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:

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Виконав

студент групи БІКСм-1-24-1.4д

Остапчук Вадим Русланович

Науковий керівник

к. т. н., доцент

Козачок В.А.

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

«Затверджую»
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

Остапчуку Вадиму Руслановичу

1. Тема роботи: Забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури;

керівник Козачок Валерій Анатолійович;

затверджені наказом ректора від «21» серпня 2025 р. №482

2. Термін подання студентом роботи «01» грудня 2025 р.

3. Вихідні дані до роботи: Нормативно-правові акти України у сфері захисту критичної інфраструктури та кібербезпеки, міжнародні стандарти ISO/IEC 27001, IEC 62443, NIST Cybersecurity Framework, наукові публікації з питань інформаційної безпеки Supervisory Control and Data Acquisition; методи аналізу загроз та уразливостей, оцінки ризиків, моделювання загроз, системного підходу; технології Supervisory Control and Data Acquisition - систем, IDS/IPS, сегментації мережі; алгоритми виявлення аномалій та оцінки ризиків; методи кількісної та якісної оцінки ризиків інформаційної безпеки.

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

4.1 Дослідити теоретичні та нормативно-правові основи забезпечення інформаційної безпеки на об'єктах критичної інфраструктури, проаналізувати сучасні кіберзагрози та нормативну базу .

4.2 Розробити порядок створення систем захисту інформації на об'єкті критичної інфраструктури, створити алгоритм визначення актуальних загроз та методику підвищення рівня інформаційної безпеки автоматизованої системи управління.

4.3 Розробити практичні рекомендації щодо забезпечення інформаційної безпеки конкретного об'єкта критичної інфраструктури на основі аналізу загроз та вразливостей Supervisory Control and Data Acquisition - систем.

5 Перелік графічного матеріалу:

Презентація доповіді, виконана в Microsoft PowerPoint.

6 Дата видачі завдання «15» лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів підготовки роботи	Термін виконання	Примітка
1.	Уточнення постановки завдання	15.02.2025 – 22.02.2025	Виконано
2.	Аналіз літератури	23.02.2025 – 01.03.2025	Виконано
3.	Обґрунтування вибору рішення	01.03.2025- 03.03.2025	Виконано
4.	Збір даних	20.09.2025- 16.10.2025	Виконано
5.	Виконання та оформлення розділу 1.	17.10.2025- 25.10.2025	Виконано
6.	Виконання та оформлення розділу 2.	26.10.2025- 05.11.2025	Виконано
7.	Виконання та оформлення розділу 3.	05.11.2025- 15.11.2025	Виконано
8.	Вступ, висновки, реферат	16.11.2025- 20.11.2025	Виконано
9.	Апробація роботи на науково-методичному семінарі та/або науково-технічній конференції	24.11.2025	Виконано
10.	Оформлення та друк текстової частини роботи	10.12.2025	Виконано
11.	Оформлення презентацій	04.12.2025- 12.12.2025	Виконано
12.	Отримання рецензій	02.12.2025	Виконано
13.	Попередній захист роботи	21.11.2025	Виконано
14.	Захист в ЕК	16.12.2025- 18.12.2025	Виконано

Студент _____ Остапчук Вадим Русланович
(підпис) (прізвище, ім’я, по батькові)

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

РЕФЕРАТ

Кваліфікаційна робота присвячена технологіям забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури.

Робота складається зі вступу, трьох розділів, що містять 7 рисунків та 2 таблиці, висновків і списку використаних джерел, який налічує 60 найменувань. Загальний обсяг роботи становить 111 сторінок.

Об’єктом дослідження в роботі є процес забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури.

Предметом дослідження є методи, технології та організаційні механізми побудови комплексних систем захисту інформації в автоматизованих системах управління критично важливими об'єктами.

Метою роботи є підвищення рівня захищеності автоматизованих систем управління об'єктами критичної інфраструктури від сучасних кіберзагроз шляхом розроблення комплексу науково обґрунтованих рекомендацій щодо вдосконалення систем інформаційної безпеки.

Для досягнення мети необхідно вирішити такі завдання у роботі:

- проведено аналіз існуючих підходів до забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури;
- досліджено особливості архітектури, принципи функціонування та вразливості автоматизованих система управління, які впливають на рівень їх захищеності;
- обґрунтовано необхідність комплексного підходу до організаційного, технічного та нормативно-правового забезпечення інформаційної безпеки автоматизованих систем управління в Україні;

- охарактеризувати досвід зарубіжних країн щодо побудови систем кіберзахисту промислових і критичних інформаційних систем;
- провести аналіз основних загроз і типових кібератак на автоматизовані системи управління, визначити потенційні шляхи їх реалізації;
- розробити пропозиції та рекомендації щодо вдосконалення системи забезпечення інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури.

Наукова новизна одержаних результатів полягає в тому, що в роботі запропоновано удосконалений алгоритм визначення актуальності загроз безпеці інформації з урахуванням коефіцієнта небезпеки та специфіки енергетичних об'єктів критичної інфраструктури, розроблено методику підвищення рівня інформаційної безпеки автоматизованих систем управління на основі п'яти функцій, чотирьох рівнів захисту та профілів захищеності, та отримано комплекс практичних рекомендацій щодо забезпечення кібербезпеки Supervisory Control and Data Acquisition систем з економічним обґрунтуванням доцільності їх впровадження.

Галузь застосування. Запропоновані підходи можуть бути використані для створення та модернізації систем кіберзахисту на об’єктах критичної інфраструктури - у галузях енергетики, транспорту, промисловості, телекомунікацій, а також у державних інформаційних системах.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ, КРИТИЧНА ІНФРАСТРУКТУРА, КІБЕРЗАГРОЗИ, СЕГМЕНТАЦІЯ МЕРЕЖ, МЕРЕЖЕВІ ПРОТОКОЛИ БЕЗПЕКИ.

ЗМІСТ

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АСУ - автоматизована система управління

АСУ ТП - автоматизована система управління технологічними процесами

ІБ - інформаційна безпека

ІКС - інформаційно-комунікаційна система

ІКСМ - інформаційно-комунікаційна система та мережа

ІТС - інформаційно-телекомунікаційна система

КСЗІ - комплексна система захисту інформації

КСІІ - критична система інформаційної інфраструктури

ОКІ - об'єкт критичної інфраструктури

ПЛК - програмований логічний контролер

AES (Advanced Encryption Standard) - стандарт симетричного шифрування

CERT-UA (Computer Emergency Response Team of Ukraine) - Команда реагування на комп'ютерні надзвичайні події України

DMZ (Demilitarized Zone) - демілітаризована зона

DoS (Denial of Service) - відмова в обслуговуванні

HMI (Human-Machine Interface) - інтерфейс людина-машина / операторська станція

IDS/IPS Intrusion Detection/Prevention System) - система виявлення/запобігання вторгнень

IP (Internet Protocol) - інтернет-протокол

NIST (National Institute of Standards and Technology) - Національний інститут стандартів і технологій

RTU (Remote Terminal Unit) - віддалений термінальний пристрій

SCADA (Supervisory Control and Data Acquisition) - диспетчерське управління та збір даних

SIEM (Security Information and Event Management) - управління інформацією про безпеку та подіями

SOC (Security Operations Center) - центр операцій безпеки

SP (Special Publication) - спеціальна публікація

USB (Universal Serial Bus) - універсальна послідовна шина

VLAN (Virtual Local Area Network) - віртуальна локальна мережа

VPN (Virtual Private Network) - віртуальна приватна мережа

ВСТУП

Актуальність теми. Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням кількості та складності кіберзагроз, спрямованих на об'єкти критичної інфраструктури. За даними джерела [1] Global Threat Landscape Report 2025, у 2024 році кількість кібератак зросла на 87% порівняно з попереднім роком, при цьому найбільш вразливими виявилися енергетичні системи, транспортні мережі, телекомунікації та фінансові установи. В Україні ситуація є особливо напруженою – у 2024 році інтенсивність кібератак на об'єкти критичної інфраструктури збільшилася на 48%, що зумовлено гібридною війною та синхронізованими атаками на державні та промислові системи.

Автоматизовані системи управління технологічними процесами (АСУ ТП), зокрема SCADA-системи, становлять основу функціонування критичної інфраструктури та контролюють життєво важливі процеси в енергетиці, на транспорті, у водопостачанні та інших галузях. Порушення їх функціонування може призвести до катастрофічних наслідків – від масових відключень електроенергії до техногенних катастроф та загрози життю людей. Досвід кібератак на українську енергетику у 2015-2016 роках (BlackEnergy, Industroyer) продемонстрував реальність таких загроз та критичну необхідність посилення захисту промислових систем управління.

Водночас аналіз стану інформаційної безпеки АСУ ТП на об'єктах критичної інфраструктури України виявляє численні системні проблеми: відсутність належної сегментації мереж, використання незашифрованих промислових протоколів, недосконалі механізми автентифікації, брак систем виявлення вторгнень та недостатню підготовку персоналу. За даними CERT-UA, у 2025 році фіксується в середньому 15 інцидентів щодня, при цьому 73% успішних атак починаються з фішингу. Нормативно-правова база у сфері захисту критичної інфраструктури потребує подальшого розвитку та

гармонізації з міжнародними стандартами IEC 62443, ISO/IEC 27001 та NIST SP 800-82.

Більшість об'єктів критичної інфраструктури стикаються з низкою проблемних питань у сфері управління ризиками інформаційної безпеки, зокрема:

1. неможливість раннього виявлення та ідентифікації актуальних кіберзагроз для промислових систем управління;
2. відсутність методології комплексної оцінки ризиків з урахуванням специфіки технологічних процесів та потенційних наслідків для критичної інфраструктури;
3. відсутність чітких критеріїв оцінювання ризиків інформаційної безпеки АСУ ТП, на основі яких здійснюється порівняльний аналіз для подальшої обробки ризику;
4. відсутність планів реагування на кіберінциденти та відновлення функціонування критичних систем;
5. недосконаліть системи обміну інформацією про загрози та вразливості між операторами критичної інфраструктури;
6. складність адаптації міжнародних методик управління ризиками до специфіки вітчизняних об'єктів критичної інфраструктури.

За таких умов розроблення науково обґрунтованих підходів до забезпечення інформаційної безпеки автоматизованих систем управління об'єктами критичної інфраструктури на основі ризик-орієнтованого підходу набуває особливої актуальності та становить важливе завдання як для теорії інформаційної безпеки, так і для практики захисту критично важливих об'єктів держави.

Вище перелічене підтверджує актуальність даного дослідження.

Мета роботи полягає у підвищенні рівня захищеності автоматизованих систем управління об'єктами критичної інфраструктури від сучасних кіберзагроз шляхом розроблення комплексу науково обґрунтованих рекомендацій щодо вдосконалення систем інформаційної безпеки на основі ризик-орієнтованого підходу.

Для досягнення цієї мети в роботі необхідно вирішити такі **завдання**:

1. систематизувати теоретичні основи та нормативно-правову базу забезпечення інформаційної безпеки об'єктів критичної інфраструктури, проаналізувати статистику та сучасні тенденції кіберзагроз;
2. дослідити порядок створення комплексних систем захисту інформації та систем управління інформаційною безпекою на об'єктах критичної інфраструктури;
3. проаналізувати міжнародний досвід забезпечення інформаційної безпеки критичних систем інформаційної інфраструктури в різних країнах світу;
4. розробити алгоритм визначення актуальних загроз безпеці інформації та методику підвищення рівня інформаційної безпеки автоматизованих систем управління критично важливими об'єктами;
5. провести детальний аналіз обраного об'єкта критичної інфраструктури, виявити загрози та вразливості його інформаційної безпеки, здійснити оцінку ризиків;
6. розробити практичні рекомендації щодо забезпечення інформаційної безпеки на досліджуваному об'єкті критичної інфраструктури з обґрунтуванням економічної доцільності їх впровадження.

Виходячи з цього, **об'єктом дослідження** є процеси забезпечення інформаційної безпеки автоматизованих систем управління об'єктами критичної інфраструктури. **Предмет дослідження –** методи, технології та

організаційні механізми побудови комплексних систем захисту інформації в автоматизованих системах управління критично важливими об'єктами на основі оцінки та управління ризиками інформаційної безпеки.

Методи дослідження. Для досягнення мети та вирішення поставлених завдань у роботі застосовано такі наукові методи: системний аналіз – для дослідження архітектури та вразливостей промислових систем управління; методологія оцінки ризиків NIST SP 800-82 – для визначення актуальності загроз та їх потенційного впливу, порівняльний аналіз – для вивчення міжнародного досвіду кіберзахисту критичної інфраструктури США, країн ЄС та інших держав, метод моделювання – для розроблення алгоритму визначення загроз та методики підвищення рівня інформаційної безпеки.

Наукова новизна одержаних результатів. Наукова новизна полягає в тому, що в роботі запропоновано удосконалений алгоритм визначення актуальності загроз безпеці інформації з урахуванням коефіцієнта небезпеки та специфіки енергетичних об'єктів критичної інфраструктури, розроблено методику підвищення рівня інформаційної безпеки автоматизованих систем управління на основі п'яти функцій, чотирьох рівнів захисту та профілів захищеності, та отримано комплекс практичних рекомендацій щодо забезпечення кібербезпеки SCADA - систем з економічним обґрунтуванням доцільності їх впровадження.

Теоретичне та практичне значення роботи полягає в обґрунтуванні необхідності та дослідженні можливості впровадження комплексної системи захисту інформації на об'єктах критичної інфраструктури на основі ризик-орієнтованого підходу. Результати дослідження впроваджені у вигляді конкретних технічних та організаційних рекомендацій для посилення захисту автоматизованої системи управління умовного об'єкта критичної інфраструктури та можуть бути використані при створенні, модернізації та експлуатації систем кіберзахисту на інших об'єктах критичної інфраструктури.

Галузь застосування. Результати роботи можуть бути використані для впровадження комплексних систем захисту інформації на об'єктах критичної інфраструктури в галузях енергетики, транспорту, телекомунікацій та оборонної промисловості на основі ризик-орієнтованого підходу, а також як матеріал для використання у навчальному процесі при підготовці фахівців з інформаційної безпеки та кіберзахисту.

Апробація результатів дипломної роботи. Основні положення роботи викладалися

1) в тезах доповіді на Студентській науковій конференції «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 24 листопада 2025 року) [2].

2) в статті в журналі «Кібербезпека: освіта, наука, техніка» - стаття прийнята до опублікування (2025) [3].

Розділ 1. ТЕОРЕТИЧНІ ТА НОРМАТИВНО-ПРАВОВІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та класифікація об'єктів критичної інфраструктури

Об'єкти критичної інфраструктури (ОКІ) - об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [4].

Об'єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

Об'єкти критичної інфраструктури відіграють ключову роль у функціонуванні суспільства, економіки та безпеки країни. Це спеціальні об'єкти, без яких неможливе нормальне функціонування суспільства або які можуть стати об'єктом спеціальної уваги через свою важливість.

Типи об'єктів критичної інфраструктури можуть включати, але не обмежуються:

- Енергетичні системи: Це можуть бути електростанції, підстанції, газопроводи, нафтопроводи та інші системи, які забезпечують постачання енергії.
- Транспортні системи: Вони включають залізниці, аеропорти, порти, мости, тунелі, автомагістралі та інші мережі, які забезпечують рух людей та товарів.
- Телекомунікації: Це системи зв'язку, включаючи мобільних операторів, інтернет-провайдерів, супутникові мережі, які забезпечують зв'язок і обмін даними.

- Водопостачання та очищення води: Об'єкти, що забезпечують доступ до питної води, водопостачання та системи очищення води.
- Фінансові установи: Банки, біржі, платіжні системи - системи, які забезпечують функціонування фінансової системи.
- Медичні установи: Це лікарні, клініки, аптеки, які надають медичні послуги.
- Інформаційні технології та Інтернет: Інфраструктура, яка забезпечує доступ до інформації, оброблення даних та функціонування Інтернету.

ОКІ вважаються критичними через їхню важливість для економіки, безпеки та добробуту суспільства. Тому, вони можуть стати об'єктом уваги для кіберзлочинців, терористичних груп чи інших зловмисників, які можуть намагатися завдати шкоду або спричинити перешкоди їхньому нормальному функціонуванню.

Захист об'єктів критичної інфраструктури від кіберзагроз стає все більш важливим у світі, де технології стають ключовими для практично кожної сфери діяльності. Однак, важливо пам'ятати, що безпека ОКІ - це завдання, яке вимагає постійного вдосконалення, моніторингу та реагування на змінюючіться загрози.

Визначення критичності об'єктів критичної інфраструктури має велике значення, оскільки це визначає, які об'єкти та системи вважаються критичними для функціонування суспільства та економіки.

Щоб визначити критичні об'єкти, необхідно враховувати кілька ключових критеріїв [5]:

- Вплив на суспільство: Це оцінка, як об'єкт впливає на повсякденне життя людей. Наприклад, електростанції забезпечують електроенергією міста, тож їх відсутність може призвести до кризової ситуації у суспільстві.

- Вплив на економіку: Важливість об'єкта для економіки. Наприклад, фінансові установи, банки, біржі, є серцем фінансової системи та є критичними для функціонування економіки.
- Потенційний ризик: Оцінка можливого ризику, який може виникнути в разі недоліку, втрати доступу або атаки на об'єкт. Наприклад, системи водопостачання або медичні установи можуть бути критичними в разі їхнього відмову чи порушення.
- Стратегічний або символічний важливість: Деякі об'єкти можуть мати стратегічне значення для країни або символічне значення для нації.
- Визначення критичності об'єктів критичної інфраструктури вимагає не лише технічного аналізу, але й ретельної оцінки їхньої важливості для суспільства. Цей підхід дозволяє краще розуміти, які об'єкти потребують особливої уваги та заходів з кіберзахисту для забезпечення безпеки, стійкості та продовження їхнього нормального функціонування в умовах загроз.

Критичні об'єкти мають стратегічне значення для функціонування суспільства. Їх порушення або недолік може призвести до серйозних наслідків, включаючи значний вплив на економіку, безпеку, здоров'я громадян та соціальну стабільність.

При оцінці критичності об'єктів критичної інфраструктури, необхідно також враховувати потенційні загрози та вразливості, які можуть призвести до великих збитків або відмови в роботі. Кіберзагрози, природні катастрофи, технічні відмови або навіть акти тероризму - усі ці фактори можуть вплинути на критичну інфраструктуру.

Крім того, визначення критичності допомагає у створенні стратегій та планів дій для підвищення рівня захисту. Вироблення протоколів реагування

на можливі загрози та забезпечення належного рівня кіберзахисту - важливі аспекти в управлінні ризиками для критичних об'єктів.

Додатково, оцінка критичності допомагає приділити увагу ресурсів та фінансів для покращення захисту та виявлення найбільш критичних моментів, де можливий найбільший вплив заходів кіберзахисту.

Порядок визнання об’єкта критичною інфраструктурою встановлений Кабінетом Міністрів України та станом на 2023 рік регламентується Постановою № 1109 [6]. А от рішення щодо такого визнання приймають секторальні органи — державні органи, відповідальні за захист секторів чи підсекторів критичної інфраструктури.

В цілому, визначення критичності об'єктів критичної інфраструктури є важливим етапом у забезпеченні ефективного кіберзахисту, реагуванні на можливі загрози та запобіганні виникненню серйозних проблем для суспільства та економіки.

1.2 Статистика та сучасні тенденції кіберзагроз для ОКІ

В Україні у 2025 році ситуація стала напруженою. Інтенсивність кібератак на об’єкти критичної інфраструктури побила всі попередні рекорди. Кабінетом Міністрів України та станом на 2023 рік 48% [7]. Нещодавно фіксували синхронізовані атаки на місцеві органи влади, оборонні підприємства і великі міські сервіси. Часто все це відбувається одночасно з реальними обстрілами та диверсіями.

Кількісні показники та типи атак

- CERT-UA у 2025 році фіксує в середньому 15 інцидентів щодня й відстежує понад 150 активних кластерів кіберзлочинних груп [8].
- 73% успішних атак починаються з фішингу - основних “воріт” для проникнення у мережі ОКІ.
- Перелік основних загроз: програми-вимагачі (ransomware),

компрометація ланцюгів постачання, AI-генеровані атаки, DDoS, зломи SCADA/ICS, впровадження шкідливого ПЗ, соціальна інженерія (з використанням deepfake та ШІ), хакерські атаки через підрядників, атак на хмарні сервіси та критичні адміністрування.

Приклади ключових інцидентів

- Зупинка енергомереж через кібератаки (фіксовано як в Україні, так і у ЄС у 2024-2025).
- Вимагальницькі атаки на фінансові установи: лише в І півріччі 2025 світові збитки сектору від таких інцидентів склали понад 2,7 млрд доларів [9].
- Злам систем водопостачання, проникнення у сервери великих залізничних операторів та об’єктів енергетики (як в Україні, так і в країнах-членах ЄС).
- Синхронізовані атаки на ОКІ з використанням фішингу, бот-мереж та гібридних впливів у воєнний час.

Серед тенденцій 2025:

- Стрімке зростання атак, де використовуються штучний інтелект і глибокі фейки для розробки персоналізованого шкідливого контенту.
- Перехід хакерів до моделі RaaS (ransomware as a service) - кіберугруповання діють як “IT-фірми”, продаючи атаки на замовлення.
- Зростання кібершпигунства та гібридних операцій із державною підтримкою, особливо проти центрів прийняття рішень, інфраструктур обліку, енергетики та фінансів.
- Масове зростання збитків у результаті компрометації постачальників IT-послуг, хмарних сервісів, платіжних систем, фінустанов.

1.3 Основні завдання із забезпечення інформаційної безпеки автоматизованих систем управління об’єктами критичної інфраструктури

Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз [10]. Щодо національних інтересів інформаційна безпека означає такий стан захищеності інформаційних ресурсів особи, суспільства й держави, який забезпечує реалізацію та прогресивний розвиток життєво важливих для них інтересів. Щодо можливих негативних впливів різних видів інформаційної безпеки – це захищеність інформації та підтримуючої інфраструктури від випадкових чи навмисних природних або штучних впливів, які можуть заподіяти шкоду їхнім власникам або користувачам. Інформаційна безпека також означає рівень захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави і нейтралізації негативних наслідків інформатизації суспільства.

Захист інформації передбачає систему заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності тощо, а контроль за національним інформаційним простором – заходи щодо мінімізації збитків від здійснення як іноземними державами, так і внутрішніми організаціями підривних психологічних операцій. Рівень достатності інформаційного забезпечення державних органів та недержавних організацій і фірм визначають, виходячи з їхніх потреб в інформації для прийняття рішень у кожному конкретному випадку. Рівень захисту визначають для кожного певного виду інформації окремо.

Наслідки інформаційної безпеки:

трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів можуть істотно відрізнятися,

інформаційна безпека не зводиться лише до захисту інформації.

Суб'єкт інформаційних відносин може постраждати (зазнати збитків) не тільки від несанкціонованого доступу, а й від пошкодження системи, що спричинило, приміром, перерву в обслуговуванні клієнтів. Для відкритих організацій (наприклад, навчальних закладів) захист інформації не стоїть за своїм значенням на першому місці.

Елементи інформаційної безпеки: доступність (можливість за визначений час отримати необхідну інформаційну послугу), цілісність (актуальність і несуперечливість інформації, її захищеність від руйнування і несанкціонованої зміни), конфіденційність (захист від несанкціонованого доступу). Одним із видів національної безпеки є інформаційна безпека України (серед інших видів такої безпеки – політична, економічна, військова, екологічна, міжнародна, соціальна, регіональна).

Інформаційна безпека України – передбачений Конституцією захист політичних, державних, громадських інтересів країни, загальнолюдських і національних цінностей [11]. Вона охоплює, по-перше, дотримання вимог чинного законодавства щодо неприпустимості зловживань свободою ЗМІ, недопущення закликів до насильницької зміни конституційного ладу і захоплення влади, порушення територіальної цілісності держави, пропаганди війни, насилля, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягань на права і свободи людини, суспільства, по-друге, запобігання розміщенню відомостей, що становлять державну таємницю, чи відомостей з обмеженим доступом, а також текстових матеріалів, які переміщаються через державний кордон України інформаційні ресурси – інформація з усіх напрямів життєдіяльності суспільства, організована у формі документів (бібліотек, архівів, фондів, баз даних), а також інші форми організації інформації інформаційні загрози – сукупність факторів, що створюють небезпеку порушення конституційних прав і свобод особистості, державної таємниці, збереження важливої для суспільства інформації через несанкціоноване поширення (витоку, викрадення, копіювання), втрати,

спотворення, підробки, знищення, модифікації, копіювання, блокування інформації та інші форми незаконного втручання в такі ресурси.

Концепція (основи державної політики) національної безпеки України (прийнята Верховною Радою України 16.11.997) визначила основні загрози інформаційній безпеці України [12]. Зовнішні загрози запровадження іноземними державами обмежень щодо України на поширення інформації та нових інформаційних технологій, розвід прагнення іноземних державних органів і спеціальних служб, протиправна діяльність різних іноземних формувань та груп у сфері інтересів України, інформаційна експансія з боку інших держав, стихійні катаклізми і катастрофи. Внутрішні загрози відсутність науково обґрунтованої політики інформаційної безпеки України, недосконаліть законодавчої бази у сфері інформаційних відносин та інформаційної безпеки, невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері, повільність входження України у світовий інформаційний простір, брак у міжнародного співтовариства об'єктивного уявлення про Україну, витік інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації що є власністю держави, запровадження цензури, недосконаліть державної структури забезпечення інформаційної безпеки України, протиправні дії державних органів, політичних та економічних структур, окремих громадян в інформаційній сфері, виникнення нештатних, непередбачених ситуацій у системах, процесах, що ґрунтуються на використанні інформаційних технологій, внаслідок чого зростає ступінь ризику заподіяння збитків, а також їх розмірів, недосконаліть чи відсутність технічних засобів забезпечення інформаційної безпеки.

Основні завдання із забезпечення безпеки інформації на об'єктах критичної інфраструктури держави такі [13]:

- нормативне, правове регулювання у сфері забезпечення безпеки інформації в критичній інфраструктурі держави;

- визначення загроз безпеки інформації та виявлення уразливостей у програмному та апаратному забезпеченні об'єктів критичної інфраструктури держави;

- оцінка реальної захищеності критичної інфраструктури держави;

- розроблення вимог щодо забезпечення безпеки інформації в критичній інфраструктурі держави;

- розроблення та реалізація заходів для убезпечення інформації в критичній інфраструктурі держави;

- підготовка фахівців із забезпечення безпеки інформації в критичній інфраструктурі держави;

- здійснення контролю і нагляду в галузі забезпечення безпеки інформації в критичній інфраструктурі держави;

- інформаційне, матеріально-технічне і науково-технічне забезпечення безпеки інформації в критичній інфраструктурі держави.

1.4 Нормативно-правове регулювання в сфері забезпечення інформаційної безпеки автоматизованих систем управління об’єктами критичної інфраструктури

Аналіз чинної нормативної бази показує, що поняття “інформаційна безпека України” досить широко застосовується в Конституції України та низці інших нормативно-правових актів, підготовлених і затверджених Верховною Радою, Президентом України, Кабінетом Міністрів, центральними органами виконавчої влади. Так, ст. 17 Конституції наголошує, що забезпечення інформаційної безпеки – “одна з найважливіших функцій держави, справа всього українського народу”, а Закон України “Про Концепцію Національної програми інформатизації” проголошує, що “інформаційна безпека є невід’ємною частиною політичної, економічної, оборонної та інших складових національної безпеки” [14]. У ст. 23 “Воєнної доктрини України” прямо вказується, що “здійснення заходів щодо

забезпечення інформаційної безпеки є одним із основних завдань Збройних сил України в мирний час" [15]. А в ст. 20 зазначається, що характерними рисами сучасної збройної боротьби, серед іншого, є "зростання ролі і значущості протиборства в інформаційній сфері, використання новітніх інформаційних технологій". У ст. 13 Закону України "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" [16] надається визначення поняття "інформаційна безпека" – це "… стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через:

неповноту, невчасність та невірогідність інформації, що використовується;

негативний інформаційний вплив;

негативні наслідки застосування інформаційних технологій;

несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації".

Разом з цим у Законі України "Про інформацію" визначення "інформаційна безпека" взагалі немає. А в Законі України "Про основи національної безпеки України" [17], який є основним орієнтиром забезпечення безпеки нашої держави, сутність "інформаційної безпеки" подано як невід'ємний складник національної безпеки України без точного визначення цього поняття.

Як бачимо, у наведених документах надаються лише загальні визначення терміну "інформаційна безпека" до того ж, не узгоджені між собою. Але ці документи не містять системних підходів до забезпечення інформаційної безпеки в Україні, не визначають суб'єктів інформаційної діяльності та не розподіляють повноважень між ними.

У той же час, більш нормативно опрацьованими є питання кібернетичної безпеки. Так, наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94 затверджено "Порядок координації діяльності органів державної влади, органів місцевого

самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" [18].

Метою цього Порядку є організація координації діяльності з питань запобігання вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також впровадження єдиної процедури надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів. Проте цим документом не визначено механізм координації щодо діяльності з протидії інформаційним загрозам. Вагомим зрушенням у нормативно-правовому регулюванні національної безпеки в інформаційній сфері загалом стало розроблення та введення в дію Доктрини інформаційної безпеки України (далі – Доктрина), яка була підготовлена на виконання Указу Президента України "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року" №47/2017 [19].

Слід відзначити, що Доктрина стала першим вітчизняним нормативно-правовим документом, у якому проголошується особливе місце інформаційної безпеки в системі забезпечення національної безпеки, а саме з одного боку – як невід'ємного складника кожної зі сфер забезпечення національної безпеки і як важливої самостійної сфери забезпечення національної безпеки – з іншого боку.

Окрім того, важливою новацією Доктрини стало чітке виокремлення трьох головних напрямів державної політики у забезпеченні інформаційної безпеки України: технологічного розвитку, захисту інформації та "інформаційно-психологічного, зокрема щодо створення сприятливого психологічного клімату в національному інформаційному просторі".

Стосовно інформаційно-психологічного напряму в Доктрині визначаються такі життєво важливі інтереси особи, як захищеність від деструктивних інформаційно-психологічних впливів; суспільства – щодо збереження і примноження духовних, культурних і моральних цінностей Українського народу; держави – недопущення інформаційної залежності та блокади України, інформаційної експансії з боку інших держав та міжнародних структур. Останнім часом розроблено низку нових законопроектів стосовно інформаційної безпеки держави, а саме “Про засади інформаційної безпеки України”, “Про кібернетичну безпеку України”, “Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України”. У цих законопроектах частково враховано зазначені недоліки вітчизняного законодавства. Слід зазначити, що події в інформаційному просторі України, викликані агресією з боку РФ, змусили керівництво держави до більш рішучих кроків у цей сфері.

У Міністерстві економічного розвитку і торгівлі України 20 липня 2018 року оприлюднено для обговорення Проект Закону «Про критичну інфраструктуру та її захист». Проект розроблено відповідно до Указу Президента України від 16 січня 2017 р. №8 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури”» [20]. Документ пропонує встановити принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначає правові та організаційні засади забезпечення її діяльності і має стати складовою частиною законодавства України у сфері національної безпеки.

Проект передбачає створення Уповноваженого органу у справах захисту критичної інфраструктури, який відповідатиме за формування та реалізацію державної політики у сфері захисту критичної інфраструктури. Проект не містить порядку створення цього органу, однак встановлює, що Положення про Уповноважений орган у справах захисту критичної інфраструктури України затверджується Кабінетом Міністрів України.

Стаття 14 Проекту визначає низку суб'єктів, які входять до державної системи захисту критичної інфраструктури, зокрема: Уповноважений орган у справах захисту критичної інфраструктури України; міністерства та інші центральні органи виконавчої влади; правоохоронні та розвідувальні органи; Служба безпеки України; Збройні Сили України, інші військові формування, утворені відповідно до законів України; місцеві державні адміністрації; оператори критичної інфраструктури та громадські організації.

Законодавство України на сьогодні не містить спеціальних норм щодо регулювання «обмеження та блокування доступу» до окремих об'єктів та ресурсів, за винятком статті 39 Закону України «Про телекомунікації» [21], яка зобов'язує операторів і провайдерів телекомунікацій на підставі рішення суду обмежувати доступ своїх абонентів до ресурсів, через які здійснюється розповсюдження дитячої порнографії, а також вимог законодавства щодо захисту авторських та суміжних прав в Інтернеті.

Більше того, ні зазначений Проект, ні інші закони не дають визначення того, які саме заходи можуть вважатись «обмеженням та блокуванням доступу». Натомість, Кримінальний процесуальний кодекс України, а також Закони України «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність» та, власне, Закон України «Про Службу безпеки України» [22] передбачають достатньо повноважень для належного реагування і припинення незаконних дій, у тому числі, несанкціонованого втручання в діяльність критичної інфраструктури.

Варто також зауважити, що у випадках, коли йдеться про обмеження доступу до інформаційних ресурсів, відповідно до п. 4.5. Стратегії кібербезпеки України, що була затверджена Указом Президента України від 15 березня 2016 року № 96/2016, боротьба з кіберзлочинністю може передбачати запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу), але виключно за рішенням суду.

Зважаючи на те, що операторами об’єктів критичної інфраструктури можуть бути не лише державні органи, але й приватні суб’єкти, надання автоматичного доступу до будь-якої, в першу чергу конфіденційної інформації, яка ними зберігається, може становити втручання в підприємницьку діяльність.

Відповідно до статті 7 Закону України “Про доступ до публічної інформації” конфіденційна інформація про особу може поширюватися у визначеному нею порядку за їхнім бажанням відповідно до передбачених ними умов, тобто, за згодою такої особи. Поширення конфіденційної інформації без згоди допускається лише в інтересах національної безпеки, економічного добробуту та прав людини у визначеному законом порядку. Зазначений Проект передбачає лише повноваження щодо доступу до інформації з обмеженим доступом, але не встановлює порядку такого доступу.

У прикінцевих та перехідних положеннях Проекту пропонується внести зміни до Закону України «Про доступ до публічної інформації» [23], відповідно до яких, інформація щодо об’єктів критичної інфраструктури та запроваджених заходів їх захисту, яку не віднесено до державної таємниці, буде вважатися службовою інформацією. Проект також пропонує поширити частину третю статті 9 зазначеного Закону, яка встановлює заборону на обмеження доступу до переліків відомостей, що становлять службову інформацію і які складаються суб’єктами владних повноважень, також на переліки, які складаються об’єктами критичної інфраструктури.

При цьому, відповідно до статті 8 Проекту до об’єктів критичної інфраструктури належать підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва продуктів, харчування, охорони здоров'я;

3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

5) є об'єктами підвищеної небезпеки;

6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;

7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення».

1.5 Висновки до першого розділу

У першому розділі було систематизовано основні поняття, характеристики та класифікацію об'єктів критичної інфраструктури, що дає змогу чітко визначити їхню роль у забезпеченні національної безпеки та стабільного функціонування держави. Проаналізовано актуальні кіберзагрози, спрямовані на ОКІ, та відзначено тенденцію до зростання інтенсивності та складності атак, що підсилює необхідність впровадження комплексних заходів захисту.

Розглянуто ключові принципи та основні завдання забезпечення інформаційної безпеки автоматизованих систем управління критично важливими об'єктами, включно з ідентифікацією загроз, оцінюванням рівня захищеності, визначенням вимог і впровадженням технічних та організаційних заходів.

Окрему увагу приділено нормативно-правовому забезпеченню, зокрема положенням Закону України «Про критичну інфраструктуру», Доктрини інформаційної безпеки та інших національних документів, що формують основу державної політики у сфері захисту критично важливих об’єктів.

Таким чином, перший розділ створює цілісну теоретичну й законодавчу базу для подальшого аналізу практичних аспектів забезпечення інформаційної безпеки та дослідження механізмів захисту автоматизованих систем управління на об’єктах критичної інфраструктури.

Розділ 2. ПОРЯДОК СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

2.1 Визначення, призначення та порядок створення комплексної системи захисту інформації автоматизованих систем об’єктів критичної інфраструктури

Відповідно до чинного законодавства України і вимог окремих нормативних документів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах"[24] та Закону України "Про захист персональних даних"[25] обов'язковому захисту інформації підлягає: інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в т.ч. персональні дані громадян.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу. Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності [26].

Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки, проведена реорганізація системи діловодства та зберігання документів.

Інженерно-технічні заходи – сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерно-технічних заходів залежить від рівня захищеності інформації, який необхідно забезпечити.

Інженерно-технічні заходи, що проводяться для захисту інформаційної інфраструктури організації, можуть включати використання захищених підключень, міжмережевих екранів, розмежування потоків інформації між сегментами мережі, використання засобів шифрування і захисту від несанкціонованого доступу.

У разі необхідності, в рамках проведення інженерно-технічних заходів, може здійснюватися установка в приміщеннях систем охоронно-пожежної сигналізації, систем контролю і управління доступом.

Окремі приміщення можуть бути обладнані засобами захисту від витоку акустичної (мовної) інформації.

У процес створення КСЗІ залучаються такі сторони (суб'єкти КСЗІ):

- організація, для якої здійснюється побудова КСЗІ (Замовник);

- організація, що здійснює заходи з побудови КСЗІ (Виконавець);

- Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) (Контролюючий орган);

- організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктом захисту КСЗІ є інформація, в будь-якому її вигляді і формі подання. Матеріальними носіями інформації є сигнали. По своїй фізичній природі інформаційні сигнали можна розділити на такі види: електричні, електромагнітні, акустичні, а також їх комбінації. Сигнали можуть бути представлені у формі електромагнітних, механічних та інших видах коливань,

причому інформація, яка підлягає захисту, міститься в їх змінних параметрах. Залежно від природи, інформаційні сигнали поширюються в певних фізичних середовищах. Середовища можуть бути газовими, рідинними і твердими. Наприклад, повітряний простір, конструкції будівель, з'єднувальні лінії і струмопровідні елементи, заземлення та інші.

Залежно від виду та форми подання інформаційних сигналів, які циркулюють в інформаційно-телекомунікаційній системі (ІТС), у тому числі і в автоматизованих системах (АС), при побудові КСЗІ можуть використовуватися різні засоби захисту.

Порядок створення комплексної системи захисту інформації

Виконавцем робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі може бути суб’єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації (далі - ТЗІ), необхідність проведення якого визначено технічним завданням на створення КСЗІ.

Для проведення інших видів робіт з ТЗІ, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення КСЗІ необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензію на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Створення КСЗІ в ІТС здійснюється відповідно до нормативного документа системи технічного захисту інформації НД ТЗІ 3.7-003-23 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [27] на підставі технічного завдання (далі - ТЗ), розробленого згідно з вимогами нормативного документу системи технічного захисту інформації НД ТЗІ 3.7-001-99 "Методичні вказівки

щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі" [28].

До складу КСЗІ входять заходи та засоби, які реалізують способи, методи, механізми захисту інформації від:

- витоку технічними каналами, до яких відносяться канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

- несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів тощо;

- спеціального впливу на інформацію, який може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування системи захисту.

Для кожної конкретної ІТС склад, структура та вимоги до КСЗІ визначаються властивостями оброблюваної інформації, класом автоматизованої системи та умовами її експлуатації.

Для формування загальних вимог до КСЗІ в ІТС здійснюється обґрунтування необхідності її створення на підставі вимог законодавства, що встановлюють обов'язковість забезпечення конфіденційності, цілісності і доступності інформації, та обстеження середовищ функціонування ІТС - обчислювальної системи, фізичного середовища, середовища користувачів, оброблюваної інформації і технології її обробки.

За результатами детального вивчення об'єкта, на якому створюється КСЗІ, уточнення моделі загроз та моделі порушника, результатів аналізу можливості керування ризиками здійснюється вибір основних рішень з протидії всім суттєвим загрозам, формування загальних вимог, правил, обмежень, які регламентують використання захищених технологій обробки

інформації в ІТС, окремих заходів і засобів захисту інформації, діяльність користувачів всіх категорій та документальне оформлення політики безпеки.

В ТЗ викладаються вимоги до функціонального складу і порядку розробки і впровадження технічних засобів, що забезпечують безпеку інформації в процесі її обробки в обчислювальній системі ІТС, а також вимоги до організаційних, фізичних та інших заходів захисту, що реалізуються поза обчислювальною системою ІТС у доповнення до комплексу програмно-технічних засобів захисту інформації.

Проект КСЗІ розробляється на підставі та у відповідності до ТЗ. Під час розробки проекту КСЗІ обґрунтовуються і приймаються проектні рішення, які дають змогу реалізувати вимоги ТЗ, забезпечити сумісність і взаємодію різних компонентів КСЗІ, а також різних заходів і способів захисту інформації. У результаті створюється комплект робочої та експлуатаційної документації, необхідної для забезпечення тестування, проведення пусконалагоджувальних робіт, випробувань та управління КСЗІ.

Введення КСЗІ в дію включає розробку розпорядчих документів, що регламентують діяльність із забезпечення захисту інформації в ІТС, створення служби захисту інформації, розробку і затвердження Плану захисту інформації, навчання користувачів ІТС всіх категорій (технічного обслуговуючого персоналу, звичайних користувачів та адміністраторів), комплектування КСЗІ засобами захисту інформації, матеріалами, обладнанням, проведення будівельно-монтажних та пусконалагоджувальних робіт, попередніх випробувань та дослідної експлуатації КСЗІ.

Під час попередніх випробувань перевіряються працездатність КСЗІ та відповідність її вимогам ТЗ.

Під час дослідної експлуатації:

- відпрацьовуються технології оброблення інформації, обігу машинних носіїв інформації, керування засобами захисту, розмежування доступу користувачів до ресурсів ІТС та автоматизованого контролю за діями користувачів;

- співробітники служби захисту інформації та користувачі ІТС набувають практичних навичок з використання технічних та програмно-апаратних засобів захисту інформації, засвоюють вимоги організаційних та розпорядчих документів з питань розмежування доступу до технічних засобів та інформаційних ресурсів;

- здійснюється (за необхідністю) доопрацювання програмного забезпечення, додаткове налагоджування та конфігурування комплексу засобів захисту інформації від несанкціонованого доступу;

- здійснюється (за необхідністю) коригування робочої та експлуатаційної документації.

За результатами дослідної експлуатації приймається рішення про готовність КСЗІ в ІТС до представлення на державну експертизу.

2.2 Визначення, етапи створення та переваги застосування системи управління інформаційною безпекою автоматизованих систем управління об'єктів критичної інфраструктури

Сучасний етап розвитку інформаційної безпеки потребує комплексного підходу до розробки та впровадження методів і засобів захисту ресурсів інформаційно-комунікаційних систем та мереж (ІКСМ) як на технічному, так і організаційному рівні, тобто реалізації комплексного процесу. Комплексний процес організації безпеки в першу чергу має включати заходи управління інформаційною безпекою. Зазначений процес забезпечує механізми та методи, які дозволяють реалізувати комплексну політику інформаційної безпеки організації ІКСМ. Інформаційна безпека – реалізація процесу захисту інформації від широкого діапазону загроз (внутрішніх та зовнішніх), що здійснюється з метою забезпечення ефективності та надійності функціонування ІКСМ.

Міжнародні стандарти серії ISO (ISO/IEC 17799, ISO 27001, ISO 27002) є основоположними в сфері управління інформаційною безпекою.

Вони являють собою модель системи менеджменту, яка визначаєьзагальну організацію процесів, класифікацію даних, системи доступу, напрямки планування та удосконалення системи безпеки, відповідальність співробітників і оцінку ризику.

Основна ідея стандартів серії ISO – забезпечення надійного захисту інформаційних ресурсів ІКСМ та організація ефективного доступу до даних й процесу їх обробки згідно з визначеними послугами [29].

Сучасні ІКСМ уразливі до низки мережних загроз, які можуть бути результатом реалізації несанкціонованого доступу, а також розкриття, викривлення або модифікації інформації. Щоб захистити сучасні інформаційні ресурси та послуги від загроз, необхідно застосовувати відповідні заходи управління безпекою.

Під управлінням інформаційною безпекою будемо розуміти циклічний процес, що включає [30]:

постановку задачі захисту інформації; збір та аналіз даних про стан інформаційної безпеки в ІКСМ;

оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію і впровадження відповідних механізмів контролю;

розподіл ролей і відповідальності; політику безпеки;

навчання та мотивацію персоналу, оперативну роботу зі здійснення захисних заходів;

моніторинг (аудит) функціонування механізмів контролю, оцінку їх ефективності та надійності.

Процес впровадження системи управління інформаційною безпекою включає оцінку поточного стану інформаційного забезпечення захисту інформації ІКСМ, формування комплексу заходів щодо забезпечення оптимального рівня на основі оцінки ризиків. Після ідентифікації вимог безпеки варто вибирати й застосовувати заходи управління таким чином, щоб забезпечувати впевненість у зменшенні ризиків від реалізації несанкціонованого доступу. Засоби управління можуть бути обрані зі

стандартів або з безлічі інших документів та заходів управління, визначених для даного класу систем, або можуть бути розроблені, щоб задовольнити потреби компанії відповідно до обраної політики інформаційної безпеки. Згідно з міжнародним стандартом ISO 27001, система управління інформаційною безпекою – це «частина загальної системи управління організації, яка заснована на оцінці ризиків, створює, реалізує, експлуатує, здійснює моніторинг, перегляд, супровід і вдосконалення загальної інформаційної безпеки».

Відповідно до вимог ISO/IEC 27001 система управління інформаційною безпекою повинна містити такі етапи[30]:

1 етап - планування - фаза створення: створення переліку інформації, оцінки ризиків і вибору заходів та механізмів захисту;

2 етап - дія - етап реалізації та впровадження відповідних заходів;

3 етап - перевірка - фаза оцінки ефективності та надійності функціонування створеної системи. Проведення внутрішнього аудиту системи, виявлення недоліків.

4 етап - удосконалення - виконання коригувальних дій з покращення функціонування системи;

При створенні системи управління інформаційною безпекою потрібно керуватися відповідними заходами з метою підвищення ефективності захищеності сучасних ІКСМ. Заходи управління варто вибирати, ґрунтуючись на відношенні вартості реалізації послуг та впровадження систем безпеки й зниження ризиків і можливих втрат, якщо відбудеться порушення безпеки ІКСМ. Деякі з заходів управління в стандартах та нормативних документах можуть розглядатися як керівні принципи для управління інформаційною безпекою й можуть бути застосовані для організації політики безпеки. Розглянемо заходи управління інформаційною безпекою із законодавчої точки зору та узагальнені для сучасних ІКСМ.

Якщо розглядати заходи управління з законодавчої точки зору, то вони включають:

захист даних і таємність особистої інформації;

охорону інформаційних ресурсів організації;

права на інтелектуальну власність.

Заходи управління сучасних ІКСМ включають :

документи, що стосується політики інформаційної безпеки;

розподіл обов'язків, пов'язаних з інформаційною безпекою;

структура підрозділів й навчання, пов'язані з інформаційною безпекою ;

повідомлення про інциденти, пов'язані з безпекою ;

управління безперервністю.

Слід зазначити, що всі заходи управління в стандартах та нормативних документах є важливими, але застосування якого-небудь засобу управління має відповідати ризикам та можливим загрозам даної ІКСМ.

У загальному випадку система управління безпекою повинна включати (рис. 1):

автентифікацію (користувачів, даних, додатків, послуг, тощо);

авторизацію (авторизований перелік цін, ключових торговельних документів, партнерів, користувачів, керівництва);

аудит інформаційних ресурсів та послуг.

Переваги застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO:

Від якості застосовуваних новітніх технологій захисту інформації залежить не тільки збереження конфіденційності та цілісності інформації, а й взагалі існування конкретних інформаційних і телекомунікаційних сервісів, послуг та програм;

мінімізація ризиків. Впровадження системи управління інформаційною безпекою дозволяє зменшити інформаційні ризики, розкрадання і неправильне використання обладнання, пошкодження та порушення роботи інформаційної системи організації за рахунок розмежування фізичного доступу та

впровадження механізму моніторингу (аудиту) стану інформаційної безпеки. Оцінка та мінімізація ризиків дозволяє ідентифікувати загрози інформаційним ресурсам та послугам, оцінити їх уразливість і ймовірність виникнення загроз, а також можливий руйнівний вплив при реалізації несанкціонованого доступу;

зниження витрат на інформаційну безпеку. Застосування передових технологій зі створення, моніторингу та поліпшення інформаційної безпеки дозволяє знизити витратну частину бюджету, що спрямована на забезпечення інформаційної безпеки;

забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів ІКСМ;

забезпечення комплексного та централізованого контролю рівня захисту інформації.

Підхід до управління ризиками інформаційної безпеки на базі міжнародних стандартів серії ISO є проактивним та здатним допомогти інформаційним системам організацій різних рівнів та будь-якого розміру у вирішенні проблем, що виникають в процесі забезпечення відповідності інформаційної безпеки регулятивним нормам. Найбільш значними стандартами інформаційної безпеки у сфері управляння інформаційної безпеки є: критерії безпеки комп'ютерних систем, європейські критерії безпеки інформаційних технологій, федеральні критерії безпеки інформаційних технологій, канадські критерії безпеки комп'ютерних систем, загальні критерії безпеки інформаційних технологій та сім'я стандартів ISO. Усі вони визнають значення процесу управління ризиками, базові методи та затверджують концепцію процесу створення, впровадження, використання, моніторингу, перевірки, підтримання та вдосконалення системи захисту організації.

Для ефективного функціонування організації доводиться ідентифікувати та управляти багатьма процесами, а саме процесом управління ризиками інформаційного об'єкту. Процес управління ризиками безпеки дозволяє організаціям досягти поєднання максимальної економічної ефективності з

відомим та прийнятним рівнем ризику та надає керівникам різних рівнів зрозумілий метод організації та пріоритизації ресурсів з обмеженим доступом для реалізації управління ризиками. Реалізація управління ризиками безпеки дозволяє організаціям з розподіленими корпоративними мережами використовувати економічно ефективний контроль, що знижує ризик до прийнятного рівня. Визначення допустимого ризику та підхід до управління ризиками залежать від структури конкретної інформаційної системи, її розподіленості, оскільки не існує універсального рішення, а різні організації використовують різні моделі управління ризиками. Кожна модель пропонує власне поєднання точності, ресурсів, часу, складності та суб'єктивності. Інвестиції в процес управління ризиками заснований на перевіреній концепції та чіткому визначенні ролей та обов'язків. Крім того, ефективна програма управління ризиками допоможе розподіленим корпоративним мережам забезпечити дотримання чинних законодавчих вимог з забезпечення гідного рівня інформаційної безпеки.

Оцінювання ризиків організації є первинним етапом при розробці та експлуатації захищених інформаційних систем. Через оцінки ризиків ідентифікуються загрози активам, оцінюються їх уразливість й імовірність виникнення загроз, а також можливий руйнівний вплив під час реалізації несанкціонованих дій. Далі запропоновано сценарій управління ризиками інформаційного об’єкту (Рис. 2.1).

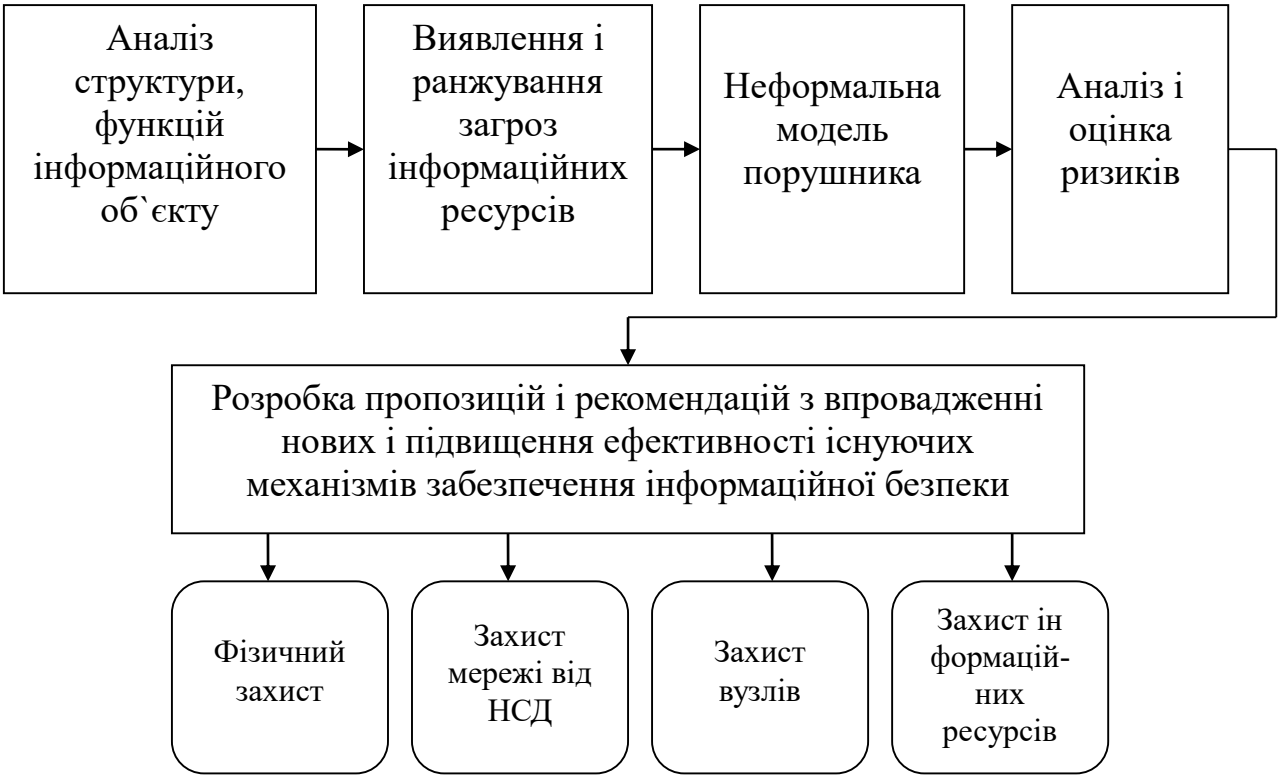

Рис. 2.1 – Сценарій управління інформаційною безпекою критично важливого об’єкта

Запропонований сценарій розрахунку ризиків складається з наступних базових складових, а саме:

визначення методології оцінювання ризику для інформаційної системи;

розроблення критеріїв ухвалення ризиків та визначення прийнятого рівня ризику;

визначення активів;

виявлення небезпеки для активів;

виявлення вразливих місць в системі захисту;

виявлення дій, які порушують конфіденційність, цілісність та доступність активів та інформаційної системи;

визначення ймовірності провалу системи безпеки за наявності переважних небезпек та вразливостей;

оцінювання рівнів ризику;

визначення прийнятності ризику або проведення процедури скорочення, використовуючи встановлені критерії допустимості та прийнятності ризику;

вибір завдань та засобів управління для скорочення ризиків з умов забезпечення ефективності захисту.

Завдання та засоби управління мають бути вибрані та впроваджені відповідно до вимог, встановлених процесом оцінки ризиків та скорочення ризиків згідно з ISO 27002 [31]. Цей вибір повинен враховувати як критерії з допустимості ризику, так і юридичні, регулятивні та договірні вимоги. Впровадження даного сценарію дозволяє підвищити ефективність та надійність створеної системи захисту інформації на базі проведення оцінки ризиків, яка визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, методи забезпечення безпеки, практичні правила та вимоги, відповідальність

співробітників, використання оцінювання ризику в контексті інформаційної безпеки підприємств. У процесі впровадження даного сценарію створюється система менеджменту інформаційної безпеки. Метою створеної системи менеджменту інформаційної безпеки є скорочення матеріальних втрат, пов’язаних з порушенням інформаційної безпеки. На основі запропонованого сценарію розроблена структурна схема оцінювання інформаційних ризиків (Рис. 2.2).

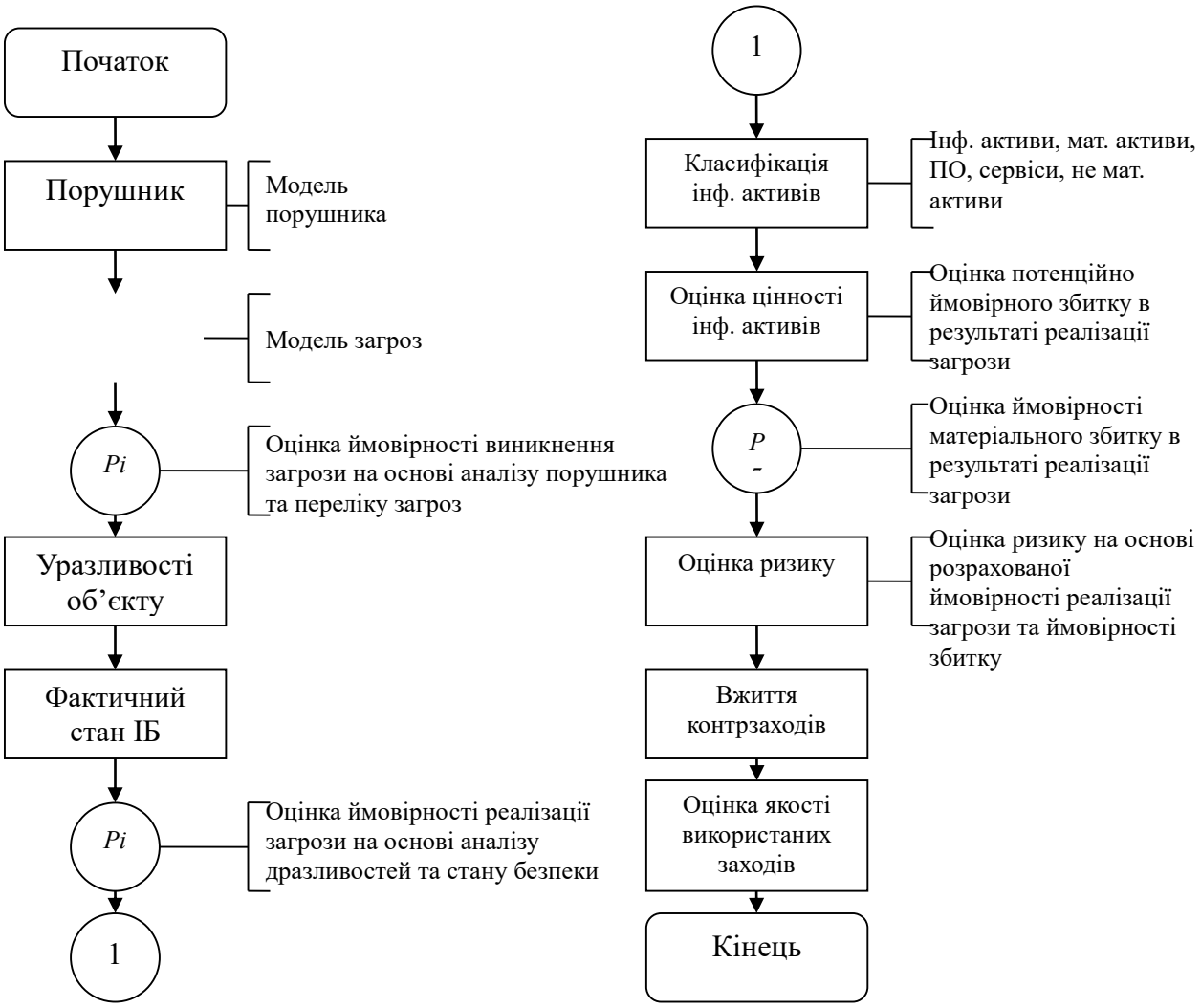

Рис. 2.2 – Структурна схема оцінювання інформаційних ризиків на критично важливих об'єктах

Після аналізу сучасних методів управління інформаційною безпекою ІКСМ згідно з міжнародними стандартами ISO стало зрозуміло: безпека цих систем - це ключ до захисту інформаційних ресурсів і сервісів у мережах передачі даних. Щоб забезпечити й утримувати цей захист, потрібно використовувати різні інструменти й заходи управління. Тут немає універсального рішення - доводиться комбінувати підходи, аби система залишалася стійкою.

2.3. Аналіз міжнародного досвіду забезпечення інформаційної безпеки під час становлення критичних систем інформаційної інфраструктури в різних країнах світу

У кожному суспільстві можливо виділити сектори, системи або мережі, від яких життєво залежить суспільство і порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівні. Комплекс цих секторів, систем або мереж почали називати ключовими або КСІІ.

Багато держав, а також терористичних та кримінальних структур інтенсивно вдосконалюють методи і способи використання інформаційних технологій та засобів для деструктивних інформаційних впливів на інформаційні ресурси інформаційно-телекомунікаційних систем і мереж державних та недержавних організацій. Таке застосування інформаційних технологій та засобів надає їм властивості так званої інформаційної зброї. Для нанесення значного збитку інтересам держави і суспільства інформаційна зброя може бути застосована і в мирний час, особливо терористичними організаціями. При цьому порушення функціонування КСІІ може призвести до розвитку надзвичайних ситуацій, пов’язаних із загибеллю людей, екологічними катастрофами, нанесенням великої матеріальної, фінансової, економічної шкоди або великомасштабними порушеннями життєдіяльності міст та населених пунктів і т.п. У цих умовах важливу роль відіграє державне регулювання діяльності щодо забезпечення безпеки інформації в КСІІ [32].

Необхідно зазначити, що на даний час в Україні проблематика, що пов’язана з визначенням КСІІ, оцінюванням актуальних загроз безпеки, побудовою систем захисту та нормативно-правовим забезпеченням цих процесів знаходяться на початковому рівні та наполегливо потребує розвитку.

У зв’язку з нарощуванням з 1998-го року загрози тероризму в розвинених країнах почалися дискусії про уразливість національних інфраструктур.

Аналізи були направлені не тільки на кібернетичні інфраструктурні системи, але і на решту областей і секторів забезпечення життя суспільства. У США PRESIDENTIAL DECISION DIRECTIVE/NSC-63 визначили КСІІ як основні системи, які можуть мати матеріальну або кібернетичну платформу і мають дію на функціональність економіки держави [33]. Ці основні системи вбирали в себе системи телекомунікації, енергосистеми, банківський і фінансовий сектори і служби, транспортну систему, постачання водою і рятувальні служби.

Питаннями КСІІ на національному рівні почали з 1998-го року займатися і європейські держави. Суспільним знаменником цієї діяльності було, перш за все, надання особливого значення охороні інформаційних і комунікаційних технологій. В Європі проблематикою КСІІ раніше всіх почали займатися у Великобританії, де в кінці 1999-го року була визначена ключова система національної інфраструктури як система, спадкоємність якої важлива для функціонування держави, втрата або порушення якої мало б або могло б піддавати загрозі життя громадян, могло б нанести серйозні негативні економічні або соціальні наслідки для суспільства чи її крупної частини. У таку систему були включені державне управління, запасні служби, енергетика і паливо, подача води, телекомунікації, забезпечення продовольством, санітарія, фінанси і економіка, комунікаційні мережі і служби, юстиція і захист громадського порядку, соціальне обслуговування, освіта, наука, а також, прогноз погоди [34].

В результаті терористичних нападів на об’єкти в США, які відбулися 11.09.2001, проблематика КСІІ і їх захист прийняли новий об’єм і масштаб. У лютому 2003-го року в США була прийнята Національна стратегія фізичної охорони критичної інфраструктури і ключових споруд (National Strategy for Physical Protection of Critical Infrastructure and Key Assets) [35], в якій критична інфраструктура визначена як системи устаткування, матеріальні і віртуальні, які життєво важливі для США і пошкодження або руйнування яких мав би вплив на зменшення безпеки, національної економічної безпеки,

національного суспільного здоров'я, або на будь-яку їх комбінацію. До секторів критичної інфраструктури були віднесені: сільське господарство, продовольство, вода, здоровий спосіб життя, запасні (рятувальні) служби, бази оборонної промисловості, телекомунікації, енергетика, транспорт, банківська справа і фінанси, хімічна промисловість і небезпечні речовини, поштове обслуговування. До ключового устаткування були віднесені національні культурні пам'ятники, ядерні електростанції, дамби (греблі), урядові і комерційні будівлі і інші місця, де концентрується велика кількість людей.

Нідерландський уряд прийняв в 2001 році план боротьби проти тероризму, складовою частиною якого є - проект захисту КСІІ. Після проведення аналізів ідентифіковано 11 секторів КСІІ, а саме: енергогосподарство, телекомунікації, питна вода, продукти, санітарія, фінанси, відведення поверхневої води, загальний порядок і безпека, законність, суспільні органи і транспорт [36].

У Чеській Республіці до 2002 року проблематика КСІІ зосереджувалася, перш за все, на комп'ютерних мережах. Під КСІІ в Чеській Республіці розуміються системи, руйнування або зменшення функціональності яких мав би серйозний вплив на економічну і суспільну стабільність, обороноздатність, безпеку і функціонування держави. У 2002 році були визначені сектори національної критичної інфраструктури, особливо комплекс силового обслуговування, комплекс подачі води, комплекс баластного господарства, транспортна мережа, комунікаційні і інформаційні системи, банковий і фінансовий сектор, запасні служби, публічні служби, державне управління і самоврядування [37].

У Польщі критична інфраструктура була визначена як функціонально сполучені засоби виробництва, інститути, служби, що є ключовими для безпека країни і її громадян, для забезпечення правильного функціонування як державних і самокерованих органів і установ, так і комерційного (приватного) сектора [38].

Об’єднання народних економік держав ЄС, їх взаємозалежність, але і необхідність протистояти сумісним або подібним погрозам, відбилися в ухваленні документа Critical Infrastructure protection in the fight against terrorism [39]. У цьому документі КСІІ визначена як фізичні засоби виробництва, інформаційні технології, мережі (транспортні, енергетичні і т. п.), служби і інші активи, розлад або руйнування яких мало б серйозні впливи на здоров’я, охорону, надійність або життєвий рівень громадян або на штатне функціонування урядів в цих державах.

Виходячи з аналізу світового досвіду до КСІІ входять:

- енергетичні об’єкти і мережі, наприклад, електричні розподільні мережі, газопроводи, нафтопроводи, збірки пального і т. п.;

- комунікаційні і інформаційні технології (наприклад, телекомунікації, радіомовні і телевізійні передавачі і мережі, інтернет);

- фінансова система (банкова справа, ринки капіталу, інвестування);

- охорона здоров’я, особливо лікарні, поліклініки, установи постачання крові, лабораторії, сантехнічна рятувальна служби;

- харчова промисловість, сільське господарство, торгівля і постачання продовольством;

- вода, особливо греблі, гідроресурси;

- транспорт, особливо авіаційний, шосейний, залізничний, комбінований, комунікаційні вузли, а також системи управління транспортом;

- виробництво, зберігання і транспорт небезпечних товарів, особливо хімічних, біологічних, радіологічних ядерних матеріалів;

- державне управління, зокрема критичні служби і установи, інформаційні мережі, важливі економічні об’єкти, стратегічні об’єкти, а також культурні пам’ятники.

Критеріями того, чи можна дану систему інформаційної інфраструктури визначити як ключову, є:

- територіальна досяжність негативних результатів, наприклад транснаціональний, народний, регіональний, локальний (місцевий) і т. п.;

- велика кількість наслідків, наприклад, гуманітарних, матеріальних, економічних, політичних або збитки і втрати відносно навколишнього середовища;

- часовий ефект наслідків, особливо коли з'являться негативні наслідки (наприклад: негайно, за 24 год.) і як довго можуть продовжуватися (наприклад: до 24 годин, до 3 днів і т. п.).

Захист КСІІ можемо визначити як сукупність заходів, які плануються і виконуються з метою:

- визначати і захищати ті системи інформаційної інфраструктури держави, що є ключовими з погляду збереження їх безпеки, функціональності, економічної і суспільної стабільності, причому необхідно рівноцінно оцінювати як державну, так і приватну сферу;

- забезпечити функціональність системи раннього попередження появи кризових ситуацій і захист тієї системи інформаційної інфраструктури, яка важлива для вирішення кризових ситуацій.

Мова йде, перш за все, про КСІІ, які є важливими з точки зору:

- забезпечення правильного функціонування уряду, органів державного управління і самоврядування, переважно в області безпеки і забезпечення основних (життєвих) товарів і послуг;

- функціональності державної і приватної сфери при забезпеченні правильного ходу економіки і функціонування суспільних служб;

- забезпечення внутрішнього порядку, суспільної стабільності і безпеки громадян.

Захист КСІІ виконуватиметься завжди як результат аналітичного процесу, зміст якого складається з:

- ідентифікації КСІІ на національному, регіональному і локальному рівні;

- ідентифікації релевантних ризиків для КСІІ;

- аналізу уразливості окремих КСІІ;

- оцінки ризиків порушення або знищення КСІІ;

- ухвалення відповідних запобіжних заходів.

Система захисту КСІІ представляє сукупність організаційних і технічних заходів для забезпечення захисту КСІІ від різних загроз (терористів, диверсантів, екстремістів), у разі появи надзвичайних або кризових ситуацій, та і від наслідків ненавмисних дій, які могли б нанести збитки для критичної інфраструктури.

Ефективна система захисту КСІІ повинна успішно протистояти різним загрозам при адекватному рівні охоронних заходів, залежно від значення КСІІ, потенційних загроз і їх можливих наслідків.

Загальні вимоги спрямовані на забезпечення діяльності в цій області органів виконавчої влади, органів місцевого самоврядування, підприємств і організацій (господарюючих суб'єктів), у віданні яких перебувають КСІІ.

Основними завданнями щодо забезпечення безпеки інформації в КСІІ є:

- нормативне правове регулювання в галузі забезпечення безпеки інформації в КСІІ; - визначення загроз безпеки інформації і виявлення вразливостей в програмному і апаратному забезпеченні КСІІ;

- оцінка реальної захищеності КСІІ;

- розробка вимог щодо забезпечення безпеки інформації в КСІІ;

- розробка та реалізація заходів щодо забезпечення безпеки інформації в КСІІ;

- підготовка фахівців у галузі забезпечення безпеки інформації в КСІІ;

- здійснення контролю та нагляду в галузі забезпечення безпеки інформації в КСІІ;

- інформаційне, матеріально-технічне та науково-технічне забезпечення безпеки інформації в КСІІ.

При цьому, зазначені завдання можуть вирішуватися на діючих КСІІ, при модернізації, а також в ході їх проектування та створення. Загальні вимоги

щодо забезпечення безпеки інформації в КСІІ розглядаються з урахуванням необхідності вирішенні цих завдань.

До КСІІ відносяться інформаційно-керуючі або інформаційно-телекомунікаційні системи, які безпосередньо здійснюють управління критично важливими об'єктами та (або) інформаційне забезпечення управління такими об'єктами. КСІІ можуть входити до складу наступних сегментів інформаційної інфраструктури:

- системи органів державної влади;
- системи органів управління правоохоронних структур;
- системи фінансово-кредитної і банківської діяльності;
- системи попередження і ліквідації надзвичайних ситуацій;
- географічні та навігаційні системи;
- мережі зв'язку загального користування на ділянках, що не мають резервних або альтернативних видів зв'язку;
- супутникові системи, що використовуються для забезпечення органів управління і в спеціальних цілях;
- системи управління транспортуванням нафти, нафтопродуктів і газу;
- програмно-технічні комплекси центрів управління взаємно зв’язаної мережі зв'язку;
- системи управління водопостачанням;
- системи управління енергопостачанням;
- системи управління транспортом (наземним, повітряним, морським);
- системи управління потенційно небезпечними об'єктами;
- системи, які не відносяться до вищевказаних, але порушення штатного режиму функціонування яких може призвести до порушення функцій управління чутливими для держави процесами зі значними негативними наслідками.

До основних особливостей КСІІ, які суттєво впливають на зміст вимог щодо забезпечення безпеки інформації, можливо віднести такі:

- технологічна інформація (забезпечує управління технологічними або чутливо важливими процесами), програмно-технічна інформація (програми системного і прикладного характеру, що забезпечують функціонування КСІІ) , командна (керуюча) та вимірювальна інформація, яка не відноситься до інформації з обмеженим доступом (якщо в таких системах циркулює інформація з обмеженим доступом, то вона підлягає захисту відповідно до діючих вимог та норм з технічного захисту інформації);

- управління безперервними технологічними процесами, що обумовлює значно жорсткіші вимоги до часу і порядку виконання автоматизованих функцій, неможливість відключення на період проведення контрольних заходів в інтересах забезпечення безпеки інформації та оцінки їх реальної захищеності від негативних інформаційних впливів;

- різноманітність КСІІ, наявність в них різнорідних, територіально та просторово розподілених елементів з поєднанням різноманітних інформаційних технологій;

- надзвичайна небезпека наслідків виведення з ладу та (або) порушення функціонування КСІІ;

- широке застосування операційних систем реального часу, необхідність адаптації програмних та програмно-апаратних засобів захисту до цих операційних систем;

- неможливість відключення систем для проведення заходів щодо забезпечення безпеки інформації.

Ключові системи різняться між собою:

- за функціональним призначенням;

- за належністю до сфери діяльності держави, суспільства (міністерству, відомству);

- за перевагою у розмірі збитку у разі виведення з ладу (порушення функціонування);

- за ступенем однорідності системи;

- за ступенем розподіленості системи;

- з базування елементів. Залежно від призначення, складу, розміщення та особливостей функціонування КСІІ розрізняється склад актуальних загроз безпеки інформації, а, отже, і зміст пропонованих вимог щодо забезпечення безпеки інформації. Загрози безпеці інформації виникають при появі джерела загроз і вразливостей в КСІІ.

Джерелами загроз безпеки інформації в КСІІ можуть бути:

- іноземні розвідувальні та спеціальні служби у разі недружньої політики іноземних держав, у тому числі в області поширення нових інформаційних технологій з різного роду обмеженнями на постачання сучасних технологій;

- терористичні організації та кримінальні структури;

- окремі сторонні особи або групи осіб з корисливими чи іншими інтересами (хакери тощо);

- представники конкуруючих фірм і організацій, іноземних економічних структур, діяльність яких спрямована проти інтересів державних структур, великих компаній, організацій і підприємств;

- обслуговуючий персонал КСІІ, у функціональні обов'язки якого не входять питання, пов’язані з функціонуванням системи (електрики, техніки, прибиральниці та інший персонал обслуговуючих підрозділів).

Вразливості КСІІ можуть мати місце в охороні системи та її елементів, в системному і прикладному програмному забезпеченні (у тому числі через помилки при його створенні і установці, неправильної конфігурації і т. п.), у процедурах доступу до оброблюваної інформації та контролю такої обробки.

Реалізовані при цьому загрози можуть бути спрямовані:

- на умисне або ненавмисне знищення або модифікацію даних, її системного і прикладного програмного забезпечення;

- на розкрадання (копіювання, крадіжку), розголошення інформації, яка може бути використана для порушення функціонування ключової системи;

- на реалізацію збоїв в роботі апаратного та програмного забезпечення шляхом навмисного або випадкового електромагнітного впливу на елементи КСІІ;

- на руйнування носіїв інформації, елементів комунікації КСІІ.

З урахуванням викладеного, метою формування вимог щодо забезпечення безпеки інформації в КСІІ є

регламентація діяльності господарюючих суб'єктів у сфері забезпечення безпеки інформації в КСІІ в інтересах протидії можливим загрозам безпеки інформації або мінімізації збитків від їх реалізації та збереження тим самим стійкого і безпечного функціонування КСІІ в умовах можливих деструктивних інформаційних впливів:

- організації забезпечення безпеки інформації в КСІІ і дій, пов’язаних з виникненням надзвичайних ситуацій;

- програмного і апаратного забезпечення безпеки інформації в КСІІ, в тому числі в інтересах збереження цілісності та доступності критично важливої інформації, її реєстрації та обліку;

- забезпечення безпеки при взаємодії КСІІ з відкритими (загального користування) інформаційними системами та мережами;

- забезпечення безпеки інформації при захисті від шкідливих програм;

- дій, пов’язаних з обслуговуванням і модернізацією КСІІ, процедур проведення огляду (атестації) організацій на право діяльності з надання державних послуг в галузі забезпечення безпеки інформації в КСІІ, здійснення державного контролю (нагляду) у галузі забезпечення безпеки інформації в КСІІ, оцінки відповідності забезпечення безпеки інформації в КСІІ встановленим вимогам.

2.4 Алгоритм визначення актуальних загроз безпеці інформації на об’єктах критичної інфраструктури

Автоматизовані системи управління об’єктами критичної інфраструктури включають до свого складу системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління, відповідно до концептуальних засад побудови комплексних систем захисту інформації [40]. Нагадаємо, що під об’єктами

критичної інфраструктури розуміємо атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку тощо.

Виникнення загроз та їх реалізація може стати причиною порушення функціонування зазначених об'єктів, утворення надзвичайних ситуацій, пов'язаних з екологічними катастрофами, заподіяння великого матеріального, фінансового, економічного збитку або великомасштабним порушенням життєдіяльності міст та населених пунктів, травмування або загибелі людей тощо.

Кожна загроза безпеці інформації, якщо вона є актуальною для систем управління об'єктами критичної інфраструктури, після ідентифікації підлягає нейтралізації та блокуванню. У системах управління критично важливими об'єктами із заданими структурно функціональними характеристиками і особливостями функціонування існує ймовірність реалізації загрози порушником з відповідним потенціалом. Реалізація цієї загрози призведе до неприпустимих негативних наслідків – збитку, втрат, шкоди.

Кожна загроза характеризується ймовірністю її реалізації і нанесеними нею збитками. Таким чином, показник актуальності загрози критично важливих об'єктів буде пропорційний ймовірності реалізації даної загрози та коефіцієнту її небезпеки.

Метою визначення актуальності загроз безпеці інформації є встановлення факту того, що існує можливість порушення конфіденційності, цілісності або доступності інформації, яка міститься на критично важливих об'єктах і чи призведе порушення хочу б одного з вказаних властивостей безпеки інформації до неприйнятих збитків [41].

У процесі визначення загроз безпеці інформації на всіх стадіях (етапах) життєвого циклу інформаційних систем необхідно регулярно проводити ідентифікацію джерел загроз, оцінювати їх можливості і визначати на цій основі загрози безпеці інформації. Дані про порушників і їх можливості з

реалізації загроз безпеці інформації, отримані при ідентифікації джерел загроз, включаються до моделі загроз безпеці інформації.

З метою проведення дослідження та аналізу взаємодії джерел загроз, власне самих загроз, сприятливих умов реалізації цих загроз, дразливостей, активів, як об’єктів впливу зловмисників, а також системи захисту інформації, яка запобігає даному впливу, розглянемо узагальнену модель процесу захисту інформації (Рис. 3.1) [42].

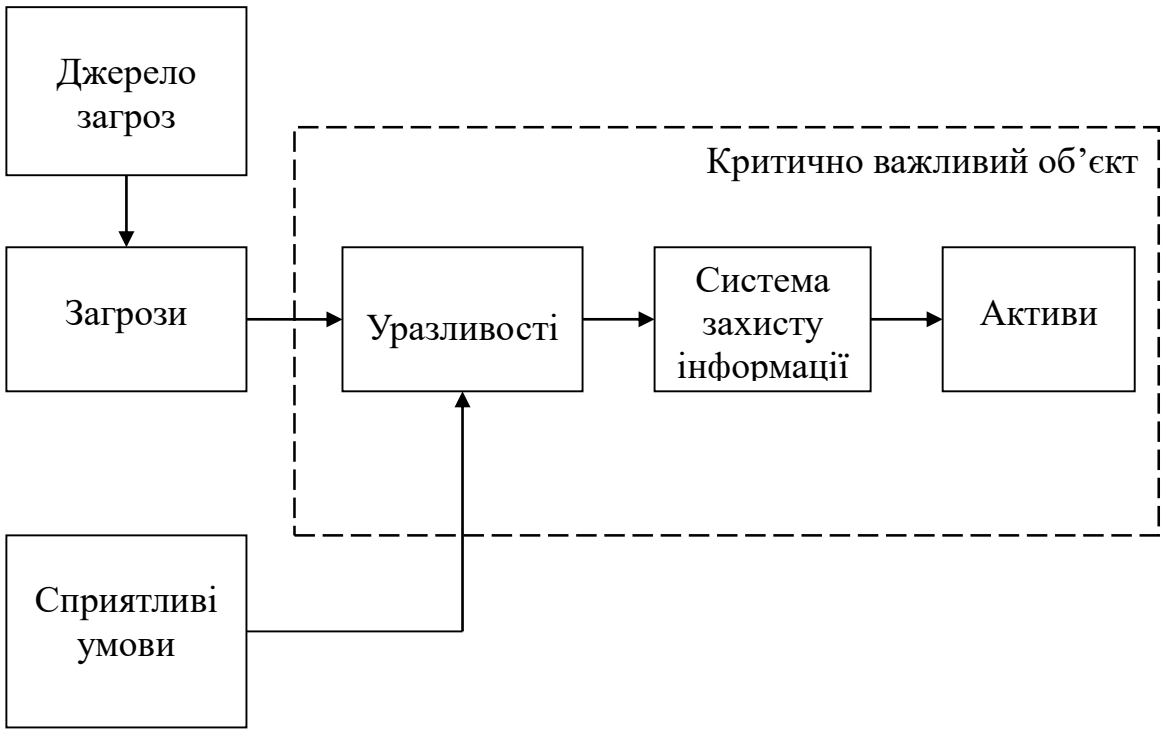

Рис. 2.3 – Узагальнена модель процесу захисту інформації критично важливих об’єктів

Таким чином, для ідентифікації загроз безпеці інформації на об’єктах критичної інфраструктури необхідно визначити джерела загроз, вразливості, сприятливі умови, активи та коефіцієнт небезпеки загроз [43]:

- джерела загроз: можливості (тип, вид, потенціал) порушників;

- вразливості, які можуть використовуватися при реалізації загроз безпеці інформації;

- сприятливі умови для реалізації загроз безпеці інформації;

- активи: об’єкту впливу критично важливих об’єктів, на які спрямована загроза безпеці інформації;

- коефіцієнт небезпеки загроз: результат і наслідки від реалізації загроз безпеці інформації.

Загроза безпеці інформації, яка циркулює на об’єктах критичної інфраструктури, буде вважатися актуальною, якщо для вказаного об’єкта з заданими структурно-функціональними характеристиками і особливостями існує ймовірність реалізації розглянутої загрози порушником з відповідним потенціалом і її реалізація призведе до неприйнятних збитків від порушення конфіденційності, цілісності або доступності інформації.

Це викликано тим, що в автоматизованих системах критично важливих об’єктів існую досить тісний взаємозв’язок автоматизованих систем з фізичними процесами і виконавчими пристроями. Тому порушення безпеки інформації в даних системах може призвести до наслідків у промисловому секторі.

Враховуючи зазначене, небезпека загрози в автоматизованих системах критично важливих об’єктів із множини загроз буде визначатися оцінкою можливих наслідків від її реалізації з позиції впливу на функціонування автоматизованих систем об’єктів критичної інфраструктури, а рівень тяжкості таких наслідків – коефіцієнтом небезпеки такої загрози.

Ймовірність реалізації загрози можливо визначити на основі аналізу статистичних даних про частоту реалізації загроз безпеці інформації (виникнення інцидентів безпеки) в автоматизованих системах критично важливих об’єктів і (або) однотипних систем.

За відсутності таких статичних даних актуальність загрози визначається на основі оцінки можливості реалізації загрози безпеці інформації, яка, в свою чергу, визначається на основі оцінки рівня захищеності автоматизованої системи критично важливих об’єктів та потенціалу порушника, необхідного для реалізації даної загрози.

Коефіцієнт небезпеки загрози можливо визначити на основі оцінки ступеня наслідків від порушення конфіденційності, цілісності або доступності в автоматизованих системах критично важливого об’єкта.

Актуальність загроз безпеці інформації визначається щодо загроз, для яких експертним методом обумовлено наступне [44]:

- можливості (потенціал) порушника достатні для реалізації загрози безпеці інформації;

- в автоматизованій системі критично важливого об’єкта є потенційні уразливості, які можуть бути використані при реалізації певної загрози безпеці інформації;

- структурно-функціональні характеристики та особливості функціонування автоматизованої системи критично важливого об’єкта не виключають можливості застосування способів, необхідних для реалізації певної загрози;

- реалізація загрози безпеці інформації призведе до порушення конфіденційності, цілісності або доступності інформації, в результаті якого можливе виникнення неприйнятних негативних наслідків і заподіяння значної шкоди.

Джерелами інформації щодо вихідних даних про загрози безпеці інформації та їх характеристики можуть бути базові та типові моделі загроз безпеці інформації, визначені нормативними документами для різних класів і типів автоматизованих систем.

Таким чином, алгоритм визначення актуальності загрози безпеці інформації на критично важливих об’єктах можна представити у загальному вигляді (Рис. 2.3) [45]

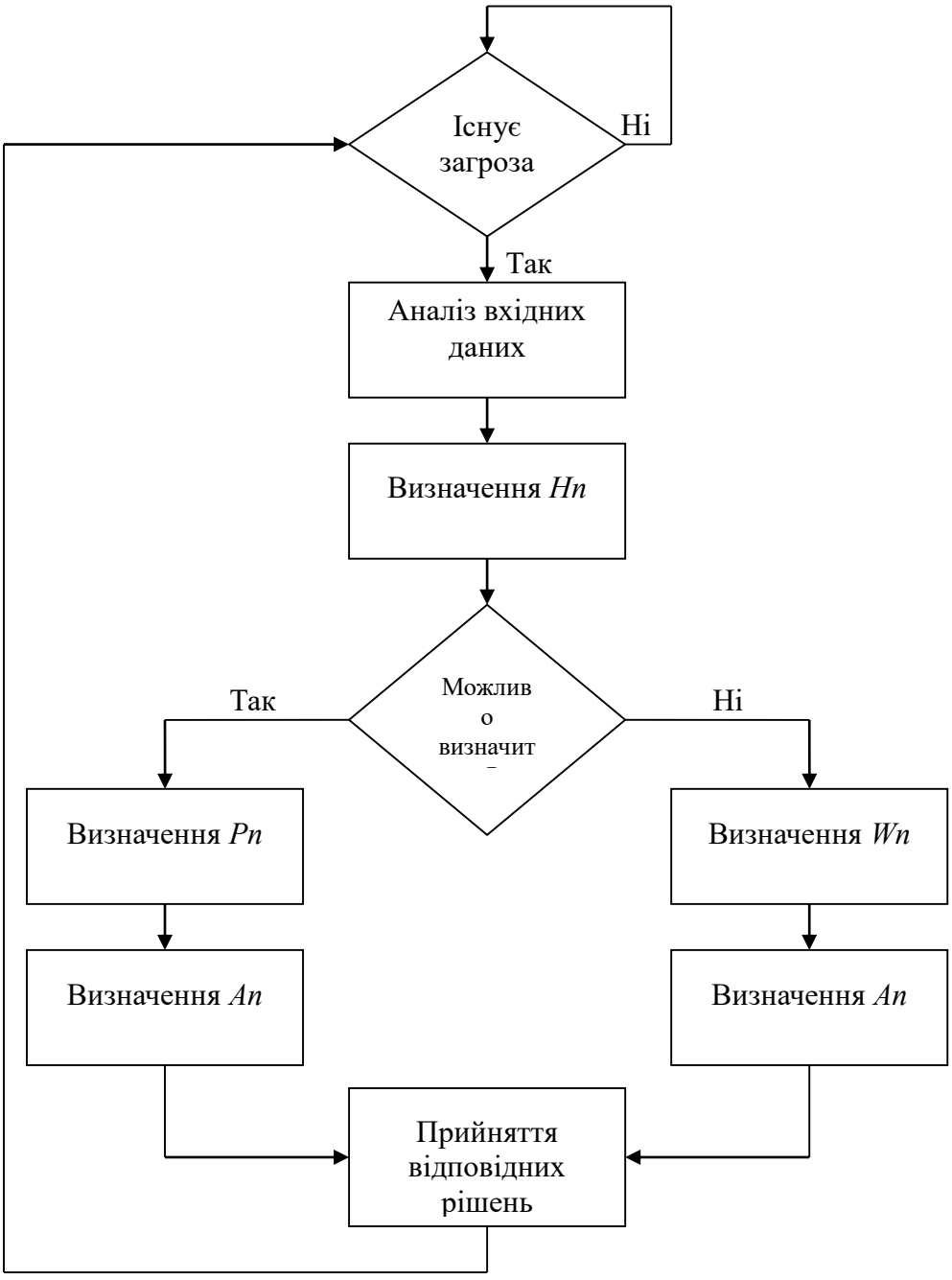

Рис. 2.4 – Алгоритм визначення актуальності загрози безпеці інформації

де:

Hn – коефіцієнт небезпеки загрози, ступінь тяжкості наслідків реалізації даної загрози;

Pn – ймовірність реалізації загрози безпеці інформації

An – актуальність загрози безпеці інформації;

Wn – можливість реалізації загрози

У випадку виявлення загрози безпеці інформації визначається її актуальність, ґрунтуючись на аналізі вихідних даних, а саме:

- наявності чи відсутності сприятливих умов для реалізації даної загрози;

- наявності чи відсутності необхідної статистики щодо фактів реалізації даної загрози;

- наявності чи відсутності у потенційних порушників мотивації для реалізації даної загрози;

- можливої частоти реалізації даної загрози;

- рівня захищеності автоматизованої системи критично важливого об’єкта щодо реалізації даної загрози;

- потенціалу порушника, необхідного для реалізації даної загрози.

Разом з тим, визначається ступінь можливих наслідків у випадку реалізації виявленої загрози.

У подальшому, в залежності від наявних вихідних даних, здійснюється або оцінка ймовірності реалізації виявленої загрози, або оцінка можливості її реалізації.

За результатами проведеної оцінки приймаються рішення щодо вжиття відповідних заходів, спрямованих на ефективне та своєчасне блокування (нейтралізацію) загроз безпеки інформації, в результаті реалізації яких можливі неприйнятні наслідки.

2.5 Методика з підвищення рівня інформаційної безпеки автоматизованих систем управління критично важливими об’єктами

Методика – це заснований на оцінці ризиків підхід для управління ризиками інформаційної безпеки. Вона складається з трьох частин: “Основа методики”, “Рівні реалізації заходів із захисту інформації” та “Профілі рівня захищеності”. Кожен компонент Методики посилює зв'язок між факторами розвитку і заходами інформаційної безпеки [46] .

Основа методики – це сукупність заходів інформаційної безпеки, бажаних цільових показників та застосовних довідкових матеріалів, які є універсальними для галузей критично важливих об’єктів інфраструктури. Основа методики базується на галузевих стандартах, нормах та загальноприйнятих методах, дозволяючи застосовувати загальні вимоги щодо заходів інформаційної безпеки та цільових показників в масштабі всього підприємства, від рівня керівництва до рівня виконання операцій/впровадження. Основа методики складається з п’яти паралельних і безперервних функцій: ідентифікації, захисту, виявлення, реагування, відновлення. Спільно ці функції забезпечують високий стратегічний рівень життєвого циклу управління ризиками підприємства. Основа методики ідентифікує базові категорії та під категорії для кожної функції і співвідносить їх з прикладами, наведеними в довідкових матеріалах, а саме: в існуючих стандартах, нормах і загальноприйнятих методах для кожної під категорії.

Рівні реалізації заходів із захисту інформації (далі – Рівні) надають інструменти для оцінки того, як підприємства розглядає ризики інформаційної безпеки та які процеси впроваджені для управління цими ризиками. Рівні описують міру, в якій методи управління ризиками інформаційної безпеки, впроваджені підприємством, відповідають характеристикам, зазначеним у Методиці (наприклад, інформованість про ризики і загрози, повторюваність та адаптивність процесів). Рівні характеризують, наскільки високою є інформаційна захищеність підприємства, в діапазоні від часткового управління ризиками (рівень 1) до адаптивного управління ризиками (рівень 4). Ці рівні відображають процес від довільних, ситуативних реагувань до гнучких підходів, що базуються на інформативності про ризики. У процесі відбору рівня підприємство має враховувати свої поточні методики управління ризиками, характеристики загроз, законодавчі та нормативні вимоги, комерційні та стратегічні цілі, а також наявні стримуючі фактори [46].

Профіль рівня захищеності (далі – Профіль) – це цільові показники, що базуються на потребах бізнесу, обрані підприємством і категорій і під категорій

Методики. Профіль можна охарактеризувати я пристосування стандартів, норм і загальноприйнятих методів до основи методики в конкретному сценарії впровадження. Профілі можуть бути використані для визначення можливостей покращення стану інформаційної безпеки шляхом порівнянн “поточного” профілю (стан “як є”) з “цільовим” профілем (стан “бажаний”). Для розробки профілю підприємство може переглянути всі категорії та під категорії та, виходячи з факторів розвитку бізнесу та оцінки ризиків, визначити, які з них є найбільш важливими; в разу необхідності можна додати категорії й під категорії, необхідні для усунення ризиків підприємства. Поточний рівень в подальшому може бути використаний для підтримки процесу встановлення пріоритетів та вимірювання процесу на шляху до цільового профілю. Поточний профіль також може бути фактором інших потреб підприємства, включаючи економічну ефективність та інновації. Профілі можуть бути використані для проведення самооцінки й обміну інформацією всередині підприємства або між підприємствами.

Управління ризиками – це безперервний процес виявлення, оцінки та реагування на ризики. Для управління ризиками підприємства повинні усвідомлювати можливість виникнення події та її вплив. За допомогою цієї інформації підприємство може визначити прийнятний рівень ризику для надання послуг і врахувати це в своєму показнику ризикостійкості.

Розуміючи свою ризикостійкість, підприємство може встановлювати пріоритетність заходів інформаційної безпеки, забезпечуючи прийняття обґрунтованих рішень про витрати на забезпечення інформаційної безпеки. Впровадження програм управління ризиками дозволяє підприємствам виміряти й реалізувати коригування своїх програм із забезпечення інформаційної безпеки. Підприємства можуть обирати різні підходи до управління ризиками, в тому числі мінімізувати вплив ризиків, передавати, уникати або приймати ризики в залежності від потенційного впливу на надання послуг критично важливих об'єктів інфраструктури.

Методика використовує процеси управління ризиками, які дозволяють підприємствам встановлювати пріоритети для рішень щодо інформаційної безпеки та обмінюватися інформацією про них. Вона підтримує регулярне оцінювання ризиків і перевірку факторів бізнесу, дозволяючи підприємствам вибирати цільові стани для заходів інформаційної безпеки, що відображають бажані цільові показники. Таким чином, Методика дає підприємствам можливість динамічно обирати й реалізовувати заходи з поліпшення управління ризиками інформаційної безпеки для середовищ IT та СУВП.

Методика є адаптивною та надає гнучкі та засновані на оцінці ризиків засоби, які можна використовувати в широкому колі процесів управління ризиками інформаційної безпеки.

Основа методики

Основа методики пропонує набір заходів для досягнення конкретних цільових показників інформаційної безпеки, а також приклади управління ризиками для досягнення таких цільових показників. Основа методики – це не контрольний список дій, що мають бути виконані. Вона надає ключові цільові показники інформаційної безпеки, визначені галуззю як корисні в управління ризиками інформаційної безпеки. Основа складається з чотирьох елементів: “Функції”, “Категорії”, “Під категорії” та “Довідкові матеріали” (Таблиця 2.1)

Таб. 2.1 Структура основи методики

Функції	**Категорії**	**Підкатегорії**	**Довідкові матеріали**
ІДЕНТИФІКАЦІЯ			
ЗАХИСТ			
ВИЯВЛЕННЯ			

РЕАГУВАННЯ			
ВІДНОВЛЕННЯ			

Взаємозв'язок та роль елементів основи методики:

Функції організують базові заходи інформаційної безпеки на найвищому рівні. Існує п’ять функцій: ідентифікація, захист, виявлення, реагування і відновлення. Вони допомагають підприємству відобразити виконуване ним управління ризиками інформаційної безпеки шляхом впорядкування інформації, дозволяючи приймати рішення з управління ризиками, реагувати на загрози, а також самовдосконалюватися, враховуючи набутий досвід. Функції також узгоджуються з існуючими методиками управління інцидентами й допомагають показати вплив інвестицій в інформаційну безпеку. Наприклад, інвестиції в планування ф тренування покращують своєчасне реагування і відновлення, в результаті чого знижується вплив на надання послуг.

Категорії – це розділи функції за групами цільових показників інформаційної безпеки, тісно пов’язаних з програмними потребами й конкретними заходами. Прикладами категорії є, зокрема, “Управління активами”, “Управління доступом” та “Процеси виявлення” [47].

Підкатегорії розділяють категорію відповідно до тих чи інших цільових показників технічних заходів та (або) заходів з управління. Вони надають набір результатів, які, хоча і не є вичерпними, допомагають досягти цільових показників у кожній категорії. Прикладами під категорій, зокрема, є “Зовнішні інформаційні системи каталізовано”, “Дані, що зберігаються, захищено” й “Повідомлення від систем виявлення досліджено”.

Довідкові матеріали – це спеціальні розділи, що містять стандарти, рекомендації та зразки загальноприйнятих методів, поширених у галузях критично важливих об'єктів інфраструктури. Розділи ілюструють способи досягнення цільових показників для кожної підкатегорії. Довідкові матеріали, представлені в Основі методики, є ілюстративними і не вичерпними. Вони базуються на міжгалузевих нормах, на які зроблено найбільше посилань при розробці Методики. П'ять функцій Основи методики описані нижче. Ці функції не призначені для формування послідовного процеси або приведення до незмінного бажаного кінцевого стану. Вони, скоріше, мають виконуватися одночасно й безперервно для формування оперативної культури, здатної протистояти динамічним ризикам інформаційної безпеки.

Ідентифікація – поглиблення знань підприємства щодо управління ризиками інформаційної безпеки відносно систем, активів, даних і можливостей. Заходи, передбачені функцією "Ідентифікація", є обов'язковою умовою ефективного використання Методики. Розуміння ресурсів, що підтримують найважливіші функції, а також пов'язаних ризиків інформаційної безпеки дозволяє підприємству зосередити свої зусилля й встановити їх пріоритети відповідно до стратегії управління ризиками.

Захист – розробка та впровадження відповідних засобів захисту інформації для забезпечення надання послуг критично важливих об'єктів інфраструктури. Функція "Захист" дозволяє обмежити або стримати вплив потенційної події інформаційної безпеки. Прикладами цільових показників в межах цієї функції є, зокрема, такі: управління доступом, інформованість та навчання, безпека даних, процеси та процедури захисту інформації, технічне обслуговування, захисні технології.

Виявлення – розробка і впровадження для виявлення події інформаційної безпеки. Функція "Виявлення" дозволяє своєчасно виявити подію інформаційної безпеки. Прикладами цільових показників категорій в межах цієї функції є, зокрема, такі: аномалії та події, безперервний моніторинг захисту, процеси виявлення.

Реагування – розробка і впровадження заходів для реагування на виявлену подію інформаційної безпеки. Функція “Реагування” дозволяє стримати вплив потенційної події інформаційної безпеки. Прикладами цільових показників категорій в межах цієї функції є, зокрема, такі: планування реагування, комунікації, аналіз, мінімізація наслідків, покращення.

Відновлення – розробка і впровадження заходів для підтримки планів щодо забезпечення стійкості та відновлення можливостей або послуг, які були порушені внаслідок події інформаційної безпеки. Функція “Відновлення” забезпечує своєчасне відновлення нормальної роботи та зменшення впливу події інформаційної безпеки. Прикладами цільових показників категорій в межах цієї функції є, зокрема, такі: планування відновлення, покращення, комунікації.

Рівні реалізації заходів із захисту інформації

Рівні реалізації заходів із захисту інформації (далі – Рівні) надають інструменти для оцінки того, як підприємство розглядає ризики інформаційної безпеки та які процеси проваджені для управління цими ризиками. Існує чотири рівня захищеності: найнижчий перший рівень – часткове управління ризиками та найвищий четвертий рівень – адаптивне управління ризиками. Рівні описують методи управління ризиками інформаційної безпеки по мірі підвищення їх суворості та складності, а також міру, в якій управління ризиками інформаційної безпеки відповідає потребам та інтегроване підприємством у загальну практику управління ризиками. Заходи управління ризиками передбачають багато аспектів інформаційної безпеки, в тому числі міру, в якій заходи із забезпечення конфіденційності та громадських свобод інтегровані підприємством у практику управління ризиками й реагувань на потенційні ризики.

Процес відбору рівня враховує поточні методи підприємства щодо управління ризиками, характеристики загроз, законодавчі та нормативні вимоги, комерційні та стратегічні цілі, а також наявні стримуючі фактори. Підприємство повинне обирати той рівень, який відповідає цілям

підприємства, може бути впроваджений і знижує ризики інформаційної безпеки для критично важливих активів і ресурсів до прийнятного рівня. Для визначення бажаного рівня підприємство повинне розглянути можливість використання зовнішніх рекомендацій, отриманих від державних відомств і установ, центрів обміну та аналізу інформації, існуючих моделей зрілості або інших джерел.

Хочу підприємствам з рівнем 1 (часткове управління ризиками) рекомендується перейти до рівня 2 або вище, рівні не представляють рівні зрілості. Прогрес до більш високих рівнів рекомендується, коли він призводить до скорочення ризиків інформаційної безпеки та є доцільним з економічної точки зору. Запорукою успішної реалізації методики є досягнення цільових показників, описаних у цільовому профілі підприємства, а не визначення рівня.

Визначення рівнів:

Рівень 1. Часткове управління ризиками.

Процес управління ризиками. Методи підприємства щодо управління ризиками інформаційної безпеки не формалізовані, а управління ризиками має довільний та іноді ситуативний характери. Пріоритетність заходів інформаційної безпеки безпосередньо не враховує цілі підприємства щодо управління ризиками, характеристики загроз, комерційні та стратегічні цілі.

Інтегрована програма управління ризиками. Інформативність про ризики на рівні підприємства є недостатньою, а спільний підхід до управління ризиками інформаційної безпеки в масштабі всього підприємства не встановлено. Підприємство реалізує управління ризиками інформаційної безпеки нерегулярно та ситуативно через неузгоджений досвід або інформацію, отриману з зовнішніх джерел. Підприємство не має процесів, що дозволяють внутрішній обмін даними з інформаційної безпеки.

Зовнішня участь. Підприємство не має впроваджених процесів, що дозволяють брати участь у координації або співпраці з іншими організаціями.

Рівень 2. Інформованість про ризики.

Процес управління ризиками. Методи управління ризиками затверджені керівництвом, але не встановлені як загальне правило в масштабі всього підприємства. Пріоритетність заходів інформаційної безпеки безпосередньо враховує цілі підприємства щодо управління ризиками, характеристики загроз, комерційні та стратегічні цілі.

Інтегрована програма управління ризиками. Інформативність про ризики наявна, але спільний підхід до управління ризиками інформаційної безпеки в масштабі всього підприємства не встановлено. Процеси та процедури, що базуються на інформативності про ризики та затверджені керівництвом, визначені та впроваджені, а персонал має достатні ресурси для виконання своїх обов'язків щодо забезпечення інформаційної безпеки. Обмін даними про інформаційну безпеку здійснюється всередині підприємства довільно.

Зовнішня участь. Підприємство знає свою роль в більшій екосистемі, але воно не формалізувало свої можливості, щоб взаємодіяти та обмінюватися інформацією з зовнішніми зацікавленими сторонами.

Рівень 3. Стабільне управління ризиками.

Процес управління ризиками. Методи підприємства щодо управління ризиками офіційно схвалені та прийняті як правило. Методи підприємства із забезпечення інформаційної безпеки регулярно оновлюються на основі пристосування процесів управління ризиками до змін комерційних або стратегічних вимог та середовища загрози й технологій, що постійно змінюється.

Інтегрована програма управління ризиками. Наявний спільний підхід до управління ризиками інформаційної безпеки в масштабі всього підприємства. Методи, процеси і процедури, що базуються на інформативності про ризики, визначені, впроваджені за призначенням, постійно переглядаються. Послідовні методи впроваджено для ефективного реагування на зміни в ризиках. Персонал має знання та навички для виконання своїх ролей і обов'язків.

Зовнішня участь. Підприємство розуміє своїх підлеглих та партнерів і отримує інформацію від цих партнерів, що дозволяє забезпечувати співпрацю і прийняття рішень, що базуються на інформованості про ризики, в рамках підприємства у відповідь на події.

Рівень 4. Адаптивне управління ризиками.

Процес управління ризиками. Підприємство адаптує свої методи інформаційної безпеки, виходячи з отриманого досвіду і прогностичних показників, одержаних із попередніх і поточних заходів інформаційної безпеки. Шляхом безперервного вдосконалення з використанням передових технологій і методів в області інформаційної безпеки підприємство активно адаптується до змінюваних обставин в галузі IT і в установлені терміни реагує на загрози, що постійно ускладнюються.

Інтегрована програма управління ризиками. У масштабі всього підприємства наявний спільний підхід до управління ризиками інформаційної безпеки, в якому використовуються методи, процеси і процедури, що базуються на інформованості про ризики, спрямовані на подолання потенційних подій інформаційної безпеки. Управління ризиками інформаційної безпеки є частиною культури підприємства й постійно розривається за рахунок отриманого досвіду, інформації з інших джерел і безперервної інформованості про заходи, що мають відношення до систем і мереж підприємства.

Зовнішня участь. Підприємство управляє ризиками та активно обмінюється інформацією з партнерами з метою забезпечення поширення і врахування точної та актуальної інформації для покращення інформаційного захисту до настання подій інформаційної безпеки.

Профіль рівня захищеності

Профіль рівня захищеності (далі – Профіль) – це узгодження функцій, категорій та під категорій з вимогами бізнесу, ризикостійкістю та ресурсами підприємства. Профіль дозволяє підприємствам створити дорожню карту для зниження ризиків інформаційної безпеки, яка узгоджена з цілями підприємства

та галузі, враховує законодавчі та нормативні вимоги й передовий галузевий досвід, а також відображає пріоритети управління ризиками. Оскільки багато підприємств мають складну структуру, вони можуть вибрати кілька профілів, узгоджених з конкретними компонентами та індивідуальними потребами підрозділу. Профілі рівня захищення можуть бути використані для опису поточного стану або бажаного цільового конкретних заходів інформаційної безпеки. Цільовий профіль зазначає цільові показники, необхідні для досягнення бажаних цілей управління ризиками інформаційної безпеки. Профілі підтримують комерційні та стратегічні цілі й допомагають обмінюватися даними про ризики всередині й між організаціями. Для забезпечення гнучкості впровадження Методики наведемо шаблони профілів.

Порівняння профілів (наприклад, поточного й цільового профілів) може виявити недоліки, що повинні бути усунуті для досягнення цілей управління ризиками інформаційної безпеки. План дій щодо усунення цих недоліків може доповнювати дорожню карту. Пріоритетність заходів з усунення недоліків має базуватися на потребах бізнесу підприємства й процесах управління ризиками. , Цей підхід, оснований на інформованості про ризики, дозволяє підприємству налаштувати методи оцінки ресурсів (наприклад, штатний розклад, фінансування) для досягнення цілей інформаційної безпеки ефективно з економічної точки зору та відповідно до пріоритетів.

Координування впровадження Методики

На Рис. 2.5 зображено умовний потік інформації та рішень на таких рівнях підприємства:

- Керівний
- Бізнес/процес
- Впровадження/операції

На керівному рівні визначаються стратегічні пріоритети, наявні ресурси й загальна ризикостійкість, рівня “Бізнес/процес”. Рівень “Бізнес/процес” вносить інформацію в процес управління ризиками, а потім співпрацює з рівнем “Впровадження/операції” для врахування потреб бізнесу і створення

профілю. Рівень “Впровадження/операції” повідомляє про хід реалізації профілю рівня “Бізнес/процес”. Рівень “Бізнес/процес” використовує цю інформацію для виконання оцінки впливу. Керівництво рівня “Бізнес/процес” повідомляє результати цієї оцінки впливу керівному рівню для інформування всіх учасників процесу управління ризиками підприємства та рівню “Впровадження/операції” для оповіщення про вплив на бізнес.

Рис. 2.5 Умовні потоки інформації та рішень всередині підприємства

Порядок використання Методики

Підприємство може використовувати Методику як ключовий елемент свого систематичного процесу виявлення, оцінки та управління ризиками інформаційної безпеки. Методика не призначена для заміни існуючих процесів. Підприємство може використовувати сів поточний процес, пристосувавши його до Методики, щоб визначити недоліки в своєму існуючому підході до управління ризиками інформаційної безпеки й розробити дорожню карту вдосконалення. Використовуючи Методику як інструмент управління ризиками інформаційної безпеки, підприємство може визначити заходи, які є найбільш важливими для надання послуг критично важливих

об’єктів інфраструктури і встановлення пріоритетності витрат для максимізації впливу інвестицій.

Методика розробляється як додаток до існуючих операцій бізнесу та системи інформаційної безпеки. Вона можу служити основою для нової програми інформаційної безпеки або механізмом поліпшення існуючої. Методика надає засіб вираження вимог інформаційної безпеки для бізнес-партнерів і клієнтів та може допомогти виявити недоліки в методах забезпечення інформаційної безпеки, вживаних на підприємстві. Вона також надає загальний набір запобіжних заходів і процесів для оцінки наслідків дотримання конфіденційності та цивільних свобод в контексті програми інформаційної безпеки.

Основний огляд методів інформаційної безпеки

Методику можна використовувати для порівняння поточних заходів підприємства в області інформаційної безпеки з тими, що описані в “Основі методики”, узгоджених з п’ятьма функціями високого рівня: ідентифікацією, захистом, виявленням, реагуванням і відновленням. Підприємство можу зясувати, що воно вже досягло бажаних результатів, тобто управління інформаційною безпекою відповідає відомим ризикам. І навпаки, підприємство може визначити, що воно має можливість (або потребу) покращити управління ризиками. Підприємство може використати цю інформацію для розробки плану дій щодо зміцнення існуючих методів інформаційної безпеки і зменшення ризиків. Підприємство також може виявити, що воно забагато інвестує для досягнення певних цільових показників. Підприємство також може виявити, що воно забагато інвестує для досягнення певних цільових показників. Воно може використати цю інформацію для перегляду пріоритетів ресурсів для зміцнення інших методів інформаційної безпеки.

Хоча ці п’ять функцій високого рівня не змінюють процес управління ризиками, вони пропонують лаконічний метод для вищих та інших керівників для визначення фундаментальних понять ризиків інформаційної безпеки,

необхідних для оцінки того, як виконується управління виявленими ризиками й наскільки підприємство відповідає на високому рівні існуючим стандартам, нормам і загальноприйнятим методам забезпечення інформаційної безпеки. Методика також може допомогти підприємству відповісти на фундаментальні питання, наприклад, “Як у нас справи?”. Після цього можна переходити до більш обґрунтованого підходу для зміцнення методів інформаційної безпеки в разі необхідності.

Створення або вдосконалення програми інформаційної безпеки

Нижчезазначені кроки демонструють, як підприємство може використовувати Методику для створення нової програми інформаційної безпеки або поліпшення існуючої. За необхідності кроки треба повторювати для забезпечення постійного вдосконалення інформаційної безпеки.

Крок 1: встановити пріоритетність і сферу застосування. Підприємство визначає свої комерційні та стратегічні цілі, встановлює пріоритети на високому рівні. За допомогою цієї інформації підприємство приймає стратегічні рішення щодо інформаційної безпеки й визначає перелік систем і активів, які підтримуватимуть обрані виробничі лінії або процеси. Методика може бути адаптована для підтримки різних виробничих ліній або процесів в межах підприємства, яке може мати різні потреби бізнесу й пов’язану з ними ризикостійкість.

Крок 2: направити зусилля. Після того як сферу застосування інформаційної безпеки визначено для виробничої лінії або процесу, підприємство ідентифікує пов’язані системи та активи, нормативні вимоги та загальний підхід до управління ризиками. Потім підприємство ідентифікує загрози і вразливості цих систем і активів.

Крок 3: створити поточний профіль рівня захищеності. Підприємство розробляє поточний профіль, вказавши наявні за даний час показники по категоріях і під категоріях “Основи методики”.

Крок 4: виконати оцінку ризиків. Ця оцінка може біти виконана відповідно до загального процесу управління ризиками, впровадженому на

підприємстві, або згідно з попередніми заходами по оцінці ризику. Підприємство аналізує операційне середовище для того, щоб розрізнити ймовірність події інформаційної безпеки і вплив такої події на підприємство. Для глибокого розуміння ймовірності та впливу подій інформаційної безпеки важливо, щоб підприємства прагнули включити до своїх процесів забезпечення інформаційної безпеки нові ризики й дані про загрози і вразливості.

Крок 5: створити цільовий профіль рівня захищеності. Підприємство створює цільових профіль, який фокусується на оцінці категорій і під категорій Методики, описуючи бажані цільові показники інформаційної безпеки підприємства. Підприємства також можуть розробити власні додаткові категорії й під категорії для врахування своїх унікальних ризиків. Підприємство може також врахувати вплив і вимоги зовнішніх зацікавлених сторін, таких як юридичні особи галузі, клієнти й ділові партнери, при створенні цільового профілю.

Крок 6: визначити і проаналізувати недоліки, встановити для них пріоритетність. Підприємство порівнює поточний і цільовий профілі для визначення недоліків. Потім створюється план дій відповідно до встановлених пріоритетів для усунення недоліків, який спирається на фактори стратегічних цілей, аналіз витрат та прибутку, а також розуміння ризиків для досягнення цільових показників у цільовому профілі. Потім підприємство визначає ресурси, необхідні для усунення недоліків. Таке використаня профілів допомагає підприємству приймати обґрунтовані рішення про заходи інформаційної безпеки, підтримує управління ризиками й дозволяє підприємству виконувати економні цільові покращення.

Крок 7: реалізувати план дій. Підприємство визначає, які заходи слід вжити для усунення недоліків (у разі наявності) виявлених на попередньому кроці. Долі підприємство відстежує поточні методи інформаційної безпеки відносно цільового профілю. Методикою визначено приклади довідкових матеріалів щодо категорій і під категорій, але підприємства визначити

самостійно, які стандарти, норми та загальноприйняті методи, включаючи специфічні для галузі, краще відповідають їх потребам.

За необхідності підприємство може повторювати кроки для безперервного оцінювання і покращення своєї інформаційної безпеки. Наприклад, підприємства можуть виявити, що частіше повторення кроку “Направити зусилля” покращує якість оцінок ризику. Крім того, підприємства можуть відстежувати прогрес шляхом оновлень поточного профілю через ітераційні інтервали, в подальшому порівнюючи поточний профіль із цільовим. Підприємства можуть також використовувати цей процес для узгодження своєї програми інформаційної безпеки з бажаним рівнем Методики щодо реалізації заходів із захисту інформації.

Інформування зацікавлених сторін про вимоги інформаційної безпеки

Методика пропонує універсальну базу для інформування про вимоги інформаційної безпеки незалежних зацікавлених сторін, відповідальних за надання найважливіших послуг критично важливих об’єктів інфраструктури. Приклади інформування:

- Підприємство може використовувати цільовий профіль, щоб висловити вимоги до управління ризиками інформаційної безпеки зовнішньому постачальнику послуг (наприклад, постачальнику хмарних технологій, що використовуються підприємством для експорту даних).

- Підприємство може висловити свій стан інформаційної безпеки за допомогою поточного профілю, щоб повідомити результати або порівняти з вимогами придбання.

- Власник/оператор критично важливого об’єкта інфраструктури, визначивши зовнішнього партнера, від якого залежить відповідна інфраструктура, може використовувати цільовий профіль, щоб передати необхідні категорії й під категорії.

- Галузь критично важливої інфраструктури може створити цільовий профіль для використання учасниками такої галузі в якості початкового базового профілю для розробки їх унікальних цільових профілів.

- Виявлення можливостей в нових або переглянутих довідкових матеріалах.

2.6 Висновки до другого розділу

У другому розділі роботи досліджено порядок створення систем захисту інформації на об'єктах критичної інфраструктури та розроблено методичні підходи до підвищення рівня їх інформаційної безпеки.

Встановлено, що комплексна система захисту інформації включає організаційні та інженерно-технічні заходи, створення яких регламентується нормативними документами НД ТЗІ 3.7-003-23 та НД ТЗІ 3.7-001-99. Обґрунтовано доцільність застосування системи управління інформаційною безпекою на базі міжнародних стандартів ISO 27001, що реалізується через чотириетапний циклічний процес планування, виконання, перевірки та удосконалення.

Аналіз міжнародного досвіду США, Великобританії, Нідерландів, Чехії та Польщі дозволив визначити спільні елементи критичних систем інформаційної інфраструктури: енергетика, телекомунікації, фінанси, транспорт, водопостачання та державне управління. Встановлено, що захист здійснюється через ідентифікацію критичних систем, аналіз ризиків і уразливості, оцінку загроз та ухвалення запобіжних заходів.

Розроблено узагальнену модель процесу захисту інформації та алгоритм визначення актуальності загроз, де актуальність визначається через ймовірність реалізації загрози та коефіцієнт її небезпеки. Запропоновано методику підвищення рівня інформаційної безпеки, що базується на п'яти функціях (ідентифікація, захист, виявлення, реагування, відновлення), чотирьох рівнях захисту та семиетапному процесі впровадження від встановлення пріоритетів до реалізації плану дій.

Розділ 3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Характеристика обраного об'єкта критичної інфраструктури

Об'єктом цього дослідження виступає SCADA-система для автоматизованого керування технологічними процесами умовного підприємства ТОВ "ЕнергоСистема". Дане підприємство належить до об'єктів критичної енергетичної інфраструктури України згідно із Законом України "Про критичну інфраструктуру". Якщо система вийде з ладу, це може спричинити масштабні відключення електроенергії і створити загрозу для національної безпеки.

Розглянута SCADA-система керує трьома трансформаторними підстанціями з напругою 110/35/10 кВ і загальною потужністю 180 МВА. Саме ці підстанції живлять електроенергією цілий промисловий район в обласному центрі. Там мешкає близько 45 тисяч людей. До мережі підключені 12 промислових підприємств - в основному це машинобудування і харчова промисловість. Окрім заводів, система підтримує роботу важливих соціальних об'єктів: дві лікарні, вісім шкіл і водоканал.

SCADA працює безупинно: 24 години на добу, 7 днів на тиждень, без жодних вихідних. Вимоги до надійності тут дуже жорсткі - коефіцієнт готовності не менше 99,97%. Це означає, що за рік система може простоювати максимум 2,6 години.

Архітектура системи класична, багаторівнева. Перший рівень - польовий (Field Level). На ньому знаходяться датчики які вимірюють струм і напругу в мережі (це трансформатори ТТ і ТН), механізми що управляють високовольтними вимикачами. Також тут встановлені мікропроцесорні пристрої захисту, наприклад Siemens SIPROTEC 5, їх приблизно 24 штуки на всіх підстанціях.

Наступним йде контролерний рівень, в ньому стоять програмовані логічні контролери (ПЛК ABB AC500 - всього 8 штук) і віддалені термінали (RTU Siemens SIMATIC S7-1500 - 15 одиниць). Вони збирають телеметрію з датчиків, виконують базові алгоритми управління прямо на місці й передають дані на SCADA-сервери.

На серверному рівні працюють два сервери. Основний - Dell PowerEdge R740 з двома Intel Xeon і 64 гігабайтами оперативної пам’яті, під управлінням Windows Server 2019. Другий сервер - повна копія першого, він працює як гарячий резерв: якщо основний вийде з ладу, він миттєво підхопить роботу. Як програмну платформу використовують Aveva System Platform (або її аналог). Сервери збирають і зберігають всі дані з контролерів, формують звіти, фіксують аварії, надсилають сигнали тривоги й обслуговують операторські станції.

Щодо операторських станцій (HMI): їх чотири, всі - на базі комп’ютерів HP ProDesk 600 G5 з Windows 10 Pro. Два робочих місця розташовані на головній підстанції, ще два - по одному на інших. На кожному столі - монітор з діагоналлю 27 дюймів. На екрані оператор бачить мнемосхеми підстанцій, які допомагають контролювати ситуацію в реальному часі (приклади показані на рис. 3.1 та 3.2).

Диспетчерський рівень - це диспетчерський пункт, який знаходиться десь за 25 км від підстанцій. Основний зв'язок іде через оптоволоконну лінію зі швидкістю 100 Мбіт/с. Якщо раптом ця лінія вийде з ладу, є запасний варіант - радіозв'язок.

У самому диспетчерському пункті працюють два автоматизованих робочих місця для диспетчерів. Звідти вони можуть управляти всім обладнанням на підстанціях - і все це віддалено, навіть не виходячи з кабінету.

Коли на підстанції стається аварія, термінали захисту одразу надсилають інформацію в SCADA-систему. Вся система пов’язує між собою мікропроцесорні пристрої і збирає дані з кожного окремого приєднання. Завдяки цьому черговий персонал бачить, як працює обладнання, прямо в реальному часі через SCADA.

Додаткова необхідна можливість, що можна дистанційно керувати комутаційними апаратами, наприклад, вимикачами. Оскільки SCADA підключена до диспетчерського пункту через мережу (див. рис. 3.1), керувати вимикачами може і оператор на самій підстанції, і диспетчер із центрального пункту [48].

Рис. 3.1 – Технологічні шафи диспетчерського пункту SCADA-системи

Постійний зв’язок між диспетчерським пунктом і SCADA системами підстанцій дає диспетчеру повний контроль над діями оперативного персоналу під час перемикань на обладнанні. Це реально знижує ризик людських помилок. Диспетчер одразу бачить, якщо на якійсь підстанції виникає аварійна ситуація, і може швидко відреагувати. Завдяки цьому вдається уникати серйозних наслідків, зокрема несанкціонованих дій операторів [49].

Рис. 3.2 – Диспетчерський пульт із SCADA-системою

На рис. 3.2 видно типовий диспетчерський пульт із SCADA-системою. Для передачі даних між різними рівнями цієї системи використовують промислові протоколи зв’язку. Між контролерами й SCADA-серверами працює Modbus TCP/IP - це один із найпопулярніших протоколів у промисловій автоматизації. Для зв’язку диспетчерського пункту з підстанціями використовується протокол телемеханіки IEC 60870-5-104 - стандарт для енергетики. А обмін між SCADA-серверами й операторськими станціями відбувається через OPC DA або сучасніший OPC UA [50].

Тут важливо згадати, що всі ці протоколи у базовій версії не мають вбудованого шифрування. Через це виникають ризики для інформаційної безпеки. Мережу побудували із кількох ізольованих сегментів. Технологічна мережа (10.100.1.0/24) об’єднує польове обладнання - контролери, RTU, захисні термінали. Мережа рівня SCADA (10.100.2.0/24) включає сервери та операторські станції. Окремо виділили диспетчерську мережу (10.100.3.0/24) для зв’язку з віддаленим пунктом. Крім цього, на підприємстві працює корпоративна мережа (192.168.0.0/16) - тут знаходяться адміністративні комп’ютери з доступом до Інтернету. Зараз між корпоративною і технологічною мережами є маршрутизація, і це суперечить рекомендаціям щодо сегментації промислових мереж. За комутацію відповідають шість

промислових комутаторів Cisco IE-3400, які підтримують VLAN і пріоритизацію трафіку через QoS. Для зв'язку з диспетчерським пунктом стоїть маршрутизатор Cisco ISR 4331.

Підприємство ТОВ "ЕнергоСистема" за законом України "Про критичну інфраструктуру" входить до об'єктів критичної інфраструктури. Причини прості: воно забезпечує електропостачання понад 10 тисяч споживачів, загальна потужність підстанцій перевищує 100 МВА, а від безперервної роботи залежать критично важливі об'єкти соціальної сфери. Якщо SCADA-система вийде з ладу або стане жертвою атаки, наслідки будуть серйозними. Технічно це означає повну втрату контролю й моніторингу обладнання потужністю 180 МВА. Через збій у роботі захисту можна втратити дороге електрообладнання - збитки від одного інциденту сягнуть 15-20 мільйонів гривень. Для людей це означає вимкнення світла для 45 тисяч осіб. Особливо небезпечно це взимку - без опалення і світла виникає пряма загроза життю. Дві лікарні, вісім шкіл, водоканал - усе це зупиниться. Промислові підприємства теж залишаться без струму й припинять роботу, а економічні втрати за добу простою перевищать 50 мільйонів гривень. З точки зору національної безпеки, компрометація такої системи може стати стартом для атак на інші об'єкти енергетики України. В умовах гібридної війни - підтверджено досвідом кібератак на українську енергетику у 2015-2016 роках.

На підприємстві вже зробили кілька базових кроків для захисту інформації. На всіх комп'ютерах і серверах стоїть антивірус McAfee Application Control, який підходить саме для промислових систем. Доступ до SCADA-системи захищений паролями, але все ще використовують тільки локальні акаунти - централізованого управління немає. Всі події система записує у стандартні журнали Windows. Серверна кімната закрита на електронні замки, всередину потрапляють лише ті, у кого є картка.

З організаційної сторони тут є інструкції для роботи зі SCADA, ведеться паперовий журнал дій персоналу. Хто має доступ до серверної - вирішує і затверджує керівництво.

Але коли починаєш розбиратись глибше, одразу видно, що системі бракує захисту. По-перше, мережу ніяк не сегментували: технологічна мережа пов’язана з корпоративною, а та - просто вихід в інтернет. Це прямий шлях для зовнішньої атаки.

Ще одна проблема - відсутність двофакторної автентифікації: користувачі заходять лише по паролю. Немає і систем виявлення вторгнень, які б могли хоча б попередити про підозрілу активність. Промислові протоколи, такі як Modbus чи IEC 104, працюють без шифрування - все йде відкритим текстом. Логи з різних систем не збирають і не аналізують разом, тому помітити інциденти непросто. Формальної політики інформаційної безпеки та плану дій у випадку кібератаки теж немає.

Резервні копії SCADA - конфігурацій роблять, але не регулярно. Оновлення безпеки на операційних системах встановлюють із запізненням - бояться, що нові патчі щось зламають у роботі SCADA. Персонал ніколи не проходив спеціальне навчання з кібербезпеки для промислових систем.

SCADA-система ТОВ "ЕнергоСистема" - це серце всієї критичної інфраструктури. Від її роботи залежить і стабільність виробництва, і енергопостачання для людей та соціальних об’єктів. Але через відкриті протоколи без шифрування, проблеми з сегментацією і автентифікацією, а також відсутність сучасних систем для виявлення атак, система залишається дуже вразливою. Якщо хтось скомпрометує або знищить SCADA, це не просто зупинка енергопостачання для тисяч людей - наслідки будуть і економічні, і соціальні, і технологічні.

Тому інформаційна безпека SCADA - це завдання номер один для підприємства. Без якісної оцінки ризиків і комплексного захисту енергосистема під загрозою. Всі ці недоліки роблять систему легкою мішенню для атак, тому потрібні чіткі, продумані рекомендації для посилення безпеки критичної інфраструктури.

3.2 Аналіз загроз та вразливостей інформаційної безпеки SCADA-системи

3.2.1 Сучасний стан безпеки SCADA-систем та історичні приклади атак

Компанія Positive Technologies провела дослідження безпеки автоматизованих систем управління технологічними процесами й показала, що ситуація у промисловій кібербезпеці справді критична [51]. Виявилося, що кожну п’яту вразливість в АСУ ТП усувають більше місяця. Половина знайдених вразливостей дозволяє зловмисникам запускати свій код на цільових системах, а для 35% уже існують публічно доступні експлойти. Найбільше серед усіх проблем - це саме SCADA-вразливості.

Якщо подивитися на архітектуру SCADA-системи ТОВ "ЕнергоСистема" (про неї йшлося в підрозділі 3.1), то помітно, що маршрутизація між корпоративною мережею, яка має доступ до Інтернету, і технологічною мережею реально відкриває двері для зовнішніх атак. А ще використання незашифрованих протоколів, таких як Modbus TCP/IP і IEC 60870-5-104, тільки додає ризиків і підвищує шанс успішної атаки.

Перша гучна кібератака на SCADA-системи - це історія з іранською ядерною програмою у 2010 році. Тоді комп’ютерний черв’як Stuxnet проник у ізольовану мережу через звичайні USB-носії й порушив роботу центрифуг для збагачення урану [52]. Цей випадок показав, що через кібератаки можна знищувати справжнє промислове обладнання. Саме ця атака змінила ставлення до загроз для АСУ ТП і стала поворотним моментом у всій сфері.

Атаки на енергетичну інфраструктуру України дійсно варто виділити окремо, особливо тому, що саме тут і знаходиться об’єкт дослідження. У грудні 2015 року сталася атака BlackEnergy на енергетичні SCADA-системи. Тоді понад 230 тисяч людей у трьох областях залишилися без світла. Хакери отримали віддалений доступ до робочих станцій операторів і просто вручну вимкнули автоматичні вимикачі на підстанціях [53].

А вже в грудні 2016 року Україна зіткнулася з новою, ще складнішою атакою - цього разу зі шкідливим ПЗ Industroyer (його ще називають CrashOverride) [54]. Цю програму створили спеціально для атак на енергетичні SCADA-системи. Вона використовує промислові протоколи - IEC 60870-5-104, IEC 61850, OPC DA - для автоматизованого управління розподільчими мережами. Industroyer може напряму взаємодіяти з обладнанням підстанцій. Через це вона особливо небезпечна для систем, подібних до ТОВ "ЕнергоСистема", де якраз працює протокол IEC 60870-5-104 [55].

Починаючи з 2010 року, методи атак на SCADA-системи сильно змінилися. Шкідливі програми тепер пишуть під конкретні АСУ ТП, самі атаки стали продуманішими, а способи доставки вірусів і маскування присутності у системі - все більш витонченими.

3.2.2 Виявлені вразливості SCADA-системи об'єкта дослідження

Після детального аналізу SCADA-системи ТОВ "ЕнергоСистема", який ми провели в розділі 3.1, стало очевидно, що тут є цілий список критичних вразливостей, і вони реально загрожують безпеці цього об’єкта критичної інфраструктури.

Головна проблема - це побудова самої мережі. Між корпоративною мережею з доступом до Інтернету і технологічною мережею SCADA-системи налаштована маршрутизація. Іншими словами, ці дві мережі можна пов’язати між собою, і це грубо порушує базовий принцип ізоляції промислових систем керування, який чітко прописаний у стандарті IEC 62443 [56].

Фактично, це відкриває “пряму дорогу” для кібератак ззовні. Згадаймо атаку BlackEnergy у 2015 році - тоді зловмисники теж зайшли саме через корпоративну мережу. Тому ця вразливість зараз - найбільша загроза для підприємства.

Ще одна серйозна проблема - промислові протоколи зв’язку тут не шифруються взагалі. Modbus TCP/IP і IEC 60870-5-104 працюють у відкритому вигляді. Це означає, що будь-хто, хто добереться до мережі, може перехоплювати всі команди, зокрема ті, що відключають вимикачі. А якщо хакер отримав доступ - він не лише читає трафік, а й може підроблювати або навіть створювати власні шкідливі команди. Атака Industroyer чітко показала, як через нешифровані протоколи можна взяти під контроль обладнання підстанцій.

Захист паролями тут теж залишає бажати кращого. Система використовує лише локальні облікові записи з паролями, і зовсім немає двофакторної аутентифікації. Через це зловмисники можуть легко підібрати пароль силою або вкрасти дані через фішинг чи соціальну інженерію. Особливо це небезпечно, враховуючи, що керування обладнанням здійснюється дистанційно з диспетчерського пункту, який знаходиться за 25 кілометрів від підстанцій.

На підприємстві взагалі немає систем виявлення чи запобігання вторгнень. Це дозволяє хакерам діяти непомічено тижнями або місяцями. Логи з різних частин системи ніхто не збирає й не аналізує централізовано - отже, виявити підозрілу активність чи інциденти майже нереально. Без моніторингу мережевої активності система фактично “сліпа” до атак.

Ще один слабкий пункт - оновлення безпеки операційних систем. Патчі для Windows Server 2019 і Windows 10 Pro встановлюють із великим запізненням, бо персонал боїться, що після оновлення щось перестане працювати в SCADA-програмах. В результаті система відкрито вразлива до

експлойтів, для яких давно існують готові інструменти атаки.

Більше того, тут немає жодного тестового стенду, де можна було б спокійно перевірити оновлення перед тим, як встановлювати їх на робочі системи.

Серйозно підводить також рівень підготовки персоналу. Працівники жодного разу не проходили навчання з кібербезпеки промислових систем, тому допускають помилки в налаштуванні захисту, неправильно розподіляють права доступу і не вміють вчасно розпізнати ознаки атаки. Вони легко стають жертвами фішингу та інших прийомів соціальної інженерії, бо просто не знають, як їх розпізнати. Додайте до цього ще відсутність чіткої політики інформаційної безпеки й плану реагування на кіберінциденти - і стає зрозуміло, що у разі реальної атаки персонал не має жодних чітких інструкцій, що робити далі.

3.2.3 Оцінка ризиків інформаційної безпеки

Щоб розкласти все по поличках і зрозуміти, наскільки серйозні загрози, ми провели оцінку ризиків за методологією NIST SP 800-82 [57]. Кожну загрозу розглядали з двох боків: наскільки ймовірно, що вона справді станеться, і який вплив матиме на працездатність системи. Ймовірність визначали, беручи до уваги, чи є у системі відповідні вразливості і наскільки ця загроза взагалі актуальна для енергетики України. А вплив оцінювали, виходячи з того, що може трапитися з населенням, економікою чи навіть національною безпекою, якщо загроза реалізується. Все це зібрано у таблицю 3.1.

Таб. 3.1 – Оцінка інформаційних ризиків SCADA-системи

№	Загроза	Ймовірність	Вплив	Рівень ризику
1	Зовнішня кібератака через незахищене з'єднання мереж (тип BlackEnergy)	Висока	Критичний	Критичний
2	Перехоплення та підміна команд управління через незашифровані протоколи	Середня	Критичний	Високий
3	Несанкціонований доступ через компрометацію паролів	Середня	Високий	Високий
4	DoS-атака на SCADA-сервери з метою порушення управління	Середня	Високий	Високий
5	Експлуатація невиправлених вразливостей операційних систем	Середня	Високий	Високий
6	Успішний фішинг персоналу з подальшим	Середня	Середній	Середній

	проникненням в систему			
7	Внесення шкідливого програмного забезпечення через USB-носії	Низька	Високий	Середній

Як, видно, з аналізу, у SCADA-системи ТОВ "ЕнергоСистема" є один критичний і чотири високих ризики. Найбільша проблема - це зовнішня кібератака через незахищене з’єднання між корпоративною і технологічною мережами. Ймовірність такого сценарію - висока, особливо зараз, коли кібератаки на енергетичну інфраструктуру України стали майже буденністю через гібридну війну. Досвід BlackEnergy та Industroyer у 2015-2016 роках добре показав, що це не вигадки, а цілком реальна загроза, яка вже ставала причиною серйозних інцидентів. Якщо таку атаку реалізують, наслідки можуть бути катастрофічними, такі як: повна втрата контролю над системою, несанкціоноване відключення світла для 45 тисяч споживачів і економічні втрати понад 50 мільйонів гривень за добу простою.

Високий рівень ризику мають й інші загрози: перехоплення команд через незашифровані протоколи, несанкціонований доступ через слабкі паролі, DoS-атаки на критичні сервери й експлуатація невиправлених вразливостей операційних систем. Кожна з цих проблем може спричинити серйозні збої в роботі системи або стати стартовим майданчиком для ще складніших атак. А якщо кілька таких вразливостей співпадуть - ризик для об’єкта критичної інфраструктури зростає ще більше. Середній рівень ризику мають загрози, пов’язані із соціальною інженерією та шкідливим ПЗ на знімних носіях. Їх ймовірність нижча завдяки базовим заходам контролю, але якщо вони спрацюють - наслідки все одно можуть бути суттєвими.

Загалом, ми отримали доволі тривожну картину того, що SCADA-система ТОВ "ЕнергоСистема" вразлива до багатьох сучасних кіберзагроз.

Незашифровані протоколи, відсутність поділу мережі, слабка автентифікація, брак систем виявлення вторгнень і недостатня підготовка персоналу - усе це відкриває багато дверей для потенційних зловмисників. Через такі прогалини система стає легкою мішенню як для простих, так і для складних цільових атак, навіть на державному рівні.

З огляду на те, наскільки ця система важлива для енергопостачання регіону і які можуть бути наслідки навіть однієї успішної атаки, потрібно якомога швидше впровадити комплексні заходи для посилення інформаційної безпеки. Далі у наступному підрозділі розглянемо детальні рекомендації для цього.

3.3 Рекомендації щодо забезпечення інформаційної безпеки

Проведений аналіз SCADA-системи ТОВ "ЕнергоСистема" виявив ряд серйозних проблем з безпекою, які потребують негайного вирішення. На основі результатів оцінки ризиків та з урахуванням міжнародних стандартів IEC 62443 і NIST SP 800-82 розроблено комплекс практичних рекомендацій для підвищення захищеності об'єкта критичної інфраструктури.

Перше, що треба зробити - відокремити мережі. Зараз промислова мережа SCADA напряму під’єднана до офісної, яка виходить в Інтернет. Через це вся система під загрозою: якщо зловмисники потраплять в офісну мережу, їм не важко дістатися і до управління підстанціями. Уже були такі ситуації - у 2015-2016 роках хакери в Україні саме так і проникали в SCADA-системи енергетики. Щоб таких речей не траплялося, промислову мережу треба фізично ізолювати від офісної й поставити між ними спеціальний міжмережевий екран. Він контролює, які дані можна передавати між мережами.

За стандартом IEC 62443 промислову мережу краще розбити на кілька зон безпеки з різним рівнем доступу. Найнижча зона - це датчики та обладнання підстанцій. Вище - контролери, що збирають дані. Ще вище - SCADA-сервери та робочі місця операторів. Між кожною зоною треба ставити захист, щоб навіть якщо хтось прорветься в одну, далі пройти не вийде. Для обміну даними між промисловою і офісною мережами треба створити буферну зону з проміжними серверами. Вони приймають дані зі SCADA і передають їх в офісну систему для звітів, але не дають можливості надсилати команди назад.

Найкраще поставити однонаправлені шлюзи - це пристрої, які фізично пропускають дані лише в один бік. Навіть якщо офісну мережу зламають, хакер просто не зможе відправити команди в SCADA.

Ще один момент - канал зв’язку між підстанціями та диспетчерським центром. Навіть якщо використовується окреме оптоволокно, його все одно можна пошкодити чи підключити підслуховуюче обладнання.

Тут весь трафік треба шифрувати через VPN із сильним шифруванням AES-256. Всередині промислової мережі кожну підстанцію краще винести в окремий віртуальний сегмент за допомогою VLAN - це підтримують ті ж Cisco IE-3400, які вже стоять. Якщо атакують одну підстанцію, це допоможе утримати зловмисників і не дасть їм перейти далі.

Друга критична проблема - це передача всіх даних у відкритому вигляді. Зараз команди керування, навіть ті, що вимикають обладнання, йдуть без жодного шифрування. Якщо хтось отримує доступ до мережі, він легко читає весь трафік і може підробити команди. Саме так працював Industroyer у 2016 році: він перехоплював протокол IEC 104 і відправляв свої власні команди на обладнання.

Рекомендується впровадити шифрування всіх каналів зв’язку. Для протоколу IEC 60870-5-104, який зв’язує диспетчерські пункти з підстанціями, існує стандартне розширення - IEC 62351 [58]. Воно додає шифрування і

автентифікацію. Треба просто оновити програмне забезпечення SCADA-серверів і Siemens-контролерів, щоб вони це підтримували.

А якщо говорити про Modbus, який передає дані між контролерами та серверами, тут усе простіше: можна налаштувати VPN-тунелі, і весь трафік піде через захищений канал. Протокол OPC DA, що працює між серверами та операторами, взагалі застарів і ніякого захисту не має. Його треба міняти на сучасний OPC UA - він вже має вбудоване шифрування й дозволяє керувати, хто і що може бачити.

Aveva System Platform вже підтримує OPC UA, тож це питання налаштування, а не заміни всієї системи [59].

Міжмережеві екрани між зонами мають робити більше, ніж просто дозволяти чи блокувати з'єднання. Вони повинні перевіряти зміст кожного повідомлення. Якщо хтось намагається відправити команду на вимкнення обладнання з комп'ютера, який не має на це права, екран має це заблокувати й записати спробу в журнал.

Третій важливий крок - посилити захист під час входу в систему. Зараз користувачі заходять у SCADA просто за паролем, який легко вкрасти через фішинг, підібрати або навіть підгледіти. Потрібна двофакторна автентифікація: крім пароля, ще один рівень підтвердження особи. Найкраще працюють персональні смарт-карти з PIN-кодом. Оператор перед початком роботи вставляє карту в зчитувач, вводить PIN і тільки тоді потрапляє в систему. Коли зміна закінчується, він забирає карту, і система сама його виходить. Це ще й вирішує проблему незаблокованих робочих місць - ніхто не залишиться в системі випадково.

Якщо потрібен віддалений доступ для техпідтримки, краще використовувати апаратні токени або генератори одноразових паролів. Підключатись до SCADA через Інтернет з будь-якої адреси - це табу. Доступ можливий тільки з чітко визначених місць і лише через захищений VPN.

Ще одна проблема - на кожній операторській станції свої локальні облікові записи. Через це важко зрозуміти, хто насправді працював у системі. Тут допоможе централізована система управління користувачами на окремому сервері Active Directory для промислової мережі, відокремленому від офісної. До цього домену підключаються всі користувачі, комп'ютери і сервери SCADA. В результаті можна з одного місця блокувати акаунти звільнених працівників, встановити єдину політику паролів (мінімум 12 символів, складність, обов'язкова зміна кожні 90 днів) і чітко бачити в журналах, хто, коли й з якої станції заходив у систему.

Далі важливо правильно розподілити права доступу. Принцип простий - кожному лише те, що йому реально потрібно. Зараз часто всім дають повні права "на всякий випадок", але це ризиковано. Треба створити різні ролі з чіткими межами. "Оператор-монітор" лише дивиться інформацію, без керування обладнанням - це для новачків або персоналу моніторингу. "Оператор підстанції" може керувати тільки своєю підстанцією, а іншими - ні.

"Старший диспетчер" керує всіма підстанціями прямо з диспетчерської, але не може змінювати налаштування системи. Інженер АСУ ТП займається саме цими налаштуваннями - він змінює параметри, але не втручається в роботу обладнання під час звичайної експлуатації. Адміністратор безпеки управляє користувачами, налаштовує політики безпеки та перевіряє журнали подій.

Коли мова про щось справді критичне, наприклад, вимкнення головного вимикача чи зміну параметрів релейного захисту, все працює за принципом "чотирьох очей". Тобто команда виконується тільки після підтвердження іншою людиною, яка має відповідні права. Ще обов'язково - якщо три-п'ять разів неправильно ввели пароль, акаунт автоматично блокується. А якщо на робочій станції 15 хвилин нічого не робити, система сама викидає користувача з сеансу.

Четвертий крок це - впровадження систем для виявлення атак. Зараз у мережі взагалі немає механізмів, які б стежили за підозрілою активністю. Якщо хакер проникне всередину, він може залишатися непоміченим тижнями, а то й місяцями. Тут потрібні спеціалізовані системи виявлення вторгнень, розраховані саме на промислові мережі. Звичайний офісний захист не підходить: він не розбирається в промислових протоколах, часто помиляється й заважає роботі.

Для таких задач потрібні рішення на кшталт Nozomi Networks Guardian, Claroty або Dragos Platform. Вони “розуміють” специфіку Modbus, IEC 104 та інших промислових протоколів. Такі системи підключаються до мережі лише для прослуховування - вони копіюють увесь трафік, аналізують його, але не втручаються у роботу обладнання. Система вивчає, як мережа поводиться зазвичай, і помічає підозрілі відхилення. Наприклад, якщо контролер раптом починає сканувати мережу або відправляє дані на дивні адреси - це вже сигнал. Або якщо хтось надсилає команду на відключення вимикача з комп’ютера, який до цього цим ніколи не займався, - треба перевірити. Окрім цього, система автоматично знаходить усі пристрої в мережі й створює карту обладнання. Це допомагає швидко побачити несанкціоновані підключення.

Журнали подій зі всіх систем потрібно зібрати в одному місці - на сервері SIEM. Вона стежить за безпекою у всій мережі. SIEM збирає логи з операційних систем (хто заходив, що міняв), з SCADA (які команди виконували, які були аварії), з контролерів (які програми запускали), з мережевого обладнання (хто підключався), а ще з антивірусів і міжмережевих екранів. Вся ця інформація потрапляє в одну купу, і система аналізує її разом. Саме так можна помітити складні атаки, які неможливо вловити, якщо дивитися лише на одну подію. Ось приклад. SIEM помічає: спочатку багато невдалих спроб входу (комусь не дає спокою чужий пароль), потім раптом вдалий вхід у дивний час, далі цей самий користувач одночасно з’являється на різних комп’ютерах (скоріше за все, акаунт вже вкрали), і після цього - зміни в

конфігурації обладнання. Кожна окрема подія виглядає цілком нормально, але разом вони одразу сигналять: тут щось не так, це атака.

Щоб усе це працювало як треба, потрібні люди, які слідкують за подіями цілодобово. Якщо підприємство невелике, цю роботу часто віддають на аутсорсинг компанії, яка розуміється на промисловій безпеці. Коли система ловить щось серйозне, вона миттєво сповіщає відповідальних - SMS, email, а інколи навіть звуковим сигналом. Ще один важливий елемент - система управління вразливостями. Раз на квартал потрібно проводити сканування усіх систем спеціальними сканерами для промислових мереж, які шукають відомі слабкі місця. Головне, щоб ці сканери працювали пасивно і не могли випадково зупинити виробничий процес.

П'ятий напрямок - це організація правильного процесу встановлення оновлень безпеки. Зараз із цим справжня біда: оновлення ставлять із великим запізненням, бо персонал боїться, що нові патчі зламають SCADA. У підсумку система лишається беззахисною перед відомими атаками. Вихід простий: треба зробити тестовий стенд, який максимально повторює робочу систему. Там має бути сервер з тією ж конфігурацією, тестові операторські станції, хоча б один контролер кожного типу та мережеве обладнання.

Оновлення спочатку ставлять на стенд, тестують щонайменше 72 години. Дивляться, чи все працює як треба, чи не виникає конфліктів, чи не “просідає” швидкість.

Ще одне важливе правило - чіткий графік оновлень залежно від їхньої критичності. Якщо це критичне оновлення безпеки, яке закриває дірку, що її вже використовують хакери, його ставлять протягом тижня після успішного тесту. Важливі оновлення - за 30 днів. Некритичні - під час планового обслуговування раз на квартал. Ставити їх треба у вихідні або під час технологічного вікна, коли можна коротко зупинити систему, не зачепивши споживачів. Для керування Windows-оновленнями найкраще підходить

Windows Server Update Services. Він дозволяє централізовано обирати, які апдейти ставити, які відкласти, і автоматично встановлювати затверджені за розкладом. Дуже важливо розмістити цей сервер саме в промисловій мережі, а не в офісній.

З контролерами й RTU треба бути ще обережнішими. Прошивки оновлюють тільки у двох випадках: якщо знайшли критичну діру, яку реально можна використати віддалено, або якщо сам виробник наполягає на оновленні через серйозну помилку. Перед цим завжди роблять повну резервну копію - без цього ніхто нічого не чіпає, щоб у разі чого швидко все повернути, як було. Оновлення проводить тільки той інженер, який реально знає це обладнання, щоб не наробити біди.

Антивірус McAfee Application Control стоїть на всіх комп'ютерах і налаштований у режимі білого списку: запускається лише те, що внесли до списку довіри, решта блокується [60]. Це набагато ефективніше за звичайний антивірус, особливо коли маєш справу з новими чи невідомими загрозами.

Ще один важливий напрямок - резервне копіювання. Зараз із цим повний хаос: копії роблять коли як, а це ризик втратити все у випадку атаки чи серйозного збою - і дані, і налаштування. Потрібна чітка, автоматизована система резервного копіювання за принципом 3-2-1: три копії даних, на двох різних типах носіїв, і одна копія - поза межами об'єкта. Щодня в автоматичному режимі треба зберігати налаштування SCADA-серверів, базу історичних даних, всі програми й конфігурації контролерів та RTU, налаштування мережевого обладнання, облікові записи користувачів, політики безпеки, і журнали подій за останній місяць з усіх систем. Першу копію зберігаємо на окремому сервері резервного копіювання в серверній головної підстанції. Другу - на зовнішніх жорстких дисках, які лежать у сейфі на іншій підстанції. Якщо на головній щось трапиться, друга копія залишиться. Третю копію шифруємо й відправляємо у зовнішнє сховище за межами об'єкта. Важливо не просто робити ці копії, а й перевіряти, чи реально можна відновити

систему. Раз на квартал на тестовому стенді тестуємо повне відновлення - дивимось, скільки часу йде, чи є проблеми. Усі носії шифруємо за допомогою AES-256 - якщо щось вкрадуть чи загубиться, дані залишаться захищеними.

Сьомим напрямком є навчання персоналу. Люди - це одночасно найважливіший елемент захисту і найслабша ланка у системі безпеки. Співробітник, який не розуміє, чим загрожують фішингові листи чи заражені флешки, легко може відкрити вірус або випадково передати пароль стороннім. Тому регулярна програма навчання з кібербезпеки потрібна всім - без винятків.

Оператори й диспетчери проходять базовий восьмигодинний курс. Їх навчають помічати фішингові листи, підозрілі повідомлення, правильно працювати з паролями, користуватися двофакторною автентифікацією, діяти при підозрілій активності, дотримуватись правил роботи з USB-накопичувачами та основам соціальної інженерії.

Інженери та адміністратори йдуть далі - у них 24-годинний розширений курс. Тут уже йдеться про специфіку атак на промислові системи, безпечне налаштування SCADA-обладнання, аналіз журналів подій, пошук слідів атак, управління оновленнями та вразливостями.

Також вивчають, як правильно організувати резервне копіювання й відновлення.

Керівники проходять короткий брифінг. Їм пояснюють кіберризики для критичної інфраструктури, можливі фінансові втрати, юридичну відповідальність і чому треба вкладати в безпеку. Без цього складно очікувати, що керівництво серйозно ставитиметься до проблеми й виділятиме ресурси.

Навчання відбувається щороку для всіх. Кожні три місяці - короткі нагадування. Після курсів усі здають тест, щоб перевірити, що засвоїли матеріал. Не зайвим буде й час від часу організовувати симуляції фішингових атак - розсилати тестові листи й дивитися, хто їх відкриє. Це не для покарання, а щоб зрозуміти, кому потрібно додаткове навчання.

Восьмим напрямком є впровадження організаційних заходів. Крім технічних рішень необхідні формальні документи та процедури. Потрібна - Політика інформаційної безпеки. Це офіційний документ, який підписує керівництво. У ньому мають бути прописані правила й вимоги для всіх співробітників. Тут і цілі компанії у сфері безпеки, і перелік відповідальних, і правила доступу до систем, і робота з паролями, і як користуватися мережею, інтернетом, мобільними пристроями, USB-носіями. Окремо - що робити у разі інциденту, і хто відповідає за порушення. Далі - План реагування на кіберінциденти. Просто і зрозуміло: що робити, якщо сталася атака. План пояснює, як розпізнати атаку, кому одразу повідомити, як ізолювати скомпрометовану систему (важливо: від мережі відключити, але не вимикати, бо там можуть бути докази), як зберегти ці докази, коли й як відновлювати роботу, і як інформувати регуляторів та поліцію. Всі, хто має стосунок до безпеки, повинні знати цей план. Щороку потрібно проводити навчання - моделюється атака, і працівники відпрацьовують свої дії. Після кожного реального інциденту план переглядають і оновлюють.

Ще один важливий момент це - процедура управління доступом. Коли приходить новий співробітник, йому створюють обліковий запис із потрібними правами.

Перевівся на іншу посаду - права змінюють. Звільнився - в день звільнення блокують обліковий запис, повертають смарт-карти й токени. Раз на квартал перевіряють, чи всі активні облікові записи справді належать працівникам, які зараз працюють. Потрібно також чітко визначити, хто у вас відповідає за інформаційну безпеку АСУ ТП. Це має бути конкретна людина, бажано на рівні заступника директора. Вона координує всі заходи, контролює дотримання політики, приймає рішення у критичних ситуаціях, звітує керівництву. І нарешті, потрібен контракт із постачальником SCADA або спеціалізованою компанією на технічну підтримку з питань безпеки. Вони своєчасно повідомляють про нові вразливості, допомагають з оновленнями,

консультують щодо безпечної конфігурації, а ще допомагають розслідувати інциденти.

Дев'ятим напрямком є посилення фізичної безпеки. Кібербезпека неефективна без фізичної безпеки - якщо зловмисник може фізично потрапити до серверної, він обійде всі цифрові захисти. Зараз є електронні замки з картками, але можна посилити. Рекомендується встановити відеокамери з записом біля входу в серверну та біля шаф з обладнанням на підстанціях. Запис зберігається мінімум 30 днів. Додати біометричну автентифікацію для особливо критичних приміщень. Вести журнал відвідувань серверної - хто, коли, навіщо заходив, хто дозволив. USB-порти на всіх операторських станціях та SCADA-серверах варто фізично заблокувати, залишивши активними тільки там, де це справді потрібно. Це запобігає підключенню несанкціонованих флешок з вірусами. Для передачі файлів використовувати тільки службові перевірені USB-носії або мережеві папки. Всі критичні шафи з обладнанням мають бути замкнені, ключі зберігаються у відповідальної особи.

Зрозуміло, що одразу всі ці рекомендації не впровадиш - це справа не одного дня. Тут потрібні чіткий план і ресурси. Варто діяти поетапно.

На першому етапі, протягом перших трьох місяців, найважливіші кроки мають отримати критичний пріоритет: фізично відокремлюємо промислову і офісну мережі та ставимо міжмережеві екрани, вводимо двофакторну автентифікацію для всіх, створюємо централізовану систему управління користувачами, налаштовуємо антивірус на режим білого списку, запускаємо щоденне автоматичне резервне копіювання, організовуємо базове навчання персоналу з кібербезпеки, розробляємо і затверджуємо Політику інформаційної безпеки.

Другий етап – це від 4 до 6 місяців. Тут фокус на впровадженні шифрування для протоколів зв'язку, встановленні систем виявлення вторгнень, створенні DMZ і однонаправлених шлюзів, сегментації мережі через VLAN,

розробці плану реагування на кіберінциденти та створенні тестового стенду.

Третій етап триває з сьомого по дванадцятий місяць. На цьому рівні впроваджуємо SIEM-систему для збору логів, налаштовуємо систему управління оновленнями, впроваджуємо систему управління вразливостями, організовуємо SOC або підписуємо контракт на аутсорсинг, проводимо розширене навчання для інженерів і адміністраторів, а також перше тренування реагування на інциденти.

Четвертий етап - це вже другий рік. Тут у хід йдуть довгострокові заходи: щорічний аудит безпеки, щоквартальні сканування вразливостей, щорічне перенавчання персоналу, оновлення обладнання, що вийшло з підтримки, і постійне вдосконалення процесів на основі досвіду.

Звісно, на все це потрібні чималі інвестиції. Але якщо порівняти витрати на захист із потенційними збитками від успішної кібератаки, вони виглядають більш ніж виправдано. Орієнтовно, на обладнання й програмне забезпечення потрібно разово 4-6 мільйонів гривень, а щороку на ліцензії, підтримку, навчання й послуги - ще 2-3 мільйони. Для порівняння: одна доба простою системи - це вже понад 50 мільйонів гривень втрат, і це ще без урахування можливого ушкодження обладнання на 15-20 мільйонів і репутаційних втрат.

Таким чином, інвестиції в безпеку окупляться навіть якщо вони запобіжать лише одному серйозному інциденту за кілька років.

3.4 Висновки до третього розділу

У третьому розділі я детально дослідив, як працює система інформаційної безпеки SCADA на об’єкті критичної енергетичної інфраструктури, і підготував практичні поради, які реально підвищують її захищеність.

Аналіз обраного об’єкта показав, що SCADA-система ТОВ "ЕнергоСистема" - ключовий елемент для стабільного електропостачання в регіоні. Вона працює цілодобово, і вимоги до її надійності дуже високі.

Проблеми встановлено - система використовує незахищені промислові протоколи, а сегментація мережі слабка.

Я вивчив основні загрози та вразливості і побачив, що ситуація з інформаційною безпекою критична. Серед головних проблем: немає чіткої межі між промисловою та корпоративною мережами, передача даних відбувається нешифрованими каналами, механізми автентифікації користувачів слабкі, систем для виявлення вторгнень бракує, а персонал майже не має підготовки з кібербезпеки. Оцінка ризиків за методологією NIST SP 800-82 підтвердила, що ризики для безперервної роботи об’єкта високі та критичні.

Спираючись на результати аналізу, я склав перелік рекомендацій, які охоплюють технічні, організаційні й процедурні заходи. Серед них - перебудова мережевої архітектури, впровадження криптографічного захисту, посилення автентифікації та контролю доступу, створення систем моніторингу безпеки, впорядкування процесів управління оновленнями й вразливостями, автоматизація резервного копіювання, системне навчання персоналу й розробка потрібних організаційних документів.

Я пропоную впроваджувати ці рекомендації поетапно, з чітким визначенням пріоритетів і строків. Також пояснив, чому вкладати гроші у безпеку вигідно тому, що витрати на захист значно менші, ніж можливі збитки від кібератаки.

Якщо ці поради втілити в життя, ризики впадуть до прийнятного рівня, система відповідатиме міжнародним стандартам і національним вимогам, а енергетична інфраструктура стане стійкішою до сучасних кіберзагроз. Це напряму вплине на стабільність електропостачання для споживачів.

ВИСНОВКИ

У цій кваліфікаційній роботі я взявся за питання інформаційної безпеки автоматизованих систем управління на об’єктах критичної інфраструктури України. На основі дослідження, я підготував цілий комплекс практичних порад, які реально допомагають підвищити їх захищеність перед сучасними кіберзагрозами.

По-перше, проведено системний аналіз теоретичних і нормативно-правових основ захисту об'єктів критичної інфраструктури, який підтвердив актуальність дослідження. За 2024 рік кількість кібератак на об’єкти критичної інфраструктури у світі зросла на 87%, а в Україні - на 48%. Наявна нормативна база досі виглядає розірваною й потребує доопрацювання. Через це комплексний підхід до захисту АСУ стає вже не просто рекомендацією, а гострою необхідністю.

По-друге, досліджено міжнародний досвід побезпечення інформаційної безпеки критичних систем у США, країнах ЄС та інших державах, що дозволило визначити найефективніші підходи до побудови систем кіберзахисту. Стверджуємо, що застосування стандартів IEC 62443, ISO/IEC 27001, NIST Cybersecurity Framework є обов'язковим для створення надійної системи захисту, тому що ці стандарти містять перевірені практикою механізми управління ризиками та забезпечення безперервності функціонування критичних об'єктів.

По-третє, розроблено алгоритм визначення актуальності загроз безпеці інформації на критично важливих об'єктах, який базується на комплексній оцінці можливостей порушників, вразливостей систем, сприятливих умов реалізації загроз та потенційних наслідків. Пропоную використовувати цей підхід для регулярної перевірки захищеності АСУ - так можна вчасно побачити нові загрози і швидко реагувати.

По-четверте, створено методику підвищення рівня інформаційної безпеки автоматизованих систем управління, яка включає п'ять функцій (ідентифікація, захист, виявлення, реагування, відновлення), чотири рівні реалізації заходів захисту та профілі рівня захищеності. Стверджуємо, що запропонована методика дозволяє підприємствам створити дорожню карту зниження ризиків, узгоджену з бізнес-цілями та ресурсами, тому що вона базується на міжнародних стандартах і враховує специфіку промислових систем управління.

По п’яте, проведено детальний аналіз SCADA-системи енергетичного об’єкта ТОВ "ЕнергоСистема". Виявив критичні вразливості, що немає сегментації між корпоративною та промисловою мережами, використання незашифрованих протоколів, слабка автентифікація, відсутність систем виявлення вторгнень, персонал недостатньо підготовлений. Оцінка ризиків за методологією NIST SP 800-82 підтвердила наявність одного критичного та чотирьох високих ризиків для безперервності функціонування об'єкта, на підставі чого обґрунтовано необхідність негайного впровадження комплексних заходів захисту.

По-шосте, розроблено комплекс практичних рекомендацій щодо забезпечення інформаційної безпеки досліджуваної SCADA-системи, який охоплює дев'ять напрямків: сегментацію та ізоляцію мереж, впровадження шифрування каналів зв'язку, посилення автентифікації та контролю доступу, створення систем моніторингу та виявлення загроз, організацію процесу оновлень безпеки, автоматизацію резервного копіювання, навчання персоналу, розробку організаційних документів та посилення фізичної безпеки. Пропонуємо впроваджувати ці рекомендації поетапно протягом дванадцяти місяців з чітким визначенням пріоритетів, тому що поетапний підхід дозволяє мінімізувати ризики порушення технологічних процесів та раціонально розподілити фінансові й людські ресурси.

По-сьоме, обґрунтовано економічну доцільність інвестицій у кібербезпеку критичної інфраструктури. Розраховано, що впровадження запропонованих заходів потребує разових інвестицій 4-6 мільйонів гривень та щорічних витрат 2-3 мільйони гривень, тоді як одна доба простою системи внаслідок кібератаки призводить до втрат понад 50 мільйонів гривень. Стверджуємо, що інвестиції в безпеку повністю виправдані та окупляться навіть у разі запобігання лише одному серйозному інциденту, на підставі чого рекомендуємо керівництву об'єктів критичної інфраструктури розглядати витрати на кібербезпеку як необхідну складову забезпечення безперервності бізнесу.

Результати дослідження мають практичне значення для підприємств енергетичної, транспортної, комунікаційної та оборонно-промислової галузей України і можуть бути використані при розробці, впровадженні та модернізації систем захисту інформації в автоматизованих системах управління на об'єктах критичної інфраструктури. Впровадження запропонованих рекомендацій дозволить підвищити стійкість критичної інфраструктури до сучасних кіберзагроз та забезпечити національну безпеку України в інформаційній сфері.

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global Threat Landscape Report 2025. Fortinet, 2025. URL: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf

2. Студентська наукова конференція «Безпека інформаційно-комунікаційних систем» (Київ: Київський столичний університет імені Бориса Грінченка, 24 листопада 2025 року).

URL: https://fitm.kubg.edu.ua/images/ФІТМ/2025/конференція_кб/Збірник_тез_конференції_Безпека_інформаційно_комунікаційних_систем.pdf

3. Крючкова Л., Складанний П., Ворохоб М. (2023). Передпроєктні рішення щодо побудови системи авторизації на основі концепції Zero Trust. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 226–242. https://doi.org/10.28925/2663-4023.2023.13.226242

4. Закон України «Про критичну інфраструктуру», від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20

5. Framework for Improving Critical Infrastructure Cybersecurity. NIST, 2018. URL: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

6. Постанова Кабінету Міністрів України «Про затвердження Порядку визнання об'єкта критичною інфраструктурою», від 09.10.2023 №1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

7. Інформація Державної служби спеціального зв'язку та захисту інформації України щодо стану кібербезпеки в Україні. 2024-2025. URL: https://cip.gov.ua/ua

8. Звіти CERT-UA (Computer Emergency Response Team of Ukraine) про

кіберінциденти. 2024-2025. URL: https://unn.ua/en/news/in-ukraine-about-15-cyberattacks-are-recorded-daily-since-the-beginning-of-the-year-state-special-communications-service

9. Analytical reports on ransomware attacks in financial sector. Cybersecurity & Infrastructure Security Agency (CISA), 2025. URL: https://www.fortinet.com/resources/cyberglossary/ransomware-statistics

10. Закон України «Про інформацію», від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

11. Закон України «Про Стратегію інформаційної безпеки», від 11.03.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

12. Закон України «Про Концепцію національної безпеки України», від 16.01.1997 № 3/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/3/97-%D0%B2%D1%80#Text

13. Закон України «Про основні засади забезпечення кібербезпеки України», від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

14. Закон України «Про Концепцію Національної програми інформатизації», від 04.02.1998 № 75/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80

15. Закон України «Про Воєнну доктрину України», від 15.06.2004 № 648/2004. URL: https://zakon.rada.gov.ua/laws/show/648/2004#Text

16. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

17. Закон України «Про основи національної безпеки України», від 19.06.2003 № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

18. Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації

України від 25.04.2008 № 51. URL: https://zakon.rada.gov.ua/laws/show/z0603-08/ed20110504

19. Указ Президента України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», від 10.01.2017 № 32/2017. URL: https://zakon.rada.gov.ua/laws/show/32/2017#Text

20. Указ Президента України «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», від 19.02.2016 № 47/2016. URL: https://zakon.rada.gov.ua/laws/show/n0014525-16#Text

21. Закон України «Про телекомунікації», від 18.11.2003 № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text

22. Закон України «Про Службу безпеки України», від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

23. Закон України «Про доступ до публічної інформації», від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

24. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 № 681/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/681-20#Text

25. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

26 Закон України «Про захист інформації в інформаційно-комунікаційних системах», від 31.05.2005 № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

27. НД ТЗІ 3.7-003-23. Порядок створення комплексних систем захисту інформації (КСЗІ). Чинний від 2023. Київ: Держспецзв'язок, 2023. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66099

28. НД ТЗІ 3.7-001-99. Порядок розроблення технічного завдання на створення

КСЗІ. Чинний від 1999. Київ: Держспецзв'язок, 1999. URL: https://tzi.com.ua/downloads/3.7-001-99.pdf

29. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management (Інформаційні технології – Методи захисту – Кодекс практики управління інформаційною безпекою). URL: https://www.iso.org/standard/39612.html

30. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements (Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги). URL: https://www.iso.org/ru/standard/27001

31. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls (Інформаційна безпека, кібербезпека та захист конфіденційності – Заходи інформаційної безпеки). URL: https://www.iso.org/ru/standard/75652.html

32. Розпорядження Кабінету Міністрів України «Про схвалення Концепції створення державної системи захисту критичної інфраструктури», від 06.12.2017 № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text

33. Presidential Decision Directive / NSC-63. Critical Infrastructure Protection. USA, 1998. URL: https://irp.fas.org/offdocs/pdd/pdd-63.htm

34. Critical National Infrastructure. National Protective Security Authority, UK.

URL:https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure?fireglass_rsn=true&utm_source

35. National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. Department of Homeland Security, USA, 2003. URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

36. Critical Infrastructure Project (CIP). Netherlands, 2003. URL: https://repository.wodc.nl/bitstream/handle/20.500.12832/2425/2960_Volledige_Tekst_tcm28421344.pdf

37. Concept of Critical Infrastructure Protection. Czech Republic. URL: https://www.researchgate.net/publication/228904583_Management_of_protection_of_Czech_Republic_critical_infrastructure_elements

38. Critical Infrastructure in Poland. URL: https://archiwum.rcb.gov.pl/en/critical-infrastructure/

39. Critical Infrastructure Protection in the Fight Against Terrorism. European Commission, 2004.

URL:https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF

40. В.А. Козачок Концептуальні засади створення комплексних систем захисту інформації в інформаційно- телекомунікаційних системах. К., ДУТ, Збірник науковихпраць «Зв'язок», 2014р., №3 (109), с. 8-13

41. Козачок В.А., Драпатий М.В. Аналіз технологій розслідування інцидентів безпеки на об'єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024, (2(26)). С. 374-391. ISSN 2663-4023

42. Conceptual model of information protection of critical information infrastructure objects of Ukraine. ResearchGate, 2022.

URL:https://www.researchgate.net/publication/357456211_Conceptual_model_of_information_protection_of_critical_information_infrastructure_objects_of_Ukraine

43. В.А. Козачок, Ю.Б. Коваленко Особливості побудови комплексних систем захисту інформації в розподілених корпоративних мережах. К., ДУТ, Збірник наукових праць «Сучасний захист інформації», 2015р., вип. 1, с. 41-47

44. Козачок В.А., Драпатий М.В. Аналіз технологій розслідування інцидентів безпеки на об’єктах критичної інфраструктури. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024, (2(26)). С. 374-391. ISSN 2663-4023

45. 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

46. Методика з підвищення рівня інформаційної безпеки критично важливих об'єктів інфраструктури. Cisco Systems, 2014. URL: https://www.cisco.com/c/dam/global/ru_ua/assets/pdf/cybersecurity-framework-021214-final_ua.pdf

47. Козачок В.А., Коршун Н.В., Мазур Н.П., Платоненко А.В., Складанний П.М. Прикладні аспекти аналізу та синтезу політик безпеки. (навчальний посібник). Київ: Вид-во КУБГ. 2021. 160 с.

48. Surface Mounted Automation Scada System. IndiaMART. URL: https://www.indiamart.com/proddetail/automation-scada-system-21098596897.html

49. 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

50. H. Hulak, et al., Dynamic model of guarantee capacity and cyber security management in the critical automated systems, in: 2nd International Conference on Conflict Management in Global Information Networks, vol. 3530 (2022) 102-111.

51. 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

52. 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

53. O. Mykhaylova, et al., Mobile Application as a Critical Infrastructure Cyberattack Surface, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 29–43.

54.'Industroyer' ICS Malware Linked to Ukraine Power Grid Attack. SecurityWeek, 2017. URL: https://www.securityweek.com/industroyer-ics-malware-linked-ukraine-power-grid-attack/

55. ДСТУ IEC 60870-5-104:2014. Пристрої та системи телемеханіки. Частина 5-104. Протоколи передавання. Доступ до мережі для ДСТУ IEC 60870-5-101 з використанням стандартних транспортних профілів. Вид. офіц. Чинний від 01.01.2015. Київ: Мінекономрозвитку України, 2015. URL: https://online.budstandart.com/ua/catalog/doc-page?id_doc=62141

56. IEC 62443. Security for industrial automation and control systems (Безпека промислових систем автоматизації та керування). URL: https://tk185.appau.org.ua/downloads/IEC_62443_2_1_ukr_draft.pdf

57. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Revision 2. NIST, 2015.

URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

58. ДСТУ IEC/TS 62351-1:2014. Управління енергосистемами та обмін пов'язаною з ними інформацією. Безпека даних та зв'язку. Частина 1. Вступ до питань безпеки. Вид. офіц. Чинний від 01.07.2015. Київ: Мінекономрозвитку

України, 2015.

URL: https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU4/dstu_IEC_TS_62351-1-2014.pdf

59. AVEVA System Platform. URL: https://www.aveva.com/en/products/system-platform/

60. McAfee Application Control. URL: https://www.mcafee.com/

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