють різні нормативно-правові режими, зокрема Загальний регламент Європейського Союзу із захисту даних (GDPR), Закон Каліфорнії про захист прав споживачів (ССРА) і Закон України «Про захист персональних даних», які спільно формують правову основу для регулювання цього процесу.

Регламент GDPR (General Data Protection Regulation)

Регламент GDPR (General Data Protection Regulation, ЄС 2016/679) є найвідомішим міжнародним стандартом, що встановлює принципи законності, справедливості й прозорості обробки даних, мінімізації обсягу зібраної інформації, її точності, обмеження зберігання, цілісності та конфіденційності. Цей документ поширюється на всі компанії, які обробляють персональні дані громадян ЄС, незалежно від країни розташування. Користувачам надаються широкі права — доступ до власних даних, виправлення, видалення (“право бути забутим”), перенесення, обмеження обробки та заборона автоматизованого профілювання. Порушення вимог GDPR тягне за собою серйозну фінансову відповідальність — штрафи можуть сягати 20 мільйонів євро або 4 % річного глобального обороту компанії. Для дотримання вимог впроваджуються процедури Data Protection Impact Assessment (DPIA), призначаються уповноважені фахівці з питань захисту даних (Data Protection Officer, DPO), застосовуються шифрування, псевдонімізація, токенизація, контроль доступу та аудит операцій обробки.

Регламент GDPR (General Data Protection Regulation, ЄС 2016/679) є основним правовим актом Європейського Союзу, який уніфікував підходи до захисту персональних даних у всіх державах-членах ЄС і став світовим

еталоном у сфері конфіденційності. Його метою є захист основних прав і свобод фізичних осіб, зокрема права на приватність і контроль над власною інформацією. Регламент запроваджує принцип “accountability” (відповідальності), який вимагає від організацій не лише дотримуватись вимог, а й бути здатними довести їх виконання. Це означає документування кожного процесу обробки даних, ведення реєстрів, проведення внутрішніх аудитів і створення політик безпеки даних.

GDPR поширюється на будь-яку організацію, яка збирає або обробляє персональні дані громадян ЄС — навіть якщо її офіс знаходиться поза межами Союзу. Це включає компанії, що пропонують товари або послуги мешканцям Європи, а також ті, які відстежують їхню поведінку в Інтернеті (наприклад, через cookies, трекери або системи аналітики). Кожен суб'єкт даних (data subject) має низку гарантованих прав, серед яких право на доступ до своїх даних, право на їх виправлення чи видалення (“право бути забутим”), право на обмеження обробки, право на перенесення даних до іншого контролера та право заперечити проти автоматизованого прийняття рішень, що може впливати на нього. Ці права забезпечують повний контроль користувача над тим, як, де і з якою метою обробляється його інформація.

Особливу увагу GDPR приділяє законним підставам обробки персональних даних. Вони включають: згоду суб'єкта даних; необхідність виконання договору; виконання юридичного обов'язку; захист життєво важливих інтересів; виконання завдання в інтересах суспільства; або законний інтерес контролера, який не перевищує прав і свобод суб'єкта даних. Кожна організація повинна чітко визначити підставу, на якій вона здійснює обробку, та задокументувати її у політиці конфіденційності. У разі збору згоди користувача ця згода має бути добровільною, конкретною, інформованою та недвозначною, а відмова від неї — такою ж простою, як і надання.

Регламент також вимагає впровадження Privacy by Design і Privacy by Default — принципів, за якими захист персональних даних закладається в архітектуру системи ще на етапі проєктування, а всі налаштування за замовчуванням забезпечують максимальну конфіденційність. Наприклад, інформаційні системи повинні передбачати шифрування даних у процесі зберігання і передавання, мінімізацію обсягу зібраної інформації, а також обмеження доступу лише для авторизованих осіб.

Для підвищення прозорості обробки даних компанії зобов'язані призначати уповноваженого з питань захисту даних (Data Protection Officer, DPO), який контролює дотримання GDPR, консультує співробітників, проводить оцінку ризиків і взаємодіє з контролюючими органами. У разі виявлення інциденту безпеки (data breach), організація повинна повідомити про

нього компетентний орган нагляду протягом 72 годин, а якщо порушення може зашкодити користувачам — також поінформувати самих суб'єктів даних.

Для оцінки ризиків перед обробкою персональної інформації проводиться Data Protection Impact Assessment (DPIA) — аналіз впливу на конфіденційність, який дозволяє виявити потенційні загрози, оцінити ймовірність витоку або зловживання даними та визначити заходи для їх зниження. Також регламент вимагає технічних і організаційних заходів захисту — шифрування (AES, RSA, ECC), псевдонімізації, токенизації, багаторівневого контролю доступу, журналювання, моніторингу й аудитів безпеки.

Важливим аспектом є міжнародна передача даних. GDPR забороняє передавати персональні дані в країни, які не забезпечують належний рівень захисту, якщо лише не існують спеціальні угоди (наприклад, Standard Contractual Clauses або Binding Corporate Rules). Це положення стимулює гармонізацію законодавства у сфері конфіденційності у всьому світі.

Порушення вимог GDPR може мати серйозні наслідки — штрафи сягають до 20 мільйонів євро або 4 % від річного світового обороту компанії, залежно від того, яка сума більша. Проте найбільшим наслідком є втрата довіри користувачів і репутаційні ризики. Успішне впровадження вимог регламенту не лише підвищує рівень безпеки даних, а й створює конкурентну перевагу, демонструючи користувачам відповідальність, прозорість і надійність компанії у цифровому середовищі.

Отже, GDPR — це не просто закон, а комплексна система управління приватністю, яка інтегрує правові, організаційні та технічні принципи захисту персональних даних. Його дотримання сприяє формуванню культури інформаційної відповідальності, забезпечує цифрову довіру та підтримує баланс між технологічним прогресом і правами людини.

Закон CCPA (California Consumer Privacy Act)

Американський закон CCPA (California Consumer Privacy Act) орієнтований на надання мешканцям Каліфорнії контролю над тим, як компанії збирають, зберігають і передають їхні дані. Закон гарантує право споживачів знати, які саме дані збираються й кому передаються, вимагати їх видалення, а також заборонити продаж інформації третім сторонам. Компанії зобов'язані забезпечити прозорість у повідомленнях про збір даних, а також не дискримінувати користувачів, які реалізують свої права. CCPA застосовується до підприємств із річним доходом понад 25 мільйонів доларів або до тих, які обробляють понад 50 тисяч записів персональних даних чи отримують понад 50 % доходу від їхнього продажу.

Закон CCPA (California Consumer Privacy Act) є одним із найважливіших нормативних актів США у сфері захисту персональних даних, який набув чинності 1 січня 2020 року та став першим масштабним законодавчим кроком

до формування американського аналога європейського GDPR. Його головна мета — надати мешканцям штату Каліфорнія більше контролю над тим, як компанії збирають, зберігають, обробляють і передають їхні персональні дані. Закон розроблено як реакцію на зростання кількості інцидентів витоку інформації, непрозорі практики цифрового маркетингу й комерційне використання персональних даних без відома користувачів.

ССРА поширюється на будь-яку компанію, що здійснює бізнес у Каліфорнії, якщо вона відповідає хоча б одному з таких критеріїв: має річний валовий дохід понад 25 мільйонів доларів США; обробляє або збирає персональні дані понад 50 000 осіб, домогосподарств чи пристроїв; або отримує понад 50 % доходу від продажу персональних даних споживачів. Закон застосовується не лише до великих корпорацій, а й до компаній-посередників, які обробляють дані від імені інших організацій, включаючи рекламні агентства, аналітичні сервіси й технологічні платформи.

Основою ССРА є чотири ключові права споживачів, які формують концепцію “digital self-determination” — цифрового самовизначення особи. По-перше, це право знати (Right to Know), яке дозволяє громадянам дізнатися, які саме персональні дані збирає компанія, з якою метою, які категорії третіх сторін мають до них доступ і протягом якого часу вони зберігаються. По-друге, право на видалення (Right to Delete) надає можливість вимагати повного або часткового видалення персональних даних із систем компанії, якщо їх подальше зберігання не є необхідним. По-третє, право на відмову від продажу (Right to Opt-Out) дозволяє користувачам заборонити передачу або продаж їхніх даних іншим суб'єктам (“Do Not Sell My Personal Information”). Нарешті, право на недискримінацію (Right to Non-Discrimination) гарантує, що компанії не можуть відмовити у послугах, підвищити ціну або знизити якість продукту для користувачів, які реалізували свої права на захист приватності.

ССРА встановлює широке визначення “персональних даних”, яке охоплює не лише ідентифікаційні дані (ім'я, адреса, номер телефону, e-mail), але й біометричні дані, геолокацію, історію пошуку, IP-адресу, дані про активність у мобільних додатках, записи дзвінків, навіть поведінкові профілі користувачів, сформовані на основі їхніх онлайн-звичок. Такий підхід відображає прагнення законодавців до максимального охоплення усіх форм цифрової інформації, яка потенційно може ідентифікувати особу.

Компанії, що підпадають під дію закону, зобов'язані дотримуватись принципу “privacy by transparency” (прозорості обробки). Це означає, що вони мають розмішувати на своїх вебсайтах чітко сформульовану політику конфіденційності, де зазначаються категорії зібраних даних, способи їх використання, строки зберігання та механізми реалізації прав користувача. Особливим обов'язком є наявність окремої кнопки або посилання “Do Not Sell

My Personal Information”, через яке споживач може заборонити продаж своїх даних третім сторонам. Крім того, підприємства повинні розробити внутрішні процедури обробки запитів користувачів і надати відповідь не пізніше ніж протягом 45 днів після отримання запиту.

ССРА також вимагає від компаній запровадження надійних технічних і організаційних заходів захисту. Це включає використання шифрування, анонімізації, контроль доступу, багаторівневу автентифікацію й системи моніторингу несанкціонованого доступу до даних. У разі витоку персональних даних компанія зобов'язана негайно повідомити споживачів та органи нагляду, а за порушення встановлених вимог можуть бути накладені штрафи — до 7 500 доларів за навмисне порушення і до 2 500 доларів за ненавмисне.

У 2023 році ССРА було розширено за рахунок прийняття California Privacy Rights Act (CPRA), який утворив спеціальний Каліфорнійський агентство із захисту приватності (California Privacy Protection Agency, CPPA), що має повноваження контролювати виконання закону, розробляти нові стандарти й проводити перевірки компаній. CPRA також додав нові категорії чутливих персональних даних (Sensitive Personal Information) — наприклад, расову чи етнічну приналежність, стан здоров'я, геолокацію в реальному часі або номери банківських рахунків.

Таким чином, ССРА і його оновлена версія CPRA створили правову основу для розвитку американської культури захисту приватності, орієнтованої на прозорість, контроль користувача й відповідальність бізнесу. Цей закон став прикладом для інших штатів США (наприклад, Вірджинії, Колорадо, Юти), які приймають подібні акти, і водночас — важливим елементом глобальної тенденції гармонізації стандартів захисту персональних даних, спрямованої на формування єдиної етики цифрової довіри у світі.

Закон України «Про захист персональних даних»

В Україні правове регулювання здійснюється відповідно до Закону України «Про захист персональних даних» (№2297-VI), який гармонізується з принципами GDPR. Закон визначає, що обробка персональних даних можлива лише за згодою суб'єкта або в межах визначеної законом мети. Вимоги включають обов'язок забезпечення технічного й криптографічного захисту баз даних, заборону передачі даних без згоди суб'єкта, повідомлення про обробку, реєстрацію баз даних і право користувача вимагати виправлення чи видалення інформації. Україна поступово імплементує положення GDPR, зокрема через законопроект про створення Національного органу із захисту даних і впровадження штрафних санкцій за європейськими зразками.

Технічні заходи захисту персональних даних включають використання криптографічних алгоритмів (AES-256, RSA, TLS 1.3) для шифрування інформації під час передавання та зберігання, а також псевдонімізацію та

токенізацію для унеможливлення ідентифікації користувача. Системи контролю доступу впроваджують багатофакторну автентифікацію, принцип мінімальних привілеїв і ведення журналів дій, а технології Data Loss Prevention (DLP) запобігають несанкціонованому копіюванню чи передаванню файлів. Постійний моніторинг, аудит і застосування SIEM-систем забезпечують виявлення аномалій у роботі та спроб витоку даних. Важливо, щоб розробники застосовували концепцію Privacy by Design — коли вимоги до конфіденційності закладаються в архітектуру інформаційних систем із самого початку.

Закон України «Про захист персональних даних» (№2297-VI від 1 червня 2010 року) є основним нормативно-правовим актом, що регламентує порядок обробки, зберігання, передачі та захисту персональних даних громадян України. Він забезпечує реалізацію конституційного права на недоторканність приватного життя та гармонізується з європейськими підходами до конфіденційності, зокрема з положеннями GDPR (General Data Protection Regulation). Основна мета закону — забезпечити законність, справедливість і безпечність обробки персональних даних, а також запобігти їхньому несанкціонованому використанню, витоку або знищенню.

Закон визначає персональні дані як будь-яку інформацію про фізичну особу, яка ідентифікована або може бути ідентифікована. До таких даних належать: ім'я, прізвище, паспортні та ідентифікаційні номери, адреса, дата народження, відомості про місце роботи, стан здоров'я, освіту, сімейний стан, фінансові показники тощо. Обробка таких даних може здійснюватися лише за згодою суб'єкта персональних даних або у випадках, передбачених законом (наприклад, для виконання трудових, податкових, фінансових чи адміністративних зобов'язань).

Основні принципи обробки персональних даних, закріплені в законі, включають:

- законність і прозорість — дані повинні збиратися на законних підставах і лише для визначених цілей;
- цільове використання — заборонено обробляти дані для цілей, не сумісних із початковою метою збору;
- точність і актуальність — оператор зобов'язаний забезпечити коректність і своєчасне оновлення інформації;
- мінімізацію даних — збір лише тих відомостей, які є необхідними для реалізації поставленої мети;
- збереження протягом обмеженого часу — дані підлягають видаленню після досягнення мети їх обробки;
- цілісність і конфіденційність — оператор має забезпечити захист даних від несанкціонованого доступу, знищення або зміни.

Оператори та розпорядники персональних даних (державні установи, підприємства, приватні компанії) несуть відповідальність за забезпечення безпеки оброблюваних даних. Закон зобов'язує їх розробляти політики конфіденційності, призначати відповідальних осіб за захист інформації, а також впроваджувати організаційні та технічні заходи безпеки. До таких заходів належать:

- аутентифікація та авторизація користувачів, обмеження доступу до баз даних за ролями;
- криптографічний захист (зокрема, алгоритми AES-256, RSA, TLS 1.3 для шифрування трафіку та збережених даних);
- резервне копіювання й відновлення інформації у разі інцидентів;
- журналювання дій користувачів і проведення аудитів безпеки;
- системи виявлення й запобігання вторгненням (IDS/IPS) та SIEM-рішення для моніторингу подій і кореляції інцидентів;
- Data Loss Prevention (DLP) — контроль над копіюванням, пересиланням і виносом файлів із систем;
- псевдонімізація та токенизація — заміна ідентифікаційних даних умовними маркерами для запобігання прямому розкриттю особи.

Важливим елементом є отримання поінформованої згоди суб'єкта даних. Згода повинна бути добровільною, усвідомленою, конкретною та оформленою письмово або в електронній формі. Суб'єкт персональних даних має право:

- отримувати інформацію про умови обробки своїх даних;
- вимагати виправлення, оновлення або видалення недостовірних чи надлишкових відомостей;
- відкликати згоду на обробку в будь-який момент;
- звернутися до суду або Уповноваженого Верховної Ради України з прав людини у разі порушення своїх прав.

Україна поступово наближає своє законодавство до європейських стандартів. У рамках процесу євроінтеграції розроблено нову редакцію закону, що передбачає створення Національного органу з питань захисту персональних даних — спеціалізованого незалежного регулятора, подібного до європейських Data Protection Authorities. Також планується запровадження штрафних санкцій, аналогічних до GDPR (у відсотках від обороту компанії), посилення відповідальності за витоки даних, а також введення обов'язкових процедур оцінки впливу на приватність (DPIA) та інцидентного звітування у разі порушення безпеки даних.

На практичному рівні підприємства повинні впроваджувати концепцію “Privacy by Design” та “Privacy by Default”, коли захист приватності інтегрується в архітектуру інформаційних систем ще на етапі проєктування, а налаштування за замовчуванням мінімізують обсяг оброблюваних даних. Це

включає автоматичне шифрування каналів зв'язку, розмежування повноважень адміністраторів, контроль життєвого циклу даних і регулярні перевірки на відповідність вимогам.

Таким чином, Закон України «Про захист персональних даних» формує національну систему управління конфіденційністю, що базується на принципах прозорості, відповідальності та технологічної безпеки. Його імплементація не лише забезпечує захист громадян у цифровому середовищі, але й створює передумови для інтеграції України у європейський простір довіри — де приватність визнається фундаментальним правом, а безпечне використання інформації стає ключовою умовою сталого розвитку цифрової економіки.

Таким чином, конфіденційність і захист персональних даних — це не лише юридичне зобов'язання, а й стратегічна складова довіри в цифровому суспільстві. Дотримання вимог GDPR, ССРА та українського законодавства сприяє формуванню культури обережного поводження з даними, зміцнює кіберстійкість підприємств і підвищує довіру користувачів. Ефективний захист персональних даних базується на поєднанні нормативних, технічних і організаційних механізмів, які забезпечують відповідальне управління інформацією, запобігають витокам і гарантують прозорість усіх процесів обробки у сучасному цифровому середовищі.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 1

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

6. Шевченко, С., Жданова, Ю., & Гаркушенко, А. (2025). Когнітивний підхід в інформаційній та кібербезпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 854–866. <https://doi.org/10.28925/2663-4023.2025.29.945>
7. Чернігівський, І., & Крючкова, Л. (2025). Тестування нейромережових моделей для вирішення задачі виявлення заражених ПК на базі цифрових слідів. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 800–817. <https://doi.org/10.28925/2663-4023.2025.29.941>
8. Романюк, В., & Платоненко, А. (2025). Аналіз якості генераторів рожевого шуму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 789–799. <https://doi.org/10.28925/2663-4023.2025.29.940>
9. Соболенко, І., & Платоненко, А. (2025). Автоматизоване виявлення аномалій у трафіку корпоративних бездротових мереж за допомогою Python: методи, реалізація та оцінка ефективності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 777–788. <https://doi.org/10.28925/2663-4023.2025.29.939>
10. Соколов, В. (2025). Технологія відслідковування переміщення абонентів територією підприємства критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 207–222. <https://doi.org/10.28925/2663-4023.2025.29.920>
11. Складанний, П., Гулак, Г., & Корнієць, В. (2025). Коаліційний підхід до управління кібербезпекою інформаційних систем що застосовують хмарні технології. Кібербезпека: освіта, наука, техніка, 4(28), 8–25. <https://doi.org/10.28925/2663-4023.2025.27.825>
12. Довженко, Н., Іваніченко, Є., Аушева, Н., Шевчук, Ю., & Луковський, Т. (2025). Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. Кібербезпека: освіта, наука, техніка, 4(28), 547–564. <https://doi.org/10.28925/2663-4023.2025.28.835>
13. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для студентів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 70 с.
14. Шевченко, С., Жданова, Ю., Складанний, П., & Іщук, М. (2025). Створення блокчейн-платформи для електронного голосування. Кібербезпека: освіта, наука, техніка, 4(28), 701–714. <https://doi.org/10.28925/2663-4023.2025.28.860>

15. Крючкова, Л., & Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. *Кібербезпека: освіта, наука, техніка*, 4(28), 766–780. <https://doi.org/10.28925/2663-4023.2025.28.863>
16. Цехмейстер, Р., Платоненко, А., Ворохоб, М., Черевик, В., & Семеняка, С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. *Кібербезпека: освіта, наука, техніка*, 3(27), 63–71. <https://doi.org/10.28925/2663-4023.2025.27.703>
17. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebeshko, B., & Khorolska, K. Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, (CPITS-II 2024) October 26, 2024. Aachen: CEUR, 2024. Vol. 3826. P. 129–138. ISSN: 1613-0073.
18. Олійник, Я., Платоненко, А., Черевик, В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. *Кібербезпека: освіта, наука, техніка*, 3(27), 100–108. <https://doi.org/10.28925/2663-4023.2025.27.705>
19. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей Курамото ДЛЯ ідентифікації дезінформації у соціальних мережах. *Кібербезпека: освіта, наука, техніка*, 3(27), 406–416. <https://doi.org/10.28925/2663-4023.2025.27.754>
20. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., Sokolov, V. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 249-264. ISSN 1613-0073.
21. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» для студентів спеціальності 123 Комп'ютерна інженерія, освітньої програми 123.00.01 Комп'ютерна інженерія / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 82 с.
22. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., Korshun, N. Models and algorithms for analyzing information risks during the security audit of personal data information system. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 155-171. ISSN 1613-0073.
23. Довженко, Н., Складанний, П., Іваніченко, Є., & Жильцов, О. (2025). Модель динамічної взаємодії безпілотних літальних апаратів із сенсорною мережею для енергоефективного моніторингу. *Кібербезпека: освіта, наука, техніка*, 3(27), 466–478. <https://doi.org/10.28925/2663-4023.2025.27.766>

24. Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z. Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 14-25. ISSN 1613-0073.
25. Гайдук, О., Зверев, В., & Гулак, Г. (2025). Кореляційний аналіз типів кіберінцидентів в контексті інформаційних технологій міжнародних комунікацій. Кібербезпека: освіта, наука, техніка, 3(27), 417–428. <https://doi.org/10.28925/2663-4023.2025.27.757>
26. Kostiuk Y., Skladannyi P., Sokolov V., Zhytsov O., Ivanichenko Y. Effectiveness of Information Security Control using Audit Logs. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 524-538. ISSN 1613-0073.
27. Kostiuk Y., Skladannyi, P., Sokolov, V., Vorokhob, M. Models and technologies of cognitive agents for decision-making with integration of Artificial Intelligence. Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025). Aachen: CEUR, 2025. Vol. 4005. P. 82–96. ISSN 1613-0073.
28. Чернігівський, І., & Крючкова, Л. (2025). Системний підхід до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів. Кібербезпека: освіта, наука, техніка, 3(27), 572–590. <https://doi.org/10.28925/2663-4023.2025.27.781>
29. Skladannyi P., Kostiuk Y., Rzaieva S., Bebeshko, B., Korshun, N. Adaptive Methods for Embedding Digital Watermarks to Protect Audio and Video Images in Information and Communication Systems. Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 13–31. ISSN 1613-0073.
30. Чернігівський, І., & Крючкова, Л. (2025). Ефективні рішення для швидкого виявлення скомпрометованих ПК в інфокомунікаційних мережах. Телекомунікаційні та інформаційні технології, 2(87), 24–32. <https://doi.org/10.31673/2412-4338.2025.029875>
31. Kostiuk Y., Skladannyi, P., Khorolska, K., Sokolov, V., Hulak, H. Application of Statistical and Neural Network Algorithms in Steganographic Synthesis and Analysis of Hidden Information in Audio and Graphic Files. Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 45–65. ISSN 1613-0073.
32. Чернігівський, І., & Крючкова, Л. (2024). Тестування антивірусних рішень для корпоративного сегменту. Безпека інформації, 30(3), 407–413. <https://doi.org/10.18372/2225-5036.30.20362>

33. Skladannyi, P., Kostiuk Y., Khorolska, K., Bebashko, B., Sokolov, V. Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. Proceedings of the Workshop Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 17–36. ISSN 1613-0073.

34. Соколов, В. (2025). Забезпечення стійкості безпроводових систем до атак глушіння. Телекомунікаційні та інформаційні технології, 1(86), 50–60. <https://doi.org/10.31673/2412-4338.2025.013623>

35. Kostiuk, Y., Rzaieva S., Khorolska, K., Mazur, N., Korshun, N. Architecture of the software system of confidential access to information resources of computer networks. Proceedings of the Workshop Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 37–53. ISSN 1613-0073.

36. Корнієць, В., & Складанний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. Телекомунікаційні та інформаційні технології, 4(85), 90–96. <https://doi.org/10.31673/2412-4338.2024.040224>

КОНТРОЛЬНІ ПИТАННЯ

1. Які ключові відмінності у вимогах до захисту між дротовими та безпроводовими мережами і як ці відмінності впливають на вибір криптографічних механізмів?

2. Чому WPA3-Enterprise з EAP-TLS вважається кращим для корпоративних Wi-Fi і яку роль відіграють 802.1X, PMF та 802.11r/k/v у стійкості до типових атак?

3. Опишіть, як багаторівнева сегментація SSID/VLAN у Wi-Fi разом із RADIUS та динамічними VLAN знижує ризик компрометації IoT-сегментів.

4. Які функції виконує Trust Center у ZigBee і чим відрізняються Network Key, Master Key та Link Key з погляду загроз replay та підміни вузлів?

5. Поясніть архітектурну роль Security Manager у Bluetooth та порівняйте режими SSP Just Works, Numeric Comparison, Passkey і OOB щодо захисту від MITM-атак.

6. У чому полягає сутність relay-атаки на NFC і які технічні та організаційні засоби найефективніше її стримують?

7. Які новації 5G щодо суверенності ідентифікаторів абонента усувають проблеми IMSI-catchers і як працює механізм SUCI та EAP-AKA'?

8. Чим обґрунтована необхідність Network Slicing у 5G для критичних сервісів і як політики безпеки для різних slices ізолюють інциденти?

9. Наведіть приклади атак sinkhole, wormhole, Sybil і selective forwarding у WSN та поясніть, які комбіновані засоби виявлення і стримування доцільні для кожної з них.

10. Сформууйте перелік мінімально необхідних вимог до безпеки пристрою IoT на етапах життєвого циклу від виробництва до списання з акцентом на secure boot, SBOM та відкликання ключів.

11. Чому шлюзи та edge-вузли є найризиковішою точкою в IoT-архітектурі і як mTLS, vault-менеджмент секретів та rate limiting знижують імовірність компрометації?

12. Порівняйте TLS, DTLS та IPsec для захисту трафіку IoT/WSN у контексті обмежених ресурсів і вимог до затримок у URLLC.

13. Які відмінності в розподілі зон відповідальності безпеки між IaaS, PaaS та SaaS і які ризики найчастіше виникають на боці користувача у кожній моделі?

14. Яку роль відіграють CASB-рішення у моделі IaaS і як інтеграція з CI/CD та контейнерними платформами підтримує DevSecOps-практики?

15. Побудуйте приклад політики Zero Trust для хмарного середовища з описом контролю доступу, перевірок на рівні API, шифрування та спостережності.

16. Запропонуйте метрики для оцінювання кіберстійкості спеціалізованих середовищ з урахуванням CIA та часу виявлення і локалізації інцидентів у SIEM/SOAR.

17. Які правові вимоги GDPR і українського законодавства є критичними для хмарної обробки персональних даних і як псевдонімізація, анонімізація та диференційна приватність їх підтримують?

18. Складіть план аудиту конфігурацій Wi-Fi інфраструктури підприємства з перевітками WPA3, 802.11w, вимкнення WPS, ротації ключів, журналювання та WIDS/WIPS.

19. Запропонуйте архітектуру безпечного оновлення прошивок для IoT з урахуванням підпису, перевірки цілісності, захищених каналів доставки, rollback-захисту та журналювання.

20. Для промислової WSN побудуйте поетапну стратегію реагування на виявлену wormhole-атаку з використанням кластеризації, ізоляції сегментів, перевидання ключів та повторного маршрутизаційного узгодження.

РОЗДІЛ 2

АРХІТЕКТУРА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ (КСЗІ) ТА ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



- 2.1. Моделювання архітектури КСЗІ на підприємстві***
- 2.2. Організаційний, технічний та політичний рівні захисту***
- 2.3. Інтеграція SIEM, SOC та засобів моніторингу***
- 2.4. Методи оцінки ефективності та тестування КСЗІ***
- 2.5. Розробка та впровадження політики безпеки***

Архітектура комплексних систем захисту інформації (КСЗІ) та політика інформаційної безпеки становлять взаємопов'язану основу побудови й функціонування системи безпеки підприємства. Комплексна система захисту інформації — це організована сукупність технічних, програмних, криптографічних та організаційно-правових заходів, спрямованих на забезпечення конфіденційності, цілісності, доступності та спостережності інформації в інформаційно-комунікаційних системах. Її архітектура визначає структуру, взаємозв'язки та функціональні рівні системи безпеки, що включають політичний, організаційний і технічний рівні. На політичному рівні формуються стратегічні цілі, принципи, політика безпеки й розподіл відповідальності між учасниками процесу. Організаційний рівень охоплює управління ризиками, аудит, реагування на інциденти, адміністрування доступу та підтримку нормативно-правової бази. Технічний рівень реалізує конкретні засоби захисту — системи ідентифікації та аутентифікації користувачів, керування доступом, криптографічного захисту, моніторингу подій безпеки (SIEM/SOC), а також технології шифрування трафіку, захищеного з'єднання,

резервного копіювання та відновлення даних для забезпечення безперервності діяльності.

Політика інформаційної безпеки є концептуальною основою КСЗІ, оскільки визначає мету, сферу дії, принципи, вимоги та порядок реалізації заходів безпеки. Вона встановлює правила класифікації інформації, умови доступу до ресурсів, відповідальність персоналу, порядок реагування на кіберінциденти, а також критерії контролю, аудиту й оновлення політики з урахуванням розвитку загроз та змін законодавства. Політика забезпечує узгодженість усіх дій у сфері безпеки, створює єдині стандарти управління ризиками й формує організаційне середовище, у межах якого архітектура КСЗІ реалізує технічну підтримку цих принципів. Таким чином, політика інформаційної безпеки виступає стратегічною складовою системи, а архітектура КСЗІ — її практичним втіленням, що забезпечує реальну стійкість, керованість та адаптивність підприємства до динамічних кіберзагроз.

2.1. МОДЕЛЮВАННЯ АРХІТЕКТУРИ КСЗІ НА ПІДПРИЄМСТВІ

Моделювання архітектури комплексної системи захисту інформації (КСЗІ) на підприємстві — це системний процес розроблення, структуризації та аналізу всіх елементів системи безпеки, що забезпечують захист інформаційних активів від внутрішніх і зовнішніх загроз. Його мета полягає у створенні цілісної моделі, яка відображає взаємозв'язки між технічними, програмними, організаційними та управлінськими компонентами системи. Такий підхід дозволяє визначити межі системи захисту, ідентифікувати критичні ресурси, сформулювати канали обробки інформації та оцінити рівень ризиків на кожному етапі її життєвого циклу.

Під час моделювання архітектури КСЗІ враховуються особливості бізнес-процесів підприємства, рівні доступу користувачів, обсяги та категорії оброблюваних даних, а також вимоги до продуктивності, надійності й відповідності нормативним актам (зокрема, Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і стандартам ISO/IEC 27001, 15408). У процесі побудови моделі визначаються функціональні області системи: управління доступом, криптографічний захист, аудит і моніторинг, резервне копіювання, реагування на інциденти, управління оновленнями, а також забезпечення безперервності діяльності (BCP/DRP). Кожен з цих компонентів проектується у вигляді підсистеми, які взаємодіють між собою через захищені канали обміну даними.

На рис. 2.1 зображено двошарову архітектуру, у якій у площині даних суб'єкт взаємодіє із системою, що вважається недовіреною до моменту прийняття рішення політики, після чого трафік прямує через Policy Enforcement Point до корпоративного ресурсу як «довірений» лише за умови виконання правил доступу; у площині

керування працює Policy Decision Point, що складається з Policy Engine та Policy Administrator і формує та застосовує рішення політики для PER через керувальні канали. Ліворуч до PDP надходять контекстні сигнали з безперервного моніторингу стану (CDM), вимог галузевого комплаєнсу, розвідки кіберзагроз і журналів активності, праворуч підключені опорні сервіси політик доступу до даних, РКІ, керування ідентичностями та SIEM для кореляції подій; усі вони разом збагачують правила авторизації та підтримують динамічну перевірку довіри на кожен запит. Таке компонування показує, як рішення доступу приймаються централізовано на основі багатих сигналів та застосовуються «на краю» в PER, забезпечуючи мінімальні привілеї, постійну валідацію, спостережуваність і узгодженість логічної моделі КСЗІ з практиками Zero Trust.

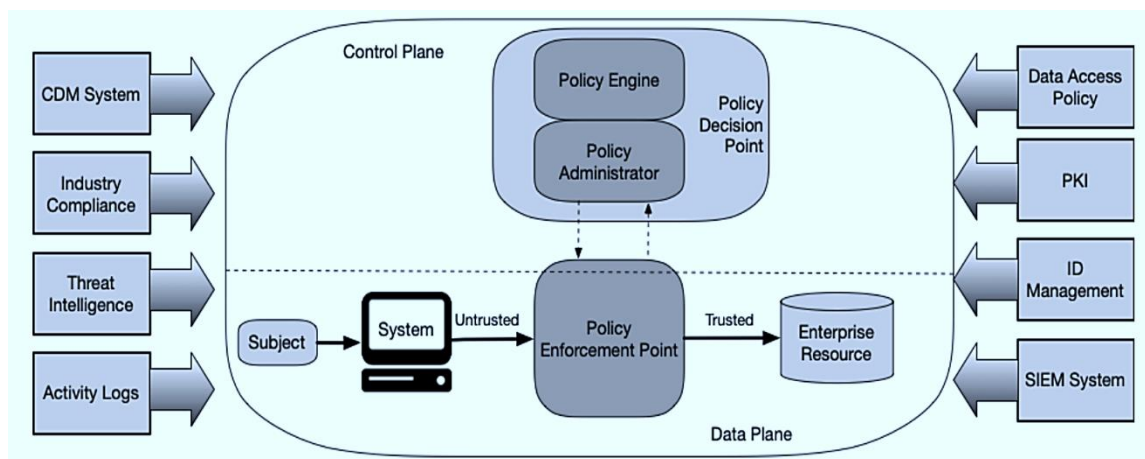


Рис. 2.1. Логічна модель Zero Trust у КСЗІ: площини керування та даних із компонентами Policy Engine/Policy Administrator (PDP) і Policy Enforcement Point (PEP)

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102]

Моделювання архітектури КСЗІ зазвичай виконується у кілька етапів.

Етап 1. Аналіз об'єкта захисту — ідентифікація інформаційних активів, визначення загроз і вразливостей, оцінка критичності процесів.

Аналіз об'єкта захисту є першим і одним із ключових етапів моделювання архітектури комплексної системи захисту інформації (КСЗІ) на підприємстві, оскільки саме він визначає, які інформаційні ресурси потребують захисту, які загрози можуть їм завдати та наскільки критичними є наслідки їх порушення. На цьому етапі здійснюється ідентифікація інформаційних активів, тобто ресурсів, що мають цінність для підприємства. До них належать дані, інформаційні системи, технічні засоби, мережеве обладнання, комунікаційна інфраструктура, персонал, а також внутрішня документація та нормативні політики. Ідентифіковані активи класифікуються за рівнем важливості: критичні, від яких залежить безперервність

бізнес-процесів; важливі, що підтримують ключові функції; і допоміжні, які забезпечують допоміжні завдання. Після цього визначаються можливі загрози, які можуть впливати на безпеку інформаційних активів. Вони поділяються на природні (стихійні лиха, пожежі), технічні (відмова обладнання, збій програмного забезпечення), людські (помилки персоналу, несанкціонований доступ) і кіберзагрози (віруси, фішинг, DDoS-атаки, експлуатація вразливостей). Для кожної загрози оцінюється її потенційний вплив на активи підприємства.

Наступним кроком є виявлення вразливостей — слабких місць у системах, процесах або організації, які можуть бути використані для реалізації загроз. До них належать технічні недоліки, такі як відсутність оновлень, слабкі паролі, помилки конфігурацій; організаційні недоліки — відсутність контролю доступу чи навчання персоналу; а також процесуальні і людські фактори, що знижують загальний рівень безпеки. Після цього проводиться оцінка критичності бізнес-процесів підприємства, яка дозволяє зрозуміти, які з них є життєво важливими для функціонування організації. Для цього здійснюється бізнес-аналіз впливу (Business Impact Analysis, BIA), у ході якого визначаються максимально допустимий час простою, час відновлення після інциденту (RTO), допустима втрата даних (RPO) і потенційні фінансові чи репутаційні наслідки.

Результатом аналізу об'єкта захисту є створення систематизованої моделі, що містить опис усіх активів, їхніх власників, переліку загроз, вразливостей, оцінку ризиків і пріоритетів для подальшого проектування архітектури КСЗІ. Цей етап формує основу для наступних фаз моделювання, таких як побудова моделей потоків даних і логічної архітектури системи безпеки. Завдяки ретельному аналізу підприємство отримує об'єктивне уявлення про свій поточний рівень захищеності, що дозволяє раціонально розподілити ресурси, впровадити ефективні заходи безпеки та забезпечити стійкість інформаційної інфраструктури до сучасних кіберзагроз.

Етап 2. Формування моделі потоків даних (DFD) — побудова діаграм, які показують рух інформації між користувачами, системами, сховищами та зовнішніми інтерфейсами.

Формування моделі потоків даних (DFD) є другим етапом моделювання архітектури комплексної системи захисту інформації (КСЗІ) на підприємстві і має вирішальне значення для розуміння того, як саме інформація переміщується всередині системи, між її компонентами та зовнішніми об'єктами. На цьому етапі здійснюється детальна побудова діаграм потоків даних, які відображають процеси обробки, передачі, зберігання та використання інформації у взаємозв'язку з користувачами, програмними засобами, сховищами та зовнішніми інтерфейсами. Основна мета цього етапу — виявити всі точки, де інформація може бути вразливою або де необхідно реалізувати механізми контролю доступу, шифрування, моніторингу чи журналювання подій.

Побудова DFD-моделі починається з визначення контексту системи, тобто зовнішніх суб'єктів, які взаємодіють з підприємством: клієнти, партнери, постачальники, регуляторні органи, а також внутрішні користувачі різних рівнів доступу. На основі цього створюється контекстна діаграма (рівень 0), що показує систему як єдиний об'єкт та її взаємозв'язки з зовнішнім середовищем через інформаційні потоки — запити, звіти, файли, повідомлення, транзакції тощо. Далі модель деталізується шляхом побудови діаграм нижчих рівнів (DFD рівня 1, 2, 3), які розкривають внутрішні процеси системи, їх взаємодію, напрямки руху інформації та взаємозв'язки із сховищами даних. Кожен процес на діаграмі відображає певну логічну функцію — наприклад, обробку запиту користувача, перевірку повноважень, запис у базу даних або передавання даних через мережу.

Особливу увагу під час формування DFD приділяють ідентифікації точок входу та виходу даних, оскільки саме вони є потенційними зонами ризику для несанкціонованого доступу або витоку інформації. Наприклад, потік «користувач → веб-сервер» вимагає впровадження аутентифікації, SSL/TLS-захисту та журналювання сесій, тоді як потік «внутрішній сервер → зовнішнє сховище» потребує шифрування, контрольних сум і перевірки цілісності. Модель потоків даних дозволяє виявити вразливі точки перетину процесів і каналів передачі, де доцільно реалізувати міжмережеві екрани, проксі-сервери, антивірусні шлюзи, VPN або системи виявлення вторгнень (IDS/IPS).

Крім того, DFD-модель допомагає встановити логічну межу між рівнями доступу, наприклад, розділити зони зовнішньої взаємодії, внутрішньої мережі та захищеної серверної частини. Це дає змогу формувати сегментацію мережі, VLAN-групи, DMZ-зони, визначати точки контролю безпеки та відповідальних за їх адміністрування. Для підвищення точності аналізу до моделі додаються позначення рівнів довіри, протоколів обміну та форматів даних, що допомагає коректно оцінити вимоги до криптографічного захисту і контролю доступу.

Результатом цього етапу є повна структурна візуалізація руху інформації в межах підприємства — від моменту її введення користувачем до зберігання, обробки, передавання або видалення. Така модель є основою для подальшого етапу логічного проектування архітектури КСЗІ, оскільки дозволяє чітко визначити, які саме компоненти системи повинні взаємодіяти, які канали потребують додаткового захисту, і які процеси мають бути під постійним моніторингом. Завдяки DFD підприємство отримує можливість побудувати прозору, контрольовану та узгоджену структуру інформаційних потоків, що мінімізує ризики витоку, спотворення чи несанкціонованої модифікації даних і забезпечує фундамент для подальшого проектування ефективної системи захисту інформації.

Етап 3. Розробка логічної моделі КСЗІ — визначення підсистем, функцій безпеки, логіки взаємодії компонентів.

Розробка логічної моделі комплексної системи захисту інформації (КСЗІ) є третім етапом моделювання архітектури і має ключове значення для формування цілісного уявлення про функціонування системи безпеки на підприємстві. На цьому етапі створюється логічна структура КСЗІ, яка описує склад підсистем, їхні функції, взаємозв'язки та логіку взаємодії компонентів між собою і з зовнішнім середовищем. Метою логічного моделювання є побудова узгодженої концепції системи безпеки, у якій організаційні, технічні та програмні механізми утворюють єдине середовище управління ризиками й захисту інформаційних активів підприємства.

Логічна модель ґрунтується на результатах попередніх етапів — аналізу об'єкта захисту та побудови моделі потоків даних (DFD). Вона конкретизує, які саме функції безпеки повинні бути реалізовані для кожного потоку, процесу чи інформаційного ресурсу, і визначає архітектуру взаємодії між ними. Кожен компонент у моделі розглядається не ізольовано, а як частина системи, яка взаємодіє з іншими елементами через захищені канали, інтерфейси або протоколи. Логічна модель включає такі базові підсистеми: ідентифікації та аутентифікації користувачів, керування доступом, криптографічного захисту інформації, моніторингу та аудиту, реагування на інциденти, резервного копіювання і відновлення даних, а також адміністрування безпеки. Для кожної підсистеми визначаються її цілі, функціональні обов'язки, зв'язки з іншими модулями та вимоги до безпеки.

Особлива увага приділяється логіці взаємодії компонентів. Наприклад, підсистема аутентифікації тісно пов'язана з контролем доступу та журналюванням подій, забезпечуючи перевірку повноважень користувача і створення записів про всі дії. Система криптографічного захисту інтегрується з модулем передавання даних, щоб шифрувати інформацію під час обміну між серверами або зовнішніми користувачами. Підсистема моніторингу (SIEM/SOC) взаємодіє з усіма компонентами системи, збираючи телеметрію, аналізуючи події безпеки, виявляючи аномалії та ініціюючи процедури реагування. Логічна модель також визначає політику довіри між елементами системи — які об'єкти мають право взаємодії, які протоколи використовуються, та які рівні привілеїв допускаються.

На етапі розробки логічної моделі також формуються механізми узгодження між рівнями безпеки — політичним, організаційним і технічним. Політичний рівень встановлює стратегічні принципи, організаційний забезпечує регламентацію процедур і розподіл відповідальності, а технічний реалізує безпосередні механізми захисту. Логічна модель повинна відображати цю ієрархію, щоб забезпечити взаємну підтримку всіх компонентів. Для цього визначаються точки інтеграції між модулями — наприклад, взаємодія антивірусного захисту з IDS/IPS або обмін даними між SIEM і системою керування доступом. Така взаємодія дозволяє створити єдину інформаційну екосистему безпеки, у якій події, виявлені на одному рівні, автоматично впливають на рішення на іншому.

У логічній моделі також розробляються сценарії обробки подій безпеки, включно з виявленням, класифікацією, реагуванням і документуванням інцидентів. Ці сценарії допомагають забезпечити узгодженість дій персоналу, своєчасність реагування та мінімізацію наслідків. Для візуалізації логіки роботи КСЗІ застосовуються UML-діаграми, блок-схеми або функціональні моделі, що показують процеси прийняття рішень, обробки запитів, передавання сигналів між компонентами системи. Це сприяє стандартизації архітектури та спрощує подальше впровадження.

Результатом розробки логічної моделі є чітко структурована схема системи захисту інформації, що описує взаємодію між усіма її елементами, канали обміну даними, рівні довіри та залежності між підсистемами. Вона стає основою для створення фізичної моделі КСЗІ, вибору конкретних технологій, програмно-апаратних засобів та інструментів моніторингу. Таким чином, логічна модель КСЗІ забезпечує системність, узгодженість і передбачуваність функціонування архітектури безпеки, створюючи передумови для ефективного управління ризиками, стабільної роботи інформаційної інфраструктури й відповідності вимогам міжнародних стандартів і законодавства у сфері кіберзахисту.

Етап 4. Проектування фізичної моделі — розміщення серверів, шлюзів, засобів шифрування, міжмережевих екранів, систем виявлення вторгнень (IDS/IPS) і SIEM.

Етап проектування фізичної моделі комплексної системи захисту інформації (КСЗІ) є четвертим у процесі створення архітектури безпеки підприємства та передбачає практичне відображення логічної структури системи на рівні реальної інфраструктури. На цьому етапі визначаються конкретні місця розташування серверів, комунікаційного обладнання, шлюзів безпеки, систем виявлення вторгнень (IDS/IPS), міжмережевих екранів, криптографічних засобів і систем моніторингу безпеки (SIEM). Метою фізичного проектування є створення оптимальної топології захисту, яка забезпечує цілісність, конфіденційність і доступність інформації з урахуванням особливостей інфраструктури, обсягів трафіку, зон довіри та ризикових факторів.

Першим кроком фізичного проектування є розподіл інфраструктури підприємства на захищені зони. Як правило, виділяються такі рівні: зовнішня зона (інтернет-сегмент), демілітаризована зона (DMZ), внутрішня корпоративна мережа, сегмент серверів і баз даних та зона управління безпекою. Між цими зонами встановлюються чітко визначені маршрути обміну інформацією, які контролюються засобами фільтрації трафіку та аутентифікації. Для цього в проєкті визначається розташування міжмережевих екранів (Firewall), які є першою лінією оборони системи. Вони фільтрують трафік за визначеними політиками, запобігають несанкціонованому підключенням, блокують небезпечні порти та протоколи, а також здійснюють глибоку перевірку пакетів (Deep Packet Inspection).

На рис. 2.2 зображено структурну схему мережевої інфраструктури підприємства, побудовану за принципом багаторівневої сегментації для підвищення безпеки та ефективності взаємодії між компонентами. Зовнішні користувачі підключаються до корпоративної мережі через Інтернет із використанням захищених VPN-каналів, що забезпечують шифрування трафіку та аутентифікацію користувачів. Вхідний трафік спочатку проходить через міжмережеві екрани у зоні WAN, а потім — через демілітаризовану зону (DMZ), де розміщуються сервери загального доступу: веб-, поштові, файлові та бази даних.

DMZ ізольована від внутрішньої мережі (LAN) за допомогою додаткового міжмережевого екрана, що мінімізує ризики проникнення до критичних ресурсів у разі компрометації зовнішніх вузлів. У LAN-зоні розташовані робочі станції користувачів, телефони, системи відеоконференцій та інше обладнання, підключене через комутатори. Крім того, передбачено бездротовий сегмент (Wireless), який має власний шлюз безпеки для контролю доступу та фільтрації трафіку. Така архітектура демонструє класичний підхід до побудови фізичної моделі КСЗІ, у якій застосовано принципи розмежування доступу, сегментації мережі, контролю взаємодії між зонами та централізованого управління безпечними каналами зв'язку.

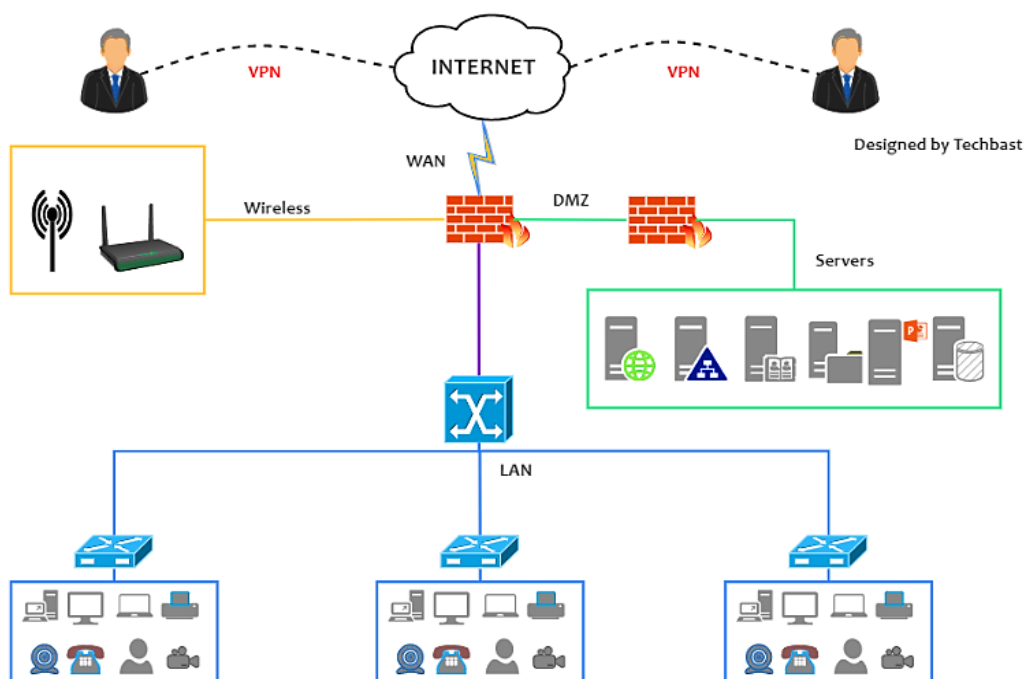


Рис. 2.2. Типова мережева архітектура підприємства з використанням зон DMZ, LAN, WAN та VPN-з'єднань

Джерело: [1-10, 18-23, 56-68, 81-102, 206-211]

У внутрішніх сегментах мережі розміщуються системи виявлення та запобігання вторгненням (IDS/IPS), які здійснюють моніторинг мережевого трафіку, виявляють аномалії, сигнатури атак і можуть автоматично блокувати шкідливі дії.

IDS/IPS інтегруються з SIEM-системою (Security Information and Event Management), що забезпечує централізований збір, аналіз і кореляцію подій безпеки з усіх компонентів мережі. SIEM дозволяє формувати єдину аналітичну картину безпеки, своєчасно виявляти інциденти, створювати звіти для аудиту й ініціювати автоматизовані сценарії реагування через SOAR-механізми (Security Orchestration, Automation and Response).

Важливим елементом фізичної моделі є засоби криптографічного захисту інформації, які впроваджуються для шифрування каналів зв'язку, аутентифікації користувачів та захисту даних у стані спокою. До них належать апаратні криптомодулі (HSM), VPN-шлюзи, SSL/TLS-сертифікати, сервіси PKI (інфраструктури відкритих ключів) і програмні засоби реалізації стандартів шифрування (AES, RSA, ECC). Усі ці компоненти повинні бути інтегровані з іншими системами безпеки, щоб забезпечити цілісний захист каналів передачі даних і критичних сховищ.

Під час проєктування фізичної моделі визначаються також топологічні особливості розміщення серверів і сховищ даних. Сервери застосунків і баз даних, які обробляють конфіденційну інформацію, розміщуються у відокремленій зоні з обмеженим доступом, фізично захищеній та обладнаній системами контролю доступу (СКД), відеоспостереженням і пожежною безпекою. Для забезпечення безперервності функціонування впроваджуються механізми резервування — дублювання каналів зв'язку, використання кластерних серверів і систем відновлення після збоїв (Failover, Backup & Recovery).

Фізична модель КСЗІ також охоплює побудову інфраструктури моніторингу та управління. У ній визначаються точки збору журналів подій, механізми синхронізації часу, протоколи обміну інформацією між компонентами безпеки та порядок адміністрування користувачів. Розробляються схеми підключення систем резервного копіювання, керування оновленнями, антивірусного захисту, а також визначаються вузли, відповідальні за підтримку сервісів аутентифікації (LDAP, Active Directory) та управління доступом (IAM).

На рис. 2.3 представлено типову модель побудови фізичної архітектури системи безпеки підприємства, у якій реалізовано багаторівневий підхід до захисту інформаційних потоків. Вхідний трафік із мережі Інтернет проходить через маршрутизатор і систему виявлення та запобігання вторгненням (IDS/IPS), що здійснює аналіз пакетів і фільтрацію потенційно шкідливої активності. Далі дані надходять до міжмережевого екрана (Firewall), який контролює доступ між зовнішніми та внутрішніми сегментами мережі, забезпечуючи ізоляцію демілітаризованої зони (DMZ), де розташовані публічні сервери — веб-, поштовий і сервер баз даних.

У середині корпоративної мережі функціонує комплекс засобів моніторингу загроз (Counter Threat Appliance), який збирає події безпеки, а також комутатор

(Switch), що з'єднує робочі станції та внутрішні сервери. Для централізованого управління та реагування на інциденти архітектура передбачає взаємодію з центром операцій безпеки (Security Operations Center, SOC), де проводиться аналітика подій і координація дій із захисту. Така структура забезпечує глибоку оборону (Defense in Depth), де кожен рівень — маршрутизатор, IDS/IPS, Firewall, DMZ, SOC — виконує власну функцію контролю, формуючи багатoshарову систему кіберзахисту, здатну ефективно протидіяти зовнішнім і внутрішнім загрозам.

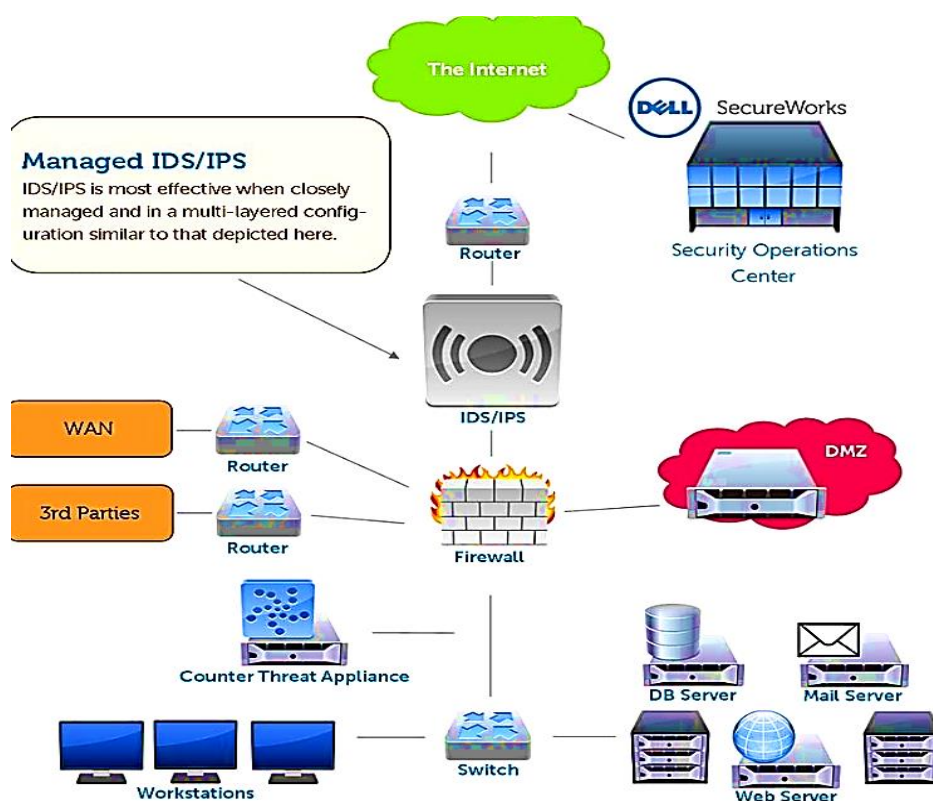


Рис. 2.3. Багатoshарова мережна безпека підприємства: DMZ, firewall, IDS/IPS, SOC/SIEM

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206-211]

Результатом цього етапу є детальна архітектурна схема фізичної моделі КСЗІ, що відображає реальне розміщення всіх апаратних і програмних компонентів системи безпеки, топологію мережеских з'єднань, логіку руху трафіку, рівні фільтрації та механізми моніторингу. Така модель забезпечує прозорість структури захисту, дозволяє оптимізувати ресурси, узгодити політики безпеки з архітектурою мережі й підготувати систему до етапу тестування, сертифікації та подальшого впровадження у промислову експлуатацію. Завдяки правильно спроектованій фізичній моделі підприємство отримує надійну, масштабовану та контрольовану інфраструктуру безпеки, здатну протистояти сучасним кіберзагрозам і забезпечувати стабільність критичних бізнес-процесів.

Етап 5. Оцінка ризиків та відповідності стандартам — перевірка адекватності архітектури, ефективності захисних механізмів і вартості впровадження.

Оцінка ризиків та відповідності стандартам є завершальним і надзвичайно важливим етапом моделювання архітектури комплексної системи захисту інформації (КСЗІ) на підприємстві, оскільки саме він дозволяє перевірити, наскільки побудована система відповідає вимогам безпеки, нормативним стандартам і економічній доцільності її впровадження. Основна мета цього етапу — оцінити адекватність архітектури КСЗІ, виявити залишкові ризики, підтвердити ефективність реалізованих захисних механізмів і забезпечити їх відповідність міжнародним та національним стандартам у сфері інформаційної безпеки.

Першим кроком є проведення ризик-аналізу, який передбачає виявлення потенційних загроз, визначення вразливостей, оцінку ймовірності їх реалізації та розрахунок можливих наслідків для інформаційних активів. Для цього використовуються такі методики, як ISO/IEC 27005, NIST SP 800-30, OCTAVE, FAIR або метод аналізу FMEA (Failure Mode and Effects Analysis). У межах аналізу формується матриця ризиків, у якій кожен ризик характеризується за рівнем ймовірності виникнення та масштабом впливу. Наприклад, ризик несанкціонованого доступу до бази даних може мати високу ймовірність і критичний вплив, тоді як збій допоміжного сервера — середню ймовірність і низький вплив. За результатами оцінки визначаються пріоритети управління ризиками — які загрози слід усунути першочергово, які мінімізувати технічними засобами, а які прийняти як допустимі залишкові ризики.

Далі проводиться перевірка ефективності захисних механізмів, реалізованих у логічній та фізичній моделях КСЗІ. Ця перевірка може включати аудит конфігурацій систем безпеки, пентест (penetration testing), оцінку вразливостей (vulnerability assessment), аналіз журналів подій SIEM, а також тестування сценаріїв реагування на інциденти. Метою є підтвердити, що впроваджені засоби — міжмережеві екрани, IDS/IPS, криптомодулі, VPN, системи резервування, контролю доступу — дійсно забезпечують необхідний рівень захисту, не створюють конфліктів між собою і не знижують продуктивність системи. На цьому ж етапі перевіряється узгодженість між політикою безпеки та технічними реалізаціями, зокрема дотримання принципів мінімізації прав доступу, сегментації мережі, ізоляції критичних систем і захисту каналів передачі даних.

Важливою складовою цього етапу є оцінка відповідності стандартам і нормативним вимогам. Архітектура КСЗІ повинна відповідати положенням міжнародних стандартів ISO/IEC 27001 (управління інформаційною безпекою), ISO/IEC 27002 (практичні засоби реалізації контролів), ISO/IEC 15408 (Common Criteria — оцінка надійності засобів безпеки), NIST SP 800-53 (контролі безпеки для інформаційних систем), а також ДСТУ 3396.1–2016 і Закону України «Про захист

інформації в інформаційно-телекомунікаційних системах». Перевірка проводиться за критеріями відповідності вимогам конфіденційності, цілісності, доступності, невідмовності та спостережності. Для систем, які обробляють персональні дані, також обов'язковою є оцінка відповідності принципам GDPR та Закону України «Про захист персональних даних».

Окрім технічних і нормативних аспектів, на цьому етапі здійснюється економічна оцінка КСЗІ. Вона включає аналіз вартості впровадження, експлуатації та супроводу системи, порівняння витрат із потенційними збитками від реалізації ризиків, а також розрахунок показників ефективності інвестицій у безпеку (ROI — Return on Investment, ROSI — Return on Security Investment). Це дозволяє керівництву підприємства приймати обґрунтовані рішення щодо доцільності подальших інвестицій у конкретні технології або заходи безпеки.

На завершення формується звіт про оцінку ризиків і відповідність стандартам, який містить опис виявлених ризиків, результати тестувань, висновки про рівень зрілості системи безпеки, а також рекомендації щодо вдосконалення архітектури КСЗІ. У документі також визначається залишковий ризик і надаються пропозиції щодо його моніторингу та контролю.

Таким чином, оцінка ризиків та відповідності стандартам завершує цикл моделювання архітектури КСЗІ, забезпечуючи її перевірку з позицій технічної надійності, регуляторної узгодженості та економічної ефективності. Саме цей етап підтверджує готовність системи до практичного впровадження, експлуатації та подальшої сертифікації, створюючи передумови для побудови стійкої, керованої та стандартизованої системи інформаційної безпеки підприємства.

Важливою складовою моделювання є використання сучасних інструментів та діаграм, таких як DFD (Data Flow Diagrams) для відображення потоків даних, UML-діаграми для моделювання структур і процесів взаємодії компонентів, а також архітектурні схеми рівнів безпеки (policy layer, control layer, protection layer). Це дозволяє візуалізувати архітектуру системи, оцінити її масштабованість, забезпечити простежуваність між бізнес-вимогами та технічними реалізаціями.

У моделі КСЗІ підприємства зазвичай виділяють три основні рівні архітектури:

- **Організаційний рівень**, який охоплює політику безпеки, процедури, регламенти, управління ризиками та відповідальність персоналу;
- **Функціональний рівень**, що описує процеси забезпечення безпеки (автентифікація, контроль доступу, моніторинг, реагування, аудит);
- **Технічний рівень**, який включає реалізацію захисних технологій — міжмережеві екрани, VPN, IDS/IPS, SIEM, системи керування ідентифікацією (IAM), криптографічні модулі, резервне копіювання та контроль цілісності даних.

Результатом моделювання є архітектурна схема КСЗІ, яка демонструє взаємодію компонентів, потоки інформації, рівні довіри, зони захисту та методи контролю. Ця модель слугує основою для розробки технічного завдання,

впровадження засобів захисту, проведення випробувань і подальшої сертифікації системи. Моделювання також дає змогу проводити сценарне планування — прогнозувати наслідки атак, перевіряти ефективність контрзаходів і оптимізувати витрати на безпеку.

Таким чином, моделювання архітектури КСЗІ на підприємстві — це не лише етап проектування, а й інструмент управління інформаційною безпекою, що забезпечує цілісність, узгодженість та адаптивність системи до динамічних умов кіберпростору. Воно дозволяє інтегрувати технічні засоби, політики, процедури та людський фактор у єдину модель, здатну ефективно протидіяти сучасним загрозам і підтримувати стійкість бізнес-процесів підприємства.

2.2. ОРГАНІЗАЦІЙНИЙ, ТЕХНІЧНИЙ ТА ПОЛІТИЧНИЙ РІВНІ ЗАХИСТУ

Організаційний, технічний та політичний рівні захисту утворюють цілісну багаторівневу архітектуру системи безпеки підприємства, де кожен рівень виконує специфічні функції, але всі вони взаємопов'язані між собою. Така структуризація дозволяє забезпечити не лише технологічну стійкість системи до кіберзагроз, а й управлінську узгодженість, відповідність законодавчим вимогам і ефективність реалізації політики безпеки в цілому. Політичний рівень формує стратегічні засади захисту інформації, визначає принципи, правила та відповідальність учасників процесу. Організаційний рівень забезпечує реалізацію цих принципів через регламенти, процедури, управління ризиками, аудит і навчання персоналу. Технічний рівень відповідає за практичне втілення заходів безпеки — захист мереж, даних, користувачів і систем за допомогою сучасних технологій та засобів контролю. Узгоджена взаємодія між цими рівнями створює єдину ефективну екосистему інформаційної безпеки, здатну адаптуватися до динамічних умов кіберпростору. Нижче подано детальний опис кожного рівня.

Політичний рівень захисту

Політичний рівень є стратегічною основою системи безпеки, що визначає принципи, цілі, пріоритети та загальні напрями забезпечення інформаційної безпеки підприємства. На цьому рівні формується політика інформаційної безпеки (ПІБ) — головний документ, який регламентує порядок обробки, зберігання, передавання, шифрування та знищення інформації. Політика встановлює вимоги до користувачів, визначає відповідальність за порушення правил, порядок реагування на інциденти, використання засобів криптографічного захисту, резервного копіювання та аудиту.

Політичний рівень також охоплює розробку нормативно-правових документів підприємства, що узгоджують внутрішні процедури із національним законодавством та міжнародними стандартами, такими як ISO/IEC 27001, NIST SP

800-53 і GDPR. На цьому рівні визначаються стратегічні цілі у сфері безпеки, розподіл ролей і повноважень між підрозділами, а також механізми управління ризиками й контролю відповідності. Важливою складовою є формування культури безпеки, що сприяє підвищенню обізнаності персоналу щодо загроз і правил поведінки з інформацією. Політика інформаційної безпеки передбачає регулярний перегляд і оновлення положень відповідно до змін у технологічному середовищі, вимог законодавства та нових кіберризиків. На її основі розробляються підпорядковані документи — стандарти, процедури, інструкції та регламенти, які конкретизують вимоги для окремих процесів і систем. Реалізація політичного рівня забезпечує узгодженість між управлінськими рішеннями, технічними заходами й практиками персоналу. У підсумку саме цей рівень визначає стратегічний курс підприємства у сфері інформаційної безпеки, створюючи фундамент для ефективної роботи організаційних та технічних механізмів захисту.

До ключових елементів політичного рівня належать:

- Стратегічні принципи безпеки: конфіденційність, цілісність, доступність, спостережність та невідомість.
- Визначення ролей і відповідальності: розмежування повноважень між керівництвом, службою безпеки, адміністраторами та користувачами.
- Нормативно-правова база: адаптація внутрішніх документів підприємства до вимог міжнародних стандартів ISO/IEC 27001, 27002, NIST SP 800-53, GDPR, Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і «Про захист персональних даних».
- Управління ризиками: визначення критеріїв оцінювання загроз, методів мінімізації та періодичного перегляду ризиків.
- Контроль відповідності (compliance): забезпечення дотримання внутрішніх політик, галузевих норм і державних регламентів.

Політичний рівень забезпечує єдність підходів до кіберзахисту на всіх рівнях управління, створює нормативну основу для діяльності технічних і організаційних підрозділів, а також сприяє підвищенню культури інформаційної безпеки серед персоналу.

ОРГАНІЗАЦІЙНИЙ РІВЕНЬ ЗАХИСТУ

Організаційний рівень — це операційно-управлінська складова системи безпеки, яка відповідає за практичну реалізацію політики безпеки, координацію дій персоналу, моніторинг ризиків і забезпечення безперервності бізнес-процесів. Він охоплює діяльність структурних підрозділів, регламентацію процесів, а також формування системи управління інформаційною безпекою (СУІБ).

На організаційному рівні визначаються ролі, обов'язки та відповідальність усіх учасників процесу — від керівництва до рядових користувачів, що забезпечує чіткий розподіл повноважень і підзвітність. Основна увага приділяється впровадженню процедур управління ризиками, розробці планів реагування на

інциденти, а також періодичному проведенню аудитів інформаційної безпеки. Важливим завданням є організація навчання персоналу та підвищення їхньої обізнаності щодо політики безпеки, принципів кібергігієни та дотримання правил доступу до інформаційних ресурсів. На цьому рівні формується система контролю доступу, управління обліковими записами та моніторингу активності користувачів для запобігання внутрішнім загрозам. Організаційний рівень також відповідає за розробку планів забезпечення безперервності діяльності (BCP) і відновлення після збоїв (DRP), що гарантують стабільну роботу підприємства в умовах кризових ситуацій. Для підвищення ефективності використовуються показники результативності заходів безпеки (KPI, KRI) і механізми зворотного зв'язку між підрозділами. У комплексі цей рівень створює керовану систему реалізації політики інформаційної безпеки, яка забезпечує узгодженість організаційних рішень із технічними та стратегічними напрямками підприємства.

Основні завдання організаційного рівня:

- Формування системи управління безпекою (ISMS): створення посадових інструкцій, політик доступу, регламентів обробки даних і планів реагування на інциденти.
- Управління ризиками: проведення регулярних оцінок загроз (Risk Assessment), розробка планів їх мінімізації (Risk Treatment Plan) та визначення залишкових ризиків.
- Контроль доступу: створення системи розмежування повноважень, управління обліковими записами користувачів, впровадження багатофакторної аутентифікації.
- Моніторинг і аудит: постійне спостереження за активністю користувачів, аналіз журналів подій, внутрішні перевірки відповідності стандартам і політикам безпеки.
- Навчання персоналу: проведення тренінгів із кібергігієни, симуляцій фішингових атак, підвищення обізнаності щодо політики конфіденційності.
- Інцидент-менеджмент: створення команд реагування (CSIRT/SOC), документування інцидентів, аналіз першопричин та формування звітності для керівництва.
- Безперервність бізнесу (BCP/DRP): планування заходів із резервного копіювання, відновлення після аварій (Disaster Recovery) і підтримання критичних процесів під час надзвичайних ситуацій.

Організаційний рівень виступає мостом між політичними вимогами та технічними рішеннями, забезпечуючи координацію людських, фінансових і технологічних ресурсів у сфері безпеки.

ТЕХНІЧНИЙ РІВЕНЬ ЗАХИСТУ

Технічний рівень є функціональним ядром КСЗІ, яке реалізує конкретні механізми й засоби захисту інформації в ІКС підприємства. Саме тут відбувається

практична реалізація принципів політики безпеки — контроль доступу, криптографічний захист, фільтрація трафіку, виявлення вторгнень і моніторинг інцидентів.

На технічному рівні впроваджуються апаратні та програмні засоби захисту, які забезпечують цілісність, конфіденційність і доступність інформації в усіх сегментах мережі. До них належать міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), засоби контролю доступу, VPN-шлюзи, антивірусні рішення та криптографічні модулі. Центральну роль відіграють системи моніторингу подій безпеки (SIEM), які збирають журнали, аналізують аномалії та формують повідомлення про інциденти для оперативного реагування. Для забезпечення безперервності роботи впроваджуються рішення з резервного копіювання, відновлення даних, дублювання каналів зв'язку та кластеризації серверів. Також важливою складовою є системи керування ідентифікацією та доступом (IAM), які гарантують дотримання принципу мінімальних привілеїв і автентичність користувачів. Технічний рівень інтегрує всі елементи безпеки в єдину архітектуру, забезпечуючи взаємодію між компонентами через захищені протоколи, сертифікати PKI та механізми багатофакторної аутентифікації. Завдяки цьому рівню КСЗІ перетворюється на стійку, контрольовану та адаптивну систему, здатну своєчасно виявляти загрози, блокувати атаки й підтримувати стабільність критичної інфраструктури підприємства.

До основних компонентів технічного рівня належать:

- Системи аутентифікації та керування доступом (IAM, LDAP, Active Directory): забезпечують ідентифікацію користувачів і контроль прав доступу до ресурсів.
- Міжмережеві екрани (Firewall) та проксі-сервери: фільтрують мережевий трафік, блокують несанкціоновані з'єднання, формують DMZ-зони для зовнішніх сервісів.
- Системи виявлення та запобігання вторгненням (IDS/IPS): аналізують мережеві пакети, виявляють аномалії та реагують на атаки в реальному часі.
- Криптографічні засоби (HSM, VPN, SSL/TLS, PKI): забезпечують захист каналів зв'язку, шифрування даних у процесі передавання та зберігання.
- Системи моніторингу та кореляції подій (SIEM/SOAR): збирають телеметрію з усіх вузлів, аналізують події, визначають шаблони атак і автоматизують реагування.
- Засоби резервного копіювання та відновлення: гарантують цілісність і доступність інформації у разі збоїв або кібератак.
- Антивірусні та антишкідливі рішення (EDR/XDR): забезпечують проактивний захист кінцевих пристроїв від вірусів, шкідливого коду та несанкціонованих дій.

Технічний рівень інтегрує всі механізми безпеки в єдину інфраструктуру, підтримуючи політику доступу, контроль подій і забезпечення цілісності даних. Його ефективність визначається регулярним оновленням, тестуванням, аудитом і взаємодією з організаційним рівнем через SOC або службу ІБ.

Технічний рівень виступає основою практичної реалізації політики безпеки, забезпечуючи автоматизацію процесів виявлення, реагування та усунення інцидентів. Він тісно взаємодіє з аналітичними системами, зокрема SIEM, SOAR і IDS/IPS, що дозволяє проводити кореляцію подій та виявляти складні атаки в реальному часі. У межах цього рівня впроваджуються механізми централізованого управління оновленнями, антивірусного захисту, контролю змін конфігурацій і шифрування даних. Важливим аспектом є побудова резервних і відмовостійких рішень, які гарантують доступність критичних сервісів навіть у разі кібератак чи технічних збоїв. Ефективність технічного рівня значною мірою залежить від інтеграції з організаційними процесами, зокрема звітністю до керівництва, управлінням ризиками та реагуванням на інциденти. Регулярне тестування та аудит дозволяють своєчасно виявляти вразливості, оновлювати засоби захисту й підтримувати відповідність стандартам безпеки. У результаті технічний рівень формує стійкий технологічний фундамент КСЗІ, який забезпечує надійний захист інформаційних активів і стабільність функціонування підприємства.

ВЗАЄМОЗВ'ЯЗОК МІЖ РІВНЯМИ

- Політичний, організаційний і технічний рівні утворюють єдину ієрархічну систему КСЗІ, де кожен рівень підтримує інший:
- політичний визначає стратегію і принципи;
- організаційний забезпечує реалізацію та контроль;
- технічний виконує функціональну реалізацію захисних механізмів.

На рис. 2.4 зображено декілька “шарів” або рівнів безпеки, які показують, як політичний, організаційний і технічний рівні можуть бути візуалізовані в структурі захисту. Верхня частина ієрархії відображає стратегічні та політичні рішення, середня — організаційні процеси й управління, а нижні шари символізують технічні засоби та інструменти, впроваджені для безпосереднього захисту систем.

Така візуалізація допомагає читачеві побачити: рішення, які приймаються на політичному рівні, “спускаються” вниз і реалізуються через організаційні процедури та технічні механізми.

Рисунок підтримує вашу тезу про те, що ці три рівні — політичний, організаційний і технічний — не існують самотійно, а взаємопов'язані та взаємозалежні.

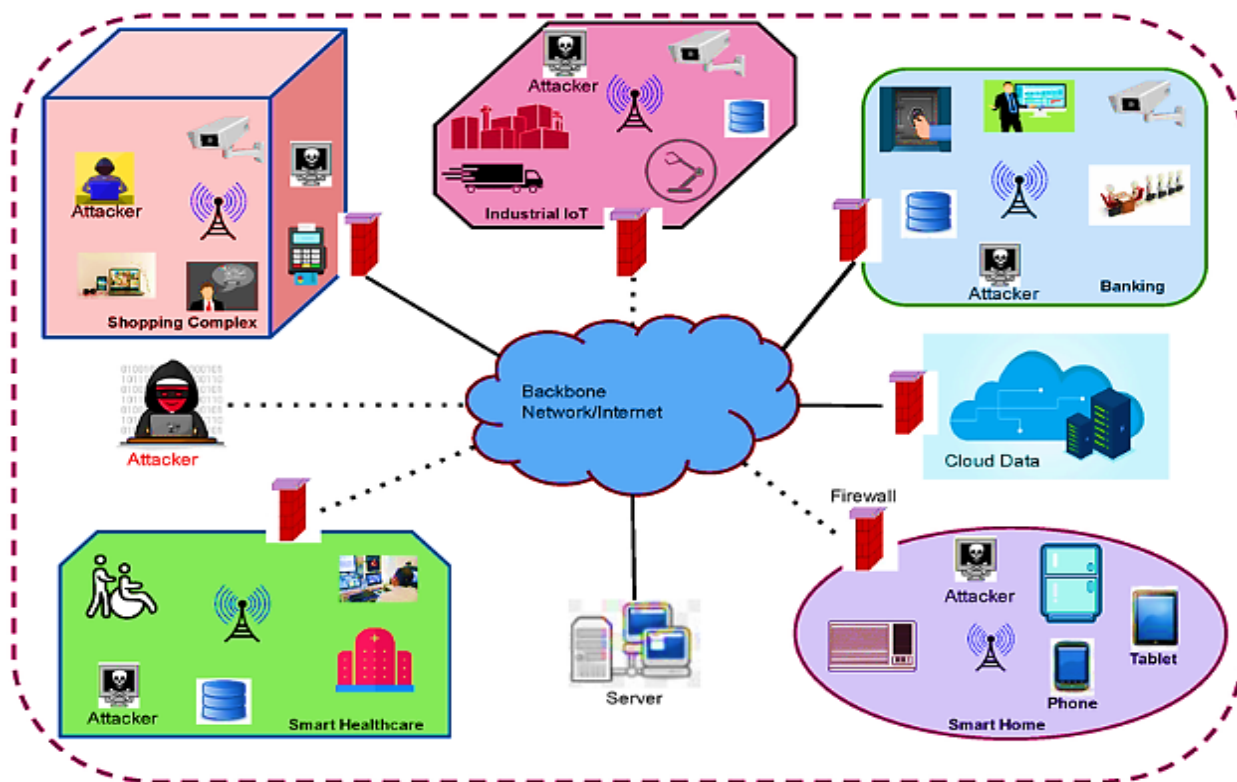


Рис. 2.4. Модель багаторівневої архітектури захисту
Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206-211]

Така взаємодія створює комплексну систему безпеки, яка є керованою, адаптивною й стійкою до змін у технологічному середовищі та загрозовому ландшафті. У результаті підприємство отримує структурований, ефективний і сертифікований підхід до захисту інформації на всіх рівнях її життєвого циклу.

Взаємозв'язок між рівнями забезпечує цілісність та узгодженість усієї системи інформаційної безпеки, де стратегічні рішення політичного рівня безпосередньо впливають на організаційні процеси й технічні засоби. Кожен рівень виконує свої функції, але їх ефективність залежить від узгодженості дій та зворотного зв'язку між ними. Політичні документи задають стандарти та вимоги, організаційний рівень трансформує їх у конкретні процедури, а технічний реалізує ці вимоги на практиці за допомогою відповідних технологій. У свою чергу, результати моніторингу технічного рівня і дані аудиту передаються на організаційний та політичний рівні для коригування політик і підвищення ефективності захисту. Така багаторівнева взаємодія формує безперервний цикл удосконалення системи безпеки, що базується на принципах адаптивності та ризик-орієнтованого підходу. Завдяки цьому КСЗІ здатна гнучко реагувати на нові загрози, підтримувати відповідність міжнародним стандартам і забезпечувати безперервність бізнес-процесів. Таким чином, взаємопідтримка між політичним, організаційним і

технічним рівнями створює надійну архітектуру кіберзахисту підприємства, орієнтовану на стабільність, розвиток і стійкість до сучасних викликів.

2.3. ІНТЕГРАЦІЯ SIEM, SOC ТА ЗАСОБІВ МОНІТОРИНГУ

Інтеграція SIEM, SOC та засобів моніторингу є ключовим елементом сучасної архітектури комплексної системи захисту інформації (КСЗІ), що забезпечує своєчасне виявлення, аналіз і реагування на кіберзагрози. Вона поєднує технологічні інструменти, аналітичні механізми та організаційні процеси в єдину екосистему безпеки, яка діє в режимі реального часу. Основна мета інтеграції полягає у створенні централізованої системи спостереження, кореляції подій і прийняття рішень, що дозволяє швидко виявляти інциденти, мінімізувати їх наслідки та забезпечувати безперервність діяльності підприємства.

Інтеграція цих компонентів дозволяє об'єднати дані з різних джерел — серверів, мережевого обладнання, кінцевих пристроїв і прикладних систем — у єдине аналітичне середовище для комплексного контролю безпеки. Завдяки системам SIEM здійснюється централізований збір і кореляція подій, а SOC координує реагування на інциденти, використовуючи автоматизовані сценарії та аналітику загроз. Засоби моніторингу, такі як IDS/IPS, EDR та NDR, формують первинний рівень спостереження, передаючи телеметрію для подальшого аналізу. Такий підхід забезпечує багаторівневу видимість стану кіберзахисту та скорочує час між виявленням і усуненням загрози. Крім того, інтеграція дозволяє реалізувати концепцію безперервного моніторингу (Continuous Monitoring), що гарантує оперативне виявлення навіть прихованих або складних атак. Вона також створює умови для автоматизації реагування через платформи SOAR, які синхронізують дії різних систем безпеки. У результаті підприємство отримує гнучку, адаптивну та самокеровану систему кіберзахисту, здатну підтримувати високий рівень стійкості до сучасних кіберзагроз.

Система SIEM (Security Information and Event Management)

Система SIEM (Security Information and Event Management) є центральним аналітичним ядром, яке відповідає за збір, нормалізацію та кореляцію подій безпеки з усіх елементів ІКС підприємства. Зібрана інформація уніфікується в єдиному форматі для подальшого аналізу, що дозволяє визначати взаємозв'язки між подіями з різних джерел. SIEM здійснює виявлення відхилень у поведінці користувачів і систем, формує сповіщення про потенційні інциденти та передає їх до центру безпеки (SOC). Завдяки цьому система забезпечує оперативне реагування на загрози, підвищуючи рівень захищеності та контрольованості інформаційного середовища підприємства.

Вона отримує дані від міжмережових екранів, серверів, робочих станцій, антивірусних систем, шлюзів, баз даних і засобів автентифікації. За допомогою алгоритмів кореляції SIEM визначає взаємозв'язки між подіями, ідентифікує аномальну поведінку користувачів, фіксує спроби несанкціонованого доступу та формує сповіщення для служби безпеки. Крім того, вона автоматизує процеси звітності, дозволяючи будувати дашборди, відстежувати тенденції ризиків і аналізувати динаміку інцидентів. У результаті SIEM забезпечує прозорість усіх процесів, підвищує ефективність моніторингу та створює інформаційне підґрунтя для оперативного прийняття рішень. Система також інтегрується з іншими компонентами кіберзахисту, такими як SOC, SOAR, IDS/IPS і EDR, що дозволяє формувати єдину екосистему безпеки. Завдяки централізованому збору й аналізу даних SIEM дає змогу зменшити час реагування на інциденти та підвищити точність виявлення загроз. У поєднанні з технологіями машинного навчання вона здатна прогнозувати потенційні атаки, забезпечуючи проактивний підхід до управління кіберризиками.

На рис. 2.5 представлено узагальнену архітектуру системи SIEM, яка демонструє процес збору, нормалізації, кореляції та аналізу подій безпеки. Система отримує дані з двох основних джерел — системних входів (System Inputs), до яких належать операційні системи, прикладні програми, пристрої та бази даних, і контекстних даних (Contextual Data), що містять інформацію про сканування вразливостей, користувачів, активи та зовнішні розвідувальні джерела про загрози (Threat Intelligence). На етапі збору та нормалізації даних (Data Collection & Normalization) відбувається уніфікація форматів журналів подій для подальшої обробки.

Після цього SIEM здійснює кореляцію, логічну обробку та агрегацію даних (Correlation, Logic Rules, Aggregation), визначаючи взаємозв'язки між подіями з різних систем і виявляючи аномалії чи індикатори компрометації. Завдяки цим процесам формується аналітична модель, яка дозволяє виявляти складні багатоступеневі атаки, що не завжди помітні при аналізі окремих логів. Результати обробки представлені у вигляді системних виходів (System Outputs) — аналітичних звітів, дашбордів і сповіщень про інциденти, які використовуються для прийняття рішень і оперативного реагування.

Таким чином, архітектура SIEM забезпечує централізоване управління подіями безпеки, дозволяючи об'єднати дані з різнорідних джерел у єдину інформаційну екосистему для глибокого аналізу, звітності та моніторингу в режимі реального часу.

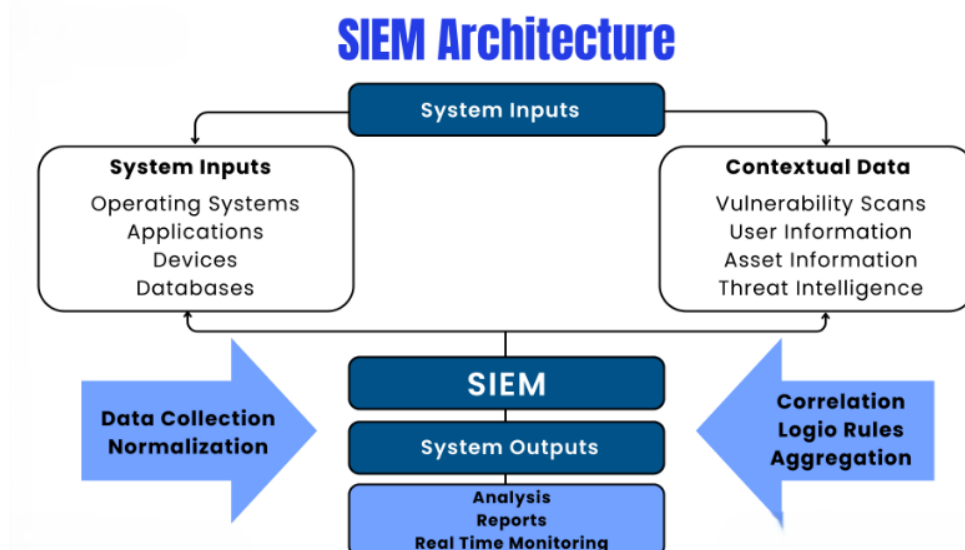


Рис. 2.5. Архітектура системи SIEM (Security Information and Event Management)

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206-211]

Система SIEM також виконує функції централізованого управління журналами подій, що дає змогу не лише зберігати, а й структурувати великі обсяги логів для подальшого аналізу. Вона підтримує інтеграцію з різними джерелами даних — від систем керування доступом і VPN-шлюзів до хмарних сервісів і мобільних пристроїв, що забезпечує повний огляд стану безпеки підприємства. Використовуючи механізми кореляції подій та поведінкової аналітики (UEBA — User and Entity Behavior Analytics), SIEM здатна виявляти приховані або багатоступеневі атаки, які проходять повз традиційні засоби захисту. Завдяки застосуванню елементів машинного навчання (ML) і штучного інтелекту (AI) система може самостійно розпізнавати відхилення від нормальної активності та формувати рекомендації для реагування.

Крім аналітичної функції, SIEM виступає платформою для автоматизації реагування, передаючи сигнали до SOC або систем SOAR, які ініціюють блокування атак, ізоляцію уражених хостів чи зміну політик доступу. Для керівництва й аудиторів система генерує звіти про інциденти, відповідність стандартам (compliance reports) і показники ефективності безпеки, що сприяє підвищенню підзвітності та оптимізації управлінських рішень. Важливою перевагою SIEM є її здатність створювати єдину інформаційну картину загроз, об'єднуючи дані з різнорідних систем — від мережевих пристроїв до прикладних сервісів. Таким чином, SIEM стає не просто інструментом моніторингу, а центральним елементом аналітичної інфраструктури КСЗІ, який перетворює неструктуровані дані на цінну аналітику, забезпечуючи швидке прийняття рішень і підвищення рівня кіберстійкості підприємства.

SOC (Security Operations Center)

SOC (Security Operations Center) — це операційний центр кіберзахисту, який забезпечує безперервне спостереження за станом інформаційної безпеки, аналіз інцидентів та координацію дій у разі атак. Його фахівці працюють цілодобово, реагуючи на сигнали, отримані від SIEM та інших систем моніторингу. SOC виконує кілька ключових функцій: класифікує інциденти за рівнем критичності, проводить розслідування джерел загроз, ізолює уражені вузли та здійснює усунення наслідків атак. У складі SOC часто використовується технологія SOAR (Security Orchestration, Automation and Response), яка автоматизує виконання типових сценаріїв реагування, наприклад блокування облікового запису чи відключення скомпрометованого пристрою. SOC також проводить ретроспективний аналіз після інцидентів, розробляє рекомендації щодо посилення захисту та формує звітність для керівництва. Завдяки централізованому підходу SOC стає ядром управління кібербезпекою, яке поєднує технології, процеси та людей в єдиний координаційний механізм.

На рис. 2.6 представлено узагальнену модель функціонування SOC (Security Operations Center) — операційного центру безпеки, який забезпечує безперервний моніторинг, аналіз і реагування на кіберінциденти. SOC виконує сім взаємопов'язаних функціональних блоків, що утворюють замкнений цикл управління інформаційною безпекою підприємства. Першим етапом є Threat Intelligence — збір і аналітика даних про потенційні загрози з внутрішніх і зовнішніх джерел, що дозволяє проактивно виявляти ризики. Далі формується Knowledge Base, яка накопичує інформацію про інциденти, типові сценарії атак і методи реагування, забезпечуючи безперервне вдосконалення роботи центру. Блок Ticketing відповідає за реєстрацію, пріоритизацію та відстеження інцидентів у процесі їх усунення. Четверта складова — Security Information and Event Management (SIEM) — виконує централізований збір, кореляцію та аналітику подій безпеки з різних систем. П'ятий етап — Aggregation/Correlation — передбачає об'єднання й аналіз великих обсягів даних для виявлення взаємозв'язків між подіями та індикаторами компрометації. Шостий блок — Log Collection — забезпечує збір журналів подій з усіх компонентів ІКС, що є основою для аналітики та розслідувань. Завершальний етап — Reporting, Research & Development, який включає створення звітів, оцінку ефективності захисних заходів, оновлення правил кореляції та розробку нових підходів до кіберзахисту.

Таким чином, дана схема відображає повний цикл діяльності SOC — від виявлення загроз і накопичення знань до реагування, звітності та постійного вдосконалення системи безпеки.



Рис. 2.6. Структура та основні функції центру безпеки SOC (Security Operations Center)

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206-211]

SOC функціонує за багаторівневою структурою, що передбачає розподіл аналітиків за рівнями компетенції — від L1 (оператори моніторингу), які відстежують потоки подій у реальному часі, до L3 (експертів з цифрової криміналістики та розвідки загроз), що займаються глибинним аналізом складних атак. На першому рівні здійснюється первинна фільтрація та класифікація подій, тоді як другий рівень відповідає за верифікацію інцидентів, аналіз журналів, створення сценаріїв реагування та ескалацію критичних випадків. Вищі рівні SOC, зазвичай інтегровані з Threat Intelligence платформами, отримують дані з відкритих джерел, галузевих обмінів (ISAC/ISAO) і комерційних розвідслужб, що дозволяє прогнозувати загрози ще до їх прояву в інфраструктурі підприємства.

Ключовим компонентом SOC є панель моніторингу (Dashboard), яка відображає показники стану безпеки — кількість інцидентів, рівень ризиків, швидкість реагування (MTTR), середній час виявлення (MTTD) тощо. SOC тісно взаємодіє з іншими службами підприємства — IT-відділом, адміністраторами мереж, відділом комплаєнсу та керівництвом, забезпечуючи оперативний обмін інформацією про інциденти та зміни політик безпеки. Для підвищення ефективності роботи застосовується інтеграція з SIEM та SOAR, що дозволяє автоматизувати рутинні завдання, зменшити навантаження на аналітиків і скоротити час між виявленням та усуненням загрози.

Важливою складовою діяльності SOC є цикл безперервного вдосконалення (Continuous Improvement Cycle) — після кожного інциденту команда проводить розбір подій, уточнює сценарії реагування, оновлює правила кореляції у SIEM і

вдосконалює внутрішні процедури. Це дозволяє формувати адаптивну модель безпеки, що постійно розвивається разом із новими типами загроз. Крім того, SOC виконує функцію аудиту та контролю відповідності стандартам ISO/IEC 27035, NIST SP 800-61 і вимогам регуляторів, готуючи звіти про стан інформаційної безпеки та рівень зрілості системи захисту. Таким чином, SOC не лише реагує на інциденти, а й виконує роль центру стратегічного управління ризиками, інтегруючи аналітичні, технічні й організаційні процеси для побудови стійкої, керованої й проактивної системи кіберзахисту підприємства.

Засоби моніторингу безпеки

Засоби моніторингу безпеки є сенсорним рівнем інтегрованої системи, який забезпечує збір телеметрії, подій і технічних показників з усіх компонентів інфраструктури. До них належать IDS/IPS (Intrusion Detection/Prevention Systems), які аналізують мережевий трафік, виявляють спроби вторгнення та блокують підозрілу активність; EDR/XDR (Endpoint/Extended Detection and Response) — системи, що контролюють дії користувачів і процесів на робочих станціях, забезпечуючи проактивний захист від шкідливого ПЗ; NDR (Network Detection and Response) — засоби аналізу поведінки мережевих об'єктів, здатні фіксувати аномалії у комунікаціях між вузлами. Окрім цього, важливу роль відіграють системи контролю цілісності (File Integrity Monitoring), які відстежують зміни у конфігураціях та базах даних, і системи управління журналами (Log Management), що зберігають та структурують логи для подальшого аналізу у SIEM. Завдяки цим інструментам формується повна картина подій, яка дозволяє своєчасно виявляти відхилення від нормальної поведінки систем і користувачів.

На рис. 2.8 представлено схему інтеграції засобів моніторингу безпеки різних рівнів — NDR (Network Detection and Response), EDR (Endpoint Detection and Response) та XDR (Extended Detection and Response), — які спільно формують багаторівневу систему виявлення та реагування на загрози. На нижньому рівні розміщено NDR, що аналізує мережевий трафік і дозволяє виявляти аномальні переміщення, lateral movement та атаки, засновані на мережевій активності. Вище розташовано EDR, який фокусується на кінцевих точках — робочих станціях і серверах, — забезпечуючи глибоке дослідження процесів, дій користувачів і шкідливих програм, а також усунення загроз. На найвищому рівні — XDR, який об'єднує дані з різних джерел безпеки (мережа, кінцеві точки, хмарні сервіси, поштові системи) в єдине інформаційне поле для підвищення точності аналітики.

У результаті такої інтеграції підприємство отримує покращену видимість інцидентів, швидше реагування та точніше виявлення загроз, а також комплексний захист усіх компонентів інформаційної інфраструктури. Ця архітектура створює основу для побудови проактивної системи кіберзахисту, здатної адаптуватися до нових типів атак і мінімізувати ризики компрометації.

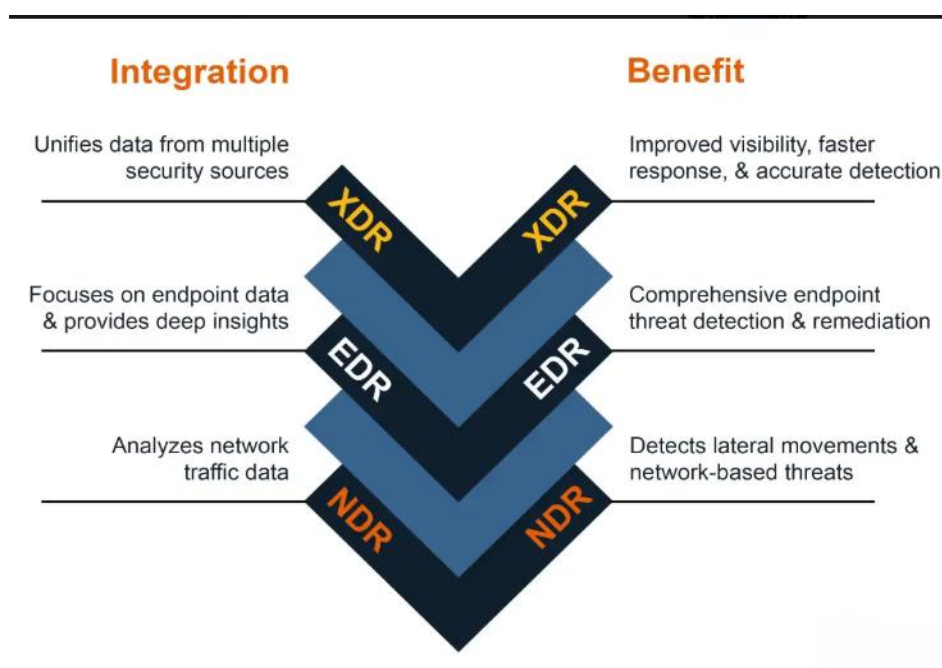


Рис. 2.8. Взаємодія та переваги систем моніторингу безпеки NDR, EDR та XDR
Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 201]

Засоби моніторингу безпеки виконують ключову роль у забезпеченні оперативного виявлення загроз, створюючи основу для роботи аналітичних систем та центрів реагування. Вони функціонують як “очі та вуха” КСЗІ, постійно збираючи й передаючи телеметрію до SIEM і SOC для подальшого аналізу. IDS (Intrusion Detection System) здійснює пасивний аналіз мережевого трафіку, виявляючи відомі та невідомі атаки за сигнатурами, евристикою чи поведінковими шаблонами, тоді як IPS (Intrusion Prevention System) активно блокує шкідливу активність у реальному часі. Такі системи здатні запобігати експлойтам, DDoS-атакам і спробам сканування портів, створюючи бар’єр між корпоративною мережею та зовнішнім середовищем.

EDR (Endpoint Detection and Response) орієнтується на кінцеві пристрої користувачів і сервери, аналізуючи процеси, мережеві з’єднання, доступ до файлів і поведінку користувачів. Його розширена версія — XDR (Extended Detection and Response) — поєднує дані з різних рівнів інфраструктури (мережа, хмара, кінцеві точки, поштові системи), формуючи єдине інформаційне поле загроз. Ці системи підтримують автоматизовані дії реагування, наприклад ізоляцію зараженого вузла, завершення процесів, видалення шкідливих файлів або скидання облікових даних. NDR (Network Detection and Response) аналізує трафік у реальному часі, використовуючи методи машинного навчання для виявлення прихованих каналів зв’язку, тунелювання чи нетипової активності в сегментах мережі.

Крім засобів виявлення, важливим елементом є File Integrity Monitoring (FIM), що контролює зміни у критичних системних файлах, конфігураціях та базах даних. FIM сигналізує про будь-які несанкціоновані модифікації, які можуть свідчити про проникнення або внутрішню загрозу. Log Management виступає інструментом збору, агрегування та нормалізації логів з усіх джерел ІКС, створюючи структуровану базу для подальшої аналітики у SIEM. Ці журнали подій містять неоціненну інформацію для розслідування інцидентів, відстеження ланцюга атак і підтвердження відповідності політикам безпеки.

Взаємодія між усіма засобами моніторингу дозволяє створити мультишаровий рівень спостереження, у якому інформація проходить через кілька етапів фільтрації та аналізу. Це підвищує точність виявлення загроз, зменшує кількість помилкових спрацьовувань і оптимізує роботу SOC. У сучасних умовах ці засоби інтегруються з хмарними аналітичними платформами, що дозволяє масштабувати моніторинг, зберігати історичні дані й застосовувати штучний інтелект для прогнозування атак. Таким чином, засоби моніторингу безпеки є не лише інструментом спостереження, а й активним елементом кіберзахисту, який забезпечує раннє попередження про інциденти, підвищує оперативність реагування та зміцнює загальну кіберстійкість підприємства.

У процесі інтеграції всі три компоненти — SIEM, SOC і моніторингові засоби — функціонують як єдина екосистема. Дані з сенсорів моніторингу надходять у SIEM, де вони аналізуються та корелюються, після чого інформація передається до SOC для прийняття рішень і виконання дій реагування. Такий підхід забезпечує замкнений цикл безпеки — від збору подій до усунення інциденту. Крім того, сучасні інтегровані системи використовують технології штучного інтелекту й машинного навчання, які допомагають прогнозувати потенційні загрози, зменшувати кількість помилкових спрацьовувань і підвищувати точність аналітики. У підсумку інтеграція SIEM, SOC і засобів моніторингу формує динамічну, самонавчальну та керовану систему кіберзахисту, здатну забезпечити стабільність бізнес-процесів і відповідність міжнародним стандартам інформаційної безпеки.

2.4. МЕТОДИ ОЦІНКИ ЕФЕКТИВНОСТІ ТА ТЕСТУВАННЯ КСЗІ

Методи оцінки ефективності та тестування комплексної системи захисту інформації (КСЗІ) спрямовані на визначення її здатності забезпечувати необхідний рівень безпеки інформаційних активів підприємства відповідно до вимог стандартів, політик і законодавства. Оцінювання ефективності КСЗІ є ключовим етапом життєвого циклу системи безпеки, адже дозволяє перевірити відповідність реалізованих механізмів встановленим вимогам, виявити вразливості, визначити залишкові ризики та оцінити реальну стійкість системи до кіберзагроз. Основною

метою є забезпечення впевненості у тому, що всі технічні, організаційні й криптографічні засоби захисту працюють узгоджено та забезпечують конфіденційність, цілісність і доступність даних у межах інформаційно-комунікаційної системи.

Оцінка ефективності базується на поєднанні аналітичних, експериментальних та статистичних методів. Аналітичні методи дозволяють формалізувати процес оцінювання через використання моделей ризику та математичних показників. Для цього застосовуються підходи FMEA (Failure Mode and Effects Analysis) для аналізу потенційних відмов системи, FAIR (Factor Analysis of Information Risk) для кількісного вимірювання ризиків за ймовірністю та вартісними показниками, а також SWOT- і GAP-аналіз для виявлення невідповідностей між поточним станом безпеки та цільовими стандартами. Важливим інструментом є експертне оцінювання, яке дозволяє отримати зважену оцінку ефективності на основі думок фахівців з кіберзахисту.

Імітаційні та експериментальні методи спрямовані на практичну перевірку роботи КСЗІ в умовах, наближених до реальних. Найпоширенішим є penetration testing (пентест), коли спеціалісти моделюють дії зловмисників для виявлення можливих шляхів проникнення до системи. Методи red teaming і blue teaming передбачають сценарне протистояння між командами атакуючих і захисників, що дозволяє перевірити оперативність реагування та узгодженість дій. Паралельно проводяться оцінки вразливостей (vulnerability assessment), які дають змогу автоматично виявляти недоліки в конфігураціях, програмному забезпеченні та мережевих службах. Для визначення стійкості системи до пікових навантажень використовують stress testing — випробування працездатності та надійності компонентів КСЗІ в умовах перевантаження чи збоїв.

Статистичні методи оцінювання ефективності базуються на аналізі результатів роботи систем моніторингу, зокрема IDS/IPS, SIEM та EDR. Основними метриками є показники TPR (True Positive Rate), що характеризує відсоток правильно виявлених атак, FPR (False Positive Rate), який відображає кількість помилкових спрацьовувань, а також MTTD (Mean Time to Detect) і MTTR (Mean Time to Respond), що показують швидкість виявлення та реагування на інциденти. В економічному аспекті ефективність визначається через показник ROI (Return on Security Investment), який демонструє співвідношення між витратами на кіберзахист і отриманим зниженням ризику чи запобіганням втратам.

Крім цих показників, у практиці оцінювання ефективності КСЗІ застосовуються також метрики MTTC (Mean Time to Contain) та MTTN (Mean Time to Normal), які відображають швидкість ізоляції загрози й повного відновлення системи після інциденту. Для комплексного аналізу використовується Incident Detection Rate (IDR), що визначає частку виявлених атак серед усіх зафіксованих спроб проникнення. Важливе значення має також Incident Containment Rate (ICR)

— відсоток інцидентів, локалізованих без подальшого поширення або ескалації. Для вимірювання стабільності роботи системи застосовується показник System Availability (SA), який характеризує відсоток часу, протягом якого інформаційна система залишається працездатною та захищеною. У процесі аналізу отримані статистичні дані агрегуються в динамічні звіти SIEM, що дозволяє виявляти тенденції зростання або зниження ефективності засобів безпеки. Такий підхід забезпечує кількісне підтвердження результативності КСЗІ, сприяє оптимізації використання ресурсів і підвищенню рівня готовності підприємства до сучасних кіберзагроз.

Тестування КСЗІ охоплює декілька видів перевірок. Функціональне тестування забезпечує перевірку правильності роботи всіх компонентів системи — засобів контролю доступу, шифрування, журналювання, резервного копіювання та відновлення. Тестування на проникнення дає змогу перевірити реальну стійкість системи до зовнішніх атак. Важливою частиною є тестування політик безпеки, що перевіряє правильність налаштувань у міжмережевих екранах, VPN, SIEM та Active Directory, а також перевірка відповідності стандартам ISO/IEC 27001, GDPR, DORA чи NIST SP 800-53. Такий аудит дозволяє оцінити не лише технічний стан системи, а й відповідність організаційних процедур міжнародним вимогам.

На рис. 2.9 представлено ключові метрики, що використовуються для оцінювання ефективності реагування на кіберінциденти в межах комплексної системи захисту інформації. Ці показники дозволяють оцінити, наскільки швидко та результативно система виявляє, локалізує та усуває загрози, а також відновлює нормальну роботу підприємства після інциденту. Основними серед них є MTTD (Mean Time to Detect) — середній час, необхідний для виявлення кіберінциденту з моменту його виникнення, та MTTC (Mean Time to Contain) — час, який витрачається на ізоляцію й нейтралізацію загрози. Після виявлення інциденту важливу роль відіграє MTTR (Mean Time to Respond), що показує, скільки часу потрібно для повного реагування та ліквідації наслідків атаки. Показник MTTN (Mean Time to Normal) відображає тривалість відновлення систем до стабільного стану, тоді як Incident Containment Rate характеризує відсоток успішно локалізованих інцидентів, які не призвели до подальшого поширення. Метрика First Contact Resolution Rate визначає ефективність роботи аналітиків SOC, показуючи частку інцидентів, вирішених під час першого реагування. Завершує набір показників Cost per Incident, який вимірює середній фінансовий вплив інциденту з урахуванням втрат продуктивності, витрат на відновлення даних і репутаційних збитків. Сукупно ці метрики формують основу кількісного аналізу ефективності КСЗІ, забезпечуючи можливість порівняння динаміки безпеки, оптимізації процесів реагування та підвищення рівня кіберстійкості підприємства.

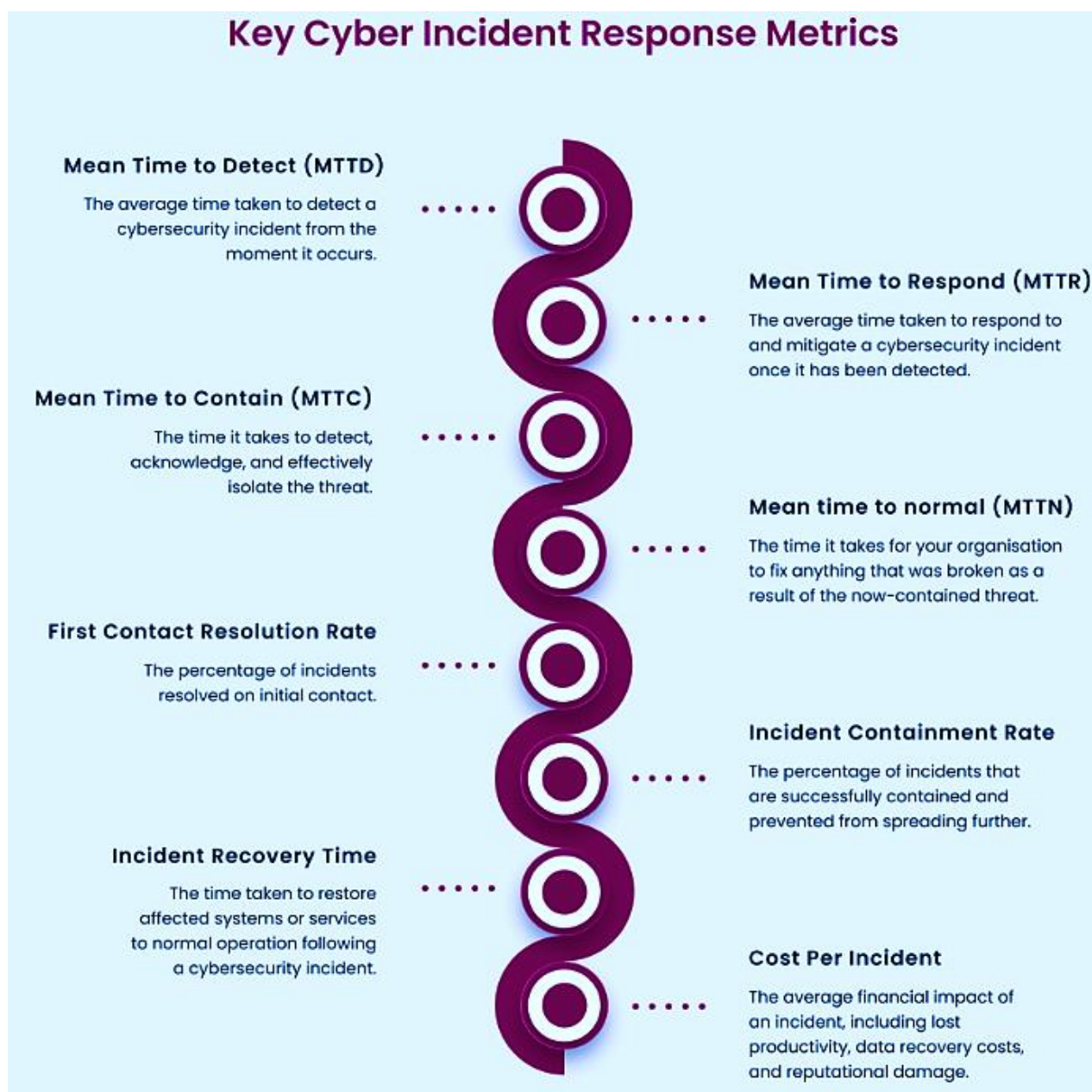


Рис. 2.9. Ключові метрики оцінювання ефективності реагування на кіберінциденти

Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206]

Комплексна оцінка ефективності КСЗІ завершується формуванням висновків про стан системи, ступінь її відповідності нормативним вимогам і можливі напрями вдосконалення. Результати тестувань і розрахунків використовуються для оновлення політик безпеки, перегляду ризиків та оптимізації витрат на кіберзахист. Регулярне проведення таких перевірок є запорукою підтримання високого рівня кіберстійкості, забезпечення надійності функціонування інформаційно-комунікаційних систем і дотримання міжнародних стандартів безпеки. Таким

чином, методи оцінки ефективності та тестування КСЗІ формують цілісну систему контролю якості захисту інформації, що забезпечує безперервне вдосконалення й адаптацію до нових кіберзагроз.

2.5. РОЗРОБКА ТА ВПРОВАДЖЕННЯ ПОЛІТИКИ БЕЗПЕКИ

Розробка та впровадження політики безпеки є одним із ключових етапів створення комплексної системи захисту інформації (КСЗІ), оскільки саме політика визначає стратегічні принципи, цілі та загальні правила управління інформаційною безпекою в межах підприємства. Політика безпеки (ПБ) — це базовий нормативний документ, який регламентує порядок доступу до інформаційних ресурсів, обробку, передавання, зберігання й знищення даних, а також визначає відповідальність усіх учасників процесу. Її основною метою є забезпечення конфіденційності, цілісності та доступності інформації, що обробляється в інформаційно-комунікаційній системі (ІКС), відповідно до вимог законодавства, міжнародних стандартів ISO/IEC 27001, NIST SP 800-53, DORA та внутрішніх регламентів підприємства.

На етапі розроблення політики безпеки проводиться детальний аналіз поточного стану захищеності інформаційних активів, виявлення потенційних загроз, оцінювання ризиків і визначення критичних процесів. На основі цих даних формуються принципи управління безпекою, визначаються зони відповідальності та повноваження між підрозділами. Важливою складовою є класифікація інформації за рівнями важливості й визначення відповідних заходів захисту для кожної категорії даних — від відкритих до конфіденційних чи критичних для бізнесу. Політика має встановлювати порядок доступу користувачів до інформаційних ресурсів, умови автентифікації, правила використання засобів криптографічного захисту, журналювання дій, резервного копіювання та знищення інформації.

Додатково на цьому етапі визначаються вимоги до технічних і програмних засобів захисту, таких як міжмережеві екрани, системи виявлення вторгнень, антивірусне ПЗ та засоби управління доступом. Розробляються регламенти реагування на інциденти, що описують порядок дій персоналу у випадку витоку, спроби несанкціонованого доступу чи компрометації даних. Формуються вимоги до ведення журналів подій безпеки, їх зберігання, аналізу та передачі до систем моніторингу типу SIEM для подальшої кореляції. Особлива увага приділяється забезпеченню безперервності бізнес-процесів (BCP) і відновленню після аварій (DRP), щоб гарантувати стабільність роботи підприємства навіть у разі критичних інцидентів. У політиці безпеки також мають бути визначені вимоги до підрядників і партнерів, які мають доступ до інформаційних ресурсів, з урахуванням принципів довірених взаємодій і відповідальності сторін. На завершення формується план

затвердження та комунікації політики серед усіх працівників, що включає ознайомлення персоналу, навчання та підписання угод про дотримання вимог інформаційної безпеки.

Розроблення політики безпеки здійснюється міждисциплінарною групою, до складу якої входять представники керівництва, служби інформаційної безпеки, IT-відділу, юристи та фахівці з управління ризиками. Ця група визначає стратегічні цілі, узгоджує політику з бізнес-процесами підприємства та формує узгоджені вимоги до всіх користувачів ІКС. Проект документа проходить кілька етапів погодження — спочатку внутрішню експертизу, потім затвердження керівництвом і, за потреби, аудит відповідності зовнішнім стандартам. Після ухвалення політика стає офіційним регламентом, який зобов'язує всіх працівників дотримуватися визначених вимог і процедур.

На цьому етапі також розробляються супровідні документи — стандарти, інструкції, процедури та положення, що деталізують реалізацію окремих пунктів політики безпеки на практиці. Важливим завданням групи є забезпечення узгодженості політики з національними законами, галузевими нормативами та міжнародними вимогами, такими як ISO/IEC 27001, NIST SP 800-53 чи GDPR. Проводиться аналіз можливих конфліктів між політикою безпеки та чинними регламентами підприємства, з подальшим внесенням змін для усунення невідповідностей. Після затвердження політика публікується у внутрішньому інформаційному просторі підприємства — на порталі чи в корпоративній базі знань — для забезпечення відкритого доступу персоналу до її положень. Паралельно розробляється план комунікації, який включає роз'яснювальні заходи, тренінги та обов'язкове ознайомлення всіх співробітників із ключовими вимогами політики. Завдяки цьому процесу формується спільне розуміння ролі кожного працівника у забезпеченні інформаційної безпеки та підвищується рівень корпоративної культури кіберзахисту.

Впровадження політики безпеки передбачає не лише технічну інтеграцію правил у ІКС (через системи контролю доступу, SIEM, SOC, DLP, IAM), але й організаційні заходи — навчання персоналу, проведення інструктажів і тестування знань. У межах цього процесу створюється система управління інформаційною безпекою (СУІБ), яка забезпечує постійний моніторинг виконання політики, аудит дотримання вимог і зворотний зв'язок для вдосконалення процедур. Особлива увага приділяється формуванню культури безпеки серед працівників, адже навіть найсучасніші технічні рішення можуть втратити ефективність без належної обізнаності персоналу.

Рис. 2.10 демонструє пірамідальну модель, де в основі розташована політика (Policy), над нею — стандарти (Standards), далі йдуть процедури (Procedures), рекомендації / кращі практики (Guidelines / Best Practices) і на верхньому рівні — базові налаштування (Baselines). Ця модель показує, як політика задає стратегічні

рамки (що треба робити), стандарти визначають обов'язкові вимоги, процедури описують порядок дій, а рекомендації і базові налаштування допомагають у практичній імплементації. Така ієрархія добре підходить до теми «Розробка та впровадження політики безпеки», оскільки ілюструє зв'язок між різними рівнями нормативного забезпечення інформаційної безпеки.

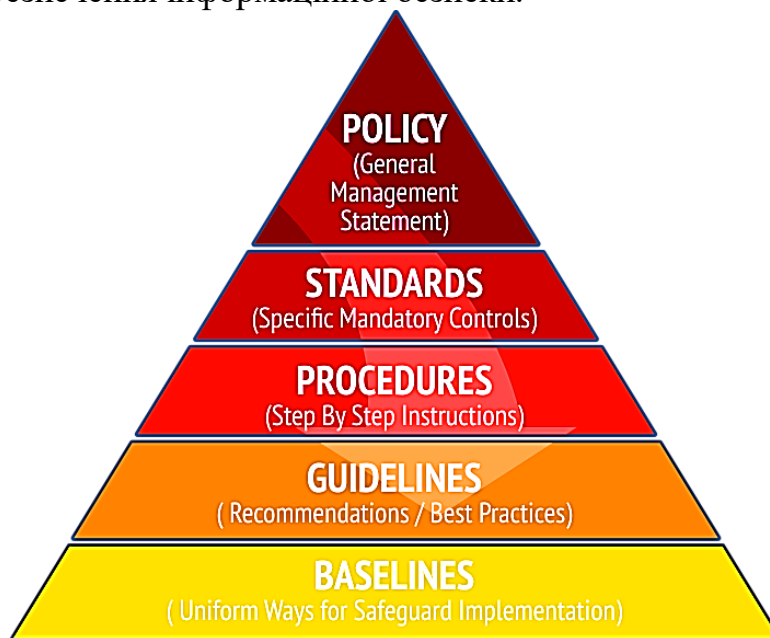


Рис. 2.10. Ієрархія інформаційної політики та елементів безпеки
Джерело: [1-10, 18-23, 28-36, 56-68, 81-102, 206]

Політика безпеки не є статичним документом — вона повинна регулярно переглядатися й оновлюватися відповідно до змін у технологічному середовищі, законодавстві, організаційній структурі чи виявлених нових ризиків. Періодична ревізія політики здійснюється з використанням результатів аудитів, тестів на проникнення, аналізу інцидентів і звітів SIEM. На основі цих даних вносяться корективи до процедур доступу, реагування, резервного копіювання, управління вразливостями та управління ризиками. Таким чином, політика безпеки виступає живим механізмом управління, який постійно адаптується до нових викликів і забезпечує динамічну стійкість підприємства в умовах розвитку кіберзагроз.

Крім того, до процесу оновлення політики залучаються всі зацікавлені сторони — служба інформаційної безпеки, IT-відділ, керівництво та зовнішні аудитори, що забезпечує комплексний підхід до удосконалення документу. Під час ревізії враховуються не лише технічні аспекти, а й поведінкові фактори, зокрема дисципліна користувачів і рівень дотримання правил безпеки. Оновлена політика має проходити обов'язкове погодження, затвердження й доведення до відома всіх співробітників підприємства. Для цього організовуються навчальні сесії, інструктажі та тестування, які допомагають закріпити знання нових вимог і

процедур. Важливо також забезпечити контроль за виконанням оновлених положень через систему внутрішнього моніторингу, регулярні звіти та внутрішні аудити. Результати таких перевірок стають основою для подальшого вдосконалення політики, створюючи замкнутий цикл постійного поліпшення. У підсумку це дозволяє підприємству зберігати високу адаптивність до змін середовища, своєчасно реагувати на нові ризики й підтримувати відповідність найкращим міжнародним практикам інформаційної безпеки.

Оновлення політики безпеки супроводжується оцінкою її ефективності, що проводиться шляхом порівняння поточних показників безпеки з визначеними KPI та KRI. Для цього залучаються як внутрішні експерти, так і зовнішні аудитори, які здійснюють незалежну перевірку відповідності політики стандартам ISO/IEC 27001 та вимогам наглядових органів. Усі зміни фіксуються у реєстрі редакцій документа, що забезпечує простежуваність і контроль за історією оновлень. Після внесення змін проводиться повторне затвердження політики керівництвом підприємства та інформування всіх працівників про актуалізовані положення. Додатково проводяться тематичні навчання й тестування персоналу, щоб гарантувати розуміння нових вимог і процедур. У результаті формується замкнутий цикл управління політикою безпеки — від аналізу й перегляду до реалізації, навчання та постійного вдосконалення, що підвищує рівень кіберстійкості всієї системи.

Також на цьому етапі здійснюється аналіз впливу оновленої політики на бізнес-процеси, щоб уникнути конфліктів між вимогами безпеки та операційною ефективністю. Для оцінювання результативності впроваджених змін використовуються метрики, такі як зниження кількості інцидентів, скорочення часу реагування (MTTR) та підвищення показника відповідності (compliance score). На основі отриманих даних розробляються рекомендації щодо подальшої оптимізації політики, зокрема вдосконалення процедур управління доступом, резервного копіювання й реагування на інциденти. Важливим аспектом є проведення незалежної сертифікації або повторного аудиту для підтвердження відповідності міжнародним стандартам. Результати оцінювання документуються в аналітичному звіті, який подається керівництву для прийняття стратегічних рішень щодо розвитку системи безпеки. Таким чином, процес оновлення та оцінки ефективності політики перетворюється на безперервний цикл вдосконалення, що забезпечує стабільність і прогнозованість системи захисту. У підсумку це гарантує не лише технічну, але й управлінську зрілість підприємства в сфері інформаційної безпеки.

У результаті ефективно розроблена й впроваджена політика безпеки створює нормативну основу для функціонування всіх підсистем КСЗІ, узгоджує технічні, організаційні та правові аспекти кіберзахисту, підвищує рівень довіри до ІКС і забезпечує відповідність діяльності підприємства міжнародним стандартам інформаційної безпеки.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 2

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
6. Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S.(2025) Intelligent System for Simulation Modeling and Research of Information Objects. Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025), May 13–14, 2025, Kyiv, Ukraine, Vol-4053, P. 237-251. ISSN 1613-0073.
7. Агашков, А., Шевченко, С., Бондарчук, А., & Жебка, В. (2024). Шляхи підвищення транспортних операцій за допомогою хмарних логістичних рішень. Телекомунікаційні та інформаційні технології, 4(85), 4–15. <https://doi.org/10.31673/2412-4338.2024.047191>
8. Sokolov, V., Kostiuk, Y., Skladannyi, P., Korshun, N. (2025). Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements. Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies", ICST 2025, Vol-4048, P. 397 - 411. ISSN 1613-0073.
9. Бондарчук, А., Складанний, П., Жебка, В., & Стражніков, А. (2024). Оптимізація системи зарядки електромобілів на основі методів дослідження операцій. Телекомунікаційні та інформаційні технології, 3(84), 86–93. <https://doi.org/10.31673/2412-4338.2024.038693>
10. Крючкова, Л., Башкевич, Є., & Куцибала, М. (2024). Програмна реалізація алгоритмів виокремлення контурів зображень об'єктів в інтелектуальних системах відеоспостереження. Телекомунікаційні та

інформаційні технології, 2(83), 14–29. <https://doi.org/10.31673/2412-4338.2024.022439>

11. Оксанич, І., Гречанінов, В., Литвинов, В., & Складанний П. (2024). Особливості забезпечення гарантоздатності та кіберстійкості інформаційного обміну в складних умовах. Телекомунікаційні та інформаційні технології, 2(83), 105–113. <https://doi.org/10.31673/2412-4338.2024.022128>

12. Крючкова, Л., Яремчук, Д., & Пазинін, А. (2024). Планування навантаження контейнерів за допомогою лінійного програмування. Телекомунікаційні та інформаційні технології, 2(83), 114 –119. <https://doi.org/10.31673/2412-4338.2024.022935>

13. Цирканюк, Д., & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 2(26), 140–154. <https://doi.org/10.28925/2663-4023.2024.26.675>

14. Козачок, В., & Драпатий, М. (2024). Аналіз технологій розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 2(26), 374–391. <https://doi.org/10.28925/2663-4023.2024.26.699>

15. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Кібербезпека: освіта, наука, техніка, 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>

16. Корнієць, В., & Жданова, Ю. (2024). Методика формування швидкісного імітостійкого шифру багато алфавітної заміни. Кібербезпека: освіта, наука, техніка, 2(26), 476–486. <https://doi.org/10.28925/2663-4023.2024.26.723>

17. Руда, Х., Сабодашко, Д., Микитин, Г., Швед, М., Бордуляк, С., & Коршун, Н. (2024). Порівняння методів цифрової обробки сигналів та моделей глибинного навчання у голосовій аутентифікації. Кібербезпека: освіта, наука, техніка, 1(25), 140–160. <https://doi.org/10.28925/2663-4023.2024.25.140160>

18. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 1(25), 330–343. <https://doi.org/10.28925/2663-4023.2024.25.330343>

19. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. Кібербезпека: освіта, наука, техніка, 1(25), 390–400. <https://doi.org/10.28925/2663-4023.2024.25.390400>

20. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в

системах забезпечення інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 1(25), 468–486. <https://doi.org/10.28925/2663-4023.2024.25.468486>

21. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. Кібербезпека: освіта, наука, техніка, 4(24), 185–195. <https://doi.org/10.28925/2663-4023.2024.24.185195>

22. Крючкова, Л., & Леонтьук, Н. (2024). Програмно-апаратна реалізація алгоритму швидкої оцінки потужності Wi-Fi сигналу в точках простору урбанізованого приміщення. Кібербезпека: освіта, наука, техніка, 4(24), 241–256. <https://doi.org/10.28925/2663-4023.2024.24.241256>

23. Крючкова, Л., & Дяків, В. (2024). Програмна реалізація розрахунку просторового розподілу поля рамкових антен. Кібербезпека: освіта, наука, техніка, 4(24), 312–320. <https://doi.org/10.28925/2663-4023.2024.24.312320>

24. Іосіфов, Є., & Соколов, В. (2024). Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. Кібербезпека: освіта, наука, техніка, 4(24), 398–414. <https://doi.org/10.28925/2663-4023.2024.24.398414>

25. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Кібербезпека: освіта, наука, техніка, 3(23), 258–273. <https://doi.org/10.28925/2663-4023.2024.23.258273>

26. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. Кібербезпека: освіта, наука, техніка, 3(23), 318–327. <https://doi.org/10.28925/2663-4023.2024.23.318327>

27. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. Кібербезпека: освіта, наука, техніка, 3(23), 338–347. <https://doi.org/10.28925/2663-4023.2024.23.338347>

28. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. Кібербезпека: освіта, наука, техніка, 2(22), 6–18. <https://doi.org/10.28925/2663-4023.2023.22.618>

29. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. Кібербезпека: освіта, наука, техніка, 2(22), 68–83. <https://doi.org/10.28925/2663-4023.2023.22.6883>

30. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Бржезька, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Кібербезпека: освіта, наука, техніка, 2(22), 148–155. <https://doi.org/10.28925/2663-4023.2023.22.148155>

31. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 2(22), 156–167. <https://doi.org/10.28925/2663-4023.2023.22.156167>
32. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 2(22), 168–178. <https://doi.org/10.28925/2663-4023.2023.22.168178>
33. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(21), 99–120. <https://doi.org/10.28925/2663-4023.2023.21.99120>
34. Спасітелєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. *Кібербезпека: освіта, наука, техніка*, 1(21), 193–210. <https://doi.org/10.28925/2663-4023.2023.21.193210>
35. Костюк Ю., Бебешко Б., Складанний П., Рзаєва С., Хорольська К. Оптимізація буфера та пріоритетів для забезпечення безпеки У Bluetooth-мережах. *Безпека інформаційних систем і технологій*. 2025. 2(8), 5-16.
36. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. *Кібербезпека: освіта, наука, техніка*, 1(21), 223–233. <https://doi.org/10.28925/2663-4023.2023.21.223233>
37. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. *Кібербезпека: освіта, наука, техніка*, 4(20), 174–182. <https://doi.org/10.28925/2663-4023.2023.20.174182>
38. Соколов, В., & Складанний, П. (2023). Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». *Кібербезпека: освіта, наука, техніка*, 4(20), 183–204. <https://doi.org/10.28925/2663-4023.2023.20.183204>

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні етапи включає процес моделювання архітектури комплексної системи захисту інформації (КСЗІ) на підприємстві?
2. Які типи інформаційних активів підлягають ідентифікації під час аналізу об'єкта захисту?
3. Що відображає модель потоків даних (DFD) у контексті побудови архітектури КСЗІ?

4. Які основні елементи входять до логічної моделі КСЗІ та яку роль вони відіграють у системі безпеки?
5. Які компоненти включає фізична модель КСЗІ і як вони забезпечують захист інформаційних ресурсів?
6. Які функції виконує політичний рівень у багаторівневій архітектурі системи захисту інформації?
7. У чому полягає роль організаційного рівня захисту інформації на підприємстві?
8. Які основні засоби реалізації безпеки використовуються на технічному рівні КСЗІ?
9. Як взаємодіють між собою політичний, організаційний і технічний рівні в єдиній системі захисту?
10. Чому важливо підтримувати узгодженість між рівнями архітектури КСЗІ?
11. Які основні функції виконує система SIEM (Security Information and Event Management) у структурі КСЗІ?
12. У чому полягає завдання центру кіберзахисту SOC (Security Operations Center) і як він взаємодіє з SIEM?
13. Яку роль відіграють засоби моніторингу безпеки (IDS/IPS, EDR, NDR) у забезпеченні кіберзахисту підприємства?
14. Як інтеграція SIEM, SOC та моніторингових систем підвищує ефективність виявлення та реагування на кіберзагрози?
15. Які переваги надає використання штучного інтелекту й машинного навчання в аналітичних системах SIEM та SOC?
16. Які основні методи використовуються для оцінки ефективності комплексної системи захисту інформації?
17. У чому полягає різниця між penetration testing, red teaming і vulnerability assessment під час тестування КСЗІ?
18. Які основні показники ефективності (KPI, TPR, FPR, MTTD, MTTR) застосовуються для оцінювання стану інформаційної безпеки?
19. Яку роль відіграє аудит і сертифікація у процесі перевірки відповідності КСЗІ міжнародним стандартам ISO/IEC 27001, NIST чи DORA?
20. Які основні етапи включає розробка, впровадження та регулярне оновлення політики інформаційної безпеки на підприємстві?

РОЗДІЛ 3

УПРАВЛІННЯ РИЗИКАМИ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ: МОДЕЛІ, МЕТОДИ ТА ІНСТРУМЕНТИ ОЦІНКИ



- 3.1. Методології ризик-менеджменту: ISO/IEC 27005, NIST SP 800-30, FAIR**
- 3.2. Методи кількісної та якісної оцінки ризиків**
- 3.3. GAP-аналіз, SWOT, FMEA як підходи до оцінки вразливостей**
- 3.4. Моделі загроз і векторів атак у ризик-орієнтованому управлінні**
- 3.5. Адаптивне управління ризиками на основі машинного навчання**
- 3.6. Виклики безпеки у хмарних та SDN-мережах**
- 3.6. Автоматизований моніторинг, візуалізація та аудит ризиків у системах управління інформаційною безпекою**

Управління ризиками в інформаційній безпеці охоплює системний процес виявлення, аналізу, оцінювання та мінімізації ризиків, які можуть впливати на конфіденційність, цілісність і доступність інформаційних активів підприємства. Метою такого управління є досягнення оптимального рівня безпеки за умов обмежених ресурсів шляхом балансування між витратами на захист і потенційними збитками від реалізації загроз. Основу сучасного ризик-менеджменту становлять міжнародні стандарти ISO/IEC 27005, NIST SP 800-30 і модель FAIR, які визначають структуровану послідовність дій для ідентифікації активів, аналізу вразливостей, моделювання сценаріїв атак, розрахунку ймовірностей подій і формування ефективних заходів реагування.

У практичному аспекті управління ризиками базується на створенні політики безпеки, що визначає критерії прийнятного ризику, рівні допуску та механізми контролю. Важливою складовою є побудова матриці ризиків, яка поєднує ймовірність настання події з масштабом її впливу на діяльність підприємства. Для підвищення точності оцінювання використовуються кількісні методи, зокрема статистичний аналіз, байєсівські мережі та моделі на основі нечіткої логіки. Сучасні інструменти управління ризиками інтегруються в системи моніторингу безпеки (SIEM, SOAR) і забезпечують автоматизоване виявлення інцидентів та реагування на них у режимі реального часу. Процес управління ризиками є безперервним і передбачає регулярний перегляд результатів, адаптацію заходів до нових загроз і вдосконалення системи контролю. Такий підхід дає змогу забезпечити сталу роботу інформаційних систем, підтримувати довіру користувачів і зменшувати ймовірність критичних кіберінцидентів.

Методи оцінювання ризиків поділяються на якісні та кількісні: перші базуються на експертних підходах, SWOT-аналізі, GAP-аналізі та методі FMEA, тоді як другі використовують математичні, статистичні й імовірнісні моделі, включаючи байєсівський аналіз, нечіткі множини, машинне навчання та моделювання Монте-Карло. Практична реалізація ризик-менеджменту здійснюється за допомогою спеціалізованих програмних інструментів, таких як RiskWatch, OCTAVE Allegro, CRAMM, OpenFAIR Toolkit або інтегрованих систем моніторингу безпеки типу SIEM/SOAR (Splunk, IBM QRadar, Wazuh). Ефективне управління ризиками передбачає впровадження циклу PDCA (Plan–Do–Check–Act), який забезпечує безперервне вдосконалення процесів безпеки, підвищення стійкості інформаційної інфраструктури до загроз і адаптацію політики захисту до динамічних умов кіберпростору.

3.1. МЕТОДОЛОГІЇ РИЗИК-МЕНЕДЖМЕНТУ: ISO/IEC 27005, NIST SP 800-30, FAIR

Методології ризик-менеджменту в інформаційній безпеці забезпечують систематизований підхід до виявлення, аналізу, оцінювання та мінімізації ризиків, які можуть впливати на інформаційні активи підприємства. Однією з найпоширеніших є методологія ISO/IEC 27005, розроблена як складова системи управління інформаційною безпекою (ISMS) відповідно до стандарту ISO/IEC 27001. Вона визначає повний життєвий цикл управління ризиками — від контекстуалізації середовища, ідентифікації активів і загроз до оцінки, оброблення та моніторингу ризиків.

Методологія базується на ітеративному процесі, який включає п'ять основних етапів: встановлення контексту, оцінювання ризику, оброблення ризику, прийняття рішень і постійний моніторинг. ISO/IEC 27005 рекомендує застосовувати як якісні, так і кількісні методи оцінювання, а також передбачає документування всіх етапів для підвищення прозорості та повторюваності процесу. Головна перевага цієї методології полягає у її універсальності — вона може бути адаптована під будь-який тип підприємства, галузь або масштаб ІКС, інтегруючись із корпоративними процесами управління безпекою.

ISO/IEC 27005

ISO/IEC 27005 — це міжнародний стандарт, який визначає методологічну основу для управління ризиками інформаційної безпеки в межах системи менеджменту інформаційної безпеки (СМІБ), побудованої відповідно до ISO/IEC 27001. Його головна мета полягає у наданні підприємствам систематизованого підходу до ідентифікації, аналізу, оцінювання, оброблення та моніторингу ризиків, що можуть вплинути на конфіденційність, цілісність і доступність інформаційних активів. Стандарт не нав'язує конкретних інструментів або моделей, а пропонує гнучку структуру, яку можна адаптувати до будь-якої галузі, масштабу або рівня зрілості інформаційної системи.

На рис. 4.1 представлено узагальнену модель процесу управління ризиками інформаційної безпеки згідно зі стандартом ISO/IEC 27005. Процес починається з етапу встановлення контексту (Context Establishment), під час якого визначаються межі системи, бізнес-цілі, нормативно-правові вимоги, зацікавлені сторони та критерії прийнятності ризику. Після цього здійснюється оцінювання ризику (Risk Assessment), що включає три взаємопов'язані етапи: ідентифікацію ризику (Risk Identification), аналіз ризику (Risk Analysis) та оцінку ризику (Risk Evaluation). На етапі ідентифікації визначаються активи, загрози, вразливості та потенційні наслідки для безпеки. Аналіз ризику передбачає розрахунок імовірності реалізації загрози та масштабу можливих збитків, що дозволяє кількісно або якісно оцінити рівень ризику. Далі проводиться оцінка ризику, у межах якої порівнюються отримані результати з критеріями прийнятності, визначаються пріоритети реагування та формується план дій.

Наступним етапом є оброблення ризику (Risk Treatment), що передбачає вибір і впровадження заходів контролю для зниження, передачі, уникнення або прийняття ризику. Після впровадження заходів визначається залишковий ризик (Residual Risk) — рівень ризику, який залишається після реалізації всіх передбачених заходів безпеки. Важливу роль у процесі відіграють комунікації та консультації (Communication & Consultation), що

забезпечують обмін інформацією між усіма учасниками процесу управління ризиками, сприяють узгодженості рішень і підвищують прозорість управлінських дій.

Додатково у схемі представлено базу знань про ризики конфіденційності (Privacy Risk Knowledge Base), яка накопичує інформацію про відомі загрози, уразливості, типові сценарії інцидентів і засоби контролю. Її використання дозволяє підвищити точність аналізу, стандартизувати підходи до оцінювання ризиків і забезпечити повторюваність результатів. Процес є циклічним — результати оцінки та залишкових ризиків стають основою для перегляду контексту та вдосконалення системи управління безпекою. Такий підхід забезпечує безперервне поліпшення, адаптивність і стабільність процесів інформаційної безпеки в межах підприємства.

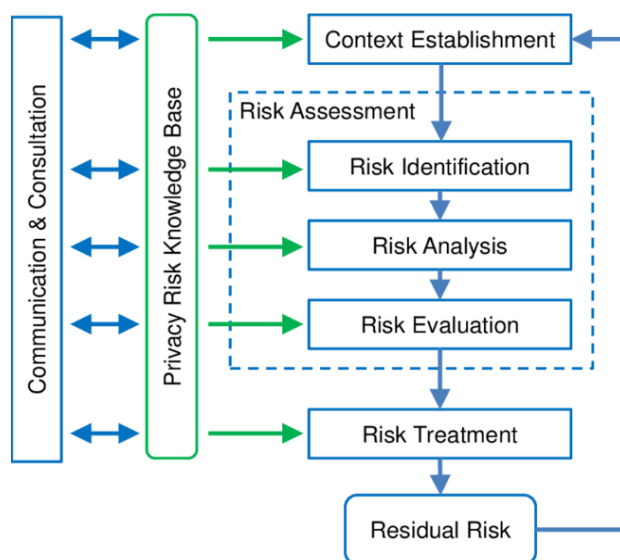


Рис. 3.1. Процес управління ризиками відповідно до методології ISO/IEC 27005

Джерело: [1-9, 11-26, 32-48, 60-65]

В основі ISO/IEC 27005 лежить цикл PDCA (Plan–Do–Check–Act), який забезпечує безперервне вдосконалення процесу управління ризиками. На етапі Plan (Планування) визначається контекст організації, встановлюються цілі безпеки, визначаються активи, власники активів, їхня вартість і залежності. Під час Do (Виконання) проводиться ідентифікація загроз, вразливостей і можливих інцидентів, визначаються сценарії атак і джерела ризику. Далі здійснюється оцінювання ризику, яке включає три складові: аналіз (визначення ймовірностей і наслідків), оцінку (порівняння з критеріями прийнятності) та оброблення ризику (вибір заходів контролю).

На етапі Check (Перевірка) здійснюється моніторинг ефективності реалізованих заходів, перегляд ризиків і коригування політики безпеки, а етап Act (Поліпшення) передбачає оновлення процесів управління з урахуванням змін у зовнішньому середовищі, нових загроз чи технологій.

Процес управління ризиками відповідно до ISO/IEC 27005 складається з кількох логічно пов'язаних етапів.

1. Визначення контексту — формулювання меж системи, визначення бізнес-цілей, правових і нормативних вимог, а також ролей і відповідальності учасників процесу.
2. Ідентифікація ризиків — виявлення активів, загроз, вразливостей і потенційних наслідків для інформаційної безпеки.
3. Аналіз ризиків — оцінювання ймовірності реалізації загроз і масштабів їх впливу з використанням якісних або кількісних методів.
4. Оцінювання ризиків — порівняння отриманих значень із визначеними критеріями прийнятності та визначення пріоритетів для реагування.
5. Оброблення ризиків — вибір і впровадження заходів контролю: зниження, передача, уникнення або прийняття ризику.
6. Моніторинг і перегляд — постійне відстеження змін, оцінка ефективності заходів і оновлення реєстру ризиків.

Стандарт підкреслює важливість документування всіх етапів, створення реєстру ризиків, у якому фіксуються активи, загрози, вразливості, рівень ризику, власники ризиків і статус реалізації заходів. Такий підхід забезпечує простежуваність процесу і є основою для аудиту та вдосконалення системи безпеки. Важливо, що ISO/IEC 27005 не обмежується лише технічними аспектами — він охоплює організаційні, людські та правові чинники, що впливають на ризики.

На рис. 3.2 зображено ітеративну модель управління ризиками відповідно до стандарту ISO/IEC 27005, яка охоплює послідовні етапи від встановлення контексту до прийняття ризику. Процес починається з встановлення контексту (Context Establishment), де визначаються цілі, межі системи, критерії прийнятності ризику та чинники, що впливають на безпеку. Далі виконується оцінювання ризику (Risk Assessment), яке включає ідентифікацію, оцінку (Risk Estimation) та оцінювання ризику (Risk Evaluation). На цих етапах визначаються активи, загрози, вразливості, ймовірність реалізації ризику та потенційні наслідки. Якщо результати оцінки задовільні, здійснюється оброблення ризику (Risk Treatment) — вибір і реалізація заходів для його зниження, передачі, уникнення або прийняття. Після перевірки ефективності заходів відбувається прийняття ризику (Risk Acceptance), що фіксує залишковий ризик, прийнятний для підприємства. Процес супроводжується комунікацією (Risk

Communication), яка забезпечує обмін інформацією між учасниками, та моніторингом і переглядом (Risk Monitoring and Review), що гарантують актуальність і безперервне вдосконалення системи управління ризиками.

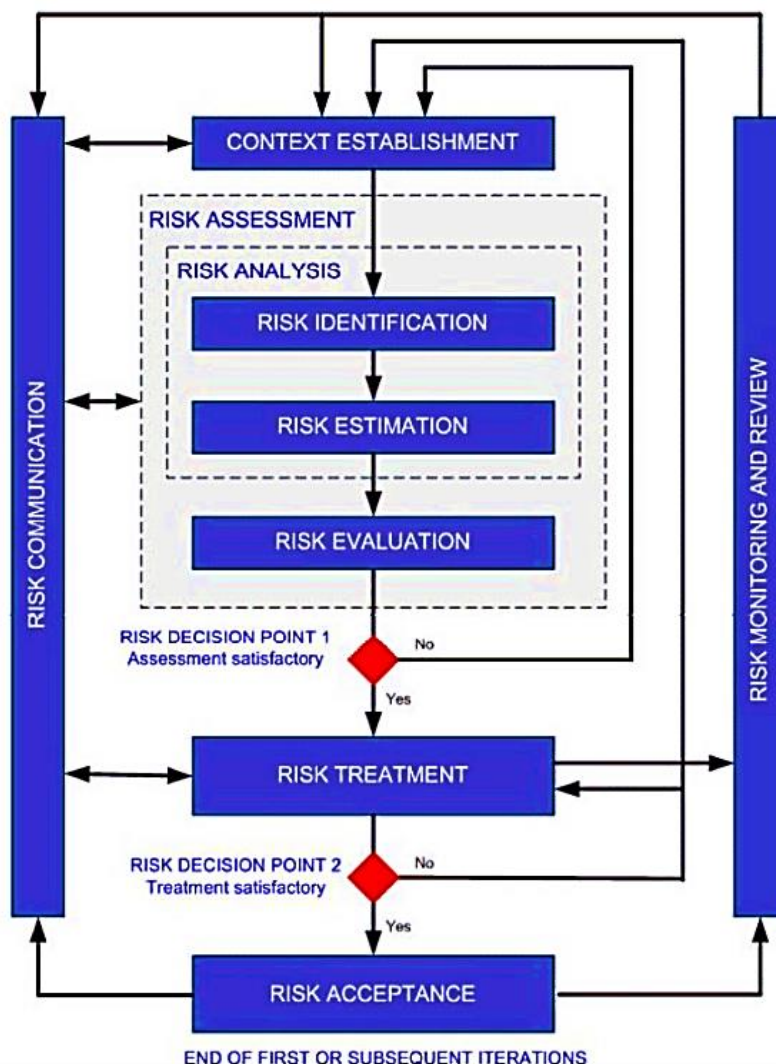


Рис. 3.2. Ітеративний процес управління ризиками інформаційної безпеки відповідно до ISO/IEC 27005

Джерело: [1-9, 11-26, 32-48, 60-65, 78-95, 102-125]

Ключовою особливістю ISO/IEC 27005 є його інтеграційність. Він може взаємодіяти з іншими міжнародними стандартами, зокрема ISO/IEC 31000 (загальний менеджмент ризиків), ISO/IEC 27002 (практичні заходи контролю безпеки), ISO/IEC 27019 (захист енергетичних систем) і NIST RMF. Це робить його універсальним інструментом для створення комплексної системи управління безпекою, яка поєднує технічні, адміністративні та стратегічні компоненти.

Впровадження ISO/IEC 27005 дозволяє підприємствам систематизувати підхід до управління ризиками, уникнути хаотичних або реактивних дій, зменшити ймовірність критичних інцидентів та оптимізувати витрати на захист. Завдяки орієнтації на безперервне вдосконалення, цей стандарт сприяє формуванню культури безпеки, де управління ризиками стає невід'ємною частиною стратегічного управління інформаційними ресурсами підприємства.

NIST SP 800-30

Інша ключова методологія — NIST SP 800-30, створена Національним інститутом стандартів і технологій США (NIST), що надає практичні рекомендації щодо проведення аналізу ризиків для інформаційних систем. Вона визначає ризик як функцію від ймовірності виникнення загрози та впливу вразливості на актив. Методологія складається з трьох етапів: підготовки до оцінювання, виконання оцінки ризиків і звітування про результати. Основна увага приділяється створенню моделей загроз, визначенню сценаріїв атак, кількісному вимірюванню наслідків і розробленню стратегій мінімізації ризиків. Особливістю NIST SP 800-30 є її орієнтація на прийняття управлінських рішень, а не лише на технічний аналіз. Ця методика широко застосовується в державних і комерційних структурах США, зокрема в рамках Risk Management Framework (RMF), який забезпечує єдність між оцінюванням ризиків, контролем і аудитом безпеки.

На рис. 3.3 зображено процес оцінювання ризиків відповідно до методології NIST SP 800-30, який є складовою системи управління ризиками в інформаційній безпеці. Процес розпочинається з етапу підготовки до оцінювання ризику, де формується контекст аналізу, визначаються цілі, межі, критерії прийнятності ризику та організаційна рамка управління. Далі виконується ідентифікація джерел загроз і подій, які можуть вплинути на безпеку інформаційних активів, з урахуванням як зовнішніх факторів (кіберзагрози, техногенні події), так і внутрішніх (помилки персоналу, недоліки конфігурації). Наступним кроком є визначення вразливостей і умов, що сприяють реалізації загроз, тобто технічних, організаційних або людських слабких місць, які підвищують ризик інциденту. Після цього здійснюється оцінка ймовірності виникнення події, що відображає реальну можливість реалізації конкретної загрози з урахуванням наявних засобів захисту та контролю. На наступному етапі визначається потенційний вплив інциденту на конфіденційність, цілісність і доступність інформації, що дозволяє кількісно або якісно оцінити масштаби можливих збитків. Завершальним елементом є визначення рівня ризику як функції від ймовірності настання події та очікуваного впливу, що

дозволяє сформуванати підґрунтя для прийняття управлінських рішень щодо мінімізації або прийняття ризиків. Усі етапи процесу супроводжуються постійними комунікаціями та обміном інформацією між учасниками, що забезпечує узгодженість дій, прозорість процесу й ефективність реагування. Важливою складовою є також підтримання оцінювання ризиків, яке передбачає регулярне оновлення результатів і повторну оцінку в разі зміни умов функціонування системи або появи нових загроз. Такий підхід забезпечує безперервність управління ризиками, підвищує адаптивність системи безпеки та сприяє прийняттю обґрунтованих стратегічних рішень у сфері інформаційного захисту.

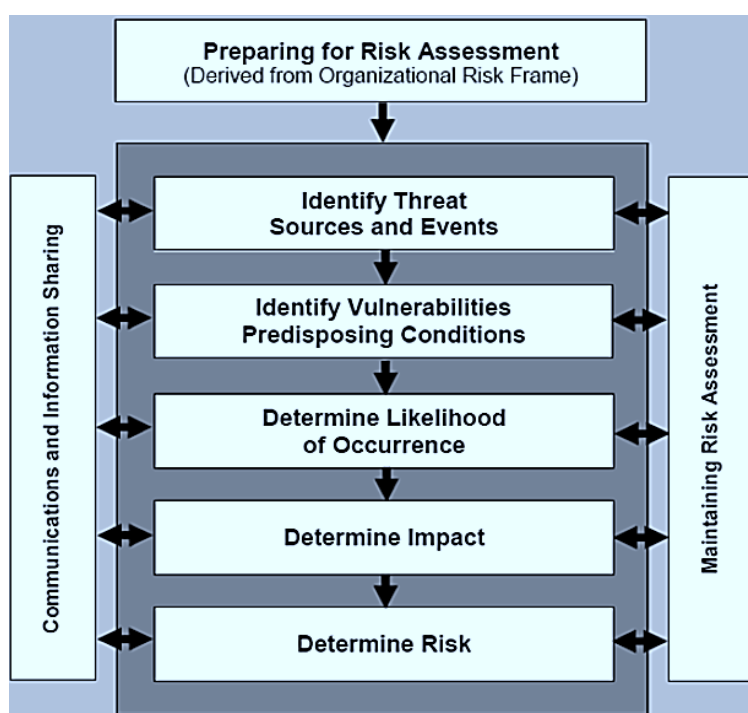


Рис. 3.3. Процес оцінювання ризиків відповідно до методології NIST SP 800-30

Джерело: [1-9, 11-26, 32-48, 60-65]

Методологія NIST SP 800-30 є однією з найдетальніших і найструктурованіших моделей оцінювання ризиків у сфері інформаційної безпеки, що поєднує аналітичну точність з практичною орієнтацією на прийняття рішень. Її головна мета полягає в тому, щоб допомогти організаціям виявити, оцінити та визначити пріоритетність ризиків для інформаційних систем, а також вибрати ефективні заходи контролю з урахуванням витрат, критичності ресурсів і бізнес-цілей. Вона базується на інтегрованій структурі управління ризиками — Risk Management Framework

(RMF), яка охоплює весь життєвий цикл інформаційної системи — від розроблення до експлуатації й утилізації.

Перший етап — підготовка до оцінювання ризику (Prepare Stage) — передбачає визначення цілей, масштабів, контексту і критеріїв прийнятності ризику. На цьому етапі ідентифікуються активи, які потребують захисту, визначаються межі системи, ролі та відповідальність учасників, а також формується команда експертів. Особливу увагу приділено класифікації інформації та визначенню її рівня впливу (impact level) відповідно до категорій: низький, середній або високий. Також відбувається аналіз нормативно-правових вимог, політик безпеки та зовнішнього середовища, у якому функціонує система.

Другий етап — виконання оцінки ризиків (Conduct Stage) — є центральним у методології. Він включає п'ять основних кроків:

1. Ідентифікацію загроз — визначення потенційних джерел небезпеки, серед яких можуть бути природні події, технічні відмови, внутрішні або зовнішні зловмисники.
2. Визначення вразливостей — виявлення слабких місць у системі, політиках, процедурах або людському факторі, які можуть бути використані загрозами.
3. Оцінювання ймовірності реалізації загроз — визначення того, наскільки вірогідно, що конкретна загроза скористається вразливістю, з урахуванням існуючих засобів захисту.
4. Оцінювання наслідків (impact assessment) — визначення потенційного впливу на конфіденційність, цілісність і доступність інформаційних активів.
5. Обчислення рівня ризику (risk determination) — поєднання ймовірності загрози з величиною наслідків для отримання узагальненого показника ризику, що може бути представлений як числове значення або категорія (низький, середній, високий).

Третій етап — звітність і управління ризиками (Report and Manage Stage) — охоплює документування результатів аналізу, визначення пріоритетів для реагування, розроблення планів пом'якшення ризиків (Risk Mitigation Plans) і рекомендацій щодо впровадження відповідних контролів. Результати оцінки використовуються для ухвалення управлінських рішень щодо прийняття, передачі, зменшення або уникнення ризиків. Стандарт передбачає обов'язкове формування Risk Register — реєстру, у якому фіксуються всі виявлені ризики, їхній рівень, власники ризиків, план дій і стан реалізації контрзаходів.

Важливою особливістю NIST SP 800-30 є її кількісно-якісний підхід: ризик оцінюється не лише описово, а й за допомогою числових показників,

що дозволяє проводити порівняння варіантів рішень і моделювати наслідки. Стандарт підтримує використання методу дерева відмов (Fault Tree Analysis), аналізу причин і наслідків (Cause-Effect Analysis), аналізу сценаріїв атак та методу Монте-Карло для симуляцій можливих результатів. Завдяки цьому NIST SP 800-30 забезпечує можливість створення точних моделей загроз і прогнозування потенційних інцидентів.

Крім того, методологія NIST SP 800-30 тісно пов'язана з іншими документами сімейства NIST, зокрема SP 800-37 (Risk Management Framework), SP 800-39 (Enterprise Risk Management) та SP 800-53 (Security and Privacy Controls). Така взаємодія гарантує цілісність процесу управління ризиками на всіх рівнях — від стратегічного планування до операційного контролю. Завдяки своїй гнучкості NIST SP 800-30 може бути застосована як у великих державних структурах, так і в приватних компаніях для оцінювання ризиків у хмарних сервісах, промислових системах керування (ICS/SCADA), критичній інфраструктурі та фінансових технологіях.

Отже, NIST SP 800-30 є не лише технічним документом, а комплексною методологією, що поєднує аналітику, управлінський підхід і практичні інструменти для систематичного виявлення, оцінювання та зниження ризиків інформаційної безпеки. Її застосування сприяє формуванню доказової бази для прийняття рішень, підвищує прозорість процесів безпеки, зміцнює довіру між підрозділами та забезпечує відповідність міжнародним вимогам до кіберзахисту.

FAIR (Factor Analysis of Information Risk)

Третьою важливою методологією є FAIR (Factor Analysis of Information Risk) — модель кількісного аналізу ризиків, що дозволяє перетворювати невизначеність у конкретні фінансові показники. FAIR базується на розкладанні ризику на окремі компоненти: частоту подій, ймовірність успішної атаки, масштаб збитків та їх очікувану вартість. Цей підхід дозволяє визначати очікувані фінансові втрати (Expected Loss), що надає змогу керівництву підприємства порівнювати варіанти інвестицій у безпеку на основі економічної доцільності. На відміну від ISO/IEC 27005 і NIST SP 800-30, методологія FAIR орієнтована на кількісне вимірювання ризику через моделювання, симуляцію Монте-Карло та побудову розподілів імовірності збитків. Вона активно використовується у фінансовому секторі, критичній інфраструктурі та великих корпораціях, де необхідна формалізована економічна оцінка ризику.

Методологія FAIR (Factor Analysis of Information Risk) є першою уніфікованою кількісною моделлю для вимірювання ризиків інформаційної безпеки в грошовому еквіваленті, що дозволяє перейти від якісних суджень до точних, фінансово обґрунтованих рішень. Її основна концепція полягає в

тому, що будь-який ризик можна представити як функцію від частоти подій (frequency) та величини втрат (loss magnitude). FAIR допомагає зрозуміти, наскільки часто можуть відбуватися інциденти безпеки, який потенційний збиток вони можуть спричинити та яку економічну вигоду підприємство може отримати від впровадження певних контрзаходів.

Ключовою особливістю FAIR є ієрархічна структура факторів, яка розкладає ризик на чітко визначені змінні. На верхньому рівні розглядаються дві основні категорії: Loss Event Frequency (LEF) — частота виникнення події втрати, і Loss Magnitude (LM) — величина втрат. Частота подій, своєю чергою, ділиться на Threat Event Frequency (TEF) — частоту появи загрози, і Vulnerability (Vuln) — ймовірність того, що загроза призведе до успішної атаки. Величина втрат поділяється на Primary Loss (PL) — прямі втрати (наприклад, пошкодження даних, зупинка сервісів, витрати на відновлення) та Secondary Loss (SL) — непрямі втрати (репутаційні ризики, юридичні штрафи, зниження довіри клієнтів). Такий поділ дозволяє точно визначати, які саме чинники впливають на ризик і які з них мають пріоритет у мінімізації.

Для кількісного аналізу FAIR використовує статистичні методи моделювання. Найчастіше застосовується метод Монте-Карло, що дозволяє згенерувати тисячі можливих сценаріїв реалізації ризику з урахуванням розподілу ймовірностей для кожної змінної. У результаті отримується крива розподілу очікуваних втрат (Loss Exceedance Curve), яка показує, з якою ймовірністю можуть бути перевищені певні рівні фінансових збитків. Це дає змогу керівництву підприємства ухвалювати рішення на основі прогнозованого впливу на бюджет, а не інтуїтивних оцінок.

FAIR не лише оцінює рівень ризику, а й дозволяє виконувати порівняльний аналіз заходів безпеки. Наприклад, можна порівняти дві альтернативні стратегії — впровадження нової системи шифрування або навчання персоналу — і визначити, яка з них дає більше зниження очікуваних збитків при менших витратах. Це робить FAIR надзвичайно корисним інструментом для CISO (Chief Information Security Officer), фінансових директорів і аналітиків з управління ризиками, оскільки він переводить мову безпеки в мову бізнесу — “гроші, імовірності, наслідки”.

Важливою складовою моделі FAIR є уніфікована термінологія та документована методика розрахунків, що забезпечує узгодженість між підрозділами підприємства. Стандарт передбачає створення Risk Scenarios Library — бібліотеки сценаріїв ризиків, яка містить типові загрози, параметри частоти подій, значення збитків і результати попередніх оцінок. Це полегшує повторне використання даних і підвищує точність майбутніх оцінювань. FAIR також може бути інтегрований із методологіями ISO/IEC

27005 або NIST SP 800-30, виконуючи роль кількісного доповнення до якісного ризик-аналізу.

Сучасні програмні реалізації FAIR включають OpenFAIR Toolkit, RiskLens Platform, Xactium Risk Management та інші рішення, що автоматизують моделювання ризиків і формування звітів для топменеджменту. Ці системи дозволяють швидко перераховувати ризики при зміні параметрів або появи нових загроз, що особливо актуально в умовах динамічних кіберзагроз і регуляторних вимог, таких як DORA чи GDPR.

На рис. 3.4 подано структуру моделі FAIR (Factor Analysis of Information Risk), яка є міжнародним стандартом кількісного аналізу ризиків в інформаційній безпеці та операційній діяльності. Модель побудована на принципі поділу загального ризику (RISK) на дві головні складові: частоту подій втрати (Loss Event Frequency, LEF) та величину втрат (Loss Magnitude, LM). Частота подій втрати відображає, наскільки часто може відбуватися інцидент, і визначається двома основними факторами — частотою загрозливих подій (Threat Event Frequency, TEF) та вразливістю (Vulnerability). TEF, у свою чергу, залежить від частоти контактів (Contact Frequency) між загрозою та активом і ймовірності дії (Probability of Action, PoA) з боку зловмисника або зовнішнього чинника. Ці показники враховують як випадкові, так і навмисні дії, а також рівень мотивації та ресурсів атакуючої сторони. Вразливість (Vulnerability) визначається співвідношенням між здатністю загрози (Threat Capability, TCap) та силою опору (Resistance Strength, RS) — чим вищі можливості зловмисника і нижча стійкість системи, тим більша ймовірність успішної атаки. Друга складова ризику — величина втрат (Loss Magnitude, LM) — складається з первинних втрат (Primary Loss), що включають безпосередні фінансові збитки (наприклад, пошкодження обладнання, витрати на відновлення, втрату даних), і вторинних втрат (Secondary Loss), пов'язаних із непрямими наслідками, такими як репутаційні втрати, штрафи, судові витрати або зниження довіри клієнтів. Вторинні втрати також поділяються на частоту подій вторинних втрат (Secondary Loss Event Frequency) та величину вторинних втрат (Secondary Loss Magnitude).

Таким чином, модель FAIR дозволяє кількісно оцінити ризик, визначивши його як функцію від частоти подій і очікуваних втрат. Її застосування забезпечує можливість точного прогнозування фінансових наслідків кіберінцидентів, порівняння вартості контрзаходів і визначення економічно обґрунтованих рішень щодо безпеки. FAIR перетворює абстрактні поняття ризику на конкретні числові показники, що робить її

ключовим інструментом для стратегічного управління інформаційною безпекою в сучасних підприємствах.



Рис. 3.4. Модель кількісного аналізу ризиків FAIR (Factor Analysis of Information Risk)

Джерело: [1-9, 11-26, 32-48, 60-65]

Таким чином, методологія FAIR перетворює управління ризиками інформаційної безпеки на кількісно обґрунтований процес, який забезпечує вимірюваність, порівнюваність і економічну доцільність рішень. Вона допомагає підприємствам не лише усвідомлювати рівень ризику, але й оцінювати його у фінансовому вираженні, що дозволяє інтегрувати безпеку в загальну бізнес-стратегію та підвищити ефективність інвестицій у кіберзахист.

Отже, ISO/IEC 27005 забезпечує стратегічну та управлінську основу ризик-менеджменту, NIST SP 800-30 формує методику системного аналізу загроз і вразливостей, а FAIR надає кількісні інструменти для фінансової оцінки ризиків. У комплексі ці три підходи створюють узгоджену методологічну базу, яка дозволяє підприємствам різного масштабу формувати зрілу систему управління інформаційною безпекою, що поєднує аналітичну точність, гнучкість і практичну результативність.

3.2. МЕТОДИ КІЛЬКІСНОЇ ТА ЯКІСНОЇ ОЦІНКИ РИЗИКІВ

Методи кількісної та якісної оцінки ризиків є важливою складовою процесу управління ризиками в інформаційній безпеці, оскільки саме вони дозволяють визначити рівень загроз, оцінити їхній вплив на активи підприємства та обґрунтувати необхідність впровадження заходів захисту. Залежно від доступності даних, складності системи та цілей аналізу застосовуються якісні або кількісні підходи, а в більшості випадків — їх комбінація.

Якісні методи оцінювання

Якісні методи оцінювання базуються на експертних судженнях і використовують описові категорії на кшталт «високий», «середній» або «низький» рівень ризику. Вони ефективні тоді, коли точних статистичних даних недостатньо або коли потрібно швидко оцінити загальний стан безпеки. Найпоширенішими якісними методами є SWOT-аналіз, що дозволяє визначити сильні й слабкі сторони системи, можливості та загрози; GAP-аналіз, який допомагає виявити розрив між поточним станом безпеки й вимогами стандартів ISO/IEC 27001; FMEA (Failure Mode and Effects Analysis), орієнтований на пошук можливих відмов, їхніх причин та наслідків; а також Delphi-метод, що базується на колективній експертній оцінці через серію опитувань для досягнення узгодженої думки. Одним із найпростіших і водночас найуживаніших є метод матриці ризику, який поєднує ймовірність виникнення події з масштабом її наслідків та дозволяє візуально визначити пріоритети реагування. Перевагами якісних методів є простота, швидкість і доступність, однак вони мають суттєвий недолік — суб'єктивність оцінок, що ускладнює точне порівняння результатів і визначення фінансових втрат.

Кількісні методи оцінки ризиків використовують математичні та статистичні моделі, які дозволяють отримати об'єктивні числові показники рівня ризику, часто у фінансовому вираженні. Одним із базових підходів є метод очікуваних втрат (ALE — Annual Loss Expectancy), у якому ризик розраховується за формулою $ALE = SLE \times ARO$, де SLE — очікувана вартість збитків від одного інциденту, а ARO — середня кількість таких подій за рік. Значного поширення набули ймовірнісні моделі, зокрема метод Монте-Карло, який передбачає багаторазове моделювання випадкових сценаріїв розвитку подій для визначення діапазону можливих втрат. Байєсівський аналіз ризику дозволяє коригувати ймовірності з урахуванням нових даних, а метод дерева відмов (FTA — Fault Tree Analysis)

застосовується для моделювання взаємозв'язків між подіями, що можуть призвести до інциденту. Серед сучасних інструментів особливе місце посідає модель FAIR (Factor Analysis of Information Risk), яка визначає ризик як добуток частоти подій втрати (Loss Event Frequency) на величину втрат (Loss Magnitude) та дозволяє оцінювати фінансовий вплив кіберінцидентів із використанням статистичних симуляцій. Ці методи забезпечують більшу точність і дають змогу здійснювати економічно обґрунтоване планування заходів безпеки, проте потребують значних ресурсів, надійних даних і високої кваліфікації аналітиків.

Основні кількісні методи:

Метод очікуваних втрат (ALE — Annual Loss Expectancy)

Метод очікуваних втрат (ALE — Annual Loss Expectancy) є одним із найпоширеніших кількісних методів оцінювання ризиків у сфері інформаційної безпеки, оскільки дозволяє перевести можливі загрози в конкретні фінансові показники. Його головна ідея полягає у визначенні того, яких середньорічних втрат може зазнати підприємство внаслідок реалізації певного ризику, тобто наскільки реальною є шкода від інцидентів безпеки у грошовому еквіваленті. Цей метод використовується для прийняття управлінських рішень щодо доцільності інвестицій у захисні заходи, вибору пріоритетів безпеки та визначення економічної ефективності впровадження контрзаходів.

Оцінювання за методом ALE здійснюється поетапно. Спочатку визначаються всі інформаційні активи підприємства, їхня вартість і критичність для бізнесу, тобто наскільки важливою є кожна система або ресурс для безперервності діяльності. Потім ідентифікуються загрози, що можуть вплинути на ці активи, і відповідні вразливості, які можуть сприяти їх реалізації. Далі оцінюються можливі наслідки від кожної потенційної події — це може бути втрата даних, простої системи, витрати на відновлення або збитки, пов'язані з репутаційними ризиками. На основі цих оцінок визначається середня сума збитків, яку підприємство зазнає під час одного інциденту, а також частота, з якою такі події можуть відбуватися протягом року. Комбінація цих параметрів дозволяє обчислити очікувану річну величину втрат для конкретного виду ризику.

Результати аналізу за методом ALE є практично орієнтованими: отримане значення дозволяє порівняти можливі збитки з витратами на впровадження заходів безпеки. Наприклад, якщо середньорічні очікувані втрати від атаки на сервер становлять 50 тисяч гривень, а встановлення системи захисту коштує 30 тисяч, то інвестиція є економічно виправданою, адже потенційна вигода від зменшення ризику перевищує витрати. Таким

чином, ALE допомагає ухвалювати зважені рішення, орієнтуючись не лише на технічні, а й на фінансові критерії.

Метод очікуваних втрат має низку переваг. Він є простим у застосуванні, не потребує складних розрахунків або спеціального програмного забезпечення, надає зрозумілі результати у грошовому вимірі та легко інтегрується в загальну систему ризик-менеджменту. Завдяки цьому ALE широко використовується як у великих корпораціях, так і у середніх підприємствах для визначення пріоритетності інвестицій у безпеку. Крім того, метод дозволяє проводити порівняльний аналіз між різними активами або підрозділами підприємства, визначаючи, у яких випадках ризики мають найбільший економічний вплив.

На рис. 3.5 зображено послідовний процес оцінювання ризиків на основі методу очікуваних втрат, який дає змогу кількісно визначити потенційні фінансові наслідки реалізації загроз для підприємства. Процес розпочинається з ідентифікації ризиків, коли визначаються активи, на які можуть впливати потенційні загрози, та оцінюється їхня критичність для бізнесу. Далі відбувається визначення річної частоти виникнення подій (Annual Rate of Occurrence), тобто кількості разів, коли подібний інцидент може статися протягом року. На цьому етапі також обчислюється очікуваний розмір збитків від однієї події (Single Loss Expectancy), що відображає середній фінансовий ефект від кожного інциденту. Наступний етап — пріоритизація ризиків, у межах якої ризики ранжуються за рівнем впливу та ймовірністю виникнення, що дозволяє спрямовувати ресурси на найбільш критичні з них. Після цього здійснюється розподіл ресурсів (Allocation of Resource) для розроблення та впровадження заходів зниження ризику. Завершальним етапом є моніторинг і перегляд результатів, які забезпечують постійну актуальність оцінки ризику та відповідність управлінських рішень реальним умовам діяльності підприємства.

Загалом діаграма демонструє логічну структуру методу ALE, у якій кожен етап пов'язаний із попереднім, утворюючи замкнутий цикл управління ризиками. Основною метою є перехід від якісного опису загроз до кількісного вимірювання потенційних втрат, що дозволяє приймати економічно обґрунтовані рішення щодо доцільності інвестування у заходи інформаційної безпеки.

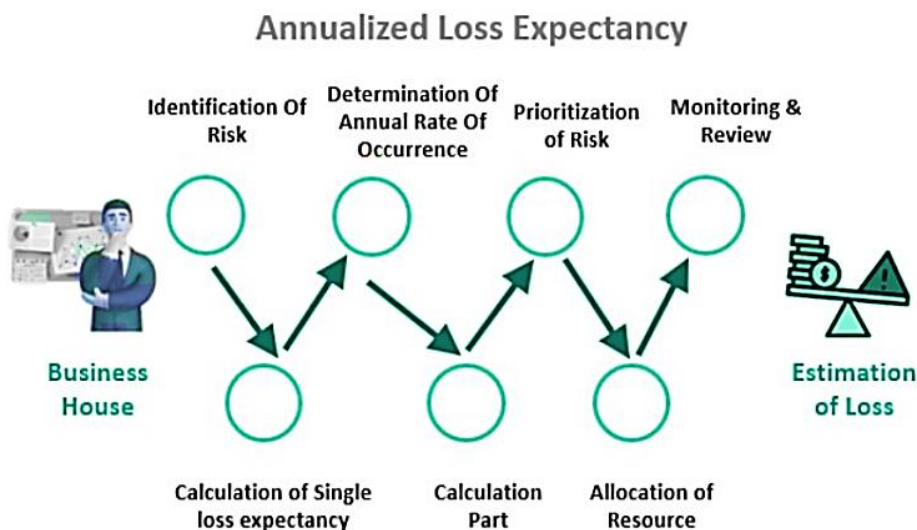


Рис. 3.5. Процес оцінювання ризиків за методом очікуваних втрат (ALE — Annualized Loss Expectancy)

Джерело: [1-9, 11-26, 32-48, 60-65]

Однак цей підхід має і певні обмеження. Точність оцінки значною мірою залежить від достовірності вихідних даних, зокрема від наявності статистики інцидентів, історії порушень або експертних оцінок. Метод переважно зосереджений на прямих фінансових збитках і не враховує непрямих втрат, таких як репутаційні наслідки, юридичні санкції чи втрату довіри клієнтів. Крім того, він не враховує динаміку сучасних кіберзагроз, які змінюються швидко, і не завжди відображає взаємозалежність між різними ризиками.

Попри ці недоліки, метод очікуваних втрат залишається одним із найефективніших і найпрактичніших інструментів кількісної оцінки ризику в інформаційній безпеці. Його головна цінність полягає у можливості перетворити абстрактні уявлення про ризик у конкретні фінансові показники, що дозволяє обґрунтувати бюджет на безпеку, оцінити ефективність захисних інвестицій та встановити економічно раціональні межі прийнятного ризику. Завдяки цьому ALE широко використовується в межах міжнародних стандартів, таких як ISO/IEC 27005 та NIST SP 800-30, і залишається базовим інструментом для стратегічного управління ризиками на підприємстві.

Метод Монте-Карло

Метод Монте-Карло — використовує статистичне моделювання для прогнозування ймовірного розподілу втрат. Проводиться багаторазова симуляція випадкових подій, що дозволяє отримати криву розподілу ризику. Метод Монте-Карло є одним із найпотужніших і найгнучкіших

кількісних підходів до оцінювання ризиків, який широко застосовується в інформаційній безпеці, фінансовому менеджменті та інженерії для прогнозування можливих наслідків невизначених подій. Його сутність полягає у використанні статистичного моделювання, що передбачає багаторазове проведення симуляцій випадкових подій із заданими параметрами. Такий підхід дозволяє побудувати повну картину можливих сценаріїв розвитку подій, визначити розподіл ризику та оцінити ймовірність виникнення різних рівнів втрат.

Основна ідея методу Монте-Карло полягає в тому, що складні системи з великою кількістю змінних і випадкових факторів можна описати через численні випадкові випробування, під час яких кожна змінна приймає випадкові значення в межах певного інтервалу або розподілу ймовірностей. Для оцінки ризику в інформаційній безпеці визначаються ключові параметри, що впливають на величину втрат — наприклад, частота атак, ймовірність успішного порушення безпеки, час простою системи, фінансовий збиток від кожного інциденту. Далі для кожного параметра задається математична модель — нормальний, експоненційний, логнормальний або інший розподіл, який відображає його поведінку в реальних умовах.

На практиці процес оцінки ризику за методом Монте-Карло відбувається у кілька послідовних етапів. Спочатку формується модель ризику, що включає всі релевантні фактори та взаємозв'язки між ними. Потім для кожного фактора встановлюються можливі діапазони значень та функції розподілу. Далі за допомогою програмних засобів, таких як @Risk, Crystal Ball або MATLAB, запускається велика кількість симуляцій — від кількох тисяч до мільйонів повторів. У кожній ітерації програма випадковим чином генерує нові значення для кожного параметра згідно з визначеним розподілом і обчислює підсумковий результат — наприклад, величину фінансових втрат від кіберінциденту. Отримані результати об'єднуються в сукупність, що утворює криву розподілу ризику, яка показує ймовірність перевищення певного рівня збитків.

Крива розподілу, отримана в результаті симуляції, дозволяє визначити не лише середнє очікуване значення втрат, а й ймовірність екстремальних подій — тобто ситуацій, коли збитки можуть бути набагато більшими, ніж середні. Це дає можливість підприємству оцінити не лише типові, а й критичні сценарії, що мають низьку ймовірність, але високий потенційний вплив. Таким чином, метод Монте-Карло надає повну картину ризикового профілю системи, що дозволяє ухвалювати зважені управлінські рішення, планувати резерви безпеки та розробляти стратегії реагування на різні варіанти розвитку подій.

Однією з головних переваг цього методу є його здатність працювати з високим рівнем невизначеності. У сфері інформаційної безпеки часто бракує точних історичних даних про частоту кібератак чи вартість інцидентів, тому традиційні методи оцінки ризиків можуть бути недостатньо точними. Метод Монте-Карло компенсує це, дозволяючи враховувати широкий спектр можливих значень і моделювати навіть рідкісні події. Крім того, він забезпечує можливість оцінити вплив одночасної дії кількох чинників ризику, які можуть мати нелінійну взаємозалежність.

Метод має і певні обмеження. Його точність на пряму залежить від правильності вибору вхідних розподілів і параметрів, а також від кількості проведених симуляцій — чим більше повторів, тим надійнішими є результати, але тим більшими стають обчислювальні витрати. Крім того, для побудови моделі ризику необхідні глибокі знання предметної області та наявність якісних статистичних даних. Проте, попри складність реалізації, метод Монте-Карло забезпечує виняткову гнучкість і глибину аналізу, роблячи його одним із найцінніших інструментів кількісного ризик-менеджменту.

У підсумку, метод Монте-Карло дає змогу перетворити оцінку ризику на науково обґрунтований процес, що враховує невизначеність, варіативність та взаємодію численних факторів. Його застосування в інформаційній безпеці дозволяє прогнозувати фінансові наслідки кіберінцидентів, порівнювати альтернативні заходи захисту, визначати ймовірність критичних втрат і формувати оптимальні стратегії управління ризиками. Саме тому цей метод є невід'ємною частиною сучасних підходів до кількісного аналізу ризиків у рамках стандартів ISO/IEC 27005, NIST SP 800-30 і FAIR.

Байєсівський аналіз ризиків

Байєсівський аналіз ризиків — базується на теоремі Байєса для уточнення ймовірностей подій з урахуванням нових даних. Цей метод особливо ефективний у динамічних середовищах, де умови ризику змінюються.

Байєсівський аналіз ризиків є одним із найсучасніших і найгнучкіших методів кількісного оцінювання ризиків, який поєднує математичну точність із можливістю адаптації до змінного середовища. Його основою є теорема Байєса, що дозволяє уточнювати ймовірність настання певної події на основі нових доказів або даних. Іншими словами, цей метод надає змогу постійно оновлювати оцінку ризику, виходячи не лише з попереднього досвіду, а й з поточної ситуації. Саме тому Байєсівський підхід особливо ефективний у динамічних умовах — наприклад, у сфері кібербезпеки, де

рівень загроз, технології атак і поведінка зловмисників змінюються надзвичайно швидко.

Суть Байєсівського аналізу полягає в тому, що ризик не розглядається як фіксована величина, а як ймовірнісний процес, який еволюціонує з накопиченням інформації. Початково аналітик формує так звану апріорну ймовірність — тобто початкове припущення про ризик на основі історичних даних, експертних оцінок або попередніх моделей. Коли надходять нові відомості — наприклад, виявлено нову вразливість у системі чи зафіксовано спроби вторгнення, — ці дані використовуються для оновлення оцінки ризику, формуючи апостеріорну ймовірність. Таким чином, кожне нове спостереження або інцидент не просто фіксується, а безпосередньо впливає на зміну рівня ризику, роблячи модель більш точною та актуальною.

Процес Байєсівського аналізу ризиків зазвичай складається з кількох етапів. На першому етапі визначається система показників ризику: тип загрози, уразливість, можливий вплив, частота виникнення подій. Далі формується початкова ймовірнісна модель, у якій кожен параметр має власну розподілену ймовірність. На другому етапі відбувається спостереження або збір нових даних — наприклад, з журналів подій SIEM, аналітики SOC або з систем моніторингу безпеки. Отримана інформація використовується для перерахунку ймовірностей на основі теореми Байєса, що дозволяє зменшити невизначеність і наблизити оцінку ризику до реального стану системи.

Однією з головних переваг цього методу є його адаптивність. На відміну від класичних статистичних моделей, які ґрунтуються на фіксованих даних і не оновлюються автоматично, Байєсівський аналіз реагує на зміну умов у режимі реального часу. Наприклад, якщо певна загроза виявляється рідше, ніж очікувалося, або нові системи захисту знижують ймовірність успішної атаки, модель одразу коригує свої розрахунки. Це робить метод надзвичайно ефективним для систем, що працюють у середовищах із високою динамікою ризиків — таких, як корпоративні мережі, хмарні сервіси, мобільні платформи чи інфраструктури критичної важливості.

Ще однією перевагою Байєсівського аналізу є можливість інтеграції суб'єктивних експертних оцінок із об'єктивними статистичними даними. Наприклад, коли відсутня достовірна статистика щодо частоти певних атак, можна використати оцінки фахівців безпеки як апріорну основу, а потім поступово вдосконалювати її у міру накопичення реальних даних. Це дозволяє поєднати аналітичний досвід з автоматизованими методами обробки інформації, що особливо важливо для систем раннього попередження про кіберінциденти.

Байєсівський підхід також зручний для побудови ієрархічних моделей ризику, коли складні системи розглядаються як сукупність підсистем із власними ймовірностями загроз і наслідків. Така структура дозволяє враховувати взаємозв'язки між компонентами безпеки — наприклад, як збої в одному сегменті мережі можуть підвищити ризик атак у суміжних сегментах. За допомогою Байєсівських мереж можна моделювати каскадні ефекти, прогнозувати ймовірність критичних відмов і визначати найуразливіші точки системи.

Попри свої численні переваги, метод має певні обмеження. Для його ефективного застосування необхідна велика кількість достовірних даних і якісно побудовані моделі розподілу ймовірностей. У випадках, коли інформація є неповною або суперечливою, результати можуть бути наближені. Крім того, розрахунки вимагають значних обчислювальних ресурсів, особливо при моделюванні складних багаторівневих систем.

У сучасних умовах Байєсівський аналіз ризиків активно використовується в рамках стандартів ISO/IEC 27005, NIST SP 800-30 та FAIR, зокрема для побудови прогнозних моделей кіберризиків, оцінки ефективності заходів безпеки й динамічного оновлення політик реагування. Його застосування дозволяє підприємствам підтримувати актуальність оцінки ризиків, швидко реагувати на зміни у кіберсередовищі та приймати обґрунтовані рішення щодо розподілу ресурсів безпеки. Завдяки здатності враховувати як історичні, так і нові дані, Байєсівський аналіз є потужним інструментом побудови інтелектуальної, адаптивної системи управління ризиками, здатної передбачати ймовірність майбутніх інцидентів і мінімізувати їхній вплив на інформаційні активи підприємства.

Метод дерева відмов (FTA — Fault Tree Analysis)

Метод дерева відмов (FTA — Fault Tree Analysis) — графічний підхід, який моделює логічні зв'язки між причинами відмов і кінцевими подіями. Дозволяє оцінити ймовірність комплексних інцидентів.

Метод дерева відмов (FTA — Fault Tree Analysis) є одним із найефективніших і водночас наочних підходів до кількісного аналізу ризиків, який широко використовується в інформаційній безпеці, технічній діагностиці та управлінні критичними системами. Його суть полягає у побудові ієрархічної логічної моделі, яка показує, як поєднання різних причин, збоїв або вразливостей може призвести до виникнення певної небажаної події — наприклад, до втрати даних, відмови системи чи порушення конфіденційності інформації. Такий підхід дає змогу не лише візуалізувати причинно-наслідкові зв'язки, а й кількісно оцінити ймовірність настання складних інцидентів, що виникають через комбінацію декількох факторів.

Процес аналізу за методом ФТА починається з визначення верхньої події (top event) — тобто головного інциденту, якого необхідно уникнути або ймовірність якого потрібно оцінити. Це може бути, наприклад, несанкціонований доступ до бази даних, відмова сервера або порушення цілісності інформації. Після цього виконується декомпозиція події, під час якої встановлюються всі можливі безпосередні причини, що можуть призвести до цього інциденту. Кожна з таких причин, у свою чергу, розкладається на ще більш детальні фактори — технічні, програмні, людські чи організаційні. У результаті формується розгалужена структура — “дерево”, у якому верхній вузол представляє головну подію, а нижні — її складові причини.

В основі ФТА лежить логічне моделювання із використанням спеціальних логічних операторів, які показують, як взаємодіють між собою різні фактори. Наприклад, елемент AND (І) позначає, що для виникнення верхньої події необхідна одночасна наявність кількох умов (наприклад, збій у системі контролю доступу та відмова резервного каналу зв'язку), тоді як оператор OR (АБО) вказує, що достатньо виникнення лише однієї з причин, щоб відбулася відмова. Такий підхід дозволяє формалізувати навіть дуже складні сценарії з багатьма взаємопов'язаними чинниками.

На наступному етапі проводиться кількісний аналіз дерева відмов, який передбачає визначення ймовірностей для кожної базової події (наприклад, відмова обладнання, людська помилка, збої ПЗ). Ці ймовірності можуть бути отримані з історичних даних, статистичних звітів або експертних оцінок. Далі, використовуючи правила логічних операцій, розраховується сумарна ймовірність виникнення верхньої події. У результаті аналітик отримує числове значення ризику, яке відображає, наскільки ймовірно, що певна критична подія відбудеться протягом заданого періоду.

Однією з найцінніших особливостей методу ФТА є його можливість визначення критичних елементів системи. За допомогою дерева відмов можна легко побачити, які саме вузли або компоненти мають найбільший вплив на загальний ризик, і, відповідно, які з них потребують першочергового вдосконалення або додаткових засобів контролю. Наприклад, якщо ймовірність відмови внаслідок помилки оператора виявляється більшою, ніж через технічний збій, це сигналізує про необхідність підвищення кваліфікації персоналу або вдосконалення процедур доступу.

Метод дерева відмов має низку очевидних переваг. По-перше, він забезпечує високу наочність, що полегшує сприйняття навіть складних ризикових сценаріїв керівництвом і не технічними спеціалістами. По-друге,

він дозволяє системно оцінювати комбінації подій, які в сукупності можуть призвести до серйозного інциденту, тоді як ізольований аналіз окремих загроз часто не показує повної картини. По-третє, FTA добре інтегрується з іншими методами аналізу, такими як FMEA чи HAZOP, утворюючи єдину аналітичну основу для комплексного управління ризиками.

Водночас метод має і певні обмеження. Побудова дерева відмов вимагає глибокого розуміння структури системи, її процесів та потенційних взаємозв'язків між компонентами. Для складних ІТ-інфраструктур дерево може мати сотні вузлів, що ускладнює його підтримку та оновлення. Крім того, метод не завжди враховує часові аспекти — наприклад, послідовність подій або затримки у реакції системи. Проте в поєднанні з динамічними моделями ризику та статистичними підходами FTA забезпечує високий рівень точності й глибини аналізу.

У сфері інформаційної безпеки метод дерева відмов застосовується для оцінки надійності систем захисту, аналізу сценаріїв збоїв у мережах, моделювання наслідків кіберінцидентів та оптимізації архітектури безпеки. Він дає змогу побудувати детальну карту залежностей між загрозами, вразливостями та подіями, що є надзвичайно цінним для створення систем раннього виявлення атак і планів відновлення після інцидентів.

На рис. 3.6 представлено базову логічну модель методу дерева відмов (FTA), яка демонструє, як поєднання елементарних подій може призвести до виникнення верхньої (основної) події — Event. Діаграма побудована у вигляді ієрархічної структури, де кожен рівень відображає причинно-наслідкові зв'язки між подіями, а логічні оператори визначають умови їх взаємодії. У верхній частині схеми розташована головна подія, що є об'єктом аналізу — наприклад, відмова системи, збій сервісу чи інцидент безпеки. Нижче показано три типи логічних елементів, які задають правила формування вихідної події на основі вхідних подій. Оператор OR (АБО) означає, що вихідна подія настане, якщо відбудеться хоча б одна з вхідних подій. Оператор AND (І) визначає, що вихідна подія виникне лише у випадку, коли спрацюють усі вхідні події одночасно. Оператор XOR (Виключне АБО) вказує, що вихідна подія відбудеться, якщо реалізується лише одна з альтернативних вхідних подій, але не обидві одночасно.

У нижній частині дерева зображені базові події (Basic events) — це початкові, найпростіші інциденти або відмови компонентів, які ініціюють розвиток небажаного сценарію. Кожна з них може мати власну ймовірність виникнення, яка надалі використовується для розрахунку загальної ймовірності настання верхньої події. Таким чином, діаграма ілюструє фундаментальний принцип методу FTA: через логічне комбінування базових подій у вузли AND, OR і XOR можна моделювати складні

причинно-наслідкові ланцюги відмов. Цей підхід забезпечує системне бачення джерел ризику, дозволяє оцінити їхній внесок у загальну відмову системи й визначити найуразливіші компоненти для підвищення надійності або безпеки інформаційної інфраструктури.

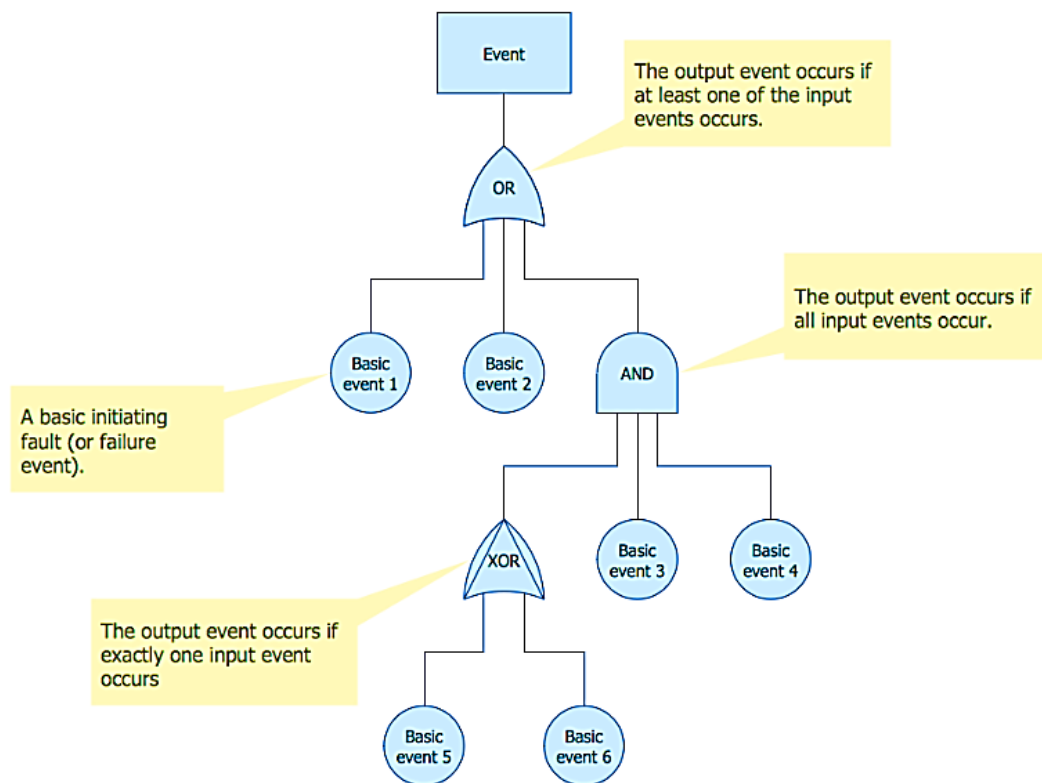


Рис. 3.6. Логічна структура методу дерева відмов (Fault Tree Analysis, FTA)

Джерело: [1-9, 11-26, 32-48, 60-65]

Таким чином, метод дерева відмов (FTA) є універсальним інструментом кількісного аналізу ризиків, який поєднує логічну строгість, структурну наочність і практичну цінність. Його використання дозволяє не лише виявити найбільш критичні точки у системі безпеки, а й розробити пріоритетні заходи для запобігання інцидентам, мінімізації втрат і підвищення загальної стійкості інформаційної інфраструктури підприємства.

FAIR (Factor Analysis of Information Risk)

FAIR (Factor Analysis of Information Risk) — сучасна кількісна модель, яка розкладає ризик на частоту подій втрати (*Loss Event Frequency, LEF*) та величину втрат (*Loss Magnitude, LM*). За допомогою статистичних методів і симуляцій визначається очікувана вартість збитків, що дозволяє порівнювати альтернативні заходи безпеки.

Модель FAIR (Factor Analysis of Information Risk) є сучасним, формалізованим підходом до кількісної оцінки ризиків в інформаційній безпеці, який дозволяє переводити абстрактні загрози у вимірювані фінансові показники. Її головна мета полягає у тому, щоб надати об'єктивну, аналітично обґрунтовану оцінку рівня ризику, яка може бути використана для прийняття управлінських і фінансових рішень. На відміну від традиційних якісних підходів, що ґрунтуються на суб'єктивних оцінках експертів, модель FAIR використовує статистичні методи, симуляції й аналітичне моделювання, дозволяючи точно оцінити очікувані збитки від реалізації кіберзагроз.

Сутність FAIR полягає у розкладанні ризику на дві ключові складові — частоту подій втрати (Loss Event Frequency, LEF) та величину втрат (Loss Magnitude, LM). Частота подій втрати відображає, як часто може відбутися інцидент, і залежить від кількох факторів: інтенсивності дій зловмисників, рівня їхньої мотивації, наявності вразливостей та здатності системи чинити опір атакам. Величина втрат, у свою чергу, показує масштаб збитків у разі реалізації події та включає як прямі фінансові втрати (наприклад, витрати на відновлення, штрафи, втрату даних), так і непрямі, пов'язані з репутаційними наслідками, судовими витратами або зниженням довіри клієнтів.

Ключовою особливістю моделі FAIR є її ієрархічна структура, яка дозволяє деталізувати ризик до рівня окремих складових і точно оцінити вплив кожного з них. Наприклад, частота подій втрати (LEF) розраховується на основі двох параметрів: частоти загрозливих подій (Threat Event Frequency, TEF) і вразливості системи (Vulnerability). TEF описує, як часто загрози контактують із активом (наприклад, скільки разів на рік відбуваються спроби зламу), тоді як вразливість показує ймовірність того, що ці загрози будуть успішними. Вразливість визначається співвідношенням між можливостями загрози (Threat Capability) і силою опору (Resistance Strength). Якщо рівень можливостей зловмисника перевищує стійкість системи, ймовірність успіху атаки зростає.

Величина втрат (LM) у FAIR розділяється на первинні втрати (Primary Loss) — тобто прямі витрати підприємства внаслідок інциденту, та вторинні втрати (Secondary Loss), які відображають побічні економічні наслідки, наприклад, зниження вартості акцій, втрату клієнтів або штрафи від регуляторів. Вторинні втрати оцінюються за допомогою параметрів частоти вторинних подій (Secondary Event Frequency) і величини вторинних втрат (Secondary Loss Magnitude), що дає змогу визначити їхній очікуваний фінансовий ефект. Такий поділ дозволяє враховувати не лише прямий

збиток, а й довгострокові економічні наслідки, які часто виявляються набагато значнішими.

На практиці модель FAIR реалізується через імітаційне моделювання, найчастіше з використанням методу Монте-Карло. Після визначення всіх вихідних параметрів система генерує тисячі можливих сценаріїв розвитку подій, кожен з яких має свої варіації частоти інцидентів і розміру втрат. У результаті отримується розподіл імовірностей потенційних збитків, що дозволяє побачити не лише середнє очікуване значення втрат, а й ймовірність екстремальних подій із катастрофічними наслідками. Такий підхід дає змогу ухвалювати обґрунтовані рішення щодо того, які ризики є прийнятними, а які потребують негайного реагування.

Важливою перевагою FAIR є те, що вона дозволяє зіставляти вартість контрзаходів із потенційними збитками, тобто проводити аналіз економічної ефективності заходів безпеки. Наприклад, якщо модель показує, що впровадження системи шифрування зменшує очікувані збитки на 500 тисяч гривень при витратах у 200 тисяч, то таке рішення є економічно виправданим. Таким чином, FAIR забезпечує не лише аналітичну оцінку ризику, а й створює основу для фінансового планування в галузі інформаційної безпеки.

Ще однією перевагою FAIR є її універсальність і сумісність із міжнародними стандартами. Модель може бути інтегрована в системи управління ризиками, побудовані на основі ISO/IEC 27005 або NIST SP 800-30, забезпечуючи поглиблений кількісний аналіз. Вона також відповідає вимогам бізнес-аналітики, оскільки результати можна представити у формі зрозумілих звітів, графіків розподілу втрат або діаграм чутливості, що полегшує їхнє сприйняття керівництвом.

Попри свої переваги, застосування FAIR потребує наявності якісних вихідних даних і аналітичних інструментів. Без достовірної інформації про частоту загроз і масштаби втрат результати можуть мати велику похибку. Проте навіть за умов обмежених даних модель забезпечує вищу точність порівняно з традиційними експертними оцінками, оскільки враховує ймовірнісний характер ризику та варіативність параметрів.

Отже, FAIR (Factor Analysis of Information Risk) є не просто методом оцінювання ризиків, а цілісною концепцією побудови кількісної моделі інформаційної безпеки, яка поєднує аналітику, статистику й економіку. Вона дозволяє підприємствам зрозуміти, які загрози мають найбільший фінансовий вплив, скільки коштує зниження ризику до прийнятного рівня та які заходи є найбільш ефективними з точки зору витрат і вигоди. Завдяки цьому FAIR вважається одним із найточніших і найпрактичніших інструментів сучасного ризик-менеджменту, що перетворює процес

управління ризиками на економічно обґрунтований і стратегічно спрямований процес підтримки інформаційної стійкості підприємства.

Метод очікуваної корисності (*Expected Utility Theory*)

Метод очікуваної корисності (*Expected Utility Theory*) — застосовується для оцінки ризику з урахуванням уподобань або “толерантності до ризику” керівництва, що допомагає приймати рішення на стратегічному рівні.

Метод очікуваної корисності (*Expected Utility Theory*) є важливим інструментом кількісного аналізу ризиків, який дозволяє враховувати не лише об'єктивні фінансові наслідки, а й ставлення керівництва підприємства до ризику, тобто його “толерантність до ризику”. Цей підхід широко використовується у стратегічному управлінні, фінансовому аналізі та інформаційній безпеці, коли потрібно ухвалити рішення за умов невизначеності, балансуючи між потенційними вигодами й можливими втратами. Основна ідея методу полягає в тому, що люди або організації оцінюють не самі результати подій, а ступінь задоволення чи корисності, який вони приносять. Тому дві події з однаковими фінансовими наслідками можуть мати різну “цінність” для підприємства залежно від його схильності або обережності у ставленні до ризику.

Згідно з методом очікуваної корисності, кожному можливому результату ризикової події призначається певна корисність (*utility*), яка відображає рівень задоволення або вигоди, що її отримує підприємство у випадку реалізації цього результату. Потім ці значення зважуються на ймовірність настання відповідної події, і в результаті отримується очікувана корисність — показник, що характеризує середній рівень “вигоди” з урахуванням ризиків. Керівництво може порівнювати кілька альтернативних стратегій, наприклад, різні варіанти інвестицій у системи безпеки або сценарії реагування на кіберінциденти, і вибирати ту, яка має найбільшу очікувану корисність.

У практичному контексті цей метод допомагає підприємству визначити, який рівень ризику є прийнятним, і наскільки варто інвестувати у захисні заходи. Наприклад, компанія може мати два варіанти дій: залишити систему без змін із ризиком втрати 10 мільйонів гривень у разі атаки або інвестувати 3 мільйони у покращення безпеки, зменшивши ймовірність збитків до мінімуму. Обидва варіанти можуть мати однакове математичне очікування втрат, проте керівництво з низькою толерантністю до ризику надасть перевагу другому варіанту, оскільки він забезпечує більшу передбачуваність і стабільність. Таким чином, метод очікуваної корисності дозволяє враховувати психологічний і стратегічний аспект ризику, який не охоплюється стандартними фінансовими розрахунками.

Одним із ключових понять цього методу є функція корисності, яка описує, як підприємство сприймає зміни у своїх результатах. Для компаній, які є “ризико-нейтральними”, корисність зростає пропорційно до вигоди, тобто кожна додаткова гривня має однакову цінність. Для “ризико-унікальних” організацій приріст корисності від додаткового прибутку зменшується, а потенційні втрати сприймаються набагато болючіше, ніж аналогічні виграші. Натомість “ризико-схильні” організації готові свідомо приймати підвищений ризик заради можливості отримати більшу вигоду. Таким чином, форма функції корисності відображає ставлення компанії до невизначеності й дозволяє адаптувати стратегію управління ризиками відповідно до її корпоративної культури та фінансових можливостей.

Метод очікуваної корисності має важливе значення для стратегічного ризик-менеджменту, оскільки він дозволяє приймати зважені рішення в умовах багатоваріантності та неповної інформації. У сфері інформаційної безпеки цей підхід допомагає визначити, які ризики є прийнятними з погляду бізнесу, а які потребують обов'язкового контролю. Наприклад, підприємство може свідомо погодитися на певний рівень кіберризiku, якщо витрати на повне усунення загрози перевищують очікувану вигоду від такого захисту. Метод також корисний для формування профілю ризику підприємства, тобто поєднання кількісних показників і суб'єктивних уподобань керівництва, що визначає загальну “толерантність до ризику” організації.

Перевагою цього методу є його здатність поєднувати економічний і поведінковий аналіз, що робить його гнучким і практичним у застосуванні. Він не лише дає кількісну оцінку ризику, але й пояснює, чому певне рішення може бути прийняте навіть за наявності більш вигідної, з математичної точки зору, альтернативи. Це особливо актуально для високоризикових сфер, таких як фінансові технології, критична інфраструктура або хмарна безпека, де рішення мають не лише технічні, а й стратегічні наслідки.

Однак метод має і певні обмеження. Для його ефективного використання необхідно правильно визначити функцію корисності, що є складним завданням, оскільки воно потребує знання внутрішніх пріоритетів, фінансового стану та психологічних характеристик керівництва. Крім того, надмірна суб'єктивність у визначенні толерантності до ризику може призвести до спотворення оцінок і прийняття рішень, які не відповідають реальним загрозам.

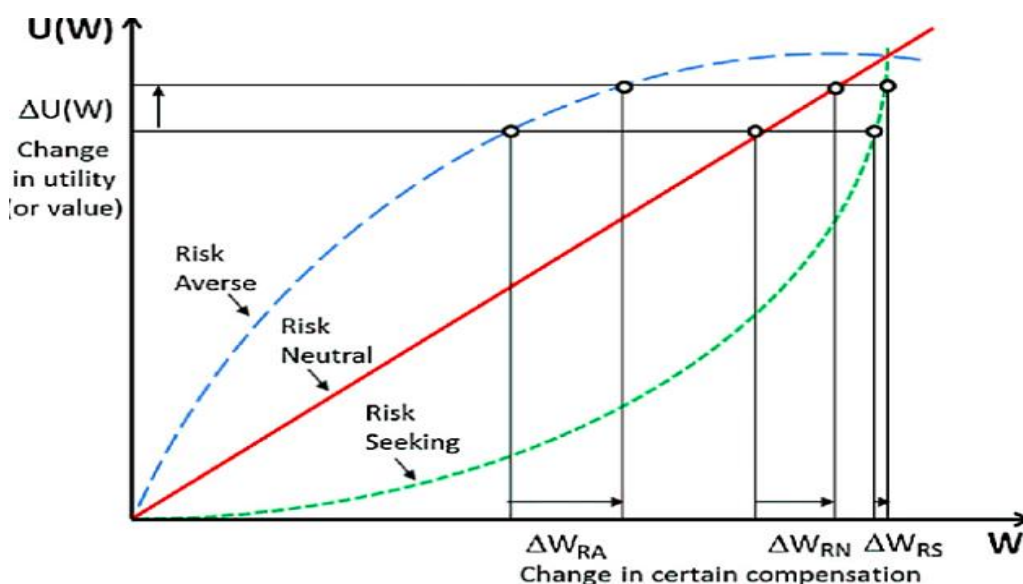


Рис. 3.7. Функції корисності для різних типів ставлення до ризику згідно з методом очікуваної корисності (Expected Utility Theory)

Джерело: [1-9, 11-26, 60-69, 75-82]

На рис. 3.7 зображено графічну інтерпретацію методу очікуваної корисності, яка демонструє, як змінюється корисність залежно від рівня вигоди або доходу. По горизонталі відкладається збільшення матеріальної вигоди, а по вертикалі — зміна у сприйнятті цієї вигоди, тобто рівень задоволення чи корисності, який отримує особа або організація. Такий підхід дозволяє оцінити, як різні суб'єкти сприймають ризик і приймають рішення за умов невизначеності. На графіку подано три типи поведінки щодо ризику. Перша — ризико-унікаюча, позначена увігнутою кривою, що свідчить про те, що кожна наступна одиниця вигоди приносить усе менше задоволення. Для таких осіб або організацій стабільність і впевненість у результаті важливіші, ніж можливість отримати більший, але невизначений прибуток. Друга — ризико-нейтральна, представлена прямою лінією, яка показує, що для таких суб'єктів корисність зростає пропорційно до вигоди, тобто кожна додаткова одиниця прибутку має однакову цінність. Третя — ризико-схильна, відображена опуклою кривою, яка означає, що такі особи готові приймати підвищені ризики заради потенційно більшої вигоди, адже для них додатковий прибуток має зростаючу цінність.

Таким чином, рисунок наочно показує, що управлінські рішення залежать не лише від об'єктивних фінансових результатів, а й від суб'єктивного ставлення до ризику. Метод очікуваної корисності дозволяє зрозуміти, як різні типи поведінки — обережність, нейтральність або схильність до ризику — впливають на вибір стратегії у сфері управління ризиками, фінансів чи інформаційної безпеки. Він допомагає керівництву

підприємства приймати більш зважені рішення, враховуючи не лише математичні показники, а й психологічне сприйняття невизначеності та прагнення до стабільності чи вигоди.

У сучасній практиці управління інформаційною безпекою метод очікуваної корисності активно використовується для розроблення політик ризик-менеджменту, визначення рівня прийнятного ризику (Risk Appetite) та оцінки ефективності інвестицій у кіберзахист. Він узгоджується зі стандартами ISO/IEC 27005, NIST SP 800-30 та підходом FAIR, доповнюючи їх поведінковим аспектом. Завдяки цьому Expected Utility Theory допомагає сформувати більш реалістичну, адаптивну і стратегічно обґрунтовану систему управління ризиками, у якій рішення ґрунтуються не лише на числах, а й на глибокому розумінні того, як організація сприймає невизначеність і готова діяти в умовах ризику.

У сучасній практиці найчастіше використовується комбінований підхід, який поєднує переваги обох методів. Спочатку проводиться якісний аналіз для ідентифікації ключових ризиків і визначення їхньої пріоритетності, а потім найкритичніші з них піддаються кількісному аналізу для точного обчислення ймовірних втрат і витрат на захист. Такий підхід дозволяє одночасно зберегти практичну гнучкість та досягти аналітичної точності. Комбінований підхід забезпечує цілісне бачення ризиків, поєднуючи експертні оцінки з об'єктивними даними, що дозволяє приймати обґрунтовані управлінські рішення. Він дає змогу врахувати не лише технічні та фінансові аспекти, а й організаційні, поведінкові й стратегічні фактори, які впливають на безпеку підприємства. Завдяки цьому управління ризиками стає більш адаптивним до змін зовнішнього середовища та специфіки діяльності організації. Крім того, такий підхід підвищує ефективність розподілу ресурсів, оскільки дає змогу концентрувати зусилля на найважливіших загрозах. Результати якісного та кількісного аналізу взаємно доповнюють одне одного, формуючи єдину основу для побудови комплексної системи захисту інформації. У підсумку комбінований підхід сприяє підвищенню рівня інформаційної стійкості підприємства, забезпечуючи збалансоване поєднання точності, економічності та стратегічної обґрунтованості рішень. Отже, якісні методи забезпечують розуміння контексту та формування загальної картини ризиків, тоді як кількісні дозволяють обґрунтувати рішення на стратегічному й фінансовому рівнях. Їхнє інтегроване використання відповідає вимогам сучасних стандартів ISO/IEC 27005, NIST SP 800-30 і FAIR, створюючи комплексну систему оцінювання ризиків, що поєднує глибину аналітики, адаптивність і практичну ефективність у забезпеченні інформаційної безпеки підприємства.

3.3. GAP-аналіз, SWOT, FMEA, DELPHI-метод, Метод матриці ризику (Risk Matrix) як якісні підходи до оцінки вразливостей

GAP-аналіз

GAP-аналіз — це якісний метод оцінки рівня інформаційної безпеки, який полягає у виявленні прогалів між поточним станом системи захисту та бажаним рівнем, визначеним нормативами, стандартами чи внутрішніми політиками підприємства. Основна мета полягає у виявленні слабких місць, недоліків у впровадженні заходів безпеки та відхилень від найкращих практик. У процесі аналізу визначаються контрольні вимоги (наприклад, ISO/IEC 27001 або NIST CSF), проводиться порівняння фактичного стану системи із заданими критеріями, після чого формується перелік невідповідностей — «GAP-зона». Результати дозволяють не лише побачити, які елементи потребують удосконалення, а й розставити пріоритети у плані усунення вразливостей. Такий підхід допомагає побудувати дорожню карту розвитку системи захисту та інтегрувати результати в загальну стратегію ризик-менеджменту.

GAP-аналіз охоплює кілька етапів, що забезпечують системність і точність результатів. На першому етапі визначається об'єкт оцінювання — це може бути вся інформаційна система підприємства або окремий її компонент, наприклад система управління доступом, мережевий периметр чи політика резервного копіювання. Далі формується еталонна база, тобто набір вимог або стандартів, з якими буде здійснюватися порівняння. Залежно від сфери діяльності підприємства, це можуть бути міжнародні стандарти ISO/IEC 27001, NIST CSF, GDPR, COBIT або галузеві нормативи.

На третьому етапі проводиться збір фактичних даних, що включає аналіз політик, технічних налаштувань, журналів подій, звітів аудиту та результатів перевірок. Після цього здійснюється оцінка відповідності, коли кожен контроль або вимога порівнюється з фактичним станом системи безпеки. Для кожного пункту визначається рівень відповідності: «виконується повністю», «виконується частково» або «не виконується». Ці результати формують основу для створення матриці розривів, у якій фіксуються виявлені невідповідності та оцінюється їхній потенційний вплив на безпеку.

На наступному етапі проводиться аналіз причин виникнення розривів, визначаються фактори, що призвели до недотримання вимог: технічні обмеження, нестача ресурсів, відсутність політик або людський фактор. Для

кожної виявленої прогалини розробляються рекомендації та план дій, який включає конкретні кроки з усунення вразливостей, відповідальних осіб, терміни виконання та необхідні ресурси. Важливо, що GAP-аналіз не обмежується виявленням проблем, а спрямований на формування покрокової дорожньої карти вдосконалення системи інформаційної безпеки.

На рис. 3.8 зображено узагальнену схему процесу GAP-аналізу, який використовується для визначення відхилень між поточним станом системи інформаційної безпеки та цільовими показниками, встановленими нормативами або політиками підприємства. Процес розпочинається з етапу ідентифікації прогалин (Identify Gap), де здійснюється збір фактичних даних про функціонування системи, аудит безпеки, аналіз політик і технічних засобів захисту. Далі відбувається дослідження причин розривів (Research Gap), що включає визначення факторів, які призвели до невідповідності стандартам — таких як недостатня автоматизація, відсутність контролів чи низький рівень обізнаності персоналу. Наступним кроком є ухвалення рішень (Decision), коли на основі отриманих результатів формується перелік заходів для усунення розривів і підвищення рівня зрілості системи захисту. Далі відбувається впровадження змін (Implement Change), яке передбачає реалізацію коригувальних дій, модернізацію інфраструктури, оновлення політик безпеки та проведення навчання персоналу. Завершальний етап — оцінка результатів (Analyze Results) — включає повторну перевірку ефективності проведених заходів і вимірювання досягнутого рівня відповідності вимогам стандартів, наприклад ISO/IEC 27001 або NIST CSF.

Таким чином, представлена схема демонструє безперервний ітеративний цикл GAP-аналізу, у якому результати кожного етапу впливають на подальші рішення. Вона наочно показує, як системний підхід до виявлення, аналізу й усунення прогалин у захисті інформації дозволяє забезпечити поступове вдосконалення політики безпеки підприємства, підвищити рівень зрілості процесів і створити основу для стратегічного управління ризиками.

Gap Analysis Process

6 Steps Flowchart: Identification, Investigation, Decision, Implementation, Analysis, Improvement

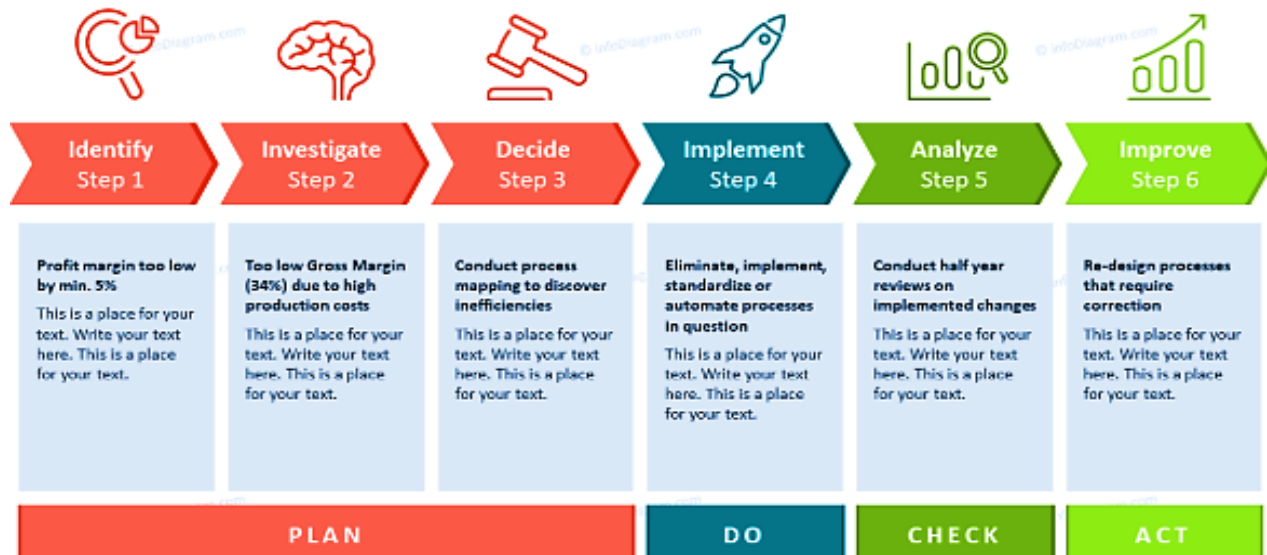


Рис. 3.8. Етапи проведення GAP-аналізу в системі інформаційної безпеки
Джерело: [1-9, 11-26, 60-69, 75-82]

Результатом проведення аналізу є звіт про стан зрілості системи захисту, який містить як опис поточних недоліків, так і рекомендації щодо підвищення рівня безпеки. На його основі підприємство може планувати пріоритети розвитку, оптимізувати використання фінансових і людських ресурсів, а також контролювати прогрес у досягненні відповідності міжнародним стандартам. Таким чином, GAP-аналіз виступає важливим інструментом стратегічного управління кіберризиками, оскільки дозволяє не лише виявити слабкі місця, але й побудувати системний підхід до підвищення інформаційної стійкості підприємства.

SWOT-аналіз

SWOT-аналіз використовується для стратегічної оцінки ризиків, зокрема вразливостей і загроз інформаційній безпеці, через виявлення внутрішніх і зовнішніх факторів впливу. Сильні сторони (Strengths) характеризують поточні переваги системи безпеки — наприклад, наявність політик доступу, SIEM або засобів резервного копіювання. Слабкі сторони (Weaknesses) вказують на внутрішні проблеми — відсутність оновлень, людський фактор або застарілі інструменти. Можливості (Opportunities) описують потенційні напрями розвитку, наприклад впровадження хмарних сервісів безпеки або автоматизацію процесів моніторингу. Загрози (Threats) — це зовнішні фактори, як-от кібератаки, зміни законодавства чи технологічна

конкуренція. Результати SWOT дозволяють виявити критичні зони, де слабкі сторони збігаються із загрозами, що формує основу для пріоритизації дій із посилення захисту.

На рис.3.9 зображено базову структуру SWOT-аналізу — одного з найпоширеніших інструментів стратегічної оцінки ризиків і вразливостей. Матриця складається з чотирьох секторів, які відображають поєднання внутрішніх і зовнішніх факторів, що можуть бути корисними (helpful) або шкідливими (harmful) для підприємства. У верхньому лівому секторі розміщено Strengths (Сильні сторони) — це внутрішні характеристики системи або організації, які створюють переваги: наприклад, ефективна політика інформаційної безпеки, наявність сертифікації ISO/IEC 27001, сучасна інфраструктура чи висококваліфікований персонал. У правому верхньому секторі — Weaknesses (Слабкі сторони), що відображають внутрішні недоліки, які знижують ефективність захисту, як-от відсутність регулярного моніторингу, застаріле програмне забезпечення чи людський фактор. Нижній лівий сектор представляє Opportunities (Можливості) — це зовнішні фактори, які можна використати для підвищення рівня захисту або розвитку системи, наприклад інтеграція хмарних сервісів безпеки, автоматизація процесів або залучення партнерів із кіберзахисту. Праворуч розміщено Threats (Загрози) — зовнішні чинники ризику, серед яких кіберзлочинність, нормативні зміни, технологічна конкуренція або глобальні інциденти, що впливають на стабільність інформаційних систем.



Рис. 3.9. Класична матриця SWOT-аналізу (Strengths, Weaknesses, Opportunities, Threats)

Джерело: [1-9, 11-26, 60-69, 75-82]

Узагальнена структура SWOT-матриці дозволяє системно зіставити внутрішні ресурси підприємства з викликами зовнішнього середовища. Вона допомагає виявити критичні зони, де слабкі сторони збігаються із зовнішніми загрозами, а також визначити напрямки розвитку, де сильні сторони можна використати для реалізації можливостей. Такий підхід

робить SWOT-аналіз ефективним інструментом стратегічного планування в інформаційній безпеці та управлінні ризиками.

SWOT-аналіз у сфері інформаційної безпеки є не лише інструментом описової оцінки, а й засобом формування стратегічного бачення розвитку системи захисту підприємства. Його проведення починається зі збору та структуризації даних про внутрішній стан системи безпеки, організаційні процеси, кадровий потенціал, технічні ресурси та зовнішнє середовище, у якому функціонує підприємство. Основна мета полягає у визначенні взаємозв'язків між внутрішніми факторами (силами й слабкостями) та зовнішніми (можливостями й загрозами), щоб створити базу для стратегічного планування та управлінських рішень.

Після первинного аналізу всі фактори заносяться у матрицю SWOT, що складається з чотирьох секторів. Для кожного з них формулюються конкретні положення, що стосуються кібербезпеки підприємства. Наприклад, до сильних сторін можна віднести ефективну політику управління доступом, високий рівень обізнаності персоналу або використання сучасних антивірусних систем. Слабкі сторони можуть включати недостатню автоматизацію реагування на інциденти, відсутність централізованого моніторингу чи обмеженість фінансування. Серед можливостей зазвичай розглядаються нові технології — впровадження хмарних платформ безпеки, застосування машинного навчання у виявленні аномалій або розвиток партнерських програм із кіберзахисту. Загрози охоплюють зовнішні чинники: посилення кібератак, зміни у законодавстві щодо захисту даних, нестабільність постачальників або поява нових типів шкідливого ПЗ.

Наступним етапом є аналіз взаємодії факторів за допомогою матриці TOWS, яка дозволяє побудувати конкретні стратегії. Вона показує, як сильні сторони можна використати для нейтралізації загроз, як можливості допоможуть подолати слабкі сторони, або як мінімізувати ризики, якщо вони перетинаються з вразливими зонами. Наприклад, якщо слабкою стороною є застаріле обладнання, а загрозою — зростання кількості DDoS-атак, то можливою стратегією стане модернізація мережевої інфраструктури з використанням хмарних захисних рішень.

Результатом SWOT-аналізу є комплексна стратегічна оцінка стану кібербезпеки, яка поєднує якісний аналіз внутрішніх можливостей підприємства та зовнішніх ризиків. Вона допомагає керівництву визначити ключові напрями розвитку системи безпеки, пріоритети інвестицій, а також виявити зони, що потребують термінових заходів. SWOT також сприяє формуванню довгострокової політики управління ризиками, узгодженої з

бізнес-цілями, нормативними вимогами та рівнем прийняттого ризику підприємства.

Таким чином, представлена схема відображає інтегрований підхід FMEA, що поєднує аналіз функцій, причин і механізмів виявлення для забезпечення повного розуміння ризиків. Вона допомагає не лише визначити критичні точки відмов, а й розробити комплекс запобіжних заходів, спрямованих на підвищення надійності, стійкості та безпеки системи.

Завдяки своїй простоті, гнучкості та універсальності SWOT-аналіз використовується на ранніх етапах побудови системи захисту або при її періодичному перегляді. Він особливо ефективний у поєднанні з кількісними методами оцінювання ризиків, такими як FAIR або ALE, що дозволяє переходити від загального бачення до конкретних рішень і кількісного вимірювання ефективності заходів безпеки. Таким чином, SWOT-аналіз є невід'ємною складовою стратегічного ризик-менеджменту, який забезпечує баланс між поточним станом безпеки, потенціалом розвитку та зовнішніми викликами інформаційного середовища.

FMEA (Failure Mode and Effects Analysis)

Метод FMEA — це систематичний підхід до виявлення потенційних відмов або дефектів у процесах, системах чи компонентах, що можуть призвести до інцидентів безпеки. Він дозволяє оцінити, як саме може виникнути збій, які наслідки він матиме для бізнесу і наскільки ймовірним є його виявлення до настання. Для кожного елемента системи визначаються можливі режими відмов, їхні причини, наслідки, наявні заходи контролю та рівень виявлюваності. Далі здійснюється якісне або напівкількісне ранжування за трьома критеріями — серйозність, частота виникнення та можливість виявлення. Це дозволяє виявити найбільш критичні вразливості, що потребують першочергового усунення. Метод широко застосовується в інженерії, кібербезпеці та управлінні якістю для запобігання інцидентам на етапі проектування або експлуатації системи.

Метод FMEA є важливим інструментом проактивного управління ризиками, який дозволяє не лише реагувати на вже наявні проблеми, а й передбачати потенційні відмови ще до того, як вони проявляться у вигляді інцидентів. У контексті інформаційної безпеки цей підхід застосовується для аналізу процесів обробки, передачі й зберігання даних, функціонування мережевих компонентів, засобів автентифікації, шифрування та моніторингу. Основна перевага FMEA полягає в тому, що він дає змогу детально структурувати ризики на рівні окремих компонентів, чітко визначити причинно-наслідкові зв'язки і запропонувати конкретні дії для мінімізації шкоди.

Процес проведення FMEA починається зі створення моделі системи або процесу, що підлягає оцінюванню. Кожен компонент або крок у процесі розглядається окремо з точки зору можливих відмов — наприклад, відмова серверного сховища, збої в системі керування доступом, помилки при оновленні програмного забезпечення чи порушення процедури резервного копіювання. Для кожної потенційної відмови визначаються причини виникнення, такі як людський фактор, технічні несправності, неправильна конфігурація або зовнішній вплив (кібератака, перебої електроживлення тощо). Далі оцінюються наслідки для системи, включно з можливими втратами даних, зупинкою бізнес-процесів, репутаційними збитками або штрафними санкціями.

Ключовим елементом методу є оцінювання ризику за трьома критеріями.

1. Серйозність (Severity) — відображає масштаб можливих наслідків відмови для безпеки та функціонування підприємства.
2. Частота виникнення (Occurrence) — характеризує імовірність того, що певна відмова відбудеться у реальних умовах експлуатації.
3. Виявлюваність (Detection) — показує, наскільки легко виявити або запобігти проблемі до того, як вона спричинить збитки.

У класичній моделі кожен параметр оцінюється за шкалою (наприклад, від 1 до 10), після чого визначається пріоритет дій (RPN — Risk Priority Number). Однак у якісному підході до інформаційної безпеки ці параметри оцінюються експертно у словесній формі — “низький”, “середній” або “високий”. Це дозволяє скласти матрицю пріоритетів, яка допомагає визначити, на які відмови потрібно реагувати насамперед.

Після ранжування відмов розробляються коригувальні заходи, спрямовані на зниження ризику або його усунення. Це можуть бути технічні дії (встановлення додаткових засобів моніторингу, оновлення ПЗ, впровадження сегментації мережі), організаційні кроки (вдосконалення процедур безпеки, навчання персоналу) або стратегічні рішення (перерозподіл ресурсів, оновлення політики безпеки). Результати FMEA документуються у вигляді таблиці відмов і наслідків, що містить опис кожної події, її причини, вплив, наявні контролі та запропоновані дії з підвищення безпеки.

На рис. 3.10 зображено тришляхову модель проведення FMEA-аналізу, яка демонструє логічну послідовність етапів виявлення, аналізу та усунення потенційних відмов у системі чи процесі. Модель поділяється на три шляхи — Path 1, Path 2 і Path 3, кожен із яких відповідає за окремий аспект аналізу ризиків. Перший шлях (Path 1) розпочинається з визначення функцій, характеристик або вимог до системи. На цьому етапі

ідентифікуються потенційні режими відмов, такі як відсутність функції, часткове або надмірне виконання, деградація з часом, переривчасте функціонування чи ненавмисна робота. Далі оцінюються можливі наслідки цих відмов для бізнес-процесів або безпеки, а також визначається серйозність їх впливу. Другий шлях (Path 2) зосереджується на пошуку причин відмов і аналізі можливості їх запобігання. Для кожної ідентифікованої відмови визначається, що саме її спричинило — технічна несправність, людська помилка, дефіцит контролів або зовнішній вплив. Також оцінюється частота виникнення подібних збоїв і розробляються дії, спрямовані на зменшення ймовірності їх повторення. Третій шлях (Path 3) орієнтований на механізми виявлення потенційних відмов до того, як вони призведуть до інциденту. Аналізується ефективність наявних засобів контролю та моніторингу, визначається, наскільки добре система здатна виявляти помилки або попереджати їх. На основі отриманих результатів формуються конкретні дії (Actions), до яких належать зміни в конструкції, технологічних процесах, процедурах контролю, стандартах або документації.

Quality-One FMEA Three Path Model

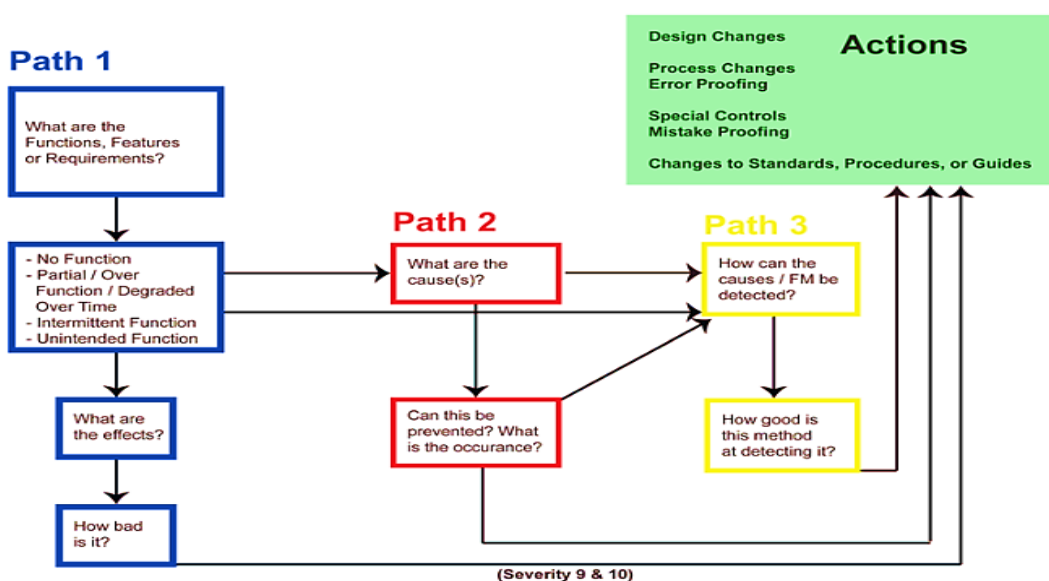


Рис. 3.10. Трикомпонентна модель FMEA (Quality-One FMEA Three Path Model)

Джерело: [38, 60-69, 75-82]

Застосування FMEA у сфері інформаційної безпеки дає змогу змістити акцент із реактивного реагування на інциденти на превентивне управління ризиками. Цей метод особливо ефективний при розробці нових інформаційних систем, модернізації IT-інфраструктури або впровадженні комплексних рішень безпеки, коли критично важливо врахувати потенційні

вразливості ще на етапі проєктування. FMEA також добре інтегрується з іншими методами оцінювання, такими як GAP-аналіз і SWOT, створюючи єдину аналітичну основу для системного управління ризиками. Отже, метод FMEA забезпечує глибоке розуміння механізмів виникнення інцидентів і дозволяє підприємству формувати превентивну культуру безпеки, де ризики не просто виявляються, а усуваються на кореневому рівні — до того, як вони стануть реальною загрозою для інформаційних активів.

Delphi-метод

Delphi-метод — це експертний підхід до якісної оцінки вразливостей, що базується на послідовних раундах анонімного опитування фахівців із метою досягнення консенсусу. У першому раунді кожен експерт оцінює ризики, вразливості або фактори загроз незалежно, після чого результати узагальнюються та аналізуються. У наступних раундах учасникам надають зворотний зв'язок у вигляді узагальнених висновків групи, що дозволяє переглянути власні оцінки. Цей процес повторюється до досягнення згоди щодо ймовірностей, впливів або пріоритетів ризиків. Метод дозволяє отримати достовірну оцінку навіть за відсутності повних статистичних даних, поєднуючи колективний досвід та об'єктивність. Завдяки анонімності усувається вплив авторитетів або групового тиску, що підвищує точність результатів.

Delphi-метод має чітко визначену структуру проведення, що забезпечує його ефективність у ситуаціях, коли кількісні дані відсутні або недостатні для об'єктивного аналізу. На початковому етапі формується експертна група, до якої входять фахівці з різних галузей, пов'язаних із досліджуваним питанням — аналітики інформаційної безпеки, адміністратори систем, аудиторі, менеджери ризиків, розробники та представники керівництва. Важливо, щоб учасники мали різний досвід і погляд на проблему, адже саме різноманітність експертиз забезпечує глибину оцінки.

Далі розробляється анкета першого раунду, яка містить перелік факторів ризику, потенційних вразливостей або сценаріїв загроз. Кожен експерт самостійно оцінює ймовірність настання події, її вплив на систему, рівень виявлюваності та можливі наслідки. Після збору даних аналітична група узагальнює результати, обчислює середні значення, діапазон оцінок і визначає ступінь розбіжності між думками.

На другому етапі результати подаються учасникам у знеособленій формі, тобто без вказівки авторів. Кожен експерт бачить узагальнені оцінки групи та аргументи, які наводили інші учасники. Завдяки цьому він може переглянути власну думку, якщо вважатиме, що колективні міркування мають раціональне підґрунтя. У наступних раундах процес повторюється,

поки розбіжності між оцінками не зменшаться до прийнятного рівня, що свідчить про досягнення консенсусу.

Delphi-метод дозволяє отримати глибокий аналітичний результат, який відображає не просто середнє значення експертних думок, а зважене бачення проблеми з урахуванням аргументів і контексту. У сфері інформаційної безпеки цей підхід часто застосовується для визначення рівня ризику окремих вразливостей, пріоритизації заходів із захисту, оцінювання зрілості процесів безпеки чи формування стратегічних прогнозів щодо нових типів загроз.

Однією з ключових переваг методу є анонімність, яка усуває вплив авторитетних учасників, суб'єктивних симпатій або тиску з боку керівництва. Це особливо важливо у великих компаніях, де рішення у сфері безпеки часто приймаються колегіально. Крім того, Delphi сприяє груповому навчанню, адже експерти, обмінюючись знаннями, отримують нове бачення проблеми, що підвищує загальний рівень компетентності команди.

На рис. 3.11 представлено послідовність основних етапів реалізації Delphi-методу — структурованого експертного підходу для досягнення колективного консенсусу щодо складних проблем, коли кількісних даних недостатньо. Процес розпочинається з етапу Start Delphi, під час якого визначається мета дослідження та загальна методологія. Далі відбувається ідентифікація потенційних експертів, де формується група фахівців із відповідними знаннями в предметній галузі. Після цього розпочинається перший раунд Delphi, який полягає у проведенні анкетування або опитування експертів щодо досліджуваного питання.

Отримані відповіді збираються та піддаються аналізу для виявлення основних тенденцій і розбіжностей у думках. На наступному етапі здійснюється оцінювання рівня консенсусу (на схемі — перевірка умови $If > 0.65$), що показує, наскільки узгодженими є оцінки учасників. Якщо згоди не досягнуто, формується зворотний зв'язок для панелістів наступного раунду, у якому надаються узагальнені результати та аргументи групи. Це дає змогу експертам переглянути власні позиції та скоригувати оцінки.

Процес повторюється кілька разів, доки рівень консенсусу не стане прийнятним. Після цього формується підсумковий звіт (Report the final results), у якому узагальнюються погоджені оцінки, пріоритети ризиків або прогнозів, і відбувається завершення процедури — End Delphi. Така ітераційна модель забезпечує поступове уточнення оцінок, усунення крайніх точок зору та отримання збалансованого експертного висновку, що підвищує достовірність результатів аналізу ризиків або вразливостей.

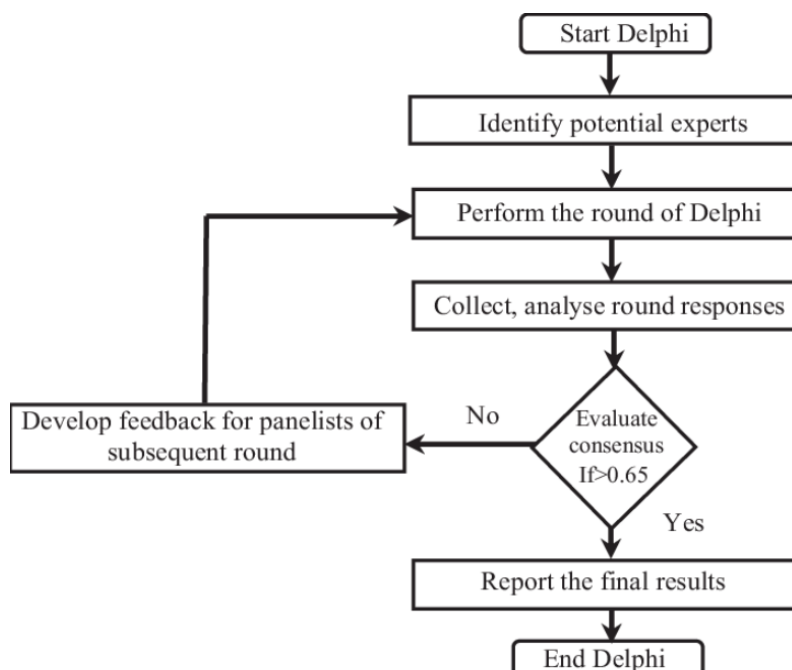


Рис. 3.11. Трикомпонентна модель FMEA (Quality-One FMEA Three Path Model)

Джерело: [38, 60-69, 75-82]

Результатом проведення Delphi-аналізу є узагальнений звіт, який містить погоджені оцінки ризиків, ранжування вразливостей, ступінь невизначеності та рекомендації щодо подальших дій. На основі цього звіту формується план управління ризиками з урахуванням думки експертів і пріоритетності виявлених проблем. Таким чином, Delphi-метод виступає гнучким і надійним інструментом якісного ризик-менеджменту, який поєднує досвід, інтуїцію та аналітичний підхід, дозволяючи приймати обґрунтовані рішення навіть у складних і динамічних умовах кіберзагроз.

Метод матриці ризику (Risk Matrix)

Метод матриці ризику є одним із найнаочніших інструментів якісної оцінки вразливостей, який відображає ризики у вигляді двовимірної таблиці, де по одній осі визначається ймовірність виникнення інциденту, а по іншій — рівень його впливу. Кожна комбінація цих параметрів утворює певну зону ризику — низьку, середню, високу або критичну. Такий підхід дозволяє швидко візуалізувати, які загрози потребують негайного реагування, а які можна контролювати в рамках прийнятного ризику. Матриця ризику широко використовується для комунікації результатів аналізу керівництву, оскільки забезпечує зрозуміле представлення складної інформації без необхідності глибокого технічного аналізу. Вона також сприяє визначенню пріоритетів у розподілі ресурсів і формуванні політики

управління ризиками. Однак для отримання достовірних результатів необхідна узгоджена шкала оцінок і регулярний перегляд значень у зв'язку зі зміною середовища загроз.

Метод матриці ризику ґрунтується на поєднанні експертної оцінки та візуального аналізу, що робить його ефективним засобом для прийняття управлінських рішень у сфері інформаційної безпеки. Основна ідея полягає в тому, щоб зіставити ймовірність реалізації певної загрози з величиною її потенційного впливу, визначивши, наскільки критичним є ризик для підприємства. У типовій матриці вісь Х відображає рівень імовірності (наприклад, “рідко”, “можливо”, “часто”, “дуже ймовірно”), а вісь Y — рівень наслідків (“незначний”, “помірний”, “серйозний”, “катастрофічний”). Кожна клітинка матриці відповідає певній комбінації цих двох параметрів і позначається кольором, що символізує рівень загрози: зелений — прийнятний ризик, жовтий — помірний, помаранчевий — високий, червоний — критичний.

У процесі оцінювання ризику наносяться на матрицю залежно від результатів попереднього аналізу або експертних висновків. Це дозволяє швидко ідентифікувати “червоні зони”, де поєднання високої ймовірності та значного впливу потребує негайного втручання, наприклад, реалізації додаткових засобів захисту або зміни політики доступу. Водночас “зелені зони” можуть бути прийнятними для підприємства в межах визначеного Risk Appetite — рівня допустимого ризику, погодженого керівництвом. Така візуалізація є особливо корисною для стратегічного планування та розподілу ресурсів, оскільки дозволяє обґрунтувати пріоритетність заходів безпеки не лише з технічної, а й з економічної точки зору.

Метод матриці ризику часто поєднується з іншими підходами — наприклад, з Delphi-методом для уточнення експертних оцінок або з FMEA для деталізації причин і наслідків потенційних відмов. Це забезпечує глибший контекст і підвищує точність класифікації ризиків. Важливо, щоб шкала оцінок (як для ймовірності, так і для впливу) була стандартизованою та узгодженою між усіма учасниками процесу, інакше порівняння ризиків між різними підрозділами стане некоректним.

Крім того, метод матриці ризику не є статичним інструментом — він потребує періодичного оновлення відповідно до динаміки загрозового середовища. Наприклад, якщо з'являються нові типи кібератак, змінюються вразливості програмного забезпечення або оновлюється законодавча база, попередньо прийнятний рівень ризику може стати неприйнятним. Тому підприємства зазвичай проводять регулярний перегляд матриці ризику — щоквартально або після значних змін у системі безпеки.

Перевагою цього методу є його зрозумілість і гнучкість: результати легко інтерпретуються як технічними фахівцями, так і управлінським персоналом. Завдяки цьому матриця ризику широко використовується у звітності перед аудиторами, регуляторами та керівництвом. Вона дозволяє не лише визначити рівень небезпеки, але й візуально обґрунтувати ефективність запланованих або вже реалізованих заходів безпеки. Крім того, матриця ризику забезпечує спільне бачення стану безпеки для всіх зацікавлених сторін, що сприяє узгодженню пріоритетів у межах підприємства. Її використання спрощує комунікацію між технічними експертами та управлінцями, перетворюючи складні аналітичні дані на зрозумілу графічну форму. Інструмент дозволяє швидко адаптувати оцінку ризиків до змін зовнішнього середовища, технологій або нормативних вимог. У підсумку матриця ризику стає основою для стратегічного планування заходів захисту, оптимізації витрат і підвищення загальної інформаційної стійкості підприємства.

На рис. 3.12 представлено класичну матрицю ризику (Risk Matrix), яка використовується для якісної оцінки рівня ризиків залежно від їхньої ймовірності (Likelihood) та серйозності наслідків (Consequence). По вертикальній осі відображено рівні ймовірності — від 1 (рідко) до 5 (майже напевно), що характеризують частоту виникнення події. По горизонтальній осі показано рівні наслідків — від 1 (незначні) до 5 (катастрофічні), які визначають масштаб потенційної шкоди для підприємства. Кожна комірка матриці є результатом комбінації цих двох параметрів і позначена кольором, що візуалізує рівень ризику. Зелений колір відповідає низькому ризику (Low), який прийнятний і не потребує негайних дій. Жовтий і помаранчевий кольори позначають помірні та високі ризики (Moderate, High), що вимагають моніторингу та впровадження запобіжних заходів. Червоні клітинки відображають екстремальний рівень ризику (Extreme), який потребує негайного реагування, оскільки поєднує високу ймовірність із серйозними або катастрофічними наслідками. Ця матриця дозволяє аналітикам і керівникам швидко визначити пріоритетність дій у сфері інформаційної безпеки, розподілити ресурси на усунення найбільш критичних загроз і прийняти обґрунтовані управлінські рішення. Вона є ключовим інструментом візуалізації ризиків у системах управління безпекою та широко застосовується в рамках стандартів ISO/IEC 27005 і NIST SP 800-30.

		Consequence				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
Likelihood	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Рис. 3.12. Матриця ризику для оцінювання ймовірності та наслідків подій
Джерело: [38, 60-69, 75-82]

У підсумку, метод матриці ризику є важливим інструментом стратегічного управління вразливостями, який допомагає підприємствам приймати зважені рішення, розставляти пріоритети у захисті активів і підтримувати баланс між рівнем безпеки та витратами на її забезпечення.

3.4. МОДЕЛІ ЗАГРОЗ І ВЕКТОРІВ АТАК У РИЗИК-ОРІЄНТОВАНОМУ УПРАВЛІННІ

Моделі загроз і векторів атак є ключовим елементом ризик-орієнтованого підходу до управління інформаційною безпекою, оскільки саме вони забезпечують структуроване розуміння потенційних джерел небезпеки, шляхів реалізації атак і можливих наслідків для інформаційних активів підприємства. Метою побудови таких моделей є виявлення всіх можливих сценаріїв порушення конфіденційності, цілісності чи доступності інформації, а також визначення їхнього впливу на бізнес-процеси. На відміну від реактивних методів, що зосереджені на усуненні вже відомих інцидентів, моделювання загроз дозволяє прогнозувати потенційні ризики,

системно ідентифікувати слабкі місця в архітектурі системи й розробляти превентивні заходи захисту.

Побудова моделі загроз починається з ідентифікації активів, які мають цінність для підприємства — бази даних, сервери, системи управління доступом, хмарні сервіси, мережеві пристрої, персональні дані користувачів тощо. Для кожного активу визначається його критичність та залежність від інших елементів системи. Далі здійснюється аналіз середовища загроз, що включає як зовнішні чинники (кібератаки, шкідливе ПЗ, фішинг, DDoS), так і внутрішні (недбалість персоналу, помилки конфігурацій, внутрішні зловживання). На цьому етапі формується повна картина можливих загроз для конкретної інформаційної системи.

Наступним кроком є визначення векторів атак, тобто шляхів, якими загроза може реалізуватися на практиці. Типові вектори включають:

- Мережеві атаки (експлуатація вразливостей у протоколах TCP/IP, DNS, HTTP, VPN тощо);
- Соціальна інженерія (фішинг, підробка електронних листів, телефонні шахрайства);
- Вразливості програмного забезпечення (SQL-ін'єкції, XSS, буферні переповнення);
- Атаки на автентифікацію та авторизацію (brute force, credential stuffing, session hijacking);
- Фізичні вектори (несанкціонований доступ до серверних приміщень, крадіжка пристроїв, пошкодження носіїв інформації).

Для кожного вектора визначається ймовірність його реалізації, ступінь впливу на активи та можливі механізми виявлення й реагування. Це дозволяє побудувати карту ризиків, що демонструє взаємозв'язки між активами, загрозами, векторами атак і заходами контролю.

Для кожного вектора атак визначається не лише його ймовірність реалізації, але й контекст, у якому він може бути використаний — тип зловмисника, рівень його мотивації, наявність технічних засобів та можливі сценарії дій. Аналізуючи ці параметри, можна оцінити потенційну шкоду для конкретних інформаційних активів, враховуючи як прямі наслідки (наприклад, витік даних, зупинка сервісу чи знищення інформації), так і опосередковані — втрату довіри користувачів, фінансові збитки чи порушення відповідності нормативним вимогам. Одночасно визначаються механізми виявлення атак, серед яких системи моніторингу подій безпеки (SIEM), засоби виявлення вторгнень (IDS/IPS), аналітика поведінкових аномалій та журнали аудиту. Реагування на кожен вектор передбачає конкретні дії — від автоматичного блокування підозрілої активності до

ізоляції сегмента мережі, оновлення політик доступу чи активації плану реагування на інциденти.

Інтегрована карта ризиків (Risk Map)

На основі цього формується інтегрована карта ризиків (Risk Map), яка наочно відображає взаємозв'язки між активами підприємства, можливими загрозами, шляхами їх реалізації та діючими заходами контролю. Така карта дозволяє побачити критичні вузли, через які атаки можуть поширюватися між компонентами системи, і визначити точки концентрації ризиків. Вона також допомагає виявити надлишкові або неефективні механізми захисту, оптимізувати витрати на безпеку та зосередити ресурси на найбільш вразливих ділянках. Карта ризиків є динамічним інструментом, який постійно оновлюється відповідно до змін в архітектурі системи, появи нових загроз або модифікацій бізнес-процесів.

Інтегрована карта ризиків забезпечує цілісне бачення стану інформаційної безпеки підприємства, дозволяючи поєднати технічні, організаційні та управлінські аспекти в єдину модель. Вона стає основою для формування рішень щодо пріоритизації інвестицій у безпеку, вибору оптимальних засобів захисту та визначення допустимого рівня ризику (Risk Appetite). На практиці така карта використовується для візуалізації результатів аудитів, моніторингу виконання планів усунення вразливостей і контролю ефективності впроваджених заходів. Завдяки гнучкості структури Risk Map її можна інтегрувати в системи управління ризиками (GRC-платформи), SIEM або корпоративні дашборди. Крім того, вона дозволяє моделювати сценарії розвитку інцидентів і прогнозувати потенційні втрати у випадку реалізації загроз. У підсумку карта ризиків стає не лише інструментом аналітики, а й засобом стратегічного управління, який забезпечує прозорість процесів кіберзахисту та підвищує готовність підприємства до реагування на динамічні виклики кіберпростору.

На рис. 3.13 представлено інтегровану карту ризиків, яка відображає взаємозв'язки між активами підприємства, потенційними загрозами, векторами атак та застосованими заходами контролю. Карта побудована у вигляді матриці, де по горизонтальній осі розташовано ймовірність реалізації ризику, а по вертикальній — рівень впливу інциденту на бізнес-процеси. Кожна точка на полі ризику відповідає певній комбінації активу, загрози та вектора атаки, що дозволяє швидко ідентифікувати критичні ділянки інформаційної інфраструктури. Зони червоного кольору позначають високий або неприйнятний рівень ризику, який потребує негайного реагування, тоді як зелені й жовті області вказують на прийнятний або контрольований рівень небезпеки.

Інтегрована карта ризиків є інструментом стратегічного управління, який допомагає виявити не лише найуразливіші точки системи, але й надлишкові або неефективні заходи захисту. Вона дозволяє оптимізувати ресурси, спрямовуючи інвестиції в ті зони, де ризик є найбільш значущим для бізнесу. Крім того, карта може динамічно оновлюватися відповідно до змін архітектури IT-середовища, появи нових кіберзагроз чи перегляду політик безпеки. Такий підхід забезпечує наочне представлення ризиків як для технічних фахівців, так і для керівництва, що сприяє прийняттю обґрунтованих рішень і підвищенню загальної стійкості підприємства до кіберзагроз.

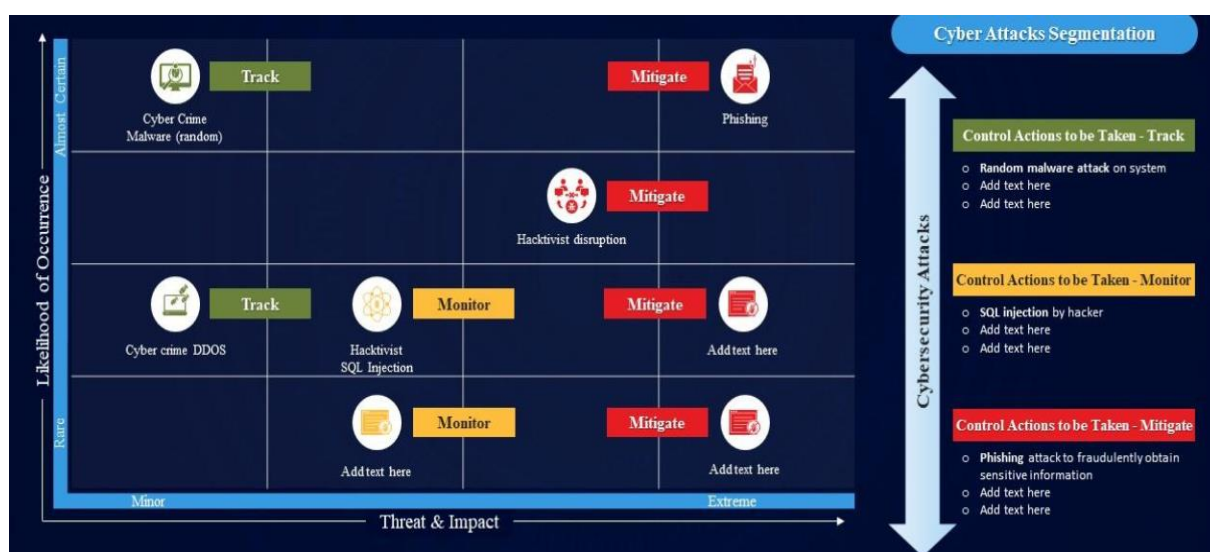


Рис. 3.13. Інтегрована карта ризиків (Risk Map) у системі управління інформаційною безпекою підприємства

Джерело: [38, 60-69, 75-82]

Завдяки такому підходу ризик-орієнтоване управління набуває системного характеру: кожен вектор атаки пов'язується з конкретними активами, а всі заходи захисту — з реальними ризиками. Це дозволяє підприємству не лише документально підтвердити зрілість системи безпеки, але й забезпечити її адаптивність до нових викликів. Таким чином, побудова карти ризиків на основі аналізу векторів атак створює основу для комплексного прийняття рішень, орієнтованих на мінімізацію потенційних втрат і підвищення стійкості інформаційної інфраструктури до сучасних кіберзагроз.

У рамках ризик-орієнтованого управління, моделі загроз використовуються не лише для аналітичного опису, а й для кількісної або якісної оцінки ризиків. На основі отриманих даних визначаються ймовірні

сценарії атак, їхня послідовність та вплив на бізнес-процеси. Наприклад, якщо атака на сервер баз даних може призвести до витоку персональних даних, то рівень ризику оцінюється як критичний, і для його зниження впроваджуються додаткові контролю — шифрування, моніторинг аномалій, обмеження доступу. У цьому контексті модель загроз стає основою для розрахунку залишкового ризику (*residual risk*), який залишається після реалізації заходів захисту.

Крім того, моделі загроз дозволяють оцінити ефективність існуючих засобів контролю, виявляючи прогалини, які можуть бути використані зловмисниками. Вони допомагають визначити пріоритетність заходів безпеки, орієнтуючись не лише на технічні аспекти, а й на економічну доцільність їх впровадження. На основі таких моделей формуються карти ризиків, що відображають взаємозв'язки між активами, загрозами, векторами атак і потенційними збитками. Це дає змогу керівництву приймати обґрунтовані рішення щодо інвестування у безпеку та формувати політику управління ризиками на стратегічному рівні. Застосування моделей загроз у комплексі з кількісним аналізом підвищує точність прогнозування ризиків та дозволяє оцінити їхній вплив у динаміці. У результаті підприємство отримує адаптивну систему ризик-менеджменту, здатну своєчасно реагувати на зміни у середовищі кіберзагроз і забезпечувати безперервність бізнесу.

Модель STRIDE

Одним із найпоширеніших підходів до побудови таких моделей є STRIDE, запропонований компанією Microsoft. Він класифікує загрози за шістьма категоріями: Spoofing (підроблення особи), Tampering (зміна даних), Repudiation (відмова від дій), Information Disclosure (витік інформації), Denial of Service (відмова в обслуговуванні), Elevation of Privilege (підвищення привілеїв). STRIDE дозволяє систематизувати всі потенційні ризики для кожного елементу системи й оцінити, наскільки ефективно поточні заходи контролю знижують ці ризики.

Модель STRIDE є основою для структурованого підходу до моделювання загроз і широко використовується під час проєктування безпечних інформаційних систем. Її головна перевага полягає в тому, що вона дозволяє розглядати безпеку не як сукупність окремих подій, а як системну властивість, яка охоплює всі етапи життєвого циклу інформаційних процесів. Кожна категорія моделі описує певний тип загрози, пов'язаний із конкретними порушеннями принципів безпеки — конфіденційності, цілісності, доступності, автентичності та невідмовності. Наприклад, Spoofing вказує на спроби зловмисника видати себе за іншу особу або систему, Tampering — на спотворення або підміну даних,

Repudiation — на неможливість довести факт здійснення дії користувачем, Information Disclosure — на несанкціоноване розкриття інформації, Denial of Service — на спроби зробити систему недоступною, а Elevation of Privilege — на отримання зловмисником прав, вищих за передбачені.

На рис. 3.14 подано узагальнену модель STRIDE, що відображає шість основних типів загроз, пов'язаних із порушенням базових властивостей інформаційної безпеки. У таблиці показано взаємозв'язок між типом загрози, порушеною властивістю системи та сутністю самої загрози. Категорія Spoofing (підроблення особи) порушує автентифікацію, оскільки зловмисник видає себе за іншу особу чи систему для отримання несанкціонованого доступу. Tampering (спотворення даних) впливає на цілісність, адже передбачає зміну інформації на диску, у мережі або пам'яті. Repudiation (відмова від дії) порушує невідомість і стосується випадків, коли користувач заперечує факт виконання певних дій. Information Disclosure (розголошення інформації) загрожує конфіденційності, оскільки передбачає доступ сторонніх осіб до даних, що підлягають захисту. Denial of Service (відмова в обслуговуванні) впливає на доступність, спричиняючи виснаження ресурсів і зупинку сервісів. Нарешті, Elevation of Privilege (підвищення привілеїв) порушує авторизацію, дозволяючи користувачу або зловмиснику виконувати дії, які не відповідають його рівню доступу. Така структурована класифікація дозволяє системно виявляти, описувати й пріоритезувати загрози, а також визначати відповідні заходи контролю для кожної категорії, забезпечуючи комплексний підхід до моделювання ризиків у процесі проектування безпечних інформаційних систем.

Під час побудови моделі STRIDE кожен компонент інформаційної системи — сервер, база даних, користувацький інтерфейс, мережевий шлюз — аналізується на предмет наявності відповідних категорій загроз. Для цього створюється діаграма потоків даних (DFD), на якій позначаються процеси, сховища, зовнішні сутності та канали передачі даних. На основі цієї моделі проводиться ідентифікація загроз для кожного елемента, після чого здійснюється оцінка рівня ризику за критеріями імовірності реалізації та потенційного впливу. Далі визначаються наявні заходи контролю — наприклад, механізми автентифікації, цілісності, журналювання або шифрування — і оцінюється, чи є вони достатніми для зниження ризику до прийняттого рівня.

STRIDE THREAT MODEL

Enter your sub headline here

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non-Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.

Рис. 3.14. Модель STRIDE для класифікації загроз інформаційним системам

Джерело: [38-54, 60-69, 75-82]

STRIDE також може бути інтегрована з іншими методиками, такими як DREAD (для кількісної оцінки ризиків), PASTA (для моделювання атак) або OCTAVE (для управління ризиками на рівні підприємства). У результаті формується детальна карта загроз, яка показує, які саме типи атак найбільш імовірні для кожного елемента системи та які контрзаходи є найбільш ефективними. Такий підхід забезпечує не лише аналітичну повноту, а й практичну придатність — модель STRIDE дає змогу пріоритизувати заходи безпеки, оптимізувати використання ресурсів і створити прозору основу для подальшої сертифікації системи відповідно до міжнародних стандартів ISO/IEC 27005 або NIST SP 800-30.

Методологія PASTA (Process for Attack Simulation and Threat Analysis)

Іншим підходом є PASTA (Process for Attack Simulation and Threat Analysis), який застосовується для більш глибокого аналізу ризиків у бізнес-

контексті. Він передбачає моделювання можливих сценаріїв атак з урахуванням цілей зловмисників, вразливостей системи та очікуваного впливу на бізнес. У результаті формується модель, що дозволяє обґрунтувати пріоритетність заходів захисту на основі вартості потенційних втрат.

Методологія PASTA (Process for Attack Simulation and Threat Analysis) вирізняється своєю системністю та орієнтацією на бізнес-процеси, що робить її одним із найповніших підходів до аналізу ризиків у сфері інформаційної безпеки. На відміну від класичних технічних моделей загроз, PASTA охоплює не лише технологічні аспекти атак, а й економічні, організаційні та стратегічні чинники, що впливають на прийняття рішень. Основна ідея полягає у відтворенні реалістичних сценаріїв поведінки зловмисників — від етапу розвідки та виявлення вразливостей до експлуатації системи та досягнення кінцевих цілей, таких як компрометація даних або порушення роботи критичних сервісів.

Процес аналізу за PASTA складається із семи послідовних етапів:

1. Визначення бізнес-цілей і меж системи, на якому встановлюються пріоритетні активи, критичні сервіси та основні залежності між ними.

2. Ідентифікація загроз, що можуть вплинути на досягнення бізнес-цілей, із залученням експертів із різних підрозділів — ІТ, аудиту, менеджменту ризиків і безпеки.

3. Моделювання архітектури системи, включно з потоками даних, точками доступу, компонентами інфраструктури та можливими точками входу для атак.

4. Аналіз вразливостей, що охоплює як технічні недоліки (помилки конфігурації, незахищені API, відсутність шифрування), так і процесні (недостатній контроль доступу, людський фактор, помилки персоналу).

5. Моделювання атак і симуляція дій зловмисників, у ході якого створюються сценарії можливих вторгнень з урахуванням реалістичних тактик і технік, аналогічних до тих, що застосовуються в сучасних АРТ-кампаніях.

6. Оцінювання ризиків і визначення їхнього впливу на бізнес, де кількісно визначається рівень можливих збитків, час відновлення (RTO) та наслідки для репутації й відповідності вимогам регуляторів.

7. Формування плану пом'якшення (mitigation plan), який включає пріоритизацію контрзаходів, обґрунтовану економічними критеріями, такими як співвідношення витрат до очікуваного зниження ризику (Cost–Risk Reduction Ratio).

На рис. 3.15 зображено модель методології PASTA, яка відображає сім послідовних етапів побудови процесу аналізу загроз і моделювання атак. У

центрі діаграми представлено ядро процесу — PASTA Threat Modeling, навколо якого розташовані основні фази, що утворюють логічний цикл управління ризиками. Перший етап — Defining Objectives — полягає у визначенні бізнес-цілей, критичних активів і меж системи, що забезпечує узгодження аналізу з пріоритетами підприємства. Другий етап — Defining the Technical Scope — визначає технічні межі, архітектуру та контекст IT-інфраструктури. Далі, у процесі Application Decomposition and Analysis, проводиться деталізація компонентів системи, потоків даних і взаємодій між елементами. На четвертому етапі — Threat Analysis — здійснюється ідентифікація потенційних загроз, після чого на п'ятому етапі — Weakness and Vulnerability Analysis — виконується пошук і класифікація вразливостей. Шостий етап — Attack Modeling and Simulation — передбачає моделювання реальних сценаріїв атак з урахуванням тактик, технік і процедур зловмисників. Завершальний сьомий етап — Residual Risk Analysis and Management — включає оцінку залишкового ризику, розробку стратегії пом'якшення наслідків і прийняття рішень щодо оптимального розподілу ресурсів безпеки. Така структурована послідовність забезпечує комплексний, гнучкий та бізнес-орієнтований підхід до управління ризиками, який охоплює як технічні, так і організаційні аспекти кіберзахисту.

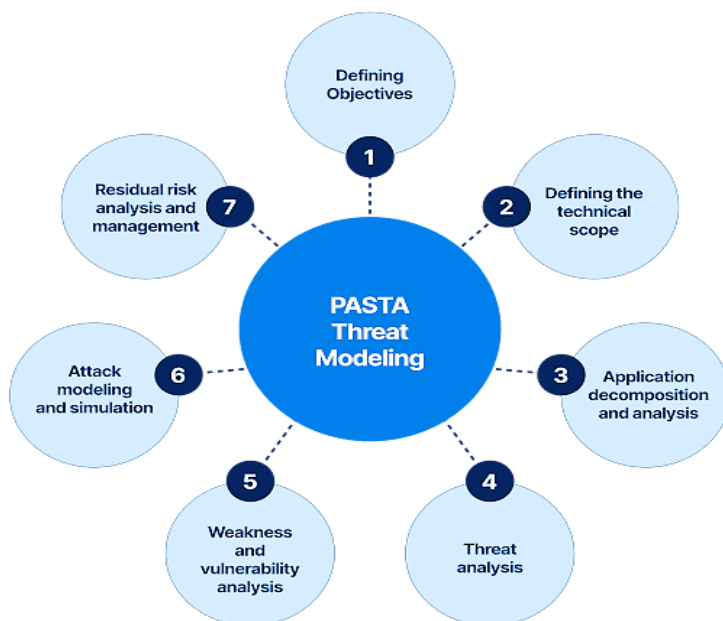


Рис. 3.15. Методологія PASTA (Process for Attack Simulation and Threat Analysis)

Джерело: [38-54, 60-69, 75-82, 91-97]

Завдяки цьому метод дозволяє не просто визначити вразливості, а й оцінити ймовірність успіху атаки та потенційні наслідки для бізнесу в

термінах втрат або перерв у роботі. У результаті формується комплексна модель, що інтегрує технічні, організаційні та фінансові аспекти ризику, дозволяючи керівництву приймати стратегічні рішення на основі реальних сценаріїв. PASTA активно використовується у великих підприємствах і державних структурах, оскільки забезпечує баланс між технічною точністю аналізу та бізнес-обґрунтованістю рекомендацій. Такий підхід підвищує зрілість системи управління ризиками, забезпечує узгодженість між IT- і бізнес-рівнями управління та формує культуру проактивного передбачення загроз у межах загальної стратегії кіберстійкості підприємства.

Для практичної реалізації моделей загроз у кібербезпеці широко використовуються діаграми потоків даних (DFD), графи атак, дерева загроз або матриці взаємозв'язків. Вони наочно відображають, які компоненти системи піддаються впливу, якими шляхами може поширюватися атака та де доцільно впроваджувати механізми виявлення або блокування.

У підсумку, моделі загроз і векторів атак є невід'ємним інструментом ризик-орієнтованого управління безпекою, який забезпечує системний підхід до виявлення, аналізу та нейтралізації потенційних небезпек. Вони дозволяють підприємству не лише знижувати ймовірність реалізації атак, але й підвищувати загальну резильєнтність (стійкість) інформаційної інфраструктури до динамічних кіберзагроз, забезпечуючи проактивне управління ризиками в умовах постійно мінливого цифрового середовища.

3.5. АДАПТИВНЕ УПРАВЛІННЯ РИЗИКАМИ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Адаптивне управління ризиками на основі машинного навчання (ML-based Adaptive Risk Management) є сучасною концепцією, що поєднує принципи традиційного ризик-менеджменту з інтелектуальними методами аналізу даних. На відміну від класичних підходів, які спираються на статичні моделі оцінки загроз і фіксовані порогові значення, адаптивна система динамічно змінює свої параметри у відповідь на зміну середовища, появу нових вразливостей або зміну поведінки користувачів. Основна мета такого підходу полягає в тому, щоб забезпечити реактивне та прогностичне управління ризиками, здатне не лише виявляти поточні інциденти, а й передбачати потенційні загрози на основі аналізу великих масивів даних (Big Data) і поведінкових патернів.

У таких системах застосовуються алгоритми машинного навчання, що здатні самостійно виявляти приховані закономірності в потоках подій без попереднього програмування правил. Вони аналізують історичні дані про

інциденти, журнали активності користувачів, мережеві аномалії та метрики продуктивності, формуючи динамічну модель ризику для кожного об'єкта або процесу. Завдяки цьому система може адаптивно змінювати політики безпеки — наприклад, підвищувати рівень автентифікації чи обмежувати доступ до критичних ресурсів під час підозрілої активності. Такий підхід дозволяє забезпечити безперервний цикл навчання, у межах якого модель удосконалюється з кожною новою подією, підвищуючи точність прогнозування ризиків. Інтеграція машинного навчання з інструментами SIEM, SOAR або XDR забезпечує автоматичне реагування на аномалії, мінімізуючи час між виявленням загрози та її нейтралізацією. У результаті адаптивне управління ризиками перетворюється на інтелектуальний механізм, який не лише реагує на загрози, а й розвивається разом із середовищем кіберризиків, забезпечуючи стійкість інформаційної інфраструктури підприємства.

У центрі адаптивної системи лежить модель машинного навчання, яка навчається на історичних даних про інциденти, журнали безпеки, телеметрію від SIEM/SOAR-платформ, результати сканування вразливостей і поведінкові дані користувачів. На основі цих даних формується профіль ризику, що описує нормальну та аномальну активність для різних елементів системи: користувачів, пристроїв, мережевих сегментів і додатків. Використовуючи алгоритми класифікації (Random Forest, SVM), кластеризації (k-Means, DBSCAN) або глибокого навчання (LSTM, Autoencoder), система може автоматично визначати ступінь відхилення від нормального стану та оцінювати рівень ризику в реальному часі. Наприклад, якщо поведінка користувача раптово змінюється — зростає кількість запитів до критичних ресурсів або відбувається підозріла авторизація з невідомої геолокації — алгоритм ідентифікує це як потенційний інцидент і підвищує рівень ризику для цього профілю.

Такі моделі здатні не лише реагувати на поточні відхилення, а й прогнозувати майбутні ризики на основі виявлених трендів у поведінці системи. Завдяки використанню механізмів прогнозного аналізу (Predictive Analytics) вони визначають, які активи з найбільшою ймовірністю можуть стати мішенню атаки. Система постійно оновлює свої параметри в режимі реального часу, враховуючи нові типи загроз і зміну контексту користувацької активності. Це забезпечує підвищення точності детекції та зменшення кількості помилкових спрацювань, що особливо важливо в умовах інтенсивного інформаційного потоку. Крім того, алгоритми машинного навчання можуть проводити кореляцію між різними джерелами даних — наприклад, поєднувати інформацію з мережевого трафіку, журналів доступу та аналітики кінцевих пристроїв для комплексної оцінки

ризик. На основі цих висновків система формує рекомендації або автоматично ініціює контрзаходи, наприклад, ізоляцію вузла чи блокування підозрілих запитів. Таким чином, модель машинного навчання стає основою самонавчальної екосистеми, яка забезпечує динамічне, точне й адаптивне управління ризиками в інформаційно-інтелектуальних системах підприємства.

Ключовою особливістю адаптивного управління ризиками є здатність системи до самонавчання. Завдяки використанню механізмів reinforcement learning (підкріплювального навчання), система постійно оновлює свої параметри, мінімізуючи ймовірність помилкових спрацювань і підвищуючи точність прогнозів. Наприклад, якщо певна подія не призвела до реальної загрози, система враховує це як “негативний приклад” і зменшує вагу відповідних ознак у подальших оцінках. Це дозволяє зменшити навантаження на аналітиків безпеки та підвищити ефективність реагування.

Інтеграція адаптивного управління ризиками з корпоративними платформами SIEM, SOAR, EDR і XDR забезпечує замкнений цикл моніторингу, аналізу та реагування. На основі аналітики ML-система може не лише попередити про потенційну загрозу, а й ініціювати автоматичні контрзаходи — наприклад, ізолювати скомпрометований вузол, змінити політику доступу, запустити перевірку цілісності файлів або відновлення з резервної копії. Таким чином, ризик знижується до прийняттого рівня без прямої участі людини.

З погляду управління, адаптивне управління ризиками дозволяє створити динамічну карту ризиків (Dynamic Risk Map), яка постійно оновлюється відповідно до змін у кіберсередовищі. На цій карті ризики відображаються в реальному часі з урахуванням ймовірності їх реалізації, потенційного впливу, залишкового ризику після застосування контрзаходів і трендів розвитку загроз. Це дає змогу керівництву підприємства приймати обґрунтовані рішення щодо інвестування в безпеку, розподілу ресурсів і пріоритезації заходів.

На рис. 3.16 представлено спрощену модель ролі штучного інтелекту (AI) у процесі управління ризиками. Центральним елементом є автоматизація ключових етапів — ідентифікації, аналізу та управління ризиками, які традиційно виконуються вручну. Завдяки використанню алгоритмів машинного навчання, система здатна автоматично збирати дані, розпізнавати закономірності, виявляти аномалії та оцінювати рівень ризику в реальному часі. Це перетворює управління ризиками на динамічний і самонавчальний процес, у якому моделі постійно вдосконалюються на основі нових даних. Як наслідок, підхід на основі AI забезпечує більш ефективні й точні стратегії управління ризиками, підвищуючи швидкість

реагування, достовірність оцінок та узгодженість рішень із поточними змінами у кіберсередовищі. Така архітектура створює основу для адаптивного ризик-менеджменту, де технології машинного навчання інтегруються у систему безпеки підприємства, забезпечуючи її стійкість, гнучкість та прогностні можливості.

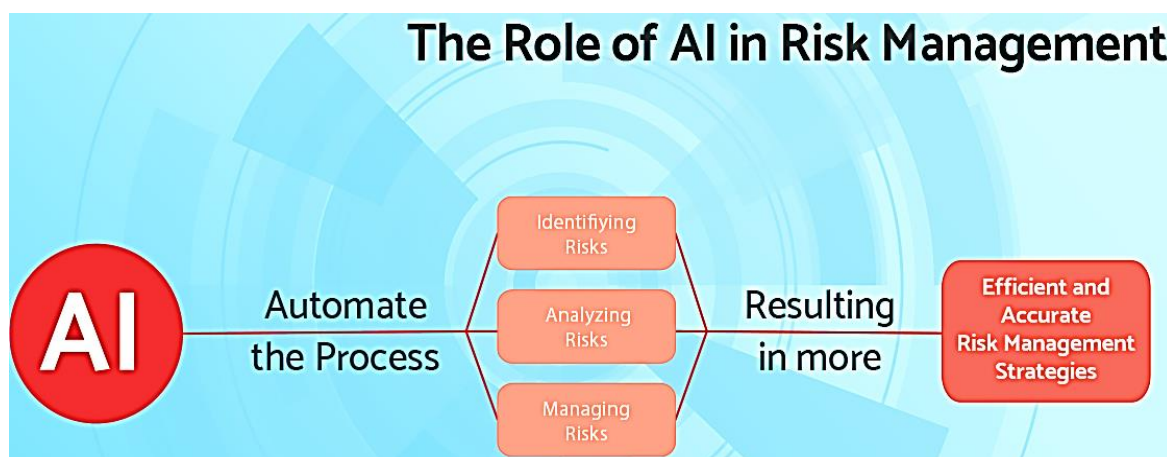


Рис. 3.16. Роль штучного інтелекту в адаптивному управлінні ризиками
Джерело: [38-54, 60-69, 75-82, 91-97]

Крім того, адаптивне управління ризиками на основі машинного навчання може інтегруватися з моделями динамічної довіри (Dynamic Trust Models), коли рівень довіри до користувача або пристрою змінюється залежно від поточного рівня ризику. Наприклад, система може тимчасово обмежити доступ до конфіденційних даних, якщо алгоритм виявив підозрілу активність, навіть без явного порушення політики безпеки. Такий підхід є основою сучасних архітектур Zero Trust Security, у яких кожна дія перевіряється, а довіра постійно переоцінюється на основі поведінкових та контекстуальних факторів.

У підсумку, адаптивне управління ризиками на основі машинного навчання створює інтелектуальну екосистему кіберзахисту, здатну самостійно аналізувати, прогнозувати й реагувати на загрози. Вона поєднує аналітику великих даних, автоматизацію процесів і когнітивні алгоритми, перетворюючи управління ризиками з реактивної діяльності на безперервний, адаптивний і прогностний процес. Такий підхід є ключовим елементом побудови стійких і самонавчальних систем інформаційної безпеки підприємства.

3.6. АВТОМАТИЗОВАНИЙ МОНІТОРИНГ, ВІЗУАЛІЗАЦІЯ ТА АУДИТ РИЗИКІВ У СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Автоматизований моніторинг, візуалізація та аудит ризиків є ключовими складовими сучасних систем управління інформаційною безпекою (СУІБ), що забезпечують безперервне відстеження стану захищеності, своєчасне виявлення відхилень і підтримку процесу прийняття рішень на основі актуальних даних. Основна мета такого підходу полягає у створенні замкненого циклу управління ризиками — від збору інформації та аналізу до реагування, перевірки ефективності заходів і подальшої оптимізації системи. Автоматизація дозволяє не лише підвищити точність і швидкість виявлення загроз, але й мінімізувати людський фактор, забезпечуючи об'єктивність оцінювання безпеки.

У сучасних умовах інформаційна безпека є динамічною системою, у якій ризики постійно змінюються через появу нових уразливостей, зміну архітектури мережі, впровадження нових технологій або поведінкових моделей користувачів. Для ефективного управління цими ризиками впроваджується автоматизований моніторинг, який здійснює безперервне спостереження за інфраструктурою підприємства, збір телеметрії з хостів, мережевих пристроїв, баз даних, хмарних сервісів і систем автентифікації. Джерелами даних є журнали подій (syslog), агенти безпеки, SIEM/SOAR-платформи, системи IDS/IPS, EDR/XDR, сканери вразливостей і засоби контролю конфігурацій. Зібрана інформація надходить до централізованого сховища, де алгоритми кореляції, машинного навчання та поведінкового аналізу виявляють аномалії, що можуть свідчити про загрози або потенційні порушення політики безпеки.

Завдяки автоматизації цей процес відбувається у режимі реального часу, що дозволяє скоротити час між виявленням загрози та реагуванням на неї до мінімуму. Система моніторингу може не лише фіксувати інциденти, а й прогнозувати можливі відхилення, аналізуючи тренди у поведінці користувачів і мережевому трафіку. Це дає змогу своєчасно виявляти ранні ознаки атак типу APT або спроби внутрішнього порушення. Автоматизований моніторинг інтегрується з модулями реагування, які можуть самостійно запускати контрдії, наприклад ізолювати вузол, блокувати IP-адресу або надсилати сповіщення адміністраторам безпеки. Отримані дані систематизуються у звітах і дашбордах, що дозволяє здійснювати візуальний контроль за рівнем ризику, ефективністю засобів захисту та станом критичних активів. Такий підхід забезпечує підприємству проактивну позицію у сфері кібербезпеки, перетворюючи моніторинг із пасивного спостереження на активний інструмент управління ризиками.

Візуалізація ризиків є наступним рівнем у системі моніторингу, який перетворює великі обсяги даних на зрозумілі для сприйняття форми — інтерактивні графіки, теплові карти, панелі керування (dashboards) та карти ризиків. Завдяки інтеграції з BI-системами (Power BI, Grafana, Kibana, Tableau) фахівці з безпеки можуть у реальному часі спостерігати динаміку змін у рівні ризику, бачити “гарячі зони” мережі, оцінювати стан захисту критичних активів і ефективність поточних заходів безпеки. Візуалізація забезпечує інформаційну прозорість між технічним і управлінським рівнями, дозволяючи керівництву швидко інтерпретувати дані без глибокого занурення в технічні деталі. На інтерактивній карті ризиків кожен вузол або сервіс має кольорове маркування за рівнем загрози (низький, середній, високий, критичний), а зв'язки між компонентами відображають потенційні шляхи поширення атаки або точки вразливості.

Третім елементом системи є автоматизований аудит ризиків, який відповідає за перевірку дотримання політик, стандартів і нормативних вимог. У рамках такого аудиту система регулярно оцінює відповідність IT-інфраструктури вимогам ISO/IEC 27001, NIST SP 800-53, GDPR, DORA, COBIT та інших регуляторних актів. Аудит включає автоматичну перевірку налаштувань доступу, шифрування, оновлення програмного забезпечення, рівня сегментації мережі, журналювання подій та інцидентів. У разі виявлення невідповідностей система генерує звіти з рекомендаціями щодо усунення порушень, а в розширених реалізаціях — ініціює автоматичні дії, наприклад, блокування облікового запису або оновлення конфігурації. Таким чином, аудит ризиків стає неперервним процесом, інтегрованим у щоденне функціонування СУІБ, а не періодичною перевіркою.

Інтеграція автоматизованого моніторингу, візуалізації та аудиту створює єдину інформаційну екосистему управління ризиками, де дані збираються, аналізуються, оцінюються й представляються у зрозумілому вигляді для прийняття рішень. Такий підхід дозволяє оперативно реагувати на події, прогнозувати тенденції розвитку загроз і підтримувати актуальний стан системи безпеки. Крім того, автоматизація сприяє впровадженню принципів continuous compliance (безперервної відповідності) і continuous monitoring, коли СУІБ постійно оцінює свою зрілість та рівень ризику, адаптуючись до змін бізнес-середовища та регуляторних вимог.

У такій екосистемі всі процеси взаємопов'язані: результати аудиту впливають на налаштування моніторингу, а виявлені під час спостереження інциденти автоматично запускають процедури перевірки відповідності та оновлення політик безпеки. Це забезпечує замкнений цикл управління ризиками, у якому кожен елемент системи постійно вдосконалюється на основі зворотного зв'язку. Візуалізація даних дозволяє керівництву не лише

бачити загальний стан безпеки, але й отримувати деталізовану інформацію про джерела ризиків, ефективність контролів і тенденції змін. Завдяки аналітичним панелям та інтерактивним звітам можливе глибоке порівняння історичних і поточних показників для оцінки динаміки загроз. Крім того, така інтеграція спрощує процес зовнішнього аудиту, оскільки система автоматично формує необхідну доказову базу відповідності міжнародним стандартам. У результаті підприємство отримує не лише ефективну технічну платформу управління ризиками, а й стратегічний інструмент, що підвищує його кіберстійкість і довіру з боку партнерів, клієнтів та регуляторів.

На рис. 3.17 представлено узагальнену архітектуру системи управління ризиками в інформаційній безпеці, яка поєднує три взаємопов'язані компоненти — автоматизований моніторинг, візуалізацію та аудит. У нижньому рівні схеми зображено джерела даних: хости, мережеві пристрої, сервери, бази даних, хмарні сервіси, SIEM/SOAR-платформи, системи IDS/IPS, EDR/XDR та агенти безпеки, які забезпечують збір телеметрії в реальному часі. Потік даних спрямовується до централізованого аналітичного ядра, де здійснюється кореляція подій, машинне навчання, поведінковий аналіз і класифікація ризиків за рівнями критичності. На середньому рівні показано модуль візуалізації — інтерактивні панелі (dashboards), карти ризиків і теплові діаграми, що відображають стан безпеки, тенденції атак, ефективність контролів та пріоритети реагування. Верхній рівень представляє автоматизований аудит відповідності, який перевіряє налаштування безпеки, політики доступу та відповідність міжнародним стандартам ISO/IEC 27001, NIST SP 800-53, GDPR, DORA, COBIT. Така система створює замкнутий цикл управління ризиками: виявлені інциденти передаються до аудиту, результати перевірок впливають на налаштування моніторингу, а дані візуалізації забезпечують підтримку стратегічних управлінських рішень. У результаті підприємство отримує єдину інформаційну екосистему, що забезпечує безперервне відстеження стану безпеки, своєчасне реагування на загрози та підвищення рівня кіберстійкості.

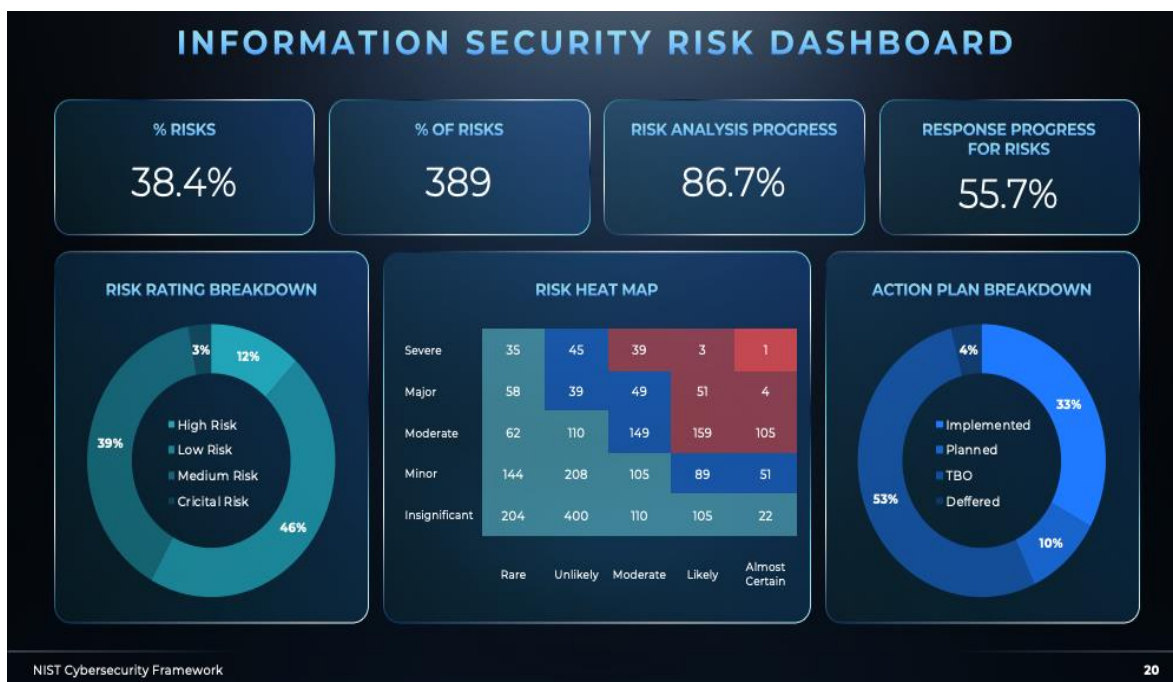


Рис. 3.17. Інтегрована система автоматизованого моніторингу, візуалізації та аудиту ризиків у СУІБ
Джерело: [38-54, 60-69, 75-82, 91-97]

Завдяки цим можливостям автоматизований моніторинг і аудит стають не просто інструментами технічного контролю, а аналітичною основою для стратегічного управління ризиками, що дозволяє організації підвищувати свою кіберстійкість, прозорість процесів і готовність до реагування на інциденти. У підсумку формується динамічна платформа управління інформаційною безпекою, здатна не лише виявляти загрози, але й пояснювати їх контекст, визначати пріоритети реагування та підтримувати прийняття обґрунтованих управлінських рішень на всіх рівнях підприємства.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 3

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.

3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

6. Shevchenko, S., Zhdanova, Y., & Spasiteleva, S. (2023). Mathematical methods in cybersecurity: Catastrophe theory. *Cybersecurity: Education, Science, Technique*, 3(19), 165–175. <https://doi.org/10.28925/2663-4023.2023.19.165175>

7. Sokolov, V. (2022). Approaches to the formation of scientific thinking in cybersecurity high school students. *Cybersecurity: Education, Science, Technique*, 2(18), 124–137. <https://doi.org/10.28925/2663-4023.2022.18.124137>

8. Shevchenko, S., Skladannyi, P., Nehodenko, O., & Nehodenko, V. (2022). Study of applied aspects of conflict theory in security systems. *Cybersecurity: Education, Science, Technique*, 2(18), 150–162. <https://doi.org/10.28925/2663-4023.2022.18.150162>

9. Sukaylo, I., & Korshun, N. (2022). The influence of NLU and generative AI on the development of cyber defense systems. *Cybersecurity: Education, Science, Technique*, 2(18), 187–196. <https://doi.org/10.28925/2663-4023.2022.18.187196>

10. Костюк Ю., Бебешко Б., Гулак Г., Складанний П., Рзаєва С., Хорольська К. (2024) Забезпечення кібербезпеки та швидкодії передачі даних у безпроводних мережах. *Безпека інформації*, т. 30, №3, 365-375.

11. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. *Cybersecurity: Education, Science, Technique*, 1(17), 145–158. <https://doi.org/10.28925/2663-4023.2022.17.145158>

12. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to provide control and management of privileged access in the IT environment. *Cybersecurity: Education, Science, Technique*, 4(16), 98–112. <https://doi.org/10.28925/2663-4023.2022.16.98112>

13. Borkivska, O., Zhurakovskiy, B., & Platonenko, A. (2022). Smart city information system based on LoRa technology. *Cybersecurity: Education, Science, Technique*, 4(16), 113–128. <https://doi.org/10.28925/2663-4023.2022.16.113128>
14. Brzhevskaya, Z., Kyrychok, R., Platonenko, A., & Hulak, H. (2022). Assessment of the preconditions of formation of the methodology of assessment of information reliability. *Cybersecurity: Education, Science, Technique*, 3(15), 164–174. <https://doi.org/10.28925/2663-4023.2022.15.164174>
15. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Boiko, S. (2022). Insiders and insider information: Essence, threats, activities and legal responsibility. *Cybersecurity: Education, Science, Technique*, 3(15), 175–185. <https://doi.org/10.28925/2663-4023.2022.15.175185>
16. Довженко, Н., Мазур, Н., Костюк, Ю., Рзаєва, С. Інтеграція ІОТ ТА штучного інтелекту в інтелектуальні транспортні системи. *Кібербезпека: освіта, наука, техніка*. 2024. 2(26), 430–444.
17. Bogachuk, V. Sokolov and V. Buriachok, "Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 581-585, doi: 10.1109/INFOCOMMST.2018.8632151.
18. Hulak, Hennadii and Skladannyi, Pavlo and Sokolov, Volodymyr and Hulak, E. and Korniiets, V. (2022) *Dynamic model of guarantee capacity and cyber security management in the critical automated systems* 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), 3530. pp. 102-111. ISSN 1613-0073
19. Sokolov, V. Y. and Skladannyi, Pavlo and Hulak, Hennadii (2022) *Stability Verification of Self-Organized Wireless Networks with Block Encryption* Cybersecurity Providing in Information and Telecommunication Systems, 3137. pp. 227-237. ISSN 1613-0073
20. Anakhov, P. and Zhebka, V. and Poperehnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) *Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073
21. Костюк Ю., Довженко, Н., Мазур, Н., Складанний, П., Рзаєва, С. Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. *Кібербезпека: освіта, наука, техніка*. 2025. 3(27), 22–40.
22. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii and Ageyev, D. (2023) *Method for Increasing the*

Various Sources Data Consistency for IoT Sensors IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5

23. A. Carlsson, D. Ageyev, Y. Sadykov and V. Sokolov, "Sustainability Research of the Secure Wireless Communication System with Channel Reservation," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 973-977, doi: 10.1109/TCSET49122.2020.235583.

24. Складанний, П., Костюк Ю., Рзаєва, С., Самойленко, Ю., Савченко, Т. Розробка модульних нейронних мереж для виявлення різних класів мережових атак. Кібербезпека: освіта, наука, техніка. 2025. 3(27), 534–548.

25. F. Kipchuk, V. Sokolov, V. Buriachok and L. Kuzmenko, "Investigation of Availability of Wireless Access Points based on Embedded Systems," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-5, doi: 10.1109/PICST47496.2019.9061551.

26. Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threat). URL: <https://cert.gov.ua/recommendations/18>

27. Технологія VPN може загрожувати кібербезпеці. URL: <https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpnmozhe-zagrozhuvati-kiberbezpetsi-inau>

28. JP 3–12 Cyberspace Operations, 8 June 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

29. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>

30. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-162_curriculum.pdf

31. National Cyber Security Strategy Good Practice Guide (2016). URL: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>

32. Castro D. (2018). Boosting the Cyberworkforce. URL: <http://www.govtech.com/data/Boosting-the-Cyberworkforce.html>

33. Cisco - Україна. URL: <https://www.cisco.com>

34. Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради України. 2017. № 45. Ст. 403.

35. Закон України "Про інформацію".

36. Закон України "Про захист інформації в інформаційно-комунікаційних системах".
37. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT) "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги".
38. ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою".
39. ДСТУ ISO/IEC 27005:2022 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки".
40. ДСТУ ISO/IEC 27701:2022 "Розширення для управління конфіденційністю в системах управління інформаційною безпекою".
41. ДСТУ ISO/IEC 15408:2020 "Критерії оцінювання безпеки інформаційних технологій".
42. ДСТУ ISO/IEC 24762:2015 "Інформаційні технології. Методи захисту. Рекомендації з відновлення інформаційно-комунікаційних технологій після інцидентів".
43. Shevchuk, D and Harasymchuk, O and Partyka, A and Korshun, Natalia (2023) *Designing Secured Services for Authentication, Authorization, and Accounting of Users* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 207-225. ISSN 1613-0073
44. Складанний П.М., Костюк Ю.В., Мазур Н.П., Пітайчук М.А. Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології. 2025. №1(86). С. 61-74.
45. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, 1(3), 602-617. <https://doi.org/10.3390/encyclopedia1030050>
46. TajDini, M., Sokolov, V., Kuzminykh, I., Shiaeles, S., & Ghita, B. (2020). Wireless Sensors for Brain Activity—A Survey. *Electronics*, 9(12), 2092. <https://doi.org/10.3390/electronics9122092>
47. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems.[Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
48. Kostiuk, Y. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security.[Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
49. Основи баз даних : навчальний посібник / Рзаєва С.Л., Машкіна І.В., Складанний П.М., Костюк Ю.В., Рзаєв Д.О., Красюк Ю.М – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 319 с.

50. Grechaninov, Viktor and Hulak, Hennadii and Hulak, Evgen and Skladannyi, Pavlo and Sokolov, Volodymyr (2021) *Decentralized Access Demarcation System Construction in Situational Center Network Cybersecurity Providing in Information and Telecommunication Systems II* 2021, 3188 (2). pp. 197-206. ISSN 1613-0073
51. Buriachok, Volodymyr and Ageyev, Dmytro and Zhylytsov, Oleksii and Skladannyi, Pavlo and Sokolov, V. Y. (2020) *Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies* Cybersecurity Providing in Information and Telecommunication Systems, 2746. pp. 23-32. ISSN 1613-0073
52. Костюк Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., Пазинін, А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка. 2025. 4 (28), 633–655.
53. M. Vladymyrenko, V. Sokolov, V. Buriachok, A. Platonenko and D. Ageyev, "Analysis of Implementation Results of the Distributed Access Control System," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-6, doi: 10.1109/PICST47496.2019.9061376.
54. Складанний, П.М., Машкіна, І.В., Рзаєва, С.Л., Костюк, Ю.В. Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології. 2025. (2), 59-76.
55. Hu, Z., Buriachok, V., Bogachuk, I., Sokolov, V., Ageyev, D. (2021). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. In: Radivilova, T., Ageyev, D., Kryvinska, N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_29
56. F. Kipchuk, V. Sokolov, P. Skladannyi and D. Ageyev, "Assessing Approaches of IT Infrastructure Audit," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 213-217, doi: 10.1109/PICST54195.2021.9772181.

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні етапи включає процес управління ризиками згідно зі стандартом ISO/IEC 27005?
2. У чому полягає головна відмінність між підходами ISO/IEC 27005 та NIST SP 800-30 до оцінки ризиків?

3. Як у методології FAIR здійснюється кількісна оцінка ризиків інформаційної безпеки?
4. Які ключові елементи формують модель ризику в системі управління інформаційною безпекою підприємства?
5. Які показники використовуються для кількісної оцінки ризику та як вони розраховуються?
6. Чим відрізняється якісна оцінка ризиків від кількісної та в яких випадках доцільно застосовувати кожен з них?
7. У чому полягає суть GAP-аналізу та яку роль він відіграє у виявленні вразливостей системи безпеки?
8. Як SWOT-аналіз може бути використаний для стратегічного планування заходів з кіберзахисту?
9. Які етапи включає метод FMEA (Failure Mode and Effects Analysis) при оцінюванні ризиків у сфері інформаційної безпеки?
10. Як моделі загроз і векторів атак застосовуються для побудови ризик-орієнтованих стратегій захисту?
11. Що означає поняття вектор атаки, і як воно використовується в моделюванні загроз?
12. Як алгоритми машинного навчання використовуються для побудови систем адаптивного управління ризиками?
13. Які основні типи моделей машинного навчання (класифікація, кластеризація, прогнозування) застосовуються у кіберризик-менеджменті?
14. У чому полягає принцип self-learning (самонавчання) в адаптивних системах управління ризиками?
15. Як відбувається інтеграція адаптивного управління ризиками з платформами SIEM, SOAR, EDR або XDR?
16. Яку роль відіграють автоматизований моніторинг, візуалізація та аудит ризиків у сучасних системах управління інформаційною безпекою (СУІБ)?
17. Які типи даних використовуються для автоматизованого моніторингу ризиків і як здійснюється їх кореляційний аналіз?
18. Як візуалізація ризиків допомагає підвищити ефективність прийняття управлінських рішень у сфері кібербезпеки?
19. Які ключові відмінності між традиційним аудитом безпеки та автоматизованим аудитом ризиків у СУІБ?
20. Які основні виклики постають перед підприємствами при впровадженні адаптивного управління ризиками у хмарних і SDN-мережах?

РОЗДІЛ 4

ТЕХНОЛОГІЇ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ



- 4.1. Центри оперативного реагування (SOC) і їх роль у захисті**
- 4.2. Життєвий цикл інциденту: виявлення, аналіз, реагування, відновлення**
- 4.3. Автоматизація реагування за допомогою SOAR**
- 4.4. Використання штучного інтелекту для інтелектуального моніторингу подій безпеки**
- 4.5. Технології предиктивного моніторингу та прогностного реагування на інциденти**
- 4.6. Постінцидентний аналіз і lessons learned**

Технології моніторингу та реагування на інциденти безпеки становлять комплекс технічних, програмних і організаційних засобів, спрямованих на забезпечення безперервного контролю стану інформаційної безпеки, своєчасне виявлення кіберзагроз, оперативне реагування на інциденти та мінімізацію їх наслідків. Основною метою цих технологій є підтримання стійкості інформаційних систем підприємства, зменшення часу виявлення та усунення загроз, а також запобігання повторенню подібних подій у майбутньому.

Моніторинг безпеки передбачає систематичний збір, аналіз і кореляцію даних про події з різних джерел — системних журналів, мережевого трафіку, активності користувачів, серверів та кінцевих пристроїв. Для цього використовуються системи керування інформацією та

подіями безпеки (SIEM), які забезпечують централізований збір логів, аналітику, побудову звітів і візуалізацію стану кіберзахисту в реальному часі. У поєднанні з ними застосовуються системи виявлення та запобігання вторгненням (IDS/IPS), рішення для захисту кінцевих точок (EDR/XDR) та інструменти поведінкового аналізу, що дозволяють виявляти аномалії в роботі користувачів і процесів.

Реагування на інциденти включає виявлення, ідентифікацію, класифікацію, локалізацію та усунення наслідків події безпеки. У межах цього процесу важливо правильно оцінити критичність інциденту, ізолювати уражені сегменти системи, відновити пошкоджені дані, провести цифрову експертизу (форензіку) для визначення джерела атаки та забезпечити збір доказів для подальшого розслідування. Завершальним етапом є постінцидентний аналіз, який дозволяє узагальнити отриманий досвід, виявити слабкі місця в системі захисту та вдосконалити політику інформаційної безпеки.

Сучасні підходи базуються на автоматизації процесів за допомогою платформ SOAR (Security Orchestration, Automation and Response), які реалізують сценарії реагування (playbooks) та дозволяють автоматично виконувати типові дії — наприклад, блокування шкідливих IP-адрес або відключення заражених вузлів. Інтеграція штучного інтелекту та машинного навчання забезпечує можливість предиктивного моніторингу, прогнозування потенційних атак і зменшення часу реакції. У межах центрів оперативного реагування (SOC) такі рішення формують єдиний аналітичний простір, у якому поєднуються візуалізація, кореляція подій і розподіл завдань між аналітиками.

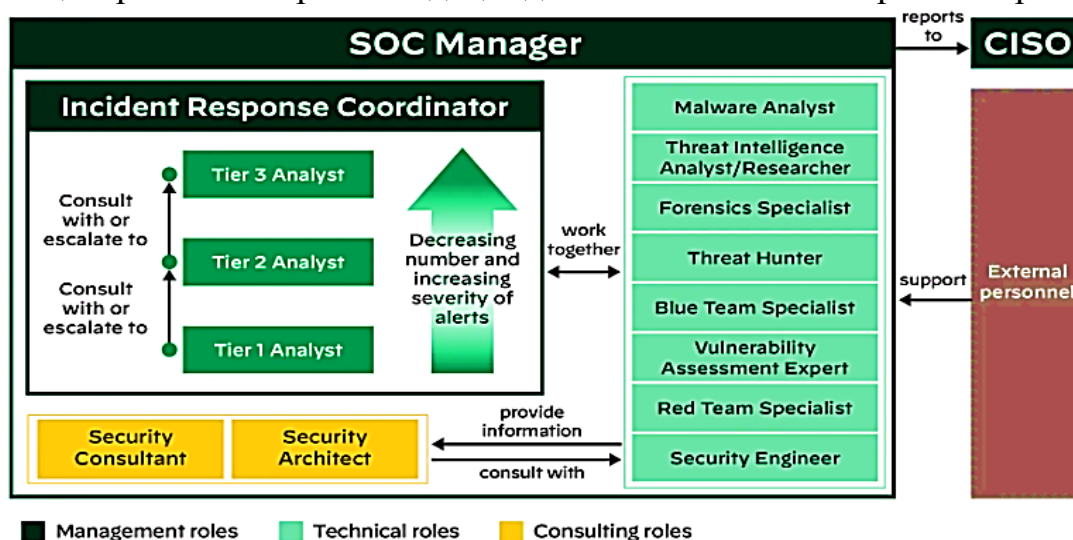
Застосування систем Splunk, IBM QRadar, ArcSight, Cortex XSOAR, Microsoft Defender XDR, Zeek, Suricata чи Snort забезпечує комплексний контроль за безпекою підприємства та дозволяє своєчасно виявляти індикатори компрометації. Відповідно до міжнародних стандартів ISO/IEC 27035 та NIST SP 800-61, технології моніторингу та реагування утворюють ядро системи управління інцидентами безпеки, сприяючи підвищенню гарантоздатності та формуванню проактивної моделі кіберзахисту підприємства.

4.1. ЦЕНТРИ ОПЕРАТИВНОГО РЕАГУВАННЯ (SOC) І ЇХ РОЛЬ У ЗАХИСТІ

Центри оперативного реагування на інциденти безпеки (Security Operations Center, SOC) є ключовим елементом сучасної системи

кіберзахисту підприємства, що забезпечує цілодобовий моніторинг, аналіз, виявлення, реагування та попередження інцидентів інформаційної безпеки. Основне завдання SOC полягає у створенні постійного циклу контролю та управління подіями безпеки, який охоплює збір, кореляцію, аналіз і реагування на всі підозрілі або потенційно шкідливі дії в інформаційно-комунікаційній системі підприємства. Такий підхід дозволяє вчасно виявляти кіберзагрози, мінімізувати наслідки атак, підвищувати рівень готовності до кризових ситуацій і забезпечувати безперервність бізнес-процесів.

На рис. 4.1 зображено узагальнену організаційну структуру центру SOC, у якій показано взаємодію управлінських, технічних і консультативних ролей у процесі моніторингу та реагування на кіберінциденти. На чолі центру перебуває SOC Manager, який звітує перед керівником із безпеки інформації (CISO) і координує діяльність усіх учасників. Безпосередньо під його керівництвом діє Incident Response Coordinator, який організовує роботу аналітиків трьох рівнів (Tier 1, Tier 2, Tier 3) залежно від складності інцидентів і критичності подій. Аналітики першого рівня виконують первинний моніторинг, обробляють оповіщення SIEM-систем і фільтрують хибні спрацьовування, передаючи складні випадки до аналітиків другого рівня, які проводять глибший аналіз подій, кореляцію сигналів і виявлення ланцюгів атак. Третій рівень аналітиків спеціалізується на форензичному аналізі, відновленні після інцидентів і розробці стратегічних рекомендацій для запобігання повторним загрозам.



Source: Security Operations Center: A Systematic Study and Open Challenges

Рис. 4.1. Структура та ролі Центру оперативного реагування на інциденти безпеки (SOC)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Паралельно з аналітичною вертикаллю функціонує технічна команда, до складу якої входять Malware Analyst, Threat Intelligence Analyst/Researcher, Forensics Specialist, Threat Hunter, Blue Team Specialist, Vulnerability Assessment Expert, Red Team Specialist і Security Engineer. Вони забезпечують дослідження шкідливого ПЗ, збір та інтерпретацію розвідувальних даних про загрози, тестування вразливостей, активне полювання на загрози та оцінку стійкості систем. Консультативний рівень представлений Security Consultant і Security Architect, які надають рекомендації щодо проектування архітектури безпеки, розробки політик і впровадження захисних рішень. Усі підрозділи SOC тісно взаємодіють між собою та із зовнішніми фахівцями, забезпечуючи підтримку та обмін інформацією про нові загрози, що дозволяє підвищити оперативність і результативність реагування. Таким чином, представлена структура відображає багаторівневий підхід до управління інцидентами безпеки, де поєднуються аналітика, технічна експертиза та стратегічне управління, спрямовані на досягнення високої кіберстійкості підприємства.

Центр SOC функціонує як аналітичний та координаційний осередок, у якому поєднуються технології моніторингу, автоматизації, аналітики даних та людський експертний досвід. Його архітектура зазвичай складається з трьох взаємопов'язаних рівнів: операційного, аналітичного та стратегічного. На операційному рівні здійснюється первинний збір і нормалізація даних із джерел, таких як журнали подій, мережевий трафік, системи виявлення вторгнень, сервери, кінцеві точки, хмарні сервіси та засоби автентифікації. На аналітичному рівні ці дані проходять обробку за допомогою систем SIEM (Security Information and Event Management), що здійснюють кореляцію подій, виявлення аномалій і формування оповіщень. Стратегічний рівень охоплює управління політиками безпеки, визначення пріоритетів реагування, координацію з іншими підрозділами підприємства та вдосконалення процесів захисту. На цьому рівні також проводиться оцінка ефективності впроваджених заходів, аналіз тенденцій розвитку загроз і вдосконалення архітектури безпеки відповідно до стандартів ISO/IEC 27035 та NIST SP 800-61.

На рис. 4.2 схематично представлено ключові компоненти сучасного SOC, які утворюють замкнений цикл моніторингу, виявлення та реагування на кіберінциденти. Центральне місце займає моніторинг і виявлення (Monitoring and Detection), що забезпечує безперервне спостереження за інформаційними потоками, журналами подій, мережевим трафіком і поведінкою користувачів. На основі отриманих даних здійснюється виявлення аномалій і формування сповіщень, які далі надходять до аналітиків SOC для оцінки рівня ризику.

Наступним етапом є реагування на інциденти та полювання на загрози (Incident Response and Threat Hunting), де спеціалісти проводять глибокий аналіз зафіксованих подій, ідентифікують джерела атак, ізолюють уражені системи та реалізують заходи з нейтралізації загроз. Третім елементом циклу виступає розвідка загроз (Threat Intelligence), яка передбачає збір, аналіз і обмін інформацією про нові вразливості, тактики та інструменти зловмисників, що дозволяє прогнозувати потенційні атаки та підвищувати готовність системи.

Завершальним компонентом є інженерія виявлення (Detection Engineering) — процес оптимізації правил виявлення, налаштування SIEM- і SOAR-платформ, тестування нових сигнатур та алгоритмів аналізу даних для підвищення точності сповіщень. Усі ці елементи взаємопов'язані та утворюють безперервний цикл удосконалення, який дозволяє центру SOC працювати проактивно, своєчасно реагувати на інциденти та адаптуватися до еволюції кіберзагроз.

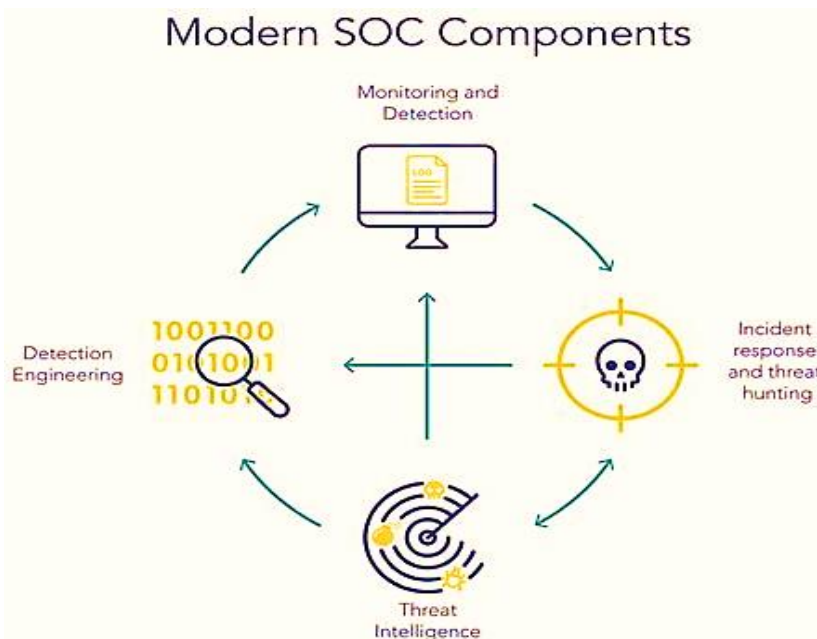


Рис. 4.2. Основні компоненти сучасного центру оперативного реагування на інциденти безпеки (SOC)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Крім того, стратегічний рівень відповідає за взаємодію з зовнішніми структурами — національними центрами кіберзахисту, CERT- і CSIRT-командами, постачальниками Threat Intelligence-даних. Це забезпечує обмін актуальною інформацією про нові вразливості, типи атак і методи реагування, що підвищує оперативність та якість рішень. Важливою

складовою діяльності SOC є формування єдиної аналітичної бази знань, у якій накопичується досвід розслідування інцидентів і типові сценарії реагування для автоматизації майбутніх дій. Завдяки такій структурі SOC перетворюється на інтегрований центр управління безпекою, що забезпечує проактивний, аналітично обґрунтований і технологічно підтриманий захист усіх інформаційних ресурсів підприємства.

Робота SOC побудована на основі стандартизованих процесів і методик, описаних у міжнародних стандартах ISO/IEC 27035 і NIST SP 800-61, які визначають життєвий цикл реагування на інциденти. Він включає етапи виявлення, ідентифікації, аналізу, локалізації, усунення, відновлення та постінцидентного вдосконалення. Кожен із цих етапів у межах SOC має чітко визначені процедури, ролі, показники ефективності (KPI) та механізми ескалації. Наприклад, аналітики першої лінії здійснюють первинний аналіз інцидентів, фільтрують хибні спрацьовування та передають складніші випадки до аналітиків другої лінії, які виконують глибокий розбір подій, виявлення ланцюгів атак і джерел компрометації. На третій лінії працюють фахівці з цифрової форензики та реагування на інциденти (DFIR), які проводять розслідування, визначають причини та розробляють рекомендації щодо запобігання повторним атакам.

Ефективний SOC базується на застосуванні передових технологій. Системи SIEM (наприклад, Splunk, IBM QRadar, ArcSight) забезпечують збір та аналіз логів у реальному часі, тоді як платформи SOAR (Security Orchestration, Automation and Response), такі як Cortex XSOAR або IBM Resilient, автоматизують виконання сценаріїв реагування (playbooks), що суттєво скорочує час реакції на інциденти. Додатково SOC інтегрується з рішеннями EDR/XDR (Endpoint/Extended Detection and Response) для контролю кінцевих пристроїв і Threat Intelligence-платформами для отримання актуальних даних про загрози, що дозволяє аналітикам будувати контекст атаки та прогнозувати подальші дії зловмисників.

Важливою функцією SOC є кореляція та контекстуалізація подій, тобто об'єднання окремих сигналів і сповіщень у логічні ланцюги, які вказують на комплексну атаку або внутрішню загрозу. Наприклад, послідовність спроб входу з різних геолокацій, зміна привілеїв користувача та аномальне завантаження мережевого трафіку можуть разом свідчити про компрометацію облікового запису. Завдяки автоматизованим механізмам аналітики SOC здатні не лише виявляти такі закономірності, а й оперативно ініціювати заходи локалізації — блокування облікового запису, ізоляцію вузла чи активацію резервних механізмів захисту.

Окреме значення мають індикатори компрометації (IoC) та індикатори поведінки (IoB), що використовуються в SOC для виявлення як

уже відомих, так і нових типів атак. На основі аналізу цих індикаторів формуються звіти про інциденти, які передаються керівництву підприємства для прийняття управлінських рішень. SOC також веде базу знань і накопичує історичні дані про попередні інциденти, що дозволяє здійснювати аналітику трендів і прогнозування кіберзагроз.

Таким чином, центри оперативного реагування є серцем системи кіберзахисту підприємства, що поєднує технологічну інфраструктуру, аналітичні інструменти та експертну діяльність фахівців з безпеки. Вони забезпечують не лише своєчасне виявлення та ліквідацію загроз, а й створюють умови для проактивного управління ризиками, підвищення кіберстійкості та вдосконалення політик інформаційної безпеки відповідно до міжнародних вимог і національних нормативів.

4.2. ЖИТТЄВИЙ ЦИКЛ ІНЦИДЕНТУ: ВИЯВЛЕННЯ, АНАЛІЗ, РЕАГУВАННЯ, ВІДНОВЛЕННЯ

Життєвий цикл інциденту інформаційної безпеки охоплює повний процес його розвитку — від моменту виявлення до повного відновлення системи та впровадження заходів, що запобігають повторенню подібних подій. Він є основою системного підходу до управління інцидентами в межах центру оперативного реагування (SOC) і визначається міжнародними стандартами, зокрема ISO/IEC 27035 та NIST SP 800-61. Такий цикл включає чотири ключові фази: виявлення, аналіз, реагування та відновлення, які перебувають у постійному взаємозв'язку та формують безперервний процес удосконалення системи безпеки.

На рис. 4.3 подано узагальнену модель життєвого циклу реагування на інциденти інформаційної безпеки, яка відображає послідовність ключових етапів управління кіберінцидентами. Першою фазою є підготовка (Preparation), під час якої формується план реагування, визначаються ролі та обов'язки членів команди, проводиться навчання персоналу, а також розгортаються технічні засоби моніторингу й захисту. Саме цей етап закладає основу ефективної взаємодії між усіма учасниками процесу та забезпечує готовність до оперативного реагування у разі виникнення інциденту. Друга фаза — виявлення (Detection) — передбачає безперервне спостереження за станом інформаційних систем, моніторинг подій, їх аналіз і класифікацію для ідентифікації потенційних загроз. На цьому етапі використовуються SIEM-, IDS/IPS- та EDR/XDR-системи, які забезпечують автоматизоване виявлення аномалій і генерацію оповіщень для аналітиків SOC. Третій етап — стримування

(Containment) — зосереджується на оперативній ізоляції інциденту для запобігання його поширенню. Здійснюється блокування шкідливих IP-адрес, відключення скомпрометованих вузлів і збереження доказової бази для подальшого аналізу. На четвертому етапі — відновлення (Recovery) — виконуються заходи з видалення шкідливого коду, відновлення функціонування систем і перевірки їхньої працездатності. Важливо забезпечити цілісність даних і переконатися у відсутності залишкових загроз, що можуть повторно активізуватися. Завершальною фазою є постінцидентна діяльність (Post-Incident), яка включає документування інциденту, оновлення політик безпеки, аналіз дій команди та обмін набутим досвідом. Цей етап сприяє вдосконаленню процедур реагування й формуванню культури постійного підвищення кіберстійкості.

Нижня частина рисунка містить ключові показники ефективності: середній час виявлення інциденту (MTTD — Mean Time to Detect, менше ніж 1 година), середній час реагування (MTTR — Mean Time to Respond, менше ніж 4 години) та рівень успішності реагування — 95%, що підкреслює результативність впровадженого циклу реагування.



Рис. 4.3. Життєвий цикл реагування на інциденти інформаційної безпеки
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Фаза виявлення є початковим етапом, коли система або аналітики SOC фіксують потенційно підозрілу подію, що може свідчити про загрозу безпеці. Для цього використовуються засоби моніторингу, такі як SIEM-платформи, IDS/IPS-системи, аналіз журналів подій, мережевий моніторинг, а також засоби контролю кінцевих точок (EDR/XDR). На цьому етапі важливо

відрізнити хибні спрацьовування від реальних загроз і своєчасно класифікувати інцидент за рівнем критичності. Ефективне виявлення ґрунтується на добре налаштованих правилах кореляції, актуальних індикаторах компрометації (IoC) та постійному оновленні баз знань про атаки. Додатково на етапі виявлення важливу роль відіграє використання механізмів штучного інтелекту та машинного навчання, які дозволяють виявляти невідомі або складні аномалії у поведінці користувачів і систем. Такі моделі навчаються на історичних даних SOC і здатні автоматично формувати профілі нормальної активності, виявляючи відхилення, характерні для спроб вторгнення. Значну увагу приділяють побудові ефективної системи оповіщень, яка повинна бути достатньо чутливою, щоб не пропускати реальні атаки, але водночас мінімізувати кількість хибних тривог. Виявлені події негайно реєструються в єдиній базі даних інцидентів, де фіксуються час, джерело, тип події та рівень ризику для подальшого аналізу. Для підвищення точності виявлення SOC інтегрує зовнішні джерела даних, такі як глобальні системи Threat Intelligence, що забезпечують оновлення інформації про нові вразливості, експлойти та індикатори компрометації. У результаті цього етапу формується первинний опис інциденту, який передається на фазу аналітичної обробки для подальшого розслідування та класифікації події.

Після ідентифікації загрози **починається фаза аналізу**, яка спрямована на визначення сутності інциденту, його джерела, механізму реалізації та потенційних наслідків. Аналітики SOC проводять глибоку перевірку отриманих даних, співставляють їх із наявними розвідувальними відомостями (Threat Intelligence), аналізують ланцюги подій і поведінку зловмисників. Застосовуються методи цифрової форензики для відновлення контексту атаки, виявлення експлоїтів і збирання доказів. Метою цього етапу є побудова повної картини інциденту, визначення його масштабу, уражених компонентів системи та ступеня загрози для бізнес-процесів. На цьому етапі використовується поєднання автоматизованих засобів аналітики та експертної оцінки фахівців, що дозволяє точно визначити, чи є подія ізольованим випадком, чи частиною складнішої атаки, наприклад багатовекторної або ланцюгової (multi-stage attack). Аналітики ретельно досліджують часові мітки, лог-файли, трафік і взаємодію між вузлами, відновлюючи послідовність дій зловмисника від моменту проникнення до реалізації цілей атаки. Значна увага приділяється визначенню точки входу (entry point) — наприклад, фішингового листа, скомпрометованого облікового запису або вразливості в програмному забезпеченні. У процесі аналізу також оцінюється потенційний вплив інциденту на конфіденційність, цілісність і доступність даних, що дозволяє правильно розставити пріоритети під час реагування. Для підвищення якості оцінки використовуються бази MITRE ATT&CK, які допомагають зіставити поведінку

атакувальника з відомими техніками й тактиками. Результатом цієї фази є детальний звіт про інцидент, який містить опис виявлених загроз, оцінку ризику, рекомендації щодо нейтралізації та подальшу передачу матеріалів до етапу реагування.

Фаза реагування передбачає безпосередні дії щодо локалізації та нейтралізації інциденту. Залежно від типу загрози можуть виконуватись операції з ізоляції заражених вузлів, блокування шкідливих IP-адрес, зміни облікових даних, оновлення політик доступу чи розгортання резервних ресурсів. Використання платформ SOAR дозволяє автоматизувати типові сценарії реагування (playbooks), що суттєво скорочує час між виявленням і ліквідацією інциденту. На цьому етапі важливо дотримуватися узгоджених процедур ескалації та комунікації між усіма учасниками процесу — аналітиками, адміністраторами систем, керівництвом і зовнішніми партнерами. Ключовим завданням цієї фази є швидке стримування поширення загрози, щоб мінімізувати її вплив на критичні сервіси та дані підприємства. Для цього проводиться сегментація мережі, відключення скомпрометованих облікових записів, тимчасове обмеження доступу до ресурсів і перевірка каналів зв'язку на наявність додаткових індикаторів компрометації. У разі масштабних атак залучаються спеціалізовані команди реагування (CSIRT або CERT), які координують дії між різними підрозділами та забезпечують технічну й правову підтримку процесу. Паралельно аналітики здійснюють збір доказової бази, фіксуючи всі дії, зміни у системі та журнали подій для подальшого аналізу і документування інциденту. Значну увагу приділяють перевірці ефективності застосованих контрзаходів, оскільки невиявлені залишкові загрози можуть призвести до повторного компрометування системи. Після стабілізації ситуації формується підсумковий звіт фази реагування, у якому відображаються результати нейтралізації, часові показники (MTTD, MTTR) та рекомендації для подальшого етапу — відновлення.

Заключною є фаза відновлення, у межах якої проводяться роботи з повернення системи до штатного режиму функціонування, перевіряється цілісність даних, відновлюється нормальна робота сервісів і мережевих з'єднань. Після цього здійснюється постінцидентний аналіз (Post-Incident Review), який дозволяє виявити першопричини події, оцінити ефективність дій під час реагування та визначити заходи для запобігання подібним ситуаціям у майбутньому. Результати цього аналізу лягають в основу оновлення політик безпеки, удосконалення процедур моніторингу, навчання персоналу та розвитку технічної інфраструктури SOC. На етапі відновлення також проводиться ретельна перевірка систем на наявність прихованих шкідливих компонентів, бекдорів або залишкових вразливостей, які могли бути

непомітними під час активної фази реагування. Для цього застосовуються інструменти контролю цілісності файлів, аналіз хешів, перевірка реєстрів і конфігурацій безпеки, а також повторне сканування вразливостей. Відновлення відбувається поетапно, починаючи з критично важливих бізнес-сервісів, із застосуванням резервних копій та перевірених джерел даних. Особливу увагу приділяють тестуванню відновлених систем — проводяться перевірки працездатності, навантажувальні тести та повторні аудитні процедури для підтвердження безпечного функціонування інфраструктури. За підсумками виконаних дій створюється підсумковий звіт із детальним описом усіх заходів, часу відновлення та ефективності реалізованих рішень. Отримані результати стають основою для вдосконалення планів реагування на інциденти, підвищення рівня підготовки персоналу та формування більш зрілої системи управління кіберінцидентами підприємства.

Таким чином, життєвий цикл інциденту — це динамічний процес, у якому кожна фаза логічно пов'язана з попередньою та наступною. Безперервність цього циклу забезпечує проактивне управління кіберризиками, підвищення готовності системи до нових загроз і формування культури інформаційної безпеки, орієнтованої не лише на реагування, а й на запобігання інцидентам у майбутньому.

4.3. АВТОМАТИЗАЦІЯ РЕАГУВАННЯ ЗА ДОПОМОГОЮ SOAR

Автоматизація реагування за допомогою платформ SOAR (Security Orchestration, Automation and Response) є одним із найважливіших напрямів розвитку сучасних центрів оперативного реагування на інциденти безпеки (SOC). Вона забезпечує інтегроване керування процесами виявлення, аналізу, класифікації, реагування та звітування, поєднуючи в єдину систему інструменти моніторингу, аналітики, оркестрації та автоматичного виконання дій. Основна мета SOAR полягає у скороченні часу між виявленням інциденту та його ліквідацією, підвищенні точності рішень і зменшенні навантаження на аналітиків SOC завдяки автоматизації рутинних завдань.

На рис. 4.4 подано концептуальну модель, яка ілюструє взаємодію ключових компонентів платформи SOAR — Security Orchestration and Automation, Threat Intelligence та Security Incident Response Platform, що разом формують єдину екосистему управління інцидентами безпеки. Центральний елемент схеми — SOAR — об'єднує ці три напрями, забезпечуючи інтеграцію технологій, процесів і аналітики в межах циклу реагування на інциденти. Компонент Security Orchestration and Automation відповідає за координацію роботи різних систем безпеки (SIEM, IDS/IPS, EDR, фаєрволів, антивірусів) і виконання автоматизованих дій відповідно до визначених сценаріїв (playbooks).

Це дозволяє скоротити час реагування на загрози, мінімізувати людський фактор і підвищити узгодженість дій у межах SOC. Компонент Threat Intelligence забезпечує надходження, аналіз і використання актуальних відомостей про кіберзагрози з внутрішніх і зовнішніх джерел. Він збагачує контекст інцидентів, дозволяючи аналітикам краще розуміти природу атак, їхні джерела та можливі наслідки. Завдяки інтеграції з аналітичними базами, Threat Intelligence допомагає виявляти нові шаблони атак, створювати превентивні правила та покращувати ефективність реагування.

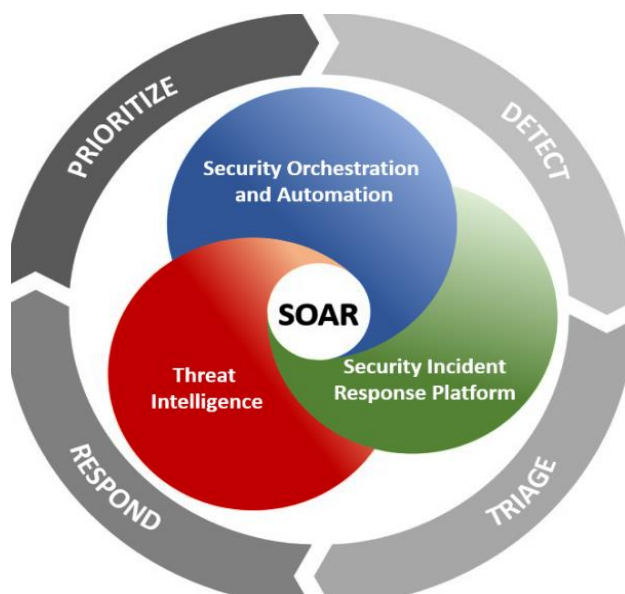


Рис. 4.4. Концептуальна модель платформи SOAR (Security Orchestration, Automation and Response) у системі кіберзахисту

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Третій елемент — Security Incident Response Platform — реалізує централізоване керування інцидентами: від моменту їхнього виявлення та класифікації до ліквідації наслідків і формування звітів. Цей модуль підтримує процес документування, ескалації та координації дій між різними учасниками команди SOC. Зовнішнє кільце схеми відображає циклічність процесу реагування, який включає етапи виявлення (Detect), оцінювання (Triage), реагування (Respond) та пріоритезації (Prioritize). Така послідовність забезпечує безперервний контроль стану безпеки, своєчасне усунення загроз і постійне вдосконалення процедур кіберзахисту. Таким чином, представлена модель демонструє, що SOAR є не просто інструментом автоматизації, а стратегічним компонентом інтелектуальної системи безпеки, який поєднує аналітику, автоматичне виконання дій і знання про загрози в єдину інтегровану платформу для підвищення кіберстійкості підприємства.

Функціонально SOAR-платформи поєднують три ключові компоненти: оркестрацію, автоматизацію та керування інцидентами. Оркестрація дозволяє інтегрувати різні системи безпеки — SIEM, IDS/IPS, EDR/XDR, фаєрволи, поштові шлюзи, системи контролю доступу, сканери вразливостей і платформи Threat Intelligence — в єдиний керований ланцюг. Автоматизація забезпечує виконання заздалегідь визначених сценаріїв реагування (playbooks), які описують покрокову послідовність дій у разі певного типу загрози. Наприклад, при виявленні фішингового листа система може автоматично ізолювати повідомлення, перевірити вкладення на наявність шкідливого коду, заблокувати відправника, повідомити користувача та створити звіт без участі аналітика. Компонент керування інцидентами дозволяє централізовано відстежувати статус кожного випадку, фіксувати хід виконання дій і взаємодію між учасниками команди реагування.

Принцип роботи платформи SOAR ґрунтується на поетапній автоматизації всього процесу реагування на інциденти, починаючи від отримання події з різних джерел до повного її закриття після усунення наслідків. У типовому сценарії робота SOAR починається з отримання сповіщення або події від SIEM-системи, антивірусного рішення, мережевого моніторингу чи зовнішніх розвідувальних джерел (Threat Intelligence). Далі система проводить автоматичну кореляцію подій, об'єднуючи кілька сигналів, що можуть стосуватися одного інциденту, і формує його профіль із зазначенням джерела, типу загрози, часу, користувача та рівня ризику.

Після первинної ідентифікації SOAR переходить до етапу аналізу, де за допомогою вбудованих правил або алгоритмів машинного навчання визначається ймовірність реальної загрози. На цьому етапі застосовуються автоматичні перевірки — аналіз URL-адрес, хешів файлів, IP-репутації, поведінкових ознак користувача, журналів подій та історії попередніх інцидентів. Якщо система підтверджує загрозу, активується відповідний playbook — набір стандартизованих дій для конкретного типу атаки, наприклад, фішинг, шкідливе ПЗ, brute-force, несанкціонований доступ тощо.

У межах цього сценарію SOAR може виконувати автоматичні дії — ізолювати заражений вузол від мережі, заблокувати обліковий запис користувача, внести IP-адресу до чорного списку, оновити правила фаєрволу, запустити сканування вразливостей або надіслати сповіщення відповідальним особам. Всі кроки виконуються у суворій послідовності, фіксуються у журналі подій та можуть супроводжуватись автоматичним формуванням звітів або аналітичних панелей (dashboards). SOAR також забезпечує механізм зворотного зв'язку — після завершення реагування система аналізує ефективність застосованих дій, оновлює базу сценаріїв і вдосконалює алгоритми реагування. Цей процес формує цикл безперервного навчання: кожен новий інцидент додає

дані для вдосконалення правил та підвищення точності автоматичних рішень у майбутньому.

Ключовою особливістю роботи SOAR є співпраця людини та машини: у разі складних або нетипових ситуацій платформа може призупинити виконання сценарію й вимагати підтвердження аналітика SOC перед виконанням критичних дій. Це дозволяє зберігати баланс між швидкістю автоматизації та контролем безпеки, уникаючи ризику помилкових рішень. Таким чином, принцип роботи SOAR полягає в оркестрації потоків даних, автоматичному аналізі загроз і виконанні дій у рамках стандартизованих сценаріїв реагування, що забезпечує скорочення часу реагування (MTTR), підвищення узгодженості дій команди, зниження кількості хибних спрацьовувань і формування замкненого циклу вдосконалення процесів безпеки в межах центру SOC.

На рис. 4.5 подано узагальнену архітектуру та логіку функціонування платформи SOAR, яка є ядром сучасних центрів оперативного реагування на інциденти безпеки (SOC). Схема демонструє, як взаємодіють основні компоненти системи — оркестрація, автоматизація, аналітика та керування інцидентами, утворюючи замкнений цикл виявлення, реагування та вдосконалення процесів безпеки. У верхній частині зображено рівень інтеграції джерел даних, який об'єднує потоки інформації з SIEM-систем, мережевих сенсорів IDS/IPS, платформ EDR/XDR, фаєрволів, антивірусів, поштових шлюзів та зовнішніх джерел Threat Intelligence. Ці дані надходять до ядра SOAR, де відбувається автоматична кореляція подій та створення єдиного профілю інциденту. На наступному рівні показано блок автоматизації сценаріїв реагування (playbooks), який реалізує заздалегідь визначені дії відповідно до типу загрози. Система автоматично виконує завдання, такі як ізоляція зараженого вузла, блокування підозрілих облікових записів, оновлення правил фаєрволу або повідомлення відповідальних осіб. Завдяки оркестрації ці дії відбуваються одночасно в різних системах безпеки, забезпечуючи швидку реакцію та узгодженість між компонентами інфраструктури.

На діаграмі також відображено механізм аналітичного зворотного зв'язку, який дозволяє системі оцінювати ефективність виконаних заходів, оновлювати правила та вдосконалювати сценарії реагування на основі накопиченого досвіду. У нижній частині схеми наведено етап керування інцидентами, що охоплює документування, аудит, створення звітів і навчання персоналу. Це забезпечує прозорість процесів SOC і формує основу для подальшого вдосконалення політик безпеки. Таким чином, представлена архітектура SOAR демонструє безперервний цикл взаємодії технологій, процесів і аналітики: від збору та кореляції подій — до автоматизованого реагування, відновлення систем і стратегічного аналізу. Вона забезпечує високу швидкість ліквідації інцидентів, мінімізує людський фактор і підвищує загальну

кіберстійкість підприємства, перетворюючи SOC із реактивного підрозділу на інтелектуальний центр проактивного управління безпекою.



Рис. 4.5. Архітектура та принцип роботи платформи SOAR (Security Orchestration, Automation and Response)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Використання SOAR значно підвищує ефективність роботи SOC завдяки можливості масштабування обробки інцидентів і зменшенню часу реагування (MTTR). Автоматизація типових операцій дозволяє аналітикам зосередитися на складних і невідомих загрозах, які потребують глибокого аналізу та експертних рішень. Крім того, SOAR забезпечує стандартизацію процесів реагування, що гарантує однакову якість виконання дій незалежно від зміни персоналу чи рівня навантаження. Кожен сценарій (playbook) може бути адаптований до конкретних вимог підприємства, політик безпеки чи регуляторних стандартів (ISO/IEC 27035, NIST SP 800-61, MITRE ATT&CK).

Важливою перевагою SOAR є можливість аналітичного зворотного зв'язку — платформа не лише виконує дії, а й аналізує результати, оновлює правила кореляції та вдосконалює механізми виявлення загроз. Вона здатна автоматично накопичувати дані про інциденти, формувати аналітичні звіти та пропонувати рекомендації на основі минулого досвіду. Інтеграція з технологіями штучного інтелекту та машинного навчання розширює можливості SOAR, дозволяючи системі самостійно визначати пріоритети інцидентів, оцінювати ризики та обирати найдоцільніший сценарій реагування.

Завдяки впровадженню SOAR підприємства досягають зменшення часу виявлення (MTTD), підвищення ефективності обробки інцидентів і зниження кількості хибних сповіщень (false positives). Крім того, платформа забезпечує прозорість управління — усі дії логуються, що дозволяє проводити аудит і

відстежувати ефективність реагування. У результаті SOC перетворюється на високоефективний аналітичний центр, здатний діяти не лише реактивно, а й проактивно, прогнозуючи загрози та автоматично вживаючи запобіжних заходів. Таким чином, автоматизація реагування за допомогою SOAR є ключовим елементом сучасної архітектури кіберзахисту. Вона об'єднує технології, людей і процеси в єдину інтегровану екосистему, що забезпечує швидкість, точність, узгодженість і безперервність дій при будь-яких інцидентах безпеки, сприяючи підвищенню кіберстійкості підприємства та оптимізації витрат на підтримку інформаційної безпеки.

4.4. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ІНТЕЛЕКТУАЛЬНОГО МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ

Використання штучного інтелекту для інтелектуального моніторингу подій безпеки є одним із ключових напрямів еволюції сучасних систем кіберзахисту та основою побудови проактивної моделі управління інцидентами в межах центрів оперативного реагування (SOC). На відміну від традиційних систем моніторингу, які спираються на сигнатурний аналіз і фіксовані правила кореляції, рішення з використанням штучного інтелекту застосовують машинне навчання, обробку великих даних і поведінкову аналітику для виявлення нових, раніше невідомих загроз. Такі системи здатні автоматично навчатися на основі історичних даних, формувати профілі нормальної активності користувачів, процесів і пристроїв, а потім виявляти відхилення, які можуть свідчити про потенційну атаку чи порушення політик безпеки. Це дає змогу значно скоротити час виявлення інцидентів, підвищити точність класифікації подій і зменшити кількість хибних сповіщень, що є критично важливим для ефективної роботи аналітиків SOC.

Інтелектуальний моніторинг подій безпеки базується на поєднанні кількох методів штучного інтелекту — машинного навчання (Machine Learning), глибокого навчання (Deep Learning), обробки природної мови (NLP) та нечіткої логіки (Fuzzy Logic). Алгоритми машинного навчання аналізують поведінкові патерни користувачів, мережевий трафік, журнали подій і системні логи, виявляючи нетипові закономірності. Моделі класифікації, такі як Random Forest, SVM, KNN або нейронні мережі, використовуються для автоматичної ідентифікації типів атак і прогнозування їхнього розвитку. Нейромережеві моделі здатні розпізнавати складні залежності між ознаками подій і виявляти приховані зв'язки, які залишаються непомітними для класичних інструментів аналізу. Застосування NLP забезпечує автоматичне оброблення неструктурованих даних — наприклад, звітів, повідомлень чи технічних

журналів, що дозволяє формувати аналітичні висновки з великого обсягу текстової інформації.

Додатково, використання нечіткої логіки (Fuzzy Logic) дає змогу системам приймати рішення в умовах невизначеності, коли подія не має чітких меж між «нормальною» та «аномальною» поведінкою. Це особливо важливо для виявлення складних багатоступеневих атак, де класичні порогові методи можуть бути неефективними. Комбінування різних підходів штучного інтелекту дозволяє створити гібридні моделі, здатні адаптуватися до змін у кіберпросторі та вдосконалювати власні алгоритми в процесі навчання. Інтелектуальні системи моніторингу постійно самонавчаються, використовуючи як поточні події, так і історичні дані для підвищення точності прогнозування та зменшення кількості хибних спрацьовувань. Вони формують динамічні профілі ризику для кожного користувача або пристрою, що дозволяє оперативно виявляти нетипову активність та визначати пріоритети реагування. Таким чином, інтеграція різних технологій штучного інтелекту в системи моніторингу подій безпеки створює основу для побудови адаптивної, самонавчальної та високоточної системи кіберзахисту нового покоління.

Особливе значення має використання штучного інтелекту для побудови систем поведінкової аналітики (UEBA — User and Entity Behavior Analytics), які відстежують дії користувачів та пристроїв, визначаючи рівень ризику кожної активності. Наприклад, якщо користувач раптово здійснює доступ до конфіденційних файлів поза робочим часом або підключається з невідомої локації, система розпізнає це як відхилення від звичного профілю та генерує попередження. Поєднання UEBA з SIEM та EDR/XDR-рішеннями дозволяє створювати багаторівневу систему аналізу, у якій штучний інтелект виконує роль «аналітичного ядра» для кореляції подій і виявлення складних багатовекторних атак.

На рис. 4.6 зображено архітектуру інтегрованої системи безпеки підприємства, яка поєднує механізми моніторингу, аналітики, оркестрації та автоматичного реагування. У центрі схеми розташовано Security Engine (Policy Engine) — ядро системи, що виконує функції кореляції подій, аналізу поведінкових моделей (Behavior Models), застосування політик безпеки (Sigma Rules) та обробки даних з різних джерел. Саме цей компонент забезпечує синтез усієї інформації, отриманої з підсистем моніторингу, і формує основу для прийняття рішень щодо подальших дій. Зліва показано джерела надходження даних: журнали подій мережі (Network/NetFlow), хмарні сервіси (Microsoft 365, Gmail, Okta), EDR-платформи (SentinelOne, CrowdStrike, Cybereason), мобільні системи безпеки (CP Harmony, CrowdStrike Mobile) та політики безпеки (MS Policy API, Nessus, CDO). Всі ці дані надходять у форматі JSON, проходять нормалізацію та об'єднуються у спільну структуру для подальшого аналізу.

Далі інформація обробляється Security Engine, який використовує внутрішні бази даних (Lava D/B) та потоки Threat Intelligence Feeds, що містять відомості про актуальні загрози, експлойти, шкідливі IP-адреси та домени. Система автоматично проводить Active Threat Hunting, виявляючи підозрілі події, поведінкові аномалії та несанкціоновані дії у мережевих потоках. На основі аналізу та політик формується рішення щодо мітки ризику інциденту, яке далі передається до підсистеми реагування.

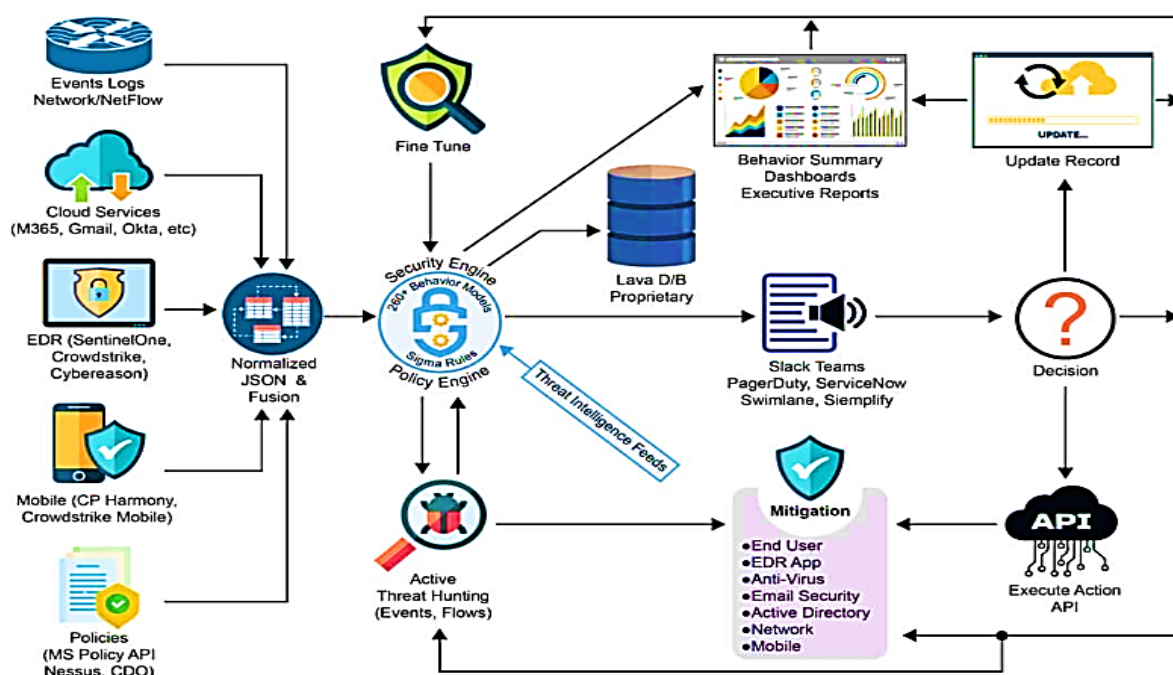


Рис. 4.6. Архітектура інтелектуального моніторингу та автоматизованого реагування на інциденти безпеки із застосуванням штучного інтелекту та платформ SOA

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Праворуч у схемі показано логіку прийняття рішень (Decision Module), що базується на результатах машинного аналізу. Якщо подія підтверджується як інцидент, ініціюється автоматизований процес реагування через API — система виконує конкретні дії за сценарієм: ізоляцію хоста, блокування облікового запису, видалення шкідливого файлу або оновлення політик доступу. Компонент Mitigation забезпечує виконання дій на рівні кінцевих користувачів, EDR-застосунків, антивірусних рішень, поштових шлюзів, Active Directory, мережевого обладнання чи мобільних пристроїв.

У верхній частині представлено блоки візуалізації та аналітики, які формують зведені звіти, дашборди й аналітичні огляди для керівництва.

Завдяки постійному оновленню записів система збагачує власну базу знань, що дозволяє коригувати моделі поведінки, оптимізувати політики й покращувати точність виявлення загроз. У процес залучені також сервіси командної взаємодії (Slack, Teams, PagerDuty, ServiceNow, Swimlane, Siemplify), які забезпечують комунікацію між аналітиками SOC та автоматичними системами реагування. Таким чином, представлена архітектура відображає повний цикл інтелектуального моніторингу — від збору та кореляції подій до ухвалення рішень і виконання дій у реальному часі. Система забезпечує високу швидкість реакції, аналітичну глибину та самонавчання, що є основою для побудови сучасного автоматизованого SOC із підтримкою штучного інтелекту.

Штучний інтелект також використовується для предиктивного аналізу кіберзагроз, який дозволяє прогнозувати можливість майбутніх інцидентів на основі поточних тенденцій, історичних даних і глобальних патернів атак. Такі моделі здатні виявляти передумови компрометації — наприклад, поступове зростання обсягу запитів до певного порту, аномальні зміни в DNS-запитах чи підвищення навантаження на окремі вузли мережі. Це дає змогу переходити від реактивного до превентивного управління безпекою, коли загроза виявляється ще до реалізації атаки. Інтеграція таких механізмів у SOC формує концепцію Cognitive Security, у якій система не лише реагує, а й самостійно робить висновки, коригує політики та пропонує оптимальні дії для аналітиків.

Інтелектуальний моніторинг із застосуванням штучного інтелекту значно підвищує ефективність обробки великих обсягів даних. Наприклад, алгоритми кластеризації дозволяють групувати схожі події, виділяючи пріоритетні для перевірки інциденти, тоді як системи ранжування за ризиками автоматично розподіляють події за рівнем критичності. Це дає змогу скоротити навантаження на аналітиків, зменшити кількість рутинних завдань і зосередитися на складних випадках, що потребують людського судження. Додатково системи AI забезпечують автоматичне формування звітів, візуалізацію трендів, побудову heatmap-діаграм активності та рекомендації щодо посилення політик безпеки.

Завдяки впровадженню штучного інтелекту SOC переходить від статичної моделі моніторингу до динамічної адаптивної системи, яка здатна вчитися, аналізувати контекст і прогнозувати поведінку атакувальників. Це формує новий рівень кіберстійкості, де система не лише реагує на інциденти, а й самостійно вдосконалює власні алгоритми, забезпечуючи безперервне вдосконалення процесів безпеки. Таким чином, штучний інтелект стає основою побудови інтелектуального SOC нового покоління, який поєднує швидкість машинної аналітики з гнучкістю людського мислення, забезпечуючи своєчасне виявлення, глибокий контекстуальний аналіз і випереджальне реагування на сучасні кіберзагрози.

4.5. ТЕХНОЛОГІЇ ПРЕДИКТИВНОГО МОНІТОРИНГУ ТА ПРОГНОЗНОГО РЕАГУВАННЯ НА ІНЦИДЕНТИ

Технології предиктивного моніторингу та прогнозного реагування на інциденти становлять новий етап розвитку систем кіберзахисту, що поєднують аналітику великих даних, штучний інтелект і машинне навчання для випереджального виявлення та нейтралізації загроз. Їхня головна мета полягає не лише у фіксації фактів атак чи інцидентів, а у передбаченні потенційних подій, які можуть вплинути на безпеку інформаційно-комунікаційної системи підприємства. На відміну від традиційних систем моніторингу, які діють реактивно — тобто реагують після виявлення загрози, предиктивний підхід дозволяє ідентифікувати ознаки майбутніх порушень завдяки аналізу закономірностей, поведінкових аномалій і тенденцій розвитку подій у кіберпросторі. Це досягається за рахунок використання прогностичних моделей, які враховують як поточні дані систем безпеки (журнали, трафік, логи), так і історичну інформацію про попередні інциденти, уразливості, патерни атак і реакції системи на них.

Основою предиктивного моніторингу є аналітика потокових даних (stream analytics) у реальному часі, що дозволяє виявляти нетипові відхилення від нормальної поведінки користувачів, додатків або мережевих з'єднань. Системи використовують алгоритми машинного та глибокого навчання (Machine Learning, Deep Learning) для побудови поведінкових профілів об'єктів — серверів, користувачів, IoT-пристроїв, мобільних клієнтів тощо. У разі, коли нова активність відхиляється від попереднього профілю, система класифікує її як потенційно небезпечну і прогнозує можливість інциденту. Такі алгоритми враховують десятки ознак, серед яких інтенсивність трафіку, час доступу, зміна привілеїв, запити до критичних файлів або сервісів, географічна локація підключення та інші поведінкові параметри.

Для досягнення високої точності прогнозів технології предиктивного моніторингу інтегруються з платформами Threat Intelligence, які забезпечують актуальну інформацію про нові види атак, шкідливі IP-адреси, домени, експлойти та тактики зловмисників. Завдяки цьому моделі прогнозування здатні враховувати не лише внутрішні дані підприємства, а й зовнішні фактори ризику. У поєднанні з системами SIEM, EDR, XDR та SOAR створюється єдина аналітична екосистема, де всі події автоматично корелюються, формуючи причинно-наслідкові ланцюги розвитку загроз. Це дозволяє виявляти складні, багатовекторні атаки ще на ранніх стадіях — наприклад, підготовку до

фішингової кампанії, несанкціоноване сканування мережі чи спроби підбору облікових даних.

Прогнозне реагування є логічним продовженням предиктивного моніторингу та полягає у випереджальному застосуванні контрзаходів, що запобігають реалізації потенційних атак. Система може автоматично змінювати політики доступу, ізолювати підозрілі вузли, оновлювати правила фаєрволу, запускати сканування вразливостей або надсилати завдання на перевірку аналітикам SOC. Завдяки механізмам адаптивного реагування платформи здатні динамічно обирати сценарій дій залежно від рівня ризику, впливу на бізнес-процеси та контексту загрози. Наприклад, якщо алгоритм прогнозує високу ймовірність експлуатації певної вразливості, система може автоматично активувати оновлення або посилити моніторинг цього сегмента мережі.

На рис. 4.7 представлено ключові напрями застосування технологій штучного інтелекту (Artificial Intelligence, AI) у сфері кібербезпеки, які забезпечують підвищення ефективності систем виявлення, запобігання та реагування на загрози. Першим елементом є *Speedier Detection* — прискорене виявлення аномалій та інцидентів за допомогою алгоритмів машинного навчання, що аналізують поведінкові патерни користувачів і систем у режимі реального часу. Другим напрямом виступає *Network Protection*, який передбачає автоматизований моніторинг трафіку та виявлення несанкціонованої активності в мережевих з'єднаннях. Третій компонент — *Anti-phishing Measures* — орієнтований на протидію фішинговим атакам через аналіз змісту електронних листів, посилань і поведінки користувачів. Четвертий напрям — *Dependable Authentication* — стосується створення надійних систем аутентифікації на основі біометричних і поведінкових параметрів, що знижує ризики компрометації облікових даних. Наступний елемент, *Behavioural Analysis*, забезпечує розпізнавання підозрілих змін у поведінці користувачів або пристроїв, що може свідчити про вторгнення чи внутрішню загрозу. Завершує модель *Defending Cybercrimes* — комплекс заходів на основі AI, які спрямовані на активне запобігання кіберзлочинам, аналіз цифрових слідів і прогнозування потенційних атак. Сукупно ці компоненти формують інтелектуальну екосистему кіберзахисту, здатну адаптуватися до нових типів загроз і діяти випереджально у сучасному цифровому середовищі.

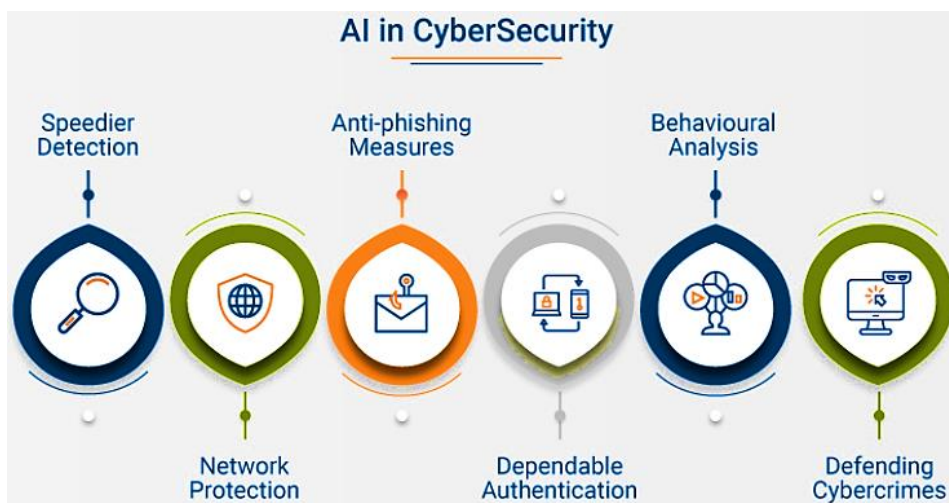


Рис. 4.7. Використання штучного інтелекту в кібербезпеці
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Ключовим елементом таких технологій є використання нейронних мереж прогнозного типу (наприклад, рекурентних LSTM- або GRU-моделей), які аналізують часові ряди подій безпеки та виявляють тенденції, що передують інцидентам. Це дозволяє оцінювати ймовірність виникнення події у певний часовий інтервал і визначати критичні точки ризику в інфраструктурі. Поєднання нейромережових моделей з алгоритмами байєсівських оцінок і нечітких правил (Fuzzy-Bayesian Inference) дає змогу враховувати невизначеність у даних і приймати зважені рішення навіть за відсутності повної інформації. Таким чином, система формує не лише реакцію, а й прогноз розвитку ситуації, що дозволяє керівництву підприємства планувати ресурси та заходи безпеки на випередження.

Результатом упровадження технологій предиктивного моніторингу та прогнозного реагування є формування інтелектуальної архітектури кіберзахисту, орієнтованої на запобігання, а не лише на усунення наслідків. Такі системи забезпечують скорочення часу виявлення загроз (MTTD) і часу реагування (MTTR), підвищують точність діагностики інцидентів і зменшують кількість хибних тривог. Вони створюють основу для побудови адаптивного SOC нового покоління, який діє проактивно, аналізує контекст у режимі реального часу та автоматично приймає рішення про відповідь на загрозу. У результаті підприємство отримує підвищену стійкість до сучасних кіберризиків, зниження операційних витрат на безпеку та можливість стратегічного прогнозування загроз у масштабах усієї інфраструктури.

4.6. ПОСТІНЦИДЕНТНИЙ АНАЛІЗ І LESSONS LEARNED

Постінцидентний аналіз і Lessons Learned є завершальним і одним із найважливіших етапів життєвого циклу управління інцидентами безпеки, оскільки саме він забезпечує перехід від реагування до вдосконалення системи кіберзахисту. Його головна мета полягає у всебічному аналізі причин, наслідків і дій, які були виконані під час ліквідації інциденту, з подальшим формуванням висновків для підвищення ефективності майбутнього реагування. Постінцидентний аналіз дозволяє не лише з'ясувати, що саме сталося, а й чому це відбулося, наскільки оперативно та ефективно спрацювали процедури реагування, які вразливості або прогалини в системі призвели до виникнення загрози.

Детальний постінцидентний аналіз охоплює як технічний, так і організаційний рівень оцінювання інциденту, забезпечуючи комплексне розуміння події. На технічному рівні здійснюється реконструкція ланцюга атаки — від моменту первинного проникнення до повного усунення наслідків, з аналізом усіх артефактів, логів, поведінкових аномалій і дій користувачів чи злоумисників. Особлива увага приділяється визначенню root cause — першопричини інциденту, тобто конкретної вразливості, помилки конфігурації або недоопрацювання в процесах безпеки, що дозволило реалізувати атаку. На організаційному рівні аналізується якість координації між командами SOC, IT-підрозділами, керівництвом і зовнішніми партнерами, а також дотримання внутрішніх політик безпеки та процедур реагування. У межах цього етапу оцінюється ефективність інструментів, таких як SIEM, SOAR, EDR або XDR, які застосовувалися для виявлення та нейтралізації загрози. Важливим результатом є визначення того, наскільки швидко вдалося локалізувати інцидент, мінімізувати збитки та запобігти повторенню подібних подій у майбутньому. Таким чином, постінцидентний аналіз виступає не лише інструментом оцінки минулого, а й стратегічним механізмом навчання, що формує основу для постійного вдосконалення політик, процедур і технологій кіберзахисту підприємства.

На рис. 4.8 представлено повний життєвий цикл управління інцидентами безпеки, який охоплює всі основні етапи — від підготовки до постінцидентного аналізу. Ця схема ілюструє безперервний процес, у якому кожен етап логічно переходить у наступний, утворюючи замкнений цикл постійного вдосконалення кіберзахисту. Етап Preparation передбачає створення політик, процедур, навчання персоналу та розгортання технічних засобів моніторингу, необхідних для своєчасного реагування на загрози. Далі йде фаза Detection, під час якої відбувається виявлення підозрілих активностей або подій за допомогою інструментів SIEM, IDS/IPS і аналітики поведінки користувачів. Етап Containment спрямований на обмеження поширення інциденту, ізоляцію уражених компонентів і мінімізацію шкоди для інфраструктури. На стадії

Eradication здійснюється усунення причин інциденту, видалення шкідливих компонентів, відновлення цілісності систем і перевірка на відсутність залишкових загроз. Фаза Recovery охоплює повернення систем до нормального режиму функціонування, тестування працездатності сервісів і перевірку ефективності впроваджених змін. Завершальний етап Post-Incident Review є ключовим для формування досвіду Lessons Learned, аналізу причин інциденту, оцінки ефективності реагування та визначення напрямів вдосконалення політик і засобів захисту. Таким чином, представлена модель відображає циклічний і динамічний характер системи реагування на інциденти, де кожен новий цикл починається з урахуванням досвіду попереднього.



Рис. 4.8. Життєвий цикл управління інцидентами безпеки (Incident Management Framework)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Процес постінцидентного аналізу починається зі збору всієї доступної інформації про інцидент — журналів подій, звітів SOC, повідомлень SIEM-систем, аналітики з EDR/XDR-платформ і звітів користувачів. Далі здійснюється кореляція подій, визначення первинної точки компрометації (root cause analysis) та відновлення повної хронології розвитку інциденту. На цьому етапі оцінюються не лише технічні аспекти, а й організаційні фактори — зокрема, якість комунікації між командами, дотримання процедур реагування, своєчасність прийняття рішень і координація між підрозділами. Це дозволяє виявити не лише технічні недоліки, а й управлінські чи людські помилки, які могли вплинути на результат.

На основі зібраних даних проводиться детальний аналіз ланцюга подій, який дозволяє простежити шлях атаки від первинного проникнення до етапу ескалації привілеїв і впливу на бізнес-процеси. Аналітики визначають, які саме вразливості або неправильно налаштовані компоненти були використані зловмисниками, і які механізми захисту не спрацювали належним чином.

Паралельно оцінюється ефективність дій співробітників SOC, швидкість реакції на інцидент і адекватність вжитих заходів із локалізації та відновлення. Важливим завданням цього етапу є визначення, чи був інцидент поодиноким випадком, чи він є частиною масштабнішої атаки або кампанії. На підставі отриманих результатів формуються практичні рекомендації щодо підвищення рівня кіберзахисту, удосконалення політик безпеки, конфігурації систем і навчання персоналу. Завершується процес підготовкою підсумкового звіту з висновками, який подається керівництву підприємства та використовується як стратегічна основа для запобігання подібним інцидентам у майбутньому.

Важливою частиною є формування звіту *Post-Incident Review (PIR)*, у якому узагальнюються ключові висновки, оцінюється ефективність використаних засобів і визначаються рекомендації щодо покращення політик безпеки. До звіту додаються детальні часові лінії подій, аналіз ланцюгів атак (kill chain), карти впливу на бізнес-процеси та пропозиції щодо модернізації систем захисту. На основі цих даних формуються коригувальні дії (Corrective Actions), спрямовані на усунення виявлених недоліків, оновлення технічних засобів, зміцнення контролів доступу чи вдосконалення процедур моніторингу. Звіт *Post-Incident Review* також містить оцінку ефективності комунікації між підрозділами під час інциденту, виявляючи можливі затримки чи непорозуміння, що вплинули на швидкість реагування. У ньому фіксуються показники часу виявлення (MTTD), реагування (MTTR) та відновлення (MTTF), що дозволяє оцінити рівень зрілості процесів кіберзахисту. Особлива увага приділяється аналізу того, як отримані уроки (Lessons Learned) можуть бути інтегровані у політики безпеки, навчальні програми для персоналу та технічні процедури. Для підвищення ефективності майбутніх дій до звіту включаються рекомендації щодо впровадження автоматизованих сценаріїв реагування, використання SOAR-платформ і розширення бази Threat Intelligence. Керівництво підприємства на основі PIR приймає рішення про оновлення інфраструктури, розподіл ресурсів і пріоритезацію проєктів безпеки. Таким чином, постінцидентний звіт стає не просто підсумком події, а стратегічним документом, який визначає подальший розвиток системи управління інформаційною безпекою підприємства.

Ключовим результатом цього етапу є створення бази знань *Lessons Learned* — систематизованого набору досвіду, який надалі використовується для навчання персоналу, оновлення інструкцій реагування та розроблення нових сценаріїв реагування (playbooks) у рамках SOAR-платформ. *Lessons Learned* забезпечують передачу практичного досвіду між аналітиками SOC, дозволяючи уникнути повторення тих самих помилок у майбутньому. Вони також стають основою для періодичних тренувань і симуляцій інцидентів (tabletop exercises), спрямованих на підвищення готовності команди реагування.

У межах бази Lessons Learned фіксуються не лише технічні аспекти інцидентів, а й організаційні уроки — наприклад, як покращити взаємодію між підрозділами, оптимізувати процедури ескалації або підвищити ефективність прийняття рішень у кризових ситуаціях. Отримані знання використовуються для формування оновлених політик безпеки, стандартів реагування та планів безперервності діяльності (Business Continuity Plans), що підвищує стійкість підприємства до майбутніх атак. Lessons Learned інтегруються у внутрішні навчальні програми, забезпечуючи постійний розвиток компетенцій співробітників SOC та IT-відділів. Для підвищення ефективності цей процес доповнюється автоматизованими аналітичними модулями, які відстежують повторюваність інцидентів і виявляють системні слабкі місця в архітектурі безпеки. На основі накопичених знань створюються динамічні сценарії реагування, що постійно вдосконалюються завдяки зворотному зв'язку між аналітиками та автоматизованими системами. Таким чином, Lessons Learned стає ключовим механізмом еволюції системи безпеки, перетворюючи кожен інцидент на джерело стратегічного вдосконалення кіберзахисту підприємства.

На рис. 4.9 зображено послідовну модель реагування на інциденти інформаційної безпеки, що складається з шести ключових етапів: Preparation (Підготовка), Identification (Ідентифікація), Containment (Локалізація), Eradication (Усунення), Recovery (Відновлення) та Post-Incident Analysis (Постінцидентний аналіз). Етап Preparation є фундаментом процесу, на якому формуються політики безпеки, створюються команди реагування, розгортаються засоби моніторингу й розробляються сценарії дій у разі інцидентів. Під час Identification система або аналітики SOC здійснюють виявлення та підтвердження факту інциденту, визначаючи його джерело, масштаб і тип загрози. На етапі Containment проводиться оперативне обмеження впливу інциденту шляхом ізоляції скомпрометованих систем, щоб запобігти подальшому поширенню атаки. Після цього виконується Eradication, що передбачає повне усунення шкідливих елементів, виправлення конфігурацій, видалення бекдорів та відновлення безпечного стану системи. Наступний етап — Recovery — спрямований на поступове повернення інфраструктури до штатного режиму роботи, тестування працездатності та перевірку стабільності. Завершує цикл Post-Incident Analysis, під час якого здійснюється детальний розбір інциденту, визначаються причини, оцінюється ефективність реагування, формуються рекомендації та оновлюються політики безпеки. Таким чином, представлена модель забезпечує замкнений процес управління інцидентами, спрямований не лише на усунення наслідків, а й на постійне вдосконалення системи кіберзахисту.

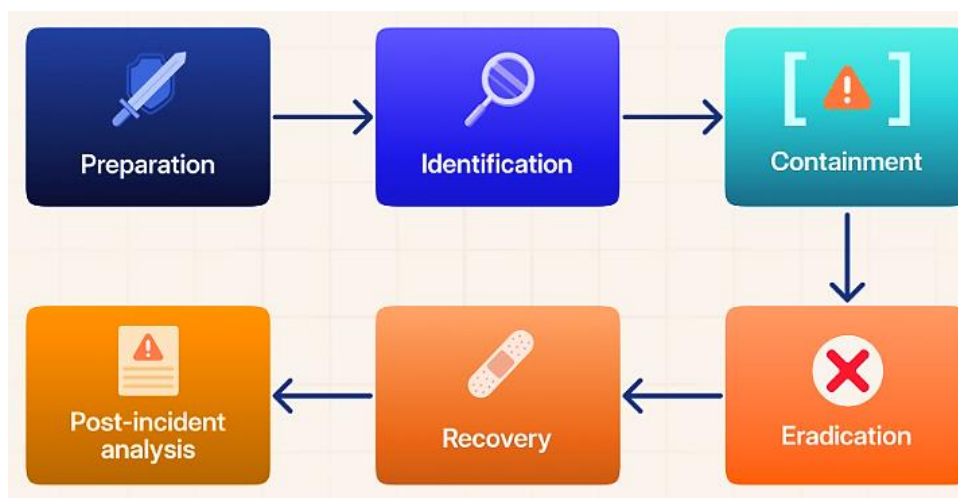


Рис. 4.9. Етапи процесу реагування на інциденти безпеки (Incident Response Process)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

У сучасних системах управління безпекою процес постінцидентного аналізу часто автоматизований і інтегрований із SIEM/SOAR-рішеннями, які збирають дані в реальному часі, формують звіти, оновлюють бази знань і відправляють аналітику керівництву. Така автоматизація значно скорочує час обробки інцидентів (MTTR) і підвищує рівень зрілості кіберзахисту підприємства. Завдяки системному підходу до постінцидентного аналізу організація отримує можливість не лише реагувати на події, а й передбачати нові загрози, вдосконалюючи свою архітектуру безпеки на основі реального досвіду. У результаті формується культура безперервного вдосконалення кіберзахисту, у якій кожен інцидент розглядається не як проблема, а як джерело знань для підвищення стійкості інформаційної системи в цілому.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 4

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication

systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.

5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.

6. Grechaninov, Viktor and Hulak, Hennadii and Sokolov, V. Y. and Skladannyi, Pavlo and Korshun, Natalia (2022) *Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center* Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. pp. 107-117. ISSN 1613-0073

7. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597.

8. Kuzminykh, I., Carlsson, A., Yevdokymenko, M., Sokolov, V. (2019). Investigation of the IoT Device Lifetime with Secure Data Transmission. In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN ruSMART 2019 2019. Lecture Notes in Computer Science(), vol 11660. Springer, Cham. https://doi.org/10.1007/978-3-030-30859-9_2

9. Buriachok, Volodymyr and Sokolov, V. Y. and Skladannyi, Pavlo (2019) *Security Rating Metrics for Distributed Wireless Systems* MoMLeT&DS. pp. 222-233. ISSN 1613-0073

10. Hu, Z.B., Buriachok, V., TajDini, M., Sokolov, V. (2021). Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_31

11. Костюк Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., Хорольська, К. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка. 2024. 1(25), 229–252.

12. Buhas, Vasyl and Ponomarenko, Ihor and Bugas, Valeriy and Ramskyi, Andrii and Sokolov, Volodymyr (2021) *Using Machine*

Learning Techniques to Increase the Effectiveness of Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 273-281. ISSN 1613-0073

13. Zhebka, V. and Skladannyi, Pavlo and Zhebka, S. and Shlianchak, S. and Bondarchuk, A. (2024) *Methodology for Predicting Failures in a Smart Home based on Machine Learning Methods* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 322-332. ISSN 1613-0073

14. Skladannyi, Pavlo and Trofimov, Olexandr and Korniets, Viktor and Vorokhob, Maksym and Opryshko, Tetiana (2023) *Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept* CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems. pp. 97-106. ISSN 1613-0073

15. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими ІОТ-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776.

16. Шевченко, Галина Володимирівна and Шевченко, Світлана Миколаївна and Жданова, Юлія Дмитрівна and Спасітелєва, Світлана Олексіївна and Негоденко, Олена Василівна (2021) *Information Security Risk Analysis SWOT* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 309-317. ISSN 1613-0073

17. I. Iosifov, O. Iosifova and V. Sokolov, "Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches," 2020 *IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 335-337, doi: 10.1109/PICST51311.2020.9468084.

18. Petriv, P. and Opirskyy, I. and Mazur, Nataliia (2024) *Modern technologies of decentralized databases, authentication, and authorization methods* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 60-71. ISSN 1613-0073

19. Astafieva, Mariia and Bodnenko, Dmitry and Lytvyn, Oksana and Proshkin, Volodymyr and Skladannyi, Pavlo (2023) *Formation of High School Students' Resistance to Destructive Information Influences* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 87-96. ISSN 1613-0073

20. Sovyn, Y. and Khoma, V. and Opirskyy, I. and Kozachok, Valerii (2023) *Minimization of Bitsliced Representation of 4×4 S-Boxes based on*

Ternary Logic Instruction Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 12-24. ISSN 1613-0073

21. Burov, O. *et al.* (2020). Cybersecurity in Educational Networks. In: Ahram, T., Karwowski, W., Vergnano, A., Leali, F., Taiar, R. (eds) *Intelligent Human Systems Integration 2020. IHSI 2020. Advances in Intelligent Systems and Computing*, vol 1131. Springer, Cham. https://doi.org/10.1007/978-3-030-39512-4_56

22. Buriachok, V., Sokolov, V. (2020). Implementation of Active Learning in the Master's Program on Cybersecurity. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, vol 938. Springer, Cham. https://doi.org/10.1007/978-3-030-16621-2_57

23. Anakhov, Pavlo and Zhebka, Viktoriia and Koretska, Viktoriia and Sokolov, V. Y. and Skladannyi, Pavlo (2022) *Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir* Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149. pp. 169-176. ISSN 1613-0073

24. Z. Hu, B. Vovkotrub, V. Buriachok, Y. Zotkin and V. Sokolov, "Bandwidth Research of Wireless IoT Switches," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 1-5, doi: 10.1109/TCSET49122.2020.235492.

25. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Abramov, Serhii and Zhylytsov, Oleksii (2022) *Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 1-10. ISSN 1613-0073

26. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Mazur, Nataliia and Ageyev, Dmytro (2021) *Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3187 (1). pp. 302-309. ISSN 1613-0073

27. Bessalov, Anatoly and Kovalchuk, L. and Sokolov, V. Y. and Skladannyi, Pavlo and Radivilova, T. (2020) *Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2746. pp. 1-13. ISSN 1613-0073

28. Bessalov, Anatolii & Grubiyan, Evgeniy & Sokolov, Volodymyr & Skladannyi, Pavlo. (2020). 3- and 5-Isogenies of Supersingular Edwards Curves. 10.48550/arXiv.2006.16111.

29. Bessalov, Anatoly and Sokolov, V. Y. and Skladannyi, Pavlo and Zhylytsov, Oleksii (2021) *Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 1-11. ISSN 1613-0073
30. V. Astapenya, V. Sokolov, P. Skladannyi and O. Zhylytsov, "Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 174-178, doi: 10.1109/PICST54195.2021.9772161.
31. V. Astapenya, V. Buriachok, V. Sokolov, P. Skladannyi and D. Ageyev, "Last Mile Technique for Wireless Delivery System using an Accelerating Lens," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 811-814, doi: 10.1109/PICST51311.2020.9467886.
32. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii (2023) *Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves* Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
33. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) *Brainwave-based authentication using features fusion* Computers & Security (129). p. 103198. ISSN 0167-4048
34. Iosifova, Olena and Iosifov, Ievgen and Rolik, Oleksandr and Sokolov, V. Y. (2020) *Techniques Comparison for Natural Language Processing* MoMLet&DS, 2631 (I). pp. 57-67. ISSN 1613-0073
35. Anakhov, P. and Zhebka, V. and Tushych, A. and Kravchenko, V. and Blazhenyi, N. and Skladannyi, Pavlo and Sokolov, Volodymyr (2022) *Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network* Journal of Theoretical and Applied Information Technology, 100 (22). pp. 6635-6644. ISSN 1817-3195
36. Y. Sadykov, V. Sokolov and P. Skladannyi, "Technology of Location Hiding by Spoofing the Mobile Operator IP Address," *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odesa, Ukraine, 2021, pp. 22-25, doi: 10.1109/UkrMiCo52950.2021.9716700.
37. Obushnyi, Sergiy and Virovets, Denis and Hulak, Hennadii and Zhurakovskiy, Bohdan (2022) *Autonomy of Economic Agents in Peer-to-Peer Systems* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 125-133. ISSN 1613-0073

38. TajDini, Mahyar and Sokolov, V. Y. and Buriachok, Volodymyr (2019) *Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio* MoMLeT&DS (2386). pp. 287-296. ISSN 1613-0073

Контрольні питання

1. Які основні функції виконує центр оперативного реагування (SOC) у системі кіберзахисту підприємства?
2. Яка різниця між SOC першого, другого та третього рівнів (Tier 1, 2, 3)?
3. Які основні компоненти та технології входять до архітектури сучасного SOC?
4. Як SIEM-платформи взаємодіють із SOC для забезпечення безперервного моніторингу подій безпеки?
5. Яку роль відіграють аналітики SOC у процесі виявлення, ескалації та реагування на інциденти?
6. Які етапи включає життєвий цикл інциденту інформаційної безпеки відповідно до стандартів ISO/IEC 27035 і NIST SP 800-61?
7. Які засоби та методи використовуються для виявлення інцидентів безпеки в корпоративних мережах?
8. У чому полягає відмінність між фазами “аналіз” і “реагування” у життєвому циклі інциденту?
9. Які основні показники ефективності (MTTD, MTTR, MTTF) застосовуються для оцінки процесу реагування на інциденти?
10. Як здійснюється фаза відновлення після інциденту та які завдання вона вирішує?
11. Що таке платформа SOAR і які основні завдання вона виконує у межах SOC?
12. Які три ключові компоненти формують функціональність SOAR-системи?
13. Як працюють сценарії реагування (playbooks) у системах SOAR і які переваги вони забезпечують?
14. У чому полягає принцип оркестрації безпеки в контексті інтеграції SIEM, IDS/IPS, EDR і SOAR?
15. Які переваги надає автоматизація реагування для зменшення часу реагування на інциденти (MTTR)?
16. Які методи штучного інтелекту найчастіше застосовуються для виявлення аномалій у системах безпеки?

17. Як алгоритми машинного навчання допомагають ідентифікувати нові або невідомі типи атак?

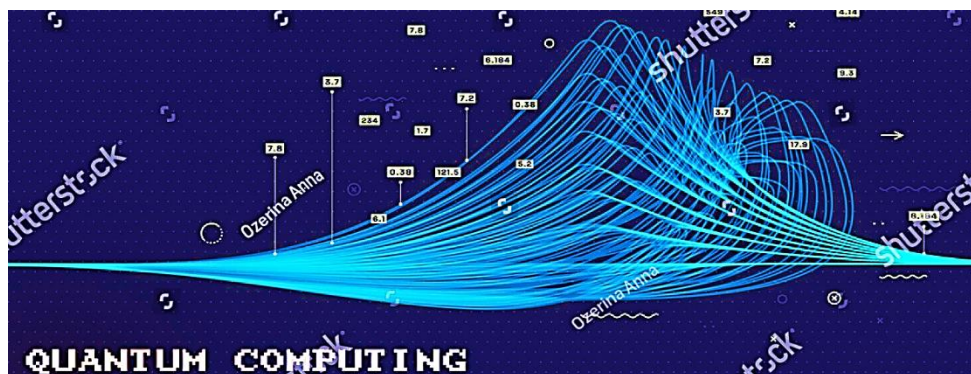
18. Яку роль відіграє обробка природної мови (NLP) у системах моніторингу кіберзагроз?

19. У чому полягає сутність предиктивного моніторингу та чим він відрізняється від традиційного підходу до виявлення інцидентів?

20. Як технології прогнозного аналізу допомагають виявляти потенційні загрози та запобігати їм на ранніх етапах?

РОЗДІЛ 5

СИНЕРГІЯ ШТУЧНОГО ІНТЕЛЕКТУ, БЛОКЧЕЙНУ ТА КВАНТОВИХ ОБЧИСЛЕНЬ У ПОБУДОВІ СИСТЕМ КІБЕРЗАХИСТУ



- 5.1. Використання штучного інтелекту та машинного навчання у виявленні кіберзагроз і аномалій поведінки**
- 5.2. Пояснюваний штучний інтелект (Explainable AI, XAI) у забезпеченні прозорості та довіри до рішень систем кіберзахисту**
- 5.3. Блокчейн-технології як основа довіри, цілісності та невідмовності в інформаційних системах**
- 5.4. Квантові обчислення та виклики для сучасної криптографії і безпеки даних**
- 5.5. актуальні підходи до концепції Zero Trust та побудови адаптивних систем захисту інформації)**

У сучасних умовах стрімкого розвитку цифрового середовища, постійного зростання обсягів даних та ускладнення кіберзагроз актуальним стає впровадження інноваційних технологій, здатних забезпечити новий рівень захисту інформації. Серед таких технологій провідне місце посідають штучний

інтелект (AI), блокчейн (Blockchain) та квантові обчислення (Quantum Computing), які формують основу майбутніх систем кібербезпеки.

Штучний інтелект відкриває нові можливості для побудови адаптивних систем захисту, здатних самостійно виявляти, аналізувати та реагувати на загрози у реальному часі. Алгоритми машинного та глибокого навчання (Machine Learning, Deep Learning) застосовуються для розпізнавання аномалій у поведінці користувачів, аналізу мережевого трафіку, прогнозування атак і зменшення кількості хибних спрацьовувань. Завдяки технологіям AI створюються інтелектуальні SOC-центри, де процеси моніторингу, аналізу та реагування автоматизовані через SOAR-платформи. Крім того, моделі штучного інтелекту здатні постійно вдосконалюватися, навчаючись на історичних даних, що дозволяє підвищувати точність виявлення нових типів атак.

Блокчейн є технологією розподілених реєстрів, яка забезпечує цілісність, достовірність і прозорість зберігання даних без потреби у централізованому посереднику. У сфері інформаційної безпеки блокчейн використовується для захисту транзакцій, управління цифровими ідентичностями, побудови децентралізованих систем автентифікації та контролю доступу. Завдяки криптографічним механізмам хешування та неможливості зміни записів, технологія забезпечує високий рівень довіри та невідомості дій. У корпоративних і державних системах блокчейн дедалі частіше застосовується для аудиту операцій, захисту журналів подій і створення перевірених ланцюгів постачання даних (data provenance).

Квантові обчислення формують нову парадигму безпеки, що поєднує величезну обчислювальну потужність з новими методами шифрування. З одного боку, квантові комп'ютери створюють загрозу для традиційних криптографічних алгоритмів (RSA, ECC), які можуть бути розшифровані значно швидше за допомогою квантових алгоритмів, таких як алгоритм Шора. З іншого боку, вони відкривають шлях до розробки постквантової криптографії (PQC), яка базується на складних математичних задачах, стійких до квантових атак. Крім того, квантові технології, зокрема квантова дистрибуція ключів (QKD), дозволяють створювати абсолютно безпечні канали зв'язку, де будь-яка спроба перехоплення одразу виявляється через зміну квантового стану.

Отже, поєднання штучного інтелекту, блокчейну та квантових обчислень визначає новий вектор розвитку систем інформаційної безпеки. Ці технології забезпечують перехід від реактивних до проактивних моделей кіберзахисту, підвищують стійкість інфраструктури до складних загроз, створюють довірчі середовища обміну даними та формують основу для майбутньої інтелектуальної, децентралізованої і квантово-стійкої архітектури безпеки.

5.1. ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ У ВИЯВЛЕННІ КІБЕРЗАГРОЗ І АНОМАЛІЙ ПОВЕДІНКИ

Використання штучного інтелекту (Artificial Intelligence, AI) та машинного навчання (Machine Learning, ML) у виявленні кіберзагроз і аномалій поведінки є одним із найефективніших напрямів розвитку сучасних систем інформаційної безпеки. У традиційних підходах до кіберзахисту основний акцент робився на сигнатурному аналізі, тобто розпізнаванні вже відомих атак на основі фіксованих шаблонів. Проте такий метод виявився малоефективним у боротьбі з новими, складними або цільовими атаками (APT), які постійно змінюють свої характеристики. Саме тому технології AI/ML відкрили можливість переходу до поведінкової аналітики (Behavioral Analytics), де система не лише розпізнає загрози за відомими ознаками, а й вчиться ідентифікувати відхилення від нормальної діяльності користувачів, процесів чи мережевих вузлів.

На рис. 5.1 представлено основні напрями застосування технологій штучного інтелекту (AI) та машинного навчання (ML) у системах кіберзахисту, які формують комплексну архітектуру інтелектуального моніторингу й реагування на загрози. Першим етапом є проактивне виявлення загроз (Proactive Threat Detection), яке дає змогу ідентифікувати потенційні атаки ще до їх реалізації завдяки аналізу поведінкових шаблонів і відхилень від норми. Другим напрямом є автоматизоване реагування на інциденти (Automated Incident Responses), що забезпечує швидке блокування шкідливої активності та мінімізацію людського втручання. Третій компонент — поведінковий аналіз і моніторинг користувачів (Behavioral Analysis & User Monitoring) — передбачає створення профілів нормальної активності користувачів і виявлення аномалій, які можуть свідчити про інсайдерські або несанкціоновані дії.

Далі важливу роль відіграє виявлення вторгнень на основі аномалій (Anomaly-Based Intrusion Detection), де алгоритми машинного навчання аналізують трафік, системні події та взаємодії у мережі для розпізнавання невідомих типів атак, включно з zero-day загрозами. П'ятий напрям — розвідка загроз і прогнозування (Threat Intelligence & Prediction) — базується на використанні аналітики великих даних і нейронних мереж для передбачення можливих сценаріїв атак і побудови моделі поведінки зловмисників. Завершальним елементом є виявлення фішингових атак (Phishing Detection), де системи на основі штучного інтелекту аналізують тексти електронних листів, посилення, метадані та поведінкові сигнали користувача для запобігання соціальній інженерії та викраденню облікових даних. Загалом, наведена схема демонструє синергію аналітичних, прогностичних і автоматизованих можливостей AI/ML, які формують інтелектуальну екосистему кіберзахисту,

здатну самонавчатися, адаптуватися до нових загроз і забезпечувати безперервний моніторинг інформаційної безпеки в реальному часі.



Рис. 5.1. Використання штучного інтелекту та машинного навчання у виявленні кіберзагроз і аномалій поведінки

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Машинне навчання дозволяє системам безпеки аналізувати великі масиви даних із різних джерел — журналів подій, мережевого трафіку, систем автентифікації, IoT-пристроїв та хмарних сервісів — і виділяти приховані закономірності. Алгоритми класифікації, такі як Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN), а також нейронні мережі (CNN, LSTM, Autoencoders), використовуються для автоматичної ідентифікації типів атак і прогнозування ймовірності інцидентів. Наприклад, за допомогою рекурентних нейромереж (LSTM) можна аналізувати часові ряди подій безпеки та виявляти підозрілі патерни, які передують спробам проникнення або несанкціонованому доступу.

Машинне навчання (Machine Learning, ML) є ключовим інструментом у сучасних системах кіберзахисту, оскільки воно дозволяє автоматизувати аналіз величезних обсягів даних, які постійно генеруються інформаційними системами. Ці дані можуть надходити з різних джерел — журналів подій (system logs), мережевого трафіку, систем контролю автентифікації, IoT-пристроїв, хмарних сервісів, серверів баз даних і кінцевих точок. У звичайних умовах обсяг таких даних настільки великий, що їхня ручна обробка є неможливою, тому саме ML дозволяє ефективно структурувати, очищувати, нормалізувати та аналізувати інформацію в режимі реального часу. Основна мета полягає у виявленні прихованих закономірностей і відхилень від нормальної поведінки, які можуть

свідчити про кіберзагрози, навіть якщо вони ще не мають сигнатур чи відомих ознак.

Алгоритми машинного навчання діляться на наглядові (supervised), ненаглядові (unsupervised) та гібридні (semi-supervised) методи. У наглядovому навчанні, наприклад, використовуються історичні дані про відомі атаки для тренування моделей, що дозволяє системі класифікувати нові події за аналогією з уже відомими патернами. Одним із найпоширеніших алгоритмів такого типу є Random Forest, який створює ансамбль рішень (decision trees) і на їхній основі формує статистичне рішення щодо типу або класу загрози. Іншим прикладом є Support Vector Machine (SVM) — алгоритм, що розділяє дані за допомогою гіперплощини, дозволяючи чітко відмежовувати нормальні дії від потенційно шкідливих. Такі методи особливо ефективні при виявленні фішингових атак, спроб брутфорсу або підозрілих входних з'єднань.

Для складніших сценаріїв застосовуються ненаглядові методи, такі як K-Nearest Neighbors (KNN) або Autoencoders, які здатні виявляти нові, невідомі раніше аномалії, що не підпадають під відомі шаблони. Наприклад, Autoencoders можуть навчатися на нормальних даних і сигналізувати про будь-яку подію, яка не вписується у звичний профіль системи, що особливо корисно для виявлення інсайдерських загроз або zero-day атак.

Нейронні мережі, зокрема Convolutional Neural Networks (CNN), використовуються для аналізу структурованих даних або візуалізацій трафіку, що дозволяє виявляти складні просторові взаємозв'язки між подіями. У той же час Recurrent Neural Networks (RNN), а особливо їхні розширення — Long Short-Term Memory (LSTM) — ефективно працюють із часовими рядами даних, які притаманні системам безпеки. Це дає змогу аналізувати послідовність подій, виявляючи підозрілі закономірності, що можуть вказувати на початок підготовки атаки. Наприклад, LSTM-моделі можуть виявити ланцюжок дій, характерних для багатовекторної атаки: спочатку сканування портів, потім спроба входу з різних IP-адрес, і, нарешті, передача даних у невідомий зовнішній домен.

У більш складних сценаріях ML використовується для прогнозування ймовірності інцидентів. Це досягається шляхом побудови моделей, що враховують історичні події, контекст середовища, поведінку користувачів і стан мережі. Наприклад, якщо алгоритм фіксує нетипову активність користувача під час вихідних днів або з нового пристрою, він може автоматично підвищити рівень ризику й ініціювати процедури додаткової перевірки.

На рис. 5.2 представлено основні переваги застосування методів машинного навчання (Machine Learning, ML) у процесах виявлення аномалій у системах кіберзахисту. Центральним елементом схеми є концепція ML Anomaly Detection, що забезпечує автоматичне виявлення відхилень від нормальної поведінки користувачів, пристроїв або процесів у реальному часі. Завдяки цим

технологіям досягається адаптивна продуктивність (Adaptive Performance) — система здатна самонавчатися та підлаштовуватися під змінні умови кіберсередовища без потреби у постійному втручанні людини. Одночасно відбувається спрощення керування системою (Simpler System Handling), адже алгоритми ML автоматизують процеси аналізу логів, мережевого трафіку та поведінкових даних, зменшуючи навантаження на аналітиків SOC. Використання машинного навчання сприяє значній економії часу (Time Saving) — автоматичні моделі можуть обробляти великі обсяги інформації за лічені секунди, виявляючи потенційні загрози швидше, ніж традиційні методи. Це, у свою чергу, забезпечує зниження ризиків (Risk Reduction), оскільки система здатна прогнозувати інциденти ще до їхнього настання, попереджаючи компрометацію або витік даних. Важливою перевагою є підвищення надійності (Reliability Increasing), адже моделі ML зменшують кількість хибних спрацьовувань і підвищують точність ідентифікації загроз.

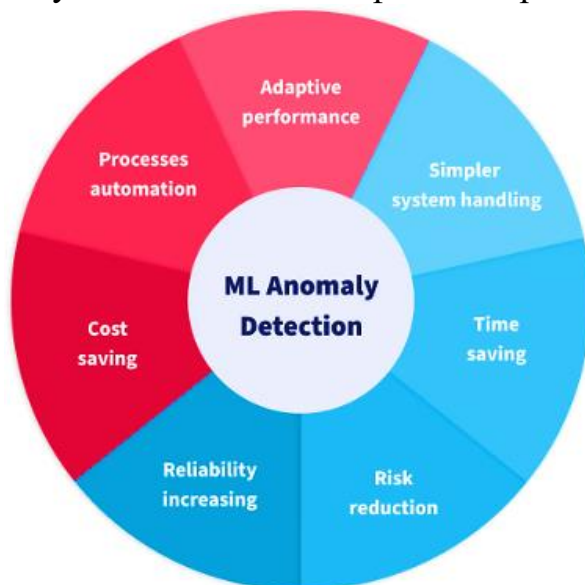


Рис. 5.2. Переваги використання машинного навчання у виявленні аномалій (ML Anomaly Detection)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Крім того, технології машинного навчання дозволяють оптимізувати витрати (Cost Saving), зменшуючи потребу у великих командах аналітиків і скорочуючи час простоїв систем у разі інцидентів. Останнім, але не менш важливим аспектом є автоматизація процесів (Processes Automation), що дає змогу забезпечити безперервний моніторинг і реагування у режимі 24/7, підвищуючи рівень кіберстійкості підприємства. Загалом, наведена схема демонструє, що впровадження ML у виявлення аномалій забезпечує не лише

підвищення ефективності кіберзахисту, а й створює умови для побудови інтелектуальної, адаптивної та економічно доцільної системи безпеки.

Важливою характеристикою ML-систем є здатність самонавчатися, тобто оновлювати свої моделі на основі нових даних. Це дозволяє постійно адаптуватися до змін у кіберпросторі, нових типів атак і стратегій зловмисників. У результаті машинне навчання стає ядром адаптивного кіберзахисту, що не лише реагує на відомі загрози, а й прогнозує нові, формуючи динамічну, стійку до змін модель безпеки. Таким чином, ML є не просто допоміжною технологією, а фундаментом для побудови інтелектуальних систем виявлення й реагування на кіберзагрози (IDS/IPS, SIEM, EDR, XDR). Його впровадження дозволяє перейти від реактивної моделі безпеки до прогнозно-аналітичної, де кожна подія розглядається як елемент складної поведінкової картини, що піддається аналізу, узагальненню й передбаченню.

Завдяки навчальним моделям на основі великих даних (Big Data Analytics) системи здатні не лише фіксувати порушення, а й визначати ступінь ризику кожної події, автоматично ранжуючи загрози за критичністю. Це дозволяє аналітикам SOC (Security Operations Center) зосередитися на найважливіших інцидентах і уникати перевантаження хибними тривогами (false positives). Використання методів кластеризації (наприклад, K-means, DBSCAN) допомагає виявляти невідомі типи атак або нові поведінкові шаблони, які не були описані у попередніх базах знань.

Особливої актуальності набуває інтеграція AI/ML із системами SIEM (Security Information and Event Management), де машинні алгоритми виконують автоматичну кореляцію подій, виділяють аномалії та генерують оповіщення у реальному часі. У поєднанні з технологіями EDR/XDR (Endpoint/Extended Detection and Response) це створює багаторівневу екосистему аналізу поведінки, здатну не лише виявляти, а й прогнозувати потенційні атаки на основі попередніх інцидентів.

Штучний інтелект також активно використовується в системах User and Entity Behavior Analytics (UEBA), які формують поведінкові профілі користувачів і пристроїв. Якщо система виявляє, що користувач діє нетипово (наприклад, підключається з іншої геолокації або завантажує незвично великі обсяги даних), вона автоматично ініціює перевірку чи блокує доступ. Такий підхід значно підвищує точність і швидкість реагування, адже система здатна самостійно виявляти складні багатовекторні атаки, включно з інсайдерськими загрозами.

Додатково AI використовується у прогнозному аналізі кіберризиків, коли моделі глибокого навчання (Deep Learning) оцінюють потенційний розвиток інцидентів на основі поточних тенденцій і контексту подій. Це дає змогу перейти від реактивного до проактивного підходу, коли система запобігає загрозам ще до їхньої реалізації. У поєднанні з технологіями SOAR (Security Orchestration,

Automation and Response) та Threat Intelligence штучний інтелект формує адаптивну архітектуру кіберзахисту, де кожен новий інцидент стає джерелом навчання для майбутнього вдосконалення системи.

Таким чином, використання AI та ML у сфері кібербезпеки забезпечує якісно новий рівень захисту — від виявлення до прогнозування загроз. Ці технології дозволяють автоматизувати процеси моніторингу, підвищити точність аналізу, зменшити людський фактор і забезпечити гнучке реагування на динамічний ландшафт кіберризиків. У перспективі їх поєднання з пояснюваними моделями (XAI) та квантово-стійкими рішеннями стане основою інтелектуальної екосистеми кіберзахисту, здатної діяти випереджально та самонавчатися в умовах змінного кіберпростору.

5.2. ПОЯСНЮВАНИЙ ШТУЧНИЙ ІНТЕЛЕКТ (EXPLAINABLE AI, XAI) У ЗАБЕЗПЕЧЕННІ ПРОЗОРОСТІ ТА ДОВІРИ ДО РІШЕНЬ СИСТЕМ КІБЕРЗАХИСТУ

Пояснюваний штучний інтелект (Explainable Artificial Intelligence, XAI) є ключовим напрямом розвитку сучасних інтелектуальних систем кіберзахисту, спрямованим на підвищення рівня довіри, прозорості та обґрунтованості автоматизованих рішень. У традиційних моделях штучного інтелекту, зокрема нейронних мережах глибинного навчання (Deep Learning), процес прийняття рішень часто залишається «чорним ящиком» — тобто аналітики не можуть пояснити, чому система класифікувала певну подію як загрозу або, навпаки, як безпечну. Це створює ризики неправильного реагування, знижує рівень довіри до алгоритмів і ускладнює впровадження автоматизованих рішень у критичних середовищах. Саме тому XAI забезпечує механізми інтерпретації та пояснення результатів, роблячи процес прийняття рішень системи зрозумілим для аналітиків безпеки, керівників і аудиторів.

У контексті кібербезпеки пояснюваний штучний інтелект виконує подвійну функцію — підвищує ефективність виявлення загроз і зміцнює довіру до результатів аналітичних моделей. Алгоритми XAI дозволяють визначати, які саме фактори або входні ознаки вплинули на рішення системи — наприклад, чому конкретна активність користувача була класифікована як фішинг, спроба несанкціонованого доступу чи аномальна поведінка. Це забезпечується за допомогою методів локальної інтерпретації, таких як LIME (Local Interpretable Model-agnostic Explanations) або SHAP (SHapley Additive exPlanations), які дають змогу аналізувати вплив кожного параметра на кінцевий результат. Таким чином, аналітики SOC (Security

Operations Center) отримують не лише сигнал про інцидент, а й контекст — які події, дії користувача або параметри трафіку призвели до спрацювання моделі.

Однією з головних переваг ХАІ є підвищення відповідальності й довіри до систем автоматизованого реагування (SOAR), які використовують AI/ML для прийняття рішень у режимі реального часу. Завдяки пояснюваності можна не лише зрозуміти причини спрацювання, а й виявити помилки у моделі, наприклад, упередженість алгоритму або помилкове навчання на некоректних даних. Це дає змогу вчасно коригувати модель, підвищуючи її точність і зменшуючи кількість хибних сповіщень (false positives). Важливим аспектом є і дотримання нормативних вимог, зокрема у сферах критичної інфраструктури та фінансових послуг, де рішення систем безпеки мають бути обґрунтованими та відтворюваними. Пояснюваний AI допомагає забезпечити відповідність стандартам ISO/IEC 27001, NIST SP 800-53, GDPR і DORA, які вимагають прозорості процесів обробки даних і управління ризиками.

ХАІ також відіграє ключову роль у навчанні та підтримці аналітиків SOC. Коли система пояснює свої дії, фахівці можуть швидше зрозуміти логіку роботи моделей, удосконалювати правила кореляції подій і формувати більш точні політики безпеки. Це створює ефект зворотного зв'язку між людиною та алгоритмом, сприяючи розвитку гібридного інтелекту (Human-AI Collaboration) — концепції, за якої людина та AI спільно приймають рішення, використовуючи свої сильні сторони: аналітичне мислення оператора і швидкість обробки даних системи. Завдяки цьому зростає точність і швидкість реагування на інциденти, а також формується довгострокова довіра між користувачами та системою.

Пояснюваний штучний інтелект допомагає аналітикам не лише розуміти, чому саме система прийняла певне рішення, але й бачити логіку її міркувань у контексті реальних загроз. Це дає змогу ефективніше навчати нових співробітників SOC, демонструючи їм причинно-наслідкові зв'язки між подіями, правилами кореляції та результатами аналізу. ХАІ створює інтерактивне середовище навчання, де оператори можуть експериментувати з параметрами моделі та одразу бачити, як зміна ознак впливає на результат класифікації інциденту. Крім того, пояснювані моделі дозволяють виявляти приховані закономірності у поведінці загроз, які залишаються непомітними при традиційному аналізі. Такий підхід сприяє розвитку культуральної кіберграмотності у команді безпеки, де рішення AI сприймаються не як «чорна скринька», а як зрозумілий і керований інструмент. У результаті формується синергетична взаємодія людини та технології, що підвищує рівень довіри, прозорості та ефективності всього процесу кіберзахисту.

Ще одним важливим напрямом застосування ХАІ є оцінка стійкості моделей безпеки до атак на штучний інтелект (Adversarial Attacks). Пояснювані моделі дозволяють виявляти слабкі місця в алгоритмах, які зловмисники можуть використати для обходу захисту. Аналіз впливу вхідних даних допомагає підвищити надійність систем, адаптуючи їх до потенційних маніпуляцій. У результаті системи ХАІ формують прозору екосистему кіберзахисту, де кожне рішення має зрозуміле пояснення, а довіра між людиною та технологією базується на обґрунтованих і перевірених результатах.

На рис. 5.3 представлено узагальнену архітектуру застосування пояснюваного штучного інтелекту (Explainable Artificial Intelligence, ХАІ) у системах кіберзахисту, що забезпечує прозорість і довіру до автоматизованих рішень. У верхній частині схеми зображено різні джерела подій безпеки (security events): дії користувачів, мережеві з'єднання, журнали системних подій, запити до серверів та інші типи взаємодій. Ці дані потрапляють до модуля обробки даних (Data processing), який виконує фільтрацію, нормалізацію та агрегацію інформації для подальшого аналізу. Наступний етап — AI-модель (AI model), яка класифікує події як безпечні (benign), підозрілі (suspicious) або шкідливі (malicious). Модель може базуватись на алгоритмах машинного навчання, таких як нейронні мережі, дерева рішень або ансамблеві методи, що аналізують великі масиви телеметричних даних із мережевого трафіку, логів EDR/XDR, SIEM-систем та аналітики Threat Intelligence.

Після класифікації результат потрапляє до шару інтерпретації (Interpretability layer), який реалізує механізми пояснюваного штучного інтелекту за допомогою методів LIME (Local Interpretable Model-Agnostic Explanations) та SHAP (SHapley Additive Explanations). Цей модуль пояснює логіку прийнятих рішень — тобто, які саме параметри або ознаки вплинули на оцінку події як загрози. Це дозволяє аналітикам безпеки зрозуміти, чому система класифікувала активність користувача певним чином, а також перевірити коректність роботи моделі. Важливим елементом архітектури є зворотний зв'язок (Feedback loop), який забезпечує безперервне вдосконалення моделі на основі рішень аналітиків SOC. Інформація про правильність чи помилковість класифікації повертається до AI-модуля для перенавчання, що підвищує точність і зменшує кількість хибних спрацювань. На правій частині схеми показано взаємодію із системою SOAR (Security Orchestration, Automation and Response), куди надходять результати інтерпретованих рішень для автоматизованого реагування, генерації звітів та виконання дій з усунення загроз.

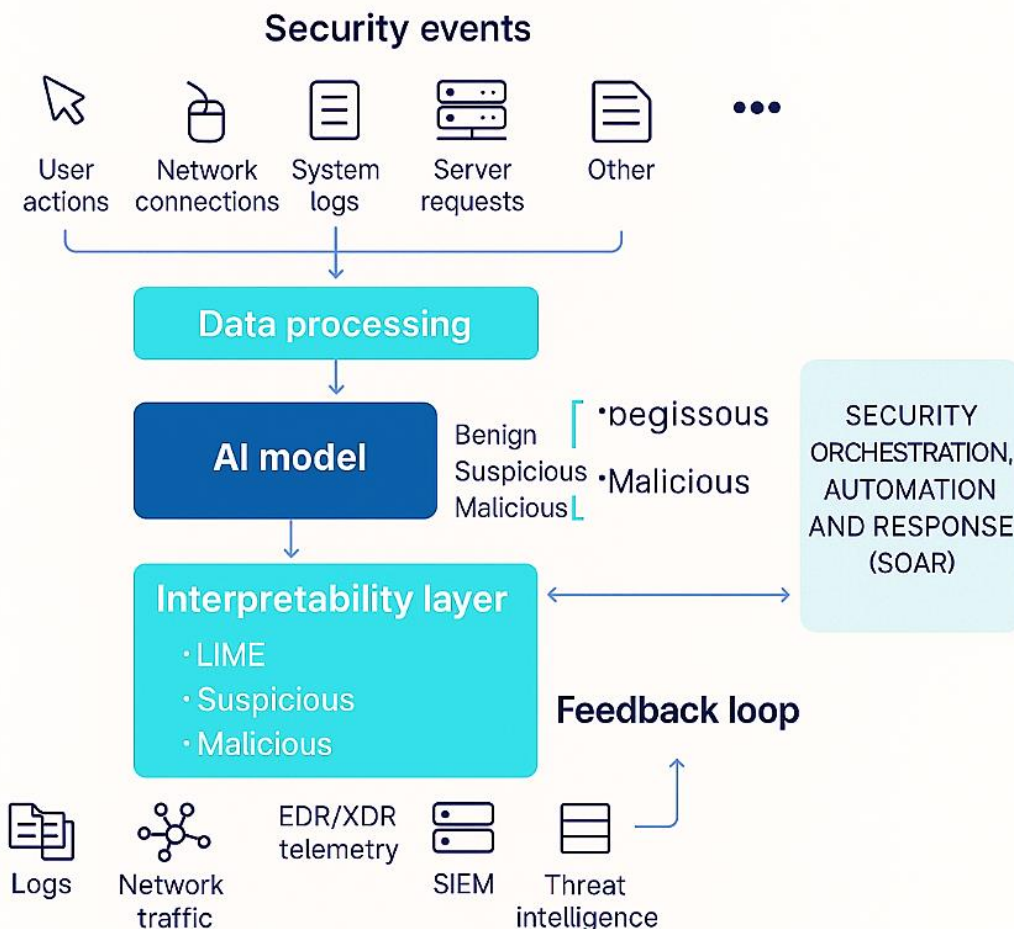


Рис. 5.3. Архітектура пояснюваного штучного інтелекту (XAI) у системах кіберзахисту

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Таким чином, пояснюваний штучний інтелект є не лише технічною інновацією, а й концептуальним кроком до етичного, відповідального та надійного використання AI у сфері безпеки. Він створює основу для формування довіри до автономних систем, дозволяє організаціям контролювати процес прийняття рішень і підвищує загальний рівень кіберстійкості. У перспективі XAI стане невід'ємною частиною інтелектуальних платформ кіберзахисту нового покоління, які не лише виявляють і прогнозують загрози, але й пояснюють, чому саме вони приймають ті чи інші рішення, роблячи безпеку більш зрозумілою, керованою та передбачуваною.

5.3. БЛОКЧЕЙН-ТЕХНОЛОГІЇ ЯК ОСНОВА ДОВІРИ, ЦІЛІСНОСТІ ТА НЕВІДМОВНОСТІ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Блокчейн-технології є фундаментальною основою довіри, цілісності та невідмовності в сучасних інформаційних системах, забезпечуючи прозоре, децентралізоване та стійке до маніпуляцій середовище зберігання і передачі даних. На відміну від традиційних централізованих моделей, де управління інформацією здійснюється єдиним посередником, блокчейн базується на розподіленому реєстрі (Distributed Ledger), у якому кожен учасник мережі має копію всієї історії транзакцій. Це гарантує, що жодна зі сторін не може змінити або видалити дані без відома інших учасників, що робить систему практично невразливою до підробки чи несанкціонованого втручання.

Цілісність даних у блокчейні забезпечується за допомогою криптографічного хешування, де кожен блок містить хеш попереднього, утворюючи безперервний ланцюг взаємопов'язаних елементів. Зміна хоча б одного байта інформації у попередньому блоці спричиняє зміну всього ланцюга, що миттєво фіксується всіма вузлами мережі. Такий механізм створює високий рівень достовірності та верифікованості даних, роблячи блокчейн ідеальним інструментом для аудиту, цифрового обліку подій і контролю цілісності файлів, логів або транзакцій. Крім того, хеш-функції у блокчейні використовуються не лише для захисту структури ланцюга, а й для забезпечення незаперечності походження даних — кожен блок має унікальний цифровий відбиток, який неможливо підробити або згенерувати повторно без зміни вмісту. Завдяки цьому будь-яка спроба несанкціонованого редагування або видалення записів стає одразу очевидною для всіх учасників мережі. У розподілених середовищах така властивість дозволяє створювати незмінні журнали дій (immutable logs), де фіксуються всі операції без можливості їх ретроспективного виправлення. Це особливо важливо для критичних систем, де прозорість і точність історії подій мають визначальне значення — наприклад, у фінансовому моніторингу, кіберфорензіці чи системах електронного документообігу. Хешування також дає змогу ефективно перевіряти автентичність даних у розподілених вузлах, не передаючи самі дані, що знижує ризик їх перехоплення або компрометації. У результаті забезпечується високий рівень довіри до інформації, адже кожен елемент блокчейна підтверджує цілісність і достовірність попереднього, формуючи незламний ланцюг безпеки.

Ще одним важливим аспектом є невідмовність (non-repudiation), тобто неможливість сторін заперечити факт своєї участі в транзакції. Завдяки цифровим підписам і децентралізованим механізмам консенсусу (Proof of

Work, Proof of Stake, Practical Byzantine Fault Tolerance) кожна дія в системі підтверджується колективно, а не централізовано. Це означає, що будь-яка транзакція, записана в блокчейн, є невідомою і незмінною, що суттєво підвищує рівень довіри у міжорганізаційних взаємодіях, фінансових операціях, електронному документообігу та управлінні ідентичністю.

Невідомість у блокчейн-системах є одним із ключових принципів забезпечення довіри, адже вона гарантує, що жодна зі сторін не може відмовитися від своїх дій після їхнього здійснення. Це досягається завдяки використанню цифрових підписів, що базуються на криптографії з відкритим ключем (Public Key Infrastructure, PKI). Кожен учасник мережі має унікальну пару ключів — приватний і публічний, де приватний використовується для підписання транзакції, а публічний — для її перевірки іншими вузлами. У результаті створюється надійний механізм автентифікації дій, який підтверджує, що певна транзакція ініційована саме конкретним користувачем і не може бути підроблена без знання його приватного ключа.

Додаткову гарантію незмінності надають механізми консенсусу, які колективно затверджують кожен запис у розподіленому реєстрі. Наприклад, у моделі Proof of Work (PoW) підтвердження транзакцій здійснюється шляхом розв'язання складних математичних задач, що потребують значних обчислювальних ресурсів, а отже, унеможливлюють фальсифікацію блоків. У системі Proof of Stake (PoS) підтвердження базується на частці (stake), яку користувач володіє у мережі, стимулюючи чесну поведінку учасників, оскільки їхня довіра ґрунтується на фінансовій відповідальності. Алгоритми Practical Byzantine Fault Tolerance (PBFT) забезпечують узгодженість рішень навіть за наявності потенційно зловмисних або несправних вузлів, гарантуючи стабільність системи без єдиного центру управління.

Завдяки поєднанню цифрових підписів і консенсусних алгоритмів блокчейн створює прозору, верифіковану та юридично значущу історію подій, де кожна транзакція має однозначного автора, час і підтвердження мережі. Це забезпечує невідомість не лише на технічному, а й на правовому рівні — дії користувачів можна відстежити, перевірити й підтвердити незалежно від їхньої волі. У контексті корпоративних і міжорганізаційних відносин такий підхід мінімізує ризики шахрайства, маніпуляцій і спорів, підвищуючи довіру до систем електронного документообігу, цифрових контрактів і розподілених фінансових сервісів. Таким чином, невідомість у блокчейні формує фундаментальний рівень кібердовіри, де кожна дія є не лише зафіксованою, а й підтвердженою колективно, що перетворює блокчейн на еталонну технологію забезпечення

відповідальності, надійності та правової значущості у цифровому середовищі.

Поєднання цифрових підписів, криптографічного хешування та консенсусних алгоритмів у блокчейні створює цілісну, достовірну й юридично підтверджену історію подій, що забезпечує найвищий рівень прозорості та підзвітності у цифрових взаємодіях. Кожна транзакція в мережі супроводжується унікальним цифровим підписом, який однозначно ідентифікує її автора, час створення та підтвердження іншими вузлами мережі. Завдяки цьому блокчейн не лише фіксує факт дії, а й гарантує її автентичність і незмінність, що є критично важливим для розв'язання питань юридичної відповідальності та доказовості цифрових подій. Такі властивості роблять технологію надзвичайно ефективною у сферах, де необхідно гарантувати довіру між сторонами без посередників — наприклад, у системах смартконтрактів, цифрового документообігу, електронного голосування, реєстрації прав власності чи аутентифікації користувачів.

На рис. 5.4 зображено узагальнену архітектуру блокчейн-системи, яка забезпечує довіру, цілісність і невідомність у розподілених інформаційних середовищах. У центрі схеми розташовано ланцюг блоків (Blockchain Ledger), де кожен блок містить криптографічний хеш попереднього, формуючи неперервну структуру даних, захищену від підробки чи несанкціонованого редагування. На кожному етапі обробки інформації застосовуються криптографічні підписи, які гарантують автентичність транзакцій і підтверджують авторство кожної дії. Навколо ланцюга зображено вузли мережі (Nodes), що беруть участь у колективному затвердженні транзакцій за допомогою механізмів консенсусу — Proof of Work, Proof of Stake або PBFT, що забезпечують узгодженість рішень без централізованого контролю.

Завдяки такій структурі досягається прозорість та надійність усіх записів, оскільки кожен вузол має копію реєстру, а будь-яка спроба змінити дані миттєво виявляється мережею. У нижній частині схеми показано приклади застосування блокчейну — від систем управління ідентичністю, електронного документообігу, фінансових транзакцій і смартконтрактів до захисту журналів подій і кіберфорензики. Цей підхід забезпечує невідомність дій користувачів, адже кожна транзакція має зафіксованого автора, точний час і підтвердження усіма учасниками мережі. Таким чином, рисунок ілюструє, як поєднання криптографії, децентралізації та консенсусних алгоритмів створює стійку архітектуру цифрової довіри, у якій кожен запис є перевіраним, незмінним і юридично значущим. Це

перетворює блокчейн на базову технологію забезпечення безпеки, прозорості та відповідальності в сучасних інформаційних системах.

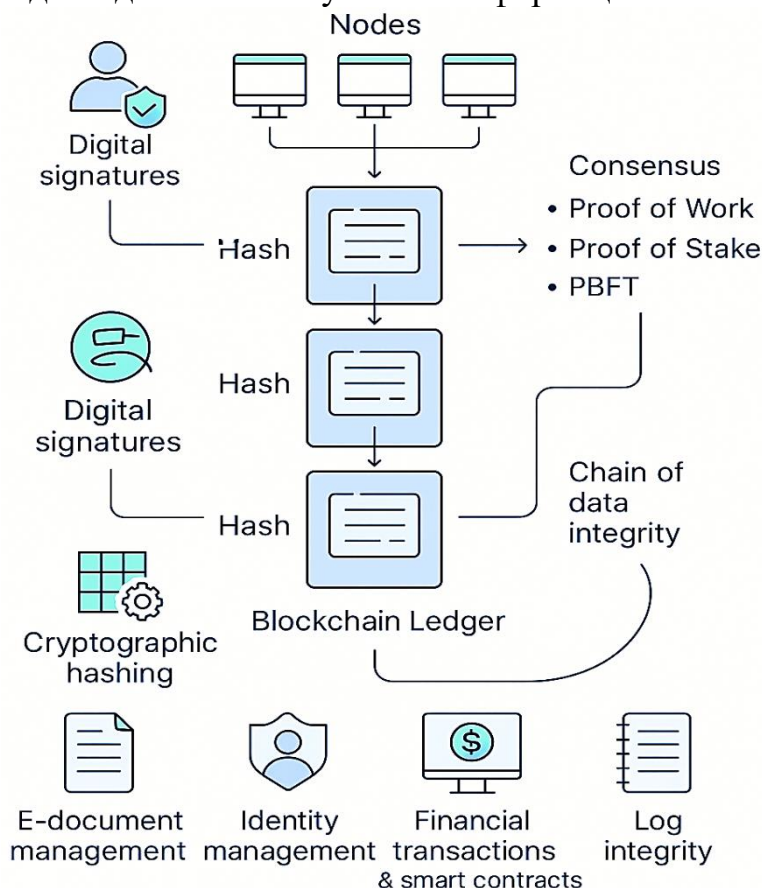


Рис. 5.4. Принципова схема забезпечення довіри, цілісності та невідомості в інформаційних системах на основі блокчейн-технологій

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На правовому рівні невідомність, що забезпечується блокчейном, дозволяє розглядати зафіксовані транзакції як цифрові докази у випадку спорів або судових розглядів. Оскільки інформація зберігається у незмінному вигляді в розподіленому реєстрі, її не можна підробити або видалити, що унеможливорює фальсифікацію доказів чи маніпуляцію даними. У корпоративних і міжорганізаційних процесах це мінімізує ризики шахрайства, подвійних транзакцій, несанкціонованих змін чи спотворень інформації. Такі властивості блокчейну створюють цифрову екосистему довіри, у якій кожна взаємодія між сторонами підкріплена криптографічним підтвердженням і колективною згодою вузлів мережі.

Крім того, невідомність у блокчейні сприяє розвитку концепції цифрової відповідальності, де всі учасники несуть рівноправну частку відповідальності за достовірність даних, що ними створюються чи

передаються. Це підвищує не лише рівень безпеки, а й загальну кіберстійкість підприємства, адже будь-яка дія — від внутрішньої транзакції до міжнародного обміну даними — може бути перевірена, простежена й підтверджена незалежно від людського фактора. У результаті формується принципово нова модель взаємодії у цифровому просторі — «довіра без довірених посередників» (trustless trust), де сама технологія гарантує справедливість, прозорість і незмінність процесів. Таким чином, невідомість, реалізована за допомогою блокчейну, виступає не лише технічним механізмом підтвердження дій, а й правовою, етичною та управлінською основою сучасних кіберсистем, що поєднує безпеку, прозорість і відповідальність у єдиній цифровій інфраструктурі.

У сфері кібербезпеки блокчейн дедалі частіше використовується для захисту журналів подій (log integrity), виявлення фальсифікацій у ланцюгах постачання (supply chain security), керування цифровими сертифікатами та аутентифікації користувачів без паролів. Наприклад, у розподілених системах моніторингу блокчейн гарантує, що записи про інциденти не можуть бути змінені після їх внесення, а в системах управління доступом забезпечує простежуваність усіх дій користувачів. Це створює умови для реалізації Zero Trust-архітектури, де жодна дія не вважається надійною без перевірки, але кожна підтверджується прозорим механізмом довіри.

Крім того, блокчейн формує нову парадигму цифрової відповідальності, де довіра не базується на авторитеті окремого посередника, а забезпечується математичними принципами і колективною валідацією. Цей підхід особливо актуальний для критичних інфраструктур, фінансових технологій, електронного урядування та систем захисту персональних даних, де ризик фальсифікації чи підміни інформації може призвести до катастрофічних наслідків.

Таким чином, блокчейн-технології виступають архітектурною основою нової моделі довіри в інформаційних системах, де кожна транзакція є прозорою, кожен запис — незмінним, а кожна взаємодія — підтвердженою. Поєднання децентралізації, криптографії та консенсусних алгоритмів створює фундамент для формування цифрового середовища з гарантованою цілісністю, надійністю й невідомістю, що відкриває перспективи побудови безпечних, самоврядних і стійких до кібератак екосистем у майбутньому.

5.4. КВАНТОВІ ОБЧИСЛЕННЯ ТА ВИКЛИКИ ДЛЯ СУЧАСНОЇ КРИПТОГРАФІЇ І БЕЗПЕКИ ДАНИХ

Квантові обчислення є однією з найреволюційніших технологій ХХІ століття, здатною радикально змінити підходи до оброблення, зберігання й захисту інформації. Їхня унікальність полягає у використанні квантових бітів (кубітів), які, на відміну від класичних бітів, можуть перебувати одночасно у станах 0 і 1 завдяки принципу суперпозиції. Це дозволяє квантовим комп'ютерам виконувати паралельні обчислення, обробляючи експоненційну кількість варіантів одночасно, що надає їм надзвичайну обчислювальну потужність порівняно з традиційними системами. Додатково принцип квантової заплутаності (entanglement) забезпечує тісний взаємозв'язок між кубітами, завдяки якому зміна стану одного елемента миттєво впливає на інші, навіть якщо вони розташовані на великій відстані. Ці властивості відкривають нові можливості для моделювання складних систем, штучного інтелекту, оптимізації логістичних процесів і, водночас, створюють серйозні виклики для сучасної криптографії та безпеки даних.

Основна загроза квантових обчислень полягає у тому, що вони здатні зламати класичні криптографічні алгоритми, які нині є фундаментом захисту інформації в усьому світі. Алгоритми RSA, ECC (Elliptic Curve Cryptography) та DSA, що базуються на складності факторизації великих чисел або розв'язанні задач дискретного логарифму, можуть бути зламані за допомогою алгоритму Шора (Shor's Algorithm), який ефективно виконує ці операції на квантовому комп'ютері. Якщо у класичній обчислювальній моделі для цього потрібні мільярди років, то квантовий процесор з достатньою кількістю кубітів може здійснити злам за лічені хвилини. Крім того, алгоритм Гровера (Grover's Algorithm) здатен прискорити перебір симетричних ключів, знижуючи їхню ефективну криптографічну стійкість удвічі. Це означає, що навіть алгоритми, які вважалися надійними — наприклад, AES-256 — можуть вимагати подвоєння довжини ключа або переходу до нових типів квантово-стійких систем.

Для нейтралізації цих ризиків активно розвивається напрям постквантової криптографії (Post-Quantum Cryptography, PQC), який передбачає створення криптографічних алгоритмів, стійких до атак із використанням квантових комп'ютерів. До таких підходів належать схеми на основі решіток (lattice-based cryptography), кодові криптосистеми (code-based), мультіваріантні поліноміальні рівняння (multivariate polynomial cryptography) та хеш-підписи (hash-based signatures). Наприклад, алгоритми CRYSTALS-Kyber і Dilithium, стандартизовані NIST у 2022–2023 роках, демонструють високу ефективність і стійкість до квантових атак. Вони не залежать від факторизації чисел чи дискретного логарифму, що робить їх непридатними для квантових атак типу Шора. Такі рішення поступово

інтегруються у сучасні протоколи безпеки, включно з TLS, VPN, eID та системами цифрових підписів.

У сфері обміну ключами перспективним напрямом є квантова криптографія, зокрема квантовий розподіл ключів (Quantum Key Distribution, QKD). Він базується на фундаментальних законах квантової механіки — принципі невизначеності Гейзенберга та неможливості клонування квантового стану (no-cloning theorem). Це означає, що будь-яка спроба перехопити квантові сигнали змінює їхні параметри, і система миттєво виявляє втручання. Найвідомішим протоколом є BB84, який дозволяє сторонам безпечно генерувати спільний ключ шифрування навіть у присутності потенційного злоумисника. Таким чином, квантова криптографія формує абсолютно новий рівень довіри в обміні інформацією, гарантуючи не лише стійкість до зламів, а й фізичну неможливість непомітного втручання у процес передачі.

Квантова криптографія має потенціал стати ключовою технологією для захисту критичних комунікацій у майбутніх інформаційних інфраструктурах, включно з урядовими, військовими та фінансовими системами. Її впровадження вже розпочато в експериментальних мережах у Європі, США, Китаї та Японії, де здійснюється передача даних між вузлами за допомогою фотонних каналів. У таких мережах квантові ключі можуть інтегруватися з класичними криптосистемами, утворюючи гібридні моделі захисту з підвищеним рівнем стійкості. Додатково досліджуються супутникові системи квантового зв'язку, що дозволяють здійснювати розподіл ключів на глобальному рівні без ризику перехоплення. Розвиток технологій квантових ретрансляторів і пам'яті (quantum repeaters, quantum memory) відкриває шлях до створення повноцінного Квантового Інтернету — мережі, у якій обмін інформацією буде захищено на фізичному рівні. У перспективі це дасть змогу побудувати абсолютно нову архітектуру довіри, де безпека забезпечуватиметься не обмеженнями алгоритмів, а самою природою квантових явищ.

На рис. 5.5 представлено спрощену ілюстрацію принципу роботи квантового розподілу ключів (Quantum Key Distribution, QKD), який забезпечує безпечний обмін шифрувальними ключами між двома сторонами — Алісою (Alice) та Бобом (Bob). Джерело фотонів (Photon Source) у Аліси генерує послідовність квантових бітів — кубітів, кожен із яких має певну поляризацію (горизонтально-вертикальну або діагональну). Ці фотони передаються по квантовому каналу до Боба, який вимірює їхній стан, використовуючи власні поляризаційні фільтри — beam splitters.

Кожен фотон несе один біт інформації (0 або 1), закодований за допомогою вибраної бази поляризації. Якщо Боб вибирає правильну базу,

його вимір збігається з бітовим значенням Аліси; якщо неправильну — отримується випадкове значення. Після серії переданих фотонів Аліса та Боб обмінюються частиною своїх баз через класичний канал і відкидають невідповідні вимірювання, отримуючи узгоджений “просіяний” ключ (Sifted Key). У результаті формується спільний криптографічний ключ, який відомий лише двом сторонам і не може бути перехоплений без виявлення втручання. Особливість такого механізму полягає у використанні фундаментальних законів квантової механіки: будь-яка спроба перехоплення або вимірювання фотонів змінює їхній стан, що миттєво виявляється системою. Це робить квантову криптографію єдиним методом, який забезпечує фізичну, а не лише математичну безпеку передавання ключів. Таким чином, протокол BB84 створює основу для майбутніх систем постквантового захисту, де надійність гарантується не обчислювальною складністю, а законами природи.



Рис. 5.5. Принципова схема роботи квантової криптографії (QKD) за протоколом BB84

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Попри великі переваги, квантові технології створюють серйозні виклики для архітектур безпеки, оскільки перехід до квантово-стійких рішень потребує масштабної модернізації інфраструктури. Під загрозою опиняються не лише криптографічні системи, а й цифрові сертифікати,

механізми автентифікації, блокчейн-технології та протоколи Zero Trust, які базуються на класичних математичних припущеннях. Вже сьогодні фахівці в галузі кібербезпеки попереджають про загрозу «Harvest Now, Decrypt Later» — коли зловмисники зберігають зашифровані дані з метою їх дешифрування у майбутньому, коли квантові комп'ютери стануть доступними. Тому стратегічним напрямом стає гібридна криптографія, що поєднує класичні алгоритми з постквантовими, забезпечуючи плавний перехід до нового покоління захисту.

У підсумку квантові обчислення виступають подвійним чинником — одночасно викликом і рушієм еволюції кібербезпеки. З одного боку, вони здатні зруйнувати чинну криптографічну парадигму, а з іншого — стимулюють створення більш стійких, математично й фізично захищених систем. Перехід до квантово-безпечної архітектури вимагає перегляду стандартів, оновлення політик безпеки, навчання персоналу й міжнародної координації зусиль. Саме адаптація до квантової епохи визначить рівень кіберстійкості майбутніх інформаційних систем, де безпека базуватиметься не лише на складності алгоритмів, а й на фундаментальних законах фізики, що гарантують достовірність і конфіденційність у цифровому світі.

5.5. АКТУАЛЬНІ ПІДХОДИ ДО КОНЦЕПЦІЇ ZERO TRUST ТА ПОБУДОВИ АДАПТИВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Концепція Zero Trust (нульової довіри) є сучасною парадигмою забезпечення інформаційної безпеки, яка виходить із базового принципу — «нікому не довіряй, перевіряй усіх». Її основна ідея полягає в тому, що жоден користувач, пристрій чи додаток не може вважатися надійним за замовчуванням, навіть якщо він знаходиться всередині корпоративної мережі. На відміну від традиційної моделі периметрової безпеки, яка передбачає захист від зовнішніх загроз, Zero Trust реалізує контроль доступу на основі контексту, ідентичності та поведінкових характеристик, застосовуючи динамічну автентифікацію, багаторівневу авторизацію та постійний моніторинг активності. Такий підхід дає змогу зменшити ризик внутрішніх загроз, атак через скомпрометовані облікові записи та lateral movement — горизонтального поширення зловмисника всередині мережі.

Крім того, концепція Zero Trust передбачає постійне підтвердження довіри на основі контекстуальних факторів, таких як місце розташування користувача, тип пристрою, рівень ризику транзакції та стан безпеки мережі. У разі виявлення відхилень система автоматично змінює політики доступу або ініціює повторну автентифікацію, забезпечуючи динамічне

реагування на загрози в реальному часі. Такий підхід формує адаптивну екосистему безпеки, у якій довіра не є статичною властивістю, а результатом безперервного аналізу поведінки, ризику й контексту кожної дії користувача чи пристрою.

Одним із ключових компонентів архітектури Zero Trust є ідентифікація й управління доступом (Identity and Access Management, IAM), що включає багатофакторну автентифікацію (MFA), політику найменших привілеїв (Least Privilege Access) і контроль сесій у реальному часі. Додатково важливим елементом є мікросегментація мережі, коли інфраструктура розділяється на ізольовані зони, доступ до яких надається виключно за перевіреними політиками. Це дозволяє обмежити масштаб потенційного компрометування системи — навіть якщо один сегмент атаковано, інші залишаються захищеними. Крім того, технології Zero Trust інтегрують поведінкову аналітику (UEBA — User and Entity Behavior Analytics), що використовує алгоритми машинного навчання для визначення аномалій у діях користувачів, пристроїв і сервісів. Завдяки цьому система може виявляти нетипові сценарії поведінки, наприклад нехарактерні запити до ресурсів, завантаження даних або спроби входу з незвичних геолокацій.

Сучасна реалізація Zero Trust передбачає не лише політичний чи адміністративний рівень, а й технічну інтеграцію з інтелектуальними системами моніторингу — SIEM, SOAR, EDR/XDR, які забезпечують автоматизоване реагування на інциденти. Дані про автентифікацію, мережеву активність і взаємодію між вузлами аналізуються в реальному часі, що дозволяє створювати адаптивну модель безпеки, здатну реагувати на зміну контексту або рівня ризику. У таких системах політики доступу не є статичними: вони постійно оновлюються залежно від поведінки користувачів, рівня довіри до пристрою, місця підключення, стану мережі та оцінки ризику транзакції. Такий підхід формує концепцію Adaptive Security Architecture (ASA), у якій безпека розглядається як динамічний процес, що самонавчається та самокоригується.

Важливою складовою сучасних адаптивних систем є застосування штучного інтелекту (AI) та машинного навчання (ML) для формування контексту довіри та автоматичного прийняття рішень. Наприклад, на основі історичних даних система може визначати типові моделі поведінки користувачів і пристроїв, а потім автоматично змінювати політики доступу у випадку виявлення відхилень. Це дає змогу реалізувати динамічне присвоєння рівня довіри (Dynamic Trust Scoring), коли кожна дія оцінюється з погляду ризику в реальному часі. Застосування таких підходів забезпечує баланс між безпекою й ефективністю роботи користувачів, оскільки система не блокує легітимну активність, але негайно реагує на потенційні загрози.

Крім того, використання AI/ML у Zero Trust дає можливість системам самонавчатися на основі попередніх інцидентів, оптимізуючи моделі виявлення аномалій та зменшуючи кількість хибних спрацювань. Інтелектуальні алгоритми можуть прогнозувати потенційні вектори атак, моделюючи поведінку зломисників і пропонуючи превентивні заходи для запобігання порушенням. У результаті архітектура безпеки набуває властивостей прогнозного аналізу ризиків (Predictive Security Analytics), що перетворює систему з реактивної на проактивну, забезпечуючи випереджальне виявлення та нейтралізацію кіберзагроз.

У межах корпоративних стратегій Zero Trust інтегрується також принцип безперервної перевірки (Continuous Verification), коли навіть після успішної автентифікації користувач підлягає постійному моніторингу. Це дозволяє виявляти компрометацію сесій, викрадення токенів доступу та інші форми сучасних атак, які можуть залишатися непоміченими у традиційних системах. Крім того, Zero Trust підтримує ідею захисту даних «на всіх рівнях» (Data-Centric Security) — від мережевого до прикладного, включно з шифруванням, токенизацією, цифровими підписами та контролем контенту на основі класифікації.

Безперервна перевірка у межах Zero Trust реалізується через поєднання телеметрії, поведінкової аналітики та адаптивної оцінки ризиків, що дозволяє системі оперативно реагувати на будь-які зміни контексту користувача або пристрою. Наприклад, якщо зафіксовано спробу доступу з нетипової геолокації, підозрілої IP-адреси або невідомого пристрою, система може автоматично вимагати повторної автентифікації або заблокувати сесію. Такий підхід мінімізує ризики внутрішніх порушень та несанкціонованих дій, забезпечуючи динамічне управління довірою в реальному часі. Крім того, принцип безперервної перевірки інтегрується з платформами SIEM, SOAR та XDR, що дозволяють здійснювати кореляцію подій, автоматизоване реагування на інциденти та формування централізованого профілю безпеки підприємства. У межах Data-Centric Security реалізується також контекстна класифікація даних, де кожен об'єкт — файл, запит чи транзакція — оцінюється за рівнем конфіденційності, критичності та відповідності політикам. У результаті формується самоадаптивна екосистема безпеки, яка не лише запобігає вторгненням, а й постійно вдосконалює свої механізми захисту завдяки аналізу поведінкових шаблонів і машинному навчанню.

На рис. 5.6 представлено узагальнену референсну архітектуру Zero Trust, яка ілюструє три основні етапи забезпечення безпеки — *Prevent* (запобігання), *Detect* (виявлення) та *Recover* (відновлення). У центрі моделі акцент зроблено на принципі найменших привілеїв (Least Privilege), який

передбачає, що кожен користувач, пристрій або процес отримує лише мінімально необхідні права доступу. Система об'єднує ключові компоненти: MFA (багатофакторна автентифікація), IAM (управління ідентичністю та доступом), SSO (єдиний вхід), PAM (керування привілейованими обліковими записами), а також MDR (виявлення та реагування на загрози). Ці елементи працюють у комплексі, забезпечуючи сувору автентифікацію, постійну перевірку довіри та моніторинг активності користувачів і систем. Архітектура підкреслює, що ефективна модель Zero Trust не обмежується лише контролем периметру, а охоплює весь життєвий цикл захисту — від попередження інцидентів до відновлення після атак. Вона формує основу адаптивної безпеки, у якій рішення приймаються динамічно на основі ризику, контексту та поведінки суб'єктів. Завдяки такому підходу досягається баланс між зручністю користувачів і високим рівнем захищеності цифрового середовища, що є ключовою метою сучасної кіберстратегії Zero Trust.



Рис. 5.6. Еталонна архітектура Zero Trust: запобігання, виявлення та відновлення

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Отже, концепція Zero Trust разом із адаптивними системами захисту формує нову архітектуру кіберстійкості, орієнтовану на гнучке управління ризиками в умовах постійно мінливого середовища. Вона забезпечує не лише технічний захист, а й стратегічну перевагу у сфері управління безпекою даних — коли довіра не є статичною властивістю, а результатом безперервного аналізу поведінки, контексту й ризику. Саме така динамічна модель стає фундаментом майбутніх кіберзахисних екосистем, де

інтелектуальні механізми прийняття рішень, самонавчання та автоматизована реакція поєднуються у єдину інтегровану систему цифрової довіри.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 5

1. V. Sokolov, P. Skladannyi and A. Platonenko, "Video Channel Suppression Method of Unmanned Aerial Vehicles," 2022 *IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO)*, Kyiv, Ukraine, 2022, pp. 473-477, doi: 10.1109/ELNANO54667.2022.9927105.
2. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) *CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073
3. Hulak, Hennadii and Kriuchkova, Larysa and Skladannyi, Pavlo and Opirskyy, Ivan (2021) *Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 137-142. ISSN 1613-0073
4. Iosifova, Olena and Iosifov, Ievgen and Sokolov, V. Y. and Romanovskyy, O. and Sukaylo, I. (2021) *Analysis of Automatic Speech Recognition Methods* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 252-257. ISSN 1613-0073
5. Zhebka, V. and Zhebka, S and Bazhan, T and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Methodology for Choosing a Consensus Algorithm for Blockchain Technology* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 106-113. ISSN 1613-0073
6. Dudykevych, V. and Mykytyn, G. and Stosyk, T. and Skladannyi, Pavlo (2024) *Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 449-457. ISSN 1613-0073
7. Shevchenko, Svitlana & Zhdanova, Yuliia & Shevchenko, Halyna & Nehodenko, Olena & Spasiteleva, Svitlana. (2023). *Information Security Risk Management using Cognitive Modeling*.
8. V. Sokolov, P. Skladannyi and A. Platonenko, "Jump-Stay Jamming Attack on Wi-Fi Systems," 2023 *IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, Lviv, Ukraine, 2023, pp. 1-5, doi: 10.1109/CSIT61576.2023.10324031.

9. Buriachok, V., Korshun, N., Zhylytsov, O., Sokolov, V., Skladannyi, P. (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspas, G. (eds) *Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies*, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_32
10. Marusenko, R., Sokolov, V., Buriachok, V. (2021). Experimental Evaluation of Phishing Attack on High School Students. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing*, vol 1247. Springer, Cham. https://doi.org/10.1007/978-3-030-55506-1_59
11. V. Astapenya, V. Sokolov and D. Ageyev, "Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum," *2020 IEEE Ukrainian Microwave Week (UkrMW)*, Kharkiv, Ukraine, 2020, pp. 203-206, doi: 10.1109/UkrMW49653.2020.9252755.
12. Brzhevskaya, Zoreslava and Kyrychok, Roman and Anosov, Andrii and Skladannyi, Pavlo and Vorokhob, Maksym (2021) *Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 257-264. ISSN 1613-0073
13. HU, ZHENG BING & Buriachok, Volodymyr & Sokolov, Volodymyr. (2019). Implementation of Social Engineering Attack at Institution of Higher Education. SSRN Electronic Journal. 10.2139/ssrn.3679106.
14. Mykhaylova, O and Fedynyshyn, T and Sokolov, Volodymyr and Kyrychok, Roman (2024) *Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 239-251. ISSN 1613-0073
15. Marusenko, R., Sokolov, V., Skladannyi, P. (2023). Social Engineering Penetration Testing in Higher Education Institutions. In: Hu, Z., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VI. ICCSEEA 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol 181. Springer, Cham. https://doi.org/10.1007/978-3-031-36118-0_96
16. Mykhaylova, O and Fedynyshyn, T and Datsiuk, A and Fihol, B and Hulak, Hennadii (2023) *Mobile Application as a Critical Infrastructure Cyberattack Surface* Cybersecurity Providing in Information and Telecommunication Systems II 2023, 3050. pp. 29-43. ISSN 1613-0073

17. Kyrychok, R., Laptiev, O., Lisnevskiy, R., Kozlovskiy, V., & Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. *Eastern-European Journal of Enterprise Technologies*, 1(9(115)), 93–101. <https://doi.org/10.15587/1729-4061.2022.253530>
18. V. Sokolov, P. Skladannyi and V. Astapenya, "Bluetooth Low-Energy Beacon Resistance to Jamming Attack," *2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT)*, Lviv, Ukraine, 2023, pp. 270-274, doi: 10.1109/ELIT61488.2023.10310815.
19. Astapenya, Volodymyr & Zhdanova, Yuliia & Shevchenko, Svitlana & Spasiteleva, Svitlana & Kryvoruchko, Olena. (2024). Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare.
20. Dudykevych, V and Yevseiev, S and Myktyyn, H and Ruda, K and Hulak, Hennadii (2024) *Detecting Deepfake Modifications of Biometric Images using Neural Networks* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 391-397. ISSN 1613-0073
21. Adamantis, M., Sokolov, V., Skladannyi, P. (2025). Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method. In: Hu, Z., Yanovsky, F., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VII. ICCSEEA 2024* 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 242. Springer, Cham. https://doi.org/10.1007/978-3-031-84228-3_5
22. Chernenko, Roman and Anosov, Andrii and Kyrychok, Roman and Brzhevskaya, Zoreslava and Spasiteleva, Svitlana (2022) *Encryption Method for Systems with Limited Computing Resources* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 142-148. ISSN 1613-0073
23. Iavich, M. and Kovalchuk, O. and Gnatyuk, S. and Khavikova, Y. and Sokolov, Volodymyr (2024) *Classical and post-quantum encryption for GDPR* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 70-78. ISSN 1613-0073
24. Romanovskiy, O. and Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2022) *Prototyping Methodology of End-to-End Speech Analytics Software* Modern Machine Learning Technologies and Data Science Workshop, 3312 (1). pp. 76-86. ISSN 1613-0073
25. Romanovskiy, O., Iosifov, I., Iosifova, O., Sokolov, V., Kipchuk, F., Sukaylo, I. (2021). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and*

Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_3

26. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography*, 8(3), 38. <https://doi.org/10.3390/cryptography8030038>

27. Syrotynskiy, R. and Tyshyk, I. and Kochan, O. and Sokolov, Volodymyr and Skladannyi, Pavlo (2024) *Methodology of network infrastructure analysis as part of migration to zero-trust architecture* Cyber Security and Data Protection 2024 (3800). pp. 97-105. ISSN 1613-0073

28. Martseniuk, Y. and Partyka, A. and Harasymchuk, O. and Shevchenko, Svitlana (2024) *Universal centralized secret data management for automated public cloud provisioning* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 72-81. ISSN 1613-0073

29. Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2021) *Natural Language Technology to Ensure the Safety of Speech Information* Cybersecurity Providing in Information and Telecommunication Systems II. Volume I, 3187 (1). pp. 216-226. ISSN 1613-0073

30. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) *Smart Home Subsystem for Calculating the Quality of Public Utilities* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073

31. V. Sokolov, P. Skladannyi and N. Mazur, "Wi-Fi Repeater Influence on Wireless Access," 2023 *IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2023, pp. 33-36, doi: 10.1109/AICT61584.2023.10452421.

32. Dreis, Y. and Korchenko, O. and Brzhevskaya, Zoreslava and Kriuchkova, Larysa and Nesterova, Olena (2024) *Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 277-289. ISSN 1613-0073

33. Virovets, Denis and Obushnyi, Sergiy and Zhurakovskiy, B. and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Integration of smart contracts and artificial intelligence using cryptographic oracles* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 39-46. ISSN 1613-0073

34. Shevchuk, D and Harasymchuk, O and Partyka, A and Korshun, Natalia (2023) *Designing Secured Services for Authentication, Authorization,*

and Accounting of Users Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 207-225. ISSN 1613-0073

35. Складанний П.М., Костюк Ю.В., Мазур Н.П., Пітайчук М.А. Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології. 2025. №1(86). С. 61-74.

36. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, 1(3), 602-617. <https://doi.org/10.3390/encyclopedia1030050>

37. TajDini, M., Sokolov, V., Kuzminykh, I., Shiaeles, S., & Ghita, B. (2020). Wireless Sensors for Brain Activity—A Survey. *Electronics*, 9(12), 2092. <https://doi.org/10.3390/electronics9122092>

38. Grechaninov, Viktor and Hulak, Hennadii and Hulak, Evgen and Skladannyi, Pavlo and Sokolov, Volodymyr (2021) *Decentralized Access Demarcation System Construction in Situational Center Network Cybersecurity Providing in Information and Telecommunication Systems II* 2021, 3188 (2). pp. 197-206. ISSN 1613-0073

39. Buriachok, Volodymyr and Ageyev, Dmytro and Zhylytsov, Oleksii and Skladannyi, Pavlo and Sokolov, V. Y. (2020) *Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies Cybersecurity Providing in Information and Telecommunication Systems*, 2746. pp. 23-32. ISSN 1613-0073

40. Костюк Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., Пазинін, А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка. 2025. 4 (28), 633–655.

41. M. Vladymyrenko, V. Sokolov, V. Buriachok, A. Platonenko and D. Ageyev, "Analysis of Implementation Results of the Distributed Access Control System," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-6, doi: 10.1109/PICST47496.2019.9061376.

42. Складанний, П.М., Машкіна, І.В., Рзаєва, С.Л., Костюк, Ю.В. Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології. 2025. (2), 59-76.

43. Hu, Z., Buriachok, V., Bogachuk, I., Sokolov, V., Ageyev, D. (2021). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. In: Radivilova, T., Ageyev, D., Kryvinska, N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_29

44. F. Kipchuk, V. Sokolov, P. Skladannyi and D. Ageyev, "Assessing Approaches of IT Infrastructure Audit," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 213-217, doi: 10.1109/PICST54195.2021.9772181.
45. Grechaninov, Viktor and Hulak, Hennadii and Sokolov, V. Y. and Skladannyi, Pavlo and Korshun, Natalia (2022) *Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center* Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. pp. 107-117. ISSN 1613-0073
46. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597.
47. Kuzminykh, I., Carlsson, A., Yevdokymenko, M., Sokolov, V. (2019). Investigation of the IoT Device Lifetime with Secure Data Transmission. In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds) *Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN ruSMART 2019* 2019. Lecture Notes in Computer Science(), vol 11660. Springer, Cham. https://doi.org/10.1007/978-3-030-30859-9_2
48. Buriachok, Volodymyr and Sokolov, V. Y. and Skladannyi, Pavlo (2019) *Security Rating Metrics for Distributed Wireless Systems* MoMLet&DS. pp. 222-233. ISSN 1613-0073
49. Hu, Z.B., Buriachok, V., TajDini, M., Sokolov, V. (2021). Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies*, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_31
50. Костюк Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., Хорольська, К. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка. 2024. 1(25), 229–252.
51. Buhas, Vasyl and Ponomarenko, Ihor and Bugas, Valeriy and Ramskyi, Andrii and Sokolov, Volodymyr (2021) *Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 273-281. ISSN 1613-0073
52. Zhebka, V. and Skladannyi, Pavlo and Zhebka, S. and Shlianachak, S. and Bondarchuk, A. (2024) *Methodology for Predicting Failures in a Smart*

Home based on Machine Learning Methods Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 322-332. ISSN 1613-0073

53. Skladannyi, Pavlo and Trofimov, Olexandr and Korniiets, Viktor and Vorokhob, Maksym and Opryshko, Tetiana (2023) *Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept* CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems. pp. 97-106. ISSN 1613-0073

54. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими ІОТ-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776.

55. Шевченко, Галина Володимирівна and Шевченко, Світлана Миколаївна and Жданова, Юлія Дмитрівна and Спасітелева, Світлана Олексіївна and Негоденко, Олена Василівна (2021) *Information Security Risk Analysis SWOT* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 309-317. ISSN 1613-0073

56. I. Iosifov, O. Iosifova and V. Sokolov, "Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 335-337, doi: 10.1109/PICST51311.2020.9468084.

57. Petriv, P. and Oprisky, I. and Mazur, Nataliia (2024) *Modern technologies of decentralized databases, authentication, and authorization methods* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 60-71. ISSN 1613-0073

58. Astafieva, Mariia and Bodnenko, Dmitry and Lytvyn, Oksana and Proshkin, Volodymyr and Skladannyi, Pavlo (2023) *Formation of High School Students' Resistance to Destructive Information Influences* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 87-96. ISSN 1613-0073

59. Sovyn, Y. and Khoma, V. and Oprisky, I. and Kozachok, Valerii (2023) *Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 12-24. ISSN 1613-0073

60. Burov, O. et al. (2020). Cybersecurity in Educational Networks. In: Ahram, T., Karwowski, W., Vergnano, A., Leali, F., Taiar, R. (eds) *Intelligent Human Systems Integration 2020. IHSI 2020. Advances in Intelligent Systems*

and Computing, vol 1131. Springer, Cham. https://doi.org/10.1007/978-3-030-39512-4_56

61. Buriachok, V., Sokolov, V. (2020). Implementation of Active Learning in the Master's Program on Cybersecurity. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, vol 938. Springer, Cham. https://doi.org/10.1007/978-3-030-16621-2_57

62. Anakhov, Pavlo and Zhebka, Viktoriia and Koretska, Viktoriia and Sokolov, V. Y. and Skladannyi, Pavlo (2022) *Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir* Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149. pp. 169-176. ISSN 1613-0073

63. Z. Hu, B. Vovkotrub, V. Buriachok, Y. Zotkin and V. Sokolov, "Bandwidth Research of Wireless IoT Switches," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 1-5, doi: 10.1109/TCSET49122.2020.235492.

64. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Abramov, Serhii and Zhylytsov, Oleksii (2022) *Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 1-10. ISSN 1613-0073

65. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Mazur, Nataliia and Ageyev, Dmytro (2021) *Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3187 (1). pp. 302-309. ISSN 1613-0073

66. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 125–156.

67. Складанний, П., Костюк, Ю., Рзаєва, С., & Мазур, Н. (2025). Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 242–269. <https://doi.org/10.28925/2663-4023.2025.31.1015>

68. Складанний, П.М., Гулак, Г.М., Костюк, Ю.В. Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. Телекомунікаційні та інформаційні технології. 2025. № 4 (89), 137-147. <https://doi.org/10.31673/2412-4338.2025.048916>

69. Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive Information Security Management in Cloud-Oriented Intelligent Transportation Systems. *Ukrainian Scientific Journal of Information Security*, 2025, vol. 31, issue 1, pp. 23-36. <https://doi.org/10.18372/2225-5036.31.20634>
70. Bessalov, Anatoly and Kovalchuk, L. and Sokolov, V. Y. and Skladannyi, Pavlo and Radivilova, T. (2020) *Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2746. pp. 1-13. ISSN 1613-0073
71. Bessalov, Anatolii & Grubiy, Evgeniy & Sokolov, Volodymyr & Skladannyi, Pavlo. (2020). 3- and 5-Isogenies of Supersingular Edwards Curves. 10.48550/arXiv.2006.16111.
72. Bessalov, Anatoly and Sokolov, V. Y. and Skladannyi, Pavlo and Zhylytsov, Oleksii (2021) *Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 1-11. ISSN 1613-0073
73. V. Astapenya, V. Sokolov, P. Skladannyi and O. Zhylytsov, "Analysis of Ways and Methods of Increasing the Availability of Information in Distributed Information Systems," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 174-178, doi: 10.1109/PICST54195.2021.9772161.
74. V. Astapenya, V. Buriachok, V. Sokolov, P. Skladannyi and D. Ageyev, "Last Mile Technique for Wireless Delivery System using an Accelerating Lens," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 811-814, doi: 10.1109/PICST51311.2020.9467886.
75. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii (2023) *Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves* Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073
76. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) *Brainwave-based authentication using features fusion* Computers & Security (129). p. 103198. ISSN 0167-4048
77. Iosifova, Olena and Iosifov, Ievgen and Rolik, Oleksandr and Sokolov, V. Y. (2020) *Techniques Comparison for Natural Language Processing* MoML&T&DS, 2631 (I). pp. 57-67. ISSN 1613-0073
78. Anakhov, P. and Zhebka, V. and Tushych, A. and Kravchenko, V. and Blazhenyi, N. and Skladannyi, Pavlo and Sokolov, Volodymyr (2022) *Evaluation Method of the Physical Compatibility of*

Equipment in a Hybrid Information Transmission Network Journal of Theoretical and Applied Information Technology, 100 (22). pp. 6635-6644. ISSN 1817-3195

КОНТРОЛЬНІ ПИТАННЯ

1. У чому полягає роль штучного інтелекту у виявленні кіберзагроз і аномалій поведінки?
2. Як машинне навчання допомагає аналізувати великі обсяги даних у системах кіберзахисту?
3. Які алгоритми машинного навчання найчастіше застосовуються для класифікації типів атак?
4. Які переваги дає використання рекурентних нейронних мереж (LSTM) у виявленні підозрілих подій безпеки?
5. У чому полягає основна ідея пояснюваного штучного інтелекту (Explainable AI, XAI)?
6. Як XAI підвищує довіру до автоматизованих рішень у системах кіберзахисту?
7. Які методи пояснюваності використовуються в XAI для аналізу впливу параметрів на рішення системи?
8. Яке значення мають інструменти LIME та SHAP у контексті пояснюваного AI?
9. Як блокчейн забезпечує цілісність і достовірність інформації в інформаційних системах?
10. У чому полягає механізм забезпечення невідмовності (non-repudiation) у блокчейн-технологіях?
11. Як криптографічне хешування сприяє збереженню структури та незмінності даних у блокчейні?
12. Які алгоритми консенсусу використовуються в блокчейн-системах для підтвердження транзакцій?
13. Які основні загрози створюють квантові обчислення для сучасної криптографії?
14. Як алгоритми Шора та Гровера впливають на стійкість класичних шифрів RSA, ECC та AES?
15. Що являє собою постквантова криптографія (PQC) і які її переваги перед традиційними методами шифрування?
16. У чому полягає суть квантового розподілу ключів (Quantum Key Distribution, QKD)?
17. Як принцип невизначеності Гейзенберга використовується у квантовій криптографії для виявлення перехоплення даних?

18. Які основні принципи концепції Zero Trust формують сучасну архітектуру безпеки?

19. Як технології штучного інтелекту й машинного навчання інтегруються в адаптивні системи Zero Trust?

20. Яким чином синергія штучного інтелекту, блокчейну та квантових обчислень формує нову парадигму кіберзахисту майбутнього?

РОЗДІЛ 6

ПРАКТИЧНІ АСПЕКТИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ І СИСТЕМ



- 6.1. Архітектура корпоративної мережі з урахуванням безпеки**
- 6.2. Використання VLAN, VPN і тунелювання**
- 6.3. Контроль доступу та багаторівнева аутентифікація**
- 6.4. Захист електронної пошти та веб-сервісів**
- 6.5. Безпека DevOps і DevSecOps-процесів**

Практичні аспекти захисту корпоративних мереж і систем охоплюють комплекс заходів, спрямованих на забезпечення безпеки інформаційних ресурсів підприємства в умовах постійного зростання кіберзагроз. У сучасних корпоративних інфраструктурах, що поєднують локальні, хмарні та віддалені компоненти, критично важливо не лише знати теоретичні засади інформаційної безпеки, а й уміти застосовувати їх на практиці. Основна мета практичного захисту полягає у створенні стійкої архітектури мережі, здатної забезпечувати конфіденційність, цілісність і доступність даних навіть у разі спроб несанкціонованого доступу, збоїв або атак.

Захист корпоративних мереж починається з побудови безпечної архітектури, де передбачено логічну сегментацію трафіку за допомогою технологій VLAN, VPN та DMZ, впроваджено багаторівневу систему контролю доступу та використано шифрування каналів зв'язку через протоколи TLS, IPSec або WireGuard. У межах сучасних концепцій безпеки все більшого значення набуває підхід Zero Trust, який базується на принципі відсутності довіри до будь-якого користувача чи пристрою без перевірки його автентичності й відповідності

політикам безпеки. Це дозволяє мінімізувати ризики внутрішніх загроз і компрометації облікових даних.

Важливою складовою практичного захисту є впровадження технічних засобів безпеки, серед яких міжмережеві екрани, системи виявлення та запобігання вторгненням (IDS/IPS), а також комплексні рішення SIEM і SOAR, що забезпечують централізований моніторинг, аналіз подій і автоматизацію реагування на інциденти. Завдяки таким системам адміністратори отримують змогу своєчасно виявляти аномалії, локалізувати потенційні атаки та запобігати розвитку інцидентів, що є ключовим елементом у побудові ефективного захисного контуру підприємства.

Не менш важливим напрямом є управління доступом і контроль облікових записів користувачів. Практична реалізація політик доступу базується на моделях RBAC, ABAC, DAC або MAC, що визначають рівні привілеїв і обмеження відповідно до посадових обов'язків. Упровадження багатофакторної аутентифікації, використання криптографічних ключів і систем централізованого керування ідентичностями дозволяє знизити ризик несанкціонованого доступу та крадіжки облікових даних.

Особливу увагу приділяють забезпеченню безперервності бізнес-процесів та захисту даних шляхом резервного копіювання, реплікації та розроблення стратегій відновлення після катастроф. Хмарні сервіси дедалі частіше використовуються як елементи гібридних рішень для зберігання критичної інформації, що підвищує відмовостійкість і гнучкість систем. Паралельно важливими залишаються процедури тестування планів відновлення, оцінка ризиків та регулярне оновлення політик безпеки.

Практична реалізація захисту корпоративних систем охоплює також навчання персоналу, розроблення планів реагування на інциденти, проведення внутрішніх аудитів і впровадження механізмів постійного моніторингу. Тільки комплексний підхід, який поєднує технічні, організаційні та адміністративні заходи, дозволяє досягти високого рівня стійкості корпоративної мережі до зовнішніх і внутрішніх загроз. Таким чином, практичні аспекти захисту корпоративних мереж і систем є ключовою складовою загальної стратегії інформаційної безпеки підприємства та визначають його готовність до сучасних викликів цифрового середовища.

6.1. АРХІТЕКТУРА КОРПОРАТИВНОЇ МЕРЕЖІ З УРАХУВАННЯМ БЕЗПЕКИ

Архітектура корпоративної мережі з урахуванням безпеки — це структурно-технічна модель побудови мережевої інфраструктури підприємства,

у якій усі елементи — від фізичного обладнання до програмних компонентів — проєктуються, розгортаються та керуються з урахуванням вимог інформаційної безпеки. Така архітектура не лише забезпечує ефективну взаємодію користувачів, серверів і сервісів, а й створює багаторівневий захисний контур, який мінімізує ризики несанкціонованого доступу, витоку або порушення цілісності даних.

Основною метою безпечної архітектури корпоративної мережі є побудова стійкої системи, що гарантує конфіденційність, цілісність і доступність інформації відповідно до принципу CIA (Confidentiality, Integrity, Availability). На етапі проєктування визначаються критичні ресурси, сегменти мережі та рівні довіри, формується модель загроз, обираються технології маршрутизації, комутації та шифрування, які відповідають вимогам стандартів безпеки ISO/IEC 27033 та NIST SP 800-207.

Проєктування безпечної архітектури корпоративної мережі базується на принципі "security by design", коли вимоги до захисту враховуються на всіх етапах життєвого циклу системи — від планування топології до адміністрування та моніторингу. Кожен компонент мережі (маршрутизатор, комутатор, сервер, шлюз, система зберігання даних, користувацький пристрій) розглядається як потенційна точка ризику, що вимагає застосування політик доступу, сегментації трафіку та контролю ідентифікації.

На рис. 6.1 представлено приклад багаторівневої архітектури корпоративної мережі з урахуванням безпеки, що відображає розподіл інфраструктури підприємства на окремі функціональні сегменти та зони довіри. У верхній частині схеми зображено зовнішні підключення до Інтернету, партнерських мереж (Partners WAN), віддалених офісів і приватних каналів (Private WAN), які взаємодіють через інтернет-шлюзи та захисні екрани, розташовані на рівні Internet Edge. Далі трафік потрапляє до демілітаризованої зони (DMZ), де розміщено сервери публічного доступу, зокрема вебсервери, поштові шлюзи та балансувальники навантаження, що забезпечують безпечну взаємодію між внутрішньою та зовнішньою інфраструктурами.

Центральною частиною схеми є Campus Core, який виконує функції ядра мережі та відповідає за маршрутизацію, комутацію й фільтрацію даних між внутрішніми сегментами — корпоративною інфраструктурою, внутрішнім дата-центром (Intranet Data Center) і зовнішнім центром (Extranet Data Center). В архітектурі реалізовано принцип розмежування доступу, де кожна зона (DMZ, внутрішній і зовнішній дата-центри) захищена міжмережевими екранами, що контролюють маршрути трафіку та обмежують обмін даними відповідно до політик безпеки. На рисунку також позначено потенційні точки вразливості мережі (Network vulnerability points), які ідентифікують місця можливого перехоплення або несанкціонованого втручання. Для підвищення стійкості

архітектури використовуються VPN-з'єднання, механізми шифрування, багаторівнева автентифікація та резервні маршрути між ключовими сегментами. Така побудова корпоративної мережі забезпечує комплексний захист інформаційних потоків, ізоляцію критичних компонентів і стабільну роботу систем навіть у разі кібератак чи технічних збоїв.

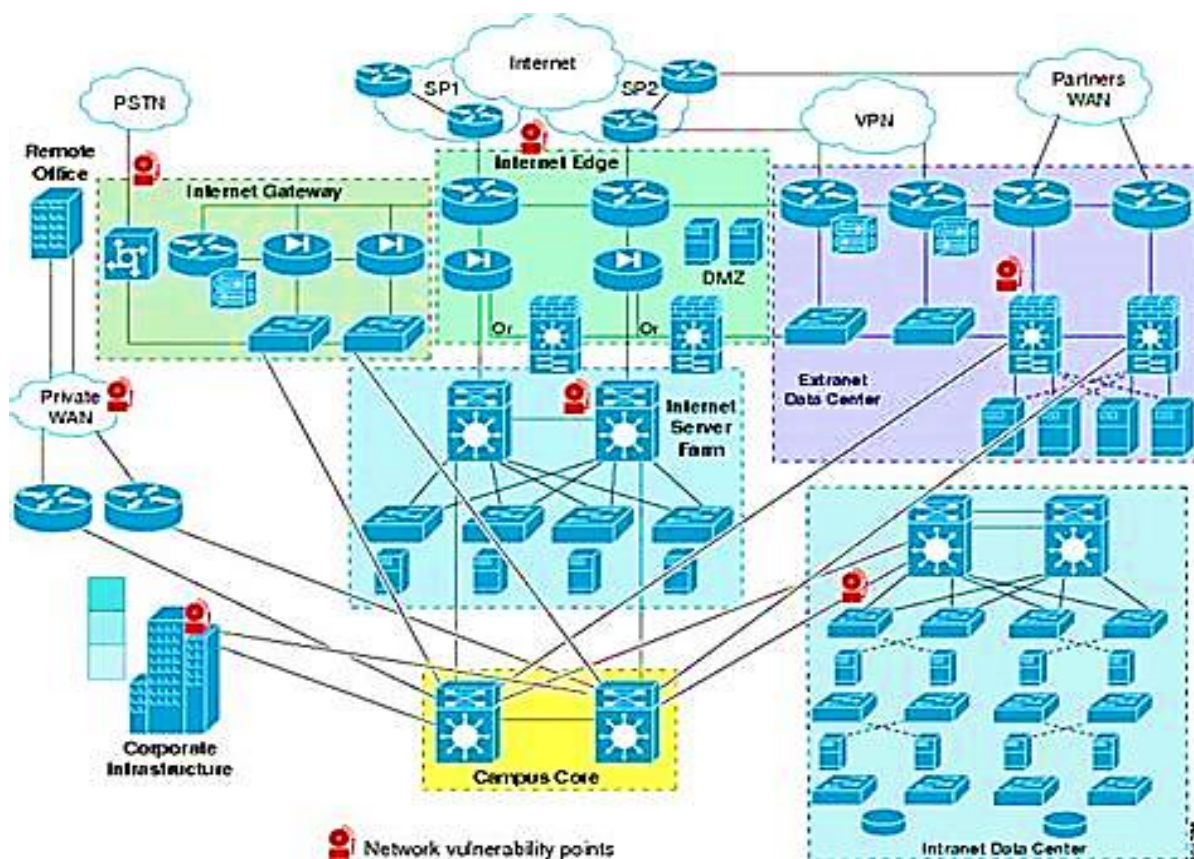


Рис. 6.1. Багаторівнева архітектура корпоративної мережі з урахуванням безпеки та зон довіри

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Архітектура корпоративної мережі зазвичай має ієрархічну структуру, що складається з трьох основних рівнів:

- **Ядро (core layer)** — основна магістраль мережі, яка забезпечує високу швидкість передачі даних між ключовими сегментами та центрами обробки інформації. На цьому рівні застосовуються високопродуктивні маршрутизатори та комутатори з підтримкою резервування каналів і протоколів динамічної маршрутизації (OSPF, BGP), а також налаштовується шифрування між сегментами для запобігання перехопленню трафіку.
- **Розподільний рівень (distribution layer)** — відповідає за фільтрацію, маршрутизацію, застосування політик безпеки та обмеження доступу між

окремими підмережами. Тут реалізуються механізми VLAN для логічної ізоляції підрозділів, міжмережеві екрани для контролю трафіку та системи IDS/IPS для виявлення аномалій.

▪ **Рівень доступу (access layer)** — забезпечує підключення кінцевих користувачів, робочих станцій, принтерів, мобільних пристроїв і сенсорних вузлів. На цьому рівні впроваджуються механізми аутентифікації (802.1X), контролю MAC-адрес, сегментації гостей мереж і обмеження привілеїв користувачів.

Ключовим елементом архітектури безпеки є сегментація мережі. Поділ інфраструктури на логічні або фізичні зони дозволяє ізолювати критичні ресурси — наприклад, сервер баз даних, фінансові або HR-системи — від звичайних користувацьких сегментів. Для розміщення зовнішніх вебсервісів та поштових серверів створюється демілітаризована зона (DMZ), яка виступає буфером між внутрішньою мережею та Інтернетом. Це дає змогу контролювати вхідний і вихідний трафік, знижуючи ризик проникнення через публічні сервіси. Ключовим елементом архітектури безпеки є сегментація мережі. Поділ інфраструктури на логічні або фізичні зони дозволяє ізолювати критичні ресурси — наприклад, сервер баз даних, фінансові або HR-системи — від звичайних користувацьких сегментів. Для розміщення зовнішніх вебсервісів та поштових серверів створюється демілітаризована зона (DMZ), яка виступає буфером між внутрішньою мережею та Інтернетом. Це дає змогу контролювати вхідний і вихідний трафік, знижуючи ризик проникнення через публічні сервіси. Крім того, сегментація підтримує принцип найменших привілеїв, коли користувачі та системи отримують доступ лише до необхідних ресурсів у межах своєї зони. Для підвищення гнучкості управління безпекою використовуються технології віртуалізації сегментів (micro-segmentation), що дозволяють створювати динамічні політики на рівні окремих додатків і сервісів. Такий підхід значно ускладнює розповсюдження шкідливого коду в мережі та забезпечує локалізацію інцидентів без впливу на критичні компоненти системи.

Особливу роль у побудові сучасної архітектури відіграє модель Zero Trust, що базується на принципі "нікому не довіряй, перевіряй завжди". Згідно з нею, доступ до ресурсів надається лише після перевірки автентичності користувача, контексту запиту, типу пристрою та відповідності політикам безпеки. Це дає можливість знизити ризики внутрішніх загроз, забезпечити динамічне керування доступом і підвищити рівень контролю за всіма взаємодіями в мережі. У рамках цієї моделі активно застосовуються технології мікросегментації, що дозволяють ізолювати кожен ресурс і мінімізувати потенційне поширення атаки. Важливою складовою Zero Trust є безперервна оцінка довіри, коли рівень доступу автоматично коригується відповідно до поведінкових факторів користувача або стану пристрою. Такий підхід створює адаптивну екосистему безпеки, у якій

кожна транзакція проходить перевірку незалежно від її джерела, що забезпечує високий рівень стійкості корпоративної мережі до сучасних кіберзагроз.

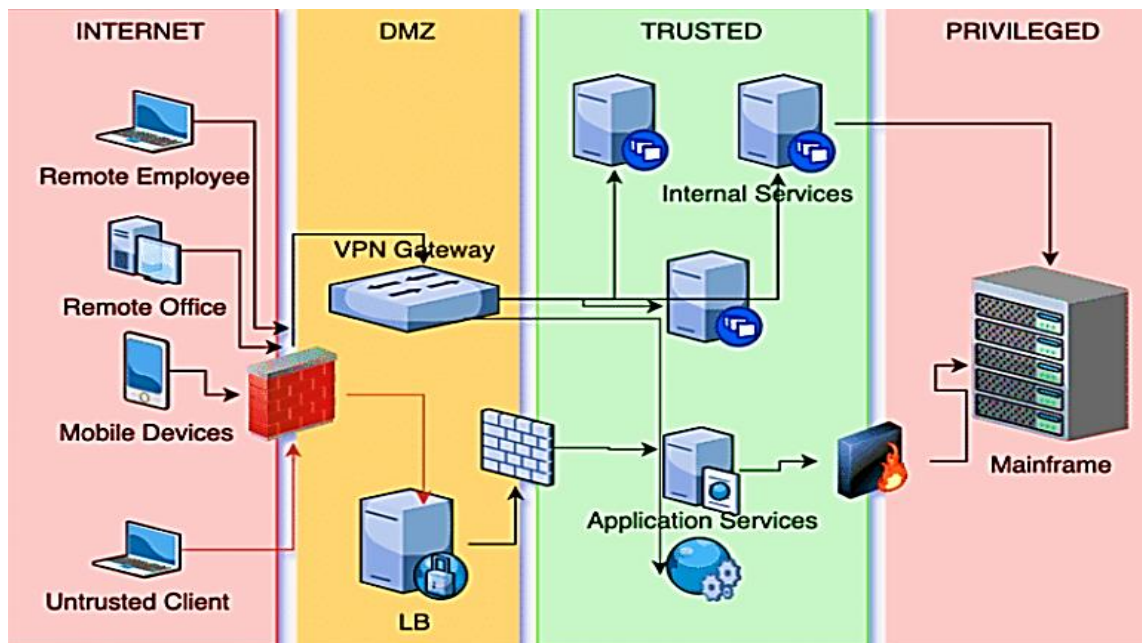


Рис. 6.2. Архітектура корпоративної мережі з урахуванням безпеки
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 6.2 зображено типовий приклад архітектури корпоративної мережі з урахуванням безпеки, що складається з чотирьох логічних зон — Internet, DMZ (демілітаризована зона), Trusted (внутрішня довірена зона) та Privileged (зона з підвищеними правами доступу). У зовнішньому сегменті Internet розташовані мобільні пристрої, віддалені офіси, робочі станції працівників і клієнти з недовіреного середовища, які ініціюють підключення через захисний екран (firewall). Далі трафік надходить у DMZ, де функціонують балансувальник навантаження (LB) та шлюз VPN, що забезпечують безпечний доступ і фільтрацію запитів.

Із DMZ дозволено обмежену взаємодію з довіреним внутрішнім сегментом Trusted, у якому розташовані внутрішні сервери, застосунки й служби, що працюють під контролем систем моніторингу та політик безпеки. Між зонами встановлено міжмережеві екрани, які контролюють напрямки обміну даними, дозволяючи лише санкціоновані запити. Найзахищенішою частиною архітектури є зона Privileged, де зберігаються основні обчислювальні ресурси — сервери баз даних і головні облікові системи (mainframe), доступ до яких здійснюється лише з перевірених внутрішніх служб за принципом найменших привілеїв. Така модель архітектури реалізує концепцію багаторівневого захисту (defense in depth) і поєднує механізми ізоляції, фільтрації, шифрування та автентифікації. Вона

гарантує, що навіть у разі компрометації одного сегмента зловмисник не отримає прямого доступу до критичних ресурсів підприємства, забезпечуючи тим самим цілісність, конфіденційність і контрольований обмін даними у корпоративній мережі.

Не менш важливим аспектом є захист каналів передавання даних. Для цього використовуються протоколи захищеного зв'язку, зокрема TLS/SSL, IPSec, SSH, WireGuard, що гарантують шифрування інформації під час обміну між клієнтами й серверами. Для віддалених співробітників створюються VPN-тунелі, які забезпечують безпечне підключення до корпоративних ресурсів через Інтернет без ризику перехоплення даних. Крім того, для підвищення рівня довіри застосовуються сертифікати цифрової автентифікації, механізми управління ключами (PKI) та регулярне оновлення криптографічних алгоритмів. Захищені канали зв'язку часто поєднуються з системами моніторингу трафіку, що дозволяють своєчасно виявляти спроби перехоплення або підміни даних. Такий підхід забезпечує цілісність переданої інформації, автентичність джерела та знижує ризик реалізації атак типу «людина посередині» (MITM).

У структурі архітектури корпоративної мережі передбачено також механізми моніторингу й управління подіями безпеки. Інтеграція систем SIEM (Security Information and Event Management) і SOAR (Security Orchestration, Automation and Response) дозволяє виявляти інциденти, аналізувати журнали подій і автоматизувати реагування на типові загрози. Такий підхід формує основу для безперервного контролю безпеки та підтримує принципи кіберстійкості.

В умовах розвитку гібридних і хмарних середовищ корпоративна архітектура має забезпечувати захист між локальними дата-центрами, віртуальними мережами (VPC) і хмарними платформами (AWS, Azure, Google Cloud). Це передбачає впровадження федеративної ідентифікації, централізованого керування доступом, шифрування даних "у русі" й "у стані спокою", а також багатофакторної аутентифікації.

Отже, архітектура корпоративної мережі з урахуванням безпеки — це не просто схема з'єднань і маршрутизаторів, а цілісна система, що об'єднує політики, стандарти, технології й процеси управління ризиками. Її ефективність визначається не лише наявністю сучасного обладнання, а й правильністю розподілу рівнів доступу, надійністю шифрування, здатністю до моніторингу та адаптації до нових кіберзагроз. Саме така архітектура створює основу кіберстійкого підприємства, готового до роботи в умовах динамічного цифрового середовища. Таким чином, архітектура корпоративної мережі з урахуванням безпеки — це не лише технічна побудова мережевої інфраструктури, а цілісна концепція, що поєднує політику безпеки, стандарти, технічні рішення й організаційні заходи. Вона формує основу надійного функціонування

корпоративних інформаційних систем, здатних протистояти сучасним кіберзагрозам і забезпечувати безперервність бізнес-процесів.

6.2. Використання VLAN, VPN і тунелювання

Використання VLAN, VPN і тунелювання є одним із ключових напрямів підвищення безпеки корпоративних мереж, оскільки ці технології забезпечують логічну ізоляцію трафіку, захист передавання даних і контроль доступу до ресурсів підприємства. Впровадження VLAN, VPN і тунелювання дозволяє створити багаторівневу систему безпеки, у якій кожен рівень виконує свою функцію — від сегментації внутрішньої мережі до шифрування трафіку між географічно віддаленими офісами. VLAN забезпечує контроль доступу на локальному рівні, дозволяючи чітко розділити мережеву інфраструктуру за відділами, ролями користувачів чи типами сервісів, що істотно зменшує ризик внутрішніх інцидентів безпеки. VLAN також сприяє впровадженню принципу мінімальних привілеїв, коли кожен користувач або пристрій має доступ лише до тих ресурсів, які необхідні для виконання його функцій. Такий підхід значно ускладнює несанкціоноване переміщення потенційного зловмисника всередині мережі, обмежуючи наслідки можливих атак лише одним сегментом. Крім того, ізоляція трафіку між VLAN підвищує продуктивність мережі, оскільки зменшується кількість широкомовних запитів і знижується навантаження на комутатори. У результаті корпоративна мережа стає більш стійкою, передбачуваною й легкою для адміністрування, забезпечуючи одночасно високу швидкодію та належний рівень інформаційної безпеки.

VPN гарантує безпечну взаємодію між віддаленими співробітниками, філіями чи партнерами, створюючи зашифровані канали обміну даними навіть через відкритий Інтернет. Тунелювання, у свою чергу, забезпечує прозору передачу пакетів різних протоколів у межах захищених каналів, що робить його ефективним рішенням для побудови гібридних корпоративних мереж і інтеграції з хмарними середовищами. Сукупне застосування цих технологій формує єдину стратегію кіберзахисту, в якій усі канали зв'язку контролюються, а доступ до ресурсів обмежується згідно з політиками безпеки. У такій архітектурі зловмисник не може легко перетнути межі між сегментами мережі або перехопити дані під час передавання, оскільки інформація шифрується та проходить через контрольні вузли. Крім того, ці технології підтримують централізоване керування, що дозволяє адміністраторам у режимі реального часу відстежувати активність користувачів, застосовувати правила безпеки та швидко реагувати на інциденти. Таким чином, використання VLAN, VPN і тунелювання

створює комплексну, масштабовану та адаптивну систему мережевого захисту, яка підвищує стійкість корпоративної інфраструктури до сучасних кіберзагроз.

Використання VLAN

Віртуальні локальні мережі (VLAN) дозволяють створювати логічно відокремлені сегменти всередині однієї фізичної інфраструктури, розділяючи користувачів і сервіси за функціональними, організаційними або безпековими критеріями. Це дає змогу мінімізувати ризик внутрішніх загроз, обмежити розповсюдження широкомовного трафіку та знизити навантаження на мережеві пристрої. VLAN-архітектура забезпечує ефективне впровадження політик доступу: наприклад, офісні користувачі, серверне обладнання, системи відеоспостереження та гостьові мережі можуть існувати в різних віртуальних сегментах, між якими встановлюються чітко регламентовані правила маршрутизації та фільтрації. Завдяки використанню VLAN адміністратор мережі отримує можливість централізовано керувати потоками трафіку та контролювати доступ між різними сегментами без потреби у фізичному розділенні мережевої інфраструктури. Це значно спрощує масштабування мережі та підвищує її гнучкість при розширенні або модернізації корпоративних систем.

На рис. 6.3 представлено приклад побудови мережевої інфраструктури з використанням віртуальних локальних мереж (VLAN), що демонструє логічну сегментацію мережі на різні групи користувачів і пристроїв без зміни фізичної топології. У даній схемі створено дві VLAN — VLAN 10 (позначену зеленим кольором) та VLAN 20 (позначену фіолетовим кольором), які об'єднують відповідні робочі станції (PC1–PC9) у незалежні мережеві домени. Кожна VLAN має власну підмережу з унікальним діапазоном IP-адрес: наприклад, для VLAN 10 — мережа 10.10.10.0/24, а для VLAN 20 — 20.20.20.0/24. Завдяки цьому користувачі однієї VLAN можуть взаємодіяти між собою, не створюючи широкомовного трафіку для інших сегментів.

Комутатори (Switch A, B, C), зображені на схемі, з'єднані між собою через транкові канали (TRUNK), які дозволяють передавати трафік кількох VLAN одночасно. Це дає можливість підтримувати логічне розділення трафіку між різними сегментами на всіх рівнях корпоративної інфраструктури. Кожен порт комутатора призначено до певної VLAN, що гарантує чітке дотримання політик безпеки та обмеження доступу користувачів лише до ресурсів своєї підмережі. Такий підхід дозволяє ефективно керувати мережею, зменшити ризик внутрішніх інцидентів, оптимізувати маршрутизацію трафіку й спростити адміністрування великих корпоративних середовищ. Таким чином, наведена схема демонструє переваги використання VLAN для підвищення керованості, безпеки й масштабованості корпоративної мережі, забезпечуючи ізоляцію трафіку, зниження навантаження на обладнання та можливість централізованого контролю доступу до критичних ресурсів підприємства.

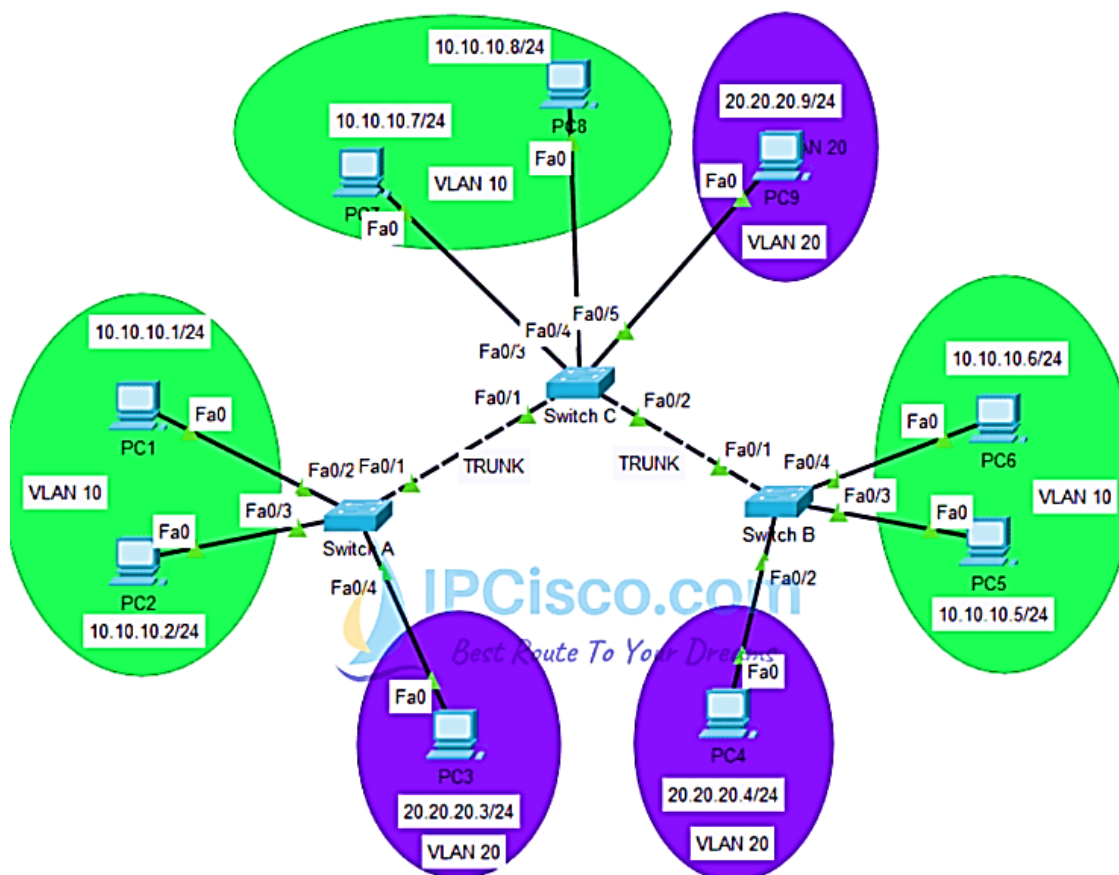


Рис. 6.3. Приклад побудови віртуальних локальних мереж (VLAN) у корпоративній інфраструктурі

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

У межах VLAN можна застосовувати різні рівні пріоритетів трафіку (QoS), що дозволяє оптимізувати роботу критичних сервісів — наприклад, VoIP-зв'язку або систем відеоконференцій. Також VLAN забезпечує більш точну ідентифікацію пристроїв у мережі, оскільки кожен сегмент має власний унікальний ідентифікатор (VLAN ID), що полегшує моніторинг і аудит активності користувачів. У системах з підвищеними вимогами до безпеки VLAN часто комбінуються з технологіями 802.1Q і 802.1X, які дозволяють здійснювати аутентифікацію на рівні порту комутатора та шифрування даних на каналному рівні. Така інтеграція унеможливує несанкціоноване підключення пристроїв і захищає від атак типу VLAN hopping. Додатково VLAN спрощує реалізацію політики найменших привілеїв, коли доступ користувачів обмежується виключно їхнім сегментом або службовою роллю. У результаті корпоративна мережа стає більш стійкою, керованою та захищеною, а потенційні інциденти

безпеки локалізуються в межах одного сегмента без впливу на всю інфраструктуру.

Використання VPN

Для організації захищеного віддаленого доступу застосовується VPN (Virtual Private Network) — технологія створення віртуальних приватних каналів у публічних мережах, які шифрують дані та забезпечують автентифікацію користувачів. Використання VPN дозволяє віддаленим співробітникам, філіям і партнерам безпечно підключатися до внутрішніх ресурсів підприємства через Інтернет, не ризикуючи втратити конфіденційність переданої інформації. Залежно від рівня реалізації, VPN може бути побудована на базі протоколів IPSec, SSL/TLS або WireGuard, які гарантують цілісність даних, перевірку ідентичності та захист від атак типу «людина посередині» (MITM). IPSec зазвичай використовується для з'єднання між мережами (site-to-site), тоді як SSL/TLS застосовується для індивідуальних користувачів (remote access VPN). У корпоративному середовищі все частіше впроваджуються гібридні VPN-рішення, що поєднують захищене з'єднання з багатофакторною аутентифікацією, обліком пристроїв і динамічним контролем доступу відповідно до політик безпеки Zero Trust.

На рис. 6.4 схематично зображено процес створення та функціонування VPN-з'єднання, яке забезпечує захищений канал обміну даними між користувачем і вебресурсом через публічну мережу Інтернет. Вихідні дані з пристрою користувача спочатку проходять через провайдера (ISP) і маршрутизатор, після чого спрямовуються до VPN-сервера, який створює зашифрований тунель між клієнтом і віддаленим сервером. У цьому тунелі вся інформація інкапсулюється та шифрується за допомогою криптографічних протоколів, таких як IPSec або TLS, що унеможливорює перехоплення або модифікацію даних третіми сторонами.

VPN-сервер виступає посередником між користувачем і цільовим вебресурсом, приховуючи справжню IP-адресу користувача та забезпечуючи анонімність під час передавання інформації. Після проходження через VPN-сервер зашифровані дані потрапляють до вебсерверу, де розшифровуються лише після перевірки цілісності та автентичності. У зворотному напрямку зворотний трафік також проходить через той самий зашифрований канал, що гарантує безпечну доставку відповідей від сайту до клієнта.

Такий механізм дозволяє створювати надійний захист від атак типу «людина посередині» (MITM), несанкціонованого моніторингу трафіку та втручання з боку провайдерів або зловмисників. У корпоративному середовищі ця технологія дає змогу співробітникам працювати з внутрішніми ресурсами підприємства з будь-якої точки світу, зберігаючи високий рівень конфіденційності, цілісності та доступності даних.



Рис. 6.4. Принцип роботи VPN-з'єднання у корпоративній мережі
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Крім того, сучасні VPN-рішення підтримують централізоване керування ключами шифрування та автоматичне оновлення сертифікатів, що підвищує рівень захищеності каналів зв'язку. Для підвищення продуктивності використовуються протоколи з оптимізованими алгоритмами шифрування, які зменшують затримки передачі даних без зниження рівня безпеки. У великих корпоративних мережах VPN інтегрується з системами SIEM і моніторингу для виявлення підозрілих дій користувачів та фіксації спроб несанкціонованого доступу. Також впроваджується сегментація VPN-з'єднань — поділ користувачів на групи за рівнем довіри або за типом пристрою, що дозволяє більш гнучко управляти доступом до ресурсів. У разі порушення політик або виявлення аномалій система автоматично припиняє сеанс з'єднання, запобігаючи розповсюдженню загроз у внутрішній мережі. Таким чином, VPN-технології виступають невід'ємним елементом комплексної системи кіберзахисту підприємства, забезпечуючи безпечну взаємодію всіх користувачів і підрозділів незалежно від їхнього фізичного розташування.

Використання тунелювання

Ще одним важливим механізмом захисту є тунелювання, що забезпечує інкапсуляцію пакетів даних одного протоколу в інший для безпечного передавання через потенційно незахищене середовище. Завдяки тунелюванню корпоративні мережі можуть організовувати захищений обмін даними між територіально розподіленими підрозділами або хмарними інфраструктурами. Найбільш поширеними технологіями тунелювання є GRE (Generic Routing Encapsulation), L2TP (Layer 2 Tunneling Protocol), OpenVPN, а також WireGuard,

який вирізняється високою продуктивністю, мінімальними затримками та сучасними криптографічними алгоритмами. Тунелі дозволяють передавати дані навіть у разі використання публічних мереж, створюючи віртуальну захищену «трубу», крізь яку проходить лише зашифрований трафік.

На рис. 6.5 представлено принцип роботи GRE-тунелю (Generic Routing Encapsulation), який забезпечує інкапсуляцію мережевого трафіку для безпечного передавання даних через публічну мережу Інтернет. GRE-тунель створює віртуальний канал між двома маршрутизаторами — клієнтським (Client Router, CR1) і маршрутизатором центру очищення трафіку (Scrubbing Center Router, SCR1). Цей канал діє як захищена «труба», у межах якої всі дані інкапсулюються в додатковий заголовок і передаються у зашифрованому вигляді, приховуючи внутрішню структуру корпоративної мережі.

Кожен кінець тунелю має дві IP-адреси — публічну, що використовується для зв'язку через Інтернет (наприклад, 3.3.3.1 і 4.4.4.1), та внутрішню тунельну адресу (192.168.1.1 і 192.168.1.2), яка використовується для обміну даними всередині зашифрованого каналу. Така схема дозволяє передавати трафік між корпоративною мережею клієнта та віддаленим центром без необхідності створення фізичних з'єднань, забезпечуючи при цьому високу швидкість і гнучкість маршрутизації. GRE-тунель є універсальним, оскільки може інкапсулювати пакети різних протоколів, включно з IPv4, IPv6 або навіть нестандартними корпоративними протоколами. Ця технологія часто використовується для організації захищеного зв'язку між географічно віддаленими підрозділами, побудови резервних каналів або реалізації інтеграції з хмарними сервісами. Завдяки GRE-тунелюванню можливо ефективно забезпечити цілісність і конфіденційність трафіку, мінімізувати ризики перехоплення та оптимізувати взаємодію між різними сегментами корпоративної мережі в умовах відкритого Інтернет-середовища.



Рис. 6.5. Схематичне зображення GRE-тунелювання між клієнтською мережею та центром очищення трафіку

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Тунелювання забезпечує не лише конфіденційність, а й цілісність переданої інформації, оскільки дані, інкапсульовані в інший протокол, стають

недоступними для перехоплення та модифікації третіми сторонами. Цей механізм часто використовується у великих підприємствах, де необхідно поєднати декілька філій або віддалених офісів в єдину корпоративну мережу без будівництва окремих фізичних каналів зв'язку. У сучасних мережах тунелі також застосовуються для інтеграції з хмарними платформами, що дозволяє створювати безпечні з'єднання між локальними дата-центрами та сервісами AWS, Azure або Google Cloud. Однією з переваг тунелювання є можливість підтримки мультипротокольного трафіку, коли в одному каналі можуть одночасно передаватися пакети різних протоколів, наприклад IPv4 та IPv6. Для підвищення безпеки часто впроваджується комбіноване тунелювання, де технології GRE або L2TP поєднуються з IPSec для створення додаткового шару шифрування. Такий підхід мінімізує ризики компрометації навіть у разі зламу окремого тунельного сегмента. Адміністратори можуть налаштовувати параметри тунелів динамічно, використовуючи політики, що враховують тип трафіку, географічне розташування вузлів або поточний рівень ризику. У результаті тунелювання стає невід'ємним інструментом побудови захищених гібридних інфраструктур, які поєднують локальні, віддалені та хмарні ресурси в єдиному захищеному інформаційному просторі підприємства.

Комбінація VLAN, VPN і тунелювання забезпечує багаторівневу ізоляцію, шифрування й контроль комунікацій, формуючи цілісну модель захищеної корпоративної інфраструктури. VLAN вирішує завдання логічного розмежування трафіку всередині підприємства, VPN — захищає з'єднання між віддаленими користувачами чи філіями, а тунелювання — гарантує конфіденційність при передаванні даних через недовірені мережі. У сукупності ці технології створюють фундамент для впровадження сучасних концепцій безпеки, таких як Zero Trust Network Access (ZTNA) і Software Defined Perimeter (SDP), які забезпечують динамічне, контекстно-залежне керування доступом і постійний контроль безпеки в усьому цифровому периметрі корпоративної мережі.

6.3. КОНТРОЛЬ ДОСТУПУ ТА БАГАТОРІВНЕВА АУТЕНТИФІКАЦІЯ

Контроль доступу та багаторівнева аутентифікація є фундаментальними складовими системи інформаційної безпеки корпоративних мереж і забезпечують захист ресурсів від несанкціонованого використання, модифікації чи витоку даних. Контроль доступу передбачає управління правами користувачів і пристроїв щодо доступу до інформаційних активів підприємства на основі принципів ідентифікації, автентифікації та авторизації. Процес ідентифікації визначає, хто саме намагається отримати доступ до системи, автентифікація

підтверджує достовірність цієї особи, а авторизація встановлює, до яких саме ресурсів і на яких умовах вона може мати доступ.

У сучасних корпоративних мережах застосовуються різні моделі контролю доступу — дискреційна (DAC), модель мандатного доступу (MAC), рольова (RBAC) та атрибутна (ABAC). Дискреційна модель базується на правах власника ресурсу, тоді як мандатна використовує суворо регламентовані політики безпеки, визначені адміністраторами. Рольова модель RBAC реалізує доступ відповідно до службових обов'язків користувача, а атрибутна ABAC додає гнучкість, дозволяючи визначати доступ на основі набору динамічних атрибутів — таких як місцезнаходження, тип пристрою, час доби або рівень ризику.

Багаторівнева аутентифікація (Multi-Factor Authentication, MFA)

Багаторівнева аутентифікація (Multi-Factor Authentication, MFA) суттєво підвищує рівень безпеки корпоративних систем, оскільки вимагає від користувача підтвердження особи за допомогою двох або більше незалежних факторів. Традиційно виділяють три категорії факторів: те, що користувач знає (пароль, PIN-код, відповідь на секретне запитання), те, що користувач має (смарт-карта, токен, мобільний пристрій) і те, ким він є (біометричні дані — відбитки пальців, розпізнавання обличчя, голосу чи райдужки ока). У корпоративних середовищах усе частіше впроваджуються системи адаптивної аутентифікації, які динамічно визначають рівень перевірки залежно від контексту — наприклад, якщо вхід здійснюється з нового пристрою чи географічного місця, система автоматично запитує додатковий фактор підтвердження.

На рис. 6.6 наведено узагальнену схему процесу багаторівневої аутентифікації, яка демонструє використання трьох основних категорій факторів підтвердження особи користувача. Перший етап — те, що користувач знає — передбачає введення логіна та пароля, тобто класичну перевірку знань, яка є найпоширенішим, але найбільш уразливим способом автентифікації. Другий етап — те, що користувач має — реалізується за допомогою мобільного пристрою, на який надходить запит на підтвердження входу. Користувач повинен вручну підтвердити дію, що унеможлиблює використання викрадених облікових даних без фізичного доступу до пристрою. Третій етап — те, ким користувач є — забезпечується через біометричну перевірку, наприклад, сканування відбитка пальця або розпізнавання обличчя.

Така комбінація факторів створює стійку систему перевірки автентичності, у якій кожен рівень незалежно підвищує загальний рівень безпеки. Навіть у разі компрометації пароля злоумисник не зможе отримати доступ без другого чи третього фактора. Подібні багаторівневі механізми активно впроваджуються у

корпоративних мережах і хмарних середовищах, оскільки забезпечують баланс між зручністю користування та високим рівнем захисту інформаційних ресурсів підприємства.

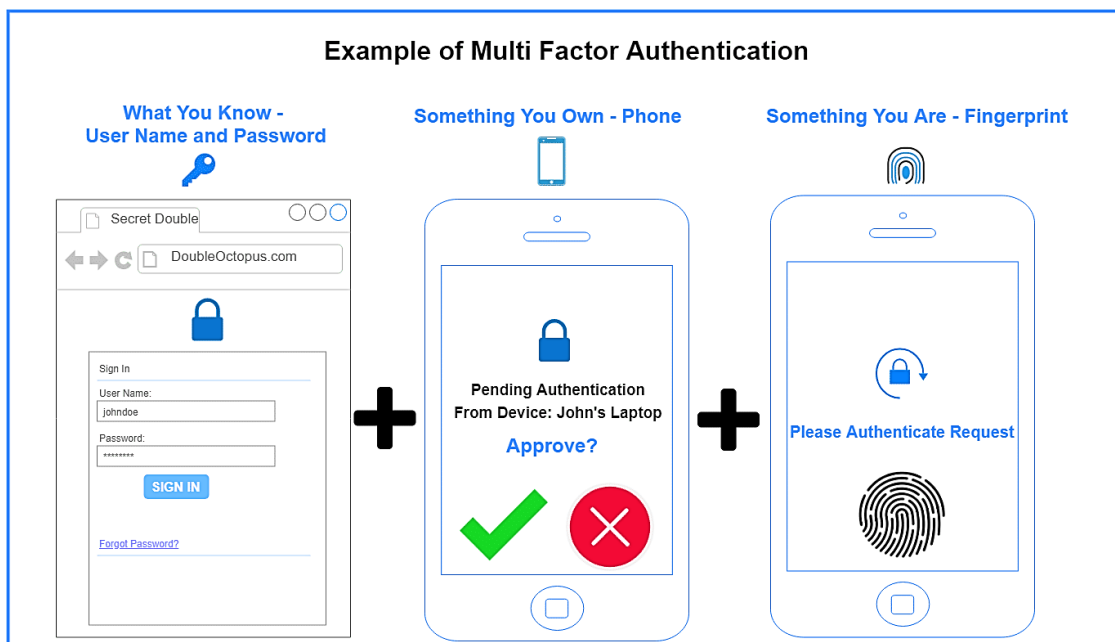


Рис. 6.6. Схематичне зображення GRE-тунелювання між клієнтською мережею та центром очищення трафіку

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Багаторівнева аутентифікація дозволяє створити додатковий рівень захисту навіть у разі компрометації одного з факторів, зменшуючи ймовірність несанкціонованого доступу до корпоративних ресурсів. Такий підхід ефективно протидіє фішинговим атакам, перехопленню паролів та використанню викрадених облікових даних, оскільки зломиснику для входу необхідно володіти не лише знанням, а й фізичним пристроєм або біометричними характеристиками користувача. Сучасні системи MFA часто інтегруються з мобільними застосунками, які генерують одноразові коди (OTP) або надсилають push-повідомлення для підтвердження входу. Крім того, набувають популярності апаратні ключі безпеки (наприклад, YubiKey), які реалізують криптографічну перевірку особи через протоколи FIDO2 та WebAuthn.

Для підвищення зручності користувачів і зменшення ризику людського фактора дедалі ширше застосовується passwordless-аутентифікація, де вхід здійснюється без введення паролів, а підтвердження особи виконується за допомогою біометрії, токенів або QR-коду. У корпоративних середовищах такі рішення поєднуються з платформами Identity and Access Management (IAM) та Single Sign-On (SSO), що дозволяє централізовано управляти ідентичностями та

політиками доступу. У межах архітектури Zero Trust багаторівнева аутентифікація стає обов'язковою умовою для кожного запиту доступу, навіть якщо користувач уже перебуває всередині корпоративної мережі.

Додатково MFA може бути інтегрована з аналітичними системами поведінкової безпеки (Behavioral Analytics), які відстежують типові дії користувача — наприклад, час активності, IP-адреси, пристрої чи шаблони натискання клавіш. У разі виявлення відхилень система автоматично вимагає повторного підтвердження особи або тимчасово блокує доступ. Такий адаптивний і динамічний підхід забезпечує баланс між високим рівнем безпеки та зручністю користування, роблячи багаторівневу аутентифікацію невід'ємним елементом комплексного захисту сучасних корпоративних мереж.

Управління політиками доступу

Для централізованого управління політиками доступу використовуються технології Single Sign-On (SSO) та Identity and Access Management (IAM), які дозволяють користувачам автентифікуватися один раз і отримувати доступ до кількох корпоративних сервісів без повторного введення облікових даних. Такі рішення інтегруються з протоколами безпеки, як-от LDAP, Kerberos, RADIUS, SAML або OAuth 2.0, забезпечуючи єдину систему управління ідентичностями. У поєднанні з Zero Trust Network Access (ZTNA) та концепцією least privilege (принцип найменших привілеїв), контроль доступу стає динамічним — користувач отримує лише ті права, які необхідні для виконання конкретного завдання, і лише на час, коли це потрібно.

Для централізованого управління політиками доступу використовуються технології Single Sign-On (SSO) та Identity and Access Management (IAM), які створюють єдину інфраструктуру ідентифікації та авторизації користувачів у межах корпоративної мережі. Це дозволяє суттєво зменшити кількість точок входу та спростити адміністрування доступу, оскільки користувач проходить автентифікацію лише один раз, отримуючи дозвіл на використання кількох застосунків, систем і хмарних сервісів без повторного введення облікових даних. Завдяки цьому підвищується не лише зручність, а й безпека — скорочується кількість паролів, які потрібно запам'ятовувати, що знижує ризик фішингу або компрометації облікових записів.

Системи IAM включають централізоване керування життєвим циклом облікових записів, тобто автоматизують створення, модифікацію, блокування та видалення доступів під час зміни ролі або звільнення співробітника. Такі рішення інтегруються з протоколами безпеки, як-от LDAP (Lightweight Directory Access Protocol), Kerberos, RADIUS, SAML (Security Assertion Markup Language) або OAuth 2.0, забезпечуючи сумісність між різними платформами та сервісами. Наприклад, протокол SAML використовується для обміну токенами

автентифікації між веб-додатками, а OAuth 2.0 — для надання обмеженого доступу до ресурсів без розкриття облікових даних користувача.

У сучасних корпоративних інфраструктурах IAM і SSO інтегруються з Zero Trust Network Access (ZTNA) — підходом, що передбачає повну відмову від традиційного довірчого периметра. У межах цієї концепції кожен запит доступу перевіряється незалежно, навіть якщо користувач уже перебуває всередині корпоративної мережі. Рішення ZTNA спільно з IAM забезпечують контекстно-залежний контроль доступу, враховуючи фактори часу, місцезнаходження, тип пристрою та поточний рівень ризику.

Додатково впроваджується принцип найменших привілеїв (least privilege), який означає, що користувач отримує мінімально необхідні права виключно для виконання своїх службових обов'язків. Доступ може бути наданий тимчасово або автоматично відкликаний після завершення завдання. Такий підхід мінімізує можливість несанкціонованого використання ресурсів, зменшує ризики внутрішніх загроз і підвищує прозорість управління безпекою.



Рис. 6.7. Управління політиками доступу в корпоративній мережі
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 6.7 представлено узагальнену схему централізованого управління політиками доступу, що реалізується за допомогою технологій SSO (Single Sign-On) та IAM (Identity and Access Management). Користувач здійснює єдину автентифікацію, після чого його запит спрямовується через сервер IAM/SSO, який перевіряє повноваження та забезпечує доступ до корпоративних ресурсів згідно з принципом найменших привілеїв (Least Privilege). Компонент ZTNA (Zero Trust Network Access) додає додатковий рівень безпеки, перевіряючи кожен запит незалежно від місцезнаходження користувача чи типу пристрою. Далі користувач отримує дозвіл лише на ті застосунки, ресурси або сервери, що необхідні для виконання конкретного завдання, а доступ може бути обмежений

у часі або відкликаний за умов зміни контексту. Така модель забезпечує адаптивний, динамічний контроль доступу, підвищуючи рівень захисту корпоративної інфраструктури.

У комплексі технології SSO, IAM, ZTNA та least privilege формують адаптивну модель управління доступом, яка поєднує централізований контроль, гнучкість політик і високий рівень автоматизації. Вони дозволяють підприємствам ефективно керувати доступом у розподілених, хмарних і гібридних середовищах, забезпечуючи при цьому відповідність міжнародним стандартам інформаційної безпеки, зокрема ISO/IEC 27001, NIST SP 800-63 і GDPR.

Моніторинг активності користувачів і пристроїв

Важливим аспектом є моніторинг активності користувачів і пристроїв. Системи User and Entity Behavior Analytics (UEBA) аналізують поведінку користувачів, визначаючи аномалії, які можуть свідчити про компрометацію облікового запису або внутрішню загрозу. У разі виявлення підозрілої активності доступ може бути тимчасово обмежений, а користувача — повторно автентифіковано або заблоковано. Такі механізми інтегруються з платформами SIEM (Security Information and Event Management) для централізованого збору, аналізу та кореляції подій безпеки в реальному часі.

На рис. 6.8 зображено узагальнену архітектуру системи моніторингу подій безпеки (SIEM — *Security Information and Event Management*), яка складається з трьох основних шарів: комунікаційного, аналітичного та шару збереження даних. На комунікаційному рівні здійснюється приймання потоків подій і сигналів тривоги в реальному часі через мережеві протоколи, зокрема TCP, а також інтеграція з вебзастосунками та API для централізованого збору інформації з різних джерел. На аналітичному рівні (Data Analysis Layer) відбувається обробка отриманих подій: дані проходять етапи попередньої фільтрації та нормалізації відповідно до заданих політик безпеки. Далі модуль кореляції аналізує залежності між подіями, використовуючи правила та схеми виявлення інцидентів. На основі цього формується оцінка ризику тривоги (Alarm Risk Assessment), де визначаються пріоритет і достовірність кожної події. Результати аналізу зберігаються у відповідних базах даних або надсилаються адміністраторам через панелі моніторингу.

Шар збереження даних (Data Persistence Layer) забезпечує накопичення історії подій і тривог, а також зберігає конфігураційні параметри SIEM, що дозволяє здійснювати подальший аудит, розслідування інцидентів і налаштування політик реагування. Така архітектура створює цілісну систему безпеки, здатну виявляти, аналізувати й пріоритезувати загрози в реальному часі, інтегруючись із UEBA, SOAR та іншими аналітичними модулями для підвищення ефективності кіберзахисту.

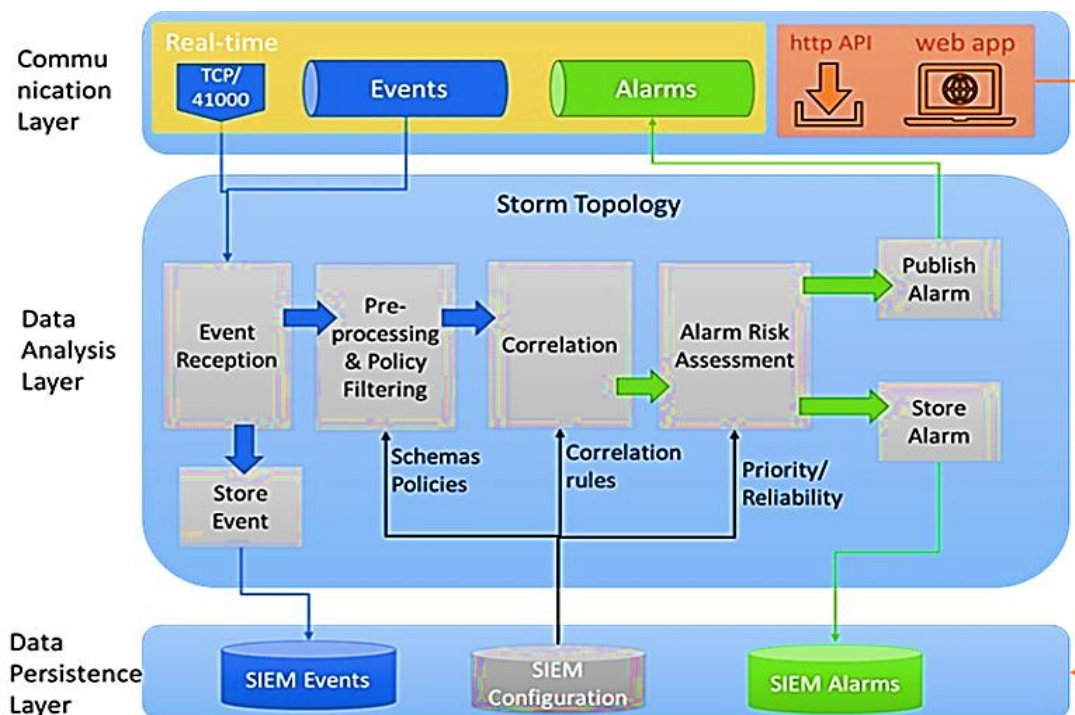


Рис. 6.8. Архітектура системи моніторингу безпеки на основі SIEM
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Моніторинг активності користувачів і пристроїв є критично важливим компонентом сучасної системи управління доступом, оскільки дозволяє своєчасно виявляти ознаки порушення безпеки та реагувати на потенційні інциденти ще до того, як вони спричинять шкоду. Системи User and Entity Behavior Analytics (UEBA) використовують методи машинного навчання, статистичного аналізу та кореляції подій для побудови профілів нормальної поведінки кожного користувача або пристрою. На основі цих профілів визначаються відхилення — наприклад, незвичайний час входу, нетипичне географічне розташування, спроби доступу до незвичних ресурсів або різке зростання обсягу переданих даних.

У разі виявлення аномалії система UEBA може автоматично генерувати сповіщення для аналітиків безпеки, ініціювати додаткову аутентифікацію користувача або ізолювати підозрілий пристрій від мережі. У поєднанні з платформами SIEM (Security Information and Event Management) ці системи створюють інтегроване середовище моніторингу, яке об'єднує журнали подій, дані мережевого трафіку, поведінкові патерни та інформацію з антивірусів і систем виявлення вторгнень (IDS/IPS). Така взаємодія дозволяє формувати повноцінну картину стану безпеки корпоративної інфраструктури в реальному часі, забезпечуючи швидке реагування на інциденти.

Крім того, сучасні системи моніторингу підтримують штучний інтелект (AI) і предиктивну аналітику, що дає змогу не лише реагувати на загрози, а й прогнозувати потенційні ризики на основі попередніх сценаріїв поведінки. Наприклад, якщо користувач зазвичай працює з офісу, але система фіксує вхід із іншої країни або підозрілої IP-адреси, доступ може бути заблокований автоматично до завершення перевірки. У корпоративних мережах із великою кількістю користувачів UEBA і SIEM також інтегруються з системами SOAR (Security Orchestration, Automation and Response), які автоматизують виконання рутинних дій — наприклад, зміну пароля, відкликання токенів чи блокування облікового запису.

На рис. 6.9 представлено узагальнену архітектуру системи User and Entity Behavior Analytics (UEBA), яка використовує технології штучного інтелекту (AI) та машинного навчання (ML) для аналізу поведінки користувачів і пристроїв з метою виявлення аномалій і потенційних загроз. На першому етапі здійснюється збір даних (Collecting Data) з різних джерел, зокрема файрволів, антивірусів, систем журналювання подій (Syslog) та систем виявлення й запобігання вторгненням (IDS/IPS). Зібрана інформація надходить до етапу базової нормалізації (Baselining Process), де формується профіль нормальної поведінки користувачів і пристроїв на основі історичних даних. Далі система переходить до етапу аналітики на базі AI/ML (AI & ML-Based Analytics System), який застосовує алгоритми навчання для порівняння поточних дій із типовими моделями поведінки. При виявленні відхилень або перевищенні порогових значень система генерує сповіщення про можливі інциденти безпеки. Ці сповіщення передаються на рівень аналізу та розслідування (Analysis & Investigation), де команди аналітиків SOC (Security Operations Center) проводять детальну перевірку, визначають рівень ризику та приймають рішення щодо реагування.

Така архітектура забезпечує безперервний моніторинг поведінки користувачів у режимі реального часу, дозволяє швидко виявляти відхилення, характерні для внутрішніх загроз або компрометації облікових записів, і автоматизує реагування через інтеграцію з SIEM і SOAR. Використання AI/ML у поєднанні з поведінковими моделями підвищує точність виявлення інцидентів, зменшує кількість хибних спрацювань і сприяє формуванню адаптивної, самонавчальної системи кіберзахисту корпоративного середовища.



Рис. 6.9. Архітектура інтелектуальної системи моніторингу активності користувачів на основі UEBA

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Таким чином, моніторинг активності користувачів і пристроїв у поєднанні з UEBA, SIEM і SOAR створює інтелектуальну екосистему безпеки, здатну виявляти, аналізувати й автоматично нейтралізувати загрози. Це забезпечує не лише контроль поточних дій, але й профілактику внутрішніх і зовнішніх атак, підвищуючи загальний рівень кіберстійкості корпоративної мережі та довіру до системи управління доступом.

Сучасні системи контролю доступу також підтримують моделі Passwordless Authentication, де замість традиційних паролів використовуються криптографічні ключі, біометрія або одноразові токени, що суттєво знижує ризики фішингу й викрадення облікових даних. Для забезпечення безпеки в розподілених і хмарних середовищах застосовуються стандарти FIDO2, WebAuthn та PKI (Public Key Infrastructure), які гарантують криптографічний захист обміну ідентифікаційними даними.

Отже, контроль доступу та багаторівнева аутентифікація формують цілісну екосистему управління ідентичностями, яка поєднує політики, технології та аналітичні механізми для забезпечення безпеки корпоративної інфраструктури. Їхня інтеграція з концепцією Zero Trust дозволяє реалізувати адаптивний, контекстно-залежний захист, що враховує поведінкові фактори, рівень ризику та стан пристроїв, створюючи ефективний бар'єр проти сучасних кіберзагроз.

6.4. ЗАХИСТ ЕЛЕКТРОННОЇ ПОШТИ ТА ВЕБ-СЕРВІСІВ

Захист електронної пошти та вебсервісів є одним із найважливіших напрямів забезпечення кібербезпеки підприємства, оскільки саме ці канали найчастіше використовуються зловмисниками для здійснення фішингових атак, поширення шкідливого програмного забезпечення, крадіжки облікових даних і компрометації корпоративних систем. Електронна пошта традиційно залишається основним інструментом ділового спілкування, але водночас і найуразливішою ланкою, тому її захист вимагає комплексного підходу, який поєднує технічні, організаційні та поведінкові заходи. Комплексна стратегія безпеки передбачає використання фільтрації контенту, шифрування, перевірки автентичності та багатофакторної аутентифікації користувачів. Важливим аспектом є навчання персоналу розпізнаванню фішингових повідомлень і підозрілої активності, що зменшує ймовірність соціальної інженерії. Для запобігання підробленню повідомлень впроваджуються технології SPF, DKIM і DMARC, які перевіряють достовірність відправників і цілісність листів. Крім того, застосування протоколів TLS, PGP або S/MIME гарантує захищену передачу інформації між поштовими серверами. У контексті вебсервісів безпека досягається через використання WAF, SSL/TLS, OAuth 2.0 та захист API від ін'єкцій і атак типу XSS чи CSRF. Усі ці заходи разом формують цілісну систему, що забезпечує надійний захист комунікаційних каналів підприємства від сучасних кіберзагроз.

Захист електронної пошти

Найефективнішим засобом протидії поштовим загрозам є впровадження багаторівневої системи фільтрації трафіку, що включає аналіз заголовків повідомлень, контенту, вкладень і посилань. Антиспам- та антивірусні шлюзи (Mail Security Gateway) перевіряють кожен вхідний лист на наявність шкідливих об'єктів, підозрілих макросів або спроб соціальної інженерії. Для виявлення фішингових атак застосовуються алгоритми машинного навчання, які аналізують доменні імена, поведінку відправника та схожість із відомими шаблонами шахрайських повідомлень.

Сучасні системи фільтрації здатні динамічно оновлювати свої бази даних загроз, використовуючи індикатори компрометації (IoC) та хмарні репутаційні сервіси. Це дозволяє виявляти навіть нові, раніше невідомі типи фішингу або шкідливих вкладень. Важливою функцією є так зване «пісочне середовище» (sandboxing), у якому вкладення листів відкриваються в ізольованому середовищі для аналізу їхньої поведінки без ризику зараження системи. Крім того, інтеграція з системами SIEM дає змогу корелювати події поштової безпеки з іншими інцидентами у корпоративній мережі. Для підвищення точності виявлення загроз застосовується поведінковий аналіз (behavioral analysis), що враховує контекст

дій користувачів і поштових клієнтів. Такий підхід забезпечує глибоку багаторівневу перевірку повідомлень, мінімізуючи ризик потрапляння небезпечних листів до користувача.

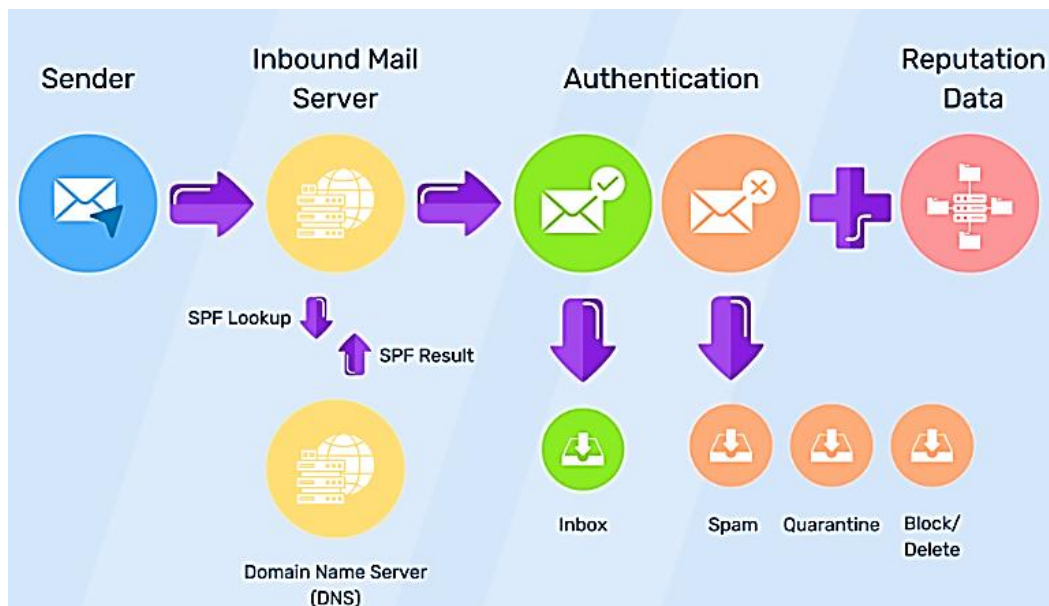


Рис. 6.10. Архітектура інтелектуальної системи моніторингу активності користувачів на основі UEBA

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 6.10 представлено спрощену схему перевірки автентичності електронних повідомлень із використанням протоколу SPF (Sender Policy Framework), який є базовим елементом системи захисту корпоративної пошти від підроблених листів і фішингових атак. Процес починається з етапу надсилання повідомлення (Sender), коли поштовий клієнт або сервер відправника ініціює передачу даних до вхідного поштового сервера (Inbound Mail Server) отримувача. Після отримання листа сервер виконує запит SPF Lookup до сервера доменних імен (DNS), щоб перевірити, чи має відправник право надсилати пошту від імені вказаного домену. У відповідь DNS повертає результат SPF Result, який визначає статус автентичності. Далі повідомлення проходить етап автентифікації (Authentication) — якщо запис SPF підтверджує легітимність відправника, лист доставляється у вхідну скриньку (Inbox). Якщо перевірка неуспішна, система оцінює ризики на основі даних репутації (Reputation Data), що враховують історію поведінки домену, IP-адресу та рівень довіри до відправника. Залежно від результату перевірки, повідомлення може бути перенаправлене у папку спаму (Spam), поміщене на карантин (Quarantine) або заблоковане/видалене (Block/Delete).

Такий підхід забезпечує ефективний захист корпоративної поштової системи від шахрайських повідомлень, підвищує довіру до електронних комунікацій і зменшує ризики компрометації облікових записів. Інтеграція SPF із технологіями DKIM та DMARC дозволяє створити комплексну модель перевірки автентичності електронної пошти, яка формує надійний бар'єр проти фішингу, спуфінгу та поширення шкідливих вкладень.

Ключову роль у забезпеченні достовірності електронних повідомлень відіграють технології автентифікації пошти — SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance). SPF визначає, які сервери мають право надсилати пошту від імені конкретного домену, DKIM додає криптографічний підпис для підтвердження цілісності повідомлення, а DMARC дозволяє власнику домену контролювати політику обробки невідповідних або підроблених листів і отримувати звіти про спроби зловживань. Використання цих технологій у комплексі істотно зменшує ризики фішингу та спуфінгу.

На рис. 6.11 зображено повний цикл перевірки електронного повідомлення за технологією DMARC (Domain-based Message Authentication, Reporting & Conformance), яка забезпечує достовірність відправника та захист корпоративної пошти від фішингу, підроблення доменів і шахрайських повідомлень. Процес починається на стороні відправника (Sender), який створює та надсилає електронний лист. Поштовий сервер відправника додає цифровий підпис DKIM (DomainKeys Identified Mail), що підтверджує цілісність і справжність вмісту повідомлення.

Після цього лист надходить на поштовий сервер отримувача (Recipient's Email Server), який виконує перевірку репутації домену, чорних списків (blacklists) і наявності автентифікаційних записів. Далі активується DMARC-політика (DMARC Policy), яка поєднує результати перевірок SPF (Sender Policy Framework) і DKIM, аналізує відповідність між доменом відправника та доменом, із якого фізично надійшов лист. Залежно від результату автентифікації застосовується одна з дій: Pass — повідомлення вважається достовірним і доставляється до вхідної скриньки, Quarantine — лист позначається як підозрілий і переміщується до папки спаму, або Block — повідомлення блокується або видаляється.

Такий механізм дозволяє ефективно запобігати підробленню електронної пошти, забезпечуючи високий рівень захисту комунікацій. DMARC виступає надбудовою над SPF і DKIM, створюючи єдиний політично орієнтований підхід до перевірки автентичності електронних повідомлень і звітності про спроби несанкціонованого використання домену. У корпоративних середовищах впровадження DMARC істотно підвищує довіру до поштових сервісів, знижує

ризиків компрометації даних і підтримує відповідність стандартам безпеки електронних комунікацій.

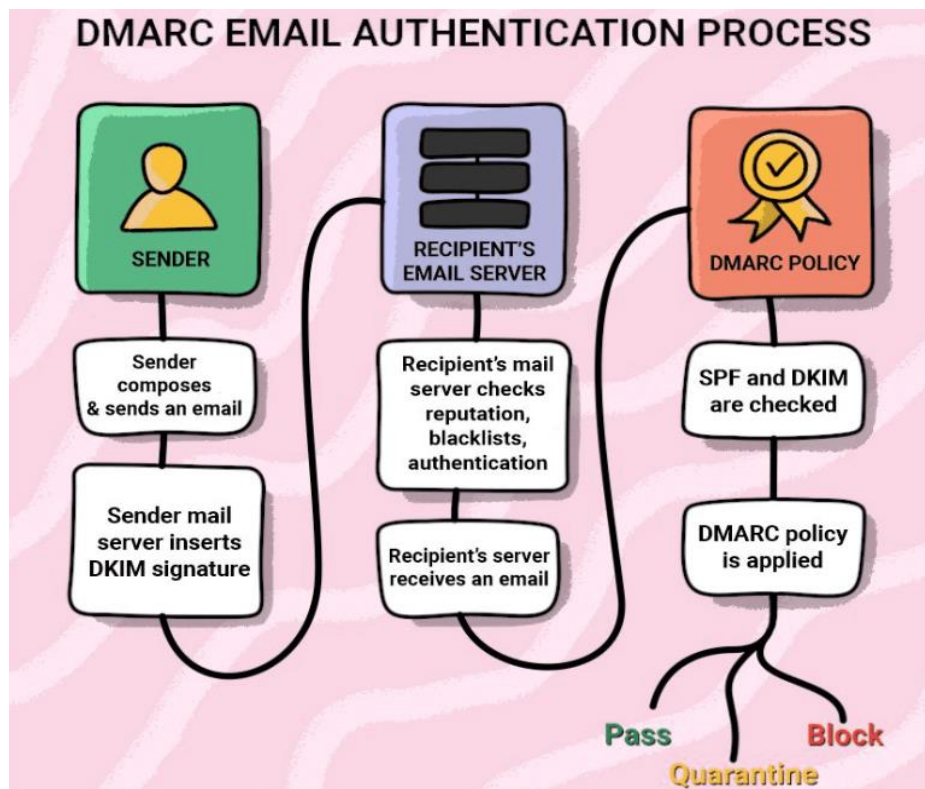


Рис. 6.11. Процес автентифікації електронної пошти за політикою DMARC
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 6. 12 показано механізм перевірки достовірності електронних повідомлень у системах корпоративної пошти з використанням трьох взаємопов'язаних технологій — SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) та DMARC (Domain-based Message Authentication, Reporting & Conformance). Процес розпочинається з надсилання повідомлення користувачем (Sender's inbox), після чого електронний лист проходить через поштовий сервер (Mail server), який звертається до DNS-сервера, де зберігаються записи SPF, DKIM і DMARC, що визначають правила автентифікації для домену відправника.

На етапі перевірки система здійснює SPF-lookup, щоб упевнитися, що пошта надійшла з дозволеного серверу, перевіряє DKIM-підпис для підтвердження цілісності повідомлення та справжності відправника, а також застосовує політику DMARC, яка поєднує результати двох попередніх перевірок і визначає подальші дії. Якщо повідомлення успішно проходить автентифікацію (Pass), воно доставляється у вхідну скриньку (Inbox) отримувача. У разі часткової невідповідності система може позначити лист як спам (Spam) або помістити його

на перевірку. Якщо ж повідомлення не проходить жодну з перевірок (Fail), воно блокується або видаляється (Block), щоб запобігти потраплянню шкідливого контенту в корпоративну поштову систему. Таким чином, представлена схема демонструє узгоджену роботу трьох ключових технологій автентифікації, які разом забезпечують високий рівень захисту електронної пошти від фішингових атак, підроблених доменів і спуфінгу, підвищуючи довіру до корпоративних комунікацій і цілісність обміну інформацією.

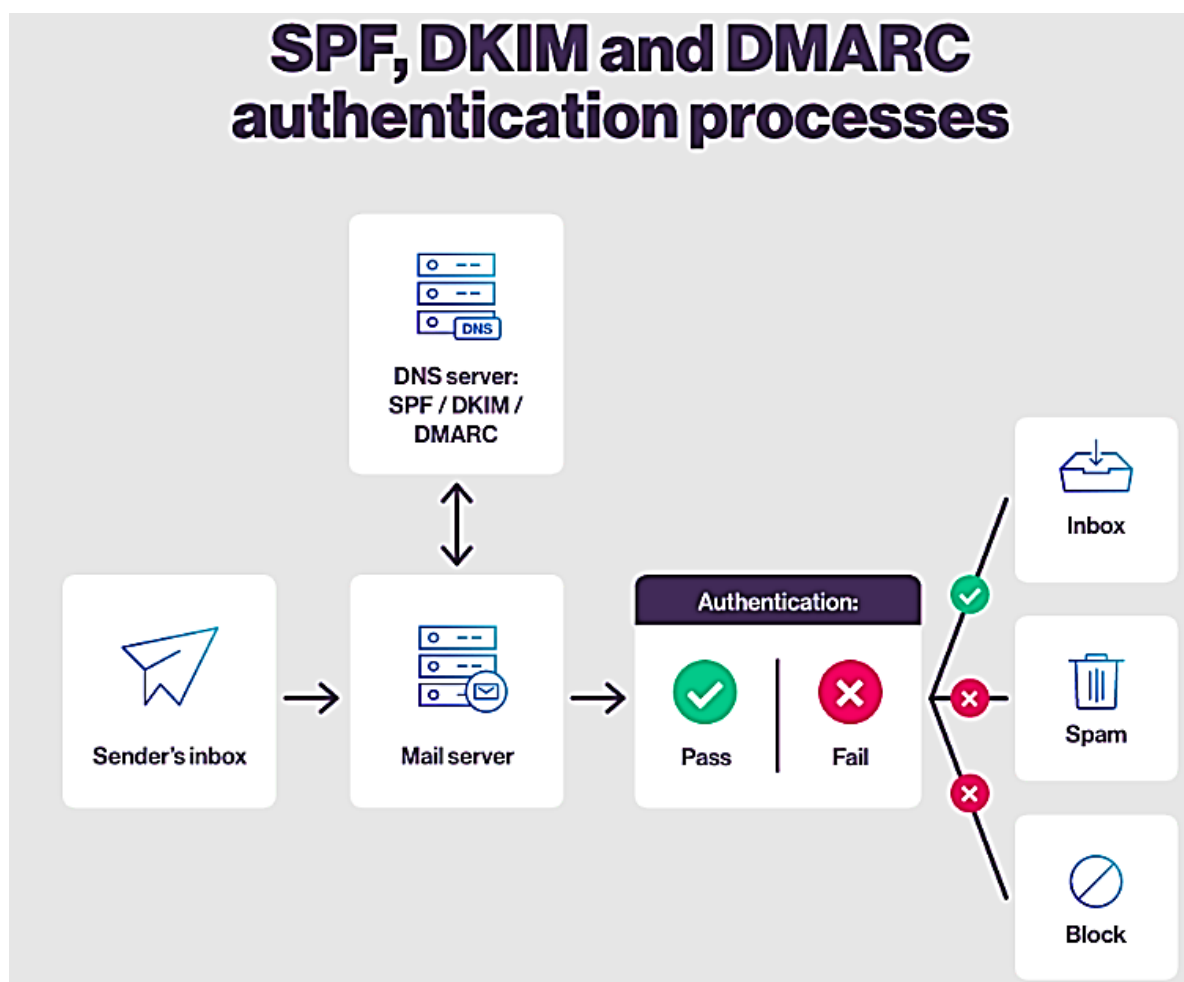


Рис. 6.12. Процес автентифікації електронної пошти за технологіями SPF, DKIM і DMARC

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Додатковим рівнем безпеки є шифрування електронної пошти. Протоколи TLS (Transport Layer Security) забезпечують захищене з'єднання між поштовими серверами, тоді як PGP (Pretty Good Privacy) та S/MIME (Secure/Multipurpose Internet Mail Extensions) застосовуються для шифрування вмісту листів і підпису повідомлень, гарантують конфіденційність і цілісність переданої інформації. На

рівні користувача важливо впроваджувати багатофакторну аутентифікацію при доступі до поштових акаунтів, що запобігає несанкціонованому входу навіть у разі викрадення пароля. Окрім цього, для захисту конфіденційних даних використовуються політики Data Loss Prevention (DLP), які контролюють передачу інформації та блокують відправлення листів із чутливими відомостями за межі корпоративної мережі.

Такі системи аналізують зміст повідомлень, вкладення та метадані, автоматично реагуючи на порушення політик безпеки — наприклад, спробу відправити файли, що містять персональні дані, фінансові звіти або комерційні таємниці. Для підвищення рівня довіри до електронних комунікацій застосовується цифровий підпис, який підтверджує автентичність відправника та гарантує, що повідомлення не було змінено під час передачі. Додатковим компонентом захисту виступає контроль геолокації та поведінковий аналіз, коли система автоматично блокує вхід із підозрілих місць або невідомих пристроїв. У корпоративних середовищах також впроваджуються системи керування ключами шифрування (Key Management Systems, KMS), які забезпечують безпечне зберігання, оновлення та ротацію криптографічних ключів, запобігаючи їхній компрометації. Окрім цього, сучасні поштові сервери інтегруються з SIEM-платформами, які відстежують спроби несанкціонованого доступу та формують аналітику інцидентів безпеки. У сукупності ці заходи створюють багаторівневий захисний бар'єр, який охоплює як процес передачі, так і зберігання листів, забезпечуючи стійкість корпоративної поштової системи до сучасних кіберзагроз.

На рис. 6.13 зображено узагальнену схему криптографічного захисту електронної пошти, яка демонструє взаємодію між відправником, поштовим сервером і одержувачем. У процесі передавання повідомлень між поштовими клієнтами (email clients) використовується протокол TLS (Transport Layer Security), який забезпечує захищений канал зв'язку для обміну даними через SMTP, POP або IMAP, запобігаючи перехопленню чи модифікації інформації під час її транспортування. TLS гарантує шифрування з'єднання на транспортному рівні, що захищає як метадані, так і зміст листа від стороннього доступу.

Для забезпечення цілісності, конфіденційності та автентичності повідомлень застосовуються два основні стандарти — S/MIME (Secure/Multipurpose Internet Mail Extensions) і PGP (Pretty Good Privacy). У першому випадку використовується інфраструктура відкритих ключів (PKI), де кожен користувач має цифровий сертифікат, підписаний центром сертифікації, що підтверджує достовірність відправника. У моделі PGP безпека базується на концепції «кіл довіри» (Circles of Trust), де користувачі самостійно підтверджують ключі один одного, створюючи децентралізовану мережу перевірених ідентичностей. Таким чином, комбінація TLS, S/MIME та PGP

забезпечує багаторівневий захист електронної пошти: TLS — для захищеної передачі даних, а S/MIME і PGP — для шифрування вмісту та цифрового підпису повідомлень. Такий підхід унеможливлює несанкціонований доступ до листів, підробку відправника або зміну інформації, гарантуючи високий рівень довіри до корпоративної поштової інфраструктури.

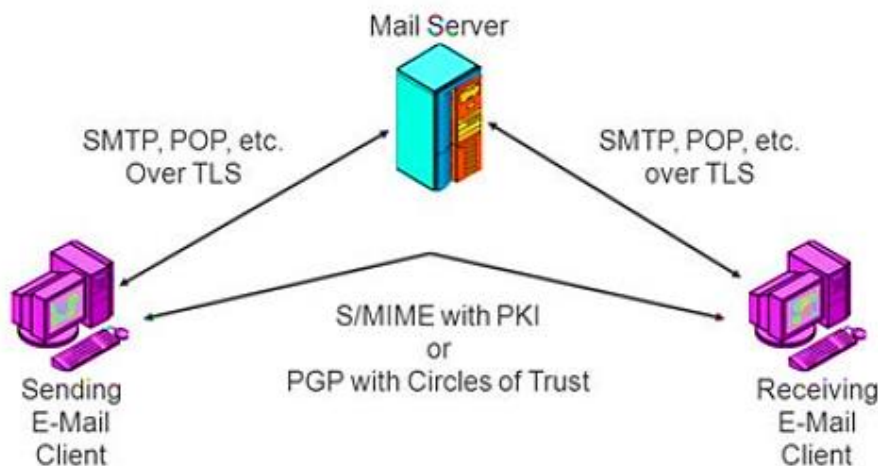


Рис. 6.13. Криптографічний захист електронної пошти з використанням TLS, S/MIME та PGP

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Такі системи аналізують вміст повідомлень, вкладення та метадані, автоматично реагуючи на порушення політик безпеки. Для підвищення довіри до комунікацій застосовується цифровий підпис, який підтверджує автентичність відправника та виключає можливість підміни листів. Важливим компонентом також є контроль геолокації та поведінковий аналіз входів до поштових акаунтів — система може автоматично блокувати спроби доступу з невідомих пристроїв або аномальних регіонів. Адміністраторам рекомендується застосовувати централізовані рішення з управління ключами шифрування (Key Management Systems), що забезпечують їх безпечне зберігання й ротацію. У сукупності ці технології створюють комплексний захисний бар'єр, який охоплює як передачу, так і зберігання електронних повідомлень, гарантуючи безпеку корпоративної поштової інфраструктури.

Захист вебсервісів

Захист вебсервісів — це не менш критичний аспект кібербезпеки, який охоплює як безпеку вебсайтів і корпоративних порталів, так і захист прикладних API, що забезпечують взаємодію між системами. Основу безпеки вебдодатків становить модель OWASP (Open Web Application Security Project), яка визначає найпоширеніші вразливості — такі як SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) та інші. Для їхнього запобігання

застосовуються вебаплікаційні фаєрволи (WAF), що фільтрують трафік на рівні HTTP/HTTPS, блокують спроби експлуатації вразливостей і контролюють запити до серверів.

Додатковим рівнем безпеки вебдодатків є використання систем виявлення та запобігання вторгненням (IDS/IPS), які аналізують мережевий трафік у реальному часі та блокують підозрілі запити ще до того, як вони досягнуть серверів. Важливим аспектом є впровадження безпечного керування сесіями — зокрема, використання унікальних токенів доступу, обмеження часу сесії та автоматичне завершення після бездіяльності користувача. Для автентифікації та авторизації користувачів широко застосовуються протоколи OAuth 2.0 і OpenID Connect, які дозволяють безпечно надавати доступ до ресурсів без передачі паролів. Значну роль у захисті вебсервісів відіграє використання HTTPS і TLS, що запобігає атакам типу «людина посередині» (MITM) та гарантує цілісність переданих даних. Сучасні платформи веббезпеки також інтегрують механізми Zero Trust Access, які перевіряють кожен запит незалежно від його походження, формуючи динамічну політику довіри. У поєднанні з регулярним тестуванням безпеки (penetration testing) і постійним моніторингом логів це створює цілісну систему кіберзахисту, яка здатна ефективно протидіяти як зовнішнім, так і внутрішнім загрозам.

На рис. 6.14 представлено узагальнену модель комплексного захисту вебсервісів, яка поєднує технічні та організаційні механізми кібербезпеки. На першому рівні показано користувача, який звертається до вебресурсу або прикладного інтерфейсу API. Його запит проходить через вебаплікаційний фаєрвол (WAF), що здійснює первинну перевірку на наявність типових загроз, визначених у моделі OWASP Top 10, зокрема SQL Injection, Cross-Site Scripting (XSS) та Cross-Site Request Forgery (CSRF). WAF аналізує вхідні HTTP/HTTPS-запити, блокує шкідливі пакети та фільтрує потенційно небезпечні операції.

На другому рівні реалізується шифрування трафіку за допомогою протоколів SSL/TLS із примусовим використанням HSTS (HTTP Strict Transport Security), що запобігає атакам типу «людина посередині» (MITM) і гарантує безпечну передачу даних. Для контролю автентичності користувачів використовується протокол OAuth 2.0, який дозволяє делегувати права доступу без передачі паролів, а також OpenID Connect — розширення OAuth для безпечної ідентифікації користувачів. Дані сесій зберігаються у вигляді JWT (JSON Web Token), що містить цифрово підписану інформацію про права користувача, термін дії та рівень довіри.

На наступному рівні представлено системи моніторингу та аналітики безпеки, зокрема SIEM (Security Information and Event Management) і UEBA (User and Entity Behavior Analytics), які здійснюють збір журналів подій, аналіз поведінки користувачів і виявлення аномалій, що можуть свідчити про спроби

зламу або компрометації акаунтів. У хмарному середовищі до архітектури інтегруються CASB (Cloud Access Security Broker), які контролюють політики доступу до хмарних застосунків і запобігають витоку даних.

Додатково на зовнішньому периметрі функціонують DDoS-захисні сервіси (Scrubbing Center), які фільтрують надлишковий трафік і забезпечують безперервність роботи вебпорталів, а балансувальники навантаження розподіляють запити між серверами, мінімізуючи ризик перевантаження. У комплексі наведена модель демонструє багаторівневий підхід до захисту вебсервісів — від користувача до хмарної інфраструктури, — що забезпечує цілісність, конфіденційність і доступність корпоративних інформаційних ресурсів.

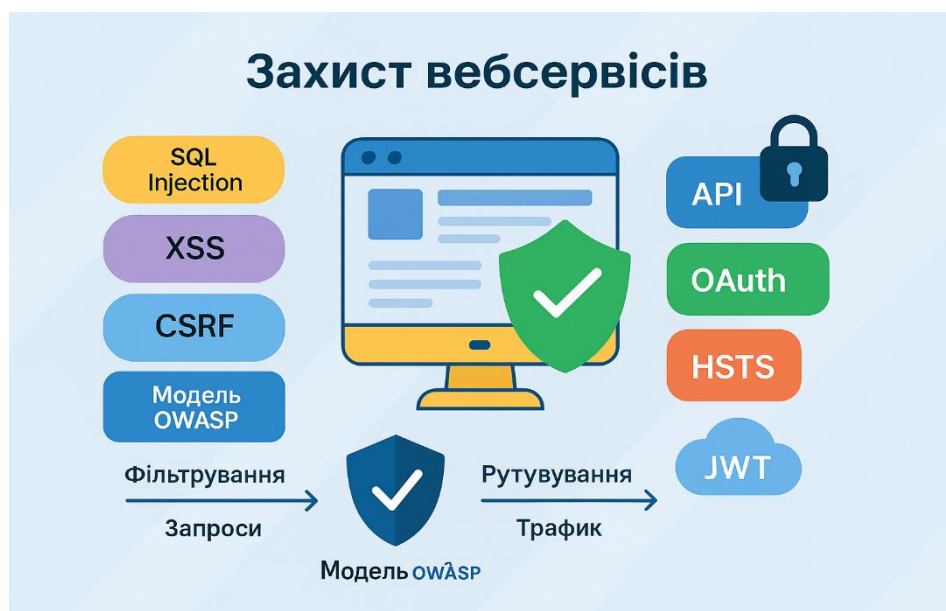


Рис. 6.14. Модель комплексного захисту вебсервісів підприємства
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Важливим компонентом є захист вебсервісів на рівні автентифікації та авторизації. Протоколи OAuth 2.0 і OpenID Connect забезпечують безпечну ідентифікацію користувачів без передачі паролів, а JSON Web Tokens (JWT) дозволяють створювати короткострокові токени доступу з контрольованими правами. Для зниження ризиків атак типу «людина посередині» (MITM) використовується примусове шифрування HTTPS-з'єднань із перевіреними сертифікатами SSL/TLS, а також механізми HTTP Strict Transport Security (HSTS), які забороняють з'єднання через незахищений протокол.

Крім того, сучасні системи захисту вебсервісів застосовують SIEM і UEBA-платформи, які збирають журнали подій, відстежують поведінку користувачів і виявляють аномалії, що можуть свідчити про спроби зламу або компрометації

облікових даних. У хмарних середовищах для захисту вебресурсів активно використовуються рішення Cloud Access Security Broker (CASB), які контролюють доступ до хмарних сервісів, здійснюють шифрування даних і застосовують політики безпеки незалежно від місця розташування користувача.

Важливим аспектом є захист від DDoS-атак, які можуть паралізувати роботу вебпорталу чи поштового сервера. Для цього використовуються спеціалізовані сервіси з очищення трафіку (scrubbing centers) і балансувальники навантаження, що автоматично розподіляють запити між серверами. Додатково впроваджуються механізми CAPTCHA, обмеження швидкості запитів (rate limiting) і системи моніторингу аномального трафіку.

У комплексі заходи із захисту електронної пошти та вебсервісів формують надійну багаторівневу систему безпеки, яка охоплює шифрування, фільтрацію, автентифікацію, моніторинг і реагування на інциденти. Вони не лише запобігають компрометації корпоративних даних, а й підвищують довіру до цифрових сервісів підприємства, забезпечуючи безперервність його бізнес-процесів у сучасному кіберсередовищі.

6.5. БЕЗПЕКА DEVOPS І DEVSECOPS-ПРОЦЕСІВ

Безпека DevOps і DevSecOps-процесів є ключовим елементом сучасного підходу до забезпечення надійності та стійкості програмних систем. Вона передбачає інтеграцію засобів безпеки на всіх етапах життєвого циклу розроблення — від написання коду до його розгортання у виробничому середовищі. Головна мета DevSecOps — зробити безпеку не окремим етапом, а безперервним процесом, що супроводжує кожен змін у програмному продукті. Для цього використовуються автоматизовані механізми перевірки коду на вразливості, контроль залежностей і тестування контейнерів перед розгортанням. Ключову роль відіграє створення безпечного CI/CD-конвеєра, у якому усі оновлення проходять сканування на відповідність політикам безпеки та стандартам ISO/IEC, NIST чи OWASP. Впровадження DevSecOps також сприяє тісній взаємодії між командами розробників, тестувальників і фахівців із кібербезпеки, що дозволяє оперативно усувати загрози ще до потрапляння у продуктивне середовище. У результаті формується культура «security by design», коли безпека стає вбудованою властивістю системи, а не зовнішнім додатком, що значно підвищує її захищеність і довіру користувачів.

У традиційних DevOps-моделях основна увага приділялася швидкості розроблення, тестування та розгортання програмного забезпечення, проте зростання кількості кіберзагроз вимагає інтеграції механізмів безпеки безпосередньо у кожен етап життєвого циклу розробки — від написання коду до

його експлуатації у виробничому середовищі. Саме такий підхід реалізується в DevSecOps (Development, Security, Operations), який передбачає автоматизовану перевірку безпеки, моніторинг уразливостей і контроль відповідності стандартам безпеки на всіх рівнях CI/CD-конвеєра (Continuous Integration / Continuous Deployment).

На рис. 6.15 зображено повний життєвий цикл DevOps, у який інтегровано процеси безпеки на кожному етапі — від розроблення до експлуатації. Модель демонструє, як у традиційний CI/CD-конвеєр (Continuous Integration / Continuous Deployment) впроваджуються механізми безпеки, утворюючи концепцію DevSecOps. Цей підхід забезпечує контроль якості коду, перевірку уразливостей, моніторинг інфраструктури та захист середовища виконання.

На етапі планування здійснюється аналіз вимог безпеки, формування політик і визначення контрольних точок для майбутнього тестування. Під час розроблення впроваджуються інструменти статичного аналізу коду (SAST), що виявляють потенційні вразливості ще до компіляції, а також контроль використання зовнішніх бібліотек і залежностей через механізми Software Composition Analysis (SCA). Далі, у процесі збирання та тестування, застосовується динамічний аналіз безпеки (DAST), який перевіряє поведінку додатка під час виконання, і налаштовуються контейнери або середовища віртуалізації з урахуванням принципів мінімальних привілеїв.

На етапі розгортання DevSecOps інтегрує політики контролю доступу, шифрування даних і перевірку конфігурацій через підхід *Infrastructure as Code (IaC)*. Система забезпечує автоматизований аудит середовища, контроль відповідності стандартам ISO/IEC 27001, NIST SP 800-53 і CIS Benchmarks. У фазі експлуатації DevSecOps передбачає постійний моніторинг, кореляцію подій безпеки через SIEM та автоматичне реагування за допомогою SOAR-платформ, що дає змогу оперативно виявляти й усувати загрози.

Рисунок наочно демонструє циклічність процесу DevSecOps — безпека не є фінальним етапом, а інтегрована у всі фази життєвого циклу розробки, утворюючи безперервний замкнений процес “Plan → Code → Build → Test → Release → Deploy → Operate → Monitor”. Такий підхід формує культуру спільної відповідальності між розробниками, адміністраторами й аналітиками безпеки, що підвищує загальну стійкість програмних систем і мінімізує ризики уразливостей ще до виходу продукту в експлуатацію.

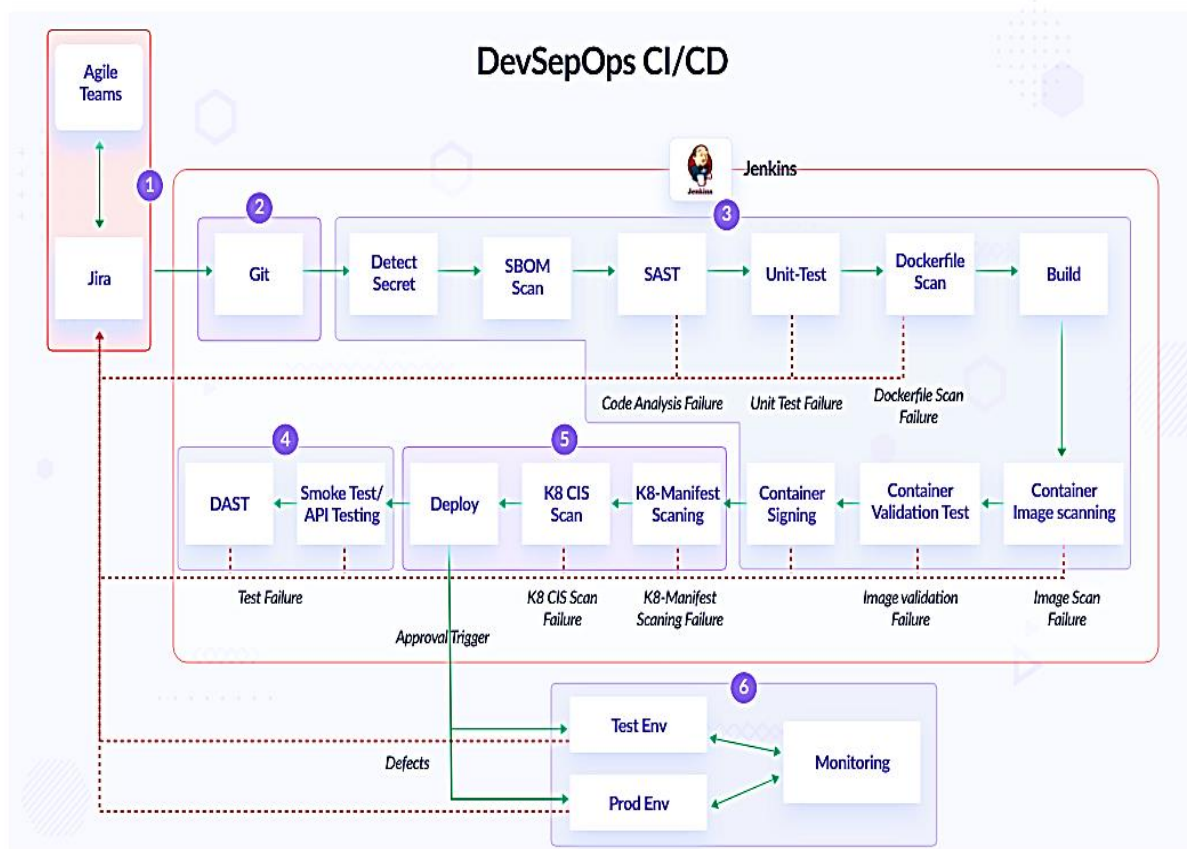


Рис. 6.15. Інтеграція безпеки в DevOps-конвеєр (DevSecOps-підхід)
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На етапі створення програмного коду впроваджуються статичний (SAST) і динамічний (DAST) аналізи безпеки, які автоматично перевіряють вихідний код і виконуване середовище на наявність уразливостей, таких як SQL-ін'єкції, небезпечне керування пам'яттю або витoki даних. Інструменти типу SonarQube, Checkmarx, Fortify чи OWASP Dependency-Check дозволяють розробникам одразу отримувати звіти про знайдені проблеми, що суттєво скорочує час на усунення ризиків. Крім того, важливо забезпечити контроль цілісності компонентів — усі сторонні бібліотеки, контейнери або пакети повинні перевірятися через механізми Software Composition Analysis (SCA) для виявлення відомих уразливостей у залежностях.

Під час побудови інфраструктури безпека реалізується за принципом “Infrastructure as Code” (IaC), що дозволяє описувати та контролювати конфігурації серверів, мереж і контейнерів у вигляді коду. Це забезпечує прозорість змін, можливість аудиту та автоматичну перевірку політик безпеки перед розгортанням середовища. Для контейнеризованих середовищ, зокрема Docker або Kubernetes, застосовуються механізми Container Security Scanning і

Runtime Protection, які перевіряють образи контейнерів на уразливості й контролюють їх поведінку під час виконання. Такі рішення, як Aqua Security, Sysdig Secure або Twistlock, дозволяють реалізувати політики контролю доступу, обмеження привілеїв та ізоляцію робочих навантажень.

Крім того, важливим аспектом безпеки DevOps є управління секретами та ключами шифрування, що запобігає витоку облікових даних, токенів і паролів. Для цього використовуються спеціалізовані сервіси, такі як HashiCorp Vault, AWS Secrets Manager або Azure Key Vault, які забезпечують централізоване шифрування, ротацію й контроль доступу до критичних параметрів середовища. Не менш значущим є впровадження Policy as Code (PaC) — підходу, який дозволяє автоматично перевіряти відповідність конфігурацій і середовищ політикам безпеки. Це дає змогу запобігати впровадженню небезпечних налаштувань ще до моменту їх розгортання.

Сучасні DevSecOps-підходи також інтегрують моніторинг безпеки в реальному часі, використовуючи SIEM- і SOAR-системи, які здійснюють збір, кореляцію та аналіз подій з різних компонентів DevOps-інфраструктури. Це забезпечує можливість оперативного реагування на інциденти безпеки, автоматизацію рутинних процесів і створення механізмів самовідновлення після атак. Важливе місце посідає й культура безпеки у команді — розробники, адміністратори та фахівці з кіберзахисту повинні спільно працювати над формуванням безпечного програмного середовища, дотримуючись принципу “Shift Left Security”, коли безпека враховується вже на етапі проектування коду.

На рис. 6.16 зображено типовий цикл DevSecOps Pipeline, який демонструє інтеграцію заходів безпеки на всіх етапах життєвого циклу розробки — від планування до розгортання. Концепція DevSecOps поєднує принципи DevOps, Continuous Integration (CI), Continuous Delivery (CD) та Agile Development, формуючи єдине середовище, у якому безпека не є окремою фазою, а постійно супроводжує процес створення, тестування й упровадження програмного продукту.

Першим етапом є Plan (Планування) — розробка архітектури, вимог і політик безпеки, що визначають межі доступу, критерії контролю цілісності та стандарти відповідності. Далі відбувається Code (Кодування), де розробники реалізують функціонал із дотриманням принципів “secure coding”, а автоматизовані засоби (SAST, SCA) перевіряють код на вразливості й небезпечні залежності. На етапі Test (Тестування) проводиться динамічний аналіз (DAST) і перевірка компонентів у контрольованому середовищі, що дає змогу виявити потенційні ризики до розгортання.

Етап Build (Збирання) забезпечує компіляцію, контейнеризацію та автоматичне підписування артефактів, після чого йде Release (Випуск) — перевірка політик безпеки, ротація секретів і підтвердження готовності продукту

до публікації. Нарешті, на стадії Deploy (Розгортання) відбувається безпечне розміщення програмного забезпечення у виробничому середовищі з контролем доступу, моніторингом подій і застосуванням інструментів SIEM/SOAR для реагування на інциденти. Рисунок демонструє, що DevSecOps — це не лінійний процес, а замкнений цикл постійного вдосконалення, у якому кожна зміна автоматично перевіряється з точки зору безпеки. Така інтеграція дає змогу швидко випускати оновлення без зниження рівня захисту, створюючи надійне, стійке та самоконтрольоване середовище розробки.

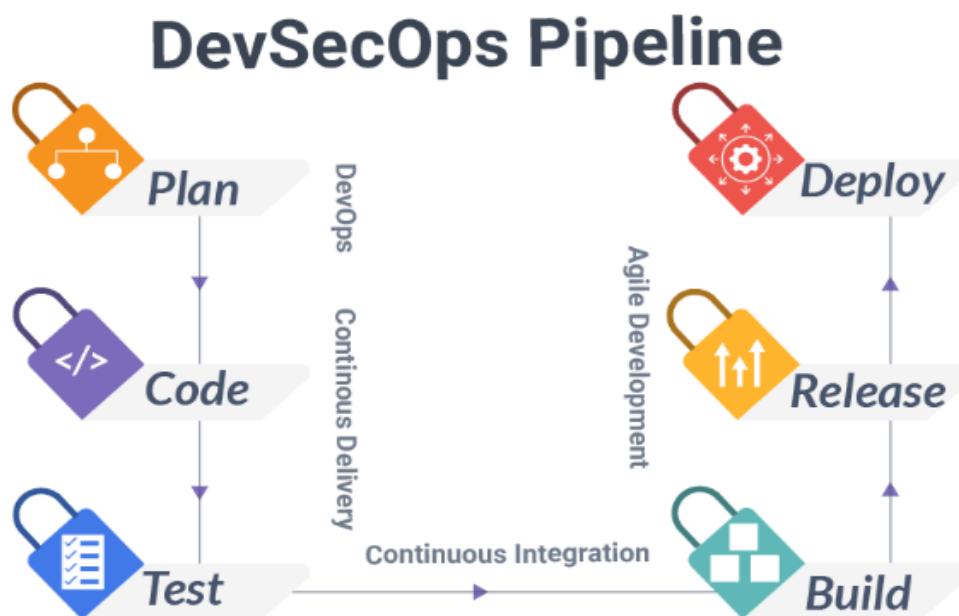


Рис. 6.16. DevSecOps-конвеєр як безперервний цикл безпечної розробки програмного забезпечення

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Додатково до технічних заходів, DevSecOps включає управління відповідністю стандартам — наприклад, ISO/IEC 27001, NIST SP 800-53, GDPR або PCI DSS. Інструменти типу Open Policy Agent (OPA) та Terraform Compliance допомагають автоматично перевіряти інфраструктуру на відповідність цим вимогам, що підвищує рівень довіри до DevOps-конвеєра. У підсумку реалізація принципів DevSecOps створює саморегульоване середовище безпеки, у якому контроль, моніторинг і реагування є невід’ємною частиною процесу розробки, а не зовнішнім етапом після випуску продукту.

На етапі розгортання DevSecOps передбачає інтеграцію сек’юрності у CI/CD-конвеєри, де кожен коміт коду супроводжується автоматичними перевітками безпеки, аналізом політик і тестуванням середовища на відповідність стандартам ISO/IEC 27001, NIST SP 800-53 або CIS Benchmarks.

Для цього застосовуються інструменти GitLab CI/CD, Jenkins, GitHub Actions, доповнені безпековими плагінами. Особливу роль відіграють секрет-менеджери (наприклад, HashiCorp Vault, AWS Secrets Manager), які забезпечують безпечне зберігання паролів, токенів і ключів доступу, запобігаючи їх витоку з вихідного коду.

Після розгортання система має бути під постійним контролем за допомогою SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) платформ, які збирають події, аналізують аномалії та автоматично реагують на інциденти. Важливо також впроваджувати моніторинг поведінки користувачів і процесів (UEBA) для виявлення нетипових дій, що можуть свідчити про спробу компрометації. Безперервне тестування безпеки включає penetration testing, red teaming та bug bounty-програми, що дозволяють виявити слабкі місця у продуктивному середовищі до того, як ними скористаються зловмисники.

Узагальнюючи, можна сказати, що DevSecOps перетворює безпеку на невід'ємну частину культури розробки, роблячи її не бар'єром, а природним елементом процесу. Такий підхід сприяє формуванню середовища довіри, де всі учасники — від розробників до адміністраторів і фахівців із безпеки — несуть спільну відповідальність за захист інформаційних систем. Це дозволяє підприємствам досягати балансу між гнучкістю DevOps і високими стандартами безпеки, створюючи надійні, масштабовані та стійкі до кібератак рішення.

Додатково важливо забезпечити безпеку ланцюга постачання програмного забезпечення (Software Supply Chain Security), оскільки більшість атак сьогодні спрямовані не на кінцевий продукт, а на його залежності або інфраструктуру CI/CD. Для цього впроваджуються механізми цифрового підпису артефактів (наприклад, через Sigstore, Cosign, Notary) і перевірка цілісності пакетів перед їхнім розгортанням. Автоматизовані системи threat intelligence інтегруються з DevSecOps-процесами, надаючи актуальну інформацію про вразливості, шкідливі бібліотеки або підозрілу активність у середовищі розробки. Окрім цього, надзвичайно важливо впроваджувати контроль ланцюга довіри (Chain of Trust), який гарантує, що кожен компонент — від вихідного коду до фінального артефакту — проходить верифікацію підпису та походження. Для цього використовуються репозиторії з перевіреними джерелами (trusted registries) і сервіси типу SLSA (Supply-chain Levels for Software Artifacts), які визначають рівень зрілості безпеки ланцюга постачання. Додатково впроваджуються системи атестації та валідації контейнерів, що перевіряють, чи збірка та деплой відбулися у безпечному середовищі з дотриманням політик DevSecOps. У рамках управління ризиками розробляються плани реагування на компрометацію компонентів ланцюга постачання, які передбачають швидке відкликання уразливих версій і перевипуск безпечних артефактів. Для підвищення прозорості

процесу використовується концепція SBOM (Software Bill of Materials) — “переліку інгредієнтів” програмного забезпечення, що дозволяє ідентифікувати всі використані залежності й оперативно оцінювати їхню безпечність. Зрештою, інтеграція інструментів моніторингу ланцюга постачання з SIEM та системами управління вразливостями (Vulnerability Management) забезпечує повний цикл контролю — від розробки до експлуатації, що мінімізує ризики втручання в процес створення програмних продуктів.

На рис. 6.17 показано етапи розвитку атаки на ланцюг постачання програмного забезпечення, починаючи з первинного компрометаційного впровадження шкідливого коду у вихідний компонент або CI/CD-процес. Далі відбувається поширення (propagation) зараженого пакета чи оновлення серед численних споживачів або організацій. Наступний етап — експлуатація (exploitation), коли шкідливий код активується, отримуючи можливість викрадення даних, встановлення віддаленого доступу чи розгортання програм-вимагачів. Завершальна стадія — вплив (impact), який проявляється у масштабних наслідках для тисяч підприємств, що використовують уражене програмне забезпечення.



Рис. 6.17. Життєвий цикл атаки на ланцюг постачання програмного забезпечення (Software Supply Chain Attack Lifecycle)
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Таким чином, модель ілюструє замкнутий цикл атаки, де кожен етап підсилює наслідки попереднього, підкреслюючи важливість контролю довіри (Chain of Trust), підпису артефактів (Sigstore, Cosign, Notary), перевірки цілісності

та використання SBOM і SLSA як засобів запобігання подібним інцидентам у DevSecOps-середовищах.

Ще одним важливим напрямом є безпека конфігурацій хмарних середовищ, яка досягається за допомогою Cloud Security Posture Management (CSPM) — інструментів, що виявляють помилки у налаштуваннях сервісів AWS, Azure або GCP та автоматично їх усувають. Крім того, DevSecOps-підхід включає автоматизоване реагування на інциденти через інтеграцію з системами оркестрації контейнерів (Kubernetes), що дозволяє у разі компрометації швидко ізолювати вразливі вузли та відновити їх із безпечних резервних образів.

Діаграма на рис. 6.18 зображає ключові функціональні можливості CSPM — такі як моніторинг конфігурацій (Configuration Monitoring), інтеграція з DevOps (DevOps Integration), відповідність (Compliance Monitoring), реагування на інциденти (Incident Response), оцінка ризиків (Risk Assessment) і інвентаризація активів (Asset Inventory). На схемі видно, що CSPM системи не просто виявляють помилки у конфігураціях, але й автоматично реагують на них або підказують кроки для усунення, інтегруючись із процесами DevOps. Діаграма підкреслює, що CSPM охоплює як оцінку поточного стану (постура), так і активне управління змінами, забезпечуючи безперервну перевірку середовища. Цей підхід критично важливий саме в DevSecOps, адже в хмарних інфраструктурах навіть незначні конфігураційні похибки можуть відкривати великі вразливості (наприклад, відкриті S3-бакети, невірні IAM-політики, відкриті порти чи невстановлене шифрування). CSPM системи дозволяють автоматично виявляти такі невідповідності й оперативно їх коригувати.

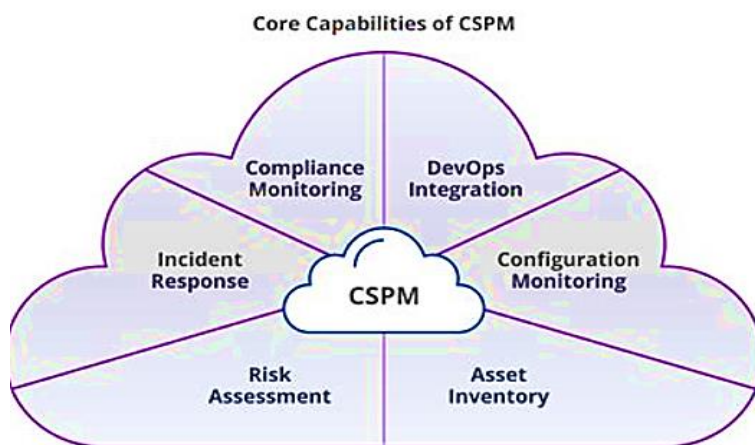


Рис. 6.18. DevSecOps-конвеєр як безперервний цикл безпечної розробки програмного забезпечення

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Особливу увагу приділяють захисту журналів і телеметрії, адже саме через неконтрольований логінг часто відбувається витік конфіденційних даних.

Використання систем secure logging (наприклад, ELK Stack, Splunk) із шифруванням і контрольованим доступом запобігає маніпуляціям із журналами подій. Завершальним елементом є побудова метрик безпеки DevSecOps, таких як Mean Time to Detect (MTTD), Mean Time to Respond (MTTR) та Security Debt Index, що дозволяють кількісно оцінювати ефективність безпекових процесів і постійно їх удосконалювати.

Додатковим механізмом підвищення безпеки є цифрове підписування логів, що гарантує їхню цілісність і достовірність навіть у разі компрометації окремих вузлів системи. Для зменшення ризику втрати або спотворення даних застосовуються розподілені сховища журналів, де записи дублюються в декількох незалежних репозиторіях. Системи кореляції подій (SIEM) інтегруються з DevSecOps-конвеєром і дозволяють у реальному часі виявляти підозрілу активність, зіставляючи журнали з різних джерел — серверів, контейнерів, хмарних сервісів і мережевих пристроїв. У поєднанні з аналітикою на основі машинного навчання (ML) це забезпечує виявлення прихованих аномалій, які можуть свідчити про інсайдерські дії або нові типи атак.

Щоб запобігти накопиченню не виправлених вразливостей, у DevSecOps-практиці формується Security Backlog, де фіксуються знайдені проблеми та їх пріоритети для усунення. Нарешті, результати моніторингу логів, метрик MTTD/MTTR і звітів SIEM систем використовуються для побудови дашбордів безпеки, які відображають поточний стан кіберзахисту підприємства й допомагають приймати стратегічні рішення щодо оптимізації процесів безпеки.

На рис. 6.19 представлено архітектуру системи secure logging із використанням платформи Splunk, яка забезпечує централізований збір, аналіз і захист журналів подій з різних компонентів ІТ-інфраструктури. У схемі відображено багаторівневу взаємодію між операційними системами, прикладними сервісами, аналітичними вузлами Splunk і користувачами, які здійснюють моніторинг безпеки. Дані з численних серверів та додатків надходять через Heavy Forwarder — спеціальний компонент, який агрегує, фільтрує й передає журнали до головного вузла Splunk для подальшої індексації та збереження. Кожен сервер має встановлений агент Splunk, що збирає локальні логи про стан операційної системи, оновлення, конфігурації та події безпеки. Отримані дані шифруються й передаються через захищені канали зв'язку до аналітичних модулів, де відбувається кореляція подій, виявлення аномалій і побудова звітів. Важливу роль у системі відіграє контроль доступу — лише авторизовані користувачі можуть переглядати або аналізувати журнали, що виключає ризик маніпуляцій із даними.

На верхньому рівні архітектури зображено спеціалізовані сервери з OS & Applications, які передають інформацію про свої оновлення, конфігурації та події у Splunk для подальшої обробки. Система дозволяє виявляти підозрілу активність

(наприклад, несанкціоновані зміни у конфігураціях чи спроби доступу), що автоматично відображається в інтерфейсі адміністратора безпеки. Таким чином, представлена архітектура демонструє принципи захищеного логування в DevSecOps, коли збір телеметрії, її аналіз і реагування на події інтегровані в єдиний процес безпеки. Використання Splunk забезпечує надійну обробку великих обсягів даних, своєчасне виявлення інцидентів і формування метрик ефективності — таких як MTTD (Mean Time to Detect) та MTTR (Mean Time to Respond), що дозволяє підвищити загальний рівень кіберстійкості підприємства.

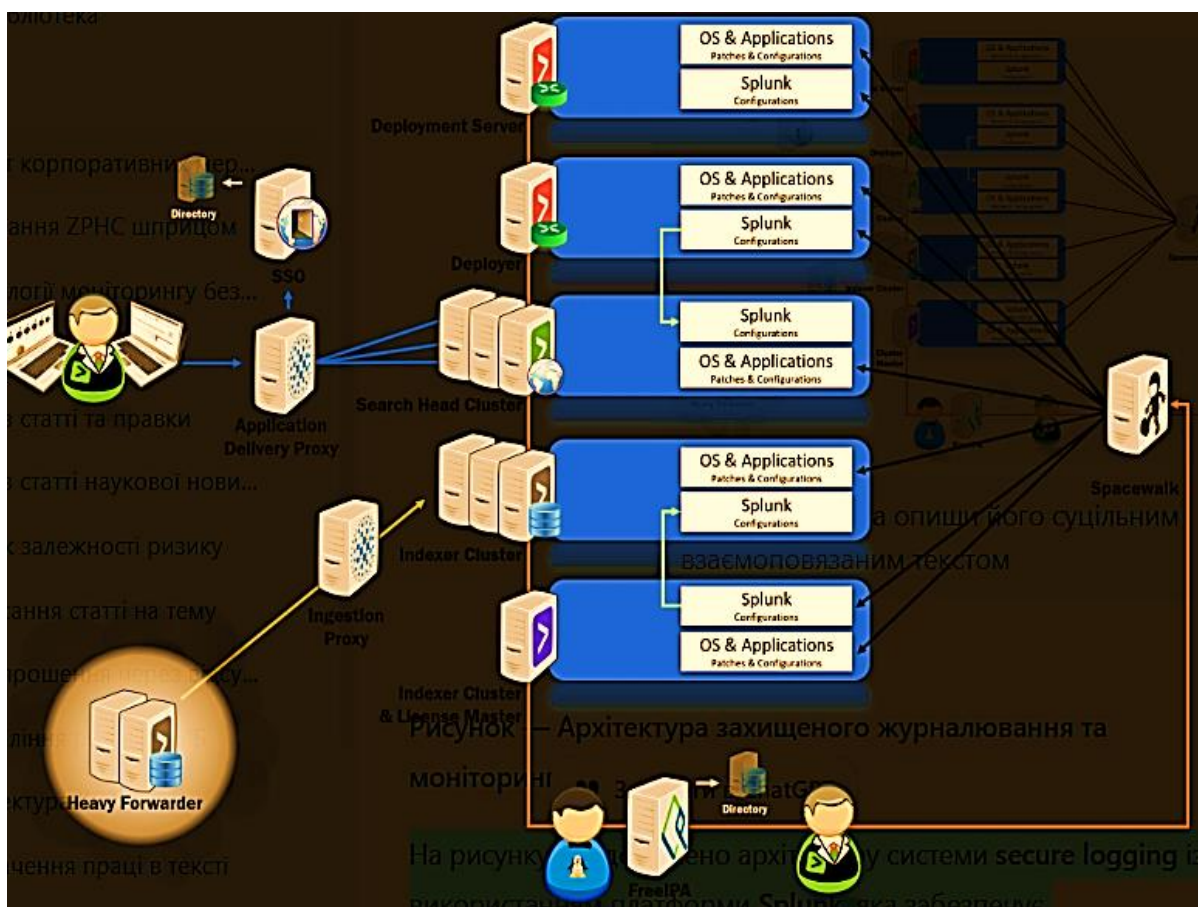


Рис. 6.19. Архітектура захищеного журналювання та моніторингу на основі Splunk

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Таким чином, безпека DevSecOps виходить далеко за межі традиційного підходу до тестування — вона перетворюється на безперервний замкнений цикл аналізу, виявлення, реагування й оптимізації, що охоплює увесь життєвий цикл ПЗ. Завдяки цьому DevSecOps не лише підвищує кіберстійкість підприємства, а й формує прозору екосистему довіри, де безпека стає фундаментом інновацій і стабільного розвитку цифрових рішень.

Такий підхід забезпечує постійне відстеження змін у вихідному коді, залежностях і середовищі збірки, мінімізуючи ризик непомічених уразливостей або компрометацій. Інтеграція інструментів типу SBOM, SLSA та Sigstore дозволяє автоматизувати перевірку походження кожного артефакту та гарантувати його цілісність. Завдяки централізованому моніторингу в межах SIEM і систем управління вразливостями створюється наскрізна видимість усіх етапів DevSecOps-процесу. Також реалізується можливість швидкого реагування на інциденти — від виявлення змін у репозиторії до відкликання скомпрометованих версій і перевипуску безпечних збірок. Важливим є і аспект навчання команд розробки та експлуатації, що формує культуру спільної відповідальності за безпеку продукту. У результаті DevSecOps еволюціонує у комплексну модель динамічного управління ризиками, де безпека стає невід'ємною частиною кожного етапу життєвого циклу програмного забезпечення.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 6

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
6. V. Sokolov, P. Skladannyi and A. Platonenko, "Video Channel Suppression Method of Unmanned Aerial Vehicles," *2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO)*, Kyiv, Ukraine, 2022, pp. 473-477, doi: 10.1109/ELNANO54667.2022.9927105.

7. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) *CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073
8. Hulak, Hennadii and Kriuchkova, Larysa and Skladannyi, Pavlo and Oprisky, Ivan (2021) *Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 137-142. ISSN 1613-0073
9. Iosifova, Olena and Iosifov, Ievgen and Sokolov, V. Y. and Romanovskyi, O. and Sukaylo, I. (2021) *Analysis of Automatic Speech Recognition Methods* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 252-257. ISSN 1613-0073
10. Zhebka, V. and Zhebka, S and Bazhan, T and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Methodology for Choosing a Consensus Algorithm for Blockchain Technology* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 106-113. ISSN 1613-0073
11. Dudykevych, V. and Mykytyn, G. and Stosyk, T. and Skladannyi, Pavlo (2024) *Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 449-457. ISSN 1613-0073
12. Shevchenko, Svitlana & Zhdanova, Yuliia & Shevchenko, Halyna & Nehodenko, Olena & Spasiteleva, Svitlana. (2023). Information Security Risk Management using Cognitive Modeling.
13. V. Sokolov, P. Skladannyi and A. Platonenko, "Jump-Stay Jamming Attack on Wi-Fi Systems," *2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, Lviv, Ukraine, 2023, pp. 1-5, doi: 10.1109/CSIT61576.2023.10324031.
14. Buriachok, V., Korshun, N., Zhylytsov, O., Sokolov, V., Skladannyi, P. (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspas, G. (eds) *Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies*, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_32
15. Marusenko, R., Sokolov, V., Buriachok, V. (2021). Experimental Evaluation of Phishing Attack on High School Students. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and*

Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing, vol 1247. Springer, Cham. https://doi.org/10.1007/978-3-030-55506-1_59

16. V. Astapenya, V. Sokolov and D. Ageyev, "Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum," *2020 IEEE Ukrainian Microwave Week (UkrMW)*, Kharkiv, Ukraine, 2020, pp. 203-206, doi: 10.1109/UkrMW49653.2020.9252755.

17. Brzhevska, Zoreslava and Kyrychok, Roman and Anosov, Andrii and Skladannyi, Pavlo and Vorokhob, Maksym (2021) *Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 257-264. ISSN 1613-0073

18. HU, ZHENG BING & Buriachok, Volodymyr & Sokolov, Volodymyr. (2019). Implementation of Social Engineering Attack at Institution of Higher Education. SSRN Electronic Journal. 10.2139/ssrn.3679106.

19. Mykhaylova, O and Fedynyshyn, T and Sokolov, Volodymyr and Kyrychok, Roman (2024) *Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 239-251. ISSN 1613-0073

20. Marusenko, R., Sokolov, V., Skladannyi, P. (2023). Social Engineering Penetration Testing in Higher Education Institutions. In: Hu, Z., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VI. ICCSEEA 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol 181. Springer, Cham. https://doi.org/10.1007/978-3-031-36118-0_96

21. Mykhaylova, O and Fedynyshyn, T and Datsiuk, A and Fihol, B and Hulak, Hennadii (2023) *Mobile Application as a Critical Infrastructure Cyberattack Surface* Cybersecurity Providing in Information and Telecommunication Systems II 2023, 3050. pp. 29-43. ISSN 1613-0073

22. Kyrychok, R., Laptiev, O., Lisnevskyi, R., Kozlovskyi, V., & Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. *Eastern-European Journal of Enterprise Technologies*, 1(9(115)), 93–101. <https://doi.org/10.15587/1729-4061.2022.253530>

23. V. Sokolov, P. Skladannyi and V. Astapenya, "Bluetooth Low-Energy Beacon Resistance to Jamming Attack," *2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT)*, Lviv, Ukraine, 2023, pp. 270-274, doi: 10.1109/ELIT61488.2023.10310815.

24. Astapenya, Volodymyr & Zhdanova, Yuliia & Shevchenko, Svitlana & Spasiteleva, Svitlana & Kryvoruchko, Olena. (2024). Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare.
25. Dudykevych, V and Yevseiev, S and Mykytyn, H and Ruda, K and Hulak, Hennadii (2024) *Detecting Deepfake Modifications of Biometric Images using Neural Networks* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 391-397. ISSN 1613-0073
26. Adamantis, M., Sokolov, V., Skladannyi, P. (2025). Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method. In: Hu, Z., Yanovsky, F., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VII. ICCSEEA 2024* 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 242. Springer, Cham. https://doi.org/10.1007/978-3-031-84228-3_5
27. Chernenko, Roman and Anosov, Andrii and Kyrychok, Roman and Brzhevskaya, Zoreslava and Spasiteleva, Svitlana (2022) *Encryption Method for Systems with Limited Computing Resources* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 142-148. ISSN 1613-0073
28. Iavich, M. and Kovalchuk, O. and Gnatyuk, S. and Khavikova, Y. and Sokolov, Volodymyr (2024) *Classical and post-quantum encryption for GDPR* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 70-78. ISSN 1613-0073
29. Romanovskiy, O. and Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2022) *Prototyping Methodology of End-to-End Speech Analytics Software* Modern Machine Learning Technologies and Data Science Workshop, 3312 (1). pp. 76-86. ISSN 1613-0073
30. Romanovskiy, O., Iosifov, I., Iosifova, O., Sokolov, V., Kipchuk, F., Sukaylo, I. (2021). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021*. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_3
31. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography*, 8(3), 38. <https://doi.org/10.3390/cryptography8030038>
32. Syrotynskiy, R. and Tyshyk, I. and Kochan, O. and Sokolov, Volodymyr and Skladannyi, Pavlo (2024) *Methodology of network infrastructure*

analysis as part of migration to zero-trust architecture Cyber Security and Data Protection 2024 (3800). pp. 97-105. ISSN 1613-0073

33. Martseniuk, Y. and Partyka, A. and Harasymchuk, O. and Shevchenko, Svitlana (2024) *Universal centralized secret data management for automated public cloud provisioning* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 72-81. ISSN 1613-0073

34. Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2021) *Natural Language Technology to Ensure the Safety of Speech Information* Cybersecurity Providing in Information and Telecommunication Systems II. Volume I, 3187 (1). pp. 216-226. ISSN 1613-0073

35. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) *Smart Home Subsystem for Calculating the Quality of Public Utilities* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073

36. V. Sokolov, P. Skladannyi and N. Mazur, "Wi-Fi Repeater Influence on Wireless Access," 2023 *IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2023, pp. 33-36, doi: 10.1109/AICT61584.2023.10452421.

37. Dreis, Y. and Korchenko, O. and Brzhevska, Zoreslava and Kriuchkova, Larysa and Nesterova, Olena (2024) *Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 277-289. ISSN 1613-0073

38. Virovets, Denis and Obushnyi, Sergiy and Zhurakovskiy, B. and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Integration of smart contracts and artificial intelligence using cryptographic oracles* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 39-46. ISSN 1613-0073

39. Марценюк , М., Козачок, В., Богданов, О., Іосіфов, Є., & Бржевська , З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Кібербезпека: освіта, наука, техніка, 2(22), 148–155. <https://doi.org/10.28925/2663-4023.2023.22.148155>

40. Машталяр, Я., Козачок, В., Бржевська, З., Богданов, О., Оксанич , І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 2(22), 156–167. <https://doi.org/10.28925/2663-4023.2023.22.156167>

41. Шевченко, С., Жданова, Ю., Складаний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах

інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 2(22), 168–178. <https://doi.org/10.28925/2663-4023.2023.22.168178>

42. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 1(21), 99–120. <https://doi.org/10.28925/2663-4023.2023.21.99120>

43. Спасітелєва, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. Кібербезпека: освіта, наука, техніка, 1(21), 193–210. <https://doi.org/10.28925/2663-4023.2023.21.193210>

44. Костюк Ю., Бебешко Б., Складанний П., Рзаєва С., Хорольська К. Оптимізація буфера та пріоритетів для забезпечення безпеки У Bluetooth-мережах. Безпека інформаційних систем і технологій. 2025. 2(8), 5-16.

45. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. Кібербезпека: освіта, наука, техніка, 1(21), 223–233. <https://doi.org/10.28925/2663-4023.2023.21.223233>

46. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. Кібербезпека: освіта, наука, техніка, 4(20), 174–182. <https://doi.org/10.28925/2663-4023.2023.20.174182>

47. Соколов, В., & Складанний, П. (2023). Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». Кібербезпека: освіта, наука, техніка, 4(20), 183–204. <https://doi.org/10.28925/2663-4023.2023.20.183204>

48. Shevchenko, S., Zhdanova, Y., & Spasiteleva, S. (2023). Mathematical methods in cybersecurity: Catastrophe theory. Cybersecurity: Education, Science, Technique, 3(19), 165–175. <https://doi.org/10.28925/2663-4023.2023.19.165175>

49. Sokolov, V. (2022). Approaches to the formation of scientific thinking in cybersecurity high school students. Cybersecurity: Education, Science, Technique, 2(18), 124–137. <https://doi.org/10.28925/2663-4023.2022.18.124137>

50. Shevchenko, S., Skladannyi, P., Nehodenko, O., & Nehodenko, V. (2022). Study of applied aspects of conflict theory in security systems. Cybersecurity: Education, Science, Technique, 2(18), 150–162. <https://doi.org/10.28925/2663-4023.2022.18.150162>

51. Sukaylo, I., & Korshun, N. (2022). The influence of NLU and generative AI on the development of cyber defense systems. *Cybersecurity: Education, Science, Technique*, 2(18), 187–196. <https://doi.org/10.28925/2663-4023.2022.18.187196>
52. Костюк Ю., Бебешко Б., Гулак Г., Складанний П., Рзаєва С., Хорольська К. (2024) Забезпечення кібербезпеки та швидкодії передачі даних у безпроводних мережах. *Безпека інформації*, т. 30, №3, 365-375.
53. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. *Cybersecurity: Education, Science, Technique*, 1(17), 145–158. <https://doi.org/10.28925/2663-4023.2022.17.145158>
54. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to provide control and management of privileged access in the IT environment. *Cybersecurity: Education, Science, Technique*, 4(16), 98–112. <https://doi.org/10.28925/2663-4023.2022.16.98112>
55. Borkivska, O., Zhurakovskiy, B., & Platonenko, A. (2022). Smart city information system based on LoRa technology. *Cybersecurity: Education, Science, Technique*, 4(16), 113–128. <https://doi.org/10.28925/2663-4023.2022.16.113128>
56. Brzhevskaya, Z., Kyrychok, R., Platonenko, A., & Hulak, H. (2022). Assessment of the preconditions of formation of the methodology of assessment of information reliability. *Cybersecurity: Education, Science, Technique*, 3(15), 164–174. <https://doi.org/10.28925/2663-4023.2022.15.164174>
57. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Boiko, S. (2022). Insiders and insider information: Essence, threats, activities and legal responsibility. *Cybersecurity: Education, Science, Technique*, 3(15), 175–185. <https://doi.org/10.28925/2663-4023.2022.15.175185>
58. Довженко, Н., Мазур, Н., Костюк, Ю., Рзаєва, С. Інтеграція ІОТ ТА штучного інтелекту в інтелектуальні транспортні системи. *Кібербезпека: освіта, наука, техніка*. 2024. 2(26), 430–444.
59. Bogachuk, V. Sokolov and V. Buriachok, "Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 581-585, doi: 10.1109/INFOCOMMST.2018.8632151.
60. Hulak, Hennadii and Skladannyi, Pavlo and Sokolov, Volodymyr and Hulak, E. and Korniiets, V. (2022) *Dynamic model of guarantee capacity and cyber security management in the critical automated systems* 2nd

International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), 3530. pp. 102-111. ISSN 1613-0073

61. Sokolov, V. Y. and Skladannyi, Pavlo and Hulak, Hennadii (2022) *Stability Verification of Self-Organized Wireless Networks with Block Encryption* Cybersecurity Providing in Information and Telecommunication Systems, 3137. pp. 227-237. ISSN 1613-0073

62. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) *Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073

63. Костюк Ю., Довженко, Н., Мазур, Н., Складанний, П., Рзаєва, С. Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. Кібербезпека: освіта, наука, техніка. 2025. 3(27), 22–40.

64. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii and Ageyev, D. (2023) *Method for Increasing the Various Sources Data Consistency for IoT Sensors* IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5

65. A. Carlsson, D. Ageyev, Y. Sadykov and V. Sokolov, "Sustainability Research of the Secure Wireless Communication System with Channel Reservation," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 973-977, doi: 10.1109/TCSET49122.2020.235583.

66. Складанний, П., Костюк Ю., Рзаєва, С., Самойленко, Ю., Савченко, Т. Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. Кібербезпека: освіта, наука, техніка. 2025. 3(27), 534–548.

67. F. Kipchuk, V. Sokolov, V. Buriachok and L. Kuzmenko, "Investigation of Availability of Wireless Access Points based on Embedded Systems," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-5, doi: 10.1109/PICST47496.2019.9061551.

68. Shevchuk, D and Harasymchuk, O and Partyka, A and Korshun, Natalia (2023) *Designing Secured Services for Authentication, Authorization, and Accounting of Users* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 207-225. ISSN 1613-0073

69. Складанний П.М., Костюк Ю.В., Мазур Н.П., Пітайчук М.А. Дослідження характеристик та продуктивності протоколів доступу до хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології. 2025. №1(86). С. 61-74.
70. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, 1(3), 602-617. <https://doi.org/10.3390/encyclopedia1030050>
71. TajDini, M., Sokolov, V., Kuzminykh, I., Shiaeles, S., & Ghita, B. (2020). Wireless Sensors for Brain Activity—A Survey. *Electronics*, 9(12), 2092. <https://doi.org/10.3390/electronics9122092>
72. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 125–156.
73. Складанний, П., Костюк, Ю., Рзаєва, С., & Мазур, Н. (2025). Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 242–269. <https://doi.org/10.28925/2663-4023.2025.31.1015>
74. Складанний, П.М., Гулак, Г.М., Костюк, Ю.В. Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. Телекомунікаційні та інформаційні технології. 2025. № 4 (89), 137-147. <https://doi.org/10.31673/2412-4338.2025.048916>
75. Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive Information Security Management in Cloud-Oriented Intelligent Transportation Systems. *Ukrainian Scientific Journal of Information Security*, 2025, vol. 31, issue 1, pp. 23-36. <https://doi.org/10.18372/2225-5036.31.20634>
76. Grechaninov, Viktor and Hulak, Hennadii and Hulak, Evgen and Skladannyi, Pavlo and Sokolov, Volodymyr (2021) *Decentralized Access Demarcation System Construction in Situational Center Network Cybersecurity Providing in Information and Telecommunication Systems II* 2021, 3188 (2). pp. 197-206. ISSN 1613-0073
77. Buriachok, Volodymyr and Ageyev, Dmytro and Zhylytsov, Oleksii and Skladannyi, Pavlo and Sokolov, V. Y. (2020) *Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies* *Cybersecurity Providing in Information and Telecommunication Systems*, 2746. pp. 23-32. ISSN 1613-0073
78. Костюк Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., Пазинін, А. Інструментальні засоби забезпечення

інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка. 2025. 4 (28), 633–655.

79. M. Vladymyrenko, V. Sokolov, V. Buriachok, A. Platonenko and D. Ageyev, "Analysis of Implementation Results of the Distributed Access Control System," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-6, doi: 10.1109/PICST47496.2019.9061376.

80. Складанний, П.М., Машкіна, І.В., Рзаєва, С.Л., Костюк, Ю.В. Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології. 2025. (2), 59-76.

81. Hu, Z., Buriachok, V., Bogachuk, I., Sokolov, V., Ageyev, D. (2021). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. In: Radivilova, T., Ageyev, D., Kryvinska, N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_29

82. F. Kipchuk, V. Sokolov, P. Skladannyi and D. Ageyev, "Assessing Approaches of IT Infrastructure Audit," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 213-217, doi: 10.1109/PICST54195.2021.9772181.

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні принципи побудови захищеної архітектури корпоративної мережі?
2. У чому полягає роль демілітаризованої зони (DMZ) у корпоративних мережах?
3. Як сегментація мережі впливає на рівень безпеки та ізоляцію критичних ресурсів?
4. Які типи фаєрволів використовуються для захисту корпоративної мережі та які їхні функції?
5. Які засоби моніторингу мережевої безпеки застосовуються у сучасних корпоративних середовищах?
6. Яке призначення технології VLAN у контексті безпеки корпоративних мереж?
7. У чому полягають відмінності між site-to-site VPN та remote-access VPN?
8. Які криптографічні протоколи використовуються у VPN для забезпечення конфіденційності даних?

9. Як реалізується тунелювання даних через незахищені канали та які основні ризики такого підходу?
10. Яким чином VLAN і VPN спільно підвищують рівень ізоляції й захисту трафіку в мережі підприємства?
11. Які основні моделі контролю доступу (DAC, MAC, RBAC, ABAC) застосовуються в корпоративних системах?
12. У чому переваги багатофакторної аутентифікації порівняно з однофакторною?
13. Як реалізується політика найменших привілеїв (Least Privilege) у корпоративних середовищах?
14. Які методи управління обліковими записами та доступом рекомендує Zero Trust Architecture?
15. Як можна інтегрувати SSO (Single Sign-On) і ZTNA (Zero Trust Network Access) у систему корпоративного доступу?
16. Які основні протоколи використовуються для автентифікації електронної пошти (SPF, DKIM, DMARC)?
17. Які типові загрози загрожують електронній пошті та як їм запобігають?
18. Яким чином вебapplікаційні фасерволи (WAF) забезпечують захист від атак типу SQL Injection і XSS?
19. Як застосування HTTPS, HSTS і TLS впливає на безпеку вебсервісів?
20. Які підходи DevSecOps використовуються для безпеки розгортання вебдодатків і моніторингу уразливостей?

РОЗДІЛ 7

МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ ТА РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ



- 7.1. Планування безперервності бізнес-процесів (Business Continuity Planning, BCP) і стратегії відновлення після катастроф (Disaster Recovery Planning, DRP) у комп'ютерних системах та мережах**
- 7.2. Резервне копіювання даних у системах інформаційної безпеки: сучасні технології, типи (повне, інкрементне, диференційне) та стратегії збереження інформаційних ресурсів**
- 7.3. Використання хмарних сервісів і гібридних інфраструктур для забезпечення цифрової безперервності функціонування підприємства**
- 7.4. Автоматизовані системи тестування та перевірки готовності до відновлення: симуляції інцидентів, моніторинг і оцінка ефективності планів DRP**
- 7.5. Впровадження вимог Регламенту DORA (Digital Operational Resilience Act) у процеси**

управління цифровою стійкістю та безперервністю комп'ютерних систем і мереж

Розділ охоплює стратегічні, організаційні та технічні підходи до забезпечення стійкості функціонування підприємства в умовах непередбачуваних інцидентів, кібератак, техногенних або природних катастроф. Його зміст спрямований на формування цілісного розуміння принципів Business Continuity Planning (BCP) та Disaster Recovery Planning (DRP), які визначають порядок дій, структуру відповідальності й послідовність заходів, необхідних для мінімізації простоїв і втрат даних.

У центрі уваги розділу — методи планування безперервності бізнес-процесів, що передбачають аналіз критичних функцій, моделювання сценаріїв ризику, визначення часу відновлення (RTO) і максимально допустимого часу простою (RPO). У практичному аспекті ці підходи поєднуються з плануванням відновлення після катастроф (DRP), яке регламентує процедури резервного копіювання, реплікації, тестування відновлюваності та підтримання альтернативних ІТ-майданчиків.

Особлива увага приділяється сучасним технологіям резервного копіювання та збереження даних, включно з повним, інкрементним і диференційним копіюванням, а також із впровадженням хмарних і гібридних рішень. Такі технології забезпечують географічну розподіленість даних і можливість швидкого доступу до резервних копій у разі збоїв основної інфраструктури. Розглядаються принципи автоматизації процесів моніторингу, побудови політик відновлення, перевірки цілісності резервів і використання DevSecOps-підходів, які інтегрують безпеку в кожен етап життєвого циклу розробки, тестування та розгортання ІТ-сервісів.

Ключовим нормативним орієнтиром для цього розділу виступає Регламент ЄС DORA (Digital Operational Resilience Act), що визначає єдині вимоги до операційної стійкості фінансових та цифрових організацій, у тому числі щодо управління ІТ-ризиками, тестування безперервності, кіберрезервних механізмів і звітності про інциденти. У межах його вимог формується підхід до інтегрованого управління безперервністю, який поєднує технічні, процедурні та організаційні заходи для забезпечення стабільності цифрової інфраструктури навіть у разі кризових подій. DORA також вимагає від підприємств упровадження системних механізмів аудиту, симуляційних тестів та сценарного аналізу, що дозволяють оцінити рівень готовності ІТ-систем до збоїв і перевірити ефективність резервних стратегій.

Важливою складовою є управління ризиками з урахуванням міжнародних стандартів ISO 22301:2019 «Security and resilience — Business continuity management systems», ISO/IEC 27031:2011 «Guidelines for ICT readiness for business continuity» та NIST SP 800-34 Rev.1 «Contingency Planning Guide for Federal Information Systems», які визначають структуру системи управління безперервністю, вимоги до документації, контролю та періодичного тестування.

Таким чином, розділ формує глибоке розуміння взаємозв'язку між управлінням безперервністю, резервним копіюванням, інформаційною безпекою та операційною стійкістю (Operational Resilience). Його вивчення дозволяє майбутнім фахівцям з кібербезпеки розробляти і впроваджувати комплексні стратегії підтримання життєздатності бізнес-процесів, відновлення ІТ-сервісів, збереження даних і забезпечення відповідності вимогам сучасних європейських і міжнародних стандартів, включно з положеннями Регламенту DORA, який закріплює нову парадигму цифрової стійкості підприємств.

7.1. ПЛАНУВАННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС-ПРОЦЕСІВ (BUSINESS CONTINUITY PLANNING, BCP) І СТРАТЕГІЇ ВІДНОВЛЕННЯ ПІСЛЯ КАТАСТРОФ (DISASTER RECOVERY PLANNING, DRP) У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Планування безперервності бізнес-процесів (Business Continuity Planning, BCP) і стратегії відновлення після катастроф (Disaster Recovery Planning, DRP) у комп'ютерних системах та мережах є ключовими елементами управління інформаційною безпекою та операційною стійкістю підприємства. Їх мета полягає у забезпеченні здатності ІТ-інфраструктури, систем зберігання даних, комунікаційних мереж і критичних бізнес-сервісів функціонувати навіть у разі серйозних інцидентів — від технічних збоїв до масштабних кіберзагроз або природних катастроф. Реалізація цих процесів передбачає системний підхід до ідентифікації ризиків, аналізу критичних залежностей і розроблення сценаріїв реагування на інциденти різної складності.

Планування BCP охоплює створення процедур збереження доступності даних і сервісів, визначення пріоритетів відновлення та підтримання комунікації між підрозділами під час кризових ситуацій. У межах DRP розробляються технічні рішення резервного копіювання, реплікації та автоматичного перемикавання на альтернативні майданчики для забезпечення безперервного функціонування систем. Особливе значення мають періодичне тестування планів відновлення, симуляційні навчання та аудит ефективності реалізованих заходів. Інтеграція принципів DORA та ISO 22301 гарантує дотримання європейських стандартів операційної стійкості й забезпечує відповідність політик безпеки

міжнародним вимогам. У підсумку, BCP і DRP формують фундамент цифрової надійності підприємства, мінімізуючи наслідки інцидентів і забезпечуючи стабільність бізнес-процесів навіть у кризових умовах.

Планування безперервності бізнес-процесів (BCP)

Планування безперервності бізнес-процесів (BCP) є стратегічним процесом, який охоплює визначення критичних функцій підприємства, їх залежностей від інформаційно-комунікаційних систем і ресурсів, а також розроблення механізмів підтримання операцій у кризових умовах. Основою BCP є Business Impact Analysis (BIA) — аналіз впливу інцидентів на діяльність підприємства, який дозволяє ідентифікувати найбільш важливі процеси, оцінити допустимі межі простою (Maximum Tolerable Downtime, MTD) і сформувати пріоритети відновлення. На основі цього визначаються два ключові параметри: RTO (Recovery Time Objective) — цільовий час відновлення, і RPO (Recovery Point Objective) — максимально допустима втрата даних у часі. Ці показники стають базою для проектування архітектури відмовостійкості, вибору технологій резервування й оптимізації планів реагування на надзвичайні ситуації.

На рис. 7.1 представлено циклічну модель процесу планування безперервності бізнес-процесів, що відображає послідовні етапи розроблення, впровадження та вдосконалення системи безперервності діяльності підприємства. Перший етап — Identify (ідентифікація) — передбачає визначення потенційних ризиків та загроз, а також проведення аналізу впливу на бізнес (Business Impact Analysis, BIA), який дозволяє встановити критичні процеси та допустимі межі простою. На другому етапі — Analyze (аналіз) — здійснюється поглиблена оцінка результатів BIA і формуються вимоги до стратегій відновлення залежно від рівня критичності функцій. Далі, у фазі Design (проектування), обираються оптимальні стратегії забезпечення стійкості, зокрема методи резервування, дублювання ресурсів і відновлення після інцидентів. Етап Execute (виконання) охоплює розроблення та впровадження планів дій, визначення відповідальних осіб, розподіл ресурсів і реалізацію механізмів координації між підрозділами. Завершальна фаза — Measure (оцінювання) — спрямована на тестування, навчання персоналу, аудит ефективності заходів і підтримання актуальності планів у відповідності до змін технологічного середовища. Таким чином, життєвий цикл BCP є безперервним процесом управління ризиками, який забезпечує стабільність бізнесу, мінімізує наслідки інцидентів і сприяє формуванню цифрової операційної стійкості підприємства.

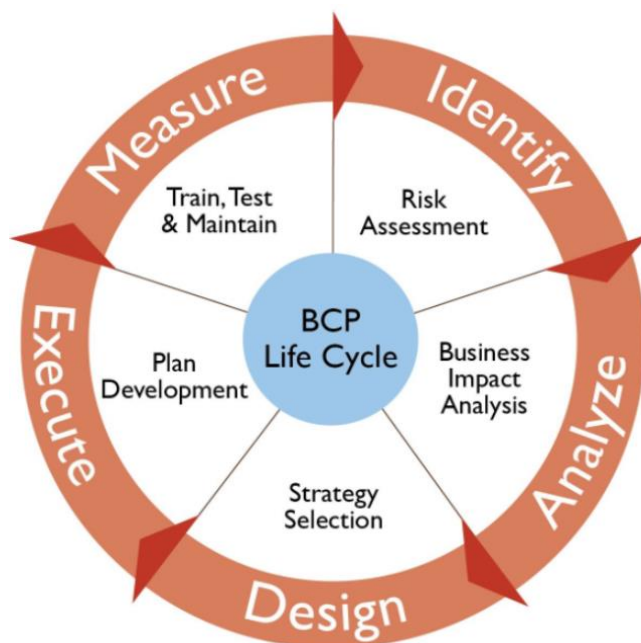


Рис. 7.1. Життєвий цикл планування безперервності бізнес-процесів (BCP Life Cycle)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

BCP передбачає створення операційного плану дій, який охоплює координацію між підрозділами, визначення відповідальних осіб, сценарії реагування на порушення, механізми альтернативних комунікацій і забезпечення доступу до ресурсів у надзвичайних ситуаціях. У сучасних умовах цей процес підтримується за допомогою спеціалізованих інструментів і методологій, що дозволяють здійснювати автоматизоване тестування готовності систем, моніторинг у реальному часі, оцінювання ефективності резервних потужностей та відповідності вимогам стандартів ISO 22301 і NIST SP 800-34.

Планування безперервності бізнес-процесів (BCP) також включає етапи документування, впровадження, тестування та постійного вдосконалення, що забезпечують життєздатність і актуальність системи безперервності. На етапі документування створюються офіційні політики, регламенти й інструкції, які описують порядок дій під час інцидентів, процедури ескалації, схеми взаємодії між бізнес-підрозділами, службами ІТ та безпеки. Особлива увага приділяється створенню матриці відповідальності (RACI), що визначає ролі осіб, залучених до реагування — від керівників кризових груп до технічних адміністраторів і фахівців із комунікацій.

На етапі впровадження BCP проводиться інтеграція заходів забезпечення безперервності у всі бізнес-процеси підприємства, включно з управлінням постачальниками, логістикою, фінансовими транзакціями та підтримкою

клієнтів. Це дозволяє мінімізувати ризики, пов'язані з людським фактором, технічними збоями чи кібератаками, які можуть вплинути на стабільність бізнесу. У цьому контексті впроваджуються контрольні точки безпеки в ІТ-інфраструктурі, здійснюється сегментація мережі, резервування каналів зв'язку, а також використання георозподілених центрів обробки даних (Data Centers), що гарантують доступність ресурсів незалежно від місця виникнення інциденту.

Важливою складовою є етап тестування та навчання персоналу, який передбачає регулярні симуляції кризових ситуацій, проведення навчальних тренувань та аудит готовності підприємства до надзвичайних подій. Під час таких тестів перевіряється ефективність комунікацій, час реакції, надійність резервних копій та здатність швидко перемикатися на альтернативні майданчики. Результати тестів фіксуються у звітах і використовуються для вдосконалення існуючих планів.

Особливе значення у сучасному BCP має цифровізація процесів безперервності, коли управління ризиками та реагування автоматизується за допомогою платформ BCM (Business Continuity Management). Ці системи інтегруються з SIEM, SOAR і Vulnerability Management, забезпечуючи централізований контроль за станом інфраструктури, виявленням відхилень і координацією дій підрозділів у режимі реального часу. Вони підтримують також ведення цифрових журналів інцидентів, генерацію звітів про ефективність відновлення та відповідність міжнародним стандартам ISO 22301, ISO/IEC 27031 і NIST SP 800-34.

Ще одним ключовим аспектом є інтеграція регуляторних вимог і галузевих норм, серед яких особливо важливим є Регламент DORA (Digital Operational Resilience Act), який визначає обов'язкові вимоги до операційної стійкості фінансових і критичних підприємств ЄС. DORA передбачає необхідність документованих BCP-процедур, періодичного тестування, аудиту готовності, контролю постачальників ІКТ-послуг і прозорості звітності про інциденти. Таким чином, BCP стає не лише внутрішньою політикою, а й елементом зовнішньої відповідності (compliance), що гарантує довіру клієнтів і партнерів.

На завершальному етапі постійного вдосконалення (continuous improvement) BCP переглядається відповідно до змін у бізнес-моделі, технологічному середовищі, нормативній базі чи результатів внутрішніх аудитів. Відбувається періодичне оновлення BIA, уточнення RTO/RPO, оптимізація процедур реагування та перевірка ефективності комунікаційних каналів. Такий підхід забезпечує не лише підтримання безперервності, а й адаптивність підприємства до нових ризиків, що виникають унаслідок цифровізації, автоматизації процесів та еволюції кіберзагроз.

Отже, сучасне планування безперервності бізнес-процесів є динамічною, інтегрованою системою управління ризиками, що поєднує стратегічне

планування, технічні рішення, людський фактор і нормативні вимоги. Воно створює основу для цифрової стійкості підприємства, забезпечуючи здатність не лише відновлюватися після інцидентів, а й функціонувати без збоїв у мінливому середовищі кіберзагроз.

Disaster Recovery Planning (DRP)

Disaster Recovery Planning (DRP) — це більш технічна складова системи безперервності, яка фокусується на відновленні ІТ-інфраструктури, баз даних, мережевих сервісів, віртуальних машин і додатків після аварій або атак. DRP включає розроблення процедур резервного копіювання, реплікації, відновлення систем і перемикання навантажень на альтернативні майданчики (Hot Site, Warm Site, Cold Site). Важливою частиною є побудова географічно розподілених центрів обробки даних (Data Centers), які забезпечують синхронізацію даних і можливість миттєвого переходу до резервних потужностей без втрати цілісності інформації.

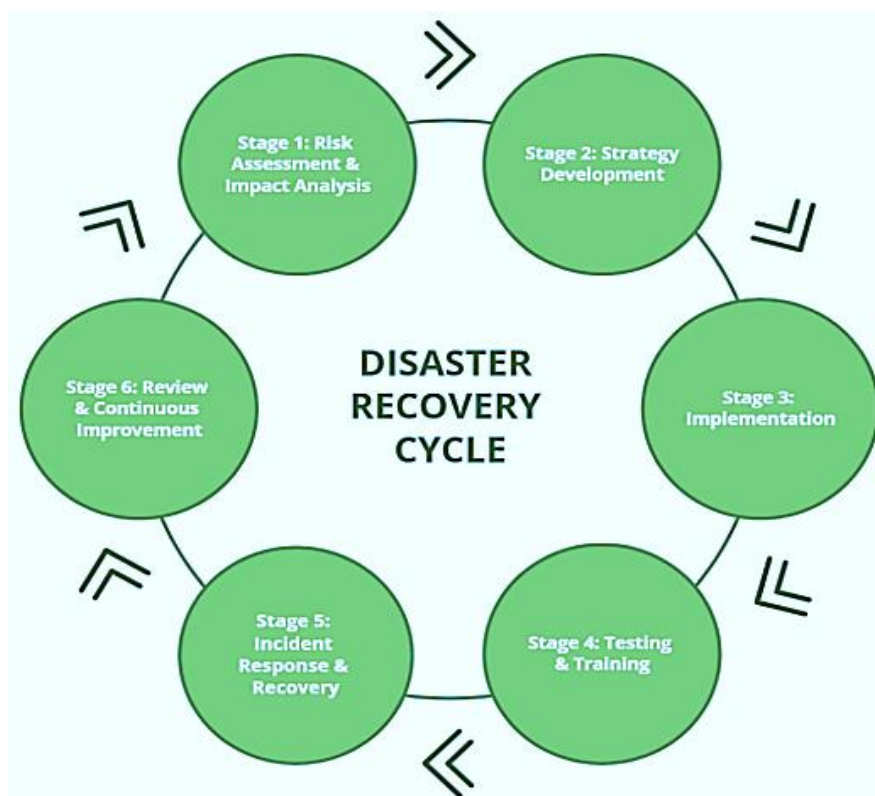


Рис. 7.2. Життєвий цикл планування відновлення після катастроф (Disaster Recovery Cycle)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рисунку показано багатofазну модель **DRP**, що відображає ключові етапи від підготовки до постійного вдосконалення. Перший етап — **Risk Assessment & Impact Analysis** — передбачає ідентифікацію загроз, аналіз можливих наслідків та визначення критичних ресурсів системи, від яких залежить робота бізнес-процесів. Далі на фазі **Strategy Development** формуються конкретні стратегії відновлення: вибір рівнів резервних майданчиків (**Hot, Warm, Cold**), рішення з реплікації, технологій резервного копіювання та синхронізації даних. На етапі **Implementation** здійснюється фізична чи логічна реалізація цих стратегій — налаштування серверів, реплікацій, мереж, перемикачів та інфраструктури резервного майданчика. Далі — **Testing & Training** — проводиться тестування процедур відновлення, навчання персоналу, симуляційні відмови, перевірка відповідності планів фактичним сценаріям. Наступна фаза — **Incident Response & Recovery** — активується під час реального або тестового інциденту, і включає фактичне відновлення систем, перемикачів навантаження, активацію резервних майданчиків. Завершальний етап — **Review & Continuous Improvement** — аналіз результатів виконання, збір уроків, корекція стратегії, оновлення планів і повторне тестування.

Ця циклічна модель підкреслює, що **DRP** не є одноразовим актом, а безперервним процесом: від аналізу ризиків до вдосконалення на основі фактичного досвіду, що забезпечує гнучкість, адаптивність і здатність підприємства до оперативного відновлення навіть у мінливих умовах.

Ефективність **DRP** залежить від вибору правильної стратегії резервного копіювання. Сучасні підходи базуються на використанні інкрементних, диференційних і дедуплікованих копій, а також технологій знімків (**snapshots**) і контейнеризації для швидкого відновлення середовищ. В умовах цифрової трансформації особливу роль відіграють хмарні сервіси — **AWS Backup, Google Cloud Storage, Azure Site Recovery**, які дозволяють створювати гібридні схеми **DR** з гнучким масштабуванням і мінімальними витратами на обладнання.

У сучасній парадигмі **DevSecOps** обидва процеси — **BCP** і **DRP** — інтегруються в життєвий цикл розробки програмного забезпечення, що дозволяє перевіряти стійкість ІТ-рішень ще на етапі їхнього створення. Автоматизовані сценарії тестування катастроф (**chaos engineering**) і симуляції відмов у **CI/CD**-процесах допомагають виявити слабкі місця, підвищити рівень готовності систем і скоротити час реакції на інциденти.

Disaster Recovery Planning (DRP) є невід'ємною частиною комплексної системи операційної стійкості підприємства та забезпечує технічну готовність ІТ-інфраструктури до швидкого відновлення після інцидентів будь-якого масштабу — від локальних відмов обладнання до масштабних кібератак чи природних катастроф. Його ключова мета полягає не лише у поверненні систем до робочого

стану, а й у мінімізації втрат даних, скороченні простоїв і забезпеченні безперервності критичних бізнес-функцій.

Структура DRP охоплює кілька взаємопов'язаних етапів: оцінку ризиків (Risk Assessment), аналіз впливу на бізнес (BIA), розроблення технічної стратегії відновлення, тестування планів і постійне вдосконалення. На етапі оцінки ризиків визначаються потенційні загрози для IT-інфраструктури — від відмов енергопостачання, збоїв обладнання, помилок адміністраторів і шкідливого ПЗ до зовнішніх атак або природних лих. Аналіз впливу (BIA) дозволяє встановити пріоритети відновлення сервісів, обчислити критичні параметри RTO (Recovery Time Objective) та RPO (Recovery Point Objective) і сформулювати стратегію відновлення, узгоджену з бізнес-цілями підприємства.

Суттєвим компонентом DRP є класифікація IT-ресурсів за рівнем критичності. Для систем першого рівня (mission-critical) передбачаються механізми синхронної реплікації даних та автоматичного перемикавання (failover) між майданчиками, тоді як менш критичні сервіси можуть відновлюватися вручну або з певною затримкою. Для цього створюються три основні типи резервних об'єктів:

- Hot Site — повністю синхронізований майданчик із актуальними даними, готовий до миттєвого перемикавання;
- Warm Site — частково підготовлений об'єкт із резервною інфраструктурою, який потребує короткого часу на активацію;
- Cold Site — майданчик без активних систем, призначений для розгортання після інциденту.

Сучасні DRP-системи базуються на технологіях віртуалізації та контейнеризації, що забезпечують портативність середовищ і швидке розгортання служб на нових ресурсах. Використання знімків систем (snapshots) та дедуплікованих копій дозволяє суттєво зменшити обсяг збережених даних, прискорюючи процес відновлення. Крім того, активно застосовуються гібридні стратегії DR, що поєднують локальні ресурси з хмарними платформами — такими як AWS Backup, Azure Site Recovery, Google Cloud Storage, IBM Cloud Resiliency Services — для створення масштабованих та економічно ефективних рішень.

Важливим напрямом розвитку DRP є автоматизація процесів відновлення. Інтеграція з системами SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) дозволяє автоматично запускати сценарії реагування на інциденти: створення копій, перемикавання трафіку, відновлення критичних вузлів та оповіщення відповідальних осіб. У результаті досягається зменшення часу простою (downtime) і підвищується точність дій під час кризових ситуацій.

Не менш важливим є етап тестування DRP, який передбачає проведення планових навчань, імітаційних відмов, симуляційних сценаріїв та аудитів ефективності. Такі тести дають змогу перевірити узгодженість дій персоналу, швидкість реакції, якість комунікації й відповідність плану вимогам ISO 22301, ISO/IEC 24762 і NIST SP 800-34. Зазвичай тести поділяють на tabletop-тренування (моделювання без фактичного втручання в систему) та live-simulation (реальні перевірки працездатності резервних майданчиків).

В умовах динамічної кіберзагрозової ситуації DRP інтегрується в DevSecOps-середовище, де кожен новий реліз програмного забезпечення автоматично проходить перевірку на стійкість до збоїв та можливість швидкого відновлення. Для цього використовуються методи chaos engineering, коли штучно створюються відмови або деградації сервісів у середовищі CI/CD, що дозволяє визначити “вузькі місця” та підвищити надійність системи ще до її впровадження у виробничу експлуатацію.

Важливим нормативним орієнтиром для DRP виступає Регламент ЄС DORA (Digital Operational Resilience Act), який зобов'язує підприємства, зокрема фінансового сектору, підтримувати план відновлення ІТ-систем із перевіреними сценаріями аварій, резервними копіями та контрольними точками. DORA також вимагає незалежного тестування, аудиту постачальників ІКТ-послуг і звітування про виконання планів DR до регуляторних органів. Це сприяє підвищенню довіри, прозорості та стійкості цифрової інфраструктури в масштабах усього ринку.

Отже, Disaster Recovery Planning є не просто технічною інструкцією з відновлення систем, а комплексною технологічно-організаційною моделлю, що забезпечує синхронізацію бізнес-цілей, ІТ-інфраструктури та кібербезпеки. Його ефективна реалізація дозволяє підприємству не лише швидко повертатися до нормального функціонування після інцидентів, а й досягати високого рівня операційної стійкості (Operational Resilience), що відповідає вимогам сучасних міжнародних стандартів і регламентів.

Регламент DORA (Digital Operational Resilience Act)

Регламент DORA (Digital Operational Resilience Act) підсилює значення BCP і DRP, визначаючи чіткі вимоги до операційної стійкості підприємств фінансового сектору, а також обов'язок впроваджувати тестування безперервності, аудит резервних процесів, звітність про інциденти й контроль постачальників критичних ІКТ-послуг. DORA формує нову культуру проактивного управління стійкістю, коли підприємства мають не лише реагувати на інциденти, а й передбачати їхні наслідки, забезпечуючи безперервність усіх цифрових операцій.

Регламент DORA (Digital Operational Resilience Act) є нормативно-правовим актом Європейського Союзу, спрямованим на створення єдиного правового поля

для забезпечення операційної стійкості (operational resilience) фінансових установ, постачальників цифрових послуг та учасників ринку інформаційних технологій. Його головна мета — гарантувати, що всі суб'єкти фінансової екосистеми здатні витримувати, реагувати, відновлюватися та адаптуватися до технологічних збоїв, кіберінцидентів і кризових подій, не втрачаючи функціональності своїх критичних бізнес-процесів.

Регламент DORA ухвалений Європейським парламентом і Радою ЄС у 2022 році (Регламент (ЄС) 2022/2554) і набирає чинності з січня 2025 року, охоплюючи банки, страхові компанії, платіжні системи, фінтех-компанії, операторів критичних ІКТ-послуг, постачальників хмарних технологій і навіть регуляторні органи. Його дія поширюється на всі види інформаційно-комунікаційних технологій (ІКТ), що використовуються у фінансовій діяльності, включаючи системи обробки даних, телекомунікації, програмне забезпечення, сервіси зберігання, шифрування, аналітику та кіберзахист.

DORA структурує вимоги до цифрової стійкості у п'ять основних напрямів:

1. *Управління ризиками ІКТ (ICT Risk Management)* — зобов'язує підприємства створювати централізовану систему управління ризиками, яка охоплює ідентифікацію, моніторинг, оцінку, мінімізацію та звітування про технологічні ризики. Всі процеси мають документуватися, а відповідальність покладатися на керівництво підприємства.

2. *Звітність та управління інцидентами (ICT-related Incident Reporting)* — передбачає обов'язкове виявлення, класифікацію, документування та оперативне повідомлення регуляторів про ІКТ-інциденти, включаючи кібератаки, збої в роботі систем або втрати даних. Це підвищує прозорість і дає змогу координовано реагувати на кризові ситуації.

3. *Тестування операційної стійкості (Digital Operational Resilience Testing)* — зобов'язує фінансові установи періодично проводити перевірки BCP і DRP, зокрема шляхом симуляційних навчань, сценаріїв відмов і «red teaming»-тестів. Результати таких перевірок мають бути задокументовані, а виявлені вразливості — усунені в найкоротший термін.

4. *Управління ризиками третіх сторін (ICT Third-Party Risk Management)* — встановлює суворі вимоги до укладання контрактів, моніторингу та аудиту постачальників ІКТ-послуг (особливо хмарних провайдерів). Підприємства повинні мати чітко визначені плани дій на випадок відмови або компрометації зовнішнього партнера.

5. *Обмін інформацією про кіберзагрози (Information Sharing Arrangements)* — стимулює фінансові установи до участі в платформах обміну аналітикою та індикаторами компрометації (IoC), що підвищує колективну безпеку сектору.

На рис. 7.3 зображено п'ять ключових напрямів, які формують основу Регламенту DORA, спрямованого на забезпечення цифрової операційної

стійкості фінансових установ та ІКТ-постачальників у Європейському Союзі. Першим елементом є управління ризиками (Risk Management), що передбачає створення системи ідентифікації, моніторингу та мінімізації технологічних ризиків, а також обов'язкову наявність планів безперервності (BCP) і відновлення після катастроф (DRP). Другий компонент — звітність про інциденти (Incident Reporting) — вимагає від організацій розроблення процесів кібербезпеки, фіксації та оперативного повідомлення про ІКТ-інциденти відповідним регуляторам. Третій напрям — тестування операційної стійкості (Digital Operational Resiliency Testing) — передбачає проведення регулярних перевірок готовності систем до кризових подій, включно з планами усунення виявлених вразливостей. Четверта складова — управління ризиками третіх сторін (ICT Third-party Risk) — встановлює вимогу контролювати та перевіряти постачальників ІКТ-послуг, які підпадають під нагляд ЄС, щоб запобігти порушенням у ланцюгу постачання. Завершальний елемент — обмін інформацією та аналітикою (Information & Intelligence Sharing) — стимулює підприємства до колективної взаємодії та обміну даними про кіберзагрози, що сприяє підвищенню загального рівня кіберстійкості фінансового сектору. У сукупності ці напрями створюють комплексну нормативну модель, яка забезпечує проактивне управління цифровими ризиками, підвищує довіру до фінансових інститутів і гармонізує стандарти безпеки в межах Європейського Союзу.



Рис. 7.3. Основні компоненти Регламенту DORA (Digital Operational Resilience Act)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Особливе місце в DORA займає вимога створення інтегрованої політики безперервності (Business Continuity Policy), яка має охоплювати всі бізнес-процеси, залежні від ІКТ. Ця політика повинна містити план безперервності (BCP), план відновлення після катастроф (DRP), а також процедури тестування, оцінювання готовності персоналу та перевірки працездатності систем у кризових ситуаціях. DORA зобов'язує керівництво фінансових організацій брати

безпосередню участь у затвердженні та перегляді цих документів, що підвищує рівень управлінської відповідальності.

Регламент також передбачає створення механізмів незалежного аудиту операційної стійкості, регулярні перегляди політик безпеки, зберігання журналів подій і логів, а також забезпечення прозорості під час взаємодії з регуляторами (наприклад, Європейським банківським органом — ЕБА, Європейським органом з цінних паперів та ринків — ESMA і Європейським органом страхування та пенсійного забезпечення — EIOPA).

Окремим положенням DORA вимагає, щоб підприємства впроваджували інтегровану архітектуру кіберстійкості, де BCP і DRP поєднуються з процесами виявлення вразливостей, реагування на інциденти, управління ланцюгом постачання програмного забезпечення та захисту критичних даних. Для цього рекомендується використовувати автоматизовані системи моніторингу, SIEM, SOAR і Threat Intelligence-платформи, які забезпечують виявлення та усунення загроз у реальному часі.

Таким чином, Регламент DORA формує нову парадигму цифрової операційної стійкості, у межах якої підприємства переходять від реактивного до проактивного управління ризиками. Він уніфікує стандарти BCP і DRP у всіх країнах ЄС, сприяє побудові довіри між фінансовими інститутами, державними регуляторами та клієнтами й забезпечує гармонізацію європейського підходу до кіберзахисту та безперервності бізнесу. Реалізація вимог DORA стає критично важливою умовою для стійкості фінансових систем, безпеки транзакцій і стабільності цифрової економіки в умовах глобальних кіберзагроз.

Отже, планування безперервності бізнес-процесів і стратегії відновлення після катастроф утворюють єдину систему операційної стійкості підприємства. Вона поєднує стратегічне управління ризиками, технічні рішення резервування, організаційні механізми взаємодії та нормативно-правові вимоги, спрямовані на збереження даних, стабільність роботи й довіру клієнтів навіть у найскладніших умовах функціонування інформаційних систем і мереж.

7.2. РЕЗЕРВНЕ КОПІЮВАННЯ ДАНИХ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СУЧАСНІ ТЕХНОЛОГІЇ, ТИПИ (ПОВНЕ, ІНКРЕМЕНТНЕ, ДИФЕРЕНЦІЙНЕ) ТА СТРАТЕГІЇ ЗБЕРЕЖЕННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Резервне копіювання даних є одним із найважливіших елементів забезпечення інформаційної безпеки, безперервності діяльності та операційної стійкості підприємства. Його головна мета полягає у відновленні доступу до критичних інформаційних ресурсів після інцидентів, пов'язаних із втратою,

пошкодженням або компрометацією даних. Сучасні підходи до резервного копіювання інтегруються у комплексні системи кіберзахисту, поєднуючи криптографічні механізми, системи контролю цілісності, багаторівневе шифрування й аналітику ризиків для забезпечення надійності процесів збереження та відновлення інформації.

Крім того, резервне копіювання тісно пов'язане з політикою управління ризиками та планами безперервності бізнесу (BCP/DRP), оскільки гарантує мінімізацію втрат у разі кібератак, відмов обладнання або людських помилок. У сучасних інформаційно-комунікаційних системах цей процес автоматизується за допомогою спеціалізованих платформ, які забезпечують моніторинг стану копій, перевірку їхньої цілісності та регулярне тестування відновлення. Важливою тенденцією є інтеграція резервних систем із хмарними сервісами та технологіями штучного інтелекту, що дозволяє прогнозувати ризики втрати даних і адаптивно змінювати частоту створення копій. Таким чином, резервне копіювання стає не лише технічним інструментом, а й ключовим компонентом стратегії кіберстійкості підприємства, спрямованої на збереження безперервності його цифрових процесів.

Основу технологій резервного копіювання становлять три основні типи: повне, інкрементне та диференційне копіювання. Повне резервне копіювання (Full Backup) передбачає створення повної копії всіх даних системи в певний момент часу. Це найнадійніший, але й найресурсоємніший метод, який потребує значного обсягу сховищ і часу на виконання. Інкрементне копіювання (Incremental Backup) зберігає лише ті дані, які змінилися після останнього резервного збереження — повного або попереднього інкрементного. Такий підхід зменшує навантаження на систему, економить простір, але ускладнює процес відновлення, оскільки потребує послідовного відновлення кількох копій. Диференційне копіювання (Differential Backup) є компромісом між двома попередніми методами: воно зберігає всі зміни, що відбулися з моменту останнього повного копіювання, забезпечуючи швидше відновлення, але потребуючи більше місця, ніж інкрементне.

Кожен із цих типів резервного копіювання має свої переваги, обмеження та оптимальні сфери застосування, тому вибір конкретної стратегії залежить від особливостей інфраструктури, критичності даних і вимог до часу відновлення (RTO) та точки відновлення (RPO). Повне копіювання зазвичай застосовується як базовий елемент резервної політики, створюючи початкову "еталонну" версію даних, з якої надалі формуються інкрементні або диференційні копії. Його головна перевага — простота відновлення, оскільки для повернення системи у працездатний стан достатньо лише одного набору даних. Проте через великі обсяги файлів і тривалість виконання цей тип найчастіше використовується

періодично, наприклад, раз на тиждень або місяць, у поєднанні з іншими підходами.

Інкрементне копіювання є оптимальним вибором для систем, у яких дані змінюються часто, але обсяг змін незначний (наприклад, у середовищах DevOps, банківських системах, CRM-платформах). Завдяки можливості зберігати лише нові або змінені файли воно забезпечує високу ефективність використання сховища, мінімізує навантаження на мережу та скорочує вікно резервування (backup window). Недоліком цього методу є складність відновлення: у разі пошкодження хоча б однієї інкрементної копії весь ланцюг може стати неповним. Тому інкрементні копії часто комбінують із регулярними повними бекапами для підвищення надійності.

Диференційне копіювання поєднує точність повного та ефективність інкрементного методів. Його використання доцільне у випадках, коли важливо забезпечити баланс між часом створення копій і швидкістю відновлення. При цьому під час кожного циклу створюється копія лише тих змін, які відбулися після останнього повного бекапу, що дозволяє скоротити час відновлення системи до мінімуму. Наприклад, у випадку інциденту адміністратору достатньо відновити повну копію та останню диференційну, без потреби послідовного збирання всіх інкрементів.

У сучасних корпоративних середовищах ці три підходи часто реалізуються в комбінованих моделях резервування, де, наприклад, щотижня виконується повний бекап, щодня — інкрементний, а щомісяця — диференційний. Такий гібрид дозволяє досягти оптимального співвідношення між ефективністю, швидкістю відновлення та витратами на інфраструктуру. Крім того, для підвищення надійності дані часто дублюються у кілька незалежних сховищ — локальних, віддалених і хмарних, що відповідає принципам стратегії “3-2-1”.

На рис. 7.4 наведено порівняльну схему трьох основних типів резервного копіювання даних — повного (Full), диференційного (Differential) та інкрементного (Incremental). У верхній частині показано принцип повного резервного копіювання, коли кожна копія містить повний набір даних системи незалежно від попередніх резервів. Такий підхід забезпечує найвищу надійність і простоту відновлення, однак потребує значних ресурсів сховища та часу на виконання. У середній частині зображено диференційне копіювання, яке охоплює всі зміни, що відбулися з моменту останнього повного бекапу. Обсяг даних, що копіюється, поступово збільшується з кожним циклом, оскільки накопичуються нові зміни. У нижній частині показано інкрементне копіювання, де зберігаються лише зміни, що відбулися після попереднього інкрементного бекапу. Такий підхід забезпечує економію пам'яті та швидкість копіювання, але ускладнює процес відновлення, оскільки потребує послідовного відтворення кількох версій. Таким чином, рисунок демонструє співвідношення між

ефективністю, швидкістю та обсягом даних для кожного типу резервного копіювання, підкреслюючи важливість вибору оптимальної стратегії залежно від вимог до часу відновлення (RTO) і точки відновлення (RPO) у системі інформаційної безпеки.

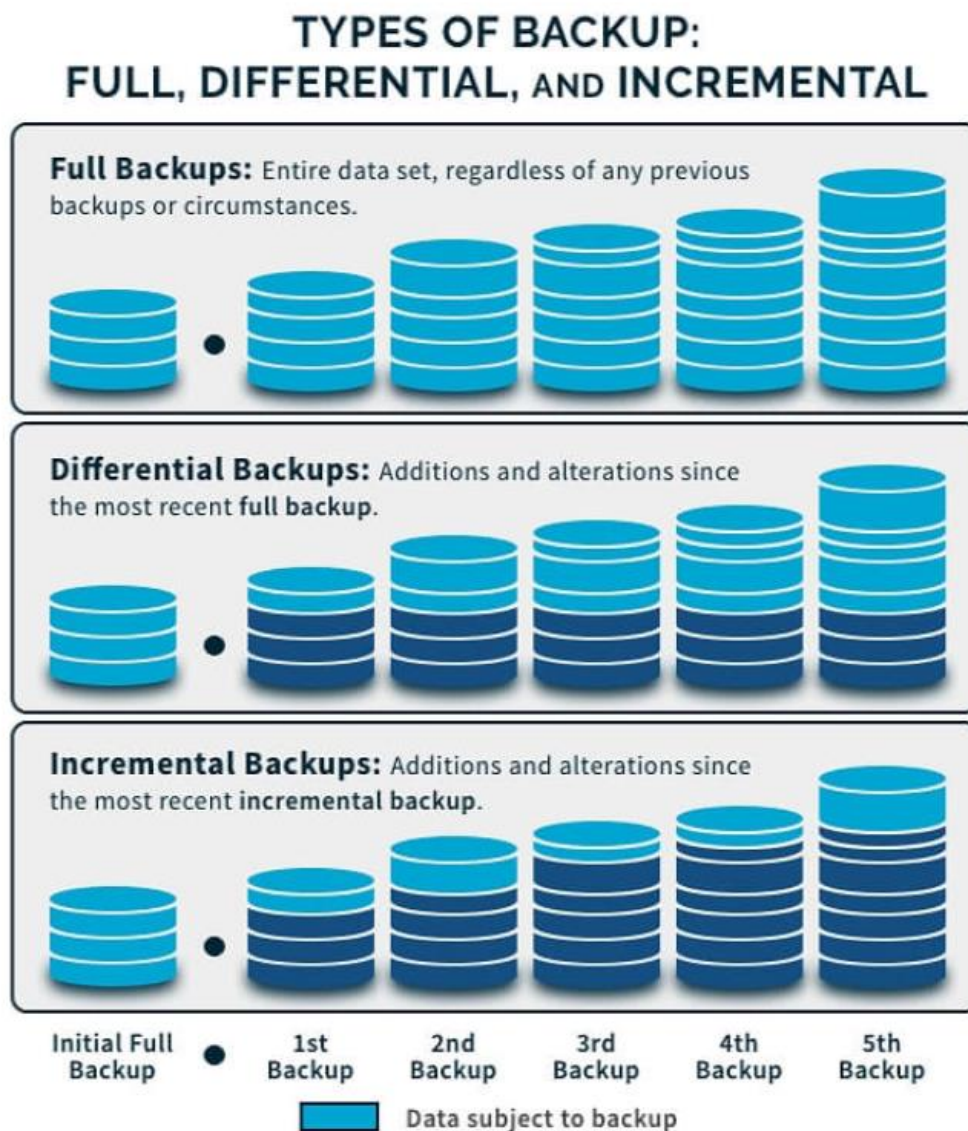


Рис. 7.4. Типи резервного копіювання: повне, диференційне та інкрементне
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Сучасні системи резервного копіювання також передбачають інтелектуальну оптимізацію процесу, коли алгоритми машинного навчання аналізують частоту змін у даних і автоматично визначають, який тип копіювання застосувати. Такий підхід дозволяє зменшити обсяг переданих даних, прискорити процеси резервування та водночас гарантувати високу надійність і відновлюваність інформації. У результаті використання комплексних стратегій

резервного копіювання забезпечує безперервність бізнес-процесів, збереження критичних активів і відповідність вимогам міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27031, ISO 22301 і NIST SP 800-34.

Сучасні технології резервного копіювання реалізуються за допомогою як локальних, так і хмарних інфраструктур. Традиційні системи, що базуються на фізичних носіях (NAS, SAN, стрічкові бібліотеки), дедалі частіше доповнюються або замінюються хмарними рішеннями — такими як AWS Backup, Google Cloud Storage, Microsoft Azure Backup, Veeam Cloud Connect, які забезпечують масштабованість, географічну розподіленість та високий рівень захисту від втрат. Хмарні сервіси дозволяють створювати гібридні стратегії резервного копіювання, де критичні дані зберігаються одночасно на локальних серверах і у віддалених дата-центрах, забезпечуючи додаткову відмовостійкість.

У сучасних умовах цифрової трансформації резервне копіювання даних набуває стратегічного значення, а його технологічна реалізація базується на поєднанні локальних і віддалених рішень, що дозволяє досягти максимальної надійності, гнучкості та швидкості відновлення. Локальні системи резервного копіювання, які включають Network Attached Storage (NAS), Storage Area Network (SAN) та стрічкові бібліотеки (Tape Libraries), продовжують відігравати важливу роль у підприємствах із високими вимогами до контролю над даними та конфіденційності. Вони забезпечують миттєвий доступ до копій, низьку затримку при відновленні й можливість ізоляції від зовнішніх мереж, що особливо актуально в контексті протидії ransomware-атакам.

Водночас, зростання обсягів даних і вимог до безперервної доступності стимулювало перехід до хмарних технологій резервного копіювання, які забезпечують масштабованість, автоматизацію та високу відмовостійкість. Провідні платформи — AWS Backup, Google Cloud Storage, Microsoft Azure Backup, IBM Cloud Object Storage, Veeam Cloud Connect — пропонують інструменти централізованого управління копіями, шифрування, контролю доступу та моніторингу стану сховищ у режимі реального часу. Хмарні сховища розподіляють дані між кількома географічними зонами (multi-region replication), що гарантує їх збереження навіть у випадку відмови цілих дата-центрів або природних катастроф. Перевагою хмарних рішень є можливість реалізації моделей "Backup as a Service" (BaaS) та "Disaster Recovery as a Service" (DRaaS), які дозволяють підприємствам передати частину відповідальності за резервування та відновлення даних спеціалізованим провайдерам. Такий підхід мінімізує витрати на фізичну інфраструктуру, зменшує потребу у власному технічному персоналі та забезпечує дотримання вимог безпеки відповідно до міжнародних стандартів (ISO/IEC 27017, SOC 2, GDPR).

Сучасна тенденція полягає у впровадженні гібридних стратегій резервного копіювання, де локальні рішення доповнюються хмарними середовищами,

утворюючи багаторівневу архітектуру захисту. Наприклад, щоденні копії можуть зберігатися локально для швидкого відновлення, тоді як щотижневі або щомісячні копії автоматично дублюються у хмару для довгострокового архівування та захисту від катастрофічних подій. Такий підхід забезпечує гнучку адаптацію до вимог RTO/RPO, дозволяючи оптимізувати витрати та гарантувати безперервність бізнес-процесів.

На рис. 7.5 представлено концептуальну схему гібридного резервного копіювання (Hybrid Cloud Backup), яка поєднує локальну та хмарну інфраструктури для забезпечення максимальної надійності та відмовостійкості. У нижній частині схеми показано різні типи джерел даних — віртуальні машини, фізичні сервери, робочі станції та ноутбуки, з яких регулярно створюються резервні копії. Ці копії спочатку зберігаються у локальному репозиторії (Local Backup Repository), що забезпечує швидкий доступ і відновлення у разі інцидентів на підприємстві. Далі з локального сховища створюється додаткова копія у хмарному середовищі (Public Cloud), що гарантує географічну розподіленість і захист від втрати даних у випадку фізичних пошкоджень або катастроф. Така архітектура забезпечує баланс між швидкістю відновлення та високим рівнем захищеності, дозволяючи реалізувати стратегію багаторівневого збереження відповідно до принципу “3-2-1”: три копії даних, на двох різних носіях, з однією копією за межами основного майданчика. Гібридне резервне копіювання є ключовим елементом сучасних систем інформаційної безпеки та безперервності бізнесу, поєднуючи гнучкість хмарних рішень із контролем і швидкодією локальних систем.

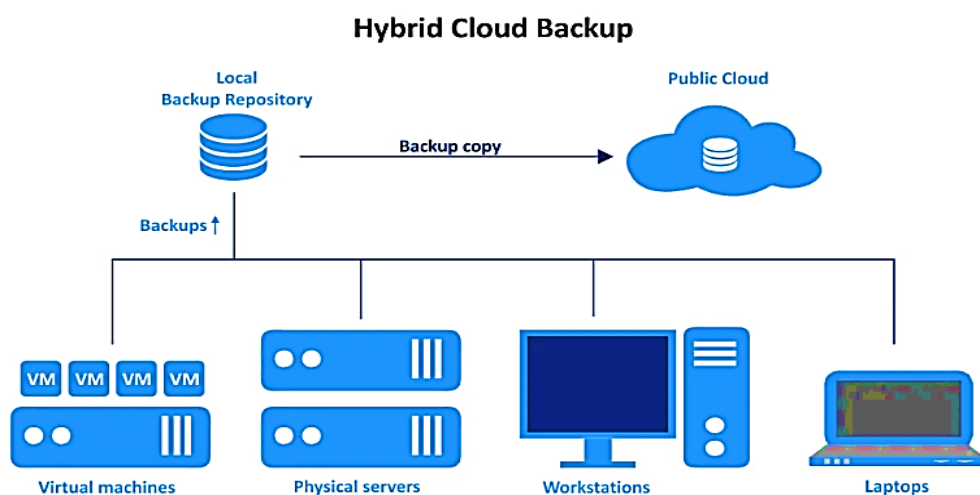


Рис. 7.5. Архітектура гібридного резервного копіювання даних
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

У контексті безпеки особливу увагу приділяють шифруванню резервних даних — як під час передачі (in transit), так і під час зберігання (at rest). Системи

резервного копіювання використовують алгоритми AES-256, RSA, TLS 1.3, цифрові підписи та токени доступу, щоб унеможливити несанкціонований доступ або підміну інформації. Крім того, впроваджується технологія імунного резервування (immutable backup), за якої резервні копії зберігаються у стані, що не підлягає зміні або видаленню протягом заданого часу. Це критично важливо для захисту від атак типу ransomware, коли зловмисники намагаються зашифрувати або знищити резервні копії.

Інноваційним напрямом розвитку є інтелектуалізація процесів резервного копіювання на основі машинного навчання та аналітики поведінкових даних. Системи можуть автоматично визначати оптимальний час для створення копій, прогнозувати ризики втрат даних, аналізувати швидкість змін у файлових системах і рекомендувати найефективніші стратегії збереження. Інтеграція таких систем із платформами SIEM, SOAR і Threat Intelligence дозволяє виявляти потенційні загрози до того, як вони вплинуть на сховища, забезпечуючи проактивний захист резервних копій.

Таким чином, сучасні технології резервного копіювання еволюціонували від ізольованих локальних рішень до інтелектуальних, децентралізованих і гібридних екосистем, здатних забезпечити не лише збереження даних, а й стратегічну безперервність бізнесу. Вони стали ключовою складовою систем управління інформаційною безпекою, операційної стійкості (Operational Resilience) та відповідності регуляторним вимогам — зокрема, стандартам ISO 22301, ISO/IEC 27031, NIST SP 800-34 і Регламенту DORA, що підкреслює важливість резервного копіювання як невід'ємного елементу кіберзахисту сучасного підприємства.

На рис. 7.6 представлено концепцію гібридного резервного копіювання (Hybrid Backup), яка поєднує переваги локального та хмарного збереження даних для забезпечення максимальної надійності, масштабованості й безперервності бізнес-процесів. У цій моделі усі дані з різних джерел — віртуальних серверів, фізичних серверів, настільних комп'ютерів і ноутбуків — передаються на спеціальний пристрій для резервного копіювання (Backup appliance), який виступає локальним сховищем першого рівня. Після створення копій дані проходять процес реплікації (Replication) до хмарного середовища (Cloud), де зберігаються у зашифрованому вигляді та можуть бути оперативно відновлені у разі втрати, пошкодження або кібератаки. Така архітектура забезпечує відмовостійкість навіть у разі виходу з ладу локальної інфраструктури, дозволяючи відновити критичні ресурси через хмару. Гібридне копіювання є ключовим елементом сучасних стратегій Disaster Recovery і Business Continuity Planning, оскільки поєднує швидкість локального відновлення з гнучкістю та географічною захищеністю хмарних технологій. Завдяки цьому підходу підприємства можуть досягати високого рівня операційної стійкості (Operational

Resilience), відповідати вимогам міжнародних стандартів ISO 22301, ISO/IEC 27031 та Регламенту DORA, а також мінімізувати ризики втрати інформації у динамічному цифровому середовищі.

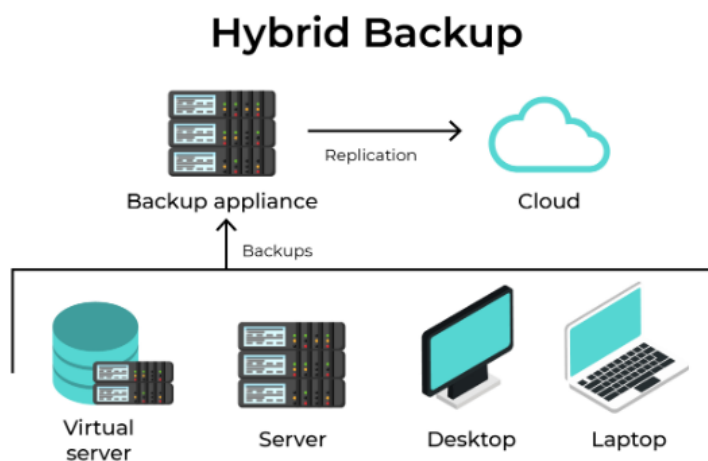


Рис. 7.6. Архітектура гібридного резервного копіювання в системах інформаційної безпеки

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Одним із ключових напрямів розвитку резервного копіювання є використання технологій дедуплікації, які усувають дублікати даних і зменшують обсяг копій, що зберігаються. Також активно впроваджуються знімки стану системи (snapshots), що дають змогу миттєво фіксувати стан віртуальних машин, баз даних або контейнерів без зупинки роботи. У середовищах, побудованих на контейнерних технологіях (Docker, Kubernetes), застосовуються policy-based backup solutions, які автоматично визначають політики збереження на основі критичності додатків і вимог до часу відновлення (RTO/RPO). Сучасні системи дедуплікації працюють як на рівні файлів, так і на рівні блоків даних, що дозволяє ефективно оптимізувати простір у сховищах і зменшити навантаження на канали передачі під час резервування. Завдяки індексації унікальних блоків і створенню хеш-ідентифікаторів зменшується кількість дубльованої інформації, що особливо актуально при збереженні великих архівів або щоденних інкрементних копій. Технологія snapshots підтримує миттєве створення контрольних точок без зупинки сервісів, що критично важливо для систем із високими вимогами до доступності — таких як банківські або телекомунікаційні платформи. У хмарних і віртуалізованих середовищах знімки інтегруються з механізмами оркестрації, що дозволяє швидко відновлювати окремі віртуальні машини, контейнери або навіть окремі бази даних.

Two Node Deduplication

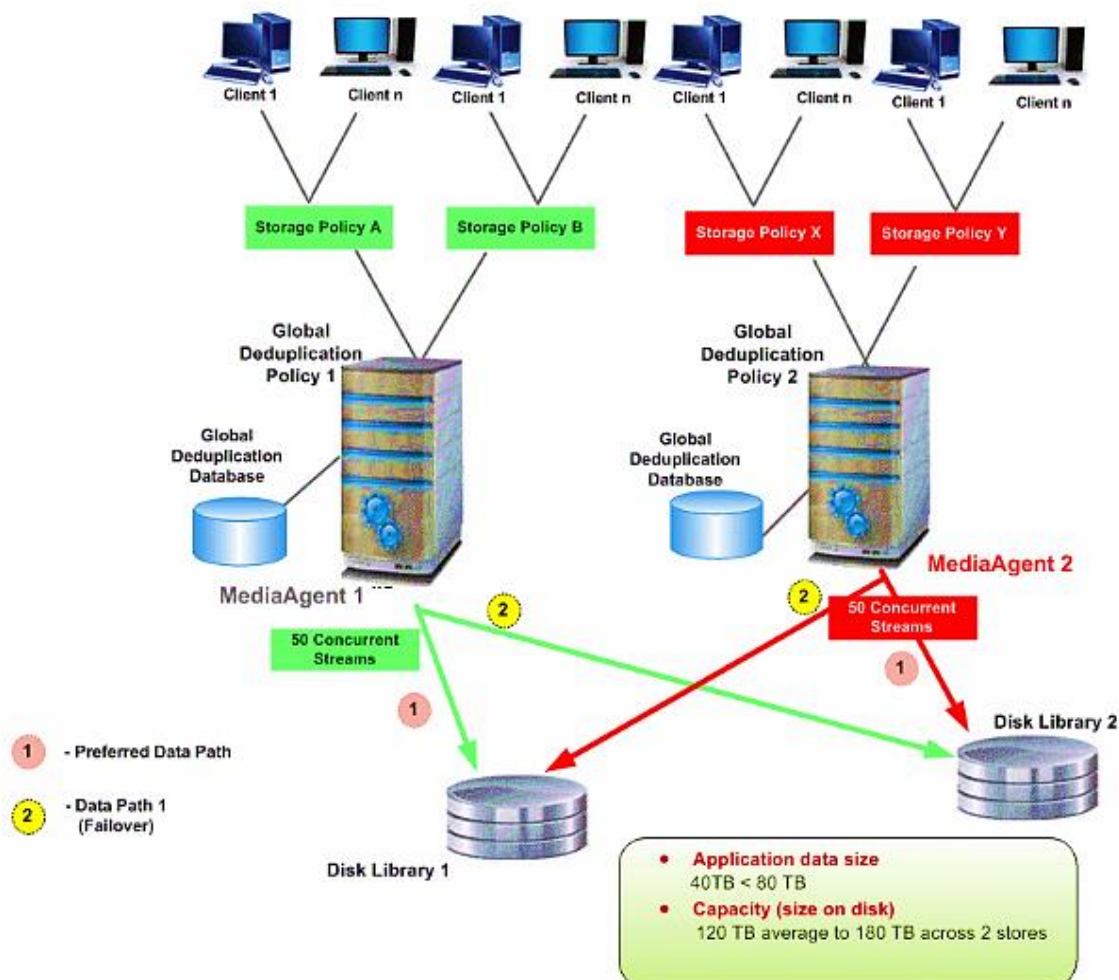


Рис. 7.7. Архітектура двовузлової дедуплікації даних у системах резервного копіювання

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 7.7 представлено архітектуру двовузлової системи дедуплікації (Two Node Deduplication), яка забезпечує оптимізацію обсягів збережених резервних копій за рахунок усунення дубльованих даних. Клієнтські пристрої передають резервні копії відповідно до визначених політик збереження — Storage Policy A, B, X, Y — до двох медіаагентів (MediaAgent 1 і MediaAgent 2), що виконують функції обробки даних і застосовують глобальні політики дедуплікації. Кожен агент має власну базу даних дедуплікації (Global Deduplication Database), у якій зберігаються хеш-ідентифікатори унікальних блоків, що дозволяє уникати повторного запису однакових сегментів під час подальших копіювань. Передача даних здійснюється через основний канал

(Preferred Data Path) із можливістю автоматичного перемикання на резервний шлях (Failover Path) у разі відмови або перевантаження. Дані зберігаються у двох бібліотеках дисків (Disk Library 1 і Disk Library 2), що забезпечують балансування навантаження, високу пропускну здатність (до 50 паралельних потоків) і масштабування сховищ. Така архітектура дозволяє зменшити загальний обсяг даних на диску на 40–60 %, підвищуючи ефективність використання ресурсів і швидкість відновлення інформації. Завдяки розподіленню процесів дедуплікації між вузлами досягається безперервність роботи системи резервного копіювання, навіть у випадку відмови одного з агентів, що робить цей підхід критично важливим для великих корпоративних інфраструктур і хмарних середовищ.

Політично керовані системи резервного копіювання (policy-based backup solutions) дедалі частіше використовують алгоритми машинного навчання для автоматичного визначення пріоритетів резервування, розподілу ресурсів і моніторингу стану копій у реальному часі. Це забезпечує адаптивне управління процесом, коли система самостійно реагує на зміну навантаження, появу нових додатків чи зміну рівня критичності даних. Також активно впроваджуються інкрементальні знімки (incremental snapshots), які фіксують лише змінені блоки, що дає змогу ще більше зменшити час створення резервних точок і обсяг переданих даних.

Додатково сучасні рішення підтримують глобальну дедуплікацію (global deduplication), коли оптимізація даних здійснюється не лише в межах одного сховища, а між усіма локаціями підприємства чи хмарними вузлами. Це забезпечує централізоване управління копіями, прискорює процеси відновлення та суттєво скорочує витрати на інфраструктуру. У підсумку комбінація дедуплікації, snapshots і політик керованого резервування формує інтелектуальну архітектуру захисту даних, яка поєднує швидкість, ефективність і надійність, відповідаючи вимогам сучасних стандартів безпеки та безперервності бізнесу.

Важливою складовою є стратегії резервного збереження даних, які визначають частоту створення копій, місце їх розміщення та політику зберігання. Найпоширенішими є стратегії “Grandfather–Father–Son (GFS)”, що передбачають поєднання щоденних, щотижневих і щомісячних копій, та стратегія “3-2-1”, згідно з якою необхідно мати три копії даних, збережені на двох різних типах носіїв, причому одна з них — поза основним майданчиком. Для підвищення захищеності застосовується офлайн-копіювання (air-gapped backup), при якому резервні носії ізольовані від мережі, що унеможливорює зараження шкідливим ПЗ чи ransomware.

На рис. 7.8 показано принцип стратегії 3-2-1 резервного копіювання, яка є однією з найефективніших практик забезпечення безперервності діяльності та інформаційної безпеки. Сутність цієї стратегії полягає у збереженні трьох копій даних: однієї робочої (Here) і двох резервних (Near і Far). Робоча копія

зберігається локально у середовищі користувача або на сервері, де здійснюється поточна обробка інформації. Перша резервна копія (Near) також розміщується локально, але ізольовано від основного робочого простору, що дозволяє швидко відновити дані у разі незначних збоїв або помилок користувача. Друга резервна копія (Far) розміщується поза межами основного майданчика (off-site), наприклад у віддаленому дата-центрі, хмарному сховищі або на фізичному носії, який зберігається в іншій географічній зоні. Таким чином, стратегія 3-2-1 передбачає розміщення копій у двох різних місцях із використанням щонайменше двох типів носіїв (наприклад, локальний диск і хмарне сховище). Це дозволяє забезпечити стійкість до фізичних ушкоджень, атак типу ransomware та катастрофічних подій, підвищуючи рівень операційної стійкості підприємства. Реалізація такої стратегії є ключовим компонентом політики резервного копіювання, рекомендованої міжнародними стандартами ISO/IEC 27040 та NIST SP 800-34.

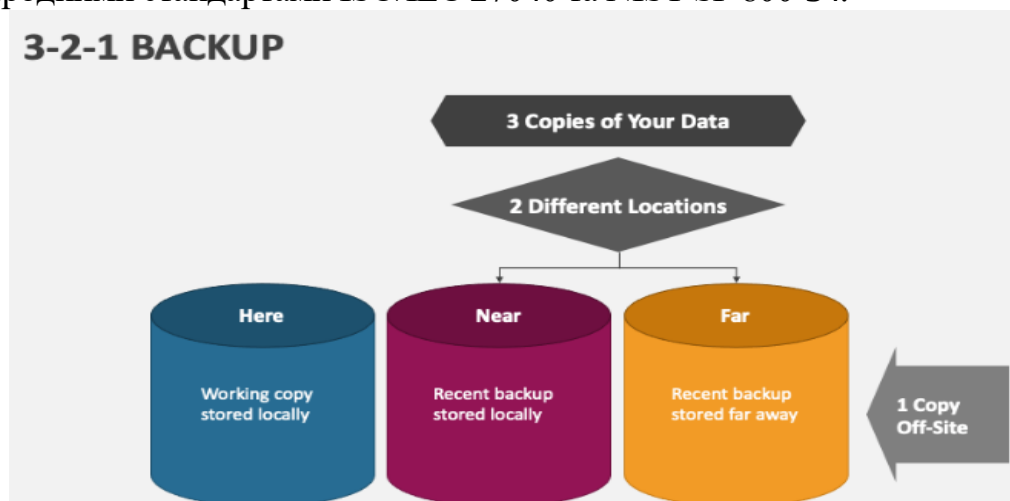


Рис. 7.8. Стратегія резервного копіювання 3-2-1 для забезпечення збереження даних

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

У межах систем інформаційної безпеки резервне копіювання тісно інтегрується з SIEM- і SOAR-системами, які відстежують стан копій, контроль доступу до сховищ і фіксують будь-які аномальні дії. Шифрування даних перед збереженням (AES-256, RSA, ECC) і контроль цифрових підписів забезпечують їх цілісність і автентичність, що є критично важливим у регульованих галузях — фінансовій, енергетичній, телекомунікаційній.

Таким чином, резервне копіювання даних є невід’ємною частиною систем управління інформаційною безпекою, оскільки забезпечує відновлюваність інформаційних ресурсів, мінімізує наслідки інцидентів та підтримує стійкість ІТ-інфраструктури підприємства. Його ефективність визначається не лише використанням сучасних технологій, а й правильним поєднанням типів

копіювання, частоти створення копій, політик зберігання та інтеграції з процесами ризик-менеджменту й безперервності бізнесу (BCP/DRP). У результаті формується комплексна система захисту даних, здатна гарантувати цілісність, доступність і конфіденційність інформації навіть у разі найсерйозніших кібератак або технічних збоїв.

7.3. ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ І ГІБРИДНИХ ІНФРАСТРУКТУР ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦИФРОВОЇ БЕЗПЕРЕРВНОСТІ ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВА

В умовах стрімкої цифровізації бізнес-процесів і зростання залежності підприємств від інформаційно-комунікаційних технологій, питання цифрової безперервності (Digital Continuity) набуває стратегічного значення. Забезпечення стабільного функціонування інформаційних систем, навіть у разі інцидентів, аварій або кібератак, стає ключовим фактором конкурентоспроможності. У цьому контексті хмарні сервіси та гібридні інфраструктури відіграють фундаментальну роль, створюючи гнучке, масштабоване та відмовостійке середовище для збереження, обробки та відновлення даних.

Хмарні технології дозволяють підприємствам не лише оптимізувати витрати на IT-інфраструктуру, але й забезпечити високу доступність сервісів завдяки географічному розподілу ресурсів і автоматичному дублюванню даних. Гібридні моделі поєднують переваги локальних і віддалених систем, що дає змогу зберігати контроль над критичними даними всередині підприємства, водночас використовуючи хмарні ресурси для масштабування та аварійного відновлення. Такий підхід значно підвищує рівень операційної стійкості, мінімізує ризики простоїв і забезпечує безперервність ключових бізнес-процесів навіть у кризових умовах. Завдяки інтеграції хмарних сервісів у політику Business Continuity та Disaster Recovery підприємства отримують можливість автоматизувати процеси резервного копіювання, моніторингу та відновлення систем. Крім того, використання хмарних платформ сприяє дотриманню міжнародних стандартів безпеки, таких як ISO 22301, ISO/IEC 27031 та Регламент DORA, що є важливою складовою кіберстійкості. У результаті хмарно-гібридні рішення формують основу для побудови цифрово зрілої екосистеми підприємства, здатної адаптуватися до динамічних викликів інформаційного середовища.

Роль хмарних технологій у цифровій безперервності

Хмарні сервіси (Cloud Services) надають підприємствам можливість використовувати розподілені ресурси для збереження критичних даних, запуску резервних копій, масштабування обчислювальних потужностей і підтримки

доступності систем у будь-яких умовах. Ключові моделі — IaaS (Infrastructure as a Service), PaaS (Platform as a Service) та SaaS (Software as a Service) — дозволяють гнучко адаптувати ІТ-інфраструктуру до змін бізнес-процесів, скорочуючи витрати на власне обладнання. Хмарні сервіси таких провайдерів, як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) та IBM Cloud, підтримують механізми автоматичного резервного копіювання, географічного дублювання даних (geo-replication) і автоматичного перемикання на резервні майданчики (failover), що забезпечує безперервну доступність навіть при критичних збоях основних серверів.

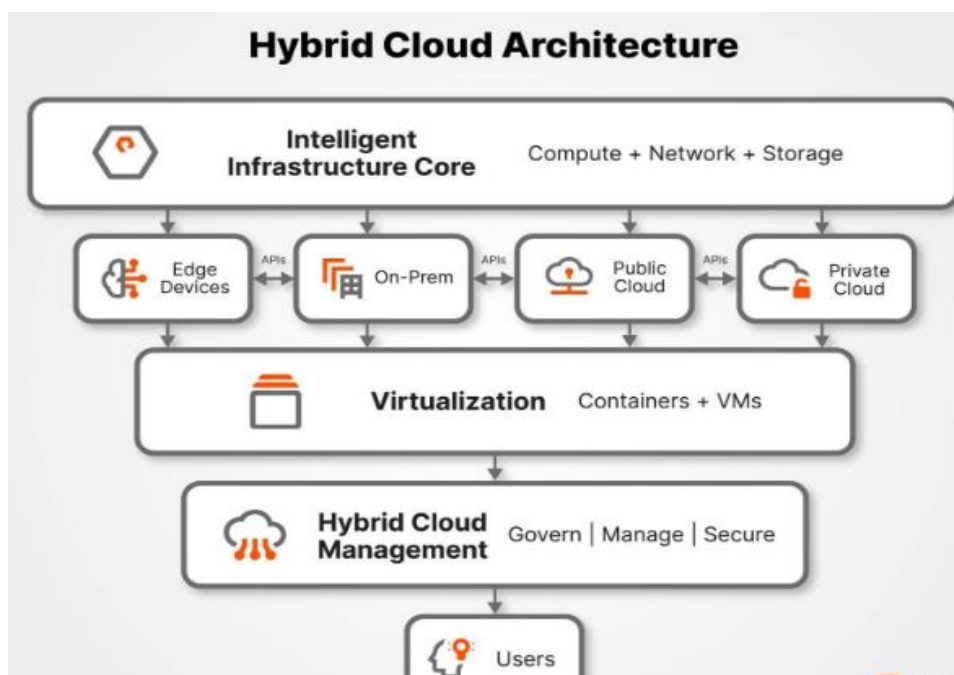


Рис. 7.9. Гібридна архітектура хмарної інфраструктури підприємства
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На рис. 7.9 представлено узагальнену схему гібридної хмарної архітектури, яка поєднує переваги локальних ресурсів (on-premises), публічних і приватних хмар, а також периферійних (edge) пристроїв. У центрі архітектури розташоване ядро інтелектуальної інфраструктури (Intelligent Infrastructure Core), що об'єднує обчислювальні ресурси, мережеві компоненти та системи зберігання даних. Через API-з'єднання забезпечується взаємодія між компонентами — локальними дата-центрами, публічними хмарними платформами (наприклад, AWS, Azure, GCP) і приватними хмарами підприємства. Наступним рівнем є віртуалізація, яка реалізується за допомогою контейнерів (Docker, Kubernetes) або віртуальних машин (VMs), що забезпечує незалежність додатків від конкретної фізичної інфраструктури. Керування всіма елементами здійснюється через модуль Hybrid

Cloud Management, який відповідає за адміністрування, моніторинг, безпеку та політику доступу. Завдяки такій моделі користувачі отримують безперервний і захищений доступ до цифрових сервісів, а підприємство — гнучкість, масштабованість і стійкість до збоїв у будь-яких умовах експлуатації.

Завдяки інтеграції хмарних сервісів у стратегію управління бізнес-процесами підприємства можуть забезпечувати високий рівень гнучкості та швидке відновлення роботи після інцидентів. Хмарна інфраструктура дозволяє масштабувати ресурси у реальному часі, реагуючи на зміни навантаження, що особливо важливо для компаній із динамічними ІТ-середовищами. Сучасні сервіси підтримують концепцію multi-cloud, яка передбачає використання кількох постачальників для підвищення надійності та уникнення залежності від одного провайдера. Крім того, хмарні платформи впроваджують засоби шифрування, керування ідентичностями (IAM) та моніторингу безпеки, що гарантує захист даних на всіх етапах їхнього життєвого циклу. Завдяки автоматизованим інструментам оркестрації та аналітики ризиків хмарні сервіси стають основою проактивного управління безперервністю діяльності. Таким чином, вони формують ядро сучасної цифрової стійкості підприємства, забезпечуючи одночасно безпеку, ефективність і надійність усіх бізнес-функцій.

Гібридна інфраструктура як модель цифрової стійкості

Гібридна інфраструктура (Hybrid Cloud Infrastructure) поєднує переваги локальних дата-центрів (on-premises) і публічних або приватних хмар. Такий підхід дозволяє розподіляти навантаження між локальними ресурсами та хмарними сервісами, оптимізуючи продуктивність і забезпечуючи високу доступність (High Availability). У разі інциденту гібридна архітектура дає змогу швидко перенести обчислювальні процеси або бази даних у хмару, де забезпечується резервне виконання бізнес-функцій без переривання операцій. Для цього використовуються технології контейнеризації (Docker, Kubernetes), віртуалізації (VMware, Hyper-V) та orchestration-платформи, що автоматично відновлюють сервіси відповідно до політики безперервності.

Гібридна модель забезпечує підприємствам гнучкість у виборі середовища для зберігання та обробки даних залежно від рівня їх критичності, конфіденційності чи регуляторних вимог. Вона дозволяє балансувати між безпекою локальних ресурсів і масштабованістю хмарних платформ, що особливо актуально для великих компаній із розгалуженою ІТ-інфраструктурою. У межах гібридних систем реалізуються механізми автоматичного перемикавання навантажень (load balancing) та інтелектуального маршрутизації трафіку, що підвищують ефективність роботи мереж і мінімізують ризик простоїв. Важливим компонентом є інтеграція засобів моніторингу та аналітики, які у реальному часі відстежують стан систем і виявляють потенційні відхилення від нормальної роботи. Завдяки цьому підприємства можуть оперативно реагувати на інциденти,

прогнозувати можливі збої та забезпечувати стійкість критичних сервісів. Таким чином, гібридна інфраструктура стає не лише технологічною платформою, а й стратегічним інструментом побудови операційної стійкості (Operational Resilience) та кібербезпеки в умовах цифрової економіки.

Хмарні стратегії резервного копіювання і відновлення

Одним із базових елементів цифрової безперервності є Disaster Recovery as a Service (DRaaS) — послуга відновлення після катастроф у хмарному середовищі. Вона дозволяє автоматизувати процеси створення резервних копій (backups), реплікації та відновлення інформаційних систем у віддалених дата-центрах провайдера. Комбінуючи DRaaS із моделлю Backup as a Service (BaaS), підприємства отримують інтегроване рішення для безперервного збереження даних, яке відповідає міжнародним вимогам безпеки (ISO/IEC 27017, NIST SP 800-34, SOC2). Наприклад, у разі кіберінциденту або фізичного пошкодження серверів компанія може відновити роботу критичних додатків у хмарі протягом кількох хвилин, забезпечуючи мінімальні значення показників RTO (Recovery Time Objective) і RPO (Recovery Point Objective).

На рис. 7.10 зображено архітектуру гібридного хмарного середовища, побудовану на базі Cisco Cloud Center, яка поєднує приватну та публічну хмару з традиційною фізичною інфраструктурою підприємства. У верхньому рівні розташовано прикладні сервіси (Application) і компоненти безпеки — Cisco CloudLock та Stealthwatch, що забезпечують контроль доступу, моніторинг подій і захист даних у процесі передачі. Центральний рівень — це керуючий модуль Cisco Cloud Center, який відповідає за інтеграцію між різними середовищами, балансування навантаження та автоматизацію розгортання додатків. Приватна хмара реалізується на основі платформ VMware, Windows Azure Pack, OpenStack та рішень Cisco, що дозволяє розгортати внутрішні сервіси з високим рівнем контролю безпеки. Публічна хмара представлена провайдерами Amazon Web Services, Microsoft Azure і Rackspace, які забезпечують масштабованість, відмовостійкість та географічне дублювання даних. Завдяки інтеграції усіх компонентів у єдину систему управління Cisco Cloud Center створюється гнучке та безпечне середовище для підтримки цифрової безперервності підприємства.

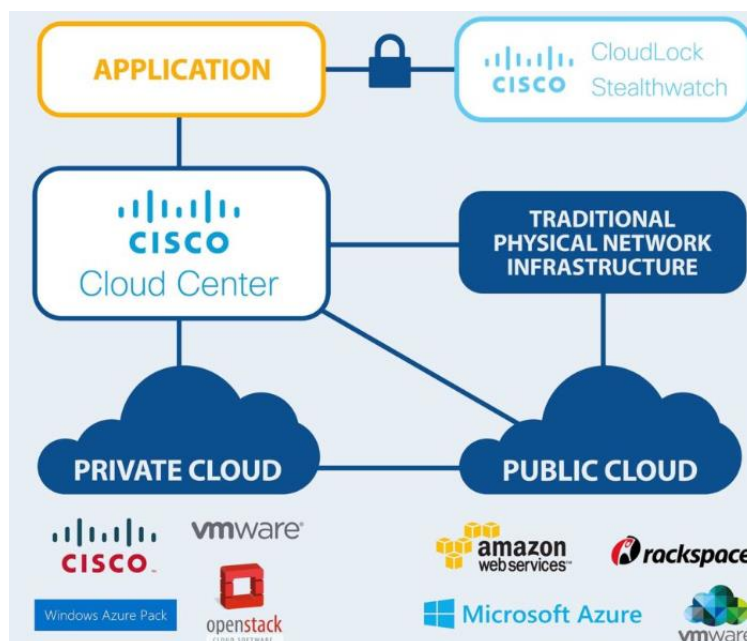


Рис. 7.10. Архітектура хмарного середовища Cisco Cloud Center у моделі гібридної інфраструктури

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Хмарні стратегії резервного копіювання також передбачають географічне дублювання даних (geo-replication), що гарантує їхню доступність навіть у разі втрати одного з дата-центрів. Провайдери впроваджують мультизонні архітектури (multi-region architectures), які дозволяють підприємствам динамічно обирати місце зберігання копій відповідно до вимог безпеки та законодавства про захист даних. Завдяки автоматизованим політикам збереження (retention policies) та шифруванню під час передавання і зберігання даних забезпечується високий рівень захисту від несанкціонованого доступу та компрометації. Крім того, сучасні DRaaS-платформи інтегруються з SIEM- і SOAR-системами, що дає змогу поєднати процеси відновлення з кібермоніторингом і реагуванням на інциденти у режимі реального часу. Це не лише скорочує час відновлення після збоїв, а й створює замкнений цикл безпеки та стійкості. У результаті хмарні стратегії резервного копіювання стають фундаментом цифрової безперервності підприємства, забезпечуючи захист, прозорість і оперативність у будь-яких умовах.

Використання контейнерних технологій і DevSecOps

Сучасна цифрова інфраструктура підприємств часто реалізується на основі контейнерних технологій (Docker, Kubernetes, OpenShift), що дозволяють гнучко переносити робочі навантаження між середовищами. Інтеграція принципів DevSecOps забезпечує безперервне тестування безпеки та стійкості додатків у процесі розробки й розгортання. У межах CI/CD-процесів впроваджується chaos

engineering — симуляція відмов і атак, яка дозволяє перевіряти ефективність резервних сценаріїв та адаптивність архітектури. Завдяки цьому безперервність цифрових сервісів підтримується навіть у середовищі постійних змін і кіберризиків.

Контейнеризація сприяє підвищенню рівня ізоляції компонентів системи, що мінімізує ризики поширення інцидентів між сервісами та спрощує управління оновленнями без зупинки роботи. Інтеграція систем оркестрації, таких як Kubernetes чи OpenShift, дозволяє автоматизувати масштабування, балансування навантажень і відновлення контейнерів у разі збоїв, що підвищує стійкість цифрових сервісів. У DevSecOps-підході безпека впроваджується на кожному етапі життєвого циклу додатка — від кодування до експлуатації — через автоматизовані перевірки вразливостей, політики доступу та контроль залежностей у ланцюгу постачання програмного забезпечення (Software Supply Chain Security). Це забезпечує не лише оперативне виявлення, а й запобігання потенційним кіберзагрозам ще до їхнього прояву. Використання контейнерів спрощує реалізацію стратегій immutable infrastructure, де середовища створюються заново після інцидентів, що мінімізує вплив компрометацій. Таким чином, поєднання контейнерних технологій і DevSecOps формує цілісну екосистему цифрової безперервності, у якій безпека, відмовостійкість і адаптивність інтегровані в саму архітектуру підприємства.

Забезпечення відповідності нормативним вимогам

Використання хмарних і гібридних рішень також відповідає сучасним міжнародним нормативам у сфері безпеки й стійкості. Зокрема, Регламент DORA (Digital Operational Resilience Act) встановлює обов'язкові вимоги до підприємств фінансового сектору щодо тестування BCP/DRP, контролю постачальників ІКТ-послуг і управління ризиками третіх сторін. Стандарти ISO 22301 і ISO/IEC 27031 регламентують підхід до планування безперервності бізнесу (Business Continuity Management, BCM) у цифрових екосистемах, а NIST SP 800-34 описує методологію побудови ефективних планів відновлення після інцидентів.

На рис. 7.12 представлено концептуальну схему нормативної відповідності у хмарних інфраструктурах, яка демонструє основні напрями управління безпекою та відповідності стандартам. Центральним елементом є Cloud Compliance — система забезпечення дотримання регуляторних вимог, політик і стандартів безпеки у хмарних середовищах. Вона включає кілька ключових складових: Governance (управління) — формування політик контролю доступу та моніторингу; Encryption (шифрування) — захист даних під час зберігання й передавання; Threat Modeling (моделювання загроз) — оцінювання ризиків і прогнозування потенційних атак; Shared Responsibility (спільна відповідальність) — розподіл обов'язків між постачальником хмарних послуг і користувачем;

Frameworks (рамкові стандарти) — застосування міжнародних нормативів, таких як ISO/IEC 27017, ISO 22301, NIST SP 800-34; та Regulations (регулювання) — дотримання вимог таких актів, як DORA, GDPR, SOC 2. Такий підхід забезпечує системність управління кіберризиками, прозорість процесів обробки даних і стійкість цифрових сервісів до інцидентів безпеки.



Рис. 7.12. Ключові складові нормативної відповідності у хмарному середовищі (Cloud Compliance)

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Крім того, стандарти ISO/IEC 27017 та ISO/IEC 27018 визначають вимоги до безпеки хмарних сервісів і захисту персональних даних у хмарних середовищах, що особливо актуально для підприємств, які обробляють конфіденційну або фінансову інформацію. У межах цих стандартів особливу увагу приділено контролю доступу, шифруванню даних, автентифікації користувачів і прозорості процесів обробки. Також важливу роль відіграють рекомендації ENISA (European Union Agency for Cybersecurity), які визначають принципи побудови операційної стійкості, інтеграції BCP/DRP у кібербезпекові політики та оцінювання ризиків хмарних провайдерів. Відповідність зазначеним нормативним актам не лише гарантує дотримання міжнародних вимог, а й підвищує рівень довіри клієнтів, партнерів і регуляторів до цифрової інфраструктури підприємства. Для цього впроваджуються регулярні аудити безпеки, тестування сценаріїв відновлення та перевірка працездатності хмарних резервів. Таким чином, забезпечення відповідності нормативним вимогам стає невід'ємною частиною цифрової безперервності, інтегрованою у всі процеси управління ризиками, кіберзахисту й операційної стійкості підприємства.

Переваги впровадження хмарно-гібридних систем

Використання хмарних сервісів і гібридних інфраструктур забезпечує низку переваг:

- Високу відмовостійкість завдяки географічно розподіленим дата-центрам.
- Масштабованість і гнучкість, що дозволяє оперативно адаптуватися до змін навантаження.
- Економічну ефективність, оскільки скорочуються витрати на апаратне забезпечення й обслуговування.
- Автоматизацію управління ризиками та моніторинг подій у режимі реального часу.
- Підвищення кіберстійкості через багаторівневу систему аутентифікації, шифрування та безпечного доступу до даних.

Крім перелічених переваг, хмарно-гібридні системи забезпечують операційну гнучкість — можливість швидкого перемикання між середовищами у разі збоїв або оновлень, без переривання бізнес-процесів. Вони підтримують інтеграцію з системами штучного інтелекту та аналітики, що дозволяє прогнозувати ризики, автоматично реагувати на інциденти та оптимізувати використання ресурсів. Завдяки використанню централізованих платформ управління безпекою підприємства можуть уніфікувати політики контролю доступу, забезпечити узгодженість між локальними та хмарними сегментами інфраструктури. Гібридні рішення також сприяють зменшенню часу простою (downtime) і підвищенню продуктивності завдяки балансуванню навантажень між різними середовищами. Важливо, що такі системи створюють основу для стійкості до кібератак, оскільки дозволяють ізолювати критичні ресурси від публічних сегментів та швидко відновлюватися після інцидентів. У результаті хмарно-гібридна інфраструктура стає не лише технологічним рішенням, а й стратегічним інструментом забезпечення цифрової безперервності, конкурентоспроможності та довготривалої стабільності підприємства.

Таким чином, хмарні сервіси та гібридні ІТ-інфраструктури стали основою цифрової безперервності підприємства, забезпечуючи взаємопов'язану екосистему для управління ризиками, резервного копіювання, моніторингу й відновлення. Їх впровадження сприяє формуванню стійкої цифрової архітектури, здатної функціонувати без збоїв навіть у кризових ситуаціях, забезпечуючи довіру клієнтів, дотримання нормативних вимог і стабільність бізнесу у цифрову епоху. Крім того, інтеграція хмарних сервісів із системами Business Continuity Management (BCM) та Disaster Recovery (DR) створює єдине середовище управління стійкістю, у якому всі процеси — від резервного копіювання до реагування на інциденти — координуються автоматично. Завдяки цьому підприємства можуть реалізовувати концепцію self-healing infrastructure, коли системи самостійно виявляють і виправляють відмови без участі оператора.

Хмарні рішення підтримують orchestration-підходи, які забезпечують синхронізоване переключення між основними та резервними майданчиками, що мінімізує простої та втрати даних. Використання технологій AI/ML у хмарному моніторингу дозволяє передбачати потенційні інциденти, оцінювати ризики в реальному часі й оптимізувати ресурси для швидкого відновлення сервісів.

Також поєднання публічних, приватних і гібридних хмар забезпечує баланс між безпекою, продуктивністю та економічною ефективністю, що особливо важливо для критичних секторів — фінансів, енергетики, охорони здоров'я. Хмарні середовища створюють умови для масштабованої кіберстійкості, де безпека, доступність і відповідність нормативним вимогам підтримуються на всіх рівнях архітектури. Завдяки централізованим панелям керування підприємства отримують повну видимість цифрової інфраструктури, можливість аналізу ефективності політик та автоматизованого вдосконалення. У результаті хмарно-гібридна модель стає не лише технологічним інструментом, а й стратегічною основою цифрової трансформації, забезпечуючи операційну готовність, кіберстійкість і безперервність бізнесу у глобальному цифровому середовищі.

7.4. АВТОМАТИЗОВАНІ СИСТЕМИ ТЕСТУВАННЯ ТА ПЕРЕВІРКИ ГОТОВНОСТІ ДО ВІДНОВЛЕННЯ: СИМУЛЯЦІЇ ІНЦИДЕНТІВ, МОНІТОРИНГ І ОЦІНКА ЕФЕКТИВНОСТІ ПЛАНІВ DRP

У сучасних умовах, коли підприємства дедалі більше покладаються на цифрову інфраструктуру, автоматизація процесів перевірки готовності до відновлення після інцидентів стає невід'ємним елементом управління операційною стійкістю. Традиційні ручні перевірки планів Disaster Recovery Plan (DRP) поступаються місцем автоматизованим системам тестування, які забезпечують безперервний контроль, симуляцію інцидентів і аналіз ефективності заходів реагування. Такі системи інтегруються у загальну архітектуру Business Continuity Management (BCM) і Information Security Management System (ISMS), дозволяючи оцінювати не лише технічну готовність, а й узгодженість дій персоналу та відповідність нормативним вимогам (ISO 22301, ISO/IEC 27031, NIST SP 800-34). Автоматизовані платформи тестування, такі як IBM Resiliency Orchestration, Zerto Continuous Data Protection або ServiceNow BCM, забезпечують повний цикл управління готовністю — від планування сценаріїв до формування звітів про відновлення. Вони дозволяють проводити регулярні або тригерні перевірки без зупинки бізнес-процесів, що мінімізує ризики людських помилок і скорочує час реагування. У таких системах застосовуються інтелектуальні аналітичні модулі, які виявляють невідповідності

між цільовими та фактичними показниками RTO і RPO, автоматично генеруючи рекомендації щодо оптимізації планів DRP. Завдяки інтеграції з SIEM- і SOAR-рішеннями автоматизовані перевірки можуть враховувати реальні кіберзагрози, оновлюючи сценарії відновлення відповідно до поточного рівня ризику.

Крім того, автоматизація сприяє формуванню цифрових двійників (Digital Twins) процесів відновлення, які дозволяють моделювати поведінку системи під час кризових подій без шкоди для продуктивного середовища. Це створює основу для адаптивного управління операційною стійкістю, де система постійно самонавчається на основі результатів тестів і вдосконалює алгоритми реагування на інциденти, забезпечуючи підприємству стійкість, передбачуваність і ефективність навіть у складних цифрових умовах.

Одним із ключових напрямів автоматизації є симуляція інцидентів (Incident Simulation), що передбачає моделювання сценаріїв відмов, кібератак, відключень живлення або втрати доступу до даних. Такі симуляції проводяться за допомогою спеціалізованих платформ (наприклад, Chaos Monkey, Gremlin, IBM Resiliency Orchestration), які створюють контрольовані збої в IT-середовищі, перевіряючи стійкість систем, ефективність резервування й здатність інфраструктури до самовідновлення. Під час симуляцій відстежуються ключові показники ефективності — RTO (Recovery Time Objective), RPO (Recovery Point Objective), MTTR (Mean Time to Recovery) та рівень автоматизації відновлення критичних бізнес-функцій. Отримані результати дозволяють ідентифікувати "вузькі місця" в архітектурі, налаштувати пріоритети відновлення та вдосконалити політики реагування.

Додатково симуляція інцидентів дозволяє здійснювати стрес-тестування системи в умовах, максимально наближених до реальних кризових ситуацій, оцінюючи поведінку додатків, серверів і мережевих елементів під навантаженням. Завдяки використанню цифрових двійників (Digital Twins) інфраструктури, можливо моделювати наслідки збоїв без впливу на продуктивне середовище, що забезпечує безпечне експериментування з різними сценаріями відновлення. Платформи симуляції часто інтегруються з системами SIEM/SOAR, що дозволяє автоматично активувати відповідні скрипти реагування, аналізувати послідовність дій і коригувати правила безпеки на основі отриманих результатів. Важливим аспектом є також аналіз поведінкових аномалій під час симульованих інцидентів — це дає змогу оцінити здатність аналітичних систем виявляти відхилення та реагувати у режимі реального часу. Розширені інструменти, такі як Gremlin Fault Injection чи Azure Chaos Studio, підтримують створення сценаріїв комбінованих відмов (наприклад, одночасна втрата доступу до бази даних і перевантаження мережі), що підвищує точність оцінки стійкості комплексних систем. Результати симуляцій фіксуються у звітах про відновлення (Recovery Assessment Reports), які порівнюють фактичні

значення RTO/RPO з цільовими показниками та надають рекомендації щодо оптимізації архітектури. На основі цих звітів формуються динамічні карти ризиків (Resilience Heatmaps), що відображають найуразливіші компоненти інфраструктури та пріоритети модернізації. Таким чином, симуляції інцидентів стають не просто інструментом тестування, а невід'ємною частиною циклу постійного вдосконалення систем відновлення (Continuous Improvement of DRP), який підвищує адаптивність і кіберстійкість підприємства.

Важливим елементом є моніторинг готовності DRP, який реалізується через інтеграцію з SIEM/SOAR-платформами (Splunk, IBM QRadar, Palo Alto Cortex XSOAR). Ці системи забезпечують збір телеметрії з різних компонентів інфраструктури — серверів, сховищ, мережових пристроїв і хмарних сервісів — і в режимі реального часу оцінюють стан систем резервування. Моніторинг дозволяє не лише виявляти відхилення, а й автоматично ініціювати тестові сценарії чи відновлювальні процедури, коли система фіксує ознаки потенційної відмови. Такий підхід забезпечує постійний контроль стану готовності до аварійного відновлення і підвищує рівень кіберстійкості підприємства.

Оцінка ефективності планів базується на багатовимірному аналізі, що включає часові, ресурсні, фінансові й ризикові метрики. Автоматизовані аналітичні системи порівнюють результати симуляцій із заданими цільовими показниками (SLA, KPI) і формують звіт про готовність до відновлення (Resilience Readiness Report). Цей звіт використовується для внутрішнього аудиту, перевірок відповідності стандартам і вдосконалення стратегій BCP/DRP.

Крім того, у процесі оцінки ефективності враховується коефіцієнт узгодженості між бізнес-пріоритетами та технічними стратегіями відновлення, що дозволяє оцінити, наскільки поточні плани DRP відповідають критичності бізнес-процесів. Автоматизовані платформи аналізу, такі як ServiceNow Business Continuity Management, Zerto Analytics або IBM Resiliency Orchestration, застосовують методи data-driven assessment, що базуються на машинному навчанні, для виявлення тенденцій і прогнозування ймовірності порушення операційної стійкості. У звітах формуються інтегровані індекси стійкості (Resilience Index), які відображають взаємозв'язок між технічними параметрами відновлення, людським фактором і фінансовими втратами. Особлива увага приділяється аналізу сценаріїв невідповідності RTO/RPO, що дає змогу виявити надлишкові затримки або недооцінені ризики. Також проводиться вартісна оцінка ефективності заходів DRP (Cost-to-Resilience Ratio), що допомагає оптимізувати витрати на резервні ресурси без зниження рівня готовності. У межах циклічних перевірок результати звітів Resilience Readiness Report автоматично порівнюються з попередніми періодами, формуючи трендовий аналіз динаміки стійкості підприємства. На основі таких даних керівництво може приймати обґрунтовані рішення щодо інвестицій у модернізацію IT-

інфраструктури, навчання персоналу або вдосконалення процедур реагування. У підсумку, автоматизована оцінка ефективності планів DRP трансформується у безперервний процес управління операційною стійкістю, де результати аналітики стають рушійною силою для адаптивного розвитку систем захисту та відновлення бізнесу.

Сучасні рішення також підтримують Machine Learning-моделі прогнозування інцидентів, які аналізують історію збоїв і поведінкові дані систем для оцінки ймовірності майбутніх відмов. На основі таких прогнозів системи здатні автоматично оновлювати плани DRP, адаптуючи їх до поточного стану інфраструктури. Крім того, застосовується Continuous Resilience Testing (CRT) — концепція безперервного тестування стійкості, що поєднує автоматизовані тести, сценарії відновлення та моніторинг у єдиний замкнений цикл.

Таким чином, автоматизовані системи тестування та перевірки готовності до відновлення забезпечують підприємствам проактивне управління стійкістю, дозволяють виявляти слабкі місця до появи інцидентів і гарантують, що плани DRP не є лише формальними документами, а дієвим інструментом забезпечення безперервності бізнесу. У результаті цифрова інфраструктура підприємства набуває властивостей самовідновлення (self-healing), що є ключовою ознакою зрілої моделі операційної стійкості (Operational Resilience) у сучасній кібереконіміці.

7.5. ВПРОВАДЖЕННЯ ВИМОГ РЕГЛАМЕНТУ DORA (DIGITAL OPERATIONAL RESILIENCE ACT) У ПРОЦЕСИ УПРАВЛІННЯ ЦИФРОВОЮ СТІЙКІСТЮ ТА БЕЗПЕРЕРВНІСТЮ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Регламент DORA (Digital Operational Resilience Act), ухвалений Європейським Союзом у 2022 році, став одним із ключових нормативних документів, що визначає стандарти операційної стійкості (Operational Resilience) у цифровому середовищі. Його метою є створення єдиної системи вимог до кібербезпеки, управління ризиками та забезпечення безперервності функціонування інформаційних і комунікаційних систем у фінансовому секторі, однак його принципи дедалі частіше застосовуються й у суміжних галузях — енергетиці, телекомунікаціях, транспорті та державному управлінні. В основі DORA лежить концепція "cyber resilience by design", яка передбачає інтеграцію механізмів захисту, моніторингу, тестування та відновлення безпосередньо в архітектуру комп'ютерних систем і мереж.

На схемі наведені основні компоненти (стовпи) Регламенту DORA, які формують основу цифрової стійкості й безперервності. Кожен «стовп» у

візуалізації репрезентує ключову вимогу: управління ризиками ІКТ (ICT Risk Management), управління інцидентами, тестування цифрової стійкості (Digital Operational Resilience Testing), управління ризиками третіх сторін (Third-Party Risk Management). Схема показує, що DORA об'єднує ці напрями в єдину логічну архітектуру, підкреслюючи взаємозв'язок між політиками, аудитом, тестуванням і контролем постачальників. Завдяки подібному представленню легше зрозуміти, як всі елементи регламенту працюють спільно для забезпечення цілісності, доступності та стійкості ІТ-інфраструктури навіть під час кризових подій.

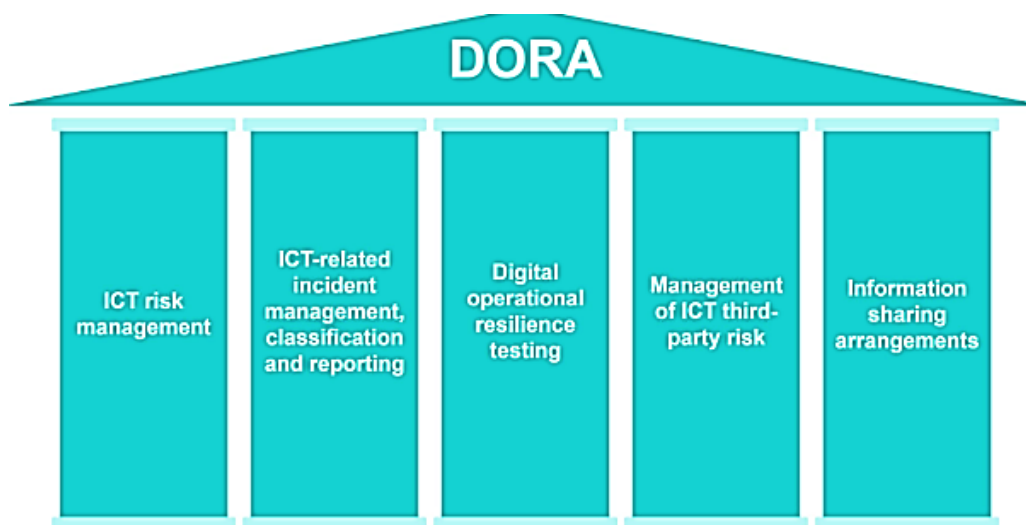


Рис. 7.13. Структура вимог DORA — «стовпи операційної стійкості»
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Однією з головних вимог Регламенту є побудова системного процесу управління ІКТ-ризиками, який охоплює ідентифікацію критичних активів, оцінку загроз, розроблення політик реагування та перевірку готовності до інцидентів. DORA зобов'язує підприємства розробляти та підтримувати плани безперервності бізнесу (BCP) і плани відновлення після інцидентів (DRP), що мають включати як технічні, так і організаційні заходи. Ці плани повинні тестуватися не рідше одного разу на рік через симуляції, стрес-тести або сценарії відмов, що дозволяє оцінити ефективність процедур відновлення та взаємодії між підрозділами. У межах тестування підприємства мають довести спроможність підтримувати RTO (Recovery Time Objective) і RPO (Recovery Point Objective) на рівнях, які гарантують безперервність ключових бізнес-функцій.

Для цього DORA передбачає впровадження автоматизованих механізмів контролю готовності, які здійснюють постійний моніторинг стану інформаційних систем і виявляють відхилення від установлених параметрів стійкості. У межах процесів управління ІКТ-ризиками використовується підхід continuous testing & monitoring, що забезпечує безперервну перевірку

працездатності резервних систем, каналів зв'язку та засобів шифрування. Також передбачається створення спеціалізованих команд з управління операційною стійкістю (Resilience Teams), які відповідають за координацію дій під час інцидентів, взаємодію з постачальниками ІКТ-послуг і забезпечення відповідності політик актуальним вимогам Регламенту. Важливим аспектом є необхідність проведення аудитів цифрової стійкості із залученням незалежних експертів, що дозволяє перевірити не лише технічні аспекти, а й рівень підготовленості персоналу до кризових ситуацій. Крім того, DORA вимагає інтеграції результатів тестувань і аудитів у систему Business Continuity Management (BCM), щоб забезпечити постійне вдосконалення процесів реагування. У підсумку ці заходи формують замкнений цикл управління стійкістю, у якому виявлення ризиків, їх оцінка, тестування, моніторинг і вдосконалення здійснюються безперервно, забезпечуючи адаптивну та проактивну модель цифрової безперервності підприємства.

Особливу увагу DORA приділяє управлінню ризиками постачальників ІКТ-послуг (Third-Party Risk Management). Відповідно до вимог Регламенту, фінансові установи та оператори критичної інфраструктури повинні здійснювати постійний аудит і моніторинг діяльності зовнішніх постачальників, які надають хмарні сервіси, послуги резервного копіювання, кіберзахисту чи технічної підтримки. Підприємства мають укладати контракти, що чітко регламентують вимоги до безпеки, звітності, планів відновлення та конфіденційності даних. У разі інциденту постачальник повинен бути готовим до швидкої передачі критичних функцій на альтернативні майданчики або до резервних провайдерів, що є частиною стратегії multi-cloud resilience.

Крім того, DORA вимагає, щоб усі постачальники ІКТ-послуг проходили періодичну оцінку ризиків і відповідали єдиним стандартам кібербезпеки, узгодженим із міжнародними нормами — такими як ISO/IEC 27001, ISO/IEC 27017 та NIST SP 800-161. Підприємства зобов'язані формувати реєстр критичних постачальників, який оновлюється на регулярній основі та містить інформацію про рівень залежності, географічне розташування дата-центрів, політику резервування й результати аудитів безпеки. DORA також передбачає обов'язкове впровадження механізмів моніторингу ланцюга постачання програмного забезпечення (Software Supply Chain Security), що дозволяє виявляти потенційно небезпечні залежності, несанкціоновані зміни у коді або вразливі бібліотеки.

У разі виявлення критичних невідповідностей постачальник має розробити план усунення порушень (Remediation Plan), який узгоджується з клієнтом і контролюється регулятором. Для запобігання каскадним збоям DORA вимагає застосування мульти-рівневого підходу до диверсифікації ІКТ-провайдерів, щоб уникнути ситуацій, коли відмова одного постачальника призводить до зупинки

всієї інфраструктури. Також запроваджується зобов'язання зберігати критичні дані в межах ЄС або на перевірених територіях, що підсилює суверенітет і контроль над інформаційними ресурсами. У сукупності ці вимоги створюють прозору систему управління залежностями, мінімізують ризики ланцюга постачання та забезпечують стійкість цифрової екосистеми підприємства навіть за умов зовнішніх загроз або кіберінцидентів.

Важливою складовою DORA є створення інтегрованих систем моніторингу та звітності щодо кіберінцидентів. Підприємства зобов'язані впроваджувати SIEM- і SOAR-рішення, які автоматизують збір, аналіз і кореляцію подій безпеки, а також забезпечують централізоване реагування на інциденти. DORA вимагає, щоб організації мали єдиний центр управління подіями (Security Operations Center — SOC), який здійснює безперервний моніторинг стану комп'ютерних систем і мереж. Крім того, усі значущі інциденти мають повідомлятися до національних компетентних органів ЄС (наприклад, EBA, ESMA або ENISA) протягом 24 годин, що підвищує рівень прозорості та координації у сфері кіберзахисту.

На рис. 7.14 зображено узагальнену структуру Регламенту Європейського Союзу DORA (Digital Operational Resilience Act), яка відображає його основні складові елементи та взаємозв'язки між ними. У центрі представлено ядро системи — управління ризиками (Risk Management), що є базовим принципом цифрової стійкості підприємства. Навколо нього розміщено ключові домени DORA, серед яких — управління інцидентами (Incidents), тестування стійкості (Resilience Tests), управління ризиками постачальників ІКТ-послуг (Third Parties), загрози та обмін інформацією (Threat & Info Sharing).

Кожен сектор діаграми деталізує певний набір процесів і вимог, передбачених Регламентом. Наприклад, блок Third Parties охоплює аудит постачальників, реєстрацію критичних партнерів, контракти, вихідні стратегії (exit strategy) і багаторівневе управління ризиками ланцюга постачання. Сектор Risk Management включає ідентифікацію, картографування, оцінку, захист, виявлення, реагування та відновлення — тобто повний життєвий цикл управління ризиками ІКТ. Компонент Resilience Tests описує механізми перевірки цифрової стійкості через тестування, планування та незалежну оцінку готовності. Діаграма також відображає принцип циклічності управління стійкістю, де всі елементи — від оцінки загроз і тестування до взаємодії з третіми сторонами — інтегровані в єдину модель безперервного вдосконалення. Завдяки такій структурі DORA забезпечує комплексне охоплення технічних, організаційних і нормативних аспектів управління цифровою безперервністю, формуючи стійку екосистему інформаційної безпеки для підприємств різних секторів.

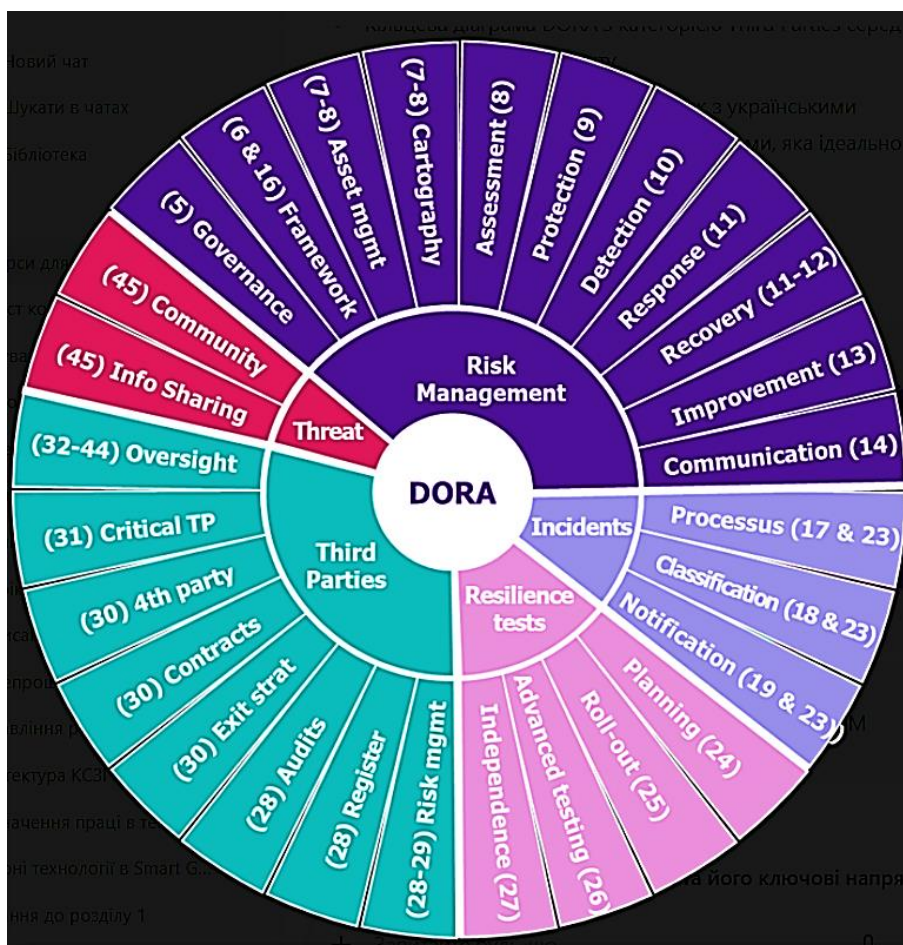


Рис. 7.13. Структура Регламенту DORA та його ключові напрями операційної стійкості

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Також DORA передбачає створення уніфікованої структури звітності (Incident Classification and Reporting Framework), яка встановлює єдині критерії для класифікації, оцінки впливу та пріоритезації кіберінцидентів. Це дозволяє регуляторам отримувати порівняльні дані, швидко оцінювати масштаби подій та координувати міждержавне реагування в межах ЄС. Системи SIEM (Security Information and Event Management) інтегруються з SOAR (Security Orchestration, Automation and Response) для автоматизації процесів аналізу журналів подій, створення інцидентних квитків і формування звітів про виконані дії.

У межах вимог DORA підприємства повинні впроваджувати механізми кореляції подій у режимі реального часу, використовуючи машинне навчання для виявлення аномалій, нетипових поведінкових патернів і потенційних ланцюгів атак. Це забезпечує можливість раннього попередження про загрози (Early Warning System) і скорочує час реагування на критичні інциденти (MTTR). Крім того, SOC-центри мають бути інтегровані у загальну систему Business Continuity

Management (BCM), щоб забезпечити безперервність бізнес-процесів навіть у разі масштабних кібератак.

Окрему увагу приділено створенню централізованих баз даних інцидентів (Incident Repositories), де накопичується інформація про всі зареєстровані події, їх причини, наслідки та ефективність ужитих заходів. Це сприяє формуванню знань для подальшого удосконалення політик кіберзахисту, підвищує рівень аналітичної зрілості та дозволяє підприємствам проводити ретроспективний аналіз загроз (Threat Intelligence Feedback Loop). Таким чином, вимоги DORA формують єдину інформаційно-аналітичну екосистему моніторингу, у якій збирання, обробка, реагування та звітність про кіберінциденти здійснюються інтегровано, уніфіковано та в реальному часі, що суттєво підвищує рівень кіберстійкості підприємств.

З точки зору технічної реалізації, впровадження вимог DORA потребує оновлення архітектури ІКС із урахуванням принципів Zero Trust, segment-based defense і adaptive authentication. Для цього застосовуються технології контейнеризації (Docker, Kubernetes), віртуалізації (VMware, Hyper-V), мультизонного резервування та географічного дублювання (geo-replication). Такі рішення забезпечують гнучкість і стійкість мереж, дозволяючи миттєво перемикаєти сервіси на резервні середовища у разі катастроф або кібератак. У поєднанні з хмарними технологіями (AWS, Azure, GCP, IBM Cloud) DORA підтримує формування гібридних IT-інфраструктур, що здатні функціонувати у режимі self-healing systems, тобто автоматично відновлювати працездатність після збоїв.

Ключовим елементом такої архітектури є впровадження принципу Zero Trust Architecture (ZTA), який базується на постійній перевірці користувачів, пристроїв і сервісів незалежно від їхнього розташування в мережі. Це забезпечується за допомогою механізмів багатофакторної аутентифікації (MFA), динамічного контролю доступу та аналізу поведінки користувачів (User and Entity Behavior Analytics — UEBA). У межах segment-based defense реалізується мікросегментація мереж, що мінімізує поверхню атаки й унеможливорює бічне переміщення загроз у разі компрометації окремого вузла.

На рис. 7.14 представлено концептуальну модель Zero Trust Architecture (ZTA), яка є ключовим елементом технічної реалізації вимог Регламенту DORA щодо забезпечення цифрової стійкості інформаційно-комунікаційних систем. Архітектура побудована за принципом «не довіряй нікому за замовчуванням» (No Implicit Trust) і базується на постійній перевірці автентичності користувачів, пристроїв і сервісів незалежно від їхнього розташування — у корпоративній

мережі, домашньому офісі чи публічному середовищі. У центрі схеми розміщено Data Plane, що охоплює всі канали зв'язку між офісами, дата-центрами, VPN-доступом і хмарними ресурсами, де кожен запит проходить динамічну перевірку на відповідність політикам безпеки.

Блок Policy Decision Point (Control Plane) відповідає за ухвалення рішень щодо доступу на основі контекстних факторів: рівня ризику, стану пристрою, типу користувача та результатів аналізу поведінки (UEBA). Цей модуль складається з Policy Engine — інтелектуального ядра, яке застосовує політики безпеки, та Policy Administration, що адмініструє правила й проводить аудит дій. Далі діє Policy Enforcement Point, який безпосередньо реалізує рішення — дозволяючи або блокуючи доступ до ресурсів, серед яких інтернет-сервіси, бази даних, SaaS-додатки чи локальні сховища.

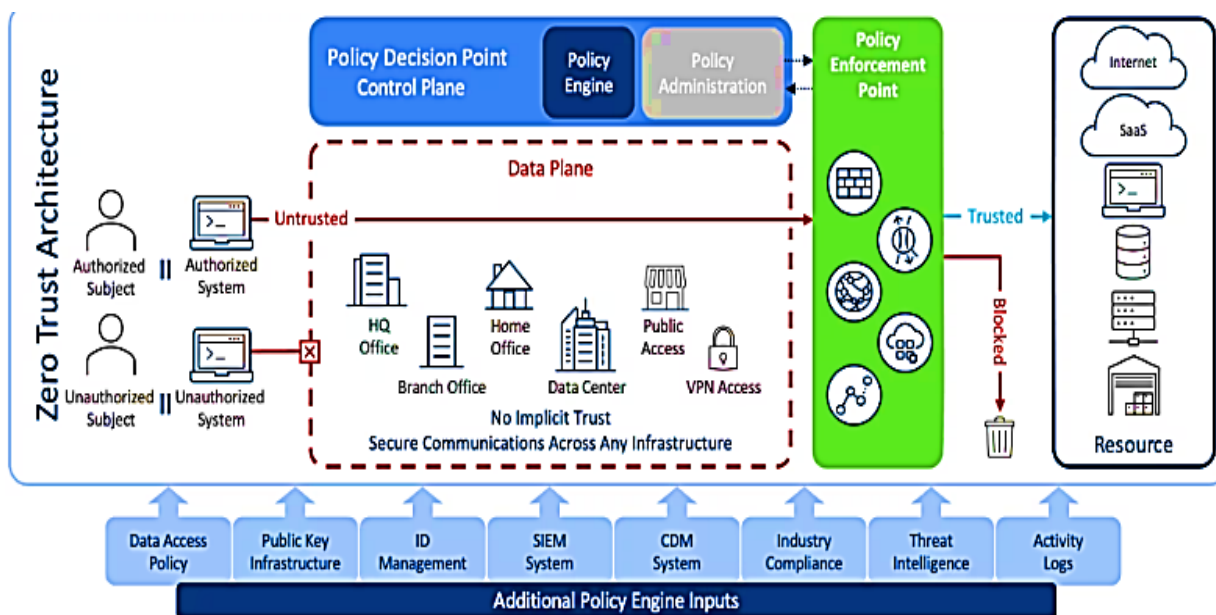


Рис. 7.14. Архітектура Zero Trust у контексті технічного впровадження вимог DORA

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Важливу роль відіграють додаткові системи, що забезпечують вхідні дані для політичного двигуна: управління ідентичностями (ID Management), інфраструктура відкритих ключів (PKI), SIEM-системи, CDM, системи відповідності стандартам (Compliance) та модулі аналізу кіберзагроз (Threat Intelligence). Саме ці компоненти підтримують безперервну оцінку довіри, виявлення аномалій і формування адаптивної політики доступу.

Таким чином, представлена архітектура демонструє, як принцип Zero Trust інтегрується в ІКС підприємства, забезпечуючи безпечний обмін даними, ізоляцію критичних сегментів, гнучке управління ризиками й автоматичну

реакцію на кіберзагрози. У межах DORA така модель виступає основою створення самовідновлюваних (self-healing) і стійких до атак гібридних ІТ-інфраструктур.

Важливою складовою технічного впровадження є інтеграція засобів оркестрації контейнерів (Kubernetes, OpenShift) із системами моніторингу стану середовищ (Prometheus, Grafana, Elastic Stack), що дозволяє відстежувати продуктивність і безпеку в реальному часі. У хмарно-гібридних середовищах застосовується автоматичне масштабування (auto-scaling) та балансування навантаження (load balancing), які підтримують безперервну роботу критичних сервісів навіть при пікових навантаженнях або відмовах вузлів.

На рис. 7.15 зображено схему інтеграції контейнерних технологій (Docker, Kubernetes, OpenShift) із системами моніторингу стану середовищ, що забезпечують спостереження за продуктивністю, безпекою та доступністю ІТ-інфраструктури в реальному часі. У центрі архітектури знаходяться контейнери, які є основними обчислювальними одиницями сучасних додатків і взаємодіють як із прикладними системами, так і з платформами оркестрації. Дані про їхній стан, продуктивність і події збираються через чотири ключові типи метрик: APM (Application Performance Monitoring) для відстеження логіки виконання додатків, Metrics для вимірювання параметрів навантаження, Logs для журналювання подій і Uptime для контролю доступності сервісів.

Kubernetes у цьому контексті виконує роль системи оркестрації, яка координує запуск, масштабування й управління контейнерами, забезпечуючи балансування навантажень між вузлами (Hosts) і гарантуючи безперервність роботи навіть у разі збоїв. Паралельно збираються метрики з рівня вузлів (CPU, пам'ять, мережеві ресурси) та інфраструктурних сервісів, які аналізуються за допомогою систем Prometheus, Grafana або Elastic Stack.

Отримані дані об'єднуються у централізованій системі спостереження (Observability Platform), де відбувається їхня кореляція, візуалізація та оцінка стану бізнес-додатків. Це дає змогу оперативно виявляти аномалії, попереджати відмови та проводити автоматичне масштабування (auto-scaling) і балансування навантаження (load balancing). Завдяки такій інтеграції забезпечується виконання технічних вимог DORA щодо операційної стійкості (Operational Resilience) — адже система може самостійно виявляти загрози, реагувати на інциденти та підтримувати стабільну роботу критичних бізнес-процесів у хмарно-гібридному середовищі.

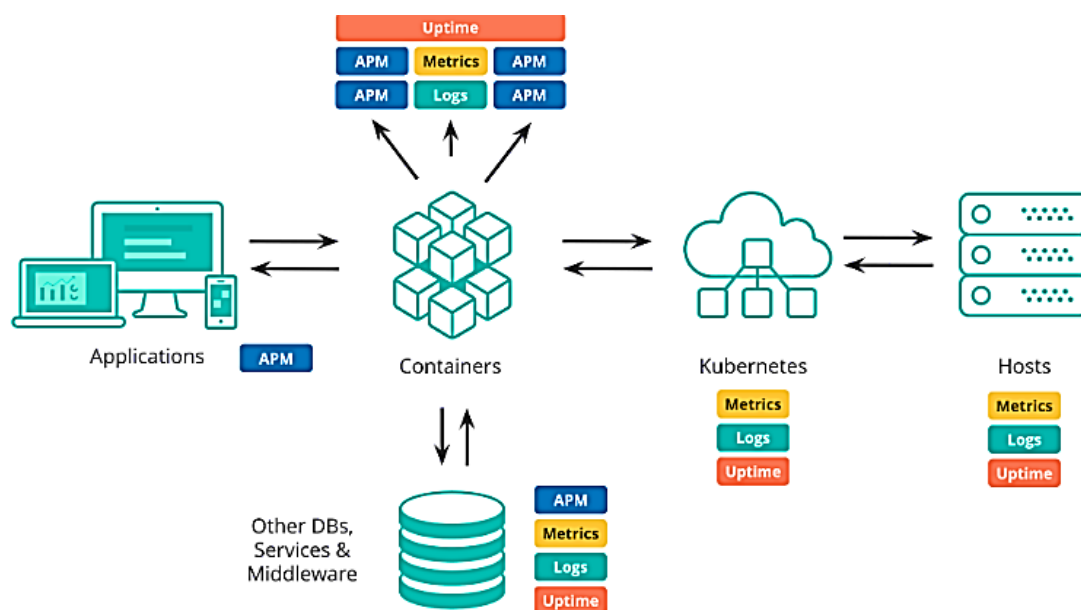


Рис. 7.15. Архітектура моніторингу контейнеризованих середовищ із використанням Kubernetes і стеку спостереження (Observability Stack)
Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

Окрім цього, реалізація вимог DORA передбачає використання систем централізованого управління політиками безпеки (Policy-based Security Management), які дозволяють синхронізувати параметри доступу, шифрування та моніторингу між локальними і хмарними сегментами мережі. У поєднанні з технологіями географічного дублювання (geo-replication) такі системи формують багаторівневу архітектуру кіберстійкості, що гарантує цілісність, доступність і відновлюваність даних у будь-яких умовах. Таким чином, технічна реалізація вимог DORA трансформує традиційні ІКС у інтелектуальні адаптивні середовища, здатні автономно реагувати на загрози, локалізувати інциденти та підтримувати операційну безперервність бізнесу.

Також Регламент DORA передбачає створення інституційного механізму кіберстійкості (ICT Operational Resilience Framework), який охоплює політики безпеки, управління ризиками, навчання персоналу та проведення внутрішніх аудитів. Підприємства повинні проводити щорічну оцінку зрілості цифрової стійкості (Digital Resilience Maturity Assessment) із використанням метрик відповідності стандартам ISO 22301, ISO/IEC 27001, NIST SP 800-34 та COBIT 2019. На основі результатів оцінки формується звіт про операційну стійкість (Operational Resilience Report), що подається керівництву та регуляторам для підтвердження готовності підприємства до цифрових інцидентів.

Крім того, DORA вимагає, щоб кожне підприємство розробило дорожню карту підвищення кіберстійкості (Resilience Improvement Roadmap), у якій визначаються конкретні етапи, строки та відповідальні особи за реалізацію

заходів щодо усунення виявлених недоліків. Важливо, щоб результати оцінки зрілості цифрової стійкості враховували не лише технічні показники, а й організаційні аспекти — культуру безпеки, рівень обізнаності співробітників і готовність керівництва до кризових ситуацій. Регламент також зобов'язує підприємства створити постійну функцію навчання та тренувань (Cyber Resilience Training and Awareness Program), спрямовану на підвищення компетенцій персоналу у сфері реагування на інциденти, резервного копіювання, відновлення систем і управління комунікацією під час криз.

Важливою частиною інституційного механізму є внутрішній аудит операційної стійкості, який проводиться незалежними експертами або спеціалізованими підрозділами для перевірки відповідності політик, процедур і технічних засобів вимогам DORA. Під час аудиту оцінюється ефективність процесів управління ризиками, наявність актуальних планів BCP/DRP, рівень автоматизації систем моніторингу та адекватність механізмів реагування. Також передбачається щорічне тестування кризових комунікацій між керівництвом, IT-відділом і зовнішніми партнерами, щоб перевірити швидкість і точність обміну інформацією під час інцидентів.

На рис. 7.16 представлено узагальнену структуру інституційного механізму ICT Operational Resilience Framework відповідно до вимог Регламенту DORA, яка поєднує управлінські, технічні та ризик-орієнтовані компоненти цифрової безпеки підприємства. У лівій частині схеми зображено блок «Leadership and Governance», що охоплює адміністративні функції, стратегічне планування, розроблення політик, визначення ролей і відповідальності, управління проєктами кібербезпеки, підвищення обізнаності та навчання персоналу. Цей рівень забезпечує керівництво процесами та формує основу корпоративної культури безпеки.

У центральній частині схеми розміщено блок «Operations and Technology», який відображає технічну складову кіберстійкості. Тут визначено ключові напрямки діяльності — архітектура системи, контроль доступу та ідентифікації, управління подіями, обробка інцидентів, безпечне знищення даних, захист електронних сервісів і робота з персональними пристроями (Bring Your Own Device). Цей сегмент відповідає за технологічну реалізацію принципів стійкості, реагування на інциденти та підтримку безперервності операцій.

У верхній частині подано блок «Risk Management and Compliance», який відображає механізми оцінки ризиків, дотримання нормативних вимог і регуляторного контролю. Саме цей рівень забезпечує узгодженість дій підприємства з міжнародними стандартами (ISO 22301, ISO/IEC 27001, NIST SP 800-34) та вимогами DORA.

Праворуч знаходиться секція «Third Party Cybersecurity», яка стосується управління ризиками постачальників ІКТ-послуг, адміністрування контрактів і

моніторингу ланцюгів постачання. Вона забезпечує надійність зовнішніх партнерів, інтегрованих у цифрову екосистему підприємства.

Загалом рисунок демонструє, як різні компоненти — управління, ризик-менеджмент, технології, взаємодія з постачальниками та людський фактор — інтегруються в єдину систему операційної стійкості, спрямовану на підвищення готовності підприємства до кіберзагроз і підтримку безперервності бізнесу в межах регламенту DORA.

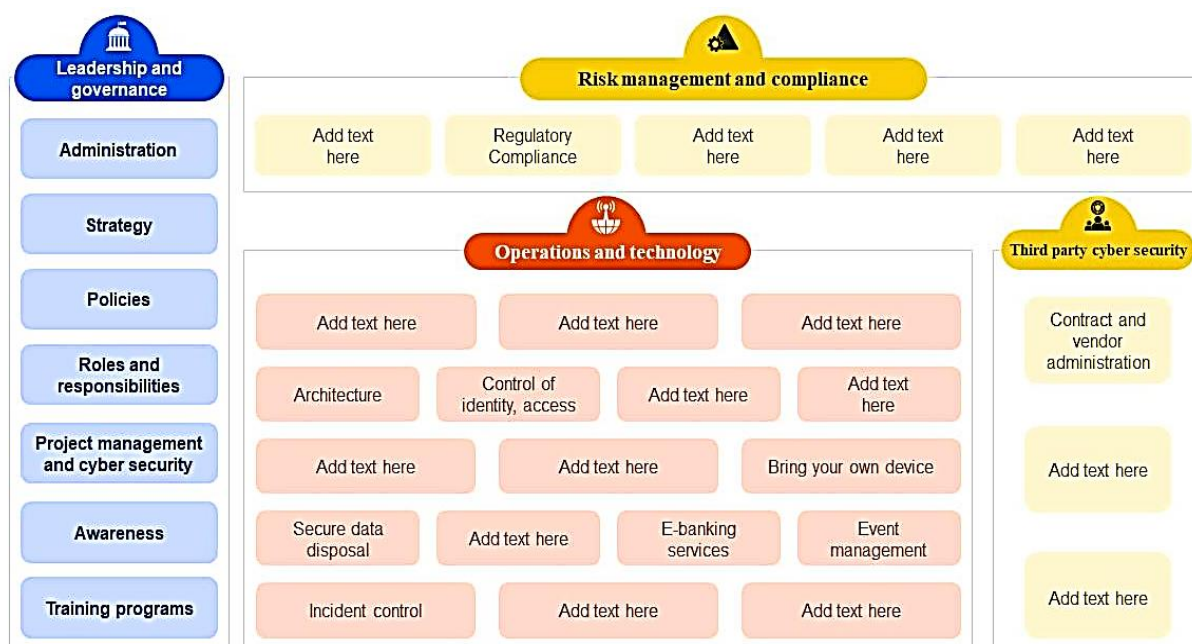


Рис. 7.16. Структурна модель інституційного механізму операційної кіберстійкості за DORA

Джерело: URL: <https://www.netacad.com/courses/cybersecurity/>

На основі цих перевірок формується інтегрований звіт про кіберстійкість (Integrated Cyber Resilience Report), який містить результати аудиту, рівень відповідності вимогам регламенту, перелік коригувальних дій і рекомендації для підвищення готовності до майбутніх викликів. Таким чином, створення інституційного механізму ICT Operational Resilience Framework за DORA не лише уніфікує підходи до управління цифровою безперервністю, але й формує культуру постійного вдосконалення кіберстійкості, що є ключовою умовою для стабільного функціонування підприємств у цифровій економіці.

У результаті впровадження DORA підприємства отримують структурований, вимірюваний і керований підхід до забезпечення цифрової безперервності, який поєднує технічні, організаційні та правові аспекти. Це дозволяє знизити рівень операційних ризиків, підвищити довіру клієнтів і

забезпечити відповідність європейським нормам кібербезпеки. Таким чином, DORA стає не лише нормативним актом, а й методологічною основою управління цифровою стійкістю, що сприяє формуванню проактивної культури кіберзахисту та стабільного функціонування комп'ютерних систем і мереж у масштабах підприємства та Європейського цифрового простору.

СПИСОК ДЖЕРЕЛ РОЗДІЛУ 7

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
6. Kostiuk, Yuliia. (2025). Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System. In book: Insider Threats and Security in Corporations. pp.205-232. <https://doi.org/10.36690/ITSC-205-232>.осно
7. Kolbasova, K and Zhurakovskiy, Bohdan and Poltorak, V and Nakonechnyi, V and Kyrychok, Roman (2023) *Smart Home Network based on Cisco Equipment* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 70-80. ISSN 1613-0073
8. Virovets, Denis and Obushnyi, Sergiy and Ramskyi, Andrii and Hulak, Hennadii (2024) *Soul Bound Token as Digital Twins in Peer-to-Peer Economic Systems* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 97-105. ISSN 1613-0073

9. Tyshyk, I. and Hulak, Hennadii (2024) *Testing an organization's information system for unauthorized access* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 17-29. ISSN 1613-0073
10. Zhebka, Serhii and Zhebka, Viktoriia and Hulak, Hennadii and Kyrychok, Roman and Platonenko, Artem (2025) *Method for Adaptive Allocation of Cryptographic Resources in Distributed Databases* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 620-628. ISSN 1613-0073
11. Dovzhenko, Nadiia & Ivanichenko, Yevhen & Skladannyi, Pavlo & Zhylytsov, Oleksii. (2024). Research of UAV and sensor network integration features for routing optimization and energy consumption reduction.
12. Zhebka, V. and Skladannyi, Pavlo and Bazak, Y and Bondarchuk, A. and Storchak, K. (2024) *Methods for Predicting Failures in a Smart Home* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 70-78. ISSN 1613-0073
13. Kriuchkova, Larysa and Tsmokanych, I. and Mazur, Nataliia and Tarasenko, D. and Osadcha, V. (2024) *Experimental determination of protective signal parameters for effective "swinging" of the carrier frequency of high-frequency imposition* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 251-259. ISSN 1613-0073
14. Kraus, N. and Kraus, K. and Shevchenko, Svitlana and Proshkin, Volodymyr (2024) *Digitalizing Production and Industry through 4.0 Technologies Implementation* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 36-47. ISSN 1613-0073
15. Kulibaba, S. and Zubyk, L. and Kurchenko, O. and Sinitsyn, I. and Mazur, Nataliia (2023) *Linked System of Data Organization and Management* Cybersecurity Providing in Information and Telecommunication Systems (3421). pp. 117-126. ISSN 1613-0073
16. Chyzhevskaya, Maryna & Романовська, Наталія & Venger, Vitalii & Sokolov, Volodymyr. (2024). Tokenomics and Perspectives of Proof of Stake.
17. Ivanichenko, Yevhen and Kozachok, Valerii and Dreis, Yurii and Nesterova, Olena and Dmytriienko, Kate (2021) *Exposing Deviations in Information Processes using Multifractal Analysis* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3187 (1). pp. 251-259. ISSN 1613-0073
18. Bilous, Vladyslav and Bodnenko, Dmitry and Lokaziuk, Oleksandra and Skladannyi, Pavlo and Abramov, Vadym (2025) *Cyber Evidence Software as the Digital Forensics Tools in the Investigation of*

Cybercrime Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 26-37. ISSN 1613-0073

19. Brzhevskaya, Zoreslava and Haidur, Halyna and Dovzhenko, Nadiia and Anosov, Andrii and Vorokhob, Maksym (2021) *Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 272-276. ISSN 1613-0073

20. Anakhov, P. and Zhebka, V. and Kravchenko, V. and Skladannyi, Pavlo and Zhylyts'ov, Oleksii (2023) *Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 269-274. ISSN 1613-0073

21. Dovzhenko, Nadiia and Barabash, Oleg and Musienko, Andrii and Ivanichenko, Yevhen and Krasheninnik, Iryna (2024) *Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism* CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine. pp. 465-470. ISSN 1613-0073

22. Obushnyi, Sergiy and Virovets, Denis and Zhytar, Maksym and Zhdanova, Yuliia (2024) *Unlocking the Economic Potential of Real Estate Tokenization in Ukraine* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 79-87. ISSN 1613-0073

23. Trofymchuk, Oleksandr and Vasyanin, Volodymyr and Sokolov, Volodymyr and Chikrii, Arkadii and Ushakova, Liudmyla (2021) *On the Use of Gray Codes for Solving 0-1 Combinatorial Problems of Optimization and Decision-Making in Environmental and Economic Systems* Information Technology and Mathematical Modeling for Environmental Safety 2021, 3021. pp. 18-28. ISSN 1613-0073

24. Tkachenko, O. and Tkachenko, K. and Tkachenko, O. and Kyrychok, Roman and Yaskevych, Vladyslav (2024) *Neural Networks in the Processing of Natural Language Texts in Information Learning Systems* Cybersecurity Providing in Information and Telecommunication Systems, 3654. pp. 73-87. ISSN 1613-0073

25. Popereshnyak, S. and Ovcharenko, V. and Novikov, Y. and Hulak, Hennadii (2024) *Detection of intrusions based on text analysis and machine learning methods in the development of information systems* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 310-318. ISSN 1613-0073

26. Tykholaz, D. and Banakh, R. and Mychuda, L. and Piskozub, A. and Kyrychok, Roman (2024) *Incident response with AWS detective*

controls Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 190-197. ISSN 1613-0073

27. Shevchenko, Svitlana & Zhdanova, Yuliia & Nehodenko, Olena & Spasiteleva, Svitlana & Nehodenko, Vitalii. (2025). Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems

28. Avdeyenko, Gleb and Narytnyk, Teodor and Saiko, Volodymyr and Kriuchkova, Larysa and Tsmokanych, Ivan (2025) *Terahertz Range Transceiver Module for Electromagnetic Protection of Objects* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 603-610. ISSN 1613-0073

29. Hulak, H., et al. (2020). Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses. Cybersecurity: Education, Science, Technique, 2(10), 6–28. <https://doi.org/10.28925/2663-4023.2020.10.628>

30. Шевченко, С., Жданова, Ю., & Гаркушенко, А. (2025). Когнітивний підхід в інформаційній та кібербезпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 854–866. <https://doi.org/10.28925/2663-4023.2025.29.945>

31. Чернігівський, І., & Крючкова, Л. (2025). Тестування нейромережових моделей для вирішення задачі виявлення заражених ПК на базі цифрових слідів. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 800–817. <https://doi.org/10.28925/2663-4023.2025.29.941>

32. Романюк , В., & Платоненко, А. (2025). Аналіз якості генераторів рожевого шуму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 789–799. <https://doi.org/10.28925/2663-4023.2025.29.940>

33. Соболенко , І., & Платоненко, А. (2025). Автоматизоване виявлення аномалій у трафіку корпоративних бездротових мереж за допомогою Python: методи, реалізація та оцінка ефективності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 777–788. <https://doi.org/10.28925/2663-4023.2025.29.939>

34. Соколов, В. (2025). Технологія відслідковування переміщення абонентів територією підприємства критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 207–222. <https://doi.org/10.28925/2663-4023.2025.29.920>

35. Складанний, П., Гулак, Г., & Корнієць, В. (2025). Коаліційний підхід до управління кібербезпекою інформаційних систем що

застосовують хмарні технології. Кібербезпека: освіта, наука, техніка, 4(28), 8–25. <https://doi.org/10.28925/2663-4023.2025.27.825>

36. Довженко, Н., Іваніченко, Є., Аушева, Н., Шевчук, Ю., & Луковський, Т. (2025). Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. Кібербезпека: освіта, наука, техніка, 4(28), 547–564. <https://doi.org/10.28925/2663-4023.2025.28.835>

37. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для студентів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 70 с.

38. Шевченко, С., Жданова, Ю., Складанний, П., & Іщук, М. (2025). Створення блокчейн-платформи для електронного голосування. Кібербезпека: освіта, наука, техніка, 4(28), 701–714. <https://doi.org/10.28925/2663-4023.2025.28.860>

39. Крючкова, Л., & Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка, 4(28), 766–780. <https://doi.org/10.28925/2663-4023.2025.28.863>

40. Цехмейстер, Р., Платоненко, А., Ворохоб, М., Черевик, В., & Семеняка, С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. Кібербезпека: освіта, наука, техніка, 3(27), 63–71. <https://doi.org/10.28925/2663-4023.2025.27.703>

41. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebashko, B., & Khorolska, K. Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, (CPITS-II 2024) October 26, 2024. Aachen: CEUR, 2024. Vol. 3826. P. 129–138. ISSN: 1613-0073.

42. Олійник, Я., Платоненко, А., Черевик, В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. <https://doi.org/10.28925/2663-4023.2025.27.705>

43. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей Курамото ДЛЯ ідентифікації дезінформації у соціальних мережах. Кібербезпека: освіта, наука, техніка, 3(27), 406–416. <https://doi.org/10.28925/2663-4023.2025.27.754>

44. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebashko, B., Sokolov, V. A system for assessing the interdependencies of

information system agents in information security risk management using cognitive maps. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 249-264. ISSN 1613-0073.

45. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» для студентів спеціальності 123 Комп'ютерна інженерія, освітньої програми 123.00.01 Комп'ютерна інженерія / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 82 с.

46. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., Korshun, N. Models and algorithms for analyzing information risks during the security audit of personal data information system. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 155-171. ISSN 1613-0073.

47. Довженко, Н., Складанний, П., Іваніченко, Є., & Жильцов, О. (2025). Модель динамічної взаємодії безпілотних літальних апаратів із сенсорною мережею для енергоефективного моніторингу. *Кібербезпека: освіта, наука, техніка*, 3(27), 466–478. <https://doi.org/10.28925/2663-4023.2025.27.766>

48. Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevska Z. Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 14-25. ISSN 1613-0073.

49. Гайдук, О., Зверев, В., & Гулак, Г. (2025). Кореляційний аналіз типів кіберінцидентів в контексті інформаційних технологій міжнародних комунікацій. *Кібербезпека: освіта, наука, техніка*, 3(27), 417–428. <https://doi.org/10.28925/2663-4023.2025.27.757>

50. Kostiuk Y., Skladannyi P., Sokolov V., Zhyltsov O., Ivanichenko Y. Effectiveness of Information Security Control using Audit Logs. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 524-538. ISSN 1613-0073.

51. Kostiuk Y., Skladannyi, P., Sokolov, V., Vorokhob, M. Models and technologies of cognitive agents for decision-making with integration of Artificial Intelligence. Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025). Aachen: CEUR, 2025. Vol. 4005. P. 82–96. ISSN 1613-0073.

52. Чернігівський, І., & Крючкова, Л. (2025). Системний підхід до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів. *Кібербезпека: освіта, наука, техніка*, 3(27), 572–590. <https://doi.org/10.28925/2663-4023.2025.27.781>
53. Skladannyi P., Kostiuk Y., Rzaieva S., Bebeshko, B., Korshun, N. Adaptive Methods for Embedding Digital Watermarks to Protect Audio and Video Images in Information and Communication Systems. *Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography*, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 13–31. ISSN 1613-0073.
54. Чернігівський, І., & Крючкова, Л. (2025). Ефективні рішення для швидкого виявлення скомпрометованих ПК в інфокомунікаційних мережах. *Телекомунікаційні та інформаційні технології*, 2(87), 24–32. <https://doi.org/10.31673/2412-4338.2025.029875>
55. Kostiuk Y., Skladannyi, P., Khorolska, K., Sokolov, V., Hulak, H. Application of Statistical and Neural Network Algorithms in Steganographic Synthesis and Analysis of Hidden Information in Audio and Graphic Files. *Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography*, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 45–65. ISSN 1613-0073.
56. Чернігівський, І., & Крючкова, Л. (2024). Тестування антивірусних рішень для корпоративного сегменту. *Безпека інформації*, 30(3), 407–413. <https://doi.org/10.18372/2225-5036.30.20362>
57. Skladannyi, P., Kostiuk Y., Khorolska, K., Bebeshko, B., Sokolov, V. Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. *Proceedings of the Workshop Cyber Security and Data Protection*, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 17–36. ISSN 1613-0073.
58. Соколов, В. (2025). Забезпечення стійкості безпроводових систем до атак глушіння. *Телекомунікаційні та інформаційні технології*, 1(86), 50–60. <https://doi.org/10.31673/2412-4338.2025.013623>
59. Kostiuk, Y., Rzaieva S., Khorolska, K., Mazur, N., Korshun, N. Architecture of the software system of confidential access to information resources of computer networks. *Proceedings of the Workshop Cyber Security and Data Protection*, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 37–53. ISSN 1613-0073.
60. Корнієць, В., & Складаний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. *Телекомунікаційні та інформаційні технології*, 4(85), 90–96. <https://doi.org/10.31673/2412-4338.2024.040224>

61. Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S.(2025) Intelligent System for Simulation Modeling and Research of Information Objects. Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025), May 13–14, 2025, Kyiv, Ukraine, Vol-4053, P. 237-251. ISSN 1613-0073.

62. Агашков, А., Шевченко, С., Бондарчук, А., & Жебка, В. (2024). Шляхи підвищення транспортних операцій за допомогою хмарних логістичних рішень. Телекомунікаційні та інформаційні технології, 4(85), 4–15. <https://doi.org/10.31673/2412-4338.2024.047191>

63. Sokolov, V., Kostiuk, Y., Skladannyi, P., Korshun, N. (2025). Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements. Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies", ICST 2025, Vol-4048, P. 397 - 411. ISSN 1613-0073.

64. Бондарчук, А., Складанний, П., Жебка, В., & Стражніков, А. (2024). Оптимізація системи зарядки електромобілів на основі методів дослідження операцій. Телекомунікаційні та інформаційні технології, 3(84), 86–93. <https://doi.org/10.31673/2412-4338.2024.038693>

65. Крючкова, Л., Башкевич, Є., & Куцибала, М. (2024). Програмна реалізація алгоритмів виокремлення контурів зображень об'єктів в інтелектуальних системах відеоспостереження. Телекомунікаційні та інформаційні технології, 2(83), 14–29. <https://doi.org/10.31673/2412-4338.2024.022439>

66. Оксанич, І., Гречанінов, В., Литвинов, В., & Складанний П. (2024). Особливості забезпечення гарантоздатності та кіберстійкості інформаційного обміну в складних умовах. Телекомунікаційні та інформаційні технології, 2(83), 105–113. <https://doi.org/10.31673/2412-4338.2024.022128>

67. Крючкова, Л., Яремчук, Д., & Пазинін, А. (2024). Планування навантаження контейнерів за допомогою лінійного програмування. Телекомунікаційні та інформаційні технології, 2(83), 114 –119. <https://doi.org/10.31673/2412-4338.2024.022935>

68. Цирканюк, Д., & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. Кібербезпека: освіта, наука, техніка, 2(26), 140–154. <https://doi.org/10.28925/2663-4023.2024.26.675>

69. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка, 2(26), 374–391. <https://doi.org/10.28925/2663-4023.2024.26.699>

70. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. *Кібербезпека: освіта, наука, техніка*, 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>
71. Корнієць, В., & Жданова, Ю. (2024). Методика формування швидкісного імітостійкого шифру багато алфавітної заміни. *Кібербезпека: освіта, наука, техніка*, 2(26), 476–486. <https://doi.org/10.28925/2663-4023.2024.26.723>
72. Руда, Х., Сабодашко, Д., Микитин, Г., Швед, М., Бордуляк, С., & Коршун, Н. (2024). Порівняння методів цифрової обробки сигналів та моделей глибинного навчання у голосовій аутентифікації. *Кібербезпека: освіта, наука, техніка*, 1(25), 140–160. <https://doi.org/10.28925/2663-4023.2024.25.140160>
73. Жданова, Ю., Шевченко, С., Спасітелєва, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 330–343. <https://doi.org/10.28925/2663-4023.2024.25.330343>
74. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. *Кібербезпека: освіта, наука, техніка*, 1(25), 390–400. <https://doi.org/10.28925/2663-4023.2024.25.390400>
75. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 468–486. <https://doi.org/10.28925/2663-4023.2024.25.468486>
76. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. *Кібербезпека: освіта, наука, техніка*, 4(24), 185–195. <https://doi.org/10.28925/2663-4023.2024.24.185195>
77. Крючкова, Л., & Леонтюк, Н. (2024). Програмно-апаратна реалізація алгоритму швидкої оцінки потужності Wi-Fi сигналу в точках простору урбанізованого приміщення. *Кібербезпека: освіта, наука, техніка*, 4(24), 241–256. <https://doi.org/10.28925/2663-4023.2024.24.241256>
78. Крючкова, Л., & Дяків, В. (2024). Програмна реалізація розрахунку просторового розподілу поля рамок антен. *Кібербезпека: освіта, наука, техніка*, 4(24), 312–320. <https://doi.org/10.28925/2663-4023.2024.24.312320>
79. Іосіфов, Є., & Соколов, В. (2024). Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. *Кібербезпека: освіта,*

наука, техніка, 4(24), 398–414. <https://doi.org/10.28925/2663-4023.2024.24.398414>

80. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 3(23), 258–273. <https://doi.org/10.28925/2663-4023.2024.23.258273>

81. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. *Кібербезпека: освіта, наука, техніка*, 3(23), 318–327. <https://doi.org/10.28925/2663-4023.2024.23.318327>

82. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. *Кібербезпека: освіта, наука, техніка*, 3(23), 338–347. <https://doi.org/10.28925/2663-4023.2024.23.338347>

83. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка*, 2(22), 6–18. <https://doi.org/10.28925/2663-4023.2023.22.618>

84. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. *Кібербезпека: освіта, наука, техніка*, 2(22), 68–83. <https://doi.org/10.28925/2663-4023.2023.22.6883>

КОНТРОЛЬНІ ПИТАННЯ

1. Які основні етапи розроблення плану безперервності бізнес-процесів (BCP)?
2. У чому полягає відмінність між планом BCP і планом DRP?
3. Які ключові показники використовуються для оцінки ефективності відновлення систем після інцидентів (RTO, RPO, MTTR)?
4. Як здійснюється аналіз впливу на бізнес (Business Impact Analysis, BIA) у процесі побудови системи безперервності?
5. Які типові загрози враховуються при плануванні DRP у комп'ютерних мережах?
6. У чому полягає різниця між повним, інкрементним і диференційним резервним копіюванням?
7. Які принципи формування політики резервного копіювання даних в інформаційній системі?
8. Як обирається оптимальний носій для збереження резервних копій (локальний, мережевий, хмарний)?

9. Які технології забезпечують цілісність і конфіденційність резервних копій (шифрування, контрольні суми, цифровий підпис)?
10. Як організовується перевірка достовірності та відновлюваності резервних копій?
11. У чому полягають переваги використання гібридної хмарної інфраструктури для забезпечення безперервності бізнесу?
12. Які технології забезпечують автоматичне масштабування й балансування навантажень у хмарних системах?
13. Як здійснюється захист даних при передачі між локальними ресурсами та хмарними середовищами?
14. Яку роль відіграють контейнери та оркестратори (Docker, Kubernetes) у забезпеченні цифрової стійкості?
15. Які ризики супроводжують використання публічних хмар у контексті інформаційної безпеки підприємства?
16. Які функції виконують системи симуляції інцидентів (Incident Simulation Platforms) у тестуванні DRP?
17. Як автоматизовані інструменти (наприклад, Chaos Monkey, Gremlin) сприяють оцінці стійкості IT-інфраструктури?
18. Які параметри відстежуються під час моніторингу ефективності планів DRP (SLA, KPI, RTO, RPO)?
19. Яким чином результати автоматизованих тестів використовуються для вдосконалення політики BCP/DRP?
20. Які основні вимоги Регламенту DORA до управління цифровою операційною стійкістю підприємства?

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Костюк Ю.В., Складанний П.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л., Ворохоб М.В. (2025) Безпека інформаційно-комунікаційних систем. Київський університет імені Бориса Грінченка, Україна, Київ. - 1017 с.
2. Костюк Ю.В., Складанний П.М., Гулак Г.М., Бебешко Б.Т., Хорольська К.В., Рзаєва С.Л. (2025) Системи захисту інформації. Київський університет імені Бориса Грінченка, Україна, Київ. - 886с.
3. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
5. Гулак Г. М., Жильцов О. Б., Киричок Р. В., Коршун Н. В., Складанний П. М. Інформаційна та кібернетична безпека підприємства : підруч. / Г. М. Гулак, О. Б. Жильцов, Р. В. Киричок, Н. В. Коршун, П. М. Складанний – Львів : Видавець Марченко Т. В., 2023. – 370 с.
6. Шевченко, С., Жданова, Ю., & Гаркушенко, А. (2025). Когнітивний підхід в інформаційній та кібербезпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 854–866. <https://doi.org/10.28925/2663-4023.2025.29.945>
7. Основи баз даних : навчальний посібник / Рзаєва С.Л., Машкіна І.В., Складанний П.М., Костюк Ю.В., Рзаєв Д.О., Красюк Ю.М – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 319 с.
8. Чернігівський, І., & Крючкова, Л. (2025). Тестування нейромережових моделей для вирішення задачі виявлення заражених ПК на базі цифрових слідів. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 800–817. <https://doi.org/10.28925/2663-4023.2025.29.941>
9. Романюк , В., & Платоненко, А. (2025). Аналіз якості генераторів рожевого шуму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 789–799. <https://doi.org/10.28925/2663-4023.2025.29.940>
10. Соболенко , І., & Платоненко, А. (2025). Автоматизоване виявлення аномалій у трафіку корпоративних бездротових мереж за допомогою Python: методи, реалізація та оцінка ефективності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 777–788. <https://doi.org/10.28925/2663-4023.2025.29.939>

11. Соколов, В. (2025). Технологія відслідковування переміщення абонентів територією підприємства критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 207–222. <https://doi.org/10.28925/2663-4023.2025.29.920>
12. Складанний, П., Гулак, Г., & Корнієць, В. (2025). Коаліційний підхід до управління кібербезпекою інформаційних систем що застосовують хмарні технології. Кібербезпека: освіта, наука, техніка, 4(28), 8–25. <https://doi.org/10.28925/2663-4023.2025.27.825>
13. Довженко, Н., Іваніченко, Є., Аушева, Н., Шевчук, Ю., & Луковський, Т. (2025). Дослідження архітектури дата-центрів з інтеграцією IoT-компонентів для забезпечення енергоефективності та кіберстійкості. Кібербезпека: освіта, наука, техніка, 4(28), 547–564. <https://doi.org/10.28925/2663-4023.2025.28.835>
14. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в інформаційно-комунікаційних системах» для студентів спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 70 с.
15. Шевченко, С., Жданова, Ю., Складанний, П., & Іщук, М. (2025). Створення блокчейн-платформи для електронного голосування. Кібербезпека: освіта, наука, техніка, 4(28), 701–714. <https://doi.org/10.28925/2663-4023.2025.28.860>
16. Крючкова, Л., & Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка, 4(28), 766–780. <https://doi.org/10.28925/2663-4023.2025.28.863>
17. Цехмейстер, Р., Платоненко, А., Ворохоб, М., Черевик, В., & Семеняка, С. (2025). Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі. Кібербезпека: освіта, наука, техніка, 3(27), 63–71. <https://doi.org/10.28925/2663-4023.2025.27.703>
18. Kostiuk, Y., Skladannyi, P., Korshun, N., Bebashko, B., & Khorolska, K. Integrated protection strategies and adaptive resource distribution for secure video streaming over a Bluetooth network. Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, (CPITS-II 2024) October 26, 2024. Aachen: CEUR, 2024. Vol. 3826. P. 129–138. ISSN: 1613-0073.
19. Олійник, Я., Платоненко, А., Черевик, В., Ворохоб, М., & Шевчук, Ю. (2025). Методи захисту інформації в технологіях IoT. Кібербезпека: освіта, наука, техніка, 3(27), 100–108. <https://doi.org/10.28925/2663-4023.2025.27.705>

20. Дмитрієнко, К., & Коршун, Н. (2025). Застосування вдосконалених моделей Курамото ДЛЯ ідентифікації дезінформації у соціальних мережах. *Кібербезпека: освіта, наука, техніка*, 3(27), 406–416. <https://doi.org/10.28925/2663-4023.2025.27.754>
21. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebashko, B., Sokolov, V. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 249-264. ISSN 1613-0073.
22. Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» для студентів спеціальності 123 Комп'ютерна інженерія, освітньої програми 123.00.01 Комп'ютерна інженерія / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 82 с.
23. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., Korshun, N. Models and algorithms for analyzing information risks during the security audit of personal data information system. Workshop on Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, (CH&CMiGIN'24) January 24–27, 2024. Aachen: CEUR, 2024. Vol. 3925. P. 155-171. ISSN 1613-0073.
24. Довженко, Н., Складанний, П., Іваніченко, Є., & Жильцов, О. (2025). Модель динамічної взаємодії безпілотних літальних апаратів із сенсорною мережею для енергоефективного моніторингу. *Кібербезпека: освіта, наука, техніка*, 3(27), 466–478. <https://doi.org/10.28925/2663-4023.2025.27.766>
25. Mashkina I., Rzaieva S., Kostiuk Y., Mazur N., Brzhevskaya Z. Cybersecurity in Intelligent Transport Systems: Current Challenges and Solutions. Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 14-25. ISSN 1613-0073.
26. Гайдук, О., Зверев, В., & Гулак, Г. (2025). Кореляційний аналіз типів кіберінцидентів в контексті інформаційних технологій міжнародних комунікацій. *Кібербезпека: освіта, наука, техніка*, 3(27), 417–428. <https://doi.org/10.28925/2663-4023.2025.27.757>
27. Kostiuk Y., Skladannyi P., Sokolov V., Zhyltsov O., Ivanichenko Y. Effectiveness of Information Security Control using Audit Logs. Proceedings of the Workshop on Cybersecurity Providing in Information and

Telecommunication Systems (CPITS 2025), 2025. Aachen: CEUR, 2025. Vol. 3991. P. 524-538. ISSN 1613-0073.

28. Kostiuk Y., Skladannyi, P., Sokolov, V., Vorokhob, M. Models and technologies of cognitive agents for decision-making with integration of Artificial Intelligence. Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025). Aachen: CEUR, 2025. Vol. 4005. P. 82–96. ISSN 1613-0073.

29. Чернігівський, І., & Крючкова, Л. (2025). Системний підхід до вирішення задачі захисту інформації в інфокомунікаційній мережі від впливу комп'ютерних вірусів. Кібербезпека: освіта, наука, техніка, 3(27), 572–590. <https://doi.org/10.28925/2663-4023.2025.27.781>

30. Skladannyi P., Kostiuk Y., Rzaieva S., Bebeshko, B., Korshun, N. Adaptive Methods for Embedding Digital Watermarks to Protect Audio and Video Images in Information and Communication Systems. Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 13–31. ISSN 1613-0073.

31. Чернігівський, І., & Крючкова, Л. (2025). Ефективні рішення для швидкого виявлення скомпрометованих ПК в інфокомунікаційних мережах. Телекомунікаційні та інформаційні технології, 2(87), 24–32. <https://doi.org/10.31673/2412-4338.2025.029875>

32. Kostiuk Y., Skladannyi, P., Khorolska, K., Sokolov, V., Hulak, H. Application of Statistical and Neural Network Algorithms in Steganographic Synthesis and Analysis of Hidden Information in Audio and Graphic Files. Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography, August 5, 2025, Kyiv, Ukraine (CQPC 2025). Vol. 4016. P. 45–65. ISSN 1613-0073.

33. Чернігівський, І., & Крючкова, Л. (2024). Тестування антивірусних рішень для корпоративного сегменту. Безпека інформації, 30(3), 407–413. <https://doi.org/10.18372/2225-5036.30.20362>

34. Skladannyi, P., Kostiuk Y., Khorolska, K., Bebeshko, B., Sokolov, V. Model and methodology for the formation of adaptive security profiles for the protection of wireless networks in the face of dynamic cyber threats. Proceedings of the Workshop Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 17–36. ISSN 1613-0073.

35. Соколов, В. (2025). Забезпечення стійкості безпроводових систем до атак глушіння. Телекомунікаційні та інформаційні технології, 1(86), 50–60. <https://doi.org/10.31673/2412-4338.2025.013623>

36. Kostiuk, Y., Rzaieva S., Khorolska, K., Mazur, N., Korshun, N. Architecture of the software system of confidential access to information resources of computer networks. Proceedings of the Workshop Cyber Security

and Data Protection, July 31, 2025, Lviv, Ukraine (CSDP 2025). Vol. 4042. P. 37–53. ISSN 1613-0073.

37. Корнієць, В., & Складанний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. Телекомунікаційні та інформаційні технології, 4(85), 90–96. <https://doi.org/10.31673/2412-4338.2024.040224>

38. Kostiuk, Y., Skladannyi, P., Sokolov, V., Rzaieva S.(2025) Intelligent System for Simulation Modeling and Research of Information Objects. Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025), May 13–14, 2025, Kyiv, Ukraine, Vol-4053, P. 237-251. ISSN 1613-0073.

39. Агашков, А., Шевченко, С., Бондарчук, А., & Жебка, В. (2024). Шляхи підвищення транспортних операцій за допомогою хмарних логістичних рішень. Телекомунікаційні та інформаційні технології, 4(85), 4–15. <https://doi.org/10.31673/2412-4338.2024.047191>

40. Sokolov, V., Kostiuk, Y., Skladannyi, P., Korshun, N. (2025). Adaptation of Network Traffic Routing Policy to Information Security and Network Protection Requirements. Proceedings of the 13th International Scientific and Practical Conference "Information Control Systems and Technologies", ICST 2025, Vol-4048, P. 397 - 411. ISSN 1613-0073.

41. Бондарчук, А., Складанний, П., Жебка, В., & Стражніков, А. (2024). Оптимізація системи зарядки електромобілів на основі методів дослідження операцій. Телекомунікаційні та інформаційні технології, 3(84), 86–93. <https://doi.org/10.31673/2412-4338.2024.038693>

42. Крючкова, Л., Башкевич, Є., & Куцибала, М. (2024). Програмна реалізація алгоритмів виокремлення контурів зображень об'єктів в інтелектуальних системах відеоспостереження. Телекомунікаційні та інформаційні технології, 2(83), 14–29. <https://doi.org/10.31673/2412-4338.2024.022439>

43. Оксанич, І., Гречанінов, В., Литвинов, В., & Складанний П. (2024). Особливості забезпечення гарантоздатності та кіберстійкості інформаційного обміну в складних умовах. Телекомунікаційні та інформаційні технології, 2(83), 105–113. <https://doi.org/10.31673/2412-4338.2024.022128>

44. Крючкова, Л., Яремчук, Д., & Пазинін, А. (2024). Планування навантаження контейнерів за допомогою лінійного програмування. Телекомунікаційні та інформаційні технології, 2(83), 114 –119. <https://doi.org/10.31673/2412-4338.2024.022935>

45. Цирканюк, Д., & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 2(26), 140–154. <https://doi.org/10.28925/2663-4023.2024.26.675>
46. Козачок, В., & Драпатий, М. (2024). Аналіз технології розслідування інцидентів безпеки на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 2(26), 374–391. <https://doi.org/10.28925/2663-4023.2024.26.699>
47. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. *Кібербезпека: освіта, наука, техніка*, 2(26), 417–429. <https://doi.org/10.28925/2663-4023.2024.26.707>
48. Корнієць, В., & Жданова, Ю. (2024). Методика формування швидкісного імітостійкого шифру багато алфавітної заміни. *Кібербезпека: освіта, наука, техніка*, 2(26), 476–486. <https://doi.org/10.28925/2663-4023.2024.26.723>
49. Руда, Х., Сабодашко, Д., Микитин, Г., Швед, М., Бордуляк, С., & Коршун, Н. (2024). Порівняння методів цифрової обробки сигналів та моделей глибинного навчання у голосовій аутентифікації. *Кібербезпека: освіта, наука, техніка*, 1(25), 140–160. <https://doi.org/10.28925/2663-4023.2024.25.140160>
50. Жданова, Ю., Шевченко, С., Спасітелева, С., & Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 330–343. <https://doi.org/10.28925/2663-4023.2024.25.330343>
51. Довженко, Н., Іваніченко, Є., Складанний, П., & Аушева, Н. (2024). Інтеграція безпеки та відмовостійкості сенсорних мереж на основі аналізу енергоспоживання та трафіку. *Кібербезпека: освіта, наука, техніка*, 1(25), 390–400. <https://doi.org/10.28925/2663-4023.2024.25.390400>
52. Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 468–486. <https://doi.org/10.28925/2663-4023.2024.25.468486>
53. Барабаш, О., Аушева, Н., Складанний, П., Іваніченко, Є., & Довженко, Н. (2024). Технічні аспекти побудови відмовостійкої інфраструктури сенсорної мережі. *Кібербезпека: освіта, наука, техніка*, 4(24), 185–195. <https://doi.org/10.28925/2663-4023.2024.24.185195>
54. Крючкова, Л., & Леонтюк, Н. (2024). Програмно-апаратна реалізація алгоритму швидкої оцінки потужності Wi-Fi сигналу в точках простору урбанізованого приміщення. *Кібербезпека: освіта, наука, техніка*, 4(24), 241–256. <https://doi.org/10.28925/2663-4023.2024.24.241256>

55. Крючкова, Л., & Дяків, В. (2024). Програмна реалізація розрахунку просторового розподілу поля рамкових антен. *Кібербезпека: освіта, наука, техніка*, 4(24), 312–320. <https://doi.org/10.28925/2663-4023.2024.24.312320>
56. Іосіфов, Є., & Соколов, В. (2024). Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. *Кібербезпека: освіта, наука, техніка*, 4(24), 398–414. <https://doi.org/10.28925/2663-4023.2024.24.398414>
57. Шевченко, С., Жданова, Ю., Спасітелева, С., Мазур, Н., Складанний, П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 3(23), 258–273. <https://doi.org/10.28925/2663-4023.2024.23.258273>
58. Крючкова, Л., & Ємельяненко, М. (2024). Захист web-ресурсу intranet від зовнішніх і внутрішніх загроз. *Кібербезпека: освіта, наука, техніка*, 3(23), 318–327. <https://doi.org/10.28925/2663-4023.2024.23.318327>
59. Крючкова, Л., & Стеблина, О. (2024). Захист смартфонів від впливу шкідливих програм в процесі зарядки у громадських місцях. *Кібербезпека: освіта, наука, техніка*, 3(23), 338–347. <https://doi.org/10.28925/2663-4023.2024.23.338347>
60. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка*, 2(22), 6–18. <https://doi.org/10.28925/2663-4023.2023.22.618>
61. Кіпчук, Ф., & Соколов, В. (2023). Модель розрахунку витрат на баг-баунті програми тестування вразливостей безпеки. *Кібербезпека: освіта, наука, техніка*, 2(22), 68–83. <https://doi.org/10.28925/2663-4023.2023.22.6883>
62. Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Брже夫ська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. *Кібербезпека: освіта, наука, техніка*, 2(22), 148–155. <https://doi.org/10.28925/2663-4023.2023.22.148155>
63. Машталяр, Я., Козачок, В., Брже夫ська, З., Богданов, О., Оксанич, І., & Литвинов, В. (2023). Дослідження розвитку та інновації кіберзахисту на об'єктах критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, 2(22), 156–167. <https://doi.org/10.28925/2663-4023.2023.22.156167>
64. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 2(22), 168–178. <https://doi.org/10.28925/2663-4023.2023.22.168178>

65. Соколов, В., & Складанний, П. (2023). Методика оцінки комплексних збитків від інциденту інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(21), 99–120. <https://doi.org/10.28925/2663-4023.2023.21.99120>
66. Спасітелева, С., Чичкань, І., Шевченко, С., & Жданова, Ю. (2023). Розробка безпечних контейнерних застосунків з мікросервісною архітектурою. *Кібербезпека: освіта, наука, техніка*, 1(21), 193–210. <https://doi.org/10.28925/2663-4023.2023.21.193210>
67. Костюк Ю., Бебешко Б., Складанний П., Рзаєва С., Хорольська К. Оптимізація буфера та пріоритетів для забезпечення безпеки У Bluetooth-мережах. *Безпека інформаційних систем і технологій*. 2025. 2(8), 5-16.
68. Ворохоб, М., Киричок, Р., Яскевич, В., Добришин, Ю., & Сидоренко, С. (2023). Сучасні перспективи застосування концепції zero trust при побудові політики інформаційної безпеки підприємства. *Кібербезпека: освіта, наука, техніка*, 1(21), 223–233. <https://doi.org/10.28925/2663-4023.2023.21.223233>
69. Добришин, Ю., Сидоренко, С., & Ворохоб, М. (2023). Автоматизована система підтримки прийняття рішення щодо відновлення пошкодженого програмного забезпечення внаслідок впливу кібератак. *Кібербезпека: освіта, наука, техніка*, 4(20), 174–182. <https://doi.org/10.28925/2663-4023.2023.20.174182>
70. Соколов, В., & Складанний, П. (2023). Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». *Кібербезпека: освіта, наука, техніка*, 4(20), 183–204. <https://doi.org/10.28925/2663-4023.2023.20.183204>
71. Shevchenko, S., Zhdanova, Y., & Spasiteleva, S. (2023). Mathematical methods in cybersecurity: Catastrophe theory. *Cybersecurity: Education, Science, Technique*, 3(19), 165–175. <https://doi.org/10.28925/2663-4023.2023.19.165175>
72. Sokolov, V. (2022). Approaches to the formation of scientific thinking in cybersecurity high school students. *Cybersecurity: Education, Science, Technique*, 2(18), 124–137. <https://doi.org/10.28925/2663-4023.2022.18.124137>
73. Shevchenko, S., Skladannyi, P., Nehodenko, O., & Nehodenko, V. (2022). Study of applied aspects of conflict theory in security systems. *Cybersecurity: Education, Science, Technique*, 2(18), 150–162. <https://doi.org/10.28925/2663-4023.2022.18.150162>
74. Sukaylo, I., & Korshun, N. (2022). The influence of NLU and generative AI on the development of cyber defense systems. *Cybersecurity:*

Education, Science, Technique, 2(18), 187–196. <https://doi.org/10.28925/2663-4023.2022.18.187196>

75. Костюк Ю., Бебешко Б., Гулак Г., Складанний П., Рзаєва С., Хорольська К. (2024) Забезпечення кібербезпеки та швидкодії передачі даних у безпроводних мережах. Безпека інформації, т. 30, №3, 365-375.

76. Hulak, H., Zhdanova, Y., Skladannyi, P., Hulak, Y., & Korniiets, V. (2022). Vulnerabilities of short message encryption in mobile information and communication systems of critical infrastructure objects. *Cybersecurity: Education, Science, Technique*, 1(17), 145–158. <https://doi.org/10.28925/2663-4023.2022.17.145158>

77. Romaniuk, O., Skladannyi, P., & Shevchenko, S. (2022). Comparative analysis of solutions to provide control and management of privileged access in the IT environment. *Cybersecurity: Education, Science, Technique*, 4(16), 98–112. <https://doi.org/10.28925/2663-4023.2022.16.98112>

78. Borkivska, O., Zhurakovskiy, B., & Platonenko, A. (2022). Smart city information system based on LoRa technology. *Cybersecurity: Education, Science, Technique*, 4(16), 113–128. <https://doi.org/10.28925/2663-4023.2022.16.113128>

79. Brzhevska, Z., Kyrychok, R., Platonenko, A., & Hulak, H. (2022). Assessment of the preconditions of formation of the methodology of assessment of information reliability. *Cybersecurity: Education, Science, Technique*, 3(15), 164–174. <https://doi.org/10.28925/2663-4023.2022.15.164174>

80. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Boiko, S. (2022). Insiders and insider information: Essence, threats, activities and legal responsibility. *Cybersecurity: Education, Science, Technique*, 3(15), 175–185. <https://doi.org/10.28925/2663-4023.2022.15.175185>

81. Довженко, Н., Мазур, Н., Костюк, Ю., Рзаєва, С. Інтеграція ІОТ ТА штучного інтелекту в інтелектуальні транспортні системи. Кібербезпека: освіта, наука, техніка. 2024. 2(26), 430–444.

82. Bogachuk, V. Sokolov and V. Buriachok, "Monitoring Subsystem for Wireless Systems Based on Miniature Spectrum Analyzers," *2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2018, pp. 581-585, doi: 10.1109/INFOCOMMST.2018.8632151.

83. Hulak, Hennadii and Skladannyi, Pavlo and Sokolov, Volodymyr and Hulak, E. and Korniiets, V. (2022) *Dynamic model of guarantee capacity and cyber security management in the critical automated systems* 2nd International Conference on Conflict Management in Global Information Networks (CMiGiN 2022), 3530. pp. 102-111. ISSN 1613-0073

84. Sokolov, V. Y. and Skladannyi, Pavlo and Hulak, Hennadii (2022) *Stability Verification of Self-Organized Wireless Networks with Block Encryption* Cybersecurity Providing in Information and Telecommunication Systems, 3137. pp. 227-237. ISSN 1613-0073
85. Anakhov, P. and Zhebka, V. and Popereshnyak, S and Skladannyi, Pavlo and Sokolov, Volodymyr (2023) *Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 240-245. ISSN 1613-0073
86. Костюк Ю., Довженко, Н., Мазур, Н., Складанний, П., Рзаєва, С. Методика захисту GRID-середовища від шкідливого коду під час виконання обчислювальних завдань. Кібербезпека: освіта, наука, техніка. 2025. 3(27), 22–40.
87. Kipchuk, F. and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii and Ageyev, D. (2023) *Method for Increasing the Various Sources Data Consistency for IoT Sensors* IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PICST). pp. 522-526. ISSN 979-8-3503-9891-5
88. A. Carlsson, D. Ageyev, Y. Sadykov and V. Sokolov, "Sustainability Research of the Secure Wireless Communication System with Channel Reservation," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 973-977, doi: 10.1109/TCSET49122.2020.235583.
89. Складанний, П., Костюк Ю., Рзаєва, С., Самойленко, Ю., Савченко, Т. Розробка модульних нейронних мереж для виявлення різних класів мережевих атак. Кібербезпека: освіта, наука, техніка. 2025. 3(27), 534–548.
90. F. Kipchuk, V. Sokolov, V. Buriachok and L. Kuzmenko, "Investigation of Availability of Wireless Access Points based on Embedded Systems," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-5, doi: 10.1109/PICST47496.2019.9061551.
91. Shevchuk, D and Harasymchuk, O and Partyka, A and Korshun, Natalia (2023) *Designing Secured Services for Authentication, Authorization, and Accounting of Users* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 207-225. ISSN 1613-0073
92. Складанний П.М., Костюк Ю.В., Мазур Н.П., Пітайчук М.А. Дослідження характеристик та продуктивності протоколів доступу до

хмарних обчислювальних середовищ на основі універсального тестування. Телекомунікаційні та інформаційні технології. 2025. №1(86). С. 61-74.

93. Kuzminykh, I., Ghita, B., Sokolov, V., & Bakhshi, T. (2021). Information Security Risk Assessment. *Encyclopedia*, 1(3), 602-617. <https://doi.org/10.3390/encyclopedia1030050>

94. TajDini, M., Sokolov, V., Kuzminykh, I., Shiaeles, S., & Ghita, B. (2020). Wireless Sensors for Brain Activity—A Survey. *Electronics*, 9(12), 2092. <https://doi.org/10.3390/electronics9122092>

95. Grechaninov, Viktor and Hulak, Hennadii and Hulak, Evgen and Skladannyi, Pavlo and Sokolov, Volodymyr (2021) *Decentralized Access Demarcation System Construction in Situational Center Network Cybersecurity Providing in Information and Telecommunication Systems II* 2021, 3188 (2). pp. 197-206. ISSN 1613-0073

96. Buriachok, Volodymyr and Ageyev, Dmytro and Zhylytsov, Oleksii and Skladannyi, Pavlo and Sokolov, V. Y. (2020) *Invasion Detection Model using Two-Stage Criterion of Detection of Network Anomalies* Cybersecurity Providing in Information and Telecommunication Systems, 2746. pp. 23-32. ISSN 1613-0073

97. Костюк Ю., Хорольська, К., Бебешко, Б., Довженко, Н., Коршун, Н., Пазинін, А. Інструментальні засоби забезпечення інформаційної безпеки від прихованих загроз в інфраструктурі хмарних обчислень. Кібербезпека: освіта, наука, техніка. 2025. 4 (28), 633–655.

98. M. Vladymyrenko, V. Sokolov, V. Buriachok, A. Platonenko and D. Ageyev, "Analysis of Implementation Results of the Distributed Access Control System," *2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, Kyiv, Ukraine, 2019, pp. 1-6, doi: 10.1109/PICST47496.2019.9061376.

99. Складаний, П.М., Машкіна, І.В., Рзаєва, С.Л., Костюк, Ю.В. Методи GDPR для забезпечення безпеки сховищ даних від витоків та загроз. Телекомунікаційні та інформаційні технології. 2025. (2), 59-76.

100. Hu, Z., Buriachok, V., Bogachuk, I., Sokolov, V., Ageyev, D. (2021). Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. In: Radivilova, T., Ageyev, D., Kryvinska, N. (eds) *Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies*, vol 48. Springer, Cham. https://doi.org/10.1007/978-3-030-43070-2_29

101. F. Kipchuk, V. Sokolov, P. Skladannyi and D. Ageyev, "Assessing Approaches of IT Infrastructure Audit," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 213-217, doi: 10.1109/PICST54195.2021.9772181.

102. Kostiuk, Yuliia. (2025). Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System. In book: Insider Threats and Security in Corporations. pp.205-232. <https://doi.org/10.36690/ITSC-205-232>.
103. Grechaninov, Viktor and Hulak, Hennadii and Sokolov, V. Y. and Skladannyi, Pavlo and Korshun, Natalia (2022) *Formation of Dependability and Cyber Protection Model in Information Systems of Situational Center* Emerging Technology Trends on the Smart Industry and the Internet of Things 2022, 3149. pp. 107-117. ISSN 1613-0073
104. Костюк, Ю., Складанний, П., Рзаєва, С., Мазур, Н., Черевик, В., & Аносов, А. (2025). Особливості реалізації мережевих атак через TCP/IP-протоколи. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 571–597.
105. Kuzminykh, I., Carlsson, A., Yevdokymenko, M., Sokolov, V. (2019). Investigation of the IoT Device Lifetime with Secure Data Transmission. In: Galinina, O., Andreev, S., Balandin, S., Koucheryavy, Y. (eds) Internet of Things, Smart Spaces, and Next Generation Networks and Systems. NEW2AN ruSMART 2019 2019. Lecture Notes in Computer Science, vol 11660. Springer, Cham. https://doi.org/10.1007/978-3-030-30859-9_2
106. Buriachok, Volodymyr and Sokolov, V. Y. and Skladannyi, Pavlo (2019) *Security Rating Metrics for Distributed Wireless Systems* MoMLeT&DS. pp. 222-233. ISSN 1613-0073
107. Hu, Z.B., Buriachok, V., TajDini, M., Sokolov, V. (2021). Authentication System by Human Brainwaves Using Machine Learning and Artificial Intelligence. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_31
108. Костюк Ю., Бебешко, Б., Крючкова, Л., Литвинов, В., Оксанич, І., Складанний, П., Хорольська, К. Захист інформації та безпека обміну даними в безпроводових мобільних мережах з автентифікацією і протоколами обміну ключами. Кібербезпека: освіта, наука, техніка. 2024. 1(25), 229–252.
109. Buhas, Vasyl and Ponomarenko, Ihor and Bugas, Valeriy and Ramskyi, Andrii and Sokolov, Volodymyr (2021) *Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3188 (2). pp. 273-281. ISSN 1613-0073
110. Zhebka, V. and Skladannyi, Pavlo and Zhebka, S. and Shlianachak, S. and Bondarchuk, A. (2024) *Methodology for Predicting Failures in a Smart*

Home based on Machine Learning Methods Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 322-332. ISSN 1613-0073

111. Skladannyi, Pavlo and Trofimov, Olexandr and Korniiets, Viktor and Vorokhob, Maksym and Opryshko, Tetiana (2023) *Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept* CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems. pp. 97-106. ISSN 1613-0073

112. Довженко, Н., Іваніченко, Є., & Костюк, Ю. (2025). Методика виявлення та локалізації кіберзагроз у хмарних середовищах з інтегрованими ІОТ-компонентами на основі графових моделей. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 762–776.

113. Шевченко, Галина Володимирівна and Шевченко, Світлана Миколаївна and Жданова, Юлія Дмитрівна and Спасітелева, Світлана Олексіївна and Негоденко, Олена Василівна (2021) *Information Security Risk Analysis SWOT* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 309-317. ISSN 1613-0073

114. I. Iosifov, O. Iosifova and V. Sokolov, "Sentence Segmentation from Unformatted Text using Language Modeling and Sequence Labeling Approaches," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 335-337, doi: 10.1109/PICST51311.2020.9468084.

115. Petriv, P. and Oprisky, I. and Mazur, Nataliia (2024) *Modern technologies of decentralized databases, authentication, and authorization methods* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 60-71. ISSN 1613-0073

116. Astafieva, Mariia and Bodnenko, Dmitry and Lytvyn, Oksana and Proshkin, Volodymyr and Skladannyi, Pavlo (2023) *Formation of High School Students' Resistance to Destructive Information Influences* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 87-96. ISSN 1613-0073

117. Sovyn, Y. and Khoma, V. and Oprisky, I. and Kozachok, Valerii (2023) *Minimization of Bitsliced Representation of 4×4 S-Boxes based on Ternary Logic Instruction* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 12-24. ISSN 1613-0073

118. Burov, O. *et al.* (2020). Cybersecurity in Educational Networks. In: Ahram, T., Karwowski, W., Vergnano, A., Leali, F., Taiar, R. (eds) *Intelligent Human Systems Integration 2020. IHSI 2020. Advances in Intelligent Systems*

and Computing, vol 1131. Springer, Cham. https://doi.org/10.1007/978-3-030-39512-4_56

119. Buriachok, V., Sokolov, V. (2020). Implementation of Active Learning in the Master's Program on Cybersecurity. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education II. ICCSEEA 2019. Advances in Intelligent Systems and Computing*, vol 938. Springer, Cham. https://doi.org/10.1007/978-3-030-16621-2_57

120. Anakhov, Pavlo and Zhebka, Viktoriia and Koretska, Viktoriia and Sokolov, V. Y. and Skladannyi, Pavlo (2022) *Increasing the Functional Network Stability in the Depression Zone of the Hydroelectric Power Station Reservoir* Emerging Technology Trends on the Smart Industry and the Internet of Things, 3149. pp. 169-176. ISSN 1613-0073

121. Z. Hu, B. Vovkotrub, V. Buriachok, Y. Zotkin and V. Sokolov, "Bandwidth Research of Wireless IoT Switches," *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, Lviv-Slavske, Ukraine, 2020, pp. 1-5, doi: 10.1109/TCSET49122.2020.235492.

122. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Abramov, Serhii and Zhylytsov, Oleksii (2022) *Modeling CSIKE Algorithm on Non-Cyclic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 1-10. ISSN 1613-0073

123. Bessalov, Anatoly and Sokolov, Volodymyr and Skladannyi, Pavlo and Mazur, Nataliia and Ageyev, Dmytro (2021) *Implementation of the CSIDH Algorithm Model on Supersingular Twisted and Quadratic Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3187 (1). pp. 302-309. ISSN 1613-0073

124. Bessalov, Anatoly and Kovalchuk, L. and Sokolov, V. Y. and Skladannyi, Pavlo and Radivilova, T. (2020) *Analysis of 2-Isogeny Properties of Generalized Form Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2746. pp. 1-13. ISSN 1613-0073

125. Bessalov, Anatolii & Grubiyani, Evgeniy & Sokolov, Volodymyr & Skladannyi, Pavlo. (2020). 3- and 5-Isogenies of Supersingular Edwards Curves. 10.48550/arXiv.2006.16111.

126. Bessalov, Anatoly and Sokolov, V. Y. and Skladannyi, Pavlo and Zhylytsov, Oleksii (2021) *Computing of Odd Degree Isogenies on Supersingular Twisted Edwards Curves* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 1-11. ISSN 1613-0073

127. V. Astapenya, V. Sokolov, P. Skladannyi and O. Zhylytsov, "Analysis of Ways and Methods of Increasing the Availability of Information in Distributed

Information Systems," *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2021, pp. 174-178, doi: 10.1109/PICST54195.2021.9772161.

128. V. Astapenya, V. Buriachok, V. Sokolov, P. Skladannyi and D. Ageyev, "Last Mile Technique for Wireless Delivery System using an Accelerating Lens," *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, Kharkiv, Ukraine, 2020, pp. 811-814, doi: 10.1109/PICST51311.2020.9467886.

129. Bessalov, Anatoly and Abramov, Serhii and Sokolov, Volodymyr and Skladannyi, Pavlo and Zhylytsov, Oleksii (2023) *Multifunctional CRS Encryption Scheme on Isogenies of Non-Supersingular Edwards Curves* Workshop on Classic, Quantum, and Post-Quantum Cryptography (CQPC 2023), 3504. pp. 12-25. ISSN 1613-0073

130. TajDini, Mahyar and Sokolov, V. Y. and Kuzminykh, Ievgeniia and Ghita, B. (2023) *Brainwave-based authentication using features fusion* Computers & Security (129). p. 103198. ISSN 0167-4048

131. Iosifova, Olena and Iosifov, Ievgen and Rolik, Oleksandr and Sokolov, V. Y. (2020) *Techniques Comparison for Natural Language Processing* MoMLet&DS, 2631 (I). pp. 57-67. ISSN 1613-0073

132. Anakhov, P. and Zhebka, V. and Tushych, A. and Kravchenko, V. and Blazhenyi, N. and Skladannyi, Pavlo and Sokolov, Volodymyr (2022) *Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network* Journal of Theoretical and Applied Information Technology, 100 (22). pp. 6635-6644. ISSN 1817-3195

133. Y. Sadykov, V. Sokolov and P. Skladannyi, "Technology of Location Hiding by Spoofing the Mobile Operator IP Address," *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odesa, Ukraine, 2021, pp. 22-25, doi: 10.1109/UkrMiCo52950.2021.9716700.

134. Obushnyi, Sergiy and Virovets, Denis and Hulak, Hennadii and Zhurakovskiy, Bohdan (2022) *Autonomy of Economic Agents in Peer-to-Peer Systems* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 125-133. ISSN 1613-0073

135. TajDini, Mahyar and Sokolov, V. Y. and Buriachok, Volodymyr (2019) *Men-in-the-Middle Attack Simulation on Low Energy Wireless Devices using Software Define Radio* MoMLet&DS (2386). pp. 287-296. ISSN 1613-0073

136. V. Sokolov, P. Skladannyi and A. Platonenko, "Video Channel Suppression Method of Unmanned Aerial Vehicles," *2022 IEEE 41st*

International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2022, pp. 473-477, doi: 10.1109/ELNANO54667.2022.9927105.

137. Bessalov, Anatoliy and Abramov, Serhii and Sokolov, Volodymyr and Mazur, Nataliia (2023) *CSIKE-ENC Combined Encryption Scheme with Optimized Degrees of Isogeny Distribution* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 36-45. ISSN 1613-0073

138. Hulak, Hennadii and Kriuchkova, Larysa and Skladannyi, Pavlo and Oprisky, Ivan (2021) *Formation of Requirements for the Electronic Record-Book in Guaranteed Information Systems of Distance Learning* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 137-142. ISSN 1613-0073

139. Iosifova, Olena and Iosifov, Ievgen and Sokolov, V. Y. and Romanovskyi, O. and Sukaylo, I. (2021) *Analysis of Automatic Speech Recognition Methods* Cybersecurity Providing in Information and Telecommunication Systems, 2923. pp. 252-257. ISSN 1613-0073

140. Zhebka, V. and Zhebka, S and Bazhan, T and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Methodology for Choosing a Consensus Algorithm for Blockchain Technology* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 106-113. ISSN 1613-0073

141. Dudykevych, V. and Mykytyn, G. and Stosyk, T. and Skladannyi, Pavlo (2024) *Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 449-457. ISSN 1613-0073

142. Shevchenko, Svitlana & Zhdanova, Yuliia & Shevchenko, Halyna & Nehodenko, Olena & Spasiteleva, Svitlana. (2023). *Information Security Risk Management using Cognitive Modeling*.

143. V. Sokolov, P. Skladannyi and A. Platonenko, "Jump-Stay Jamming Attack on Wi-Fi Systems," *2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, Lviv, Ukraine, 2023, pp. 1-5, doi: 10.1109/CSIT61576.2023.10324031.

144. Buriachok, V., Korshun, N., Zhylytsov, O., Sokolov, V., Skladannyi, P. (2023). *Implementation of Active Cybersecurity Education in Ukrainian Higher School*. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspá, G. (eds) *Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies*, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_32

145. Marusenko, R., Sokolov, V., Buriachok, V. (2021). *Experimental Evaluation of Phishing Attack on High School Students*. In: Hu, Z., Petoukhov,

S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education III. ICCSEEA 2020. Advances in Intelligent Systems and Computing*, vol 1247. Springer, Cham. https://doi.org/10.1007/978-3-030-55506-1_59

146. V. Astapenya, V. Sokolov and D. Ageyev, "Experimental Evaluation of an Accelerating Lens on Spatial Field Structure and Frequency Spectrum," *2020 IEEE Ukrainian Microwave Week (UkrMW)*, Kharkiv, Ukraine, 2020, pp. 203-206, doi: 10.1109/UkrMW49653.2020.9252755.

147. Brzhevskaya, Zoreslava and Kyrychok, Roman and Anosov, Andrii and Skladannyi, Pavlo and Vorokhob, Maksym (2021) *Analysis of the Process of Information Transfer from the Source-to-User in Terms of Information Impact* *Cybersecurity Providing in Information and Telecommunication Systems II 2021*, 3188 (2). pp. 257-264. ISSN 1613-0073

148. HU, ZHENG BING & Buriachok, Volodymyr & Sokolov, Volodymyr. (2019). Implementation of Social Engineering Attack at Institution of Higher Education. *SSRN Electronic Journal*. 10.2139/ssrn.3679106.

149. Mykhaylova, O and Fedynyshyn, T and Sokolov, Volodymyr and Kyrychok, Roman (2024) *Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap* *Cybersecurity Providing in Information and Telecommunication Systems 2024*, 3654. pp. 239-251. ISSN 1613-0073

150. Marusenko, R., Sokolov, V., Skladannyi, P. (2023). Social Engineering Penetration Testing in Higher Education Institutions. In: Hu, Z., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VI. ICCSEEA 2023. Lecture Notes on Data Engineering and Communications Technologies*, vol 181. Springer, Cham. https://doi.org/10.1007/978-3-031-36118-0_96

151. Mykhaylova, O and Fedynyshyn, T and Datsiuk, A and Fihol, B and Hulak, Hennadii (2023) *Mobile Application as a Critical Infrastructure Cyberattack Surface* *Cybersecurity Providing in Information and Telecommunication Systems II 2023*, 3050. pp. 29-43. ISSN 1613-0073

152. Kyrychok, R., Laptiev, O., Lisnevskyi, R., Kozlovskyi, V., & Klobukov, V. (2022). Development of a method for checking vulnerabilities of a corporate network using Bernstein transformations. *Eastern-European Journal of Enterprise Technologies*, 1(9(115)), 93–101. <https://doi.org/10.15587/1729-4061.2022.253530>

153. V. Sokolov, P. Skladannyi and V. Astapenya, "Bluetooth Low-Energy Beacon Resistance to Jamming Attack," *2023 IEEE 13th International Conference on Electronics and Information Technologies (ELIT)*, Lviv, Ukraine, 2023, pp. 270-274, doi: 10.1109/ELIT61488.2023.10310815.

154. Astapenya, Volodymyr & Zhdanova, Yuliia & Shevchenko, Svitlana & Spasiteleva, Svitlana & Kryvoruchko, Olena. (2024). Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare.

155. Dudykevych, V and Yevseiev, S and Mykytyn, H and Ruda, K and Hulak, Hennadii (2024) *Detecting Deepfake Modifications of Biometric Images using Neural Networks* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 391-397. ISSN 1613-0073

156. Adamantis, M., Sokolov, V., Skladannyi, P. (2025). Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method. In: Hu, Z., Yanovsky, F., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VII. ICCSEEA 2024* 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 242. Springer, Cham. https://doi.org/10.1007/978-3-031-84228-3_5

157. Chernenko, Roman and Anosov, Andrii and Kyrychok, Roman and Brzhevskaya, Zoreslava and Spasiteleva, Svitlana (2022) *Encryption Method for Systems with Limited Computing Resources* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 142-148. ISSN 1613-0073

158. Iavich, M. and Kovalchuk, O. and Gnatyuk, S. and Khavikova, Y. and Sokolov, Volodymyr (2024) *Classical and post-quantum encryption for GDPR* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 70-78. ISSN 1613-0073

159. Romanovskiy, O. and Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2022) *Prototyping Methodology of End-to-End Speech Analytics Software* Modern Machine Learning Technologies and Data Science Workshop, 3312 (1). pp. 76-86. ISSN 1613-0073

160. Romanovskiy, O., Iosifov, I., Iosifova, O., Sokolov, V., Kipchuk, F., Sukaylo, I. (2021). Automated Pipeline for Training Dataset Creation from Unlabeled Audios for Automatic Speech Recognition. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education IV. ICCSEEA 2021*. Lecture Notes on Data Engineering and Communications Technologies, vol 83. Springer, Cham. https://doi.org/10.1007/978-3-030-80472-5_3

161. Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. *Cryptography*, 8(3), 38. <https://doi.org/10.3390/cryptography8030038>

162. Syrotynskiy, R. and Tyshyk, I. and Kochan, O. and Sokolov, Volodymyr and Skladannyi, Pavlo (2024) *Methodology of network infrastructure*

analysis as part of migration to zero-trust architecture Cyber Security and Data Protection 2024 (3800). pp. 97-105. ISSN 1613-0073

163. Martseniuk, Y. and Partyka, A. and Harasymchuk, O. and Shevchenko, Svitlana (2024) *Universal centralized secret data management for automated public cloud provisioning* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 72-81. ISSN 1613-0073

164. Iosifov, Ievgen and Iosifova, Olena and Sokolov, Volodymyr and Skladannyi, Pavlo and Sukaylo, Igor (2021) *Natural Language Technology to Ensure the Safety of Speech Information* Cybersecurity Providing in Information and Telecommunication Systems II. Volume I, 3187 (1). pp. 216-226. ISSN 1613-0073

165. Bahatskyi, Oleksii and Bahatskyi, V. and Sokolov, Volodymyr (2023) *Smart Home Subsystem for Calculating the Quality of Public Utilities* Cybersecurity Providing in Information and Telecommunication Systems, 3421. pp. 168-173. ISSN 1613-0073

166. V. Sokolov, P. Skladannyi and N. Mazur, "Wi-Fi Repeater Influence on Wireless Access," 2023 *IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2023, pp. 33-36, doi: 10.1109/AICT61584.2023.10452421.

167. Dreis, Y. and Korchenko, O. and Brzhevska, Zoreslava and Kriuchkova, Larysa and Nesterova, Olena (2024) *Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 277-289. ISSN 1613-0073

168. Virovets, Denis and Obushnyi, Sergiy and Zhurakovskiy, B. and Skladannyi, Pavlo and Sokolov, Volodymyr (2024) *Integration of smart contracts and artificial intelligence using cryptographic oracles* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 39-46. ISSN 1613-0073

169. Shevchenko, Svitlana & Zhdanova, Yuliia & Shevchenko, Halyna & Nehodenko, Olena & Spasiteleva, Svitlana. (2023). *Conflict Analysis in the "Subject-to-Subject" Security System.*

170. Myrontsov, Mykyta and Noskov, Oleksii and Sokolov, Volodymyr (2021) *Method for Determining Areas of Stable Solutions of Inverse Problems of Mathematical Physics by the Example of Well Electrometry* Information Technology and Mathematical Modeling for Environmental Safety 2021, 3021. pp. 115-126. ISSN 1613-0073

171. Buriachok, V., Hadzhyiev, M., Sokolov, V., Skladannyi, P., & Kuzmenko, L. (2019). *Implantation of indexing optimization technology for*

highly specialized terms based on Metaphone phonetical algorithm. *Eastern-European Journal of Enterprise Technologies*, 5(2 (101), 43–50. <https://doi.org/10.15587/1729-4061.2019.181943>

172. Dreis, Yurii and Ivanichenko, Yevhen and Nesterova, Olena and Zhdanova, Yuliia and Dmytriienko, Kate (2022) *Restricted Information Identification Model* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 89-95. ISSN 1613-0073

173. Martseniuk, Yevhenii and Partyka, Andrii and Harasymchuk, Oleh and Cherevyk, Vyacheslav and Dovzhenko, Nadiia (2025) *Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 260-274. ISSN 1613-0073

174. Gnatyuk, S. and Sydorenko, V. and Polozhentsev, A. and Sokolov, Volodymyr (2024) *Method for managing IT incidents in critical information infrastructure facilities* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 326-333. ISSN 1613-0073

175. Shapoval, V. and Zubyk, L. and Zubyk, Y. and Kurchenko, O. and Kozachok, Valerii (2024) *Automation of Data Management Processes in Cloud Storage* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 410-418. ISSN 1613-0073

176. Dovzhenko, N. and Haidur, H. and Brzhevskaya, Zoreslava and Ivanichenko, Yevhen and Nesterova, Olena (2023) *Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes* Cybersecurity Providing in Information and Telecommunication Systems 2023, 3421. pp. 278-283. ISSN 1613-0073

177. Kulibaba, Serhii and Popereshnyak, Svitlana and Shcheblanin, Yuri and Kurchenko, Oleg and Mazur, Nataliia (2022) *Advanced Communication Model with the Voice Control and the Increased Security Level* Cybersecurity Providing in Information and Telecommunication Systems 2022, 3288 (1). pp. 64-72. ISSN 1613-0073

178. Zybin, Serhii and Khoroshko, Volodymyr and Khokhlachova, Yuliia and Kozachok, Valerii (2021) *Approach of the Attack Analysis to Reduce Omissions in the Risk Management* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 318-328. ISSN 1613-0073

179. V. Sokolov, P. Skladannyi and V. Astapenya, "Wi-Fi Interference Resistance to Jamming Attack," 2023 *IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/AICT61584.2023.10452687.

180. Shevchenko, Svitlana and Zhdanova, Yuliia and Kryvytska, O. and Shevchenko, H. and Spasiteleva, Svitlana (2024) *Fuzzy cognitive*

mapping as a scenario approach for information security risk analysis Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 356-362. ISSN 1613-0073

181. Pinchuk, Olga and Sokolyuk, Oleksandra and Burov, Oleksandr and Lavrov, Evgeniy and Shevchenko, Svitlana and Aksakovska, Valeriia (2020) *ICT for training and evaluation of the solar impact on aviation safety* ICT in Education, Research, and Industrial Applications. Proc. 16 th Int. Conf. ICTERI 2020. Volume II: Workshops. Kharkiv, Ukraine, October 6-10, 2020, CEUR-WS.org,. pp. 786-792. ISSN 1613-0073

182. Zhurakovskiy, B. and Otrokh, S. and Poliakov, M. and Poliakov, O. and Skladannyi, Pavlo (2024) *Enhancing information transmission security with stochastic codes* Classic, Quantum, and Post-Quantum Cryptography 2024, 3829. pp. 62-69. ISSN 1613-0073

183. Kriuchkova, Larysa and Tsmokanych, Ivan and Shevchenko, Svitlana and Bohdanov, Oleksandr and Mazur, Nataliia (2023) *Experimental Research of the Parameters of Danger and Protective Signals Attached to High-Frequency Imposition* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 261-268. ISSN 1613-0073

184. Berestov, Denis and Kurchenko, Oleg and Zubyk, L. and Kulibaba, Serhii and Mazur, Nataliia (2023) *Assessment of Weather Risks for Agriculture using Big Data and Industrial Internet of Things Technologies* Cybersecurity Providing in Information and Telecommunication Systems II 2023, 3550. pp. 1-13. ISSN 1613-0073

185. Tkachenko, K. and Tkachenko, O. and Tkachenko, O. and Mazur, Nataliia and Mashkina, Iryna (2024) *Ontological Approach in Modern Educational Processes* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 88-97. ISSN 1613-0073

186. Popereshnyak, S. and Novikov, Y. and Zhdanova, Yuliia (2024) *Cryptographic system security approaches by monitoring the random numbers generation* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 301-309. ISSN 1613-0073

187. Mykhaylova, O. and Stefankiv, A. and Nakonechny, T. and Fedynyshyn, T. and Sokolov, Volodymyr (2024) *Resistance to Replay Attacks of Remote Control Protocols using the 433 MHz Radio Channel* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 98-110. ISSN 1613-0073

188. Novytskyi, Anton and Sokolov, Volodymyr and Kriuchkova, Larysa and Skladannyi, Pavlo (2025) *Determining the error distribution of BLE beacons at antenna near and far fields* Cyber Hygiene & Conflict Management in Global Information Networks 2025, 4024. pp. 133-143. ISSN 1613-0073

189. Romanovskiy, O. *et al.* (2025). Accuracy Improvement of Spoken Language Identification System for Close-Related Languages. In: Hu, Z., Yanovsky, F., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education VII. ICCSEEA 2024* 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 242. Springer, Cham. https://doi.org/10.1007/978-3-031-84228-3_4
190. Kriuchkova, Larysa and Tsmokanych, I. and Vovk, M. and Mazur, Nataliia and Bohdanov, Oleksandr (2024) *Influence of Protective Signals on Dangerous Signals of High-Frequency Imposition* Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654. pp. 419-425. ISSN 1613-0073
191. Buhas, V. and Ponomarenko, I. and Buhas, N. and Hulak, Hennadii (2024) *Cybersecurity Role in AI-Powered Digital Marketing* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 1-11. ISSN 1613-0073
192. Dreis, Y. and Korchenko, O. and Sokolov, Volodymyr and Skladannyi, Pavlo (2024) *Model to formation data base of secondary parameters for assessing status of the state secret protection* Cyber Security and Data Protection 2024 (3800). pp. 1-11. ISSN 1613-0073
193. Shevchenko, Svitlana & Zhdanova, Yuliia & Astapenya, Volodymyr & Nehodenko, Olena & Spasiteleva, Svitlana. (2024). *Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels.*
194. Kolbasova, K and Zhurakovskiy, Bohdan and Poltorak, V and Nakonechnyi, V and Kyrychok, Roman (2023) *Smart Home Network based on Cisco Equipment* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 70-80. ISSN 1613-0073
195. Virovets, Denis and Obushnyi, Sergiy and Ramskyi, Andrii and Hulak, Hennadii (2024) *Soul Bound Token as Digital Twins in Peer-to-Peer Economic Systems* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 97-105. ISSN 1613-0073
196. Tyshyk, I. and Hulak, Hennadii (2024) *Testing an organization's information system for unauthorized access* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 17-29. ISSN 1613-0073
197. Zhebka, Serhii and Zhebka, Viktoriia and Hulak, Hennadii and Kyrychok, Roman and Platonenko, Artem (2025) *Method for Adaptive Allocation of Cryptographic Resources in Distributed Databases* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 620-628. ISSN 1613-0073

198. Dovzhenko, Nadiia & Ivanichenko, Yevhen & Skladannyi, Pavlo & Zhylytsov, Oleksii. (2024). Research of UAV and sensor network integration features for routing optimization and energy consumption reduction.
199. Zhebka, V. and Skladannyi, Pavlo and Bazak, Y and Bondarchuk, A. and Storchak, K. (2024) *Methods for Predicting Failures in a Smart Home* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 70-78. ISSN 1613-0073
200. Kriuchkova, Larysa and Tsmokanych, I. and Mazur, Nataliia and Tarasenko, D. and Osadcha, V. (2024) *Experimental determination of protective signal parameters for effective “swinging” of the carrier frequency of high-frequency imposition* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 251-259. ISSN 1613-0073
201. Kraus, N. and Kraus, K. and Shevchenko, Svitlana and Proshkin, Volodymyr (2024) *Digitalizing Production and Industry through 4.0 Technologies Implementation* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 36-47. ISSN 1613-0073
202. Костюк, Ю., Складанний, П., Рзаєва, С., Самойленко, Ю., & Коршун, Н. (2025). Інтелектуальні системи керування та захисту в кіберфізичних і хмарних середовищах Smart Grid. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 125–156.
203. Складанний, П., Костюк, Ю., Рзаєва, С., & Мазур, Н. (2025). Паралельна обробка даних у розширюваних хеш-структурах та оцінка їх продуктивності. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31), 242–269. <https://doi.org/10.28925/2663-4023.2025.31.1015>
204. Складанний, П.М., Гулак, Г.М., Костюк, Ю.В. Генератор хаотичних чисел із нечітким керуванням для криптографічних систем із динамічною довірою. Телекомунікаційні та інформаційні технології. 2025. № 4 (89), 137-147. <https://doi.org/10.31673/2412-4338.2025.048916>
205. Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive Information Security Management in Cloud-Oriented Intelligent Transportation Systems. Ukrainian Scientific Journal of Information Security, 2025, vol. 31, issue 1, pp. 23-36. <https://doi.org/10.18372/2225-5036.31.20634>
206. Kulibaba, S. and Zubyk, L. and Kurchenko, O. and Sinitsyn, I. and Mazur, Nataliia (2023) *Linked System of Data Organization and Management* Cybersecurity Providing in Information and Telecommunication Systems (3421). pp. 117-126. ISSN 1613-0073
207. Chyzhevska, Maryna & Романовська, Наталія & Venger, Vitalii & Sokolov, Volodymyr. (2024). Tokenomics and Perspectives of Proof of Stake.

208. Ivanichenko, Yevhen and Kozachok, Valerii and Dreis, Yurii and Nesterova, Olena and Dmytriienko, Kate (2021) *Exposing Deviations in Information Processes using Multifractal Analysis* Cybersecurity Providing in Information and Telecommunication Systems II 2021, 3187 (1). pp. 251-259. ISSN 1613-0073
209. Bilous, Vladyslav and Bodnenko, Dmitry and Lokaziuk, Oleksandra and Skladannyi, Pavlo and Abramov, Vadym (2025) *Cyber Evidence Software as the Digital Forensics Tools in the Investigation of Cybercrime* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 26-37. ISSN 1613-0073
210. Brzhevska, Zoreslava and Haidur, Halyna and Dovzhenko, Nadiia and Anosov, Andrii and Vorokhob, Maksym (2021) *Recurrent Estimation of the Information State Vector and the Correlation of Measuring Impact Matrix using a Multi-Agent Model* Cybersecurity Providing in Information and Telecommunication Systems 2021, 2963. pp. 272-276. ISSN 1613-0073
211. Anakhov, P. and Zhebka, V. and Kravchenko, V. and Skladannyi, Pavlo and Zhylytsov, Oleksii (2023) *Hybrid Study of the Geophysical Situation in the Depressed Zone of Hydroelectric Power Plants Reservoir* Cybersecurity Providing in Information and Telecommunication Systems, 3550. pp. 269-274. ISSN 1613-0073
212. Dovzhenko, Nadiia and Barabash, Oleg and Musienko, Andrii and Ivanichenko, Yevhen and Krashenninnik, Iryna (2024) *Enhancing Sensor Network Efficiency Through Optimized Flooding Mechanism* CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine. pp. 465-470. ISSN 1613-0073
213. Obushnyi, Sergiy and Virovets, Denis and Zhytar, Maksym and Zhdanova, Yuliia (2024) *Unlocking the Economic Potential of Real Estate Tokenization in Ukraine* Digital Economy Concepts and Technologies Workshop 2024, 3665. pp. 79-87. ISSN 1613-0073
214. Рзаєва С.Л., Складаний П.М., Машкіна І.В., Костюк Ю.В. (2025) Модель реалізації керування доступом на основі ролей (RBAC) у багаторівневій архітектурі сховища даних. Сучасний захист інформації, 3(63), 137–149.
215. Trofymchuk, Oleksandr and Vasyanin, Volodymyr and Sokolov, Volodymyr and Chikrii, Arkadii and Ushakova, Liudmyla (2021) *On the Use of Gray Codes for Solving 0-1 Combinatorial Problems of Optimization and Decision-Making in Environmental and Economic Systems* Information Technology and Mathematical Modeling for Environmental Safety 2021, 3021. pp. 18-28. ISSN 1613-0073

216. Tkachenko, O. and Tkachenko, K. and Tkachenko, O. and Kyrychok, Roman and Yaskevych, Vladyslav (2024) *Neural Networks in the Processing of Natural Language Texts in Information Learning Systems* Cybersecurity Providing in Information and Telecommunication Systems, 3654. pp. 73-87. ISSN 1613-0073

217. Popereshnyak, S. and Ovcharenko, V. and Novikov, Y. and Hulak, Hennadii (2024) *Detection of intrusions based on text analysis and machine learning methods in the development of information systems* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 310-318. ISSN 1613-0073

218. Tykholaz, D. and Banakh, R. and Mychuda, L. and Piskozub, A. and Kyrychok, Roman (2024) *Incident response with AWS detective controls* Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. pp. 190-197. ISSN 1613-0073

219. Shevchenko, Svitlana & Zhdanova, Yuliia & Nehodenko, Olena & Spasiteleva, Svitlana & Nehodenko, Vitalii. (2025). *Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems*

220. Avdeyenko, Gleb and Narytnyk, Teodor and Saiko, Volodymyr and Kriuchkova, Larysa and Tsmokanych, Ivan (2025) *Terahertz Range Transceiver Module for Electromagnetic Protection of Objects* Cybersecurity Providing in Information and Telecommunication Systems 2025 (3991). pp. 603-610. ISSN 1613-0073

221. Hulak, H., et al. (2020). *Cryptovirology: Security Threats to Guaranteed Information Systems and Measures to Combat Encryption Viruses*. Cybersecurity: Education, Science, Technique, 2(10), 6–28. <https://doi.org/10.28925/2663-4023.2020.10.628>

Інтернет-джерела

1. Рекомендації CERT-UA щодо протидії APT (Advanced Persistent Threat). URL: <https://cert.gov.ua/recommendations/18>

2. Технологія VPN може загрожувати кібербезпеці. URL: <https://detector.media/infospace/article/126505/2017-05-31-tekhnologiya-vpnmozhe-zagrozhuвати-kiberbezpetsi-inau>

3. JP 3–12 Cyberspace Operations, 8 June 2018. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

4. DOD Dictionary of Military and Associated Terms. As of January 2019. URL: <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>
5. Cybersecurity a generic reference curriculum (2016). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-162_curriculum.pdf
6. National Cyber Security Strategy Good Practice Guide (2016). URL: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>
7. Castro D. (2018). Boosting the Cyberworkforce. URL: <http://www.govtech.com/data/Boosting-the-Cyberworkforce.html>
8. Cisco -Україна. URL: <https://www.cisco.com>
9. Про основні засади забезпечення кібербезпеки України: Закон України // Відомості Верховної Ради України. 2017. № 45. Ст. 403.
10. Закон України "Про інформацію".
11. Закон України "Про захист інформації в інформаційно-комунікаційних системах".
12. ДСТУ ISO/IEC 27001:2015 (ISO/IEC 27001:2013, IDT) "Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги".
13. ДСТУ ISO/IEC 27002:2015 "Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою".
14. ДСТУ ISO/IEC 27005:2022 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки".
15. ДСТУ ISO/IEC 27701:2022 "Розширення для управління конфіденційністю в системах управління інформаційною безпекою".
16. ДСТУ ISO/IEC 15408:2020 "Критерії оцінювання безпеки інформаційних технологій".
17. ДСТУ ISO/IEC 24762:2015 "Інформаційні технології. Методи захисту. Рекомендації з відновлення інформаційно-комунікаційних технологій після інцидентів".

Навчальне видання

КОСТЮК Юлія Володимирівна,
СКЛАДАННИЙ Павло Миколайович

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Підручник

*Частина II. Прикладні аспекти та сучасні
технології захисту інформації в комп'ютерних
системах та мережах*