МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Андрій БЕРСИМ
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав(ла): Здобувач вищої освіти гр. УБД-41

Андрій БЕРСИМ
Ім’я, ПРІЗВИЩЕ

Керівник: Юрій ЩАВІНСЬКИЙ
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
к.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедри УКБЗІ

_____ Світлана ЛЕГОМІНОВА

“____”_____2026 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Берсиму Андрію Вікторовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методи забезпечення інформаційної безпеки критичної інформаційної інфраструктури як складової національної безпеки держави”,
керівник кваліфікаційної роботи Щавінський Юрій, к.т.н, доцент
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “20” лютого 2026 р. №51

2. Строк подання кваліфікаційної роботи “12” травня 2026р

3. Вихідні дані до кваліфікаційної роботи: *структурно-функціональний склад об’єктів критичної інформаційної інфраструктури та архітектура їхніх інформаційно-комунікаційних систем, перелік актуальних вразливостей, а також потенційні моделі порушників безпеки, нормативно-правова база України, технічна документація, специфікації програмно-апаратних засобів захисту інформації.*

4. Перелік питань, які мають бути розроблені:
4.1. Провести аналіз поняття та структури критичної інформаційної інфраструктури держави.
4.2. Здійснити комплексне дослідження методологічних підходів до професійної підготовки та підвищення рівня компетенцій персоналу у сфері кіберзахисту об’єктів критичної інфраструктури.
4.3. Проаналізувати нормативно-правову базу України у сфері забезпечення кібербезпеки та захисту критичної інфраструктури.
4.4. Розробити рекомендації щодо підвищення ефективності системи захисту критичної інформаційної інфраструктури.
5.Перелік ілюстративного матеріалу: *презентація PowerPoint.*
6. Дата видачі завдання “05“ березня 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Визначення об’єкта, предмета, мети та завдань дослідження захисту об’єктів критичної інформаційної інфраструктури.	19.03.2026	
2	Збір та аналіз науково-технічної літератури, Нормативно-правової бази України та міжнародних стандартів у сфері кібербезпеки об’єктів критичної інфраструктури.	30.03.2026	
3	Аналіз специфіки інформаційної безпеки, визначення переліку об'єктів критичної інформаційної інфраструктури та дослідження їх функціонування в межах підприємства.	09.04.2026	
4	Здійснення комплексного дослідження методологічних підходів до оцінювання ризиків інформаційної безпеки, аналізу основних загроз та вразливостей.	14.04.2026	
5	Оцінка ефективності сучасних технічних засобів захисту та формування прикладних рекомендацій.	23.04.2026	
6	Формулювання висновків та практичних результатів за результатами проведеного дослідження захисту.	30.04.2026	
7	Оформлення кваліфікаційної роботи	05.05.2026	
8	Підготовка ілюстративного матеріалу, схем інфраструктури, графіків ризиків та презентації для захисту.	10.05.2026	
9	Отримання відгуку керівника на кваліфікаційну роботу та фінальне подання до захисту.	10.06.2026	
10	Захист кваліфікаційної роботи в ЕК (ДЕК).	__.06.2026	

Здобувач вищої освіти _____ Андрій БЕРСИМ
(підпис) (Ім’я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) (Ім’я, ПРІЗВИЩЕ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Берсим А.В до захисту кваліфікаційної роботи …….
(прізвище та ініціали)

за спеціальністю 125 Кібербезпека
(код,найменування спеціальності)

освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)

на тему: "Методи забезпечення інформаційної безпеки критичної інформаційної інфраструктури як складової національної безпеки держави "
Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач БЕРСИМ Андрій у кваліфікаційній роботі провів системний аналіз управління інформаційною безпекою об'єктів критичної інфраструктури, дослідив сучасні методи навчання персоналу та розробив практичні рекомендації щодо підвищення рівня безпеки об'єктів критичної інфраструктури.

БЕРСИМ Андрій виявив глибоку технічну підготовку, здатність до самостійного вирішення складних наукових завдань та відповідальність. Результати дослідження успішно апробовані автором на двох наукових конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача БЕРСИМА Андрія на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою "Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____2026 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Берсим А.В. допускається до захисту даної роботи в екзаменаційній комісії.

Завідувач кафедри управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну бакалаврську роботу

здобувача вищої освіти БЕРСИМА Андрія

на тему “ Методи забезпечення інформаційної безпеки критичної інформаційної інфраструктури як складової національної безпеки держави ”

Актуальність. кваліфікаційна робота присвячена актуальній проблемі забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури в умовах зростання кількості кіберзагроз, збільшення масштабів кібератак та підвищення ролі інформаційних систем у функціонуванні держави. Обрана тема має важливе теоретичне та практичне значення, оскільки стабільне функціонування критичної інфраструктури є одним із ключових елементів національної безпеки України. . .

Позитивні сторони.

1. У роботі автором розглянуто теоретичні основи забезпечення інформаційної безпеки критичної інформаційної інфраструктури. Проведено аналіз сутності та ролі критичної інформаційної інфраструктури у системі національної безпеки держави, визначено основні загрози та вразливості, а також досліджено нормативно-правове забезпечення захисту критичної інфраструктури в Україні та міжнародний досвід у даній сфері. Окрему увагу приділено аналізу сучасних підходів до забезпечення кібербезпеки об’єктів критичної інфраструктури, здійснено аналіз методів і технологій забезпечення інформаційної безпеки критичних інформаційних систем. Автором наведено класифікацію методів захисту інформації, розглянуто методи виявлення кіберзагроз та атак, а також досліджено сучасні технології моніторингу та реагування на інциденти інформаційної безпеки, запропоновано комплекс заходів і методів захисту інформації, а також сформовано архітектуру системи забезпечення інформаційної безпеки та розроблені пропозиції з покращення.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Робота характеризується логічною структурою, послідовністю викладення матеріалу. Автор продемонстрував достатній рівень теоретичної підготовки та вміння застосовувати сучасні методи і технології забезпечення інформаційної безпеки для вирішення практичних завдань.

Недоліки.

У роботі недостатньо детально розглянуто питання практичної реалізації запропонованої архітектури системи захисту, окремі результати оцінювання ефективності методів захисту могли б бути представлені у вигляді більш розгорнутого порівняльного аналізу

Зазначені зауваження не мають принципового характеру та не знижують загального позитивного враження від виконаної роботи .

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні а здобувач Берсим Андрій заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

професор кафедри ТСК _____ Юрій ПЕПА

к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методів забезпечення інформаційної безпеки об’єктів критичної інформаційної інфраструктури, як складової національної безпеки держави. Робота складається зі вступу, чотирьох розділів, висновків і списку використаних джерел із 45 найменувань. Загальний обсяг роботи становить 74 аркуші, ілюстративний матеріал містить 4 рисунки та 4 таблиці.

Метою роботи є дослідження сучасних методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури, аналіз основних кіберзагроз та розроблення рекомендацій щодо захисту.

Об’єктом дослідження є процеси забезпечення інформаційної безпеки та кіберзахисту на підприємствах та установах, що віднесені до об’єктів критичної інформаційної інфраструктури.

Предметом дослідження є методи, технології та організаційно-технічні механізми забезпечення інформаційної безпеки критичної інформаційної інфраструктури.

Методи дослідження. Для вирішення поставлених завдань у роботі використано методи аналізу та узагальнення, системного аналізу, моделювання загроз, порівняльного аналізу, експертного оцінювання.

Як результат у роботі здійснено системний аналіз нормативно-правового забезпечення кібербезпеки в Україні, проведено класифікацію методів захисту та технологій моніторингу, розроблено модель захисту та рекомендації щодо підвищення рівня кібербезпеки об’єктів критичної інфраструктури.

Галузь застосування. Розроблені підходи, та практичні рекомендації можуть бути безпосередньо впроваджені операторами об'єктів критичної інфраструктури категорії, суб'єктами банківського та фінансового секторів, а також профільними службами безпеки для підвищення рівня кіберстійкості та захисту національних інтересів.

Ключові слова: КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА, МОДЕЛЮВАННЯ ЗАГРОЗ, ОЦІНЮВАННЯ РИЗИКІВ, НУЛЬОВА ДОВІРА, КІБЕРСТІЙКІСТЬ.

ABSTRACT

The qualification thesis is devoted to the study of methods for ensuring the information security of critical information infrastructure facilities as a component of the national security of the state. The thesis consists of an introduction, four chapters, conclusions, and a list of references containing 45 sources. The total volume of the thesis is 74 page, including 4 figures and 4 tables.

The purpose of the study of the thesis is to study modern methods of ensuring the information security of critical information infrastructure, analyze major cyber threats, and develop recommendations for protection.

The object the study is the processes of ensuring information security and cybersecurity at enterprises and institutions classified as critical information infrastructure facilities.

The subject of the study is methods, technologies, and organizational and technical mechanisms for ensuring the information security of critical information infrastructure.

Research methods. To solve the tasks set in the thesis, methods of analysis and generalization, system analysis, threat modeling, comparative analysis, and expert evaluation were used.

As a result, a systematic analysis of the regulatory and legal framework of cybersecurity in Ukraine, classifies protection methods and monitoring technologies, and develops a security model and recommendations for improving the cybersecurity level of critical infrastructure facilities.

Field of application. The developed approaches, models, and practical recommendations can be directly implemented by operators of category-specific critical infrastructure objects, financial and banking sector entities, as well as specialized security services to enhance cyber resilience and protect national interests.

Keywords: CRITICAL INFORMATION INFRASTRUCTURE (CII), CYBERSECURITY, THREAT MODELING, RISK ASSESSMENT, ZERO TRUST, CYBER RESILIENCE.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI	(Artificial Intelligence) - штучний інтелект
APT	(Advanced Persistent Threat) - складна цілеспрямована кібератака
BGP	(Border Gateway Protocol) - протокол міжмережевої маршрутизації
BIS	(Building Integration System) - система інтеграції безпеки будівлі
СКУД	Система контролю та управління доступом
CISA	(Cybersecurity and Infrastructure Security Agency) - агентство з кібербезпеки та захисту інфраструктури США
DDoS	(Distributed Denial of Service) - розподілена атака типу «відмова в обслуговуванні
DPI	(Deep Packet Inspection) - глибока перевірка пакетів даних
IDS	(Intrusion Detection System) - система виявлення вторгнень
IIoT	(Industrial Internet of Things) - промисловий інтернет речей
IPS	(Intrusion Prevention System) - система запобігання вторгненням
KPI	Ключові показники ефективності
КСЗІ	Комплексна система захисту інформації
OPC	(Open Platform Communications) - стандарт обміну даними між промисловими системами
SCADA	(Supervisory Control and Data Acquisition) - система диспетчерського управління та збору даних
SIEM	(Security Information and Event Management) - система управління подіями та інформацією безпеки
SOAR	(Security Orchestration, Automation and Response) - система автоматизації та оркестрації реагування на інциденти
SOC	(Security Operations Center) - центр моніторингу та реагування на інциденти інформаційної безпеки
ТЗІ	Технічний захист інформації
UEBA	(User and Entity Behavior Analytics) - аналіз поведінки користувачів та об’єктів
Zero Trust	Модель «нульової довіри» у сфері кібербезпеки
АСУ ТП	Автоматизована система управління технологічними процесами
ІКТ	Інформаційно-комунікаційні технології
ІТС	Інформаційно-телекомунікаційна система
КІІ	Критична інформаційна інфраструктура
ОКІ	Об’єкти критичної інфраструктури
ОКІІ	Об’єкти критичної інформаційної інфраструктури

ВСТУП

Кіберзагрози для критичних систем України вже давно вийшли за межі теоретичних сценаріїв. Атака BlackEnergy на три регіональні енергокомпанії у грудні 2015 року залишила без електроенергії близько 225 тисяч абонентів - і це був перший задокументований випадок кібератаки, що спричинила реальне відключення електромережі в мирний час. З того часу масштаб та інтенсивність подібних загроз лише зростали. Паралельно енергетика, фінанси, транспорт і держуправління продовжували активно переходити у цифровий простір, невпинно розширюючи поверхню можливих атак. Саме це протиріччя - між необхідністю цифровізації та зростаючими ризиками - й визначає актуальність проблеми захисту критичної інформаційної інфраструктури для сучасної України.

Наслідки успішного проникнення в критичні системи виходять далеко за межі звичного розуміння кібератаки. Збій в управлінні водопостачанням, зупинка платіжних шлюзів банків або паралізація системи диспетчеризації - це вже не просто технічні інциденти, а удари по базових умовах функціонування держави. Варто нагадати: атака NotPetya у червні 2017 року вивела з ладу інформаційні системи десятків українських міністерств, банків та підприємств, завдавши збитків на мільярди доларів.

Захист КІІ потребує не просто технічних рішень, а системного підходу, що охоплює правову базу, організаційні процедури та безперервну підготовку персоналу. Ухвалення Закону України «Про критичну інфраструктуру» у листопаді 2021 року стало важливим кроком у цьому напрямі, проте досвід показує: нормативний акт і реальний рівень захищеності конкретних об'єктів - поки що речі різні. Саме цей розрив між регуляторними вимогами та практикою їх виконання є відправною точкою дослідження.

Метою роботи є дослідження сучасних методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури, аналіз основних кіберзагроз та розроблення рекомендацій щодо захисту.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки та кіберзахисту на підприємствах та установах, що віднесені до об’єктів критичної інформаційної інфраструктури

Предметом дослідження є методи, технології та організаційно-технічні механізми забезпечення інформаційної безпеки критичної інформаційної інфраструктури.

Реалізація поставленої мети передбачає виконання таких конкретних завдань:

1. Дослідити поняття, структуру та категоризацію об'єктів критичної інформаційної інфраструктури відповідно до законодавства України та міжнародних стандартів.

2. Провести аналіз актуальних кіберзагроз і вразливостей, характерних для об'єктів КІІ, визначити головні вектори атак та оцінити потенційні наслідки їх реалізації.

3. Дослідити чинну нормативно-правову базу України у сфері кіберзахисту КІІ та визначити ступінь її узгодженості з вимогами директиви NIS2 Євросоюзу.

4. Розробити практично орієнтовану модель захисту об'єктів КІІ і сформулювати рекомендації щодо впровадження сучасних методів кіберзахисту.

Методи дослідження. У процесі розв'язання поставлених завдань застосовувались:

Аналіз та узагальнення - при опрацюванні наукових публікацій, технічних стандартів і нормативно-правових актів у сфері захисту критичної інфраструктури;

Системний метод аналізу - при вивченні структури та функціонування інформаційних систем об'єктів КІІ як єдиного взаємопов'язаного комплексу;

Моделювання загроз - при побудові сценаріїв можливих кібератак і визначенні найбільш вразливих компонентів інфраструктури;

Оцінювання ризиків - при ранжуванні потенційних загроз за ймовірністю реалізації та величиною можливих збитків;

Порівняльний аналіз - при зіставленні ефективності різних технологій і підходів до захисту інформаційних систем;

Експертне оцінювання - при визначенні пріоритетності захисних заходів і обґрунтуванні практичних рекомендацій;

Методи статичного аналізу коду - при перевірці конфігурацій систем захисту і виявленні потенційних вразливостей у налаштуваннях.

Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНИХ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

1.1 Поняття та роль критичної інформаційної інфраструктури у системі національної безпеки держави

Захист об'єктів КІІ - це зовсім інший рівень відповідальності. Відмова у звичайній компанії означає простій і збитки. Відмова на об'єкті критичної інфраструктури може паралізувати цілу галузь або позбавити мільйони людей базових послуг. Правові, організаційні та технічні складові тут мають функціонувати узгоджено - слабка ланка в будь-якій з них відкриває вхід для зловмисника чи провокує системний збій.

Увімкнувши вранці електрочайник, знявши готівку в банкоматі або зателефонувавши в поліклініку, людина навіть не замислюється, скільки рівнів цифрових систем стоїть за цими буденними діями. Держава поступово перенесла управлінські функції в цифровий простір - і разом з цим питання надійності цих систем стало питанням не ІТ-відділу, а національної безпеки. Збій у роботі КІІ торкається кожного, тому захист цих систем і є стратегічним пріоритетом.

Держуправління, енергетика, фінанси, транспорт - усі вони масово пішли у цифру впродовж буквально двох десятиліть. Швидко. Занадто швидко для того, щоб встигати вибудовувати захист. Наслідок очевидний: кожна нова цифрова функція держави - це водночас нова поверхня атаки. Гібридні конфлікти 2010-х і 2020-х це підтвердили практично: кіберзасоби дозволяють уражати стратегічні цілі без єдиного пострілу.

Листопад 2021 року - важлива точка в українському законодавстві: набрав чинності Закон «Про критичну інфраструктуру». Він нарешті дав чітку класифікацію: чотири рівні критичності залежно від масштабу можливих наслідків. КІІ у цьому законі - не просто «важливі системи». Це конкретні

мережі, комунікаційні ресурси й технологічні комплекси, від яких прямо залежать електропостачання, банківські розрахунки, зв'язок, подача води і медична допомога. Якщо вони виходять з ладу - страждають не окремі організації, а суспільство в цілому [1].

На рівні теорії це виглядає як абстракція. На рівні практики - зовсім інакше. Зупинка цифрових систем торкається конкретних людей у конкретний момент. І це далеко не завжди наслідки масштабних атак.

Найочевидніший вимір - базові потреби населення. Водопостачання, електроенергія, медична допомога - усе це тримається на комп'ютерних мережах і промислових контролерах. Відключення «Київстару» у грудні 2023 року зробило це зрозумілим без жодних пояснень: зв'язок - не зручність, це критична інфраструктура [1].

Збої у фінансовій та транспортній сферах дають відчутний економічний ефект. Кілька годин паралічу платіжних систем під час атаки 2016 року коштували операторам десятки мільйонів гривень прямих втрат - не рахуючи репутаційних.

Оборонний вимір критичної інфраструктури став особливо очевидним після лютого 2022 року. Кіберпростір і фізичний театр бойових дій взаємопов'язані безпосередньо: зупинка систем зв'язку або диспетчерського управління - це вже не технічна проблема, а оперативний результат із реальними наслідками.

Окремо стоїть суспільний вимір. Коли критичні сервіси падають на добу-дві, люди починають запитувати: а держава взагалі контролює ситуацію? Саме цей підрив довіри є окремою ціллю гібридних кампаній - не тільки технічний збій, а й психологічний ефект. Деякі регулятори цього не до кінця усвідомлюють.

Сучасні кіберзагрози давно вийшли за межі «інформаційної безпеки» у вузькому розумінні. Атака на промисловий контролер - це вже не IT-інцидент. Це потенційна аварія на виробництві. Тому кіберзахист і фізична охорона

об'єктів КІІ сьогодні вирішують схожі задачі - і мають вибудовуватись у тісній інтеграції.

Рішення про віднесення конкретного об'єкта до КІІ ґрунтується на оцінці його соціальної, політичної, економічної та екологічної ролі крізь призму забезпечення оборони і безпеки громадян. В Україні запроваджена диференційована система: чотири рівні критичності залежно від масштабу можливих наслідків [1].

Об'єкти першої категорії - виняткові за значущістю. Їх виведення з ладу здатне спричинити кризу загальнонаціонального масштабу, вражаючи одночасно кілька елементів критичної інфраструктури.

Об'єкти другої категорії - ті, порушення роботи яких може призвести до кризових явищ регіонального масштабу.

До третьої категорії належать об'єкти, відмова яких загрожує кризою місцевого рівня.

Четверта категорія охоплює об'єкти, несправність яких здатна спричинити кризу локального характеру. Ця градація виконує подвійну функцію: визначає пріоритети захисту і формує основу для диференційованого управління ризиками [1].

Цікавий парадокс: українська класифікація детальніша за європейську NIS2. Там - дві категорії (суттєві та важливі). В нас - чотири рівні критичності. Чи це краще? По-своєму так - чіткіша градація спрощує прийняття рішень про обсяг захисних заходів. Об'єкт першої категорії потребує Zero Trust і SOC на повну. Четвертої - достатньо базового регламентування [1, 2].

1.2 Основні загрози та вразливості критичної інформаційної інфраструктури

Промислове обладнання на об'єктах КІІ нерідко проектувалось ще в 1990-х - тоді питання про кіберзахист контролерів просто не стояло. Сьогодні ці самі системи підключені до мереж. Результат передбачуваний: APT-група

може роками «сидіти» в інфраструктурі, поступово просуваючись до технологічного сегменту. Виявляють таке проникнення часто вже після того, як збиток нанесено. Ліквідація наслідків займає місяці. А не завжди кваліфікований персонал, що рятує ситуацію в аварійному режимі, іноді сам стає джерелом додаткових помилок.

Морально застаріле ПЗ та обладнання - хронічна хвороба об'єктів КІІ. Системи, що проєктувались без урахування сучасних вимог кібербезпеки, містять вразливості, якими зловмисники активно користуються. Замінити їх складно, дорого і ризиковано з точки зору безперервності технологічного процесу - тому їх продовжують експлуатувати роками.

Модернізація застарілих систем вимагає тимчасового призупинення технологічного процесу, а для об'єктів КІІ це означає реальні збитки і потенційні соціальні наслідки. Тому оперативне усунення виявлених вразливостей часто відкладається на невизначений термін - і це відоме «вікно вразливості» стає улюбленою точкою входу для зловмисників.

APT-атаки - клас загроз, що дається взнаки не одразу. Зловмисник входить через фішинговий лист або вразливість периметра, потім тижнями або місяцями живе в системі непомічено. Паралельно зростає частота ransomware-кампаній проти КІІ: 2023–2024 роки зафіксували їх у фінансовому та енергетичному секторах України. Окремо - інсайдерський ризик. За даними багатьох постінцидентних розслідувань, внутрішній фактор фігурує як один із ключових векторів входу - і не завжди це свідоме зловмисництво [2, 4].

Де у КІІ найбільше дірок? Практика показує три стабільні зони: програмні вразливості (невиправлені, застарілі, погано налаштовані), апаратне забезпечення, що морально застаріло і спроектоване без думки про кіберзагрози, та слабка мережева сегментація. Частина систем на об'єктах КІІ і досі працює на платформах 15-20-річної давнини - замінити їх потрібно, але зупиняти виробничий процес заради оновлення надто дорого [4].

Невиправлені CVE - улюблений вектор зловмисників. Середній час між публікацією уразливості і її активною промисловою експлуатацією скоротився

з місяців до тижнів. Для об'єктів КІІ, де патчинг вимагає зупинки технологічного процесу, це означає хронічне «вікно вразливості» - і це відома проблема, а не теоретичний ризик [4].

Неналежна організація контролю доступу є однією з найпоширеніших точок входу для зловмисників. Відсутність MFA, слабкі паролі та некоректний розподіл прав між користувачами - ці три чинники разом кратно підвищують імовірність несанкціонованого проникнення. Усунення навіть одного з них помітно знижує ризик.

Людський фактор не зникає навіть при найсучаснішому технічному захисті - він просто змінює форму. Недотримання регламентів, ігнорування правил безпеки та низька кіберграмотність персоналу спричиняють витоки даних або збої в системах часто ефективніше, ніж зовнішні атаки. До цього додаються слабка сегментація мережі, відсутність резервного копіювання, неефективний моніторинг і використання незахищених каналів зв'язку.

Сукупна дія всіх перелічених чинників формує реальну загрозу стабільності функціонування об'єктів КІІ. Наслідки успішних атак можуть бути катастрофічними: аж до повного припинення надання ключових послуг населенню та органам державного управління.

Передусім це стосується галузей електропостачання, зв'язку, транспорту, водопостачання, водовідведення, функціонування фінансових систем та інших базових секторів, що забезпечують життєдіяльність країни.

Навіть короткочасний збій в роботі таких систем здатен спричинити відчутні економічні збитки, паралізувати держструктури і поглибити соціальну напругу. При цьому загрози можуть мати як технічне походження, так і свідомо організований деструктивний характер - відрізнити їх на початку інциденту вкрай складно.

Серед головних категорій ризиків - технічні аварії та несправності обладнання, природні катастрофи, а також зловмисні дії окремих осіб або організованих угруповань. Кібератаки, диверсії, терористичні акти та збройні конфлікти здатні дестабілізувати роботу ключових об'єктів миттєво. При

цьому принципово важливою залишається взаємозалежність елементів критичної інфраструктури - саме вона перетворює локальний інцидент на системну катастрофу.

Пошкодження електроенергетичних мереж - типовий приклад ланцюгової реакції: транспортні системи зупиняються, телекомунікації деградують, медичні заклади і державні сервіси виявляються паралізованими. Порушення роботи одного об'єкта поширюється на суміжні системи - і ліквідувати наслідки такого каскаду набагато складніше, ніж не допустити його.

Ізольованих рішень у захисті КІІ не існує. Закрити одну вразливість, не розуміючи взаємозалежностей між секторами - значить просто перенести ризик в інше місце. Саме тому аналіз загроз має охоплювати весь ланцюжок: від технічного рівня до організаційних процедур і правового регулювання.

Оцінювання загроз - це структурований аналіз, що включає ризик несанкціонованого втручання, імовірність кризових ситуацій через людські помилки чи природні явища, а також часові параметри відновлення уражених систем. Без такого підходу будь-які заходи захисту залишатимуться реактивними.

Щоб зрозуміти, де Україна перебуває у сфері захисту КІІ, потрібно порівняти її систему з тим, як це вирішено в інших. Таке порівняння не є закликом до копіювання - кожна система виросла з власного інституційного ґрунту. Але спільні риси та відмінності допомагають побачити, де наші прогалини реальні, а де - уявні.

Україна пройшла тривалий шлях від галузевої розпорошеності до більш-менш єдиного правового поля. Прийнятий у листопаді 2021 року Закон «Про критичну інфраструктуру» вперше в нашій правовій системі не просто дав визначення, а створив класифікаційну систему: чотири рівні критичності - від загальнодержавного до локального. Такого ступеня деталізації немає ні в NIS2, ні у фреймворку NIST [4].

Директива NIS2 набула обов'язкової сили в жовтні 2024 року - і це вже не рекомендації, а юридичні вимоги для всіх держав-членів ЄС. Головне нововведення - не розширений перелік секторів, а персональна відповідальність: керівник організації тепер несе пряму правову відповідальність за стан кіберзахисту, а не лише «підписує папери». Часові ліміти для повідомлення про інцидент стали жорсткими: перша нотифікація - до 24 годин, розгорнутий звіт - впродовж наступних 48. Для України, що рухається до acquis ЄС, це конкретні цільові показники: нормативне закріплення аналогічних строків звітності у вітчизняному законодавстві поки що менш деталізоване [5].

Американський підхід свідомо відрізняється від європейського - і це не слабкість. NIST Cybersecurity Framework не передбачає штрафів за невідповідність: берете до уваги - добре, не берете - ваш вибір і ваші ризики. CISA не виступає інспектором - вона консультує і надає безкоштовні інструменти для самооцінки. Регуляторний тиск тут замінений ринковим: страховий ринок кіберризиків у США перевищив 15 млрд доларів на рік, і страховики самостійно вимагають відповідності CSF як умови видачі полісу. Результат - порівнянний з примусовим ЄС-підходом, але досягнутий іншим шляхом [5, 6].

Британський підхід структурований навколо тринадцяти секторів із власними протоколами реагування. Ключова риса: акцент на секторній специфіці, а не уніфікованих вимогах. Для кожного сектору визначено власні критерії критичності та профілі загроз.

Німецька модель охоплює десять секторів і суттєво відрізняється від британської більш жорстким регуляторним контролем. Федеральне відомство з інформаційної безпеки (BSI) має право перевірок і видачі обов'язкових приписів - таких повноважень у американської CISA немає [6].

Попри різні підходи - жорсткі нормативні в ЄС, добровільно-партнерські в США, секторальні в Британії - є один спільний висновок: технічні рішення без організаційної та правової підтримки не дають результату. Де між

моделями є реальні суперечки - це питання розподілу відповідальності: хто платить за захист, хто перевіряє, і хто несе відповідальність при порушенні.

Для України, що перебуває в активній фазі євроінтеграції та одночасно в умовах реального кіберпротистояння, ці відмінності мають практичне значення. Гармонізація з NIS2 вимагає, зокрема, посилення вимог до звітування про інциденти і встановлення особистої відповідальності керівників операторів КІІ [6].

CERT-UA займає особливе місце в цій системі. За роки активного гібридного конфлікту команда накопичила досвід, якого не має жодна аналогічна структура в ЄС чи США. Публічні звіти CERT-UA за 2022–2025 роки фіксують сотні підтверджених атак на КІІ - це не академічна аналітика, а відпрацьована практика реагування. Досвід CERT-UA міг би активніше лягати в основу конкретних нормативних вимог - наразі цей потенціал використовується недостатньо [6].

Десять секторів у Німеччині, тринадцять у Великобританії, сімнадцять у США - ці відмінності у структуруванні не принципові. Принципово інше: готовність держави інвестувати в захист не лише регуляторними вимогами, а й ресурсами, підготовкою і технічною підтримкою операторів.

Усі розглянуті моделі підтверджують одне: кіберзахист - це не лише технологія. Людський фактор і організаційні процеси у більшості задокументованих інцидентів виявляються вирішальними - або як причина компрометації, або як ключ до ефективного реагування. Технічні засоби без людей і процесів - дорогий і неефективний набір інструментів.

Заходи попередження, виявлення і нейтралізації загроз, а також обмеження наслідків інцидентів - спільне ядро всіх систем. Відмінності - у деталях реалізації.

У кожній з розглянутих моделей технічні інструменти є: SIEM, засоби моніторингу, резервне копіювання. Різниця - не в наборі, а в тому, наскільки їх застосування є обов'язковим і стандартизованим. У деяких моделях це

жорстка вимога з перевіркою; в інших - рекомендація без реальних наслідків за невиконання [8, 9].

Базові поняття - загроза, ризик, стійкість, цілісність - у різних системах визначаються по-різному. Ця понятійна розбіжність ускладнює міжнародне співробітництво у реагуванні на транскордонні кіберінциденти. Для України, що прагне інтеграції в євроатлантичний простір безпеки, уніфікація понятійного апарату є практичним завданням.

1.4. Аналіз сучасних підходів до забезпечення кібербезпеки об'єктів критичної інфраструктури

Що таке кібербезпека - залежить від того, кого питати. ІТ-фахівець скаже: захист мереж і даних. Юрист вкаже на визначення з закону. Оператор промислового підприємства думатиме про контролери й SCADA. У Законі «Про основні засади забезпечення кібербезпеки України» 2017 року ці погляди принципово об'єднані: кібербезпека охоплює не лише цифрову сферу, а й фізичні об'єкти, безпосередньо пов'язані з інформаційними системами. Для КІІ це не термінологічна тонкість: якщо зловмисник вивів з ладу промисловий контролер - це одночасно кіберінцидент і потенційна фізична аварія на виробництві [10].

У 2016 році НАТО офіційно визнало кіберпростір п'ятим операційним доменом поряд із сушею, морем, повітрям і космосом. Рішення не декларативне - воно закріпило, що атаки в кіберпросторі можуть кваліфікуватись як підстава для активації статті 5 Договору. Для розуміння захисту КІІ це принципово: вразливість в інформаційній інфраструктурі означає вразливість у всіх інших доменах одночасно.

З визнання кіберпростору операційним доменом виникло й нове поняття - кіберстійкість. Це не просто «захист від атак». Кіберстійкість виходить із реалістичного припущення: абсолютного захисту не існує, й інцидент рано чи пізно станеться. Питання в тому, чи продовжує система виконувати критичні

функції під час атаки і як швидко повертається до нормального режиму після неї.

Для об'єктів КІІ - особливо промислових - це різниця між контрольованою ситуацією і катастрофою з непередбачуваними наслідками [10].

Скільки захисту «достатньо» - питання без єдиної відповіді. На практиці орієнтиром слугує ризик-орієнтований підхід: оцінюєш ймовірність загрози, множиш на можливий збиток - і отримуєш пріоритет. Далі - вибір заходів у межах бюджету. Те, що спрацьовує на паперових розрахунках, не завжди спрацьовує на реальних об'єктах - але систематичний аналіз ризиків все одно кращий за захист «по інтуїції».

Defense-in-Depth - не нова ідея. Її запозичили з військової доктрини: жодна оборонна лінія не є абсолютно непробивною, тому їх має бути кілька. У кібербезпеці це означає: якщо зловмисник обійшов периметровий файрвол - він натрапляє на EDR-рішення на кінцевих точках. Пройшов їх - стикається з мікросегментацією і жорстким контролем привілеїв. На кожному рівні - окрема лінія опору. Для КІІ з критичними ОТ-системами така глибина ешелонування є не рекомендацією, а необхідністю [10].

Кіберстійкість - не просто ІТ-характеристика. Коли мова йде про об'єкти КІІ, захист інформаційних ресурсів напряму визначає, чи продовжуватимуться технологічні процеси під час інциденту. Зупинка виробничої лінії або системи диспетчеризації - це вже державний рівень проблеми.

Управління ідентифікацією та доступом (IAM) на практиці є одним із найефективніших інструментів попередження інцидентів. Принцип мінімально необхідних привілеїв - не абстрактна рекомендація, а конкретний механізм зменшення поверхні атаки: чим менше прав у кожного акаунта, тим менше збитків від його компрометації.

Порівняльний аналіз стратегічних підходів у галузі кібербезпеки дозволив визначити ключові операційні та ризикові критерії (табл.1), а також запропонувати впровадження концепції нульової довіри (рис.1).

Таблиця 1.1

Порівняльний аналіз стратегічних підходів

Стратегія	**Основний Принцип**	**Ключові Переваги**	**Виклики Впровадження**
Zero Trust (Нульова довіра)	Постійна верифікація кожного запиту, незалежно від походження.	Ефективна протидія внутрішнім загрозам і витокам.	Висока складність інвентаризації активів.
Cyber Resilience (Стійкість)	Здатність системи функціонувати в умовах активної атаки.	Мінімізація простоїв і швидке відновлення (DR).	Потребує значних витрат на надмірність систем.
IT/OT Конвергенція	Об'єднання бізнес-мереж з технологічними процесами.	Прозорість процесів та аналітика в реальному часі.	Ризик проникнення з IT-мережі в АСУ ТП.
AI-driven Defense	Використання ШІ для виявлення аномалій та SOAR.	Швидкість реагування, що перевищує можливості людини.	Проблема "чорної скриньки" та помилкові спрацювання.

Рис.1.1. Процес впровадження Zero Trust

Побудувати дієву систему кіберзахисту на об'єктах критичної інформаційної інфраструктури без вивчення вітчизняної нормативної бази та міжнародних практик - неможливо. Парадоксально, але порівняння підходів до регулювання безпеки КІІ в Україні та Євросоюзі виявляє не лише спільні риси, а й принципові відмінності - ключові інституційні критерії відображено в (табл.1.2).

Таблиця 1.2

Порівняння нормативних підходів

Критерій порівняння	**Україна (ЗУ "Про КІ")**	**Європейський Союз (NIS2)**
Категоризація	4 категорії (від загальнодержавного до місцевого).	Поділ на «суб'єкти високої критичності" та "важливі суб'єкти".
Відповідальність	Персональна відповідальність керівників, адміністративний контроль.	Штрафи до 10 млн євро або 2% від річного обігу.
Обмін даними	Обов'язкове повідомлення через систему інцидентів ДССЗЗІ.	Дворівнева звітність: раннє попередження та фінальний звіт.

Між вітчизняним законодавством і директивами ЄС існують суттєві відмінності в підходах до правозастосування та масштабування - дані табл. 2 це підтверджують. В Україні класифікаційний механізм деталізованіший: чотири рівні критичності з виразним акцентом на персональній відповідальності керівників ОКІІ. Директива NIS2 ЄС використовує дворівневий поділ на «суттєві» та «важливі» суб'єкти - з наголосом на галузевому підході та гармонізованих вимогах [11].

Комплексна модель безпеки об'єктів критичної інфраструктури не може зводитись до одного рівня захисту. Вона охоплює водночас промислові технологічні процеси та загальну інформаційну інфраструктуру. Концептуальну схему трьох фундаментальних складових сучасного кіберзахисту - AI Defense, SCADA / OT Resilience і Cyber Resilience - разом із функціональними завданнями кожної з них представлено на (рис.1.2).

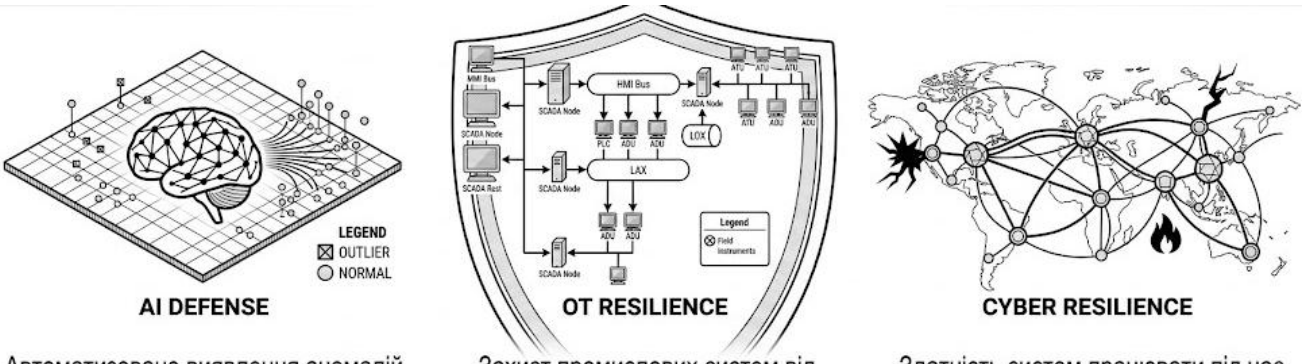

Рис.1.2. Тренди та перспективи

AI Defense будується на алгоритмах штучного інтелекту для автоматизованого виявлення аномалій у мережевому трафіку. Практика підтверджує: фіксація відхилень від штатного режиму на найраніших стадіях кібератак забезпечує оперативне реагування ще до того, як загрози набувають критичного масштабу.

OT Resilience спрямований на захист промислових систем - операційних технологій - від фізичних пошкоджень та деструктивних зовнішніх впливів.

Безпека цієї сфери гарантується суворим контролем взаємодії між людино-машинними інтерфейсами, контролерами та кінцевими польовими пристроями.

Cyber Resilience - це здатність інформаційних систем і мереж зберігати стабільну роботу й виконувати критично важливі функції навіть під час активної фази кібератак або масштабних інцидентів із широким географічним охопленням.

Головний висновок теоретичного розділу: захист критичної інформаційної інфраструктури є безпосереднім елементом системи національної безпеки, а не лише "важливим напрямком". Від стабільності КІІ залежить реальна обороноздатність, реальна економіка і реальне суспільство - без будь-яких перебільшень.

Нормативна база, як показав аналіз, перебуває в активній динаміці. Євроінтеграційний курс вимагає швидкої адаптації до вимог NIS2 - зокрема

щодо звітності про інциденти та управлінської відповідальності керівників об'єктів. При цьому Україна має ресурс, якого немає у партнерів: реальний бойовий досвід, накопичений CERT-UA в умовах активного кіберпротистояння [11].

Аналіз чинної нормативно-правової бази переконливо демонструє: українське законодавство перебуває в активній фазі змін та послідовно адаптується до стандартів Євросоюзу.

Висновки до розділу 1

Перший розділ присвячено теоретичним засадам: без їх ґрунтовного осмислення неможливо коректно сформулювати завдання захисту критичної інформаційної інфраструктури.

Огляд наукових джерел і нормативних документів переконав: КІІ - поняття значно ширше за обчислювальні та мережеві ресурси. воно охоплює весь технологічний ланцюг, від стабільності якого залежить надання ключових послуг - електропостачання, водопостачання, банківського обслуговування, телекомунікаційного зв'язку.

Реальний масштаб наслідків від порушення функціонування КІІ ілюструє низка резонансних інцидентів. Атака BlackEnergy у грудні 2015 року на українську енергетичну систему залишила без електроенергії близько 225 тисяч осіб.

Кампанія NotPetya у червні 2017 року завдала Україні збитків понад 10 мільярдів гривень. Знеструмлення мережі «Київстар» у грудні 2023-го спричинило порушення зв'язку для мільйонів абонентів більше ніж на добу. В усіх цих випадках удар по інформаційних системах миттєво впливав на фізичні процеси та повсякденне життя громадян.

Зіставлення вітчизняної нормативної бази з директивами ЄС (NIS2, CER) та досвідом США засвідчило: Україна рухається в одному напрямі з європейськими партнерами. Закон «Про критичну інфраструктуру» за своїм змістом близький до положень NIS2.

Розділ 2. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

2.1 Класифікація методів захисту інформації у критичних інформаційних системах

Парадигма кіберзахисту КІІ за останнє десятиліття зазнала принципового зсуву. Логіка «непробивного периметра» розбилася об реальність: атаки BlackEnergy, NotPetya, Colonial Pipeline показали, що ніякий периметр не є абсолютним. Нова логіка - адаптивна стійкість: система проектується з припущенням, що зловмисник рано чи пізно всередині. Питання - як мінімізувати наслідки і як швидко відновитись.

Класифікувати методи захисту можна по-різному - і будь-яка класифікація умовна. Практично важливіше зрозуміти, що конкретний інструмент робить у ланцюжку реагування. Криптографія, брандмауери, IDS/IPS - технічний рівень. Регламенти, контроль доступу, навчання персоналу - організаційний. Відповідність ISO/IEC 27001 і вимогам ДССЗЗІ - нормативний. Функціонально ж усі вони вкладаються у тріаду: не допустити атаку, виявити її якомога раніше, відновитись із мінімальними втратами після того, як вона все ж сталась. В OT-середовищі цей набір потребує доповнення: тут критичні інструменти, що розуміють промислові протоколи на рівні пакета - DPI для Modbus чи DNP3, honeypot-приманки, що виявляють розвідку зловмисника ще до активної фази атаки. Zero Trust у такій моделі - не окремий інструмент, а наскрізний принцип.

2.2. Методи виявлення кіберзагроз та атак на об'єкти критичної інфраструктури

Автоматизовані системи управління технологічними процесами (АСУ ТП) набули особливого поширення на об'єктах КІІ, насамперед в атомній та традиційній енергетиці. SCADA, DCS та їх гібридні конфігурації утворюють технологічний хребет цих об'єктів. Кількість таких систем невпинно зростає - відповідно зростає і поверхня атаки [11].

Принципова відмінність АСУ ТП від класичних ІТ-систем: нерозривний зв'язок з фізичними процесами та виконавчими пристроями. Це надає кібербезпеці в цьому середовищі зовсім іншого виміру - помилка тут може мати фізичні наслідки.

Збій АСУ ТП виходить далеко за межі фінансових втрат. Ризики для здоров'я і безпеки людей, пошкодження навколишнього середовища та репутаційні наслідки - ось що відрізняє кіберзагрози в промисловому середовищі від звичайних ІТ-інцидентів.

Оцінювання кіберризиків - фундамент, на якому будується ефективне управління загрозами для об'єктів КІІ. Власники таких об'єктів прагнуть двох речей одночасно: знизити ризик до прийнятного рівня і не перевищити розумних меж витрат. Знайти цей баланс без систематичного аналізу загроз - практично неможливо.

Вирішення завдань управління кіберризиками для КІІ потребує сучасних підходів до аналізу загроз. Результати оцінювання ризиків дають змогу чітко визначити ступінь небезпеки і обґрунтувати доцільність конкретних захисних заходів у межах наявного бюджету.

При розробці сучасних підходів до кібербезпеки критичної інфраструктури виокремлюють кілька пріоритетних напрямків дослідження та практичного впровадження.

1. Виявлення потенційних кіберзагроз для таких об'єктів, оцінку їхнього впливу, а також аналіз нових векторів атак і вразливостей.

2. Застосування штучного інтелекту, машинного навчання, блокчейн-технологій та інших інноваційних рішень для побудови активного захисту, запобігання атакам і моніторингу порушень.
3. Розробку інтегрованих стратегій захисту, які враховують специфіку кожного сектору критичної інфраструктури.
4. Впровадження міжнародних стандартів і нормативних положень у сфері кібербезпеки разом із глобальним партнерством для створення єдиної системи регуляцій.

Виявлення загроз у промисловому середовищі - задача складніша, ніж у корпоративному IT. Сигнатурний аналіз тут теж працює - але лише для відомих загроз. Нова атака, яку ще не занесено до баз, проходить повз нього непомічено. Тому для КІІ сигнатурний підхід - лише базовий рівень, не більше.

Атаки Zero-Day за означенням не мають сигнатур - тому їм протидіють інакше. Аномалійний аналіз фіксує несподівані відхилення в поведінці мережевого середовища, а UEBA забезпечує моніторинг підозрілої активності пристроїв і користувачів у реальному часі. Разом ці два методи перекривають зону загроз, де сигнатурний підхід безсилий.

Особливу цінність для систем критичної інфраструктури має технологія DPI. Вона аналізує трафік промислових протоколів - Modbus, Profinet, IEC 104 - і блокує небезпечні команди до того, як ті порушать нормальний перебіг фізичних процесів. DPI - один із небагатьох інструментів, що «розуміє» специфіку промислового середовища на рівні протоколу.

Штучний інтелект і машинне навчання змінюють логіку виявлення загроз. Замість пошуку відомого шкідливого патерну - аналіз великих масивів телеметрії і пошук прихованих аномалій. Система навчається на «нормальній» поведінці мережі і фіксує відхилення - навіть якщо ці відхилення не мають аналогів у базах сигнатур. Для КІІ, де нові атаки адаптовані під конкретний об'єкт, такий підхід дає суттєві переваги.

Honeypot-технології - це пастка. Фальшиві елементи, що імітують реальну критичну інфраструктуру, привертають увагу зловмисників і

дозволяють виявити їхню активність на початкових стадіях підготовки атаки. Задовго до того, як вони дістануться справжніх систем [11].

2.3. Технології моніторингу та реагування на інциденти інформаційної безпеки

Поставити SIEM і назвати це «системою моніторингу» - не одне й те саме, що мати робочу систему захисту. SIEM без налаштованих правил кореляції - дорога база даних логів. IDS/IPS без регулярно оновлюваних сигнатур - мертвий вантаж. SOC без підготовлених аналітиків і прописаних плейбуків реагування - люди, що дивляться в монітори, не розуміючи коли і що робити. Реальна захисна система - це узгоджена робота всіх трьох компонентів, де кожен виконує свою функцію і підсилює два інших.

SIEM на практиці виконує роль, яку важко замінити чимось одним. Система агрегує журнали подій з усього: файрволів, серверів, кінцевих точок, промислових шлюзів. Потім нормалізує їх до єдиного формату і шукає кореляції - сигнали, які кожен окремо виглядають нешкідливо, але разом утворюють патерн атаки. Без SIEM аналітик безпеки змушений вручну переглядати тисячі рядків логів з десятків різних систем. З SIEM - отримує готові тригери [12].

Встановлюючи взаємозв'язки між подіями з різних джерел, SIEM-платформи виявляють індикатори компрометації на ранніх стадіях підготовки атак. Окремо кожна подія може виглядати нешкідливо - небезпечним є їх збіг у часі й контексті.

Фізична безпека на об'єктах КІІ - не окрема від кіберзахисту сфера. Несанкціонований фізичний доступ до серверної або виробничої зони може виявитись ефективнішим вектором атаки, ніж будь-яке мережеве проникнення. Одним з підходів до управління фізичною безпекою є платформи, що консолідують підсистеми контролю доступу, відеоспостереження, пожежну та охоронну сигналізацію в єдиному

програмному середовищі. Такі рішення критично потребують підтримки відкритих інтерфейсів - щоб події фізичної безпеки могли передаватись у SIEM для кореляції з кіберподіями.

Саме через такі інтерфейси події фізичної підсистеми - відкриття дверей, спрацювання датчика руху, ідентифікація картки доступу - потрапляють до SIEM і аналізуються разом з подіями кібербезпеки. Приклад: фізичний вхід у серверну кімнату у неробочий час збігається в часі з авторизацією адміністраторського облікового запису. Без кореляції ці два події виглядають нешкідливо. Разом - це тригер для негайного розслідування.

Кореляція між фізичними і кіберподіями дозволяє виявляти атаки, що поєднують обидва вектори - наприклад, коли зловмисник спочатку отримує фізичний доступ до об'єкта, а потім намагається ввести шкідливий пристрій в мережеву інфраструктуру. Такий підхід скорочує час виявлення аномальної активності і підвищує загальний рівень ситуаційної обізнаності.

Система BIS забезпечує декілька важливих функцій:

1. Конвергенція систем. BIS консолідує відеоспостереження, системи контролю та управління доступом (СКУД), охоронну і пожежну сигналізацію, а також засоби оповіщення в єдину інтегровану екосистему.

2. Управління інцидентами. У разі спрацювання датчика система автоматично виводить на пристрій оператора відповідний план приміщення (зокрема тривимірну схему), що дозволяє суттєво скоротити час реакції на критичні події.

3. Інтеграція з IT-безпекою. Завдяки підтримці стандартів OPC і SDK події з BIS можуть бути перенаправлені у SIEM для кореляції між фізичними (відкриття дверей серверної) та цифровими (автентифікація адміністратора в цей час) інцидентами [12, 13].

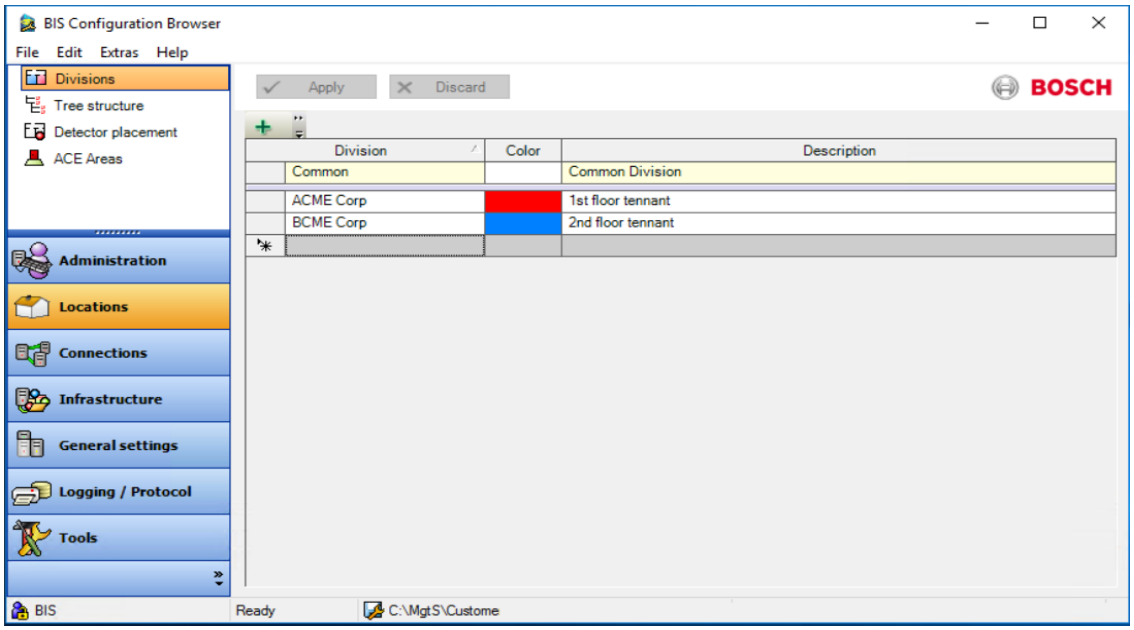

Рис.2.3. Загальний вигляд програмного забезпечення BIS

Серед інших рішень для забезпечення доступу окремої уваги заслуговують системи Inner Range серій Integriti/Inception.

Архітектурний принцип, що заслуговує окремої уваги при виборі систем контролю доступу для КІІ - децентралізована логіка прийняття рішень. Якщо контролер самостійно ухвалює рішення про доступ на місцевому рівні, система залишається працездатною навіть при тимчасових збоях мережевого з'єднання з центральним сервером. Для об'єктів, де безперервність роботи є критичною вимогою, це суттєва перевага порівняно з централізованими рішеннями.

Система підтримує велику кількість точок доступу та облікових записів. Додаткові модулі відеоаналітики - розпізнавання облич або автомобільних номерних знаків - автоматично генерують сигнали тривоги при виявленні підозрілої активності на охоронюваній території, що скорочує час реакції персоналу [14].

Інтеграція відеоаналітики з відеосерверами BIS реалізована через вбудовані алгоритми або сторонні програмні рішення з використанням протоколів ONVIF і API.

2.4. Оцінювання ефективності сучасних методів захисту критичної інфраструктури

Шифрування каналів - мінімум, нижче якого опускатись не можна. Між диспетчерськими центрами і промисловими контролерами трафік має ходити тільки захищеними тунелями. TLS 1.3 і IPSec - стандарт для таких з'єднань. Але шифрування каналу не захищає від атак, що вже діють зсередини системи - це лише одна з ліній захисту.

Для захисту збережених даних ефективним залишається симетричне шифрування з алгоритмом AES-256. Канали між сегментами OT та IT захищаються криптографічними тунелями на основі VPN або сертифікованими засобами ДССЗЗІ - залежно від нормативних вимог конкретного об'єкта.

Недооцінка шифрування на рівні кінцевих пристроїв - ПЛК, HMI-терміналів та інженерних станцій - суттєво підвищує ймовірність компрометації. Ці пристрої найчастіше стають точками входу для атак «людина посередині», оскільки їхній захист традиційно відстає від серверного рівня.

За даними CERT-UA, атаки типу DDoS упродовж 2024–2025 років - стабільна загроза для об'єктів критичної інфраструктури України. Головні мішені - державні вебпортали, банківські установи та оператори телекомунікаційних мереж. Пікові обсяги трафіку під час атак сягали кількох сотень гігабіт на секунду. Це робить ефективний захист практично нереальним без спеціалізованих засобів фільтрації [15].

Небезпека таких атак для стратегічно значущих систем - не лише в безпосередньому перериванні сервісів. Вони завдають фінансових і репутаційних збитків операторам КІІ, причому ці наслідки нерідко тривають довше, ніж сам інцидент. Протидія DDoS вимагає комплексного підходу, і першим кроком - розгортання систем постійного моніторингу мережевої активності для раннього виявлення аномальних патернів трафіку.

Раннє виявлення аномалій дозволяє ідентифікувати атаку до її повного розгортання і оперативно відреагувати. Технологічні рішення на кшталт blackhole routing через протокол BGP або спеціалізованого очищення трафіку відокремлюють шкідливі потоки від легітимних - підтримуючи стабільну роботу систем і запобігаючи критичним наслідкам для інфраструктури.

Проте цього недостатньо. Проєктування мережевої інфраструктури повинне від початку передбачати здатність до гнучкого масштабування при різкому зростанні навантаження - це необхідна умова безперебійного надання послуг під час атаки.

Систематичне планування і підготовка персоналу - не менш важлива складова ефективної відповіді на DDoS-атаки, ніж технічні засоби.

Технічні засоби захисту від DDoS - лише частина рішення. Плани реагування, прописані заздалегідь і відпрацьовані на навчаннях, скорочують час реакції в реальному інциденті в рази. Для організацій без розвиненого власного SOC виходом стають MSSP - постачальники послуг кіберзахисту з готовою інфраструктурою фільтрації. Важлива деталь: системи захисту потребують регулярного перегляду, бо вектори DDoS-атак постійно змінюються.

Найефективнішим захистом КІІ від кіберзагроз є багатоешелонований підхід. Технічні засоби, планування реагування та підготовка персоналу - ці три компоненти мають функціонувати разом. Жоден з них поодинці потрібної стійкості не дасть.

Висновки до розділу 2

Аналіз методів і технологій другого розділу показав головне: у сфері захисту КІІ немає «срібної кулі». Жоден продукт, жоден стандарт і жоден підхід не дає стовідсоткового захисту. Реальна стійкість досягається через комбінацію засобів - криптографія, сегментація, моніторинг, плани реагування - і постійне їх вдосконалення відповідно до еволюції загроз. Для промислового

середовища, де кіберінцидент може мати фізичні наслідки, це не абстрактна рекомендація.

Криптографічні засоби закривають канали передачі даних. Міжмережеві екрани і системи DPI працюють зі специфічними промисловими протоколами - Modbus, IEC 60870-5-104, DNP3. Платформи SIEM і SOC забезпечують централізований моніторинг подій безпеки. Резервне копіювання у поєднанні з планами відновлення мінімізує наслідки успішних атак і скорочує час повернення систем до штатного режиму.

Концепція Zero Trust заслуговує на окреме виділення: вона суттєво знижує ризики при компрометації облікових записів, що особливо актуально з огляду на зростання частки інцидентів, пов'язаних із діями інсайдерів. Гібридна стратегія виявлення атак - поєднання сигнатурного, аномалійного та поведінкового підходів - дає найвищу ефективність.

Розділ 3 РОЗРОБКА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТА КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

3.1. Характеристика об'єкта дослідження

Розробка моделі захисту - не разова процедура. Підприємство змінюється: з'являється нове обладнання, змінюються бізнес-процеси, розширюється мережа. Загрози теж не стоять на місці. Модель, яка відповідала реальності три роки тому, сьогодні може мати критичні прогалини. Тому технічний, організаційний і правовий виміри захисту треба переглядати регулярно - і узгоджено.

Перший крок у побудові захисту звучить просто: з'ясуйте, що саме у вас є. На практиці це нерідко стає несподіванкою. Постінцидентні розслідування регулярно фіксують одне й те саме: в інфраструктурі виявляються пристрої, про які ніхто не знав, облікові записи з адмінськими правами, які давно мали бути закриті, і ПЗ, встановлене кимось «тимчасово» роки тому. Без актуального реєстру активів захист перетворюється на стрільбу наосліп.

На основі інвентаризації будується ієрархічна структура захисних контурів. Кожен контур - своя зона довіри, свої правила доступу, свій периметр.

Архітектурне відокремлення корпоративної мережі від промислового сегменту АСУ ТП є ключовим рішенням для підприємств із виробничими процесами. Якщо ці сегменти об'єднані без належної фільтрації, компрометація поштового сервера може закінчитись втручанням у роботу виробничої лінії. Саме такий сценарій реалізовувався у низці задокументованих інцидентів на об'єктах водопостачання та енергетики у 2021–2022 роках.

Кожен користувач наділяється виключно тими правами, що необхідні для його конкретних функцій. Не більше. Принцип мінімальних привілеїв - не декларація, а архітектурна вимога.

Несанкціоновані входи, підозрілі патерни трафіку, аномальна поведінка облікових записів - усе це залишається поза увагою без безперервного моніторингу. Реагування «постфактум» у критичній інфраструктурі неприйнятне.

Резервне копіювання на ізольованих від мережі носіях - на практиці єдиний надійний засіб відновлення після ransomware-атаки. Резервна копія, доступна з основної мережі, не захищена від тих самих загроз, що й виробнича система.

На практиці варто також тестувати процедуру відновлення з резервної копії: дослідження показують, що від 20 до 30% резервних копій виявляються непридатними саме тоді, коли вони критично потрібні - через помилки конфігурації або пошкодження носія.

Резервування - фундаментальний інструмент зниження наслідків. Не допоміжний захід, а обов'язковий елемент архітектури. Повноцінна система захисту КІІ поєднує програмно-апаратні засоби, організаційні механізми і систематичний контроль.

Організаційний вимір захисту - той, де найчастіше виникають прогалини. Чудовий SIEM нічого не дасть, якщо аналітик безпеки не знає, як реагувати на сповіщення. Розписані процедури реагування, чіткий розподіл відповідальності, актуальні регламенти доступу - все це здається адміністративною рутиною до моменту інциденту. А під час інциденту саме від цього залежить, чи вдасться утримати збиток у прийнятних межах.

Реалізація цих заходів підвищує рівень захищеності і вдосконалює систему управління інформацією - не на папері, а на практиці.

Інженерно-технічні засоби захисту відбираються під конкретний об'єкт, конкретну загрозову модель і необхідний рівень безпеки. Єдиного стандартного набору немає - є принципи вибору.

Загальний технічний мінімум для підприємства такого рівня - криптографічний захист каналів, брандмауери, сегментація мереж та IAM. Але специфіка Монетного двору полягає в тому, що фізичний і кіберзахист

неможливо розглядати окремо. Виробнича зона для друку банкнот має бути ізольована фізично настільки ж ретельно, як і мережево. Тому СКУД, відеоспостереження та охоронна сигналізація - не доповнення до ІТ-безпеки, а її невід'ємна складова.

Захист інформаційних ресурсів не обмежується цифровим простором. Фізичний периметр - серверні кімнати, виробничі зони, архіви - так само потребує захисту.

Оператор КІІ може самостійно розробляти і впроваджувати КСЗІ - але лише за наявності ліцензії на відповідні роботи у сфері ТЗІ. Цей ліцензійний механізм унеможливлює некваліфіковане втручання у критично важливі захисні системи [15].

Конкретний перелік необхідних робіт визначається технічним завданням на проєктування КСЗІ.

За відсутності власних ліцензій на окремі види робіт залучаються співвиконавці з відповідними дозволами. Для систем із криптографічним захистом - ліцензія на криптографію є обов'язковою умовою.

Коли об'єкт отримує першу категорію критичності, він потрапляє під особливий нормативний режим. Постанова КМУ № 367 від квітня 2025 року - не рекомендації, а обов'язкові вимоги: оператор зобов'язаний систематично управляти ризиками, підтримувати операційну стійкість і захищати критичні ресурси. Три завдання взаємопов'язані: збій у будь-якому автоматично тягне за собою порушення в інших двох.

Проте ці вимоги не поширюються на банківські установи, суб'єктів фінансового ринку, платіжні організації та операторів платіжної інфраструктури. Їхня діяльність регулюється через Національний банк України відповідно до норм національного законодавства. Це принципова відмінність.

Монетний двір - нетиповий об'єкт з точки зору кіберзахисту. Є корпоративна мережа з усім стандартним набором: пошта, документообіг, бухгалтерія. І є виробничий ОТ-сегмент - обладнання для виготовлення монет

і банкнот з промисловими контролерами, спеціалізованим ПЗ і технологічними протоколами, які не передбачали кіберзагроз при проектуванні. Обидва рівні пов'язані. Атака на корпоративний сегмент - потенційний вхід до технологічного. Збій у виробничому - пряма загроза для готівкового обігу країни. Масштаб наслідків виходить далеко за межі самого підприємства.

Перший рівень - технічна інфраструктура: серверне обладнання, центри обробки даних, бази даних, автоматизовані робочі місця. Кожен рівень виконує власні функції і має специфічні характеристики, що визначають вимоги до захисту.

Цей рівень вирізняється використанням вузькоспеціалізованого обладнання для контролю фізичних параметрів процесів - датчиків, контролерів, виконавчих механізмів. Відмова навіть одного такого компонента потенційно порушує виробничий процес.

Незначна відмова ПЗ тут означає суттєве порушення виробництва. Тому надійність - базова, а не додаткова вимога.

Другий рівень - логічна архітектура: операційні системи, прикладні програми, спеціалізовані рішення для обробки великих масивів даних. Безперервна робота цих компонентів - умова підтримки виробничого процесу.

Зупинка виробничої лінії Монетного двору - це не корпоративний інцидент. Українська гривня виготовляється тут. Збій навіть на кілька тижнів означає порушення запланованих обсягів емісії, що відчутно на рівні готівкового обігу. Саме тому підприємство і отримало першу категорію критичності - і саме тому вимоги до його кіберзахисту не можуть бути «середніми по галузі».

Рівень захищеності Монетного двору як складної динамічної системи визначається надійністю ПЗ, захищеністю каналів зв'язку, стабільністю технічної інфраструктури і кваліфікацією персоналу. Жоден компонент не є другорядним.

Технічне завдання на КСЗІ встановлює вимоги до складу, порядку розробки та введення в дію засобів захисту. Воно задає межі, в яких проєктується вся система - від вибору технічних засобів до організаційних процедур.

Проєктування КСЗІ здійснюється в межах ТЗ. У ньому також формулюються вимоги до організаційних і фізичних заходів, що доповнюють програмно-технічний комплекс.

У процесі розробки обґрунтовуються проєктні рішення, що забезпечують виконання вимог ТЗ і сумісність між компонентами системи захисту.

Підсумком є комплект робочої та експлуатаційної документації: матеріали для тестувань, пусконалагоджувальних робіт і подальшого адміністрування.

Введення КСЗІ в експлуатацію охоплює підготовку нормативної документації, формування служби захисту, розробку Плану захисту інформації.

Навчання охоплює всі категорії користувачів: адміністраторів, звичайних користувачів і технічний персонал. Необізнаний персонал - ризик, що нівелює будь-які технічні засоби.

На фінальному етапі: комплектування КСЗІ, монтажні роботи, попередні випробування і дослідна експлуатація. Тільки після цього - повноцінне введення в дію.

3.2 Моделювання загроз інформаційній безпеці об'єкта критичної інфраструктури

Моделювання загроз для Монетного двору будується від конкретики. Перший типовий сценарій: цільовий фішинг на співробітника з доступом до виробничих систем. Зловмисник отримує точку входу в корпоративну мережу

- і далі рухається вглиб, шукаючи шляхи до OT-сегменту. Вузлові точки між корпоративною і технологічною мережами - найбільш уразливі місця, де сегрегація має бути найжорсткішою.

Початковий плацдарм у корпоративному сегменті - лише перший крок. Далі зловмисники просуваються до серверних і технологічних сегментів, експлуатуючи вразливості для підвищення привілеїв до адміністраторських. Адже саме адміністраторські права відкривають доступ до виробничих процесів - зокрема до процесів друку або емісії.

Наслідки різняться. Від бракованої продукції до витоку конфіденційних технологічних відомостей про виробництво валюти. Окремий блок моделювання загроз - технічні ризики цілісності й доступності даних: атаки ransomware, здатні дестабілізувати інформаційні системи, та приховані механізми впливу, вбудовані у програмне забезпечення шлюзів і контролерів.

Оцінювання ризиків враховує і ймовірність атак, і масштаб їхнього впливу на фінансову систему держави. Результати аналізу дають науково обґрунтовані підстави для вибору засобів захисту інформації.

Привілейований доступ - під постійним контролем у режимі реального часу. Захист критично важливих процесів - пріоритет. Звіти з кібербезпеки промислових систем (OT/ICS) та фінансового сектору одностайні: ransomware та інсайдерські дії - серед головних загроз для критичних інформаційних інфраструктур.

Згідно зі звітами з кібербезпеки промислових систем (OT/ICS) та фінансового сектору, головною загрозою для критично інформаційних інфраструктур є програми-вимагачі (Ransomware), які здатні зупинити виробничі лінії, та інсайдерські загрози наведено в діаграмі на (рис.3.4).

Рис.3.4 - Діаграма розподілу векторів атак на системи

Два ризики - ransomware і зловживання привілейованим доступом - стоять особняком з огляду на потенційні наслідки. Зашифровані виробничі системи Монетного двору означають зупинку виробництва. Витік технологічних секретів виготовлення банкнот - загрозу підробки і фінансовій безпеці. Без детального сценарного моделювання обидва вектори залишаться недооціненими у плануванні захисту.

Звіти CERT-UA і галузеві дослідження OT/ICS-безпеки за 2023–2024 роки одностайні: ransomware і несанкціоновані дії з привілейованими обліковими записами - серед топ-загроз для промислових об'єктів. Для Монетного двору це не абстрактна статистика - це пряме завдання для пріоритизації захисних заходів.

З огляду на це, подальші розділи зосереджені на трьох напрямах: мережева сегментація як інструмент протидії ransomware, концепція Zero Trust для зниження внутрішніх ризиків та ізоляція промислових контролерів від корпоративного сегмента мережі.

Ідентифікація та систематизація потенційних загроз безпеці відповідно до класичної методології STRIDE, а також визначення відповідних рівнів ризику для системи управління розглянуті в(табл.3.3).

Таблиця 3.3

Загрози для критичної інфраструктури

Категорія загроз	Опис	Рівень ризику
Spoofing (Підміна)	Підміна координат GPS або сигналів.	Високий
Tampering (Втручання)	Зміна параметрів бортового ПЗ або налаштувань ведення вогню.	Критичний
Repudiation (Відмова)	Видалення логів операцій.	Середній
Information Disclosure	Перехоплення зашифрованих каналів зв'язку.	Високий
Denial of Service (DoS)	Перевантаження систем управління.	Високий
Elevation of Privilege	Отримання прав адміністратора в системі тактичного управління.	Критичний

3.3 Розробка комплексу заходів і методів захисту інформації

Монетний двір входить до структури Національного банку України і класифікований як об'єкт КІІ першої категорії. Це означає: будь-які збої в його роботі потенційно мають загальнонаціональні наслідки. Відповідно, модель інформаційної безпеки для нього будується з урахуванням цього масштабу - а не за шаблоном «середнього підприємства».

Така модель покликана сформувати комплексну систему кіберстійкості. Три виміри - нормативно-правове підґрунтя, сучасні технічні засоби захисту та механізми контролю за діями персоналу - вона охоплює одночасно.

Багаторівнева архітектура захисту - стрижень усієї запропонованої моделі. Завдяки їй вдається знизити імовірність несанкціонованого доступу й заблокувати поширення загроз між сегментами. Вона забезпечує фізичне та логічне розмежування між корпоративною мережею й ізольованим технологічним сегментом.

Загрози для об'єктів критичної інфраструктури - принципово різні за природою. Матеріальні ризики - це фізичні та природні небезпеки: пожежі, техногенні аварії, стихійні лиха, епідемії. Їхній наслідок - не лише матеріальні збитки, а й пряме порушення роботи ключових активів та інфраструктурних компонентів. Окремо стоять ризики кібер- та інформаційної безпеки. Вони пов'язані з потенційними атаками на інформаційні й комунікаційні системи, від яких напряму залежить працездатність об'єктів критичної інфраструктури.

Кіберінциденти впливають одночасно на три параметри: безперебійність роботи, доступність сервісів і цілісність даних. Жоден з цих параметрів не можна вважати "менш важливим" для об'єктів критичної інфраструктури - вони взаємопов'язані і взаємозалежні.

Ризики ланцюга постачання заслуговують окремої уваги. Їхні джерела - перебої у забезпеченні технологічним обладнанням чи програмними продуктами, а також дії третіх осіб, здатних дестабілізувати функціонування критичної інфраструктури. Жодна зовнішня залежність не є безризиковою.

З огляду на все перелічене, оператор критичної інфраструктури зобов'язаний вести постійний моніторинг і оцінювання ризиків безпеки. До уваги беруться всі категорії загроз і будь-які інші чинники, що можуть позначатися на функціональності системи, безперервності її роботи, здатності до відновлення та загальній стійкості.

Належна стійкість об'єктів критичної інфраструктури потребує широкого спектра заходів - організаційних і технічних. Одне з першочергових завдань оператора - оцінити потребу у кваліфікованих кадрах. Необхідно чітко визначити, хто саме відповідає за підтримання критично важливих процесів і без кого безперервна робота об'єкта неможлива.

Важливо організувати умови для тривалого перебування персоналу на робочих місцях у кризових ситуаціях. Паралельно слід вибудувати механізм оперативного сповіщення співробітників - без цього будь-яка система безпеки залишатиметься неповною.

Ефективне інформування вимагає попередньо визначених комунікаційних каналів і засобів зв'язку. Саме вони забезпечують швидке оповіщення про надзвичайні ситуації або збої в роботі об'єкта.

Серед складових плану безпеки особливе місце - гарантування територіальної та фізичної стійкості об'єкта.

Для цього передбачається резервний майданчик, де діяльність об'єкта може тривати в разі ураження основного. Принципова вимога - резервна локація має бути розташована на достатній відстані. Одна загроза не повинна одночасно виводити з ладу обидва об'єкти. До плану включаються детальні процедури переведення персоналу, обладнання та критичних ресурсів - аби максимально скоротити час відновлення ключових функцій після аварії. Технічні заходи зі забезпечення стійкості переслідують аналогічну мету: підтримати безперервність інформаційних систем і виробничих процесів.

З цією метою формуються переліки критичних компонентів із прописаними сценаріями їх заміни або відновлення при виході з ладу. Цифрова стійкість при цьому залишається пріоритетним напрямом.

Серед конкретних заходів - регулярне резервування даних, дублювання каналів зв'язку і джерел живлення, автономні системи енергозабезпечення для підтримки найбільш критичних сервісів. Сучасна концепція інформаційної безпеки вимагає інтеграції захисних механізмів вже на етапі проектування - тобто на кожному кроці життєвого циклу розробки інформаційних систем (SDLC).

Логіка проста: заходи безпеки закладаються на початкових стадіях створення системи, а не прикручуються до неї постфактум. Незалежно від обраної моделі розробки - лінійної, ітеративної, спіральної чи швидкої - кожен етап SDLC повинен відповідати вимогам інформаційної безпеки з

урахуванням концепції захисту організації, масштабу проекту та рівня його складності.

Інформаційна безпека - не разова дія. Це безперервний процес, що супроводжує систему від початку й до кінця. Від обґрунтування доцільності її створення аж до виведення з експлуатації усі процеси розглядаються крізь призму актуальних вимог безпеки.

На стадії планування аналізуються потенційні загрози й ризики; паралельно з розробкою програмного забезпечення формується архітектура системи захисту. В режимі промислової експлуатації безперервно ведеться моніторинг вразливостей, здійснюється контроль конфігурацій і оцінюється актуальність загрозового середовища.

Після того як система відпрацьовує свій ресурс, постає завдання безпечного перенесення, архівування або знищення даних. Усі процеси, пов'язані зі створенням і підтримкою системи захисту інформації, вписуються в єдине нормативне та організаційне середовище, що регулює розробку й експлуатацію інформаційних систем в організації.

Такий підхід дозволяє безпечно модернізувати систему відповідно до мінливих потреб, зберігаючи прийнятний рівень ризиків. Оператори критичної інфраструктури зобов'язані своєчасно обслуговувати й ремонтувати обладнання, а також утримувати готовність до оперативної зміни постачальників у разі логістичних збоїв.

Надійність логістики досягається через диверсифікацію постачальників із урахуванням їхньої географії - це усуває критичну залежність від єдиного джерела. При виборі постачальників перевага - вітчизняним виробникам; чинні санкційні обмеження дотримуються обов'язково.

Саме це й підтримує стабільність ланцюгів постачання навіть в умовах криз. Ще один невід'ємний елемент системи безпеки - чітко прописані алгоритми дій у надзвичайних ситуаціях: засоби аварійного зв'язку між підрозділами, порядок взаємодії з державними органами та структура кризового управління. Дієвість цих механізмів перевіряється через регулярні

навчання й аудити систем управління ризиками - не рідше одного разу на три роки.

Системна безпека відрізняється від фрагментарної саме цим: окремі заходи вписані в узгоджену архітектуру, де кожен компонент доповнює інший. Для об'єктів КІІ такий підхід не є опцією - він є умовою виконання нормативних вимог і реальної захищеності.

Циклічна методологія управління ризиками будується на логіці превенції: не реагувати на наслідки, а запобігати самому інциденту й обмежувати його можливі наслідки заздалегідь. Фундамент цього процесу - аналітичне моделювання загроз, завдяки якому ризики розподіляються на прийнятні та неприйнятні.

Для ризиків, що перевищують допустимі порогові значення, розробляються додаткові захисні заходи. Вибір оптимальних рішень здійснюється з огляду на їхню результативність і необхідні витрати ресурсів. Варто врахувати: впровадження нових засобів захисту само по собі може породжувати супутні ризики - і вони також потребують окремого аналізу. Усі отримані результати фіксуються у планах безпеки та забезпечення стійкості об'єктів як складова паспорта безпеки критичної інфраструктури.

Для підтримання достатнього ступеня захищеності запроваджується система безперервного моніторингу та планових перевірок. Оператори КІІ зобов'язані постійно збирати дані про стан критичних систем; відповідність актуальним ризикам перевіряється щонайменше раз на три роки.

Цей процес передбачає:

1. Перевірку даних, зазначених у паспорті безпеки.

2. Прогнозування можливих нових сценаріїв інцидентів та аналіз вразливості систем до сучасних деструктивних методів.

3. Комплексний моніторинг змін у загальній системі управління безпекою.

На типовому об'єкті КІІ - навіть такому специфічному, як Монетний двір - бухгалтерський комп'ютер і виробничий контролер нерідко пов'язані однією

мережевою інфраструктурою. Так склалось роками: спочатку будували виробництво, потім тягнули корпоративну мережу для управлінських потреб, потім з'єднували - бо так зручніше. Результат - IT і OT-сегменти де-факто залежать один від одного, хоча проектувались під цілком різні задачі і з різними вимогами до безпеки.

Антивірус і периметровий файрвол у такій гетерогенній архітектурі - потрібні, але далеко не достатні. Якщо зловмисник пробив корпоративний периметр, він отримує плацдарм для горизонтального переміщення і рано чи пізно дістанеться до OT-сегменту. Zero Trust пропонує іншу логіку: не «все внутрішнє - довірене», а «верифікуємо кожен запит незалежно від його походження». Концептуально просто. Практично - вимагає серйозного перегляду всієї архітектури доступу.

Ключовий результат, який потрібно досягти: об'єкт продовжує виконувати критичні функції навіть у той момент, коли інцидент уже стався і ще не зупинений. Це принципово відрізняє кіберстійкість від класичного «захисту периметра».

Структурно об'єкт КІІ розглядається через три взаємопов'язані рівні - кожен зі своєю логікою захисту і своїми вразливостями.

Перший - корпоративний сегмент: адміністративні мережі, бази даних, робочі місця персоналу і поштова інфраструктура. Тут загрози класичні - фішинг, компрометація облікових записів, витік даних.

Другий - промисловий OT-сегмент: контролери, SCADA, HMI-термінали і виконавчі механізми. Тут загрози фізичні за наслідками - збій у цьому сегменті безпосередньо впливає на виробничий процес.

Третій - суміжна інженерна інфраструктура: системи електропостачання, охолодження, фізичного доступу. Вона не є ні IT, ні OT у класичному розумінні, але стабільна робота перших двох рівнів від неї прямо залежить. Компрометація цього рівня може паралізувати об'єкт без жодного мережевого удару.

Впровадження Zero Trust - не одноразовий проект, а послідовна трансформація через чотири фази. Пропустити будь-яку з них означає отримати неповну систему з гарантованими прогалинами.

Перша фаза - інвентаризація всього: пристроїв, програмного забезпечення, мережевих інтерфейсів, облікових записів. Без актуального реєстру активів решта - стрільба наосліп. Постінцидентні розслідування регулярно виявляють пристрої і облікові записи, про існування яких IT-підрозділ не знав.

Друга фаза - обов'язкова автентифікація для всіх взаємодій між системами. Без винятків і без «службових» обходів через нібито довірені сегменти. Будь-який запит - від будь-якого вузла - проходить перевірку. MFA і криптографічна автентифікація тут є мінімальним стандартом.

Третя фаза - мікросегментація і мінімальні привілеї. Кожен обліковий запис отримує доступ лише до того, що реально потрібно для виконання конкретної функції. Мережеві сегменти IT і OT розділені так, що компрометація одного вузла не відкриває автоматично шлях до інших.

Четверта фаза - безперервний збір телеметрії з усіх рівнів і аналіз у реальному часі. Не раз на тиждень, не «за потреби» - постійно. Тільки так можна виявити аномалію до того, як вона переросте в повноцінний інцидент.

Щоб забезпечити безперервність роботи навіть під час активного інциденту, модель передбачає три функціональні підсистеми - кожна вирішує свою задачу і не дублює інші.

Підсистема моніторингу будує поведінковий профіль мережі через алгоритми машинного навчання. Її задача - помітити атаку на стадії підготовки, а не після того, як вона вже активна. Відхилення від штатного патерну стає тригером для розслідування, навіть якщо сигнатура загрози ще не відома.

Підсистема захисту АСУТП від кіберфізичних атак - найспецифічніша для промислового об'єкта. Вона розділяє критичні комунікаційні шини, підтримує резервні канали і блокує деструктивні команди навіть при

компрометованому обліковому записі оператора. Ключова деталь: блокування відбувається на рівні технологічного протоколу, а не лише мережевого.

Підсистема кіберстійкості - це гарантія «продовження попри», а не «відновлення після». Її задача: не дати зупинитись ключовим функціям об'єкта, поки атака ще активна і не зупинена. Для Монетного двору це означає безперервність виробничого циклу - зупинка емісії навіть на кілька тижнів має наслідки на рівні готівкового обігу в країні.

Теоретична модель забезпечення інформаційної безпеки КІІ

Теоретична модель захисту інформації на об'єктах критичної інформаційної інфраструктури - формалізована концептуальна схема. Вона відображає структуру, складові та взаємозв'язки системи захисту. На відміну від прикладної моделі, що проектується під конкретний об'єкт, теоретична формулює загальні принципи й архітектурні підходи, придатні для будь-якого об'єкта КІІ незалежно від галузевої належності.

Запропонована теоретична модель спирається на три базові властивості, що традиційно визначають рівень інформаційної безпеки: конфіденційність даних (доступ лише для авторизованих суб'єктів), їх цілісність (захист від несанкціонованих змін) і доступність систем (безперервність роботи). До цієї тріади додані два принципи, актуальні саме для КІІ: кіберстійкість як здатність зберігати функціональність під час активного інциденту, і нульова довіра як архітектурний принцип верифікації кожного запиту.

Формально модель описується кортежем:

$$M = (O, T, V, C, R, P),$$

де:

O - множина об'єктів захисту (інформаційні активи, технологічні процеси, канали зв'язку, персонал);

T - множина актуальних загроз (кібератаки, інсайдерські дії, технічні збої, природні катастрофи);

V - множина вразливостей (програмні, апаратні, організаційні);

C - множина контрзаходів (технічних, організаційних, правових);

R - функція оцінювання ризику: R(t, v) = P(t) x I(t, v), де P(t) - ймовірність реалізації загрози t, I(t, v) - величина впливу при вразливості v;

P - політика безпеки, що визначає допустимий рівень ризику R_max та обов'язкові контрзаходи для кожного класу об'єктів.

Запропонована модель будується на чотирьох рівнях захисту, логіка яких відповідає реальному шляху зловмисника від зовнішнього периметра до виробничих систем.

Перший рівень - зовнішній периметр. NGFW фільтрує трафік на вході, IDS/IPS фіксує аномалії, DMZ розміщує публічні ресурси так, щоб їхня компрометація не відкривала пряму дорогу до внутрішньої інфраструктури. Важливо враховувати обмеженість цього рівня: NGFW за замовчуванням не розшифровує зашифрований трафік - це blind spot, який потребує окремого рішення.

Другий рівень - сегментація всередині. Мікросегментація виділяє ізольовані зони IT, OT і DMZ. Трафік між зонами шифрується. Права доступу - мінімально необхідні: не «дати побільше, щоб не заважало», а «рівно стільки, скільки потрібно для конкретної функції». Пробій одного сегменту при такій архітектурі не каскадується на інші.

Третій рівень - ізоляція технологічних процесів. Data diode - фізично однонаправлений шлюз - дозволяє передавати дані з OT-сегменту в корпоративний без жодної технічної можливості зворотного підключення. Паралельно ведеться пасивний моніторинг промислових протоколів Modbus, IEC 104 і DNP3 - він не втручається в технологічний процес, але фіксує будь-яку аномалію в командному трафіку.

Четвертий рівень - організаційний і правовий фундамент. Закон «Про критичну інфраструктуру» і Постанова КМУ № 367 задають нормативний контур. План захисту інформації описує, що і як захищається. Щорічні кібернавчання - не бюрократична вимога: люди мають відпрацювати дії під

час інциденту до автоматизму, а не згадувати про існування плану реагування в момент кризи.

Статична архітектура - лише половина моделі. Друга - цикл реагування: підготовка (плани і навчання до інциденту), виявлення (якомога рання фіксація аномалії), реагування (стримати і локалізувати), відновлення (повернутись до нормального режиму). Для об'єктів І категорії нормативно встановлений показник RTO - не більше 4 годин. Це не ціль для обговорення на нараді - це вимога, яку треба технічно забезпечити і регулярно перевіряти тестовими відновленнями.

Запропонована теоретична модель - масштабована. Вона адаптується до специфіки конкретного сектору КІІ шляхом уточнення множин O, T, V та контрзаходів C. Саме ця гнучкість робить її практично цінним інструментом для планування й оцінювання стану інформаційної безпеки об'єктів критичної інфраструктури.

3.4. Формування архітектури системи забезпечення інформаційної безпеки

В організаціях зі складною інфраструктурою захист неефективно будувати окремо для кожної системи. Один контрольний механізм - наприклад, система управління ідентифікацією або централізований моніторинг - може обслуговувати десятки систем одночасно. Ключова концепція тут - успадкування захисту: нова система «наслідує» заходи безпеки від спільної інфраструктури, не вимагаючи їх повторного впровадження.

Принцип успадкування означає: конкретна система може спиратися на заходи безпеки, що підтримуються іншими підрозділами - навіть якщо ті за неї безпосередньо й не відповідають.

На технологічному рівні перелік таких заходів охоплює захист мережевого периметра, управління доступом, механізми ідентифікації та автентифікації, а також компоненти взаємодії між доменами.

Крім технічних переваг, є і практична економічна логіка. Впровадження, сертифікація і підтримка спільного захисного механізму коштують одного разу. Якщо цей механізм закриває десять систем - витрати розподіляються між ними, замість того щоб множитись на десять.

Керівник, що чітко орієнтується у стратегічних пріоритетах компанії, точніше оцінює ризики і знаходить справді критичні активи. Відповідно - раціональніше розподіляє ресурси при реалізації захисних заходів.

Відповідальних за впровадження і контроль призначають заздалегідь. Зазвичай це власники інформаційних ресурсів, фахівці із захисту даних та представники зацікавлених підрозділів.

За призначенням і статусом заходи безпеки поділяються на конкретні та гібридні. Такий поділ спрощує розподіл відповідальності між підрозділами й розподіл ресурсів.

Гібридний захід поєднує загальноорганізаційні елементи - наприклад, корпоративний план безперервності - з компонентами, налаштованими під конкретну систему. За конкретні ж заходи відповідають власники відповідних систем та їхній персонал.

Статус заходу - спільний, конкретний чи гібридний - не є постійним. Він формується з огляду на реальні умови і може змінюватись, навіть якщо документація цього поки не відображає. Конкретний розподіл функцій у гібридних заходах залежить від структури організації, стека технологій і обраної стратегії.

Захід, спочатку орієнтований лише на одну систему, може набути статусу спільного, якщо інша система починає залежати від нього або успадковує його для власного захисту.

Статус визначається через аналіз залежностей: якщо один механізм захисту задіяний кількома компонентами - він кваліфікується як спільний. Такий підхід підвищує ефективність при проєктуванні й аудиті систем захисту.

Такий підхід дає більшу гнучкість при налаштуванні і полегшує узгоджене впровадження єдиних політик безпеки по всій інфраструктурі.

При організації віддаленого доступу до промислових систем - зокрема для технічного обслуговування - MFA є обов'язковою. Всі підключення відбуваються лише через захищені VPN. На межах між сегментами мережі розгортаються спеціалізовані засоби контролю трафіку.

Попри зовнішню простоту концепції, її реальне втілення вимагає ретельного планування та взаємодії між усіма підрозділами, задіяними у захисті інформації. Детальніше це відображено у (табл. 3.4).

Таблиця 3.4

Заходи забезпечення кіберстійкості ІТС

Напрямок стійкості	Загрози	Конкретні заходи безпеки
Мережева архітектура	Атаки на виробничу лінію з Інтернету, поширення Malware	Сувора сегментація IT (корпоративної) та OT (технологічної) мереж.
Захист даних та Криптографія	Витік макетів банкнот, Крадіжка сертифікатів	Впровадження DLP-Систем на всіх робочих Станціях. Використання Апаратних модулів.
Управління доступом (IAM)	Інсайдери, використання чужих перепусток	Сувора багатофакторна (MFA) та біометрична Автентифікація як для IT-систем, так і для Фізичного доступу.
Моніторинг (SOC/SIEM)	Приховані APT-атаки, Відкладені кіберзагрози	Цілодобовий моніторинг подій безпеки.

Централізоване управління обліковими записами і груповими політиками безпеки на великому об'єкті - не зручність, а необхідність. Без нього підтримати узгоджені налаштування безпеки на сотнях робочих станцій практично неможливо. Глибокий аналіз пакетів між IT і OT сегментами виконує роль останнього фільтра перед промисловими системами: блокує

команди, що не відповідають профілю штатного трафіку, ще на мережевому рівні.

Попри удавану нескладність самої концепції, її реальне втілення вимагає детального планування та міжвідомчої координації між усіма структурами, задіяними у забезпеченні кібербезпеки.

Кожен етап ЖЦ інформаційної системи включає конкретні завдання, що групуються у функціональні блоки.

Для кожного блоку визначаються мета, вхідні й вихідні дані, а також конкретні ролі і відповідальні особи.

На практиці інформаційну безпеку нерідко «додають» до вже готової системи - і отримують латаний захист з численними прогалинами. Правильний підхід - вбудовування вимог безпеки в кожен етап: від технічного завдання і проектування до щоденної операційної роботи і поступового виведення системи з експлуатації.

Це дає змогу підтримувати засоби захисту актуальними навіть за зміни загроз і потреб. При виведенні системи з експлуатації першочергове завдання - мінімізувати ризики при закритті та правильно врегулювати питання, пов'язані з ресурсами й обладнанням.

Особливу увагу приділяють збереженню та захисту даних, що оброблялися під час роботи системи. Вони або переносяться у нове середовище, або архівуються. Всі ці операції виконуються відповідно до чинного законодавства й внутрішніх регламентів.

Навіть після відключення системи апаратне і програмне забезпечення, а також самі дані потрібно захищати від несанкціонованого доступу - доки не завершено всі процедури ліквідації.

Це запобігає витоку даних і зловживанню технічною інфраструктурою. Стан системи в штатному режимі регулярно оцінюється і за потреби проходить повторну авторизацію.

При ліквідації головне завдання змінюється. Замість оцінки стану - безпечне завершення роботи та комплексне врегулювання питань безпеки при виведенні системи з експлуатації.

Бажано задокументувати умови функціонування системи та особливості її адміністрування. Цей накопичений досвід стає корисним при проєктуванні систем наступного покоління.

Перенесення даних у нову систему виконується паралельно з контрольованим закриттям попередньої. Вимоги безпеки дотримуються на всіх етапах без винятку.

Кожен масив даних або інтегрується у нове середовище, або надійно архівується. Оскільки системи постійно оновлюються, заходи захисту також мають підлаштовуватися - нові технології, зміни архітектури, нові загрози. Безпека - це процес, а не разовий результат.

Висновки до розділу 3

Вибір Монетного двору України як модельного об'єкта для третього розділу не є довільним. По-перше, це I категорія критичності - найвища у вітчизняній класифікації, що означає найжорсткіші нормативні вимоги. По-друге, специфіка об'єкта - суміщення корпоративної IT-інфраструктури з виробничим OT-сегментом - дозволяє продемонструвати підходи до захисту в умовах саме такої гетерогенної архітектури.

Для розробки моделі захисту ключову роль відіграли дві особливості об'єкта. Перша - гетерогенна структура: поряд зі стандартною IT-інфраструктурою (фінансові системи, бази даних) на підприємстві функціонує виробничий OT-сегмент із контролерами поліграфічного та емісійного обладнання.

Друга ключова особливість - нормативний контекст. Діяльність Монетного двору підпадає під вимоги Постанови КМУ № 367 від 19 квітня

2025 року щодо управління ризиками безпеки для об'єктів першої категорії критичності.

Для кожної з виявлених загроз сформовано відповідні контрзаходи, що склали основу запропонованої моделі захисту. В її фундаменті - три принципи.

Перший передбачає жорстку сегментацію мережі з ізоляцією IT- і OT-сегментів через застосування односпрямованих шлюзів (data diode).

Другий реалізує концепцію Zero Trust - перевірку автентичності кожного доступу і запиту без жодних винятків.

Третій принцип охоплює багаторівневу архітектуру захисту із резервуванням критично важливих компонентів.

Розділ 4 ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

4.1. Методика оцінювання ефективності системи захисту інформації

Будь-яка модель захисту без вимірюваних показників - це декларація. Є брандмауер - і що? Запущений SIEM - добре, але як зрозуміти, що він дійсно виявляє загрози, а не просто збирає логи? Четвертий розділ відповідає саме на це питання: як виміряти, чи захист функціонує так, як задумано.

Для оцінки ефективності обрано NIST CSF 2.0. Версія 2024 року суттєво доопрацьована: вперше детально враховано специфіку OT/ICS-середовищ, що безпосередньо стосується Монетного двору з його виробничим сегментом. Додатковий аргумент: CISA активно використовує CSF при роботі з операторами КІІ - значить, фреймворк пройшов перевірку в реальних умовах, а не лише в академічному середовищі. Нарешті, понятійна база CSF сумісна з NIS2, що спрощує одночасне дотримання і американських, і європейських методичних підходів.

Адаптація CSF до українського контексту має конкретний зміст. П'ять функцій фреймворку прив'язуються до вимог Постанови КМУ № 367 і статей Закону «Про критичну інфраструктуру» - так, щоб виконання нормативної вимоги одночасно закривало відповідний елемент CSF. Поєднання NIST CSF з ISO/IEC 27001 і NIST SP 800-82 для OT-середовища дає методичну основу, яка визнається і міжнародними аудиторами, і вітчизняними перевіряючими органами.

П'ять функцій циклу - не просто перелік. Ідентифікація без наступного захисту безглузда. Захист без виявлення - захист від відомого, але не від нового. Виявлення без плану реагування - сигналізація без пожежної команди. Реагування без відновлення - гасіння пожежі без відбудови. Лише у комплексі

ці п'ять функцій забезпечують те, що називають системним управлінням безпекою.

Але виокремлені рівні зрілості - не умовність. Вони відображають реальні послідовні стадії розвитку системи управління ризиками. Шлях від початкового, несистематизованого підходу до повністю адаптивної моделі на основі безперервного відстеження загроз вимагає цілеспрямованих зусиль і послідовного вдосконалення захисних механізмів.

Визначити «достатній» рівень захищеності складніше, ніж здається. Занадто жорсткий захист - витрати без пропорційної вигоди. Недостатній - реальні ризики. Баланс шукається через профіль захищеності: набір цільових показників, що відображає, яким має бути стан безпеки з огляду на нормативні вимоги, актуальні загрози та наявний бюджет. Для Монетного двору цей профіль будується навколо вимог постанови КМУ № 367 і реальних векторів атак, задокументованих у звітах CERT-UA.

Проте профіль рівня захищеності корисний одразу в кількох вимірах. Він дозволяє порівнювати фактичний стан інформаційної безпеки із цільовим і виявляти пріоритетні напрями для вдосконалення. Профілі також придатні для внутрішнього самооцінювання або обміну досвідом між організаціями. Управління ризиками - безперервний процес: ідентифікація, оцінка, опрацювання. Щоб реалізувати його ефективно, організація мусить розуміти ймовірність матеріалізації загроз і наслідки їхнього настання.

Додаткову складність вносить недостатня формалізація розуміння власної ризикостійкості. Воно дозволяє ухвалювати обґрунтовані рішення щодо інвестицій у захист і раціонального розподілу ресурсів. Спираючись на отримані дані, визначається допустимий рівень ризику і встановлюються пріоритети щодо конкретних заходів захисту.

Запровадження системи управління ризиками дає можливість не лише оцінювати дієвість наявних засобів захисту, а й своєчасно вносити корективи. Залежно від характеру ризику та його впливу на критично важливі сервіси,

організація може обирати різні стратегії: зниження, передання, уникнення або прийняття ризику.

Динамічне управління ризиками - не теоретична конструкція. Загрозове середовище змінюється: нові вектори атак, нові вразливості, нові актори. Система управління, яка не адаптується до цих змін, швидко застаріває і залишає критичні прогалини. Регулярний перегляд ризиків і заходів захисту - обов'язковий, а не бажаний елемент.

Результативність запропонованої технічної архітектури - насамперед у зменшенні ймовірності успішних атак на ключові сегменти мережевої інфраструктури. Жорстка сегментація мереж, принцип Zero Trust і багатофакторна автентифікація разом суттєво скорочують потенційну поверхню атак. Інтелектуальні системи моніторингу, своєю чергою, пришвидшують виявлення аномалій - тобто той момент, коли реагування ще може запобігти серйозним наслідкам.

Аналіз ризиків показує: перехід від розрізнених заходів безпеки до багаторівневої моделі захисту переводить більшість типових ризиків до категорії прийнятних. Паралельно забезпечується дієвий нагляд за діями користувачів із розширеними привілеями - а це пряма гарантія захищеності критично важливих систем.

Ефективність організаційного компонента системи управління безпекою - передусім питання раціонального розподілу ресурсів і чітко прописаних управлінських політик. Групування захисних заходів на загальні, гібридні та спеціалізовані категорії прямо впливає на зниження витрат при впровадженні й підтриманні системи. Уніфіковані рішення для кількох інформаційних систем скорочують фінансові витрати на розробку й сертифікацію та підвищують загальну результативність. Залучення вищого керівництва до вибору заходів безпеки - не формальність. Це необхідна умова відповідності захисних політик стратегічним цілям організації.

Ефективність системи оцінюється на основі таких показників, як кіберстійкість та безперебійність бізнес-процесів.

Резервний майданчик, розташований щонайменше за 50 кілометрів від основної локації, - не надмірність, а базова вимога. Разом із кризовими системами зв'язку і регулярним резервним копіюванням він забезпечує оперативне відновлення критично важливих функцій у межах термінів, встановлених для об'єктів І категорії критичної інфраструктури. Планова переоцінка ризиків не рідше одного разу на три роки - ще один обов'язковий елемент, що дозволяє підтримувати актуальність системи захисту в умовах постійної еволюції кіберзагроз.

Запропонована модель охоплює три виміри: технічний (архітектура захисту, засоби моніторингу), організаційний (ролі, процедури, навчання) і управлінський (критерії оцінки, цикл перегляду). Жоден з них не є самодостатнім - лише у взаємодії вони формують реально функціонуючу систему.

Оцінювання системи захисту в умовах КІІ не зводиться до одного підходу. Кількісний аналіз дає цифрові показники ризиків, якісна перевірка - картину відповідності на організаційному і технічному рівнях. Жоден з них окремо повної картини не дає.

Ключове питання: чи здатні реалізовані заходи нейтралізувати ризики, виявлені при моделюванні загроз. Підсумкова оцінка формується за трьома складовими - технічна надійність, якість управління і здатність до відновлення після інцидентів.

Результати оцінювання визначають рівень зрілості системи управління ризиками. Цей рівень переглядається щонайменше раз на три роки за участю уповноважених держорганів. Такий механізм підтримує актуальність документації і дозволяє своєчасно виявляти потенційні інциденти.

Виміряти ефективність системи захисту - завдання складніше, ніж виглядає. MTTD (час до виявлення загрози), RTO (час відновлення), відсоток покриття активів контрзаходами - метрики є, але самі по собі вони нічого не означають без порогових значень і регулярного порівняння. Стратегія

оцінювання потрібна не для звітування - для виявлення деградації захисту до того, як стається інцидент.

4.2. Аналіз результатів застосування запропонованих методів захисту

З економічної точки зору поєднання спільних і гібридних заходів розподіляє витрати між підрозділами. Механізм успадкування дає системам можливість використовувати централізовані рішення - без дублювання ресурсів.

Залучення керівництва до рішень щодо захисту - це не формальність. Це механізм, що узгоджує інвестиції в безпеку зі стратегічними пріоритетами. Результати стратегічного аналізу свідчать про позитивний вплив на безпеку ланцюгів постачання.

Орієнтація на вітчизняних виробників і відмова від підсанкційних суб'єктів - це не декларація. Такий підхід реально знижує ризик вразливостей у ланцюгу постачання і полегшує своєчасне обслуговування.

Трирічний аудит за участю держорганів - це не звітна формальність. Механізм гарантує, що засоби захисту відповідають реальним загрозам, а не тим, що існували три роки тому.

Реалізація описаних заходів дає змогу побудувати прозору й стабільну систему управління безпекою. Тільки така система здатна реально мінімізувати ризики і обмежити руйнівний вплив кіберзагроз на КІІ.

Мета методики оцінювання - отримати узгоджені й відтворювані результати. Це поглиблює розуміння ризиків для операцій та активів організації.

Для практичної реалізації методики розробляються алгоритмічні схеми і таблиці відповідно до Каталогу заходів захисту НД ТЗІ. Ці документи визначають порядок відбору засобів забезпечення безпеки.

4.3. Рекомендації щодо підвищення рівня кібербезпеки об'єктів критичної інфраструктури

Класична проблема безпеки КІІ - її «прикручують» до вже готової системи. Спочатку проектують функціонал, потім зупиняє аудит і починається виправлення архітектурних рішень, прийнятих роки тому. Ціна помилки на пізніх стадіях SDLC не просто вища - вона часом робить нормальний захист практично нереалізованим без повної перебудови системи. Вимога одна: безпека закладається в технічне завдання до початку розробки, не після.

Модель розробки підбирається під конкретну систему. Для нескладного локального рішення достатньо лінійного підходу: зафіксували вимоги - розробили - впровадили. Але для складних систем, де вимоги уточнюються в процесі, лінійна модель ризикована: вимоги безпеки, недостатньо деталізовані на початку, виявляться на фінальному етапі, коли виправити архітектуру вже дорого.

Ітеративний підхід для КІІ має очевидну перевагу: безпека перевіряється на кожному циклі, а не лише наприкінці. Це особливо важливо для об'єктів, де ціна прогалини в захисті вимірюється не у гривнях, а в доступності критичних сервісів.

Перша фаза SDLC - найдешевша для виправлення і тому найважливіша для закладення вимог безпеки. Саме тут формується модель загроз для майбутньої системи: хто може атакувати, яким чином, які активи під захистом. Вимоги безпеки, що виникають з цього аналізу, стають частиною технічного завдання - на рівних правах з функціональними.

Фаза розробки або придбання - точка, де архітектурні рішення безпеки стають незворотними. Вибір протоколів, рівнів автентифікації, механізмів шифрування - все це фіксується тут. Перед введенням в експлуатацію система проходить перевірку відповідності вимогам безпеки: для об'єктів КІІ І категорії це включає незалежний аудит конфігурацій і тестування на проникнення у відтвореному середовищі.

Операційна фаза - найтриваліша і найнебезпечніша з точки зору «дрейфу безпеки». Нові вразливості з'являються постійно. Конфігурації змінюються. Персонал плинний. Система, яка відповідала вимогам безпеки при введенні в експлуатацію три роки тому, може мати суттєві прогалини сьогодні - якщо регулярних переоцінок не проводилось. Операційний ритм: щорічна інвентаризація активів, переоцінка ризиків не рідше разу на три роки, безперервний моніторинг вразливостей.

Виведення системи з експлуатації - фаза, якій найчастіше приділяють найменше уваги. Незашифровані архіви з даними, невидалені облікові записи з адміністраторськими правами, обладнання, що «тимчасово» залишилось підключеним - стандартний результат недбалого закриття системи. Для об'єктів КІІ тут два завдання: безпечна передача або підтверджене знищення даних і документування накопиченого досвіду адміністрування для систем наступного покоління.

Проте такі системи нерідко оновлюються або замінюються сучаснішими версіями - а це може породжувати нові ризики, які потребують відповідної уваги та захисних заходів.

Тому політики безпеки потрібно постійно оновлювати й адаптувати до змін у системі. Окрему увагу слід приділити збереженню відомостей про середовище функціонування та особливостей адміністрування.

Ця інформація може стати в нагоді при розробці майбутніх систем і плануванні заходів безпеки для них. У рамках практичного виконання заходів важливо регулярно здійснювати інвентаризацію інформаційних, програмних і апаратних ресурсів - не рідше одного разу на рік. Доцільно створити або призначити спеціалізований підрозділ з питань кібербезпеки, підпорядкований безпосередньо керівництву, а також налагодити ефективну взаємодію між ІТ-службами та підрозділами захисту інформації.

Необхідно регулярно сканувати системи для виявлення вразливостей, проводити незалежний аудит безпеки та висувати чіткі вимоги до кіберзахисту для постачальників і партнерів. До пріоритетних заходів належить

впровадження MFA, надійної парольної політики, мережевої сегментації та принципу мінімальних привілеїв. Слід також забезпечити систематичне резервне копіювання даних, використання шифрування під час передачі інформації, захист електронної пошти від phishing-атак та підвищення поінформованості персоналу шляхом регулярних навчань з інформаційної безпеки. Потребує організації й безпечне зберігання журналів подій для аналізу та розслідування інцидентів.

Окрім цього, необхідно передбачити механізми виявлення несанкціонованих входів з автоматичним блокуванням облікових записів, а також забезпечити контроль над використанням зовнішніх носіїв і каналів VPN-доступу. У разі виникнення кіберінцидентів критично важливим є своєчасне інформування відповідних структур реагування: CERT-UA, Ситуаційного центру СБУ або SOC-центрів.

Окремо варто задіяти сучасні методи виявлення вразливостей - Bug Bounty-програми та автоматизовані сканери. Інтеграція заходів безпеки в усі стадії SDLC разом із комплексним упровадженням технічних, організаційних і процедурних рішень - необхідна умова дієвої системи захисту.

Це дозволить забезпечити стійкість критичної інфраструктури та мінімізувати ризики кіберзагроз.

4.4. Практичні аспекти впровадження запропонованих рішень

Практичне впровадження запропонованих рішень на базі Монетного двору як об'єкта критичної інфраструктури вимагає скоординованої взаємодії між технічними підрозділами, службою інформаційної безпеки та вищим керівництвом.

Практика розслідування кіберінцидентів на промислових об'єктах раз по раз виявляє одну й ту саму проблему: технічний підрозділ і служба безпеки діяли ізольовано. Координація між ними - не приємний бонус, а необхідна

умова виживання системи під час реального інциденту. Чіткий розподіл ролей має бути зафіксований у документах і відпрацьований на регулярних навчаннях, а не лише декларований.

Основними з них є такі:

1. Проєктувальник відповідає за розроблення всеосяжної архітектури безпеки та захисту інформації, поєднуючи функції системного архітектора і спеціаліста з кібербезпеки. За необхідності він може залучати зовнішніх експертів для вирішення складних завдань.

2. Постачальник засобів і послуг захисту несе відповідальність за реалізацію технічних рішень, надання інженерної підтримки та поставку необхідних засобів захисту. Ця діяльність також допускає залучення спеціалізованих сторонніх організацій.

3. Адміністратор безпеки виконує поточні операційні завдання, зокрема моніторинг систем, адміністрування та підтримання інформаційної безпеки. Його обов'язки передбачають постійний контроль за станом захищеності системи.

4. Незалежний оцінювач, який діє на договірній основі, здійснює аудит та оцінку дієвості впроваджених заходів із забезпечення безпеки, гарантуючи об'єктивність перевірок.

5. Орган авторизації - структура, що ухвалює остаточне рішення щодо введення системи в експлуатацію та надає дозвіл на її використання після перевірки рівня безпеки.

На практичному рівні першочергове завдання - запровадження процедур ідентифікації та MFA для користувачів і адміністраторів. Ці процедури мають бути інтегровані в загальну парольну політику організації і забезпечувати унікальну ідентифікацію кожного користувача або процесу, що діє від його імені. Особливу увагу необхідно приділити впровадженню MFA для привілейованих облікових записів та каналів віддаленого доступу.

Один із факторів підтвердження особи має генеруватися окремим пристроєм, незалежним від основної системи. Паралельно слід застосовувати

принцип мінімальних привілеїв, що обмежує права доступу користувачів виключно тими, які необхідні для виконання їхніх функцій.

Кількість привілейованих облікових записів підлягає суворому обмеженню. Адміністраторам рекомендується користуватися звичайними обліковими записами при виконанні завдань, не пов'язаних із безпекою чи налаштуванням системи.

На організаційному рівні пропонується заснування окремого підрозділу інформаційної безпеки або призначення спеціально відповідальної особи, що безпосередньо підпорядковуватиметься керівнику об'єкта.

Так само потрібно чітко визначити порядок взаємодії між IT-підрозділом і службою кіберзахисту, передусім - у частині реагування на інциденти. Відправний пункт у побудові системи - розроблення ключової нормативної документації.

До її складу мають входити концепція та програма інформаційної безпеки, опис системи й оцінка її критичності, політика безпеки і плани реалізації захисних заходів.

Окрім того, необхідно передбачити укладання договорів із постачальниками, в яких чітко прописуватимуться зобов'язання щодо повідомлення про інциденти безпеки та виявлені вразливості. Слід також врегулювати питання заміни програмного й апаратного забезпечення - передусім у разі використання рішень з країн-агресорів або від підсанкційних компаній.

У технічному плані необхідно забезпечити сегментацію мережевої інфраструктури як на фізичному, так і на логічному рівні. Обмін даними між сегментами має відбуватися через захищені вузли доступу - зокрема bastion host, jump server, DMZ або автентифіковані проксі-сервери.

За замовчуванням усі мережеві підключення мають бути заблоковані, якщо вони не дозволені явно. Важливо також регулярне оновлення документації мережевої інфраструктури, що має містити топологічні схеми, схеми підключень і таблиці маркування кабельної мережі.

Резервне копіювання критичних систем та інформаційної документації слід здійснювати зі збереженням файлів у захищених ізольованих сховищах або вогнестійких контейнерах, не підключених до загальної інфраструктури.

План резервного копіювання необхідно ретельно формалізувати та регулярно тестувати для підтвердження його ефективності.

Сукупність запропонованих заходів забезпечить дієву реалізацію системи інформаційної безпеки на об'єктах критичної інфраструктури та дозволить істотно підвищити їх стійкість перед сучасними кіберзагрозами. Розглянутий комплекс заходів і підходів формує всеосяжну й практичну модель захисту, що враховує як організаційні, так і технічні виміри. Реалізація принципів багаторівневого захисту, сегментації мережевої інфраструктури, мінімізації привілеїв доступу та застосування MFA суттєво знижує ризик несанкціонованого проникнення та пошкодження критичних систем.

Чіткий розподіл завдань і відповідальності між учасниками процесу підвищує результативність і контрольованість у сфері інформаційної безпеки.

Ключове досягнення - інтеграція захисних заходів на кожній стадії життєвого циклу інформаційних систем: це дозволяє не лише реагувати на потенційні загрози, а й передбачати їх і мінімізувати до їхньої реалізації.

Резервування, кризове планування і регулярний аудит - три елементи, що найчастіше виявляються «паперовими» на реальних об'єктах. Резервний майданчик, про який не знає ніхто, крім автора проекту; план відновлення, якого ніхто не читав; аудит, останній раз проводився п'ять років тому - типова картина.

Запропонована модель передбачає конкретні строки і відповідальних для кожного з цих елементів, а не просто рекомендує їх наявність.

Висновки до розділу 4

Оцінка ефективності захисту - не формальна глава для «повноти роботи». Без вимірюваних критеріїв неможливо зрозуміти, чи модель дійсно функціонує або лише виглядає добре на папері.

Саме тому четвертий розділ зосереджений не на описі заходів, а на способах перевірки їхньої дієвості.

Три напрями оцінювання - не довільна структура. Технічна стійкість архітектури перевіряє, чи реалізовані технічні рішення.

Ефективність організаційного управління - чи знають люди, що робити. Здатність до відновлення - чи вкладається система у нормативні терміни. Без перевірки за всіма трьома напрямами оцінка є неповною.

Метрики конкретні: MTTD (середній час від початку інциденту до виявлення), RTO (час повного відновлення), відсоток активів, охоплених контрзаходами, і рівень зрілості процесів управління ризиками. Для кожної метрики визначене цільове значення - для об'єктів I категорії RTO нормативно обмежений 4 годинами.

Впровадження багаторівневої моделі вирішує головну проблему - усуває розриви між засобами захисту, що діяли ізольовано. Результати: зменшення поверхні атаки, прискорення виявлення аномалій і скорочення часу відновлення до нормативних показників. Для операторів об'єктів I категорії пріоритетний мінімум: Security SDLC при розробці нових систем, інвентаризація активів щорічно, незалежний аудит кожні три роки згідно з каталогом НД ТЗІ, Bug Bounty для пошуку вразливостей і обов'язкова взаємодія власного SOC з CERT-UA.

Постінцидентні звіти CERT-UA і міжнародні дослідження OT/ICS-безпеки говорять одне й те саме: більшість успішних атак на КІІ відбулась не через відсутність дорогих засобів захисту, а через базові прогалини -

непатчений сервер, адміністраторський пароль «за замовчуванням», відсутній MFA на привілейованому акаунті. Жодна модель не виправить це автоматично. Потрібна система: регулярна перевірка, чіткі метрики відповідності і невідворотний цикл перегляду захисту. Саме це і пропонується в даній роботі.

Запропоновані методики і технологічні рішення спрямовані на підвищення кіберстійкості об'єктів КІІ. Для Монетного двору - як об'єкта першої категорії критичності - їх впровадження означає скорочення поверхні атаки, прискорення виявлення аномалій і скорочення часу.

ВИСНОВКИ

Кваліфікаційна робота послідовно розкрила чотири блоки: теоретичні засади захисту КІІ, методи і технології кіберзахисту, модель захисту для конкретного об'єкта (Монетний двір України, І категорія критичності) та методику оцінки ефективності цієї моделі. Нижче - підсумкові результати по кожному з них.

Технологічний аналіз показав: SIEM, IDS/IPS і SOC-центри залишаються ядром сучасного кіберзахисту КІІ. Шифрування каналів TLS 1.3/IPSec та концепція Zero Trust разом закривають основний вектор атак - компрометацію облікових даних і бічне переміщення в мережі. При цьому ШІ-інструменти виявлення аномалій не замінюють, а підсилюють ці базові засоби.

Технологічний зріз захисту охоплює не лише традиційні IT-інструменти, але й спеціалізовані рішення для OT-середовища: DPI для промислових протоколів, honeypot-системи та засоби виявлення аномалій у SCADA.

SIEM, IDS/IPS, SOC, методам шифрування, архітектурній концепції Zero Trust та інструментам виявлення аномалій на основі методів штучного інтелекту.

Застосована методологія STRIDE дала змогу систематизувати загрози для Монетного двору: програми-вимагачі та зловживання привілейованим доступом виявились двома основними ризиками - що підтверджується даними CERT-UA і міжнародними звітами з OT/ICS-безпеки. Розроблена модель захисту будується на трьох принципах: жорстка IT/OT-сегментація, Zero Trust і багаторівнева архітектура із резервуванням критичних компонентів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 10.05.2026).
2. Звіти CERT-UA (Computer Emergency Response Team of Ukraine) про 105 кіберінциденти. 2024-2025. URL: https://cert.gov.ua/article/17696 (дата звернення: 09.05.2026).
3. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive), 2022. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 13.05.2026).
4. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 16.05.2026).
5. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 2.0, 2024. URL: https://www.nist.gov/cyberframework (дата звернення: 20.05.2026).
6. CISA. Cybersecurity Best Practices for Industrial Control Systems. URL: https://www.cisa.gov (дата звернення: 23.05.2026).
7. Network and information security: proposal for a european policy approach (2014) URL: https://www.steptoe.com/a/web/485/811.pdf (дата звернення: 05.04.2026).
8. IBM Security. SIEM and SOC Technologies Overview, 2024. URL: https://www.ibm.com/topics/siem (дата звернення: 07.04.2026).
9. IBM Security. SIEM and SOC Technologies Overview. URL: https://www.ibm.com/topics/siem (дата звернення: 25.04.2026).
10. Про основні засади забезпечення кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 23.05.2026).

11. NIST SP 800-82 Rev.3 Guide to Operational Technology (OT) Security. National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final (дата звернення: 22.05.2026).

12. Bosch Security Systems. Building Integration System (BIS). Technical Documentation, 2024. URL: https://www.boschsecurity.com (дата звернення: 20.05.2026).

13. BIS Manual. URL:https://media.boschsecurity.com/fs/media/pb/media/extranet/bosch_access_control_and_bms/bis_operation_guide_en.pdf (дата звернення: 17.05.2026).

14. Secure Access Control Systems | Inner Range Solutions. Inner Range. URL: https://www.innerrange.com (дата звернення: 20.05.2026).

15. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/367-2025-п#Text (дата звернення: 17.05.2026).

16. Державна служба спеціального зв’язку та захисту інформації України. щодо стану кібербезпеки в Україні, 2024–2025. URL: https://cip.gov.ua/ua (дата звернення: 07.05.2026).

17. Деякі питання об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: http://zakon.rada.gov.ua/laws/show/1109-2020-п/ed20201009#n22 (дата звернення: 19.05.2026).

18. Деякі питання паспортизації об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/818-2023-п#Text (дата звернення: 11.05.2026).

19. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту. Офіційний вебпортал

парламенту України. URL: https://zakon.rada.gov.ua/laws/show/984_002-08/ed20081208#n41 (дата звернення: 18.05.2026).

20. Закон України «Про інформацію», від 02.10.1992 № 2657-XII.URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.05.2026).

21. Кримінальний процесуальний кодекс України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 12.05.2026).

22. Про затвердження Кодексу системи передачі. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/v0309874-18/ed20180314#n72 (дата звернення: 19.05.2026).

23. Про затвердження Методики та Критеріїв і показників оцінки стану захищеності об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/z0375-25#Text (дата звернення: 20.05.2026).

24. Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/rada/show/v0023519-21#Text (дата звернення: 18.05.2026).

25. Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/415-2023-п#Text (дата звернення: 10.05.2026).

26. Про затвердження Порядку проведення моніторингу рівня безпеки об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/821-2022-п#Text (дата звернення: 20.05.2026).

27. Про захист інформації в інформаційно-комунікаційних системах.

Офіційний вебпортал парламенту України.URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 11.05.2026).

28. Про Концепцію (основи державної політики) національної безпеки України. Офіційний вебпортал парламенту України.URL: https://zakon.rada.gov.ua/laws/show/3/97-вр/ed19980611#Text (дата звернення: 13.05.2026).

29. Про Концепцію Національної програми інформатизації. Офіційний вебпортал парламенту України. URL:https://zakon.rada.gov.ua/laws/show/75/98-вр (дата звернення: 09.04.2026).

30. Про реалізацію експериментального проекту щодо нарощування спроможностей радіоелектронного прикриття об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/881-2025-п#Text (дата звернення: 19.05.2026).

31. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 22.05.2026).

32. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України". Офіційний вебпортал парламенту України. URL:http://zakon5.rada.gov.ua/laws/show/287/2015. (дата звернення: 22.05.2026).

33. Прогноз кіберзагроз 2024 - H-X Technologies. H-X Technologies. URL: https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua (дата звернення: 22.05.2026).

34. Стратегія кібербезпеки України. Указ Президента України №96/2021 від 26 серпня 2021 р. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/96/2021#Text (дата звернення: 22.05.2026).

35. Audit log. Zabbix: The enterprise-class open source observability solution. URL: https://www.zabbix.com/documentation/current/en/cloud/audit_log(дата звернення: 20.05.2026).

36. Cisco Systems. Zero Trust Security Model Overview. URL: https://www.cisco.com/c/en/us/products/security/zero-trust.html (дата звернення: 29.04.2026).

37. Deploy Zabbix in the cloud. Zabbix: The enterprise-class open source observability solution. URL:https://www.zabbix.com/documentation/current/en/cloud/quickstart (дата звернення: 16.05.2026).

38. ENISA. Good Practices for Security of Internet of Things in the Context of Smart Manufacturing. URL: https://www.enisa.europa.eu (дата звернення: 23.05.2026).

39. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 23.04.2026).

40. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls. URL: https://www.iso.org/standard/27002 (дата звернення: 23.04.2026).

41. Monitor Windows with Zabbix agent. Zabbix: The enterprise-class open source observability solution. URL:https://www.zabbix.com/documentation/7.0/en/manual/quickstart/monitor_windows (дата звернення: 21.05.2026).

42. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 21.05.2026).

43. Secure Your Access. Zero Trust at Scale. Cisco. URL: https://www.cisco.com/c/en/us/products/security/zero-trust.html (дата звернення: 13.04.2026).

44. VMware. Virtualization and Infrastructure Security Guidelines. URL: https://www.vmware.com/security.html (дата звернення: 27.04.2026).

45. Web monitoring items. Zabbix: The enterprise-class open source observability solution. URL:https://www.zabbix.com/documentation/current/en/manual/web_monitoring/items (дата звернення: 20.05.2026).