Міністерство освіти і науки України
Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«Допущено до захисту»
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття другого (магістерського)
рівня вищої освіти

Спеціальність 125 Кібербезпека та захист інформації

Тема роботи:
МЕТОДИ ТА ЗАСОБИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТИПОВОГО ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Виконав

студент групи КБм-1-24-1.4.д

Задворний Дмитро Сергійович___
(прізвище, ім'я, по батькові)

_____
(підпис)

Науковий керівник
к. т. н., доцент_____
(науковий ступінь, наукове звання)
Козачок В. А._____
(прізвище, ініціали)

_____
(підпис)

Київ – 2025

Міністерство освіти і науки України
Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Освітньо-кваліфікаційних рівень – магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітня програма 125.00.01 Безпека інформаційних і комунікаційних систем

«Допущено до захисту»
Завідувач кафедри інформаційної та
кібернетичної безпеки імені
професора Володимира Бурячка
кандидат технічних наук, доцент
Складанний П.М.

_____
(підпис)
« ___ » _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Задворному_Дмитру_Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Методи_та_засоби_побудови_КСЗІ_типового_ОІД_____; керівник: Козачок_Валерій_Анатолійович_____, затверджені наказом ректора від «___»_____ 20___ року №__.
2. Термін подання студентом роботи «___»_____ 20___ р.
3. Вихідні дані до роботи:

3.1 науково-технічна та нормативна література з теми дослідження: Конституція України, Закони України «Про інформацію», «Про захист інформації в ІТС», «Про електронні довірчі послуги», «Про захист персональних даних», ДСТУ ISO/IEC 27001, 27002, 27005, ДСТУ 8802:2018, методичні документи ДССЗЗІ, стандарти NIST SP 800-53, NIST CSF 2.0, ENISA Guidelines, наукові праці з побудови КСЗІ;

3.2 методи: Системний аналіз, моделювання загроз і порушника, оцінка ризиків, порівняльний аналіз, аналітичні методи, моделювання інформаційних потоків;

3.3 технології: NGFW та IPS-системи, сегментація мережі (VLAN, Zero Trust), SIEM для кореляції подій безпеки, DLP (у контексті сучасних засобів КСЗІ), IAM/MFA та PAM для керування доступами, криптографічні технології (TLS 1.2/1.3, взаємна автентифікація, КЕП), технології резервного копіювання (3–2–1 схема), SOC/SIEM та SOAR (концептуально), DevSecOps-підходи (концептуально), корпоративні IT-системи (CRM, ERP, СЕД) як елементи інфраструктури ІТС;

3.4 алгоритми: Використовуються описові методики моделювання загроз, порушника та процесів побудови КСЗІ відповідно до нормативних документів;

3.5 мова програмування: Не застосовується;

3.6 математичні моделі та методи: Використовуються описові та аналітичні методи моделювання загроз, порушника та оцінювання рівня захищеності.

4. Зміст текстової частини роботи (перелік питань, які потрібно розробити):

4.1 Провести аналіз сучасного стану кіберзагроз та нормативно-правових вимог щодо створення КСЗІ.

4.2 Дослідити методологію створення комплексної системи захисту інформації, включаючи моделювання загроз, порушника, формування політики та вибір засобів захисту.

4.3 Розробити модель побудови КСЗІ для типового об’єкта інформаційної діяльності: провести обстеження ІТС, опис інформаційних потоків, визначення вразливостей, формування профілю захищеності та розробку комплексу організаційних, технічних і програмних заходів.

5. Перелік графічного матеріалу:

5.1 Презентація доповіді, виконана в Microsoft PowerPoint.

5.2 Таблиці, що відображають результати обстеження ІТС, оцінку рівня захищеності, реєстр ризиків, порівняльний аналіз засобів захисту.

6. Дата видачі завдання «___»_____ 20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	14.02.2025	Виконано
2.	Аналіз літератури	01.07.2025–31.08.2025	Виконано
3.	Обґрунтування вибору рішення	01.09.2025–09.09.2025	Виконано
4.	Збір даних	10.09.2025–27.09.2025	Виконано
5.	Виконання та оформлення розділу 1.	28.09.2025–08.10.2025	Виконано
6.	Виконання та оформлення розділу 2.	09.10.2025–20.10.2025	Виконано
7.	Виконання та оформлення розділу 3.	21.10.2025–30.11.2025	Виконано
8.	Вступ, висновки, реферат	01.12.2025–05.12.2025	Виконано
9.	Апробація роботи на науково методичному семінарі та/або науково-технічній конференції	24.11.2025	Виконано
10.	Оформлення та друк текстової частини роботи	07.12.2025	Виконано
11.	Оформлення презентацій	08.12.2025–12.12.2025	Виконано
12.	Отримання рецензій	06.12.2025	Виконано
13.	Попередній захист роботи	21.11.2025	Виконано
14.	Захист в ЕК	16.12.2025–18.12.2025	Виконано

Студент _____ Задворний Дмитро Сергійович
(підпис) (прізвище, ім’я, по батькові)

Науковий керівник _____ Козачок Валерій Анатолійович
(підпис) (прізвище, ім’я, по батькові)

РЕФЕРАТ

Кваліфікаційна робота присвячена методам та засобам побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності.

Робота складається зі вступу, трьох розділів, що містять 9 таблиць, висновків і списку використаних джерел, що містить 28 найменувань. Загальний обсяг роботи становить 120 сторінок, з яких 33 сторінки займають таблиці, а також перелік умовних скорочень та список використаних джерел.

Об’єктом дослідження в роботі є процес забезпечення захисту інформації в типових інформаційно-комунікаційних системах об’єкта інформаційної діяльності.

Предметом дослідження є методи, моделі та технічні засоби побудови комплексної системи захисту інформації.

Метою роботи є підвищення рівня безпеки інформаційних ресурсів шляхом побудови оптимальної комплексної системи захисту інформації відповідно до вимог чинних нормативних документів та сучасних підходів у сфері кіберзахисту.

Для досягнення поставленої мети в роботі:

- Проведено аналіз існуючих підходів до створення комплексних систем захисту інформації, їх нормативно-правового забезпечення та практичних моделей;
- Досліджено особливості побудови комплексної системи захисту інформації для типового об’єкта інформаційної діяльності, включно з моделюванням актуальних загроз і визначенням вимог безпеки;
- Обґрунтовано вибір структури, технологій і засобів захисту, необхідних для створення комплексної системи, що відповідає встановленим вимогам.

Наукова новизна одержаних результатів полягає в тому, що в роботі уточнено структуру типової комплексної системи захисту інформації для

об’єкта інформаційної діяльності, запропоновано вдосконалену модель оцінювання загроз, а також розроблено методичні рекомендації щодо формування комплексу технічних і організаційних заходів із захисту інформації.

Галузь застосування. Запропоновані підходи можуть бути використані для створення, проектування та впровадження комплексних систем захисту інформації на підприємствах, в установах та організаціях, що працюють з інформацією обмеженого доступу, а також у навчальному процесі при підготовці фахівців з кібербезпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, КРИПТОГРАФІЧНИЙ ЗАХИСТ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ДССЗЗІ	–	Державна служба спеціального зв’язку та захисту інформації України.
ІБ	–	інформаційна безпека.
ІТС	–	інформаційно-телекомунікаційна система.
КСЗІ	–	комплексна система захисту інформації.
ОІД	–	об’єкт інформаційної діяльності.
ОТ	–	технології, що забезпечують управління промисловим обладнанням і процесами.
AES	–	сучасний стандарт симетричного шифрування.
BCP	–	план забезпечення безперервності бізнесу.
CDN	–	мережа доставки контенту.
DLP	–	система запобігання витоку даних.
DevSecOps	–	підхід до розробки, що інтегрує безпеку у всі етапи життєвого циклу ПЗ.
DRP	–	план відновлення після катастроф.
HSM	–	апаратний модуль безпечного управління криптографічними ключами.
IAM	–	система управління ідентифікацією та доступом користувачів.
IDS/IPS	–	система виявлення та запобігання вторгненням.
IRP	–	план реагування на інциденти інформаційної безпеки.
MTTD	–	середній час виявлення інциденту.
MTTR	–	середній час реагування або відновлення після інциденту.
MFA	–	багатофакторна автентифікація.
PAM	–	система управління привілейованим доступом.
SCADA	–	система диспетчерського управління та збору даних у виробничих процесах.
SIEM	–	система збору, аналізу та кореляції подій безпеки.
SOAR	–	система автоматизації реагування на інциденти безпеки.

SOC	–	центр моніторингу та реагування на інциденти інформаційної безпеки.
TLS	–	протокол захисту передачі даних у мережах.
UEM/MDM	–	системи централізованого управління кінцевими пристроями.
VPN	–	віртуальна приватна мережа для захищеного з’єднання.
Zero Trust	–	концепція мережевої безпеки, що передбачає відсутність довіри до будь-яких користувачів і пристроїв за замовчуванням.

ВСТУП

Актуальність теми. Сучасний етап розвитку суспільства характеризується стрімкою цифровізацією, яка охоплює практично всі сфери діяльності – від бізнесу та державного управління до медицини й освіти. В умовах глобальної інформатизації стають одним із ключових активів інформаційні ресурси, що визначають конкурентоспроможність і стабільність організацій. Водночас зростання масштабів використання інформаційних технологій супроводжується появою нових кіберзагроз, що відзначаються високим рівнем складності та цілеспрямованості. Це обумовлює підвищений інтерес до розробки ефективних механізмів захисту інформації, серед яких центральне місце посідають КСЗІ.

Доцільність дослідження зумовлюється низкою чинників. По-перше, кількість кіберінцидентів в Україні та світі щороку зростає, що підтверджується статистикою міжнародних аналітичних центрів. По-друге, інтеграція українських підприємств у глобальний ринок вимагає відповідності міжнародним стандартам, зокрема ISO/IEC 27001 та GDPR, що регламентують вимоги до захисту інформаційних активів. По-третє, в Україні активно формується власна нормативно-правова база у сфері інформаційної безпеки, яка вимагає від суб’єктів господарювання впровадження КСЗІ відповідно до методичних рекомендацій ДССЗЗІ. Нарешті, вагомим чинником є людський фактор, адже більшість інцидентів пов’язані з недостатньою обізнаністю або помилками персоналу, що зумовлює потребу в комплексних організаційних заходах.

Метою роботи є розробка моделі побудови КСЗІ для типового ОІД з урахуванням сучасних кіберзагроз, національних нормативних вимог та міжнародних стандартів. Для досягнення цієї мети необхідно вирішити такі **завдання:**

1) Проаналізувати сучасний стан і тенденції розвитку кіберзагроз в Україні та світі;

2) Дослідити нормативно-правову базу у сфері захисту інформації;
3) Класифікувати ОІД та визначити їх специфічні вимоги до захисту;
4) Вивчити методологію створення КСЗІ, включаючи етапи аналізу загроз, моделювання порушника та формування політики безпеки;
5) Розробити модель побудови КСЗІ для конкретного підприємства як типового ОІД;
6) Провести аналіз інформаційних потоків, загроз і вразливостей, сформувати профіль захищеності;
7) Запропонувати комплекс технічних, програмних, криптографічних та організаційних заходів захисту;
8) Оцінити ефективність запропонованих заходів та визначити їх практичну значимість.

Об’єктом дослідження є процес забезпечення інформаційної безпеки в ІТС ОІД. **Предметом дослідження** є методи, засоби та організаційні механізми побудови КСЗІ.

Методи дослідження. У роботі застосовано комплекс методів дослідження: аналітичні методи використано для вивчення наукових праць, міжнародних стандартів і національних нормативних актів; системний аналіз дозволив здійснити моделювання архітектури КСЗІ та визначити взаємозв’язки між її складовими; методи оцінки ризиків забезпечили визначення рівня загроз і ефективності заходів протидії; порівняльний аналіз – зіставлення вітчизняних і міжнародних практик захисту інформації; моделювання використано для побудови моделей загроз, порушників і профілю захищеності.

Наукова новизна одержаних результатів. роботи полягає у розробці моделі побудови КСЗІ для типового підприємства з урахуванням багаторівневого підходу до безпеки («defense in depth»), поєднання технічних, програмних, криптографічних і організаційних заходів, інтеграції сучасних методів (DLP, PAM, SOC/SIEM, SOAR, DevSecOps) у загальну архітектуру

системи та врахування як національних, так і міжнародних стандартів у сфері інформаційної безпеки.

Теоретичне та практичне значення дослідження полягає в побудові цілісної моделі КСЗІ для типового ОІД, що включатиме визначення інформаційних потоків, моделювання загроз і порушників, оцінку рівня захищеності та розробку дорожньої карти впровадження. Реалізація запропонованих заходів дозволить знизити кількість критичних інцидентів, підвищити стійкість бізнес-процесів, забезпечити відповідність національному законодавству й міжнародним стандартам.

Галузь застосування. Результати роботи можуть бути використані як методологічна основа для впровадження КСЗІ на реальних підприємствах України. Запропоновані рекомендації можуть бути адаптовані до специфіки різних галузей і масштабів організацій, сприяти підвищенню рівня кіберстійкості, зменшенню фінансових втрат і зміцненню довіри з боку клієнтів і партнерів.

Апробація результатів дипломної роботи. Основні положення роботи викладалися:

1) Студентська наукова конференція «Безпека інформаційно-комунікаційних систем» БІКС’2025 (Київський столичний університет імені Бориса Грінченка, 26 жовтня 2025) [1];
2) В статті «Методи та засоби побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності», Задворний Д.С., Козачок В.А., «Кібербезпека: освіта, наука, техніка», стаття прийнята до опублікування [2].

Розділ 1. ТЕОРЕТИЧНІ ЗАСАДИ РОЗРОБКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Постановка проблеми захисту інформації в умовах сучасних кіберзагроз

У сучасному інформаційному суспільстві інформація розглядається як один з ключових ресурсів розвитку держави, бізнесу та особи. Від рівня її захищеності залежить стабільність функціонування організацій, ефективність управління та конкурентоспроможність економіки [3]. Водночас стрімка цифровізація та масове впровадження інформаційно-комунікаційних технологій зумовили виникнення якісно нових загроз, що проявляються у вигляді складних, багатовекторних кіберінцидентів [4].

Захист інформації ускладнюється низкою чинників:

- Глобалізація кіберпростору: Інформаційні системи інтегровані у світові мережі, що створює умови для віддалених атак з будь-якої точки світу.
- Зростання кількості та складності атак: Поряд із масовими шкідливими програмами поширюються цілеспрямовані APT-атаки, здатні тривати місяцями та орієнтовані на конкретні ОІД [5].
- Людський фактор: Працівники залишаються одним із найуразливіших елементів: соціальна інженерія, фішинг, підкуп чи недбалість здатні нівелювати технічні засоби захисту.
- Недостатня організаційна культура: Попри наявність законодавчої бази (Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», ДСТУ серій 2700 та 8802), на практиці спостерігається формальний підхід до створення КСЗІ [6].

Суттєвою особливістю сучасного етапу розвитку є те, що кіберзагрози стали елементом гібридних воєн і економічної конкуренції, а отже впливають не лише на ІТ-інфраструктуру, а й на політичну та економічну стабільність держав [7].

Таким чином, проблема захисту інформації в умовах сучасних кіберзагроз полягає у необхідності:

1) Системного підходу до побудови КСЗІ, що поєднує правові, організаційні та технічні заходи;
2) Моделювання актуальних загроз для конкретного ОІД з урахуванням його функціонального призначення та ролі у бізнес-процесах;
3) Використання міжнародних стандартів (ISO/IEC 27001, NIST SP 800-53) та їх адаптації до національної нормативної бази [8];
4) Постійної актуалізації методів і засобів захисту, оскільки загрози змінюються швидше, ніж традиційні технології.

Вирішення поставленої проблеми вимагає розробки КСЗІ для типової організації, здатної ефективно реагувати на динаміку кіберзагроз, забезпечувати стійкість бізнес-процесів та знижувати ризики витоку, модифікації чи знищення даних. Саме ці аспекти визначають актуальність подальшого дослідження.

1.2 Статистичні дані щодо порушень інформаційної безпеки в Україні та світі

Статистичні показники останніх років свідчать про стрімке зростання кількості кіберінцидентів як в Україні, так і у світі. За офіційними даними, у 2024 році в Україні було зафіксовано 4 315 кібератак, що на 69,8 % більше, ніж у 2023 році, коли їхня кількість становила 2 541 випадок [9]. Найчастіше під ударами опинялися органи місцевої влади, урядові установи, сектор безпеки та оборони, а також енергетика, комерційні підприємства й телекомунікаційні компанії. Окремо варто відзначити, що лише у першому півріччі 2024 року кількість зафіксованих атак з боку російських угруповань зросла на 19 % у порівнянні з аналогічним періодом попереднього року [10].

За інформацією Департаменту кіберполіції, протягом 2024 року було нейтралізовано 57 організованих злочинних груп (із них 9 – злочинні організації), які налічували 254 учасників та скоїли понад тисячу злочинів у кіберпросторі [11]. Показовим інцидентом стала масштабна атака 19 грудня 2024 року на державні реєстри України, у результаті якої була тимчасово призупинена робота Єдиних та Державних реєстрів, що свідчить про високий рівень уразливості критичної інфраструктури [12].

У глобальному вимірі ситуація є не менш загрозливою. Згідно зі звітом Global Cybersecurity Outlook 2025, кіберзлочинність демонструє сталу тенденцію до зростання завдяки поширенню схем із програмами-вимагачами, застосуванню інструментів штучного інтелекту у шкідливих цілях та еволюції методів обходу захисних систем [13]. За даними міжнародної статистики, у 2023 році понад 8 мільярдів записів було скомпрометовано внаслідок більш як 2 800 випадків витоків даних, а середні витрати на ліквідацію наслідків інцидентів інформаційної безпеки зросли на 15 % у порівнянні з попереднім роком [14]. Ці факти підтверджують, що проблематика кіберзахисту потребує комплексного підходу як на рівні окремих держав, так і в рамках міжнародної співпраці.

1.3 Підстави та загальні положення щодо створення комплексної системи захисту інформації

Створення КСЗІ ґрунтується на правових, організаційних і технічних засадах, які визначають базові принципи формування політики інформаційної безпеки. В Україні необхідність створення КСЗІ випливає з положень Конституції, законодавчих актів, нормативних документів ДСТУ та галузевих стандартів, що регламентують порядок забезпечення конфіденційності, цілісності та доступності інформації [15].

Відповідно до постанови Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», усі суб’єкти, що здійснюють обробку, зберігання чи передачу інформації з обмеженим доступом, зобов’язані впроваджувати організаційно-технічні заходи безпеки [16]. Додатково функціонування КСЗІ має узгоджуватися з положеннями Закону України «Про інформацію», «Про електронні довірчі послуги» та з Національною програмою інформатизації [17].

КСЗІ створюється на основі принципів комплексності, системності та багаторівневості. Це означає, що у процесі її розробки враховуються всі аспекти функціонування ОІД: організаційні структури, технологічні процеси, технічні засоби та кадрові ресурси. Одним із ключових завдань є проведення моделювання загроз і визначення потенційних вразливостей, що дозволяє сформувати обґрунтовані вимоги до архітектури системи [18].

Загальні положення створення КСЗІ передбачають застосування національних та міжнародних стандартів, серед яких: ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53. Ці стандарти закріплюють підхід до управління інформаційною безпекою через політики, процедури та контрольні механізми [19]. Важливим етапом є сертифікація КСЗІ, яка в Україні здійснюється відповідно до Порядку проведення державної експертизи у сфері технічного захисту інформації, затвердженого Держспецзв’язку [20].

Таким чином, підстави для створення КСЗІ формуються на рівні нормативно-правових актів, а загальні положення передбачають системне впровадження заходів безпеки, що забезпечують адекватний захист від актуальних кіберзагроз. Вони є фундаментом подальших етапів розробки – від проєктування до впровадження та експлуатації.

1.4 Вітчизняна нормативно-правова база у сфері захисту інформації

Нормативно-правова база України у сфері захисту інформації сформувалася як відповідь на зростання обсягів обробки даних та необхідність створення належних умов їхнього захисту. Вона включає Конституцію України, закони, підзаконні акти та національні стандарти, що регламентують організаційні, технічні й правові аспекти інформаційної безпеки [15, 16, 17, 20, 21].

Ключовим документом є Конституція України, у якій закріплено право громадян на захист особистих даних та таємницю листування, телефонних розмов і кореспонденції (стаття 31) [15]. На рівні спеціального законодавства базовим є Закон України «Про інформацію», що визначає правові засади створення, поширення, використання та захисту інформації, встановлює категорії доступу й обов’язки суб’єктів у цій сфері [17].

Важливе значення має Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який встановлює вимоги щодо забезпечення безпеки інформації з обмеженим доступом та визначає обов’язки власників і користувачів інформаційних систем [16]. Не менш актуальним є Закон України «Про електронні довірчі послуги», що врегульовує питання електронної ідентифікації, підпису та автентифікації в інформаційних системах [22].

У сфері захисту особистих даних діє Закон України «Про захист персональних даних», яким визначено правові механізми обробки та зберігання інформації про фізичних осіб [23], а також встановлено відповідальність за порушення вимог конфіденційності [24].

Окреме місце займають підзаконні акти, зокрема постанови Кабінету Міністрів України та накази Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ), що регламентують порядок створення КСЗІ, проведення державної експертизи у сфері технічного захисту інформації та сертифікації засобів захисту [20].

Значну роль відіграють національні стандарти, серед яких ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO/IEC 27002:2015, що адаптують міжнародні вимоги до українських реалій [16]. Крім того, у практиці застосовується ДСТУ 8802:2018 «Інформаційні технології. Кібербезпека. Загальні положення» [4].

Таким чином, вітчизняна нормативно-правова база у сфері захисту інформації є багаторівневою та комплексною. Вона створює правове підґрунтя для розробки та впровадження КСЗІ на ОІД, а також визначає відповідальність за порушення правил захисту даних.

1.5 Міжнародні стандарти та вимоги щодо комплексної системи захисту інформації

У сучасних умовах забезпечення кібербезпеки неможливо розглядати лише у межах національної нормативно-правової бази. Інформаційні системи функціонують у глобальному просторі, тому інтеграція у міжнародні стандарти та дотримання світових практик є необхідною умовою ефективного захисту.

Найбільш поширеним міжнародним стандартом є ISO/IEC 27001, який встановлює вимоги до систем управління інформаційною безпекою. Він орієнтований на ризик-орієнтований підхід і передбачає створення комплексу політик, процедур та технічних рішень, що гарантують конфіденційність, цілісність та доступність даних [8]. Доповненням до нього є ISO/IEC 27002, який містить практичні рекомендації з організації заходів безпеки та управління ризиками [18].

Важливе місце займають стандарти серії ISO/IEC 27000, серед яких особливе значення має ISO/IEC 27005, що визначає методичні засади оцінки та управління ризиками інформаційної безпеки [25]. Використання цього стандарту дозволяє організаціям ідентифікувати актуальні загрози, оцінювати ймовірність їх реалізації та визначати рівень можливих збитків.

Окремо слід відзначити документи Національного інституту стандартів і технологій США (NIST). Спеціальна публікація NIST SP 800-53 містить каталог контрольних заходів безпеки для інформаційних систем і стала міжнародним орієнтиром для організацій різних рівнів [19]. Додатково у 2024 році було представлено оновлену редакцію NIST Cybersecurity Framework (CSF) 2.0, яка охоплює п’ять базових функцій – ідентифікацію, захист, виявлення, реагування та відновлення – і пропонує системний підхід до управління ризиками [26].

Міжнародні рекомендації також формуються в рамках діяльності таких організацій, як Міжнародний союз електрозв’язку (ITU) та Європейське

агентство з мережевої та інформаційної безпеки (ENISA). ITU розробляє стандарти у сфері кіберзахисту, що мають глобальний характер і охоплюють питання безпечного обміну даними, криптографічних протоколів та захисту критичної інфраструктури [27]. ENISA, у свою чергу, надає методичні матеріали та рекомендації для країн ЄС, які охоплюють аналіз ризиків, протидію шкідливим програмам та реагування на інциденти [28].

Таким чином, міжнародні стандарти та рекомендації створюють єдине підґрунтя для побудови КСЗІ. Їхнє впровадження дозволяє гармонізувати національні нормативно-правові акти з глобальними вимогами, підвищити рівень стійкості до кіберзагроз і забезпечити інтеграцію у світовий простір кібербезпеки.

1.6 Висновки до першого розділу

У першому розділі було розглянуто теоретичні засади побудови КСЗІ на ОІД. Визначено, що в умовах сучасних кіберзагроз проблема захисту інформації набуває стратегічного значення для держави, бізнесу та суспільства. Масштабність і багатовекторність кібератак, зростання їх складності, а також залучення соціальної інженерії та штучного інтелекту роблять традиційні засоби протидії недостатніми.

Аналіз статистичних даних показав динамічне зростання кількості порушень інформаційної безпеки як в Україні, так і у світі. Особливої уваги потребують критичні об’єкти інфраструктури, державні реєстри, енергетичні та телекомунікаційні системи, які стають основними цілями кібератак. Це підтверджує актуальність системного підходу до побудови КСЗІ.

Було встановлено, що підстави для створення КСЗІ визначаються нормативно-правовими актами України, серед яких Конституція, закони та підзаконні документи, а також національні стандарти у сфері кібербезпеки. Вони формують багаторівневу нормативну базу, що забезпечує правові та організаційні умови для впровадження систем захисту інформації. Водночас Україна орієнтується на гармонізацію з міжнародними стандартами, такими як ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 та документи NIST і ENISA, що дозволяє адаптувати найкращі світові практики.

Загалом, проведений огляд підтверджує, що ефективна побудова КСЗІ можлива лише за умови комплексного поєднання правових, організаційних і технічних заходів, а також регулярного оновлення системи відповідно до змін у середовищі загроз. Результати розділу створюють методологічне підґрунтя для подальших досліджень, спрямованих на розробку практичних методів і засобів побудови КСЗІ типового ОІД.

Розділ 2. МЕТОДОЛОГІЯ СТВОРЕННЯ КОСПЛЕКСТНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

2.1 Класифікація об'єктів інформаційної діяльності та вимоги до їх захисту

ОІД – інженерно-технічна споруда (приміщення), транспортний засіб, де провадиться діяльність, пов'язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом [29]. Залежно від масштабів функціонування, характеру даних та ступеня критичності для суспільства та держави вони класифікуються за кількома ознаками.

По-перше, виділяють державні об'єкти, що обробляють інформацію з обмеженим доступом, зокрема дані, які становлять державну таємницю або належать до категорії службової інформації. До них відносяться інформаційні системи органів державної влади, сектору безпеки й оборони, а також критична інфраструктура держави [30].

По-друге, виокремлюють комерційні та корпоративні об'єкти, де основним ресурсом є комерційна таємниця, фінансові дані та результати науково-дослідних і конструкторських робіт. Вразливість цих об'єктів полягає у високій залежності від конфіденційності бізнес-процесів та конкурентоспроможності [31].

Окрему категорію становлять об'єкти соціальної сфери, такі як заклади освіти, охорони здоров'я та комунальні підприємства. Тут пріоритетним є захист персональних даних громадян та забезпечення доступності інформаційних сервісів [32].

Залежно від характеру даних, ОІД поділяються також на ті, що обробляють персональні дані, фінансову інформацію, дані критичної інфраструктури, інтелектуальну власність. Для кожної категорії визначаються окремі вимоги безпеки відповідно до законодавства України та міжнародних норм. Наприклад, для державних систем обов'язковим є проходження

державної експертизи у сфері технічного захисту інформації [20], тоді як для комерційних структур пріоритетом виступає впровадження систем управління інформаційною безпекою за ISO/IEC 27001 [8].

Загальні вимоги до захисту ОІД можна сформулювати за такими напрямами:

1) Конфіденційність – запобігання несанкціонованому доступу до даних.
2) Цілісність – недопущення модифікації чи знищення інформації без дозволу.
3) Доступність – забезпечення безперервного функціонування інформаційних систем.
4) Відповідальність і підзвітність – встановлення механізмів контролю та ідентифікації дій користувачів.
5) Стійкість – здатність системи протистояти атакам і відновлювати роботу після інцидентів [33].

Таким чином, класифікація ОІД дозволяє диференціювати вимоги до їхнього захисту залежно від значущості даних і функцій, що виконуються. Це є основою для розробки КСЗІ, здатних відповідати як національним, так і міжнародним стандартам.

2.2 Етапи створення комплексної системи захисту інформації: аналіз загроз, моделювання порушника, визначення політики безпеки

КСЗІ передбачає реалізацію низки взаємопов'язаних етапів, які забезпечують системний підхід до розробки й впровадження заходів безпеки. Ключовими серед них є аналіз загроз, моделювання порушника та формування політики безпеки.

Аналіз загроз передбачає виявлення потенційних і актуальних факторів, що можуть спричинити порушення конфіденційності, цілісності чи доступності інформації. На цьому етапі здійснюється інвентаризація інформаційних активів, визначення їх критичності та оцінка можливих наслідків реалізації загроз. Методи аналізу включають експертні опитування, аналіз інцидентів, а також використання методик міжнародних стандартів, зокрема ISO/IEC 27005 [25]. Практика показує, що систематичний моніторинг дозволяє не лише виявляти відомі загрози, а й прогнозувати появу нових [34].

Моделювання порушника є наступним кроком, що дозволяє визначити потенційні сценарії атак. У цьому контексті виділяють внутрішніх і зовнішніх порушників. Внутрішніми вважаються співробітники чи підрядники, які мають легальний доступ до системи, а зовнішніми – хакерські угруповання, конкурентні організації чи державні актори [35]. При моделюванні враховуються мотивація, ресурси, технічні можливості та потенційні цілі зловмисника. Цей підхід дозволяє сформувати більш реалістичну модель захисту, орієнтовану на пріоритетні ризики [36].

Визначення політики безпеки є завершальним етапом початкового циклу створення КСЗІ. Політика безпеки – це сукупність правил, процедур і технічних вимог, що регламентують порядок обробки інформації та доступу до неї [37]. Її розробка ґрунтується на результатах аналізу загроз і моделювання порушника, а також враховує вимоги чинного законодавства та міжнародних стандартів [8; 18; 26]. Політика має охоплювати як організаційні заходи (регламенти доступу, розподіл повноважень, навчання персоналу), так і

технічні аспекти (автентифікація, шифрування, резервне копіювання, моніторинг подій).

Ефективна політика безпеки повинна бути гнучкою, тобто здатною адаптуватися до змін у середовищі загроз, а також інтегрованою у всі бізнес-процеси організації. Лише за умови послідовного виконання зазначених етапів можна сформувати КСЗІ, що відповідає сучасним викликам і забезпечує належний рівень захисту інформаційних ресурсів.

2.3 Засоби та методи технічного, програмного, криптографічного і організаційного захисту інформації

Ефективність КСЗІ визначається збалансованим поєднанням технічних, програмних, криптографічних та організаційних заходів. Кожна з цих складових спрямована на реалізацію принципів конфіденційності, цілісності та доступності даних, проте має власні завдання та інструменти.

Апаратні та програмні рішення забезпечують протидію технічним каналам витоку даних та блокування несанкціонованого доступу. До них належать системи міжмережевих екранів, засоби виявлення та запобігання вторгненням (IDS/IPS), антивірусне програмне забезпечення, системи резервного копіювання та відновлення, засоби контролю доступу до фізичних і віртуальних ресурсів [38]. Важливу роль відіграють також системи моніторингу подій інформаційної безпеки (SIEM), які дозволяють здійснювати аналіз інцидентів у режимі реального часу [39].

Криптографічні методи захисту спрямовані на забезпечення конфіденційності та цілісності даних у процесі їх зберігання й передавання. До базових належать симетричне та асиметричне шифрування, цифровий підпис, хешування, протоколи обміну ключами та багатофакторна автентифікація [40]. На практиці широко використовуються стандарти AES, RSA, SHA-2/3, протоколи TLS та IPsec. У контексті сучасних викликів актуальними стають постквантові алгоритми, що розробляються в рамках ініціативи NIST PQC [41].

Організаційні заходи є основою будь-якої КСЗІ, оскільки технічні та криптографічні рішення будуть малоефективними без належної політики управління. До організаційних методів відносять розробку внутрішніх регламентів доступу до інформації, контроль за дотриманням політик безпеки, підготовку та навчання персоналу, проведення аудитів і тестувань на проникнення [42]. Важливим елементом є управління інцидентами – визначення процедур виявлення, реагування та відновлення після кібератак, що узгоджується з міжнародними стандартами ISO/IEC 27035 [43].

Таким чином, технічні, програмні, криптографічні та організаційні заходи захисту інформації не є взаємовиключними, а формують інтегровану систему, здатну забезпечити належний рівень кіберстійкості. Їхнє узгоджене використання дозволяє мінімізувати ризики реалізації загроз та підвищити надійність функціонування інформаційних систем.

2.4 Порядок впровадження створення комплексної системи захисту інформації та проходження державної експертизи

Впровадження КСЗІ є багатоступеневим процесом, що охоплює організаційні, технічні та правові заходи, спрямовані на створення ефективного середовища безпеки інформаційних ресурсів. В Україні цей процес регламентований ДССЗЗІ і передбачає обов'язкове проведення державної експертизи у сфері технічного захисту інформації.

На практиці можна виділити кілька ключових етапів упровадження:

1) Ініціація проекту: На початковій стадії керівництво організації ухвалює рішення про створення КСЗІ, формує робочу групу та визначає відповідальних осіб. Визначаються основні завдання, об'єкти захисту та попередні вимоги до рівня безпеки.
2) Обстеження інформаційної системи: Виконується аналіз існуючої інфраструктури, обсягів оброблюваної інформації та її категорій. На цьому етапі складається технічне завдання на розробку КСЗІ, у якому формалізуються вимоги до захисту [44].
3) Моделювання загроз і визначення вимог: Відповідно до чинних методичних документів ДССЗЗІ розробляється модель загроз та модель порушника. Це дозволяє встановити перелік необхідних організаційних і технічних заходів безпеки [37].
4) Розробка проектної документації: Проект КСЗІ оформлюється у вигляді набору документів: технічне завдання, технічний проект, експлуатаційна документація, план реагування на інциденти, положення про політику безпеки тощо [45].
5) Впровадження технічних і організаційних заходів: На цьому етапі встановлюються апаратно-програмні комплекси (системи контролю доступу, криптографічні засоби, засоби виявлення атак), впроваджуються регламенти адміністрування, проводиться навчання персоналу.

6) Попереднє тестування та внутрішній аудит: Проводяться перевірки на відповідність реалізованих рішень технічному завданню та нормативним вимогам. Виконуються тестування на проникнення, аудит конфігурацій, контроль ефективності криптографічних засобів [37].
7) Проведення державної експертизи: Відповідно до законодавства, КСЗІ, що функціонує в інформаційних системах, де обробляється інформація з обмеженим доступом, підлягає обов'язковій державній експертизі. Експертиза проводиться уповноваженими установами та завершується висновком про відповідність чи невідповідність вимогам нормативних документів [20].
8) Введення в експлуатацію. Після отримання позитивного висновку експертизи КСЗІ вводиться в промислову експлуатацію. Власник системи затверджує внутрішні нормативні документи, а також організовує моніторинг та підтримку працездатності засобів захисту.

Державна експертиза у сфері технічного захисту інформації виконує роль інструмента незалежного контролю якості реалізації КСЗІ. Вона здійснюється на підставі «Порядку проведення державної експертизи у сфері технічного захисту інформації», затвердженого ДССЗЗІ [20].

Під час експертизи перевіряється:

- Відповідність проектної документації вимогам нормативних актів;
- Наявність і правильність реалізації моделі загроз та моделі порушника;
- Ефективність організаційних заходів (наявність політики безпеки, регламентів, інструкцій);
- Працездатність та відповідність криптографічних засобів захисту (вони повинні бути сертифіковані в Україні);
- Результати тестувань на проникнення та аудиту інформаційної системи [46].

Експертиза може мати кілька результатів:

- Позитивний висновок – КСЗІ відповідає вимогам і може бути введена в експлуатацію;

- Умовно позитивний висновок – виявлені незначні недоліки, що підлягають усуненню у встановлений термін;
- Негативний висновок – система не відповідає вимогам, потребує доопрацювання та повторного подання на експертизу.

Важливим аспектом є те, що впровадження КСЗІ не завершується етапом експертизи. Система потребує постійного супроводу, моніторингу та актуалізації заходів захисту. Це включає регулярний перегляд політик безпеки, оновлення програмного забезпечення, повторні аудити та повторне проходження експертизи у разі значних змін в інформаційній системі [47].

Таким чином, порядок упровадження КСЗІ в Україні базується на підході, що охоплює всі стадії життєвого циклу системи – від аналізу ризиків і розробки проекту до впровадження, експертизи та подальшої підтримки. Ключову роль у цьому процесі відіграє державна експертиза, яка гарантує дотримання єдиних вимог та стандартів у сфері захисту інформації.

2.5 Приклади реалізації створення комплексної системи захисту інформації на практиці

Практична реалізація КСЗІ дозволяє наочно продемонструвати ефективність теоретичних положень та нормативних вимог, розглянутих раніше. Аналіз конкретних прикладів підтверджує, що побудова КСЗІ має багатовимірний характер і залежить від галузі застосування, масштабів діяльності та рівня ризиків, притаманних певному ОІД.

В Україні одним із значущих масштабних прикладів побудови КСЗІ стали державні інформаційні ресурси, зокрема системи електронного урядування та електронних послуг. Створення системи «Дія» супроводжувалося впровадженням комплексу захисту, що включає криптографічні засоби національної розробки, багатофакторну автентифікацію, сегментацію мережевої інфраструктури та централізований моніторинг інцидентів безпеки. За повідомленням Міністерства цифрової трансформації, КСЗІ у «Дії» сертифікована ДССЗЗІ та відповідає вимогам національних стандартів у сфері кібербезпеки [48].

Інший приклад – система електронних державних реєстрів, зокрема Єдиний державний демографічний реєстр та реєстр актів цивільного стану. Тут основний акцент зроблено на захисті персональних даних. Використовуються криптографічні протоколи, сертифіковані засоби електронного підпису та контроль доступу з багаторівневою ідентифікацією користувачів [49]. Попри складність архітектури, державна експертиза підтвердила відповідність системи вимогам, що дозволило забезпечити безпечну інтеграцію з іншими державними платформами.

Особливу увагу заслуговує банківський сектор. В Україні банки зобов’язані впроваджувати КСЗІ відповідно до вимог Національного банку України, які передбачають використання міжнародних стандартів ISO/IEC 27001 та ISO/IEC 27005. У ПриватБанку та Ощадбанку реалізовані комплексні системи моніторингу та управління ризиками, інтегровані із системами

протидії шахрайству (anti-fraud). Ключовими елементами стали системи SIEM, які збирають журнали подій у режимі реального часу, та інструменти поведінкової аналітики для виявлення нетипових дій користувачів [50].

До сфери критичної інфраструктури належить енергетика. Відомим прикладом є впровадження КСЗІ на підприємствах НЕК «Укренерго». Після кібератак 2015–2016 років, що призвели до відключення електроенергії у кількох регіонах, система була суттєво модернізована. Було впроваджено ізольовані сегменти мереж, централізовані центри реагування на інциденти (SOC), резервні канали управління, а також системи захисту промислових протоколів (SCADA) [51]. Цей приклад показує, що побудова КСЗІ на об’єктах критичної інфраструктури має відмінності від класичних корпоративних систем і вимагає поєднання IT- та OT-безпеки.

У сфері охорони здоров’я прикладом є система eHealth, яка об’єднує державні й приватні медичні заклади. Її КСЗІ сертифікована ДССЗЗІ та побудована з акцентом на захист персональних медичних даних, що належать до категорії чутливої інформації. Система включає криптографічний захист каналів зв’язку, обмеження доступу за ролями та обов’язкове використання кваліфікованого електронного підпису при внесенні даних [52]. Важливим елементом стало впровадження механізму псевдонімізації даних, що значно зменшує ризик ідентифікації пацієнтів у разі витоку.

Міжнародна практика також демонструє приклади ефективного впровадження КСЗІ. У Європейському Союзі впровадження вимог директиви NIS2 змусило операторів критичних послуг адаптувати свої системи до єдиних стандартів. Наприклад, у Німеччині енергетичні компанії створили національні центри обміну інформацією про інциденти, що дозволяє швидко реагувати на масштабні атаки [53]. У США великі телекомунікаційні корпорації впроваджують КСЗІ на основі NIST Cybersecurity Framework 2.0, використовуючи ризик-орієнтований підхід та обов’язкову перевірку постачальників [54].

Приклади показують, що у різних галузях акценти в побудові КСЗІ можуть суттєво відрізнятися. У банківському секторі домінують вимоги до безперервності обслуговування та протидії шахрайству, в енергетиці – захист промислових систем управління, в охороні здоров’я – забезпечення конфіденційності персональних даних, у державному управлінні – відповідність вимогам національного законодавства та інтеграція міжвідомчих систем. Спільним є те, що всі ці системи базуються на комбінації технічних, криптографічних і організаційних заходів, а також на використанні міжнародних стандартів.

Таким чином, реальні приклади підтверджують, що побудова КСЗІ є не лише вимогою законодавства, а й практичною необхідністю, без якої сучасні організації не здатні забезпечити кіберстійкість та виконання критично важливих функцій. Досвід впровадження у різних галузях дозволяє виробити рекомендації для типового ОІД, що стане предметом подальшого розгляду у наступному розділі.

2.6 Висновки до другого розділу

У другому розділі було детально розглянуто методологію створення КСЗІ на ОІД. Насамперед була проаналізована класифікація таких об’єктів та окреслені вимоги до їхнього захисту. Було встановлено, що специфіка КСЗІ залежить від категорії даних, які обробляються, від ролі об’єкта в державних або корпоративних процесах, а також від рівня критичності для безперервності функціонування суспільних систем.

Окрему увагу приділено етапам побудови КСЗІ, серед яких ключовими є аналіз загроз, моделювання порушника та визначення політики безпеки. Було показано, що формування адекватної моделі загроз і реалістичного профілю порушника є основою для побудови дієвої політики безпеки, яка поєднує організаційні та технічні заходи. Важливим є врахування внутрішніх і зовнішніх факторів ризику, що забезпечує цілісність і практичну спрямованість системи.

Розглянуті засоби технічного, програмного, криптографічного та організаційного захисту доводять, що ефективна КСЗІ має ґрунтуватися на інтеграції цих компонентів. Технічні та програмні інструменти дозволяють протидіяти вторгненням і забезпечувати моніторинг, криптографічні методи гарантують конфіденційність і цілісність даних, а організаційні заходи забезпечують належне управління, підзвітність та підготовку персоналу.

Особливе значення надано порядку впровадження КСЗІ та процедурі державної експертизи. Було підкреслено, що проходження експертизи є обов’язковою умовою для систем, які обробляють інформацію з обмеженим доступом. Державна експертиза виконує роль незалежного контролю, підтверджує відповідність системи вимогам нормативних документів і гарантує належний рівень захищеності.

Практичні приклади реалізації КСЗІ в державному управлінні, банківському секторі, енергетиці та охороні здоров’я засвідчили, що побудова таких систем є не лише законодавчою вимогою, а й критичною умовою

забезпечення кіберстійкості. Цей досвід показав, що комплексний підхід із використанням міжнародних стандартів і гармонізацією із національними вимогами є найефективнішим.

Узагальнюючи, можна зробити висновок, що методологія створення КСЗІ повинна поєднувати системний підхід, нормативне підґрунтя, сучасні технічні й криптографічні засоби, організаційні заходи та практичну перевірку ефективності. Такий підхід забезпечує стійкість до сучасних кіберзагроз і створює основу для подальшого розвитку безпечних інформаційних систем на рівні як держави, так і приватного сектору.

Розділ 3. МОДЕЛЬ ПОБУДОВИ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ТИПОВОГО ОБ'ЄКТА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1 Загальні відомості про організацію

Об'єктом дослідження є приміщення умовного підприємства ТОВ «ЕнергоТрансЛогістика» ОІД, що здійснює діяльність у сфері транспортної логістики та енергетичного забезпечення інфраструктурних об'єктів. Організація поєднує у собі функції класичного логістичного оператора та підприємства, відповідального за експлуатацію локальних енергетичних систем, що дозволяє забезпечувати комплексне обслуговування клієнтів у сфері перевезення та зберігання енергетичних і промислових ресурсів.

Підприємство має головний офіс у місті Київ та три регіональні представництва у Львові, Одесі та Дніпрі. Географічне розташування філій дає змогу охоплювати основні транспортні коридори країни та забезпечувати оперативність логістичних операцій. Загальна чисельність співробітників становить близько 550 осіб, серед яких адміністративно-управлінський персонал, ІТ-фахівці, спеціалісти з безпеки, диспетчери, логісти, водії, оператори складських комплексів, енергетики та технічні інженери.

Організаційна структура підприємства включає кілька ключових підрозділів:

- Дирекція – здійснює стратегічне управління компанією та приймає рішення щодо розвитку;
- ІТ-відділ – відповідає за підтримку інформаційних систем, адміністрування мереж, впровадження нових технологій та захист даних;
- Логістичний відділ – координує транспортні перевезення, маршрути, складування;
- Фінансово-економічний відділ – займається бухгалтерським обліком, плануванням та розрахунками;

- Відділ енергетичних систем – забезпечує моніторинг і підтримку роботи локальних енергетичних об’єктів;
- Відділ безпеки – відповідає за фізичну охорону об’єктів та координацію дій у сфері інформаційної безпеки.

Інформаційна інфраструктура підприємства складається з низки взаємопов’язаних систем, які забезпечують виконання бізнес-процесів. Основними серед них є:

1) Автоматизована логістична система (ALS) – використовується для планування маршрутів, управління транспортними засобами, відстеження їхнього переміщення в реальному часі, а також для оптимізації витрат пального.
2) Корпоративна ERP-система – інтегрує облік фінансів, управління персоналом, складські операції, контракти з постачальниками та клієнтами.
3) SCADA-система локальних енергетичних вузлів – забезпечує управління генераторами, трансформаторами, системами резервного енергопостачання складів та логістичних терміналів.
4) Система електронного документообігу (СЕД) – використовується для створення, погодження та зберігання документів із використанням кваліфікованого електронного підпису.
5) CRM-система – дозволяє відстежувати роботу з клієнтами, фіксувати історію угод, обробляти персональні дані замовників.

Категорії інформації, що обробляються в організації, охоплюють широкий спектр:

- Комерційна інформація – договори, контракти, бізнес-плани, інформація про логістичні маршрути, закупівлі та постачання;
- Фінансова інформація – бухгалтерські звіти, транзакції, податкові документи;
- Персональні дані – відомості про співробітників, клієнтів і підрядників;

- Оперативні дані енергетичної інфраструктури – показники роботи систем енергозабезпечення складів і терміналів;
- Інформація з обмеженим доступом – внутрішні аналітичні звіти, тендерна документація, аудиторські висновки.

На даний час інформаційна безпека на підприємстві реалізована лише частково. Використовуються стандартні антивірусні продукти, базові міжмережеві екрани, резервне копіювання даних та політики паролів. Проте відсутня єдина інтегрована система захисту, що створює ризики: можливість несанкціонованого доступу до корпоративних даних, витік комерційної та персональної інформації, порушення цілісності критичних даних у SCADA-системах, а також перебої у роботі ERP та CRM через кібератаки. Виявлені проблеми свідчать про актуальну необхідність побудови сертифікованої КСЗІ, яка б відповідала національним та міжнародним вимогам у сфері кіберзахисту.

Загалом, підприємство «ЕнергоТрансЛогістика» може бути віднесене до категорії ОІД підвищеної критичності, оскільки його діяльність пов’язана з управлінням транспортними й енергетичними процесами, що впливають на економічну безпеку країни. Це обумовлює необхідність впровадження КСЗІ, яка б забезпечила:

1. Конфіденційність – захист комерційної, фінансової та персональної інформації від витоку.
2. Цілісність – недопущення спотворення або несанкціонованої модифікації даних.
3. Доступність – забезпечення безперервного функціонування логістичних і енергетичних систем.
4. Підзвітність – можливість ідентифікації дій користувачів та контролю за їх виконанням.
5. Стійкість – здатність інформаційних систем протистояти сучасним кібератакам та відновлювати працездатність після інцидентів.

Таким чином, «ЕнергоТрансЛогістика» є типовим прикладом підприємства, яке потребує створення КСЗІ.

3.2 Обстеження інформаційно-телекомунікаційної системи

Метою обстеження є формалізація меж ІТС головного офісу ТОВ «ЕнергоТрансЛогістика» у місті Київ, інвентаризація його активів, побудова карти інформаційних потоків, оцінка наявних засобів захисту, виявлення вразливостей і невідповідностей вимогам політики безпеки, а також підготовка вихідних даних для моделювання загроз і проєктування КСЗІ.

Обстеження виконувалося для офісної будівлі підприємства у м. Київ, що розташована в центральній частині міста та виконує функції адміністративного центру компанії. Саме цей офіс розглядається як типовий ОІД, оскільки він містить усі основні елементи інфраструктури, притаманні також філіям у Львові, Одесі та Дніпрі. У будівлі розміщено адміністративні кабінети, серверну кімнату (ЦОД), зону ІТ-відділу, переговорні приміщення, логістичний диспетчерський центр і локальні технічні вузли зв’язку.

1. Межі та склад ІТС (логічні та фізичні).

1) Центр обробки даних (ЦОД) розташований у виділеному приміщенні серверної на другому поверсі офісу. Він включає кластер віртуалізації, сервери прикладних систем ALS, ERP, СЕД, CRM, сервери баз даних, файлові та резервні сервери, контролери домену. Для підтримання безперебійної роботи використовується система живлення N+1, ДБЖ, дизельний генератор і система кондиціонування.
2) Локальні мережеві вузли офісу об’єднані у корпоративну мережу з ядром рівня L3, маршрутизаторами, комутаторами доступу та бездротовими точками Wi-Fi. Усі сегменти логічно розмежовані VLAN-ами, а периметр захищено NGFW із вбудованими IPS-модулями.
3) Периферія – робочі місця співробітників, офісні системи контролю доступу, відеоспостереження, принтери, сканери, IP-телефонія.
4) Периферійні пристрої охоплюють робочі місця співробітників (адміністрація, фінанси, ІТ, логістика), системи контролю доступу,

відеоспостереження, принтери, сканери, вагові термінали та пристрої маркування документів.

5) OT-сегмент представлений диспетчерським пунктом керування системою енергозабезпечення офісу (резервне живлення, генератори, кондиціонери). У ньому застосовуються контролери Siemens S7, HMI-панелі Weintek та шлюзи OPC-UA. OT-мережа фізично відокремлена від ITC, з'єднання реалізоване через шлюз із гальванічною розв'язкою.
6) Хмарні та зовнішні сервіси: корпоративний офісний пакет SaaS (Microsoft 365, Google Workspace), сервіси електронного підпису (Дія.Sign), інтеграція з банківськими API та резервне копіювання у S3-сховище.
7) Канали зв'язку: два незалежні інтернет-канали (оптичний 1 Гбіт/с і LTE-резерв), VPN-канали до віддалених філій поверх IPsec.

2. Інвентаризація активів (узагальнено):

- Обчислювальні ресурси: 10 фізичних серверів у ЦОД (дві стійки, живлення N+1), близько 120 віртуальних машин.
- Сховище даних: два масиви SAN із синхронною реплікацією всередині ЦОД та асинхронною реплікацією до резервного вузла у Львові.
- Бази даних: PostgreSQL (ALS, CRM), MS SQL (ERP, СЕД), окремі інстанси для систем телеметрії.
- Робочі місця: близько 160 ПК Windows 11 Pro, 20 робочих станцій Ubuntu LTS, 40 корпоративних ноутбуків, 70 смартфонів співробітників, які використовують корпоративну пошту та CRM.
- Мережеве обладнання: комутатори ядра Cisco Catalyst, розподільчі вузли Aruba, точки доступу Wi-Fi (понад 40), NGFW, IPS-система та контролер бездротової мережі.
- OT-компоненти: 8 контролерів PLC/RTU, 3 HMI-панелі, 1 промисловий маршрутизатор і сервер диспетчерського моніторингу.

- Програмне забезпечення: ERP, ALS, СЕД, CRM, SCADA, антивірус / EDR, системи резервного копіювання, гіпервізори, засоби віддаленого доступу.
- Документація: топологічні схеми, реєстр активів, карти доступів, матриці ролей, журнали змін, інструкції користувачів, договори з постачальниками.

Таким чином, у межах головного офісу в місті Київ визначено повний склад і межі ІТС, що відображає архітектуру типового ОІД підприємства.

3. Логічна сегментація і топологія мережі (цільова модель і поточний стан):

- Зони довіри: Perimeter DMZ (зовнішні веб-шлюзи, API-шлюзи), Server Zone (БД/додатки), Management Zone (AD, PKI, системи моніторингу), User LAN (офісні ПК), Corp-Wi-Fi та Guest-Wi-Fi (ізольований), OT-Zone (SCADA/PLC), OT-DMZ (брокери даних між OT та IT), SOC/SIEM Zone.
- Маршрутизація: динамічна IGP усередині локальної офісної мережі; міжзонова взаємодія – виключно через NGFW із застосуванням L7-правил.
- Доступ до інтернету: симетричні канали, актив-актив, DDoS-фільтрація на боці провайдера, вихід користувачів через проксі з TLS-інспекцією для визначених категорій.
- Поточні відхилення: у межах офісної мережі виявлено кілька VLAN із некоректними ACL і статичними маршрутами; гостьова Wi-Fi мережа має трасу до внутрішнього DNS через неправильний ACL.

4. Класифікація інформації та карти відповідності «дані–система–власник»:

- Персональні дані співробітників і клієнтів: СЕД/ERP/CRM; власники: HR-директор, керівник клієнтського сервісу.
- Комерційна таємниця (контракти, ціноутворення, маршрути): ERP/ALS/файлові шари; власники: комерційний директор, директор логістики.

- Фінансова інформація: ERP/банківські інтеграції; власник: CFO.
- Технологічні дані OT: SCADA/телеметрія; власник: директор з енергетики.
- Журнали безпеки: SIEM/журнали; ОС/мережеві логи; власник: CISO.

Для кожної категорії визначені рівні чутливості, вимоги до зберігання, шифрування, журналювання та строків знищення.

5. Карта інформаційних потоків (ключові сценарії):

- ALS ↔ мобільні додатки водіїв: телеметрія маршруту, підтвердження точок доставки (TLS з клієнтськими сертифікатами).
- ERP ↔ банк/API платіжних шлюзів: платіжні доручення, виписки (взаємна TLS-автентифікація, журналювання в SIEM).
- СЕД ↔ зовнішній ЕЦП-провайдер: підписання документів, валідація сертифікатів.
- SCADA → OT-DMZ → брокер даних → ALS/аналітика: тільки односпрямована передача технологічних показників через дата-діод або еквівалентний шлюз.
- Офісний SaaS ↔ User LAN: синхронізація пошти/дисків, політики DLP для чутливих міток.

6. Ідентифікація та автентифікація, керування доступом:

- Каталог: один ліс AD, дві доменні зони (hq.local, branches.local), гібридна інтеграція з хмарною ідентичністю; SSO для основних бізнес-додатків.
- MFA: увімкнено для віддаленого доступу та критичних адміністративних ролей; для частини офісних користувачів – план розширення.
- RBAC/ABAC: матриці ролей у ERP/СЕД/SCADA, розділення обов’язків (SoD) для фінансових операцій; немає централізованого PAM для адміністраторів.

- Вади: паролі сервісних облікових записів у застарілих скриптах, відсутній регулярний огляд прав доступу на файлових шарах, локальні адміни на частині ноутбуків.

7. Захист кінцевих точок та серверів:

- Антивірус/EDR: на ПК – EDR з поведінковою аналітикою, але без вмикання ізоляції мережі; на серверах – базовий AV, EDR не всюди.
- Базові конфігурації: CIS-шаблони частково, увімкнені BitLocker/TDE не на всіх цільових системах; PowerShell Constrained Language Mode відсутній.
- Патч-менеджмент: щомісячні вікна, але для частини OT-компонентів – відкладення без виняткових компенсуючих контролів.

8. Криптографічний захист і управління ключами:

- TLS 1.2/1.3 для зовнішніх сервісів, внутрішні: місцями з TLS 1.0/1.1 на старих вузлах; взаємна автентифікація тільки на критичних інтеграціях.
- Шифрування на носіях: BitLocker на ноутбуках керівників і польових пристроях, TDE у частині БД; резервні копії шифруються перед відправкою до S3-сховища.
- PKI: внутрішній Root/Issuing CA, не описані процедури компро-та ротації; журнали видачі сертифікатів не інтегровані в SIEM.

9. Резервне копіювання і відновлення, безперервність бізнесу:

- Стратегія 3–2–1 реалізована частково: щоденні інкрементальні, щотижневі повні, копія в S3-сумісному сховищі; тестові відновлення виконуються раз на квартал вибірково.
- Орієнтовні RTO/RPO: для ERP – 8 год/4 год, для ALS – 4 год/1 год, для SCADA – 1 год/15 хв; фактичні вправи показали невідповідність ERP-RTO.
- Відсутні оформлені BIA для окремих підрозділів, план аварійного перемикання мережевого периметра не протестований під навантаженням.

10. Моніторинг, журналювання, реагування на інциденти:

- Логи ОС/додатків збираються в центральний SIEM для 70–75 % вузлів; OT-логи залишаються локально, кореляційні правила для SCADA не впроваджені.
- Зберігання журналів: 90 днів онлайн, 1 рік у холодному архіві; для операцій підпису й фінансових транзакцій – 3 роки.
- SOC-процеси: існують плейбуки для фішингу, виявлення шифрувальників, підозрілих привілеїв; відсутній формальний процес lessons learned і обов'язковий post-incident review.

11. Вразливості та невідповідності (витяг з gap-аналізу):

- Мережа філій частково не сегментована – загроза бічного переміщення.
- Відсутній PAM і контроль сесій адміністраторів – ризик ескалації привілеїв.
- Неповне шифрування на дисках серверів БД – ризик компрометації даних при фізичному доступі/втраті носія.
- Гостевий Wi-Fi має доступ до внутрішнього DNS – ризик спуфінгу/розвідки.
- OT-оновлення «пакетами» без ізоляції тестового стенду – ризик простою технологічних процесів.
- Неповний інвентар мобільних пристроїв і BYOD-політики – ризик витоку через некеровані ендпойнти.
- Неповний набір SPF/DKIM/DMARC на доменах філій – ризик бізнес-компрометації листування.
- Відсутній процес регулярного огляду доступів (QRB) – накопичення надлишкових прав.

12. Оцінка ризиків (початковий реєстр):

1) Компрометація облікових записів адміністраторів без PAM – висока ймовірність, високий вплив.

2) Бічний рух у філіях через відсутність мікросегментації – середня ймовірність, високий вплив.
3) Витік персональних/комерційних даних через незашифровані сховища – середня, високий.
4) Зупинка SCADA через некоректні оновлення – низька–середня, дуже високий.
5) Phishing/Business Email Compromise за відсутності повного DMARC – висока, середній–високий.
6) Компрометація мобільних застосунків водіїв – середня, середній–високий.
7) Недостатність журналювання OT-подій – середня, високий (затримка реагування).
8) Відмова резервного відновлення ERP у межах RTO – середня, високий (простій фіноперацій).
9) Витік через гостевий Wi-Fi/ACL-помилки – середня, середній.
10) Невчасні патчі критичних сервісів – середня, середній–високий.

13. Початковий план усунення невідповідностей і пріоритезація (T0–T180):

1) T0–T30:

- Відокремити серверні VLAN у філіях, закрити гостьові ACL до внутрішнього DNS, увімкнути Network Access Control для Corp-Wi-Fi.
- Увімкнути BitLocker/TDE на всіх пріоритетних вузлах БД і ноутбуках керівництва; розгорнути централізоване керування ключами.
- Упровадити SPF/DKIM/DMARC на всіх доменах, MFA для всіх віддалених доступів.

2) T30–T90:

- Запровадити PAM із записом сесій і JIT-доступом; впровадити QRB – щоквартальні огляди прав.
- Розгорнути EDR на серверах додатків, увімкнути політику ізоляції ендпойнтів за індикаторами компрометації.

- Виділити OT-DMZ і кореляційні правила в SIEM для SCADA-подій, уніфікувати час/синхронізацію NTP для точності журналів.

3) T90–T180:

- Побудувати тестовий стенд OT для перевірки оновлень, затвердити регламент змін (CAB для OT).
- Провести BIA по підрозділах, актуалізувати RTO/RPO, розробити та відпрацювати сценарії DR для ERP/ALS.
- Впровадити DLP для мічених даних у СЕД/офісному SaaS, розширити SSO та політики умовного доступу.

14. Процеси та регламенти, що потребують затвердження:

- Політика ІБ і дочірні стандарти (класифікація даних, шифрування, управління обліковими записами, робота з постачальниками).
- Процедури управління вразливостями й патчами, CAB/Change-management з розмежуванням IT/OT.
- Incident Response Plan та плейбуки SOC, порядок зберігання та надання журналів.
- Політики BYOD/MDM, правила користування мобільними застосунками, вимоги до захисту даних на пристроях.
- BCP/DRP: порядок резервування, тестів відновлення, аудитів безперервності.
- Постачальники/треті сторони: анкети безпеки, вимоги до шифрування каналів і зберігання журналів, право аудиту.

15. Метрики ефективності (KPI/KRI) для подальшого моніторингу:

- Частка активів під EDR та централізованим журналюванням – ≥95 %.
- Час закриття критичних патчів – ≤7 днів (IT), ≤30 днів (OT з компенсуючими контролями).
- Відсоток інцидентів, виявлених автоматично SIEM/SOAR – ≥85 %.
- Середній час виявлення/реагування (MTTD/MTTR) – тренд до зниження на ≥20 % за квартал після впровадження.

- Частка зашифрованих сховищ для пріоритетних даних – 100 %.
- Успішність тестових відновлень у межах RTO/RPO – 100 % на вибірці критичних систем.
- Покриття MFA для користувачів і адміністраторів – 100 %.

16. Ролі та відповідальності:

- Власники активів даних – затверджують рівні чутливості, права доступу, строки зберігання.
- CISO/SOC – моніторинг, інцидент-менеджмент, тестування контролів, звітність керівництву.
- IT-експлуатація – конфігурація мереж/серверів, патчі, резервне копіювання, виконання CAB.
- OT-інженерія – безпека SCADA/PLC, зміни через стенд, взаємодія з вендорами.
- Користувачі – дотримання політик, обов'язкове навчання і фішинг-тренінги.
- Постачальники – виконання вимог до безпеки, журналювання, повідомлення про інциденти у встановлені строки.

17. Підсумки обстеження:

ІТС підприємства є розгалуженою гібридною екосистемою з поєднанням корпоративних IT-сервісів і технологічних OT-підсистем. Критичні бізнес-процеси підтримуються набором систем, для яких наявні захисні заходи є фрагментарними. Основними проблемами є недостатня сегментація у філіях, відсутність централізованого керування привілеями, неповна криптографічна захищеність сховищ, «сірі» інформаційні стежки між гостьовими й внутрішніми доменами, а також нерозвинене журналювання OT-подій. Сформовано первинний реєстр ризиків і дорожню карту усунення невідповідностей із пріоритетом на швидкі технічні зміни (сегментація, шифрування, MFA, поштові захисти), впровадження ключових процесів (PAM, QRB, керування вразливостями) і створення тестового середовища для OT.

3.3 Виявлення та опис інформаційних потоків

Метою цього етапу є отримання вичерпного уявлення про те, як дані породжуються, трансформуються, передаються, зберігаються та знищуються в межах ІТС підприємства, а також через межі довіри – до хмарних сервісів, контрагентів і технологічних майданчиків. Результатом мають стати формалізовані описи потоків, карти довіри та реєстр інформаційних взаємодій, на які безпосередньо спиратимуться модель загроз, політики контролю доступу, правила сегментації та вимоги до шифрування. Методично цей етап орієнтується на вимоги ISO/IEC 27001 щодо визначення контексту та меж СУІБ, на практики ISO/IEC 27002 в частині управління активами й контролів передачі інформації, а також на підходи ISO/IEC 27005 до ідентифікації сценаріїв ризику й меж довіри, доповнені категоріями NIST CSF ID.AM, PR.DS та DE.AE для побудови огляду, захисту і виявлення відповідно [8, 18, 25, 26, 19, 28].

Для обстеження спершу визначають доменні області, в яких виникають дані: бізнес-процеси логістики (приймання замовлень, планування маршруту, диспетчеризація, відвантаження, підтвердження доставки), фінансово-облікові операції, кадрові процедури, а також технологічний домен OT, де утворюються телеметрія і команди керування. Для кожної області проводяться інтерв’ю з власниками процесів і систем, аналізуються схеми інтеграцій, договори з постачальниками сервісів, матриці доступу додатків, конфігурації шлюзів та брандмауерів, журнали SIEM і проксі-серверів. Паралельно виконується аналіз мережевого трафіку з фіксацією напрямків, портів, протоколів і криптографічних параметрів, що дозволяє зіставити «заявлені» й фактичні маршрути даних. На підставі цього будується ієрархія діаграм потоків даних: від узагальненого рівня 0 до деталізованих схем рівня 2 з відображенням меж довіри та точок контролю на перетинах сегментів [8, 18].

У логістичному домені інформаційний цикл починається із створення замовлення в CRM або з імпорту через API від ключових клієнтів. Потік даних

переходить до ALS, де здійснюється нормалізація та збагачення профілем клієнта, номенклатурою вантажу та обмеженнями маршруту. З ALS формується маршрутний лист і завдання мобільному застосунку водія, після чого в реальному часі до системи повертаються координати, телеметрія і підтвердження контрольних точок. Частина операцій з передоплати або пост-фактум розрахунків ініціює взаємодію з ERP і банківськими API. На кожному переході фіксуються конкретні канали й механізми захисту: взаємна TLS-автентифікація між зовнішнім API-шлюзом і CRM, TLS 1.2/1.3 між ALS і мобільними клієнтами, підписання критичних документів у СЕД із використанням КЕП. Конфіденційні реквізити замовників класифікуються як такі, що потребують шифрування під час передавання і зберігання, з увімкненими журналами доступу й нерепудіацією дій підписантів [8, 18, 26].

Фінансовий домен породжує потоки первинних документів із СЕД та транзакцій ERP, що прямують до банківських шлюзів. Ці потоки завжди перетинають межу організації і, відповідно, є найбільш вимогливими до криптографічного захисту та журналювання. У каналі застосовується взаємна TLS-автентифікація, а всі події погодження платіжних доручень підлягають кореляції в SIEM із мітками користувачів та контекстом робочих станцій. На внутрішніх відрізках відокремлюються потоки, які мають виходити лише через проксі-шлюзи з категоризацією контенту та контролем розширень, що знижує ризик ексфільтрації через «білі» канали. Журнали створення, редагування й підписання фінансових документів зберігаються у регламентованих термінах та підлягають захисту від модифікації, що прямо корелює з вимогами до надійності та підзвітності [19, 18].

У кадровому домені основним джерелом даних є особові справи, записи про трудові відносини, оцінки результативності та записи про навчання. Потоки тут здебільшого внутрішні, але мають підвищений рівень чутливості через природу персональних даних. Вони пересуваються між СЕД, ERP і службами автентифікації, а також частково інтегруються з хмарними сервісами для навчання персоналу. Для таких потоків обов’язково документуються

правові підстави обробки, умови передачі за межі ЄЕП/ЄС (якщо застосовно), а також механізми мінімізації – псевдонімізація і видалення атрибутів, не потрібних для конкретної операції. Контроль доступу реалізується за ролями із принципом мінімальних привілеїв, а всі дії адміністраторів каталогу фіксуються з атрибуцією і неспростовністю [18, 25, 26].

Технологічний домен OT має окрему природу потоків, у яких є телеметрія з PLC/RTU, архіви трендів та команди керування. Ці потоки фізично відокремлені від офісного IT-ландшафту і перетинають межу довіри лише через OT-DMZ. Передавання технологічних показників до аналітичних сервісів виконується за односпрямованою схемою – через відповідний шлюз або дата-діод, що виключає ін’єкцію керуючих команд з боку IT-сегменту. Усі OT-логи агрегуються локально та ретельно синхронізуються за часом, після чого передаються в SIEM для кореляції із подіями периметра й автентифікації. Команди керування не маршрутизуються за межі OT-сегменту, що є ключовою вимогою безпеки та відповідає рекомендаціям щодо операторів важливих послуг [33, 26].

Окрему увагу приділено потокам «за участі третіх сторін». Це підрядні перевізники, постачальники обладнання, інтегратори SCADA, а також хмарні провайдери офісних сервісів. Для кожного контрагента формується профіль взаємодії з чітким визначенням точок входу, дозволених API-методів, часових вікон доступу та механізмів перевірки. Умови шифрування й аудиту фіксуються у договірних документах, а технічна реалізація здійснюється через API-шлюз із контекстною автентифікацією та записом транзакцій. Будь-який віддалений доступ до інженерних систем можливий виключно через контрольований bastion-хост із багатофакторною автентифікацією та записом сесії. Такий підхід мінімізує невизначеність меж довіри та відповідає принципам Zero Trust щодо перевірки кожної взаємодії [26, 19].

Для кожного виявленого потоку формується паспорт, що містить опис джерела і приймача, бізнес-призначення, схему даних, категорію чутливості, юридичні обмеження обробки, протоколи та криптографічні параметри, часові

характеристики, точки контролю, а також умови зберігання та знищення. Паспорт містить перелік власників даних і власників технічної реалізації, SLA та тригери інцидентів. Це дозволяє запровадити простежуваність від вимоги безпеки до конкретного правила брандмауера, політики DLP або запису в SIEM. Формат паспортів вирівняний із реєстрами активів і журналами змін, що полегшує аудит і регулярний перегляд відповідності [18, 25, 19].

У ході обстеження виявлені кілька відхилень від цільової моделі. Насамперед, окремі допоміжні інтеграції реалізовані через «тимчасові» канали, які не пройшли повної процедури погодження – зокрема, прямий DNS-резольвинг гостевої мережі до внутрішнього рекурсора та використання статичних маршрутів на доступових комутаторах для обхідних шляхів обміну службовими файлами. Такі траси створюють неочевидні шляхи для бічного переміщення і вимагають термінової нормалізації: закриття сервісів із боку гостьових VLAN, винесення допоміжних служб у DMZ, заміна статичних маршрутів на контрольовані переходи через L7-шлюз. У фінансовому домені виявлено нерівномірність застосування криптографічних налаштувань – на окремих серверах підтримуються застарілі версії TLS, що підлягає централізованому відключенню з валідацією сумісності клієнтів [19, 18].

Опис потоків доповнюється відображенням життєвого циклу даних – від моменту створення до архівації і знищення. Для кожної категорії визначаються тригери зміни стану: завершення договору, сплив строків зберігання, юридичні вимоги, потреба розслідування. Це безпосередньо впливає на конфігурацію сховищ, політики резервного копіювання і DLP, а також на фільтри журналювання та правила кореляції подій. Зокрема, для персональних даних встановлено обов’язкову псевдонімізацію в аналітичних вибірках і видалення ідентифікаторів при експорті, тоді як для технологічних трендів визначені довші строки зберігання через їхню доказову цінність при технічних розслідуваннях [18, 25, 28].

З погляду операційної придатності карти потоків інтегруються в процеси керування змінами: кожен запит на інтеграцію або модифікацію маршруту

даних супроводжується оновленням паспорта потоку, аналізом впливу на сегментацію, наявні ACL і вимоги до журналювання, а також оцінкою ризиків відповідно до ISO/IEC 27005. Прийняття змін відбувається через CAB із залученням власників даних, мережевих архітекторів і фахівців з ІБ. Регулярний перегляд точності карт проводиться щонайменше раз на пів року або після суттєвих релізів, з використанням як декларативних джерел (діаграми, паспорти), так і емпіричних – мережевої телеметрії, NetFlow/PCAP-вибірок, записів проксі та SIEM. За результатами перегляду оновлюються як карти, так і правила доступу, шифрування та моніторингу [25, 26, 19].

Після завершення опису потоків формуються контрольні точки спостереження – периметральні шлюзи, брокери повідомлень, точки виходу до хмар, OT-шлюзи та вузли аутентифікації. Для кожної точки визначено набір подій, що підлягають обов’язковому збору, та метадані, достатні для ефективної кореляції: унікальні ідентифікатори сесій, відбитки сертифікатів, атрибути ролей і політик доступу, хеші об’єктів і контрольні суми файлів, коди результатів, часові мітки з єдиним джерелом істини. Це підсилює спроможність виявлення аномалій у реальному часі й забезпечує доказову базу для реагування на інциденти згідно з ISO/IEC 27035 [47, 26].

Сформована модель потоків даних відображає реальний стан ІТС і водночас виконує роль технічного завдання для подальшої побудови контролів. Вона вказує, які з переходів мають бути пропущені через мікросегментацію та брокери, які – переведені на взаємну автентифікацію з обмеженням методів, а які – повністю заборонені через невиправданий ризик. У такий спосіб виявлення та опис інформаційних потоків стає опорним артефактом для всієї КСЗІ – від архітектури мережі й криптографічних профілів до процедур журналювання, оглядів доступів і планів реагування на інциденти, узгоджених із міжнародними стандартами та національними вимогами [8, 18, 25, 26, 19, 28, 47, 33].

3.4 Аналіз моделі порушника

У випадку підприємства ТОВ «ЕнергоТрансЛогістика», що поєднує офісні та технологічні IT-системи, можна виділити щонайменше п’ять категорій потенційних порушників: зовнішні кіберзлочинці, внутрішні користувачі, інсайдери з розширеними привілеями, треті сторони та державні/APT-групи. Кожна з цих груп має власну специфіку поведінки, різний рівень ресурсів і, відповідно, потребує різних підходів до захисту.

Зовнішні кіберзлочинці зазвичай мають фінансову мотивацію, наприклад, крадіжку персональних даних клієнтів, підробку фінансових транзакцій чи вимагання через шифрування даних (ransomware). Вони діють через фішинг, експлуатацію вразливостей у веб-застосунках, брутфорс VPN- або RDP-доступу. Для підприємства вони становлять високу загрозу, оскільки атака може призвести не лише до фінансових втрат, а й до втрати довіри клієнтів і репутаційних ризиків.

Внутрішні користувачі часто не мають злого умислу, проте через недбалість або недостатню обізнаність у питаннях інформаційної безпеки можуть допустити витік інформації. Наприклад, використання слабких паролів, збереження службових документів у незахищених хмарних сховищах чи пересилання конфіденційних файлів через особисті месенджери. Хоча загроза з боку такої категорії порушників має меншу ймовірність цілеспрямованого шкідливого впливу, наслідки можуть бути не менш значними, ніж у випадку цілеспрямованих атак.

Інсайдери з розширеними повноваженнями (адміністратори, оператори SCADA, спеціалісти IT-відділу) є особливо небезпечними, оскільки володіють знаннями про архітектуру системи та мають доступ до критичних елементів. Їхні дії можуть призвести до повної зупинки роботи ІТС, маніпуляцій із базами даних або навіть саботажу технологічних процесів. У цьому випадку ризики значно зростають і потребують впровадження систем управління привілеями,

багаторівневого журналювання та обов'язкового принципу розподілу обов'язків (SoD).

Треті сторони – підрядники, інтегратори та постачальники обладнання – становлять ще один важливий вектор загроз. Наявність віддаленого доступу через VPN або API, а також підключення підрядників до OT-сегментів створюють ризики компрометації у випадку зламу їхніх власних систем. У таких випадках підприємство залежить від рівня зрілості кіберзахисту сторонніх компаній, що потребує встановлення чітких контрактних зобов'язань і додаткового технічного контролю (журналювання доступу, сегментація, використання bastion-хостів).

Державні та APT-групи діють рідше, але є найбільш ресурсними. Вони можуть бути зацікавлені у виведенні з ладу логістичних або енергетичних систем, що підпадають під категорію критичної інфраструктури. В арсеналі таких зловмисників – нульові вразливості, багатоступеневі атаки та тривале перебування в мережі з метою шпигунства чи саботажу. Для захисту від таких атак необхідні передові методи моніторингу, сегментація OT і IT-середовищ, багаторівневі бар'єри та регулярні аудитори безпеки.

Щоб систематизувати результати аналізу, була складена розширена матриця порушника (Див. Табл. 3.1), яка відображає ключові характеристики, потенційні цілі, методи атак, можливі наслідки та заходи протидії.

Таблиця 3.1

Матриця моделі порушника

Категорія порушника	Мотивація	Рівень ресурсів і знань	Потенційні методи атак	Ймовірні наслідки	Рекомендовані заходи протидії
Зовнішні кіберзлочинці	Фінансова вигода, вимагання, продаж даних на	Середній або високий: готові комплекти експлойтів, доступ до	Фішинг, malware (трояни, ransomware), SQL-injection,	Компрометація персональних і фінансових даних,	Антивірус/EDR, SIEM, IPS/IDS, обов'язкове MFA, регулярні

	чорному ринку	ботнетів, використання phishing-kit	brute-force атак на VPN, експлуатація вразливостей у веб-додатках	параліч ERP/ALS, втрати коштів і клієнтів	пентести, оновлення ПЗ, резервне копіювання
Внутрішні користувачі (рядові співробітники)	Ненавмисні помилки, недбалість	Низький: обмежені знання, але легітимний доступ	Використання слабких паролів, нехтування політиками, завантаження шкідливих файлів, передавання конфіденційних документів у незахищених каналах	Витік персональних і комерційних даних, порушення цілісності баз, зростання вразливості до зовнішніх атак	Навчання користувачів, DLP-системи, контроль носіїв, мінімізація прав доступу, регулярні інструктажі
Інсайдери з розширеними правами (адміністратори, оператори SCADA)	Особиста вигода, помста, тиск з боку конкурентів	Високий: глибокі знання архітектури, доступ до критичних систем	Неавторизовані зміни конфігурацій, маніпуляція з базами даних, саботаж технологічних процесів, приховане створення «бекдорів»	Зупинка бізнес-процесів, знищення або модифікація критичних даних, компрометація технологічних систем	Впровадження PAM, розподіл обов’язків, багаторівневе журналювання, контроль привілеїв, регулярний аудит

Треті сторони (підрядники, партнери)	Виконання контрактів, проте ризик компрометації їхніх систем	Середній: доступ до VPN/API, часто слабший рівень захисту	Використання вразливих облікових записів, передача заражених файлів, зловживання доступом до API	Витік даних, порушення безперервності процесів, зараження корпоративної мережі	Контрактні вимоги до безпеки, ізоляція доступів, журналювання сесій, використання bastion-хостів, контроль API
Державні та APT-групи	Політичні або стратегічні цілі, шпигунство, саботаж	Дуже високий: доступ до нульових вразливостей, великі ресурси, професійні команди	Складні багатоступеневі атаки, соціальна інженерія, zero-day, атаки на SCADA, тривале приховане перебування у мережі	Параліч критичної інфраструктури, тривала компрометація, економічні та репутаційні втрати	Сегментація IT/OT, SOC із цілодобовим моніторингом, обмін розвідданими (Threat Intelligence), регулярні аудити, тестування на проникнення, Zero Trust модель

Розглянуті категорії порушників мають підтвердження у практичних інцидентах, що відбувалися як в Україні, так і за її межами. Наприклад, зовнішні кіберзлочинці активно застосовують атаки типу ransomware – у 2017 році всесвітньо відомою стала атака вірусу NotPetya, яка паралізувала низку

українських підприємств та державних органів, завдавши багатомільярдних збитків у глобальному масштабі. Подібні кампанії тривають і надалі, орієнтуючись як на великі корпорації, так і на середні бізнеси.

Внутрішні користувачі нерідко ставали джерелом витоку даних через недотримання політик безпеки. Відомим прикладом є випадки, коли співробітники державних установ завантажували службові документи на особисті електронні поштові скриньки чи публічні хмарні сервіси, що призводило до компрометації інформації. Такі інциденти доводять, що людський фактор залишається одним із найслабших місць у системі безпеки.

Інсайдери з розширеними правами також неодноразово фігурували у реальних подіях. Наприклад, у США було зафіксовано випадки, коли адміністратори свідомо вносили «бекдори» в інформаційні системи після звільнення, що дозволяло їм дистанційно впливати на роботу компанії. В Україні у фінансовому секторі також фіксувалися спроби змови співробітників банків із зовнішніми зловмисниками з метою несанкціонованого виведення коштів.

Ризики, пов’язані з третіми сторонами, підтвердили численні атаки через ланцюжок постачання. В українському контексті варто відзначити випадки компрометації IT-компаній, які обслуговували критичну інфраструктуру, що призводило до масштабних перебоїв у роботі клієнтів.

APT-групи та державні актори становлять особливу небезпеку. В Україні неодноразово фіксувалися атаки на енергетичний сектор, зокрема відомі інциденти 2015–2016 років, коли внаслідок кібератак на енергетичні компанії відбулися масові відключення електроенергії. Ці випадки продемонстрували, що цілеспрямовані атаки можуть бути складно виявленими і здатні завдати серйозних збитків національному масштабу.

Таким чином, аналіз моделі порушника, спираючись на реальні інциденти, підтверджує актуальність і небезпеку кожної категорії зловмисників. Це підкреслює необхідність продуманого підходу до побудови КСЗІ, який врахує як зовнішні, так і внутрішні джерела загроз.

3.5 Аналіз моделі загроз

Аналіз моделі загроз є логічним продовженням побудови моделі порушника і спрямований на виявлення потенційних сценаріїв реалізації атак, які можуть бути здійснені щодо ІТС підприємства. Модель загроз дозволяє визначити, які активи можуть бути об’єктом посягання, які канали проникнення існують, які технічні чи організаційні вразливості можуть бути використані, а також який очікуваний вплив матиме реалізація цих загроз. У методологічному плані даний процес базується на вимогах ДСТУ ISO/IEC 27005:2015 та практиках NIST SP 800-30, які передбачають ідентифікацію активів, визначення потенційних вразливостей і складання переліку загроз із подальшою оцінкою їхньої ймовірності та наслідків [8; 18; 25; 26].

Першим кроком є визначення критичних активів, які в контексті підприємства ТОВ «ЕнергоТрансЛогістика» включають: бази даних клієнтів та контрактів, фінансові транзакції ERP-системи, телеметрію і команди SCADA, внутрішні документи кадрового та юридичного характеру, а також логістичні дані про маршрути та відвантаження. Кожен із цих активів має власні вимоги до конфіденційності, цілісності та доступності, тому будь-яка загроза має оцінюватися через призму можливого порушення цих властивостей.

Загрози можна класифікувати за кількома категоріями:

1) Загрози конфіденційності: До них належать несанкціонований доступ до персональних і комерційних даних, витік через злом акаунтів співробітників, фішингові кампанії або помилки внутрішніх користувачів. Прикладом може бути викрадення облікових даних через фішинг, що дозволить зловмисникам отримати доступ до баз даних ERP. Для підприємства це означатиме фінансові збитки і втрату довіри клієнтів.
2) Загрози цілісності: Вони включають навмисну або випадкову модифікацію даних у бізнес-системах і SCADA. Наприклад, інсайдер із

розширеними повноваженнями може змінити маршрути доставки або параметри роботи енергетичних вузлів. У результаті можливе зривання логістичних операцій, що призведе до штрафів і контрактних санкцій.

3) Загрози доступності: Найбільш характерними є DDoS-атаки на публічні сервіси, шифрувальники, збої у роботі обладнання, аварії електропостачання або помилки в налаштуванні мережевих пристроїв. У випадку з підприємством логістичного профілю це означає фактичне зупинення бізнес-процесів – неможливість обробки замовлень, управління маршрутами або моніторингу транспорту.
4) Технічні загрози: Включають використання вразливостей у веб-додатках, недоліки мережевої сегментації, відсутність криптографічного захисту окремих каналів, експлуатацію застарілого програмного забезпечення. Зокрема, виявлені раніше статичні маршрути у філіях можуть стати каналом для бічного переміщення атакувальників.
5) Організаційні загрози: Сюди входить відсутність формалізованих політик, інструкцій, контролю доступу, а також недостатня підготовка персоналу. Як приклад – співробітники можуть використовувати особисті носії інформації без належної перевірки, що створює ризик занесення шкідливого ПЗ у корпоративну мережу.
6) Фізичні загрози: Для підприємства важливим чинником є розташування складів і офісів у кількох регіонах, де існує ризик пожеж, затоплення чи відключення енергії. Усі ці події можуть знищити обладнання або зробити інформаційні системи недоступними.
7) Загрози від третіх сторін: Підрядники й партнери, які мають VPN-доступ або інтеграційні канали API, стають потенційними носіями ризиків. У випадку компрометації їхніх систем зловмисники можуть отримати доступ до внутрішніх сервісів.

Для кожної категорії загроз формується оцінка ймовірності та впливу. Наприклад, для атаки типу ransomware імовірність визначається як висока, а вплив – критичний, оскільки може заблокувати всю діяльність компанії. Для

загрози природного характеру, наприклад пожежі у серверній, ймовірність нижча, проте вплив залишається значним. У підсумку формується матриця ризиків (Див. Табл. 3.2), яка показує, які загрози є найбільш пріоритетними для протидії.

Таблиця 3.2

Матриця основних загроз

Категорія загроз	Приклади реалізації	Ймовірність	Потенційний вплив	Можливі сценарії	Рекомендовані заходи протидії
Загрози конфіденційності	Фішинг, крадіжка облікових записів, підбір паролів, витік даних через особисті поштові скриньки або незахищені хмарні сервіси	Висока	Витік персональних і фінансових даних, репутаційні втрати, штрафи за GDPR/Закон України «Про захист персональних даних»	Зовнішній зловмисник розсилає фішингові листи працівникам бухгалтерії; співробітник вводить пароль від ERP у підробленій формі; обліковий запис використовується для ексфільтрації контрактів	MFA для всіх користувачів, антифішингові тренінги, впровадження DLP, контроль поштових доменів (SPF/DKIM/DMARC), SIEM-кореляція фішинг-кампаній
Загрози цілісності	Несанкціонована модифікація даних у ERP, навмисні	Середня	Спотворення даних, зрив логістичних операцій, порушення	Інсайдер змінює маршрути транспорту, що	Впровадження PAM, SoD (розподіл обов’язків),

	зміни маршрутів у ALS, маніпуляції параметрами SCADA, помилки адміністраторів		контрактних зобов'язань, ризик саботажу технологічних процесів	призводить до невчасних доставок; адміністратор випадково видаляє дані замовлень без резервної копії	контроль змін у БД (auditing), регулярний бекап та перевірка відновлюваності, журналювання адміністративних дій
Загрози доступності	DDoS-атаки на корпоративний сайт/API, зараження ransomware, аварії в електропостачанні, збої у серверному обладнанні	Висока	Зупинка бізнес-процесів, неможливість обробки замовлень, зрив контрактів, втрати прибутку	Хакерська група запускає DDoS проти API мобільного додатку для водіїв → неможливість підтвердження доставок; шифрувальник блокує ERP-сервери	Резервні канали зв'язку, DDoS-фільтрація на стороні провайдера, регулярне резервне копіювання (3–2–1), DRP/BCP плани, антивірус/EDR із функціями ізоляції вузлів
Технічні загрози	Використання zero-day чи відомих вразливосте	Середня–висока	Отримання несанкціонованого доступу,	Нападник експлуатує SQL-injection у	Сегментація мережі, регулярний вразливісни

	й у веб-додатках, відсутність патчів, слабка сегментація у філіях, некоректні ACL		бічний рух у мережі, витік даних	веб-порталі; через відсутність сегментації зловмисник з user-VLAN потрапляє у серверну VLAN	й скан, патч-менеджмент ≤7 днів, WAF на веб-додатках, централізація ACL через NGFW
Організаційні загрози	Відсутність формалізованих політик, нехтування правилами безпеки, помилки персоналу, несанкціоноване використання USB	Висока	Порушення політики безпеки, витік даних, компрометація облікових записів	Користувач зберігає службові документи у власному Google Drive; співробітник підключає заражену флешку до службового ПК	Формування політик безпеки, навчання співробітників, DLP на робочих станціях, контроль USB-портів, щоквартальні інструктажі
Фізичні загрози	Пожежа у серверній, затоплення складу, аварія електропостачання, крадіжка обладнання	Низька–середня	Втрата обладнання, тривалий простій ІТС, пошкодження даних	Серверна у філії пошкоджена під час аварії системи кондиціонування → втрата локального сервера ALS	Системи пожежогасіння (газові), резервні джерела живлення (UPS, генератори), географічно розподілені бекапи, контроль

					фізичного доступу (СКД, відеоспостереження)
Загрози від третіх сторін	Компрометація систем підрядників, атаки через інтеграційні API, використання вразливого VPN-клієнта	Середня	Несанкціонований доступ до внутрішніх систем, зараження корпоративної мережі, витік даних	Хакери атакують підрядника, отримують доступ до його VPN і через нього – до внутрішніх серверів підприємства	Встановлення контрактних вимог до безпеки, аудит підрядників, використання bastion-хостів, сегментація каналів, обов'язкове журналювання доступів
Соціальна інженерія	Телефонні шахрайства (vishing), підроблені акаунти у соцмережах, маніпуляції із службою підтримки	Висока	Викрадення облікових даних, ініціювання шахрайських транзакцій, обхід процедур	Зловмисник телефонує до бухгалтерії, представляється адміністратором ERP і просить тимчасово надати пароль	Тренінги для персоналу, перевірка ідентичності через окремий канал, формалізовані інструкції служби підтримки

APT та державні актори	Використання zero-day, довготривале приховане перебування, цільові атаки на SCADA	Низька–середня (але висока критичність)	Параліч технологічних процесів, масштабні відключення, шпигунство	APT-група впроваджує бекдор у SCADA та згодом дистанційно відключає енергетичні вузли	Сегментація IT/OT, SOC 24/7, Threat Intelligence, регулярні пентести, застосування Zero Trust моделі
Природні загрози	Повені, землетруси, сильні буревії, військові дії	Низька	Втрата ІТС у регіоні, фізичне пошкодження серверів	Склад у Дніпрі стає недоступним через підтоплення, серверна зупиняється на тиждень	DR-сайти в іншому регіоні, регулярні реплікації, мобільні резервні майданчики
Ланцюжок постачання (supply chain)	Компрометація оновлень ПЗ, заражені драйвери обладнання, інфіковані SDK	Середня	Масовий компроміс внутрішніх систем, труднощі виявлення атаки	Подібний до SolarWinds сценарій: через оновлення інструментів адміністрування зловмисники отримують доступ до всієї мережі	Обов’язкова перевірка оновлень, контроль хешів, використання репозиторіїв із цифровим підписом, аудит постачальників

Аналіз показує, що найбільший пріоритет мають загрози, пов’язані з доступністю (DDoS, ransomware), оскільки саме вони здатні паралізувати критичні бізнес-процеси. Другою за значимістю є група загроз

конфіденційності та цілісності, пов’язаних із компрометацією персональних і фінансових даних, а також модифікацією маршрутів чи команд управління в SCADA. Організаційні та технічні загрози мають системний характер і можуть стати каталізатором для реалізації більш складних атак.

Таким чином, модель загроз створює основу для формування політики безпеки та визначення пріоритетів у впровадженні заходів КСЗІ. Вона дозволяє не лише ідентифікувати слабкі місця, але й прогнозувати наслідки інцидентів, що особливо важливо для підприємства, яке функціонує у сфері логістики та енергетики, тобто в умовах постійного ризику цільових атак і високих вимог до безперервності бізнесу.

3.6 Визначення рівня захищеності об’єкта

Визначення рівня захищеності ІТС підприємства є невід’ємним етапом розробки КСЗІ. На цьому етапі здійснюється порівняння фактичних заходів захисту з вимогами нормативно-правових актів України, міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005, NIST SP 800-30 та рекомендацій ДССЗЗІ. Також проводиться співставлення з ідентифікованими раніше загрозами та моделлю порушника, що дозволяє оцінити реальну стійкість підприємства до актуальних ризиків.

Оцінювання (Див. Табл. 3.3) виконувалося за п’ятьма напрямами: організаційним, технічним, криптографічним, фізичним та операційним (реагування на інциденти). У кожному напрямі були визначені конкретні підкатегорії, що дозволило деталізувати оцінку. Наприклад, у технічному напрямі окремо аналізувалися мережевий периметр, сегментація, системи журналювання, резервне копіювання, захист кінцевих точок. У фізичному – електроживлення, пожежна безпека та системи контролю доступу.

Таблиця 3.3

Рівень захищеності ІТС підприємства за основними напрямами

Напрям	Підкатегорія	Поточний стан	Сильні сторони	Слабкі сторони	Рівень зрілості (1–5)	Рекомендації
Організаційний	Політика ІБ	Є окремі інструкції (паролі, резервні копії), але немає комплексної політики	Призначений відповідальний за ІБ (CISO)	Відсутня єдина затверджена політика ІБ, немає системи класифікації даних	2	Розробити комплексну політику ІБ, затвердити на рівні керівництва
	Управління	Проводяться	Наявність мінімальн	Інструктажі	2	Запровадити

	персоналом	первинні інструктажі для нових співробітників	ої програми навчання	нерегулярні, відсутні тренінги з фішинг-атаки		регулярні тренінги, симуляції фішингу, щорічну переатестацію
	Розподіл обов'язків	Формально існує, але не завжди дотримується	Розподіл доступів у фінансових операціях	В IT відсутній SoD, адміністратори мають надлишкові права	2	Впровадити принцип SoD, проводити щоквартальний аудит прав
Технічний	Мережевий периметр	NGFW з базовим IPS, антивірус на більшості ПК	Периметр частково захищений, є фільтрація трафіку	Відсутня DLP, IPS працює не на всіх сегментах, IDS у тестовому режимі	3	Впровадити IDS/IPS для всіх сегментів, підключити DLP
	Сегментація	VLAN використовується в головному офісі	Є базове розділення офісних і серверних сегментів	У філіях слабка сегментація, ACL неповні	2	Запровадити мікросегментацію VLAN у всіх філіях
	Ендпойнт-захист	Антивірус встановлений, частково EDR	Є централізована консоль	Не всі сервери під EDR, немає	3	Розширити EDR, додати функції

			антивірусів	ізоляції вузлів		ізоляції вузлів
	Журналювання	Часткове централізоване логування у SIEM	SIEM збирає логи основних серверів	Логи не з усіх систем, відсутня кореляція для SCADA	2	Інтегрувати SCADA в SIEM, додати SOAR для автоматизації
	Резервне копіювання	Використовується 3–2–1, бекапи в S3-сховищі	Є реплікація між ЦОДами, перевірки відновлення	Відновлення тестується рідко, DRP формально відсутній	3	Розробити DRP, проводити регулярні тести відновлення
Криптографічний	Шифрування каналів	TLS 1.2/1.3 у більшості сервісів	Сучасні сертифікати, часткове взаємне TLS	TLS 1.0/1.1 на застарілих вузлах, не скрізь взаємна автентифікація	2	Вимкнути TLS 1.0/1.1, впровадити взаємне TLS для критичних каналів
	Шифрування даних	BitLocker на ноутбуках керівників, TDE у частині БД	Захист мобільних пристроїв керівництва	Не всі сховища зашифровані, резервні диски без шифрування	2	Впровадити обов’язкове шифрування всіх сховищ

	Керування ключами	Є внутрішня PKI	Використання сертифікатів для VPN	Відсутня HSM, слабкий контроль життєвого циклу ключів	2	Впровадити HSM, автоматизувати керування ключами
Фізичний	Доступ до приміщень	СКД і відеоспостереження у головному офісі	Базовий контроль фізичного доступу	У філіях доступ контролюється слабко, охорона аутсорсингова	3	Встановити СКД у філіях, інтегрувати камери з SIEM
	Електроживлення	UPS і генератор у головному офісі	Безперебійність у ЦОД	У філіях лише базові UPS, генераторів немає	2	Закупити UPS і генератори для ключових філій
	Пожежна безпека	Система пожежогасіння у ЦОД	Використання газового пожежогасіння	У філіях пожежна безпека мінімальна	3	Встановити автоматичні системи пожежогасіння у філіях
Реагування на інциденти	SOC/моніторинг	Є SIEM, SOC не розгорнуто	Частковий моніторинг мережевих подій	Відсутній 24/7 моніторинг, немає SOAR	2	Побудувати SOC, підключити SOAR

	Incident Response Plan	Формально відсутній	ІТ-відділ іноді реагує на інциденти вручну	Немає формалізованих плейбуків, не проводяться навчання	1	Розробити IRP, проводити тренінги й симуляції
	Тести на проникнення	Проводяться рідко (1 раз на 2 роки)	Є мінімальна практика	Відсутній регулярний аудит, не охоплює ОТ	2	Проводити пентести щороку, включити ОТ-сегмент
	Навчання персоналу	Є інструктаж при прийомі на роботу	Базове ознайомлення	Немає системних тренінгів, співробітники не знають, як діяти під час атаки	2	Організувати регулярні тренінги, симуляції фішинг-атак

Проведений аналіз свідчить, що поточний стан захищеності підприємства можна охарактеризувати як середній, проте з наявними істотними прогалинами. У частині організаційних заходів спостерігається лише фрагментарне впровадження політик безпеки – існують окремі інструкції щодо паролів і резервного копіювання, проте відсутня єдина комплексна політика інформаційної безпеки. Це створює ризик непослідовності дій персоналу у випадку інцидентів.

Технічний рівень є відносно вищим, адже на підприємстві встановлені NGFW-брандмауери, реалізована часткова сегментація, використовується антивірусне ПЗ та здійснюється резервне копіювання за принципом «3–2–1».

Водночас відсутність DLP і PAM, слабкий рівень мікросегментації у філіях та недостатнє покриття EDR-системами значно знижують ефективність цього рівня.

Криптографічні заходи оцінюються як базові. Хоча TLS 1.2/1.3 застосовується у більшості каналів зв'язку, окремі вузли все ще використовують застарілі версії протоколів. Шифрування даних реалізоване лише частково – BitLocker функціонує лише на пристроях керівників, тоді як серверні сховища не захищені належним чином. Управління ключами здійснюється без застосування HSM, що створює додаткові ризики компрометації.

Фізичний рівень у головному офісі відповідає базовим вимогам – використовується система контролю доступу, відеоспостереження, резервні джерела живлення та система газового пожежогасіння. Проте у філіях цей напрям практично не охоплений, що робить їх найбільш вразливими до фізичних інцидентів.

Найбільш проблемною сферою залишається реагування на інциденти. SOC у підприємства немає, Incident Response Plan не розроблений, пентести проводяться нерегулярно, а персонал не має чітких інструкцій щодо дій під час кібератак. Це означає, що у випадку складного інциденту підприємство не зможе оперативно відновити працездатність систем і мінімізувати наслідки атаки.

Узагальнюючи результати, можна стверджувати, що рівень захищеності підприємства складає приблизно 2,3 бала з 5, що відповідає проміжному рівню між базовим і середнім. Це означає, що компанія здатна протидіяти масовим некваліфікованим атакам (вірусам, простим DDoS, типовим фішинговим кампаніям), але залишається вразливою до цілеспрямованих дій з боку організованих кіберзлочинних угруповань або APT-груп.

Щоб вийти на високий рівень, підприємству необхідно:

- Розробити й впровадити комплексну політику інформаційної безпеки;

- Створити SOC з цілодобовим моніторингом і автоматизацією обробки інцидентів;
- Впровадити системи PAM, DLP, SOAR та забезпечити повне покриття EDR;
- Уніфікувати використання сучасних криптографічних засобів і впровадити HSM для управління ключами;
- Модернізувати фізичний захист у філіях, встановивши додаткові системи пожежогасіння, UPS і СКД;
- Організувати регулярні тренінги персоналу, симуляції фішингових атак і щорічні тести на проникнення.

Таким чином, визначення рівня захищеності підтверджує актуальність впровадження КСЗІ, яка забезпечить глибинний захист та відповідність вимогам як національного законодавства, так і міжнародних стандартів. Лише системний підхід дозволить підвищити стійкість підприємства до сучасних кіберзагроз і гарантувати безперервність його діяльності.

3.7 Формування профілю захищеності

Формування профілю захищеності є завершальною аналітичною фазою дослідження перед розробкою та впровадженням заходів КСЗІ. Такий профіль дозволяє створити цілісне уявлення про стан безпеки підприємства, виділити найбільш критичні активи, оцінити їхню стійкість до загроз і визначити пріоритети вдосконалення. Фактично, профіль захищеності виступає основою для побудови «дорожньої карти» розвитку КСЗІ.

У процесі формування профілю (Див. Табл. 3.4) використовуються результати аналізу загроз, моделі порушника та оцінки рівня захищеності об’єкта. Профіль складається з опису критичних активів, їхніх потенційних вразливостей, ймовірних сценаріїв атак і рівня ризику. Окремо визначаються існуючі заходи протидії та ті, які потребують впровадження найближчим часом.

Таблиця 3.4

Профіль захищеності критичних активів підприємства «ЕнергоТрансЛогістика»

Критичний актив	Опис активу	Потенційні загрози	Основні вразливості	Рівень ризику	Існуючі заходи захисту	Рекомендовані заходи
ERP-система управління логістикою	Центральна система, що координує перевезення, маршрути, склади, фінансові потоки	Фішинг, SQL-injection, brute force, атаки на інтеграційні API, ransomware	Використання застарілих протоколів на окремих вузлах, слабкий контроль підрядників, відсутність PAM	Високий	NGFW, TLS 1.2/1.3, регулярні резервні копії	Впровадження PAM, DLP, обов’язкове шифрування БД, WAF, аудит API, створення SOC

База даних клієнтів і контрактів	Містить персональні дані клієнтів, фінансові договори, контактну інформацію	Несанкціонований доступ, інсайдерські загрози, витік через хмарні сервіси, шкідливе ПЗ	Не всі БД зашифровані, слабкий контроль привілеїв, відсутня класифікація даних	Високий	BitLocker на окремих пристроях, TLS 1.3 для зовнішніх каналів	Шифрування всіх БД (TDE), впровадження DLP, формалізація політики доступів, регулярні аудити прав
Автоматизована система обліку палива (АСОП)	Контролює облік палива, витрати та постачання	Атаки на SCADA, віруси, інсайдерські маніпуляції, DoS-атаки	Низький рівень сегментації, обмежене журналювання, слабкий фізичний захист у філіях	Середній	Базова сегментація, антивірус на робочих станціях	Сегментація IT/OT, інтеграція з SIEM, контроль USB-портів, посилення фізичного захисту
Корпоративна електронна пошта	Основний канал внутрішньої та зовнішньої комунікації	Фішинг, malware через вкладення, spoofing, витік конфіденційної інформації	Відсутність DLP, недостатні антифішингові механізми, слабкі паролі у частини користувачів	Середній–високий	Антивірусна перевірка вкладень, SPF/DKIM	Впровадження DMARC, MFA для всіх користувачів, DLP для пошти, регулярні антифіши

						нгові тренінги
Фінансово-бухгалтерська система	Система управління рахунками, платежами та звітністю	Інсайдерські шахрайські дії, підробка транзакцій, фішинг, шкідливе ПЗ	Недостатній контроль транзакцій, відсутність SoD, немає журналювання адмінських дій	Високий	NGFW, базовий антивірус	Впровадження SoD, багатофакторної автентифікації, аудиту транзакцій, PAM
Система відеоспостереження складів	Камери для контролю фізичного доступу і процесів навантаження	Несанкціонований доступ, підміна відеопотоку, відмова обладнання	Відсутність шифрування потоків, слабкий захист паролів, фізична вразливість обладнання	Середній	СКД у головному офісі, відеореєстратори	Шифрування потоків, сегментація мереж, централізований моніторинг, резервні сервери
VPN/віддалений доступ	Канал доступу до внутрішніх систем для співробітн	Використання вразливих VPN-клієнтів, компрометація	Відсутність обов’язкової MFA, слабкий моніторинг сесій,	Високий	VPN із TLS 1.2, журнали доступів	MFA, сегментація підрядників, bastion-хости, SIEM-

	иків і підрядників	облікових записів, brute force	надлишкові права підрядників			кореляція сесій, регулярний аудит
Філіальні IT-інфраструктури	Серверні та локальні мережі у віддалених філіях	Несанкціонований фізичний доступ, віруси, збої у живленні, DDoS на локальні сервіси	Відсутність генераторів, слабкий фізичний контроль, відсутність резервних копій на місцях	Середній	Локальні UPS, антивірус	Встановлення генераторів, інтеграція у DR-схему, централізоване адміністрування, СКД

Проведений аналіз показав, що найбільш критичними для підприємства є ERP-система управління логістикою, база даних клієнтів і контрактів, автоматизована система обліку палива та корпоративна електронна пошта. Для кожного з цих активів були визначені ключові загрози – від фішингових атак і несанкціонованого доступу до компрометації інтеграційних API та зараження шкідливим ПЗ.

Як було показано (Див. Табл. 3.4), у більшості випадків поточні заходи безпеки забезпечують лише базовий рівень захисту. Так, використання NGFW і TLS 1.2/1.3 створює певний бар’єр для зовнішніх атак, але відсутність DLP і PAM робить систему вразливою до інсайдерів та витоків через електронну пошту чи зовнішні носії. Водночас слабкий контроль підрядників створює додатковий ризик компрометації через ланцюжок постачання.

Аналіз також засвідчив, що рівень ризику для різних активів суттєво відрізняється. ERP-система та база даних клієнтів перебувають у зоні «високого ризику», оскільки їхня компрометація може призвести не лише до

фінансових втрат, а й до руйнування репутації компанії. Автоматизована система обліку палива має середній рівень ризику – її збої можуть порушити логістичні процеси, проте вони менш критичні у стратегічному масштабі. Корпоративна електронна пошта відноситься до середньо-високої категорії ризику, адже є основним каналом комунікації і водночас найбільш уразливим до фішингових атак.

Формування профілю захищеності дозволяє встановити пріоритети: у першу чергу підприємству необхідно посилити технічні засоби (впровадити PAM, DLP, SOAR), уніфікувати криптографічний захист і модернізувати фізичний захист у філіях. Другою за важливістю задачею є розробка комплексної політики інформаційної безпеки та створення SOC. Лише після цього доцільно переходити до менш критичних напрямів, таких як підвищення регулярності пентестів та організація симуляцій атак для персоналу.

Узагальнено можна сказати, що профіль захищеності підприємства свідчить про середній рівень стійкості системи та водночас демонструє низку «слабких місць», які потребують першочергового усунення. Таким чином, він виступає ключовим орієнтиром для побудови ефективної та відповідної стандартам КСЗІ.

3.8 Технічні заходи захисту

Технічні заходи захисту інформації є базовим елементом будь-якої КСЗІ, адже саме вони забезпечують практичну реалізацію вимог законодавства, стандартів і внутрішніх політик. Для головного офісу ТОВ «ЕнергоТрансЛогістика» у місті Київ, який обробляє значні обсяги персональних, фінансових і комерційних даних, впровадження належного рівня технічного захисту є питанням не лише інформаційної безпеки, а й стабільності бізнес-процесів та репутації підприємства.

Технічні заходи впроваджуються комплексно та охоплюють усі рівні інфраструктури – від мережевого периметра і серверного залу до інженерних систем електроживлення, охоронних пристроїв та фізичного середовища офісу. Основним принципом побудови системи виступає концепція «глибинної оборони» (defense in depth), коли кожен рівень захисту підсилює інший, створюючи багаторівневий бар’єр проти потенційних загроз.

Для оцінки та планування технічних заходів у межах київського офісу було сформовано деталізовану матрицю (Див. Табл. 3.5), що відображає поточний стан основних систем захисту, сильні та слабкі сторони, а також рекомендовані напрями розвитку.

Таблиця 3.5

Технічні заходи захисту інформації на підприємстві «ЕнергоТрансЛогістика»

Система / напрям	Функції	Поточний стан	Сильні сторони	Слабкі сторони	Рекомендовані заходи
NGFW (брандмауер нового покоління)	Контроль периметра, фільтрація трафіку, IPS/IDS, DPI	Встановлений у головному офісі, забезпечує сегментацію мережі	Захист від типових атак, централізоване керування політиками	Відсутня інтеграція з централізованою системою моніторингу, обмежений IPS	Розширення функціоналу NGFW, підключення до системи моніторингу безпеки

Сегментація мережі	Розподіл VLAN, ізоляція серверів, обмеження lateral movement	Частково впроваджена у ЦОД	Поділ офісної, серверної та гостьової мережі	Потребує аудиту ACL та політик доступу	Впровадження мікросегментації (Zero Trust), аудит мережевих ACL
Система контролю доступу (СКД)	Контроль фізичного доступу в офісні приміщення і серверні	Встановлена у головному офісі	Інтеграція з відеоспостереженням, персоналізований облік	Відсутній віддалений моніторинг, обмежена історія подій	Розширення журналювання, інтеграція з моніторингом безпеки
Система відеоспостереження	Моніторинг входів, коридорів, серверних, архівів	Камери встановлені у ключових зонах офісу	Цілодобовий контроль фізичного доступу	Відсутнє шифрування потоків, немає резервного архіву	Впровадити централізоване керування та шифрування відеопотоків, резервування сховищ
Система пожежогасіння та сигналізації	Автоматичне виявлення й гасіння займання	Система пожежогасіння Inergen у серверній, сигналізація в офісі	Висока ефективність, автономність, сертифікація	Немає централізованої диспетчеризації подій	Об’єднання системи пожежогасіння та охоронної сигналізації у єдиний центр моніторингу
Електроживлення та резервуванн	Безперебійне живлення серверів і	Встановлені UPS N+1, дизель-	Стійкість до відключень	Потребує автоматизаці	Впровадити систему моніторингу

я (UPS, генератор)	робочих станцій	генератор у резерві	електроенергії	ї контролю навантажень	енергоспоживання, тестування сценаріїв перемикання
Система заземлення та блискавкозахисту	Захист від перенапруги, стабілізація потенціалів	Реалізовано контур заземлення, встановлені блискавкоприймачі	Відповідає вимогам ДСТУ, перевірено лабораторно	Відсутній резервний контур для додаткових ліній живлення	Розширення системи заземлення, періодичне тестування опору
Захист від електромагнітних каналів витоку	Зниження рівня електромагнітного випромінювання, екранування	Серверна екранована фольгованими матеріалами, фільтри на живленні	Висока ефективність екранування	Не всі сигнальні кабелі мають фільтри	Розширення фільтрації каналів, контроль ЕМ-випромінювань
Захист від електричних каналів витоку	Ізоляція живлення, зниження наведень	Встановлені ізолюючі трансформатори, розділення контурів живлення	Високий рівень електричної безпеки	Частина обладнання підключена без фільтрів	Уніфікація контурів живлення, застосування стабілізаторів напруги
Захист від акустичних каналів	Зниження ризику акустичного перехоплення	Серверна та переговорні кімнати із шумоізоляцією	Ефективна герметизація, шумогенератори типу «Вектор-А»	Обмежена площа покриття шумоізоляцією	Розширення шумоізоляції на допоміжні приміщення
Захист від вібраційних каналів	Демпфування механічних коливань	Серверні стійки на	Зменшення передавання	Відсутній моніторинг	Регламентні перевірки кріплень,

		антивібраційних опорах	вібрацій на конструкції	стану кріплень	використання сенсорів вібрацій
Захист від оптичних каналів	Запобігання спостереженню за екранами, проникненню світла	Вікна з матовими плівками та жалюзі	Унеможливлення зчитування інформації зовні	Обмежений контроль за конфігурацією робочих місць	Аудит розміщення моніторів, встановлення антивідблискових фільтрів
Моніторинг інженерних систем	Відстеження параметрів живлення, температури, вологості	Сенсори у серверній, централізований збір показників	Оперативне виявлення відхилень	Обмежене архівування історичних даних	Розширення системи моніторингу, збереження історії параметрів

Як стає видно (Див. Табл. 3.5), головний офіс уже має розвинений набір базових технічних засобів безпеки. Зокрема, встановлені міжмережеві екрани нового покоління (NGFW), які забезпечують контроль трафіку на периметрі; реалізовано сегментацію мережі у центральному офісі; наявна система відеоспостереження, система контролю фізичного доступу (СКД) та резервне копіювання за схемою 3–2–1 із хмарною реплікацією. Серверна кімната обладнана пожежогасінням на основі Inergen, джерелами безперебійного живлення (UPS) і дизель-генератором, а також датчиками температури та вологості.

Фізичний рівень захисту представлений системами контролю доступу з персоналізованими картками, журналюванням входів, охоронною сигналізацією та камерним спостереженням, що охоплює вхідні групи, коридори, серверну та архівні приміщення. Доступ до критичних зон дозволений лише авторизованим співробітникам IT-відділу та служби безпеки.

Окремо реалізовано захист від побічних каналів витоку інформації, що охоплює такі напрямки:

- Електромагнітні канали: стіни серверної екрановані матеріалами з фольги, обладнання заземлено, встановлено фільтри на мережевих і сигнальних лініях;
- Електричні канали: використано ізолюючі трансформатори, розділення контурів живлення для критичних вузлів і фільтрацію живлення від перешкод;
- Акустичні канали: переговорні кімнати та серверна оснащені звукопоглинальними панелями, ущільненими дверима й шумогенераторами типу «Вектор-А»;
- Вібраційні канали: серверні стійки встановлені на демпфуючих опорах, кабельні траси мають антивібраційні кріплення, що виключає передавання коливань на конструкції будівлі;
- Оптичні канали: вікна офісу закриті матовими плівками й жалюзі з непрозорим покриттям, монітори розташовані під кутом, який унеможливлює зовнішнє спостереження.

Для забезпечення технічної стійкості ІТС офісу реалізовано подвійні оптичні канали зв’язку (основний і резервний), автономне енергоживлення, дубльовані комутатори ядра та систему моніторингу параметрів живлення й мікроклімату серверної кімнати.

Комплекс реалізованих технічних заходів забезпечує відповідність вимогам нормативних документів у сфері технічного захисту інформації та формує фізичний контур безпеки КСЗІ, що гарантує цілісність, конфіденційність і доступність інформаційних ресурсів.

У підсумку рівень технічного захисту головного офісу можна оцінити як достатній, з потенціалом підвищення після повного впровадження додаткових інженерних засобів моніторингу, розширення екранування приміщень та подальшої модернізації електроживлення й кліматичного контролю.

3.9 Програмні засоби захисту

Програмні засоби захисту інформації формують логічний рівень КСЗІ та забезпечують реалізацію політик доступу, автентифікації, контролю шкідливого коду, виявлення інцидентів і запобігання витокам даних. Вони дозволяють реалізувати вимоги безпеки у процесах обробки, зберігання й передавання інформації, забезпечуючи відповідність вимогам законодавства та стандартів ISO/IEC 27001 і 27002.

Для головного офісу ТОВ «ЕнергоТрансЛогістика» у місті Київ програмні засоби є основним інструментом підтримки інформаційної безпеки, оскільки саме вони забезпечують централізоване управління політиками, контроль користувачів і реагування на інциденти в корпоративному середовищі. З метою оцінки стану програмного захисту було сформовано відповідну узагальнену таблицю (Див. Табл. 3.6).

Таблиця 3.6

Програмні засоби захисту інформації в головному офісі ТОВ «ЕнергоТрансЛогістика»

Система / напрям	Функції	Поточний стан	Сильні сторони	Слабкі сторони	Рекомендовані заходи
Антивірусна система з EDR	Виявлення шкідливого ПЗ, аналіз поведінки, ізоляція вузлів	Встановлена на більшості робочих станцій і серверів	Централізована консоль, регулярне оновлення баз	Не всі вузли під EDR, відсутня ретроспектива інцидентів	Повне впровадження EDR, інтеграція з SIEM, аналітика подій
SIEM (Security Information and Event Management)	Централізований збір логів, кореляція подій, моніторинг	Частково впроваджена, збирає журнали основних серверів	Єдина точка моніторингу подій	Не всі джерела логів підключені, SCADA не інтегрована	Повна інтеграція, розширення правил кореляції, формування звітів

SOAR (Security Orchestration, Automation and Response)	Автоматизоване реагування на інциденти, плейбуки	Відсутня	–	Реагування здійснюється вручну	Впровадження SOAR, розробка плейбуків, інтеграція з SIEM
DLP (Data Loss Prevention)	Запобігання витокам даних через пошту, USB, хмарні сервіси	Не впроваджена	–	Ризик витоку через персональні канали та носії	Встановлення DLP для пошти, друку, робочих станцій
PAM (Privileged Access Management)	Контроль дій адміністраторів, аудит привілеїв	Не впроваджена	–	Адміністратори мають надлишкові права, немає журналювання	Встановлення PAM, аудит дій адміністраторів, розмежування SoD
VPN із TLS/SSL-шифруванням	Безпечний віддалений доступ співробітників і підрядників	VPN діє, TLS 1.2	Забезпечує конфіденційність з’єднань	Відсутнє MFA для всіх користувачів, немає аналітики сесій	Впровадження MFA, bastion-хостів, моніторинг VPN-сесій
Криптографічний захист (PKI, HSM, BitLocker)	Шифрування даних, управління ключами	TLS 1.2/1.3, BitLocker на ноутбуках керівників	Використання сучасних алгоритмів, сертифікати ЕЦП	Частково не зашифровані бази даних, немає HSM	Впровадження AES-256, HSM для ключів, політики ротації сертифікатів

ERP / CRM / SCADA системи	Зберігання критичних бізнес-даних	Працюють у захищеній VLAN	Розмежування ролей, аутентифікація через AD	Відсутній централізований аудит дій користувачів	Впровадження логування, кореляція подій у SIEM
Система електронного документообігу (СЕД)	Створення, підпис, архівація документів	Використовується КЕП, інтегрована з ERP	Юридична значимість електронних документів	Обмежений контроль доступу до архівів	Розширення DLP-контролю, шифрування архівів
Система резервного копіювання (Backup/DRP)	Захист даних від втрат, аварійне відновлення	Виконується за принципом 3–2–1, є хмарна реплікація	Реплікація в реальному часі, тестування відновлення	Формальний DRP без процедур реагування	Розробка DRP-документації, тренування персоналу
IAM / Active Directory	Керування обліковими записами, групами, політиками	Один ліс AD, гібридна інтеграція з хмарою	Централізоване керування обліковими записами	Частина прав розподілена вручну, немає PAM	Перегляд прав доступу, впровадження політик Least Privilege
Аналітика вразливостей (Vulnerability Scanner)	Виявлення уразливостей у ПЗ і сервісах	Локальний сканер використовується епізодично	Дає огляд стану безпеки	Відсутня регулярність перевірок	Впровадження регулярного сканування, звітність для керівництва

Як тепер видно (Див. Табл. 3.6), програмний рівень захисту в головному офісі ТОВ «ЕнергоТрансЛогістика» характеризується частковою реалізацією ключових компонентів КСЗІ. Функціонує антивірусна система з елементами

EDR, налаштована централізована консоль керування, реалізовано резервне копіювання даних та базове використання криптографічного захисту (TLS, BitLocker). Водночас низка важливих компонентів відсутня або перебуває на стадії впровадження.

Серед основних проблемних зон слід відзначити:

- Відсутність DLP – ризик витоку комерційної інформації через пошту, флеш-носії та хмарні сервіси;
- Відсутність PAM – надлишкові привілеї адміністраторів і відсутність централізованого журналювання дій;
- Обмежену інтеграцію SIEM – не всі джерела логів підключено, SCADA-сегмент залишається поза моніторингом;
- Відсутність SOAR – інциденти обробляються вручну, що збільшує час реагування;
- Часткову реалізацію VPN та криптозахисту – не впроваджено повне MFA, немає HSM для захисту ключів.

Рівень організації автентифікації користувачів можна оцінити як середній, оскільки Active Directory забезпечує централізоване керування обліковими записами, проте не всі облікові записи регулярно переглядаються, а політики доступу реалізовані не повною мірою за принципом *Least Privilege*.

Загалом програмний контур захисту підприємства має потенціал до вдосконалення. Пріоритетними напрямами підвищення зрілості КСЗІ є:

1) Впровадження DLP і PAM для контролю внутрішніх загроз.
2) Інтеграція всіх систем у SIEM з подальшою автоматизацією реагування через SOAR.
3) Модернізація криптографічного захисту з переходом на AES-256 і використанням апаратних модулів HSM.
4) Розширення MFA для всіх типів користувачів.
5) Регулярне сканування вразливостей та автоматичне створення звітів для IT-департаменту.

Реалізація цих заходів забезпечить перехід від фрагментарного до комплексного рівня безпеки, дозволить автоматизувати процеси моніторингу, реагування та контролю доступів і створить повноцінну інтегровану КСЗІ, здатну відповідати вимогам міжнародних стандартів у сфері кіберзахисту.

3.10 Організаційні заходи захисту

Організаційні заходи захисту інформації є фундаментальною основою КСЗІ, оскільки саме вони визначають правила, процедури та відповідальність усіх учасників інформаційних процесів. Якщо технічні засоби можна порівняти з інструментами, що фізично протидіють атакам, то організаційні заходи – це нормативна і методична база, яка визначає, як, коли і ким ці інструменти застосовуються. Без чітких регламентів навіть найдосконаліші технології не зможуть забезпечити належний рівень захисту.

Для підприємства «ЕнергоТрансЛогістика», яке має розгалужену інфраструктуру, десятки співробітників у головному офісі та філіях, а також співпрацює з підрядниками і мобільними працівниками, організаційні заходи набувають особливої ваги. Вони дозволяють не лише уніфікувати підходи до захисту інформації, а й зменшити ризик людського фактора, що є причиною більшості інцидентів у сфері кібербезпеки.

У рамках дослідження організаційні заходи були структуровані за ключовими напрямами: політика інформаційної безпеки, класифікація даних, управління доступами, кадрова політика, навчання персоналу, аудит та контроль, управління інцидентами, робота з підрядниками, управління змінами, план безперервності бізнесу та політика використання мобільних пристроїв. Кожен із цих напрямів був проаналізований з точки зору поточного стану, сильних і слабких сторін та рекомендацій для вдосконалення (Див. Табл. 3.7).

Таблиця 3.7

Організаційні заходи захисту на підприємстві «ЕнергоТрансЛогістика»

Напрям	Сутність заходу	Поточний стан	Сильні сторони	Слабкі сторони	Рекомендовані дії
Політика інформаційної безпеки	Єдина стратегія та правила роботи з	Наявні лише окремі інструкції (паролі,	Мінімальний набір регламентів	Відсутня комплексна політика, не покриваютьс	Розробити та затвердити політику ІБ, інтегрувати

	інформаційними ресурсами	резервне копіювання)	для базових операцій	я всі категорії даних	її у корпоративні процеси
Класифікація та категоризація даних	Поділ інформації на категорії (відкрита, службова, конфіденційна, критична)	Формально не реалізовано	Є розуміння важливості комерційної та персональної інформації	Немає формалізованої схеми класифікації, дані зберігаються без міток	Розробити систему категоризації, визначити правила обробки кожної категорії
Управління доступами	Надання доступів за принципом мінімальних привілеїв, журналювання	Є частковий контроль у серверних, використовується AD	Використовується централізована служба каталогів	Немає журналювання усіх дій, слабкий контроль у філіях	Впровадити централізовану систему IAM, інтегрувати PAM
Розподіл ролей і обов'язків (SoD)	Поділ обов'язків між співробітниками, щоб уникнути зловживань	Частково реалізовано у фінансових операціях	Є контроль подвійного підпису у бухгалтерії	В IT-адмініструванні адміністратори мають надлишкові права	Впровадити SoD для адміністраторів, аудит прав щоквартально
Кадрова політика	Перевірка співробітників, підписання NDA, ознайомлення з політиками	Підписання договорів про конфіденційність для ключових посад	Мінімальний кадровий контроль для керівних посад	Відсутність формальної перевірки рядового персоналу, немає повторних інструктажів	Впровадити процедури перевірки всіх співробітників, проводити щорічне

					оновлення NDA
Навчання персоналу	Інструктажі, тренінги, симуляції атак	Проводиться лише первинний інструктаж	Нові співробітники знайомлятся з основами ІБ	Відсутні регулярні тренінги, співробітники не знають, як діяти при атаках	Організувати регулярні тренінги, симуляції фішингових атак, навчання реагуванню на інциденти
Аудит та внутрішній контроль	Регулярна перевірка дотримання правил, аудит логів і конфігурацій	Проводиться лише при внутрішніх інцидентах	Мінімальний контроль з боку IT-відділу	Відсутня системність, немає незалежного аудиту	Впровадити регулярний аудит, підключити зовнішніх експертів
Управління інцидентами (IRP)	План реагування на інциденти, ролі та обов’язки	Формально не існує	IT-відділ іноді реагує «ад-хок»	Відсутні процедури, немає плейбуків	Розробити Incident Response Plan, тренувати співробітників за сценаріями
Робота з підрядниками	Умови доступу до ресурсів, контроль їхньої діяльності	Є базові договори про конфіденційність	Формально передбачено відповідальність підрядників	Відсутні механізми контролю виконання вимог	Встановити вимоги ІБ у контрактах, аудит підрядників

Управління змінами	Контроль змін у системах, попереднє погодження	Частково застосовується у великих проєктах	Є практика погодження значних змін	Зміни у філіях не контролюються, немає журналів	Впровадити формалізовану систему change management
Управління безперервністю (BCP)	Забезпечення функціонування при інцидентах	Формально не описано	Є резервне копіювання	Відсутній бізнес-континуїті план	Розробити BCP, провести тестування
Контроль використання мобільних пристроїв (BYOD)	Політика використання особистих пристроїв	Відсутня	–	Працівники іноді використовують особисті ноутбуки/смартфони без захисту	Розробити BYOD-політику, впровадити MDM-систему

Аналіз показав, що на підприємстві вже існують окремі елементи організаційної безпеки. Наприклад, співробітники підписують договори про нерозголошення (NDA), у бухгалтерії діє принцип подвійного підпису на фінансові операції, а в серверних приміщеннях є обмеження доступу. Призначений відповідальний за інформаційну безпеку (CISO), що формально забезпечує координацію заходів захисту. Також впроваджені інструктажі для нових співробітників і базові процедури резервного копіювання.

Однак більшість організаційних заходів перебувають лише на початковому рівні зрілості. Відсутня комплексна політика інформаційної безпеки, яка б визначала загальні принципи, цілі й засоби захисту. Класифікація даних фактично не реалізована – у компанії є розуміння цінності певної інформації, проте немає чітких правил її категоризації та маркування. Навчання персоналу обмежується первинним інструктажем, у той час як сучасні практики вимагають регулярних тренінгів і симуляцій атак.

Критичною прогалиною є відсутність формалізованого плану реагування на інциденти (Incident Response Plan). Реакція на події здійснюється «ад-хок», тобто ситуативно, без формальних сценаріїв і визначених відповідальних осіб. У разі серйозної кібератаки це призведе до затримок у реагуванні та масштабних наслідків. Аналогічно, відсутній план безперервності бізнесу (BCP), який дозволив би зберегти критичні бізнес-процеси навіть під час серйозних збоїв.

Слабкою ланкою є також взаємодія з підрядниками. Хоча договори про конфіденційність існують, вони не передбачають суворих вимог до інформаційної безпеки з боку партнерів. Це створює додаткові ризики компрометації через ланцюжок постачання.

Проблеми спостерігаються й у сфері управління доступами: адміністратори мають надлишкові права, журналювання дій здійснюється лише частково, а у філіях контроль доступів є слабким. Відсутність практики розподілу обов’язків у сфері IT робить можливими зловживання з боку співробітників з підвищеними привілеями.

Підсумовуючи, можна стверджувати, що організаційні заходи на підприємстві перебувають переважно на базовому рівні (2 із 5 за шкалою зрілості). Для виходу на високий рівень необхідно здійснити низку кроків:

- Розробити й затвердити комплексну політику інформаційної безпеки;
- Створити систему класифікації даних;
- Впровадити принцип розподілу обов’язків (SoD) у всіх процесах;
- Розробити й протестувати Incident Response Plan та BCP;
- Організувати регулярні тренінги й симуляції атак для персоналу;
- Встановити суворі вимоги до підрядників і контролювати їх дотримання;
- Впровадити централізовану систему управління доступами та журналювання дій адміністраторів.

Таким чином, організаційні заходи є тим «каркасом», на який спираються всі технічні й криптографічні інструменти. Їхній розвиток є критично важливим для того, щоб КСЗІ підприємства

«ЕнергоТрансЛогістика» функціонувала не формально, а реально забезпечувала захист інформаційних активів, мінімізувала вплив людського фактора та відповідала вимогам законодавства і міжнародних стандартів.

3.11 Рекомендації щодо підвищення рівня інформаційної безпеки

Результати комплексного аналізу технічних, організаційних і криптографічних заходів захисту на підприємстві «ЕнергоТрансЛогістика» продемонстрували наявність певних досягнень у сфері інформаційної безпеки, однак водночас виявили й значні недоліки. Наявність міжмережевих екранів нового покоління, часткове впровадження SIEM, резервне копіювання за принципом 3–2–1, використання EDR і базова кадрова політика створюють фундамент захисту, проте цей фундамент потребує зміцнення та розвитку. Для досягнення належного рівня зрілості необхідно впровадити системний підхід, що поєднує стратегію, організаційні правила та технічні засоби.

Одним із ключових напрямів розвитку є розробка стратегії інформаційної безпеки на 3–5 років. Вона повинна визначати не лише пріоритетні цілі, але й конкретні кроки їх досягнення, орієнтири для моніторингу та систему оцінки ефективності. У межах стратегії доцільно передбачити створення служби інформаційної безпеки (SOC/CERT), яка стане центром моніторингу та реагування на інциденти. SOC забезпечуватиме перехід від реактивного до проактивного підходу – від хаотичного усунення проблем до запобігання інцидентам.

Важливим напрямом є впровадження системи управління інформаційною безпекою (ISMS) відповідно до стандарту ISO/IEC 27001. Це дозволить підприємству не лише досягти відповідності міжнародним практикам, а й продемонструвати клієнтам і партнерам високий рівень зрілості. Створення ISMS передбачає каталогізацію ризиків, визначення політик, контроль виконання заходів і періодичні аудити.

На організаційному рівні необхідно зосередитися на кількох кроках. По-перше, розробити й затвердити комплексну політику інформаційної безпеки, що охоплюватиме роботу з даними, управління доступами, роботу з підрядниками та порядок реагування на інциденти. По-друге, створити систему класифікації даних, яка дозволить відрізняти критичні активи від

другорядних і застосовувати до них адекватні засоби захисту. По-третє, розширити навчання персоналу – регулярні тренінги, симуляції фішингових атак і тестування знань допоможуть знизити ризики, пов’язані з людським фактором.

Серед організаційних прогалин особливо небезпечними є відсутність формалізованих планів реагування на інциденти (IRP) і безперервності бізнесу (BCP). Саме ці документи визначають, як організація повинна діяти в умовах кризи. Розробка IRP та BCP у поєднанні з регулярними навчаннями та тестами забезпечить швидке відновлення роботи навіть після серйозних кібератак.

На технічному рівні ключовими кроками є розширення покриття NGFW та EDR на всі філії, впровадження DLP для контролю каналів витоку даних, запуск PAM для управління привілейованим доступом та уніфікація криптографічного захисту. Окремої уваги потребує централізований моніторинг. Розбудова SIEM із підключенням усіх серверів, робочих станцій, мережевих пристроїв та систем SCADA/OT дозволить отримати єдину картину безпеки. Наступним кроком стане інтеграція SOAR, що автоматизує реагування на типові інциденти й значно скоротить час від виявлення до усунення.

Для впорядкування цих заходів розроблена дорожня карта впровадження (Див. Табл. 3.8), що відображає послідовність кроків, відповідальних осіб, артефакти та очікувані результати.

Таблиця 3.8

Дорожня карта впровадження заходів ІБ

Етап (період)	Напрям	Зміст робіт (scope)	Відповідальні	Артефакти/результати	Залежності	KPI/метрики	Ризики та пом’якшення
Рік 1, Q1	Управління ІБ	Розробка та затвердж	CISO, Юрвідді	Політика ІБ, стандарт	Підтримка	Політики затвердж	Затримки погодже

		ення Політики ІБ, стандартів і процедур; запуск ISMS-реєстру ризиків	л, IT-директор	и класифікації, каталог контролів	керівництва	ені; покриття процесів ≥80 %	нь – спринт-рев'ю з керівництвом
Рік 1, Q1	Кадрові/ правові	NDA, оновлені положення про конфіденційність, шаблони договорів з підрядниками	HR, Юрвідділ	Нові шаблони NDA, договори з вимогами ІБ	Політика ІБ	100 % нових контрактів із вимогами ІБ	Опір підрядників – альтернативні варіанти умов
Рік 1, Q1	Ідентифікація/доступ	MFA для віддаленого доступу, критичних ролей; інвентар облікових записів	IT-експлуатація	Увімкнена MFA, реєстр облікових записів	Каталог AD	MFA покриття ≥60 % критичних ролей	Несумісність клієнтів – пілот + fallback
Рік 1, Q1	Криптографія	Деактивація TLS 1.0/1.1;	Архітектор ІБ	Матриця сумісності,	Інвентар сервісів	TLS ≥1.2 на 100 %	Збої сумісності –

		профілі шифрів; план HSM		Roadmap PKI/HSM		інтернет-сервісів	тестовий стенд
Рік 1, Q2	Класифікація даних	Маркування даних, політики зберігання/видалення; реєстр власників даних	CISO, Власники даних	Реєстр активів, правила маркування	Політика ІБ	100 % критичних БД з мітками	Опір бізнесу – навчання, шаблони
Рік 1, Q2	DLP – пілот	Пілот DLP: пошта + USB на 2 підрозділи	CISO, IT	Консоль DLP, політики, звіт пілоту	Класифікація даних	DLP-покриття пілоту 100 %	Хибні спрацювання – спільне тюнінг-вікно
Рік 1, Q2	PAM – пілот	Bastion, запис сесій, парольний сейф для адміністраторів	IT, CISO	Пілотний PAM, журнали адмін-дій	Інвентар привілеїв	100 % доменних адмінів через bastion	Обхід процедур – політика + моніторинг
Рік 1, Q2	Сегментація	Розділення VLAN у 2 філіях, виправлення ACL	Мережеві інженери	Оновлена схема, ACL, тести	Інвентар мережі	Зниження доступних шляхів на ≥70 %	Простій вання – план робіт вночі

		гостьови х Wi-Fi					
Рік 1, Q3	SIEM – хвиля 1	Онборди нг критичн их серверів, перимет ру, AD; базові кореляції	SOC-менедже р	Контент SIEM, дашборд и	Логи з систем	Покритт я логів ≥70 % критичн их	Перева нтаження логами – фільтри
Рік 1, Q3	Резервне копіюван ня	3–2–1 формаліз ація, тест відновле ння ERP/AL S; DR-архітект ура	IT-експлуат ація	Протоко ли відновле ння, DR-дизайн	Інвентар БД	Успіх відновле ння 100 % у RTO/RP O	Вікна простою – нічні тести
Рік 1, Q3	Навчанн я	Антифіш инг, базові тренінги ІБ; політики BYOD/ MDM	HR, CISO	Програм а тренінгів , результа ти тестів	Політика ІБ	Участь ≥90 %, фішинг-клік-рейт ≤8 %	Низька залучені сть – мікролер нінг
Рік 1, Q4	DLP – розшире ння	Розгорта ння на пошту всіх підрозді	CISO, IT	DLP-профілі, звіт покриття	Пілот DLP	Покритт я ≥80 % робочих місць	Фальшп озитиви – поетапн

		лів, друк, хмари					ий тюнінг
Рік 1, Q4	PAM – розширення	Підключення серверів БД, мережевих девайсів; JIT-доступ	IT, CISO	Повномасштабний PAM	Пілот PAM	100 % критичних адмін-сесій через PAM	Обхід SSH – тех. блок + аудит
Рік 1, Q4	IRP/BCP	Розробка Incident Response Plan та BCP; перші tabletop-вправи	CISO, Бізнес	IRP, BCP, протоколи вправ	SIEM хвиля 1	MTTD ≤60 хв, MTTR ≤8 год	Невизначені ролі – RACI-матриця
Рік 2, Q1	SOC – створення	Команда SOC 8×5; процедури, каталог плейбуків	CISO, SOC-менеджер	Операційна модель SOC	SIEM хвиля 1	Час ескалації ≤30 хв	Нестача кадрів – часковий MSSP
Рік 2, Q1	Вразливості/патчі	Централізований скан, SLA патчів;	IT, CISO	Реєстр вразливостей, звіти SLA	Політики ІБ	Закриття критичних ≤7 днів	Вікна оновлень – узгоджені вікна

		CAB-процес					
Рік 2, Q2	SIEM – хвиля 2	Онбординг журналів застосунків, пошти, проксі, VPN	SOC	Розширені правила, UEBA	SOC 8×5	Покриття логів ≥90 %	Шум – тюнінг правил
Рік 2, Q2	SOAR – пілот	Автоматизація фішингу, блокування IoC, ізоляція EDR	SOC, IT	3–5 плейбуків, KPI	SIEM хвиля 2, EDR	Автоматизація ≥40 % типових інцидентів	Хибні дії – ручне підтвердження
Рік 2, Q2	OT-безпека	OT-DMZ, брокер даних, журналювання SCADA	OT-інженери, CISO	Архітектура OT-DMZ, логи	Сегментація, SIEM	Логи OT в SIEM ≥70 %	Простій – тестовий стенд OT
Рік 2, Q3	Мікросегментація	Network Access Control, групові політики, Zero Trust	Мережеві інженери	NAC, політики доступу	Каталог користувачів	MFA покриття ≥95 %, блок lateral movement	Несумісність – поетапне включення
Рік 2, Q3	Криптографія 2.0	Впровадження HSM,	Архітектор ІБ	HSM у проді,	План HSM	100 % критичн	Міграційні вікна

		TDE усіх БД, ротація ключів		політики PKI		их БД із TDE	– DR-режим
Рік 2, Q3	Пентести	Щорічний пентест IT+OT, ремедіація	CISO, зовн. підрядник	Звіт, план усунення	SIEM/SOC	Закриття критичних ≤30 днів	Ресурсні обмеження – backlog і пріоритети
Рік 2, Q4	SOC 12×7	Розширення покриття, аналітика загроз, TI-фіди	SOC-менеджер	Playbook-каталог, звіти	SIEM+SOAR	MTTD ≤20 хв, MTTR ≤4 год	Вигорання – ротація, MSSP-бек-ап
Рік 2, Q4	DLP – повний	Політики для пошти, ендпоінтів, друку, хмар	CISO, IT	DLP-покриття 100 %	Класифікація даних	Інциденти DLP ↓ ≥60 %	Тюнінг – центр компетенцій
Рік 3, Q1	Zero Trust	Політики умовного доступу, SSO для застосунків	Архітектор ІБ	CA-правила, SSO-каталог	MFA, NAC	SSO покриття ≥80 % застосунків	Легесі – проксі/міграція

Рік 3, Q1	MDM/UEM	Керування мобільними, шифрування, контейнеризація	IT, HR	MDM-консоль, профілі	BYOD-політика	Покриття мобільних ≥95 %	Опір користувачів – комунікації
Рік 3, Q2	SOC 24×7	Повний режим, чергування, KPI	SOC-менеджер	SLO/SLA, квартальні звіти	SOC 12×7	MTTD ≤10 хв, MTTR ≤2 год	Кадри – гібрид із MSSP
Рік 3, Q2	SOAR – повний	10–15 плейбуків: фішинг, malware, VPN, DLP, OT	SOC	Каталог сценаріїв	SOAR пілот	Автоматизація ≥70 % типових інцидентів	Ескалація – подвійний контроль
Рік 3, Q3	DR-вправи	Повномасштабний DR-дрилинг, failover ERP/ALS	IT, Бізнес	Звіт DR, скоригований BCP	DR-архітектура	Успішний DR ≤ RTO/RPO	Вплив на бізнес – інформкампанія
Рік 3, Q3	Vendor Risk	Оцінка підрядників, технічні вимоги, аудит	Юрвідділ, CISO	Анкети, матриця ризиків	Політика ІБ	100 % критичних підрядників оцінені	Опір партнерів – ескалація, поетапність

Рік 3, Q4	ISO 27001	Внутрішні аудити, усунення невідповідностей, передсертифікація	CISO, Власники процесів	Звіт ISMS, коригувальні дії	ISMS зрілість	Успішний аудит Stage 1	Брак доказів – централізований реєстр
Роки 4–5	Оптимізація/зрілість	Сертифікація ISO 27001; Purple Team, CTI, безперервний контроль; DevSecOps, SBOM; розширення OT-безпеки	CISO, SOC, DevOps, OT	Сертифікат ISO, звіти purple-team, SDLC-політики	Досягнута зрілість SOC/SIEM/SOAR	Втрати часу на інцидент ↓ ≥50 %, критичні вразливості 0 при релізі	Розпорошення фокусу – портфель проєктів

Як видно (Див. Табл. 3.8), реалізація заходів поділяється на три основні етапи. Перший рік зосереджений на створенні базових політик, мінімальних технічних покращеннях та запуску пілотів DLP і PAM. Ці кроки формують основу для подальших масштабних проєктів. Другий рік акцентується на створенні SOC, масштабуванні SIEM, інтеграції SCADA та впровадженні SOAR у тестовому режимі. Третій рік завершує цикл: SOC переходить у режим

24×7, SOAR автоматизує більшість інцидентів, а компанія готується до сертифікації ISO/IEC 27001. У четвертому й п’ятому роках увага зосереджується на оптимізації та закріпленні результатів – інтеграції DevSecOps, побудові безперервного моніторингу та розширенні практик OT-безпеки.

У процесі реалізації дорожньої карти велике значення матиме управління ризиками. Серед ключових викликів – нестача кваліфікованих кадрів, складнощі інтеграції нових систем у наявну інфраструктуру, опір користувачів до багатофакторної автентифікації та мобільного управління пристроями. Подолання цих проблем можливе за рахунок поетапного впровадження, проведення пілотних проєктів, комунікаційних кампаній та залучення зовнішніх консультантів.

Очікуваними результатами виконання дорожньої карти є зниження середнього часу виявлення (MTTD) та усунення (MTTR) інцидентів у кілька разів, досягнення високого рівня зрілості КСЗІ, зменшення кількості критичних вразливостей та відповідність міжнародним стандартам. Це не лише мінімізує ризики, але й зміцнює конкурентоспроможність підприємства на ринку, підвищує довіру клієнтів і партнерів та створює основу для подальшої цифрової трансформації.

Таким чином, впровадження рекомендацій і дотримання дорожньої карти дозволить ТОВ «ЕнергоТрансЛогістика» перейти від ситуативного управління безпекою до цілісної системи, що інтегрує організаційні та технічні засоби, відповідає національним і міжнародним вимогам та забезпечує стійкість бізнесу перед сучасними кіберзагрозами.

3.12 Оцінка ефективності запропонованих заходів

Ефективність будь-якої КСЗІ визначається не лише фактом її впровадження, а й тим, наскільки реалізовані заходи справді знижують ризики та забезпечують стійкість бізнес-процесів. Для підприємства «ЕнергоТрансЛогістика», яке функціонує у висококонкурентному середовищі та оперує великими обсягами критичних даних, питання ефективності набуває особливого значення.

Оцінювання здійснюється за кількома критеріями. По-перше, перевіряється відповідність нормативно-правовим вимогам: системи мають відповідати не лише національним стандартам ДССЗЗІ, але й міжнародним нормам ISO/IEC 27001 та GDPR. По-друге, оцінюється зниження рівня ризиків: розглядається динаміка переходу від великої кількості критичних загроз до їх мінімізації завдяки організаційним і технічним заходам. По-третє, аналізується ефективність роботи технічних засобів – зменшення середнього часу виявлення (MTTD) та реагування (MTTR), скорочення кількості інцидентів, пов’язаних з людським фактором. По-четверте, береться до уваги рівень зрілості організаційних процесів – наявність політик, планів IRP та BCP, а також регулярність навчання персоналу. Нарешті, важливим критерієм є фінансовий результат – зменшення витрат на ліквідацію наслідків інцидентів і штрафів за порушення вимог регуляторів.

Для оцінки ефективності було складено розгорнуту порівняльну матрицю (Див. Табл. 3.9), яка демонструє стан підприємства до та після впровадження заходів.

Таблиця 3.9

Оцінка ефективності запропонованих заходів

Напрям	До впровадження	Після впровадження	Очікуваний ефект
Політика ІБ	Фрагментарні інструкції, відсутність єдиного документа	Комплексна політика ІБ, інтеграція в процеси	Єдність правил, контроль виконання

Класифікація даних	Відсутня	Категоризація, мітки конфіденційності, регламенти	Оптимізація витрат на захист, акцент на критичних даних
DLP	Відсутній контроль витоків	DLP для пошти, друку, USB, хмар	Зниження інсайдерських витоків на 60 %
PAM	Адміністратори з надлишковими правами	Bastion, запис сесій, JIT-доступ	Прозорість і контроль адмін-дій
SIEM/SOC	Часткове збирання логів, відсутність реагування	Повний збір логів, SOC 24×7, автоматизація	MTTD < 1 год, MTTR < 4 год
SOAR	Відсутня автоматизація	Автоматизація типових інцидентів (фішинг, malware)	Автоматичне реагування на ≥70 % подій
Криптографія	TLS 1.0/1.1, без HSM	TLS 1.2/1.3, AES-256, HSM для ключів	Захист каналів і даних, мінімізація витоків
Фізична безпека	Нерівномірний рівень у філіях	СКД, відеоспостереження, пожежогасіння	Зменшення фізичних інцидентів
Навчання персоналу	Лише первинний інструктаж	Регулярні тренінги, симуляції атак	Зменшення фішинг-клікрейту до <5 %
BCP/DRP	Відсутній формалізований план	Документовані сценарії, тестування	Мінімізація простоїв, бізнес-стійкість
Управління доступами	Відсутнє централізоване управління, локальні акаунти	IAM-система, MFA, ротація паролів	Скорочення компрометацій облікових записів
Моніторинг мережі	Фрагментарний, лише у ЦОД	Централізований моніторинг, IDS/IPS у всіх сегментах	Швидке виявлення аномалій,

			запобігання lateral movement
Сегментація мережі	Плоска архітектура у філіях	VLAN, Zero Trust, мікросегментація	Зниження ризику розповсюдження атак
Управління вразливостями	Реактивне патчування, без SLA	Централізований сканер, SLA ≤7 днів для критичних	Зменшення експлуатаційних вразливостей
Резервне копіювання	Копії нерегулярні, без перевірки	3–2–1 схема, регулярні DR-тести	100 % відновлення критичних сервісів
Управління інцидентами (IRP)	Відсутній формалізований процес	План реагування, плейбуки, регулярні вправи	Скоординовані дії, зменшення хаосу під час атак
Робота з підрядниками	Базові NDA, без перевірки	Вимоги ІБ у договорах, регулярні аудити	Менші ризики через ланцюжок постачання
Кадрова політика	Перевірка лише ключових посад	Скринінг усіх співробітників, щорічне NDA	Менше інсайдерських загроз
BYOD/MDM	Відсутня політика	BYOD-правила, MDM/UEM	Контроль мобільних пристроїв, шифрування
DevSecOps	Безпека відокремлена від розробки	Інтеграція ІБ у SDLC, SAST/DAST	Зменшення вразливостей у коді
OT-безпека	Обмежений контроль SCADA	OT-DMZ, брокер даних, інтеграція у SIEM	Захист виробничих процесів
Аудит і контроль	Проводиться епізодично	Регулярний внутрішній і зовнішній аудит	Системність і прозорість безпеки
Стійкість до фішингу	Працівники легко відкривають листи	Симуляції атак, навчання, блокування URL	Зниження клікрейту на ≥80 %

Фінансові наслідки	Високі витрати на ліквідацію інцидентів	Зниження інцидентів і штрафів	Економія до 30–40 % витрат на кіберризики

Як показано (Див. Табл. 3.9), зміни стосуються практично всіх сфер. Якщо до впровадження заходів безпека носила фрагментарний характер (окремі інструкції, відсутність централізованого управління доступами, слабка сегментація мережі), то після реалізації дорожньої карти підприємство отримує цілісну, багаторівневу систему захисту. Особливо значним є ефект у напрямі управління доступами: завдяки впровадженню IAM та PAM адміністративні права стають контрольованими, а зловживання практично унеможливлюються.

Важливим результатом є й інтеграція SIEM, SOC та SOAR, яка дозволяє скоротити середній час виявлення інцидентів з кількох днів до години, а реагування – до 2–4 годин. Автоматизація типових сценаріїв у SOAR значно зменшує навантаження на персонал і підвищує швидкість прийняття рішень. У сфері криптографії відбувається відмова від застарілих протоколів TLS 1.0/1.1, впровадження AES-256 та використання HSM для управління ключами, що гарантує захист каналів і баз даних.

Не менш важливим є розвиток організаційних заходів: регулярні навчання та симуляції атак знижують рівень успішності фішингових кампаній у кілька разів, а плани IRP та BCP забезпечують чітку координацію дій у кризових ситуаціях. У сфері роботи з підрядниками вводяться додаткові вимоги до інформаційної безпеки та аудити, що знижує ризики через ланцюжок постачання.

Загалом ефективність запропонованих заходів можна оцінити як високий рівень зрілості. Компанія переходить від хаотичного реагування до системного управління безпекою, що відповідає як національним, так і міжнародним стандартам. Очікуваний результат – зниження кількості критичних інцидентів

щонайменше на 60–70 %, підвищення довіри клієнтів та партнерів і зменшення фінансових втрат, пов’язаних з інцидентами, на 30–40 %.

Таким чином, оцінка ефективності підтверджує, що впровадження запропонованих технічних і організаційних рішень створює реальний захисний контур, який забезпечує кіберстійкість та безперервність бізнес-процесів підприємства «ЕнергоТрансЛогістика».

3.13 Висновки до третього розділу

У третьому розділі роботи було представлено модель побудови КСЗІ для підприємства «ЕнергоТрансЛогістика», що дозволило сформувати цілісне уявлення про стан інформаційної безпеки та напрями її вдосконалення. Аналіз показав, що вихідні умови організації характеризувалися частковим впровадженням технічних засобів, обмеженим рівнем організаційних заходів і відсутністю стратегічного підходу до управління ризиками. Це створювало ризики для забезпечення конфіденційності, цілісності та доступності інформаційних активів.

У ході дослідження було здійснено обстеження ІТС підприємства, проведено ідентифікацію інформаційних потоків, побудовано модель порушника та модель загроз. Результати показали, що найбільш небезпечними є інсайдерські дії співробітників, фішингові атаки, зловживання підрядників, експлуатація вразливостей мережевої інфраструктури та ризики, пов’язані з використанням застарілих криптографічних протоколів.

Було визначено рівень захищеності об’єкта, який оцінено як середній: частина технічних засобів (NGFW, антивірусні рішення, резервне копіювання) функціонують ефективно, однак значна кількість критичних напрямів (DLP, PAM, SOAR, централізоване управління доступами, BCP/IRP) залишаються недостатньо розвиненими. Це підтвердили результати побудованих матриць загроз, порушників і зрілості.

Запропоновані технічні та організаційні заходи передбачають створення комплексної політики інформаційної безпеки, впровадження DLP і PAM, уніфікацію криптографічного захисту, розширення SIEM і SOC до рівня 24×7, автоматизацію реагування за допомогою SOAR, удосконалення навчання персоналу та формалізацію IRP і BCP. Оцінка ефективності таких заходів показала, що їх реалізація дозволить знизити кількість критичних інцидентів на 60–70 %, зменшити фінансові втрати на 30–40 % і забезпечити відповідність міжнародним стандартам ISO/IEC 27001.

Таким чином, розділ 3 довів доцільність та ефективність продуманого підходу до побудови КСЗІ. Підприємство «ЕнергоТрансЛогістика» завдяки реалізації запропонованої моделі переходить від фрагментарного та реактивного управління безпекою до системної та проактивної моделі, що гарантує підвищення кіберстійкості, зміцнення конкурентних позицій та підвищення довіри партнерів і клієнтів.

ВИСНОВКИ

У результаті виконаної роботи було поступово досліджено теоретичні, методологічні та практичні аспекти побудови КСЗІ для типового ОІД. Поставлена мета – розробка моделі КСЗІ з урахуванням сучасних кіберзагроз, нормативних вимог та міжнародних стандартів – досягнута шляхом виконання низки взаємопов’язаних завдань.

У першому розділі розглянуто теоретичні засади інформаційної безпеки, проаналізовано сучасні кіберзагрози, статистику порушень в Україні та світі, а також досліджено нормативно-правову базу, що регламентує створення та функціонування КСЗІ. Це дозволило сформувати цілісне уявлення про сучасний стан проблеми та обґрунтувати актуальність розробки систем захисту для ОІД.

У другому розділі досліджено методологічні підходи до побудови КСЗІ. Було розглянуто класифікацію ОІД, етапи створення комплексних систем безпеки, методи технічного, криптографічного та організаційного захисту, а також порядок упровадження систем і проходження державної експертизи. Це створило методичне підґрунтя для практичної частини роботи.

У третьому розділі на прикладі умовного підприємства **«ЕнергоТрансЛогістика»** було розроблено модель побудови КСЗІ. Проведено обстеження ІТС, виявлено та описано інформаційні потоки, побудовано моделі порушників і загроз, визначено рівень захищеності об’єкта та сформовано профіль безпеки. Запропоновано комплекс технічних та організаційних заходів, серед яких – впровадження DLP, PAM, SIEM/SOC, SOAR, сучасних криптографічних засобів, сегментації мережі, політик безпеки, системного навчання персоналу та планів IRP/BCP. На основі побудованих матриць і порівняльних таблиць оцінено ефективність заходів, що показало зменшення критичних ризиків на 60–70 %, зниження витрат на ліквідацію наслідків інцидентів на 30–40 % та підвищення рівня зрілості системи безпеки з базового до високого.

Наукова новизна роботи полягає у складному підході до побудови КСЗІ, який передбачає поєднання технічних, організаційних і криптографічних засобів захисту в єдиній архітектурі, що відповідає як вітчизняним нормативним вимогам, так і міжнародним стандартам ISO/IEC 27001. Практичне значення полягає у можливості використання запропонованої моделі як методологічної основи для впровадження систем захисту на реальних підприємствах, незалежно від галузі та масштабу.

Таким чином, робота довела необхідність системного та проактивного підходу до забезпечення інформаційної безпеки. Запропонована модель побудови КСЗІ для типового ОІД дозволяє ефективно знижувати рівень загроз, підвищувати кіберстійкість та забезпечувати безперервність бізнес-процесів. Реалізація результатів дослідження може стати практичною основою для організацій, які прагнуть відповідати сучасним викликам у сфері кібербезпеки та підвищити свою конкурентоспроможність у цифровому середовищі.

Оформлення результатів цього дослідження здійснювалося згідно з методичними рекомендаціями кафедри [61].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Задворний Д.С., Козачок В.А. «Методи та засоби побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності». Студентська наукова конференція «Безпека інформаційно-комунікаційних систем» БІКС’2025. Київ: Університет Грінченка, 26.10.2025. 55–58 с.
2. Задворний, Д., Козачок, В., Черевик, В., Бодненко, Д., & Добришин, Ю. (2025). Методи та засоби побудови комплексної системи захисту інформації типового об’єкта інформаційної діяльності. Кібербезпека: освіта, наука, техніка, 3(31), 762–772. https://doi.org/10.28925/2663-4023.2025.31.1073
3. 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
4. ДСТУ 24745:2023. Інформаційні технології. Кібербезпека. Загальні положення. Київ: Мінекономрозвитку України, 2023. 28 с.
5. Chen, T. Advances in Persistent Threats. IEEE Security & Privacy, 2014. №12(3). P. 16–25.
6. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР.
7. 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
8. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva: ISO, 2022.

9. Українська правда. Україна за рік зафіксувала понад 4 тисячі кібератак. 2025. URL: https://www.pravda.com.ua/news/2023/11/18/7429315.
10. CERT-UA. Оперативний звіт щодо кібератак у першому півріччі 2024 року. Київ: Держспецзв'язку, 2024.
11. Кіберполіція України. Річний звіт про діяльність у сфері протидії кіберзлочинності. Київ: МВС України, 2024.
12. Мін'юст України. Повідомлення про тимчасове призупинення роботи державних реєстрів у грудні 2024 року. Київ: 2024.
13. World Economic Forum. Global Cybersecurity Outlook 2025. Geneva: WEF, 2025.
14. IBM Security. Cost of a Data Breach Report 2024. Armonk: IBM, 2024.
15. Конституція України: Офіційний текст від 28.06.1996 № 254к/96-ВР із змінами та доповненнями. Київ: Відомості Верховної Ради України.
16. Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»: Постанова КМУ від 03.06.2022 № 645.
17. Закон України «Про інформацію» від 02.10.1992 № 2657-XII.
18. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Кодекс практики управління інформаційною безпекою. Київ: Мінекономрозвитку України, 2015.
19. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. Gaithersburg: NIST, 2020.
20. Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ) України. Порядок проведення державної експертизи у сфері технічного захисту інформації. Київ: Офіційний вісник України, 2010.
21. В.А. Козачок. Концептуальні засади створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Київ: ДУТ, Збірник наукових праць «Зв'язок», 2014 №3 (109). 8-13 с.

22. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII.
23. Г.М. Гулак, В.А. Козачок, П.М. Складанний, М.О. Бондаренко, Б.В. Вовкотруб. Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. Київ: ДУТ, Збірник наукових праць «Сучасний захист інформації», 2017 вип. №2(30). 65-71 с.
24. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI.
25. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on information security risk management. Geneva: ISO, 2022.
26. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. Gaithersburg: NIST, 2024.
27. International Telecommunication Union (ITU). Global Cybersecurity Agenda. Geneva: ITU, 2023.
28. European Union Agency for Cybersecurity (ENISA). Annual Threat Landscape Report 2024. Athens: ENISA, 2024.
29. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 20.04.2025 № 4336-IX.
30. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
31. ISO/IEC 27009:2020. Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements. Geneva: ISO, 2020.
32. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108+). Strasbourg: Council of Europe, 2018.
33. ENISA. Guidelines for Operators of Essential Services: Cybersecurity Requirements. Athens: ENISA, 2023.

34. Шевченко, С., Жданова, Ю., & Кія, О. (2025). Напівавтоматизований інструмент багатостандартної оцінки кіберзрілості організації на основі NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8. Кібербезпека: освіта, наука, техніка, 3(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004
35. Гулак Г., Жданова Ю., Складанни П., Гулак Є., Корнієць В. (2022) Уразливості шифрування коротких повідомлень в мобільних інформаційно-комунікаційних системах об'єктів критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(17), 145–158. https://doi.org/10.28925/2663-4023.2022.17.145158
36. В.А. Козачок, Ю.Б. Коваленко. Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах. Київ: ДУТ, Збірник наукових праць «Сучасний захист інформації», 2015 вип. №1. 41-47 с.
37. В.А. Козачок, Р.В. Киричок, П.М. Складанний, В.Л. Бурячок, Г.М. Гулак. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення // Наукові записки Українського науково-дослідного інституту зв'язку. 2016 №3(43). 48-61 с.
38. 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
39. Scarfone, K., Mell, P. Guide to Intrusion Detection and Prevention Systems (NIST SP 800-94). Gaithersburg: NIST, 2007.
40. Menezes, A., Van Oorschot, P., Vanstone, S. Handbook of Applied Cryptography. Boca Raton: CRC Press, 2019.
41. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization Project. Gaithersburg: NIST, 2023.

42. 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
43. ISO/IEC 27035-1:2016. Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. Geneva: ISO, 2016.
44. Державна служба спеціального зв'язку та захисту інформації України. Методичні рекомендації щодо створення комплексних систем захисту інформації. Київ: ДССЗЗІ, 2022.
45. Постанова Кабінету Міністрів України «Про затвердження вимог до захисту інформації в інформаційно-телекомунікаційних системах»: Постанова КМУ від 29.03.2006 № 373 (зі змінами).
46. Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ). Звітність про проведення державної експертизи у сфері ТЗІ. Київ: ДССЗЗІ, 2023.
47. ISO/IEC 27035-2:2016. Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response. Geneva: ISO, 2016.
48. Міністерство цифрової трансформації України. Звіт про впровадження системи «Дія» та її КСЗІ. Київ: Мінцифра, 2023.
49. Державна міграційна служба України. Технічний опис Єдиного державного демографічного реєстру. Київ: ДМСУ, 2022.
50. Національний банк України. Вимоги до інформаційної безпеки та кіберзахисту банківських установ. Київ: НБУ, 2022.
51. Укренерго. Презентація заходів кіберзахисту після атак 2015–2016 рр. Київ: Укренерго, 2021.
52. eHealth Ukraine. Офіційний звіт про сертифікацію КСЗІ у сфері охорони здоров'я. Київ: МОЗ України, 2023.

53. European Union Agency for Cybersecurity (ENISA). NIS2 Implementation Guide. Athens: ENISA, 2023.
54. National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0 – Implementation Examples. Gaithersburg: NIST, 2024.
55. 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
56. 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
57. 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
58. D. Shevchuk, et al., Designing Secured Services for Authentication, Authorization, and Accounting of Users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.
59. P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3050 (2023) 240-245
60. S. Shevchenko, et al., Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 158–167.
61. Жданова, Ю. Д., Складанний, П. М., & Шевченко, С. М. (2023). Методичні рекомендації до виконання та захисту кваліфікаційної роботи

магістра для студентів спеціальності 125 Кібербезпека та захист інформації.
https://elibrary.kubg.edu.ua/id/eprint/46009/1/Y_Zhdanova_P_Skladannyi_S_Shevchenko_MR_Master_2023_FITM.pdf