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: “ТЕХНОЛОГІЇ ЗАПОБІГАННЯ І ПРОТИДІЇ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УСТАНОВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Нікіта БАРАНОВ

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Нікіта БАРАНОВ

Керівник:
д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____” _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Баранову Нікіті Борисовичу

Тема кваліфікаційної роботи: “Технології запобігання і протидії внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури”

керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА *доктор економічних наук, професор*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “30” жовтня 2025 р. № 467.

1. Строк подання кваліфікаційної роботи “25” грудня 2025 р.
2. Вихідні дані до кваліфікаційної роботи:.
3. Перелік питань, які потрібно розробити:
   1. Дослідити теоретичні засади інформаційної безпеки об’єктів критичної інфраструктури
   2. Проаналізувати внутрішні загрози інформаційній безпеці, методи протидії
   3. Запропонувати технології попередження внутрішніх загроз інформаційної безпеки
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання “02” жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідити теоретичні засади інформаційної безпеки об’єктів критичної інфраструктури	27.10.2025	
4.	Проаналізувати внутрішні загрози інформаційній безпеці, методи протидії	03.11.2025	
5.	Запропонувати застосування технологій попередження внутрішніх загроз	11.11.2025	
6.	Формулювання висновків за результатами дослідження.	21.11.2025	
7.	Оформлення роботи.	29.11.2025	
8.	Оформлення презентації.	05.12.2025	
9.	Отримання рецензії на роботу.	10.12.2025	
10.	Захист в ЕК.	20.01.2026	

Здобувач вищої освіти _____ Нікіта БАРАНОВ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(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 магістра

Направляється здобувач Баранов Н.Б. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Технології запобігання і протидії внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури "
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **БАРАНОВ Нікіта** у кваліфікаційній роботі проаналізував теоретичні засади інформаційної безпеки об'єктів критичної інфраструктури, вивчив практичне застосування систем моніторингу та аудиту доступу до інформаційних ресурсів, а також дослідив внутрішні загрози інформаційній безпеці та методи протидії. **БАРАНОВ Нікіта** показав високу теоретичну і практичну підготовку, вільне володіння науково-дослідницькими методами, вміння самостійно знаходити шляхи вирішення проблеми дослідження роботи. Це дозволяє оцінити кваліфікаційну роботу здобувача **БАРАНОВ Нікіта** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Баранов Н.Б. допускається до захисту даної роботи в Екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Баранова Нікіти Борисовича
на тему "Технології запобігання і протидії внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури"

Актуальність Зростання кількості та складності внутрішніх загроз, які становлять одну з найбільш небезпечних категорій ризиків для установ критичної інфраструктури має важливе значення у реаліях сучасного світу. Своєчасне виявлення, запобігання та нейтралізація таких загроз є ключовими чинниками забезпечення стабільності функціонування критично важливих систем та безперервності надання послуг.

Позитивні сторони

1. У роботі досліджено теоретичні засади інформаційної безпеки об'єктів критичної інфраструктури, визначено внутрішні загрози інформаційній безпеці, представлено технології попередження внутрішніх загроз інформаційної безпеки .
2. Кваліфікаційна робота оформлена відповідно до вимог. Розробка матеріалу здійснено відповідно до плану роботи, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків та графіків. Студент опрацював значну джерельну базу: більше 50 електронних джерел, постанов та законів.
3. За результатами кваліфікаційної роботи запропоновано рекомендації щодо забезпечення протидіям внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури.

Недоліки

1. Доцільно було б приділити більше уваги вивченню системи управління інцидентами безпеки, а також використанню зазначених у роботи методів.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Баранов Нікіта Борисович заслуговує присвоєння кваліфікації "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

Рецензент: завідувач кафедри Систем та технологій кібербезпеки,
д.т.н, професор _____ *підпис* Галина ГАЙДУР

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 84 стор., 13 рис., 60 джерел.

Метою роботи є дослідження технологій протидії інформаційній безпеці установ критичної інфраструктури.

Об'єктом дослідження є забезпечення інформаційної безпеки критичної інфраструктури.

Предмет дослідження – технології що запобігають внутрішнім загрозам інформаційної безпеки.

Методи дослідження. Застосовуються методи аналізу ризиків і вразливостей, які передбачають систематичне вивчення можливих каналів проникнення загроз. Ефективним є використання методів моделювання сценаріїв кібератак та тестування на проникнення з метою оцінки рівня захищеності інформаційних систем. Також впровадження методів безперервного моніторингу та аудиту, що забезпечують оперативне виявлення аномальних дій та порушень інформаційної безпеки.

Короткий зміст роботи. Як результат, у роботі проведено аналіз сучасних технологій і методів запобігання та протидії внутрішнім загрозам інформаційної безпеки в установах критичної інфраструктури, з урахуванням впливу цифрових трансформацій та розвитку штучного інтелекту. Окремо розглянуто технічні, організаційні та управлінські аспекти забезпечення безпеки, а також роль людського фактору в захисті від загроз. На основі отриманих результатів запропоновано концептуальну модель для виявлення та нейтралізації внутрішніх загроз у критичних системах.

Галузь застосування. Розроблені підходи можуть бути застосовані при плануванні та впровадженні системи управління інформаційною безпекою критичної інфраструктури для протидії загрозам, що виникають у процесі забезпечення інформаційної безпеки.

КЛЮЧОВІ СЛОВА: ІНФОРМАЦІЙНА БЕЗПЕКА, КРИТИЧНА ІНФРАСТРУКТУРА, ТЕХНОЛОГІЇ ПРОТИДІЇ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ABSTRACT

Text part of the qualification work for obtaining a master's degree: 84 pages, 13 figures, 60 sources.

The purpose of the work is to study technologies for counteracting information security threats to critical infrastructure institutions.

The object of the study is to ensure the information security of critical infrastructure.

The subject of the study is technologies that prevent internal threats to information security.

Research methods. The study of internal threats to information security in critical infrastructure institutions requires a comprehensive, interdisciplinary approach that covers technical, organisational, psychological and managerial aspects.

Summary of the work. As a result, the work analyses modern technologies and methods for preventing and countering internal threats to information security in critical infrastructure institutions, taking into account the impact of digital transformations and the development of artificial intelligence. Technical, organisational and managerial aspects of security, as well as the role of the human factor in protecting against threats, are considered separately. Based on the results obtained, a conceptual model for identifying and neutralising internal threats in critical systems is proposed.

Scope of application. The developed approaches can be applied in the planning and implementation of a critical infrastructure information security management system to counter threats arising in the process of ensuring information security.

KEYWORDS: INFORMATION SECURITY, CRITICAL INFRASTRUCTURE, COUNTERMEASURES, INFORMATION SECURITY MANAGEMENT SYSTEM.

ЗМІСТ

ВСТУП

1. Обґрунтування актуальності теми дослідження

Актуальність теми. Розвиток інформаційного суспільства супроводжується швидким зростанням обсягів оброблених та переданих даних, а також активним впровадженням цифрових технологій у всі сфери життєдіяльності. Інформаційні ресурси, інформаційно-комунікаційні системи й мережі стають не просто допоміжними засобами, а критичними компонентами управління, виробництва, фінансів, транспорту, енергетики, охорони здоров’я, оборони та безпеки держави.

У таких умовах інформаційна безпека є одним із ключових чинників національної безпеки. Будь-яке порушення функціонування інформаційних систем може призвести до масштабних економічних, соціальних або екологічних наслідків. З огляду на це, захист об’єктів критичної інфраструктури (КІ) є пріоритетним напрямом державної політики більшості країн світу, зокрема й України.

В Україні проблема внутрішніх загроз набуває особливої актуальності у зв’язку з війною та гібридними формами агресії проти держави. Зловмисники активно використовують людський фактор для отримання доступу до критичних систем — шляхом вербування співробітників, впливу через соціальні мережі, підкупу або дезінформації. Тому тема кваліфікаційної роботи є актуальною так як розробка сучасних технологій запобігання та протидії внутрішнім загрозам є не лише науково-технічним, а й стратегічним завданням національної безпеки.

Мета роботи полягає у створенні науково обґрунтованої системи підходів і технологій, які дозволяють ефективно запобігати, виявляти та нейтралізовувати внутрішні загрози інформаційній безпеці в установах критичної інфраструктури, з урахуванням сучасних тенденцій цифрової трансформації, розвитку штучного інтелекту та змін у поведінці персоналу. Обсяг дослідження охоплює як теоретичні, так і прикладні аспекти проблеми.

Об’єктом дослідження є процес забезпечення інформаційної безпеки установ критичної інфраструктури, який охоплює сукупність технічних, організаційних, нормативно-правових і кадрових заходів, спрямованих на захист інформаційних ресурсів, запобігання, виявлення та нейтралізацію загроз, що можуть поставити під загрозу стабільність і безперервність функціонування таких установ. Об’єкт дослідження охоплює не лише технологічну складову інформаційної безпеки, а й людський, організаційний і управлінський аспекти, які разом формують систему захисту від внутрішніх порушень.

Предметом дослідження є технології, методи, інструменти та організаційні підходи, що забезпечують запобігання, виявлення та протидію внутрішнім загрозам інформаційної безпеки в установах критичної інфраструктури. Дослідження охоплює й організаційні механізми — формування політик безпеки, регламентацію повноважень, аудит користувацьких дій, розділення обов’язків, моніторинг привілейованого доступу, навчання персоналу та підвищення рівня кіберкультури.

Методи дослідження - застосовуються методи моделювання сценаріїв кібератак, що дають змогу відтворити реальні умови можливих загроз і оцінити ефективність діючих механізмів захисту. Тестування на проникнення, яке є важливою складовою цих методів, дозволяє перевірити систему на стійкість до зовнішніх і внутрішніх атак, виявляючи слабкі місця в її архітектурі та програмному забезпеченні. Додатково використовуються методи обробки великих обсягів даних та аналізу поведінки користувачів, що дозволяє виявити підозрілі патерни та знизити ймовірність успішних атак, спрямованих на порушення внутрішньої безпеки установи.

Наукова новизна кваліфікаційної роботи полягає у розвитку нових теоретичних і методологічних засад забезпечення інформаційної безпеки установ критичної інфраструктури, зокрема в контексті протидії внутрішнім загрозам. У роботі сформовано системне уявлення про природу інсайдерських ризиків, їх класифікацію, динаміку виникнення та механізми впливу на інформаційні ресурси. Запропоновано концептуальну модель виявлення та запобігання внутрішнім загрозам, яка враховує як технологічні індикатори (аномалії в інформаційних

потоках, дії користувачів, несанкціоновані запити), так і людський фактор (мотиви, поведінкові особливості, рівень обізнаності персоналу).

Практичне значення кваліфікаційної роботи має важливе значення адже її результати можуть бути безпосередньо використані у діяльності організацій, які експлуатують об’єкти критичної інфраструктури, а також у підрозділах, що відповідають за кібербезпеку, інформаційний захист і управління ризиками. Запропоновані підходи дають змогу підвищити рівень стійкості інформаційних систем до внутрішніх загроз шляхом удосконалення процесів моніторингу користувацької активності, оптимізації системи контролю доступу, впровадження поведінкової аналітики (UEBA) та технологій запобігання витоку даних (DLP).

Галузь застосування має перспективу подальшого розвитку — зокрема, у напрямі автоматизації процесів виявлення інсайдерських дій із використанням штучного інтелекту, машинного навчання та прогнозної аналітики, що відкриває можливості створення інтелектуальних систем запобігання внутрішнім загрозам нового покоління.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Інформаційна безпека критичної інфраструктури є важливою складовою національної безпеки, оскільки критична інфраструктура включає в себе життєво важливі об'єкти, функціонування яких має безпосередній вплив на стабільність держави. Кіберзахист об'єктів критичної інфраструктури забезпечується шляхом здійснення суб'єктами заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки [6]. Це можуть бути енергетичні, транспортні, фінансові, комунікаційні, медичні та інші системи, порушення роботи яких може призвести до серйозних наслідків для економіки, громадської безпеки та національної оборони.

Інормаційна безпека охоплює захист інформаційних систем, що забезпечують функціонування цієї інфраструктури, від можливих загроз і вразливостей. Основними складовими ІБ є конфіденційність (захист інформації від несанкціонованого доступу), цілісність (забезпечення правильності і достовірності даних), доступність (забезпечення безперервного доступу до систем) і аутентифікація (підтвердження особи користувача).

Для ефективного забезпечення важливими є кілька теоретичних моделей і принципів. Зокрема, модель конфіденційності, цілісності та доступності (CIA) є основою для розуміння ключових вимог до безпеки. Модель загроз і ризиків дозволяє оцінити можливі загрози і визначити відповідні заходи для їх нейтралізації. Принципи "найменшого привілею", де користувачам надається лише той доступ, який необхідний для виконання їхніх завдань, та резервування, що передбачає створення копій критичних даних для відновлення після інцидентів, також є важливими аспектами інформаційної безпеки. Установи критичної інфраструктури, що мають безпосереднє відношення до забезпечення інформаційної безпеки України, включають органи державної влади, енергетичні компанії, телекомунікаційні та транспортні мережі, а також фінансові установи та системи управління кризовими ситуаціями. До таких установ належать Національний банк

України, який відповідає за стабільність фінансової системи та захист електронних платіжних систем; оператори телекомунікаційної інфраструктури, зокрема «Укртелеком» та «Київстар», що забезпечують зв'язок та доступ до Інтернету; енергетичні компанії, такі як «Укренерго», що управляє електричними мережами країни, а також атомні станції, які забезпечують постачання енергії; Міністерство внутрішніх справ України, яке здійснює нагляд за національною безпекою, включаючи кібербезпеку; Державна служба з надзвичайних ситуацій, яка бере участь у реагуванні на техногенні катастрофи, зокрема кіберінциденти; Міністерство оборони України та Генеральний штаб Збройних Сил України, що забезпечують захист державних інформаційних систем у сфері оборони; а також «Укрзалізниця», транспортна інфраструктура, що є важливою частиною економічної та логістичної стабільності країни. Захист інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави від кібератак забезпечується власником (розпорядником) таких систем відповідно до законодавства у сфері захисту інформації та кібербезпеки [2]. Усі ці установи мають критичне значення для забезпечення функціонування національної безпеки та стабільності держави, тому їх інформаційні системи потребують високого рівня захисту від можливих кіберзагроз.

Розглянемо NIST (Національний інститут стандартів і технологій) який є провідною організацією, що розробляє стандарти та рекомендації для забезпечення кібербезпеки та захисту критичної інфраструктури від загроз інформаційній безпеці. Оскільки критична інфраструктура є основою функціонування країни, включаючи енергетику, транспорт, фінансові установи, охорону здоров'я та інші важливі сектори, її захист від кіберзагроз є пріоритетним завданням національної безпеки. NIST надає організаціям чіткі рекомендації для оцінки, управління та нейтралізації ризиків, а також створення надійної системи безпеки, яка включає комплекс технічних, організаційних і правових заходів.

Одним із основних інструментів, що пропонує NIST, є NIST Cybersecurity Framework (CSF)**,** який допомагає організаціям створити стратегію захисту критичних систем від загроз, спричинених як зовнішніми, так і внутрішніми факторами. CSF охоплює п’ять основних функцій: Ідентифікація (визначення

активів, загроз і вразливостей у системах), Захист (встановлення захисних механізмів, таких як шифрування і контроль доступу), Виявлення (моніторинг і виявлення аномалій у реальному часі), Реагування (швидка реакція на інциденти для мінімізації збитків), та Відновлення (розробка планів відновлення після інцидентів).

Цей фреймворк дозволяє організаціям оцінити поточний рівень зрілості їхніх систем безпеки і розробити план покрокового вдосконалення. NIST також розробляє спеціалізовані публікації, такі як NIST SP 800-53, яка надає контрольні механізми для захисту інформаційних систем критичної інфраструктури. Включені в неї рекомендації допомагають в управлінні ризиками і підвищенні стійкості до кіберзагроз, включаючи технічні, організаційні та адміністративні заходи безпеки (контроль доступу, моніторинг, виявлення аномалій, шифрування даних, верифікація ідентичності користувачів). Для промислових і енергетичних об’єктів, які є частиною критичної інфраструктури, NIST розробив SP 800-82**,** що пропонує рекомендації щодо захисту промислових контролерів і автоматизованих систем, які є вразливими до кіберзагроз.

Для ефективного управління ризиками NIST використовує Risk Management Framework (RMF) — методологію для оцінки та мінімізації ризиків. Цей підхід складається з кількох етапів: ідентифікація ризиків (виявлення загроз і вразливостей), оцінка ризиків (аналіз потенційних наслідків для критичних систем), вибір заходів захисту, впровадження цих заходів і постійний моніторинг рівня безпеки. Завдяки RMF організації можуть систематично підходити до управління кіберризиками та вдосконалювати свої стратегії безпеки. NIST також активно працює над забезпеченням відповідності міжнародним стандартам, таким як ISO/IEC 27001, що регулює управління інформаційною безпекою на глобальному рівні. Це дозволяє організаціям критичної інфраструктури відповідати єдиним стандартам для забезпечення високого рівня захисту та захисту персональних даних і конфіденційної інформації.

Для практичної реалізації рекомендацій NIST використовуються різноманітні технічні інструменти, зокрема шифрування даних для захисту переданої та збереженої інформації, системи виявлення вторгнень (IDS/IPS) для моніторингу

мережі, механізми аутентифікації та контроль доступу для запобігання несанкціонованому доступу до систем. Крім того, важливими є плани реагування на інциденти та відновлення після катастроф, що дозволяють швидко відновити роботу критичної інфраструктури після кібернападів.

1.1. Поняття та значення критичної інфраструктури для національної безпеки

Поняття критична інфраструктура (КІ) є ключовим у сучасних підходах до забезпечення національної безпеки, оскільки саме ця інфраструктура забезпечує стале функціонування суспільства, економіки та держави загалом. Під критичною інфраструктурою розуміють сукупність об’єктів, систем, мереж і служб, від безперебійного функціонування яких залежить економічна стабільність, обороноздатність, здоров’я населення, екологічна безпека та державне управління.

У міжнародній практиці визначення КІ має декілька інтерпретацій, але всі вони зводяться до спільного розуміння — це ті ресурси, які є життєво необхідними для підтримання базових суспільних процесів. Згідно з документом Європейського Союзу “Directive 2008/114/EC on the identification and designation of European critical infrastructures”, критичною є така інфраструктура, руйнування або порушення функціонування якої може мати серйозний вплив на охорону здоров’я, безпеку, економічне чи соціальне благополуччя громадян.

В українському законодавстві термін «критична інфраструктура» закріплений у Законі України «Про основні засади забезпечення кібербезпеки України» (2017) та в постанові Кабінету Міністрів України № 518 від 9 жовтня 2020 року «Про затвердження Порядку формування переліку об’єктів критичної інфраструктури» [7]. У цих документах КІ визначається як сукупність об’єктів, систем і мереж, порушення функціонування яких може призвести до негативних наслідків для національної безпеки, оборони, економіки, навколишнього середовища, здоров’я або життя людей.

До таких об’єктів належать:

- енергетичні системи (електро-, газо-, нафто- та теплопостачання);
- транспортна інфраструктура (авіаційна, залізнична, морська, автомобільна);
- фінансово-банківський сектор;
- телекомунікаційні та інформаційні мережі;
- системи охорони здоров’я та фармацевтичної логістики;
- підприємства оборонно-промислового комплексу;
- водопостачання, каналізація, комунальні послуги;
- об’єкти державного управління, органи влади, урядові інформаційні системи.

Критична інфраструктура є основою функціонування будь-якої сучасної держави, оскільки саме від її стабільності та безперебійної роботи залежить національна безпека, економічна стійкість, соціальний добробут і навіть політична стабільність суспільства. У широкому розумінні поняття «критична інфраструктура» охоплює сукупність об’єктів, систем і мереж, вихід з ладу або пошкодження яких може призвести до значних негативних наслідків для життєдіяльності населення, національної економіки, екології та державного управління.

Згідно з Законом України “Про основні засади забезпечення кібербезпеки України” (2017 р.) [7], критичною вважається інфраструктура, яка забезпечує функціонування життєво важливих суспільних і економічних процесів. До її складу належать об’єкти енергетики, транспорту, зв’язку, фінансової системи, оборонно-промислового комплексу, охорони здоров’я, водопостачання, інформаційних систем управління державоютощо (відповідно до Постанови Кабінету Міністрів України № 563 від 9 жовтня 2020 р., кожен сектор критичної інфраструктури має свої критерії віднесення об’єктів до категорії “критичних”, залежно від масштабу наслідків у разі їх порушення).

Державна політика у сфері захисту критичної інфраструктури в Україні формується відповідно до Національної стратегії кібербезпеки (2021 р.) та Стратегії забезпечення національної безпеки (2020 р.). Вона передбачає впровадження комплексних заходів, що включають:

- Розроблення нормативно-правової бази, яка регламентує категоризацію об’єктів, відповідальність суб’єктів критичної інфраструктури та процедури обміну інформацією про інциденти.
- Створення Національної системи захисту критичної інфраструктури, до складу якої входять державні органи (РНБО, Держспецзв’язку, СБУ, МВС, Міненерго тощо), галузеві CERT-команди, а також приватні оператори.
- Впровадження ризик-орієнтованого підходу, що дозволяє оцінювати й пріоритизувати загрози залежно від їхнього потенційного впливу.
- Розвиток системи кіберрозвідки та моніторингу, що забезпечує раннє виявлення загроз і підвищує стійкість державних інформаційних ресурсів.

Розпорядженням Кабінету Міністрів України від 06.12.17 р. затверджено Концепцію створення державної системи захисту критичної інфраструктури, де серед проблем, що потребують розв’язання, визначено відсутність єдиних критеріїв та методології віднесення об’єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації [13].

Сьогодні Україна активно розбудовує власну національну систему кіберстійкості, що поєднує превентивні, реактивні та відновлювальні заходи. В межах цієї системи функціонує Національний координаційний центр кібербезпеки (НКЦК) при РНБО України, який забезпечує координацію дій між державними структурами, Службою безпеки України, Держспецзв’язку, МВС, Міністерством оборони, а також приватними підприємствами, які володіють критичною інфраструктурою. Крім того, активно працює CERT-UA — команда реагування на комп’ютерні надзвичайні події, яка займається моніторингом, аналізом і реагуванням на кібератаки проти державних і стратегічних об’єктів.

Після масштабних кібератак на енергетичну інфраструктуру України у 2015–2016 роках (так звані атаки BlackEnergy і Industroyer), питання кіберзахисту критичних об’єктів набуло особливого значення. Ці інциденти стали яскравим прикладом того, що кіберзагрози можуть безпосередньо впливати на фізичну безпеку громадян. Інформаційна безпека також виконує профілактичну функцію, сприяючи зниженню ризику інцидентів за рахунок превентивного виявлення

вразливостей, постійного моніторингу та навчання персоналу. Сучасні кіберзлочинці та кібертерористи здебільшого здійснюють асиметричні атаки, спрямовані на досягнення стратегічних цілей без застосування високотехнологічних засобів збройного характеру [5].

Більшість розвинених країн світу приділяють значну увагу питанням захисту КІ. У США діє програма Critical Infrastructure Protection (CIP), координована Агентством з кібербезпеки та інфраструктурної безпеки (CISA). Її мета — забезпечити стійкість 16 секторів критичної інфраструктури, серед яких енергетика, транспорт, комунікації, охорона здоров'я та фінанси. США є однією з провідних країн у сфері кіберзахисту. У країні діє Агентство з кібербезпеки та безпеки інфраструктури (CISA), яке координує зусилля з охорони КІІ. Уряд США впроваджує підхід Zero Trust, що передбачає максимальний рівень контролю за всіма мережами, пристроями та користувачами. Також відповідно до законодавства США, компанії критичної інфраструктури повинні повідомляти про кіберінциденти протягом 72 годин [17].

У країнах ЄС діє Європейська програма захисту критичної інфраструктури (EPCIP), що передбачає гармонізацію законодавства, обмін інформацією між країнами та впровадження спільних стандартів безпеки. Досвід США та ЄС демонструє, що найефективнішою моделлю є партнерство держави і приватного сектору, коли держава встановлює вимоги й координує дії, а приватні компанії забезпечують впровадження технічних засобів захисту. Україна поступово впроваджує подібну модель через залучення енергетичних, телекомунікаційних, банківських та транспортних компаній до системи кіберзахисту національного рівня.

Стійкість критичної інфраструктури залежить від трьох взаємопов'язаних чинників:

1. Фізичної безпеки — захисту обладнання, приміщень, мереж і персоналу.

2. Кібербезпеки — захисту інформаційних систем, мереж і даних.

3. Організаційної стійкості — здатності системи швидко реагувати на інциденти, відновлювати роботу і підтримувати безперервність процесів.

1.2. Визначення і класифікації внутрішніх загроз інформаційній безпеці

У сучасному інформаційному суспільстві, де більшість державних і приватних процесів залежить від цифрових технологій, питання внутрішніх загроз інформаційній безпеці набуває особливої актуальності. Якщо раніше основна увага приділялася зовнішнім атакам — хакерам, шкідливому програмному забезпеченню, несанкціонованим вторгненням — то сьогодні дедалі частіше джерело небезпеки криється всередині самої організації.

Під внутрішньою загрозою інформаційній безпеці розуміють дії, бездіяльність або умови, створені суб’єктами, які володіють правомірним доступом до інформаційних систем і які можуть призвести до порушення конфіденційності, цілісності чи доступності даних. Характерною особливістю внутрішніх загроз є те, що вони часто залишаються непоміченими тривалий час. Інсайдер діє з використанням власних облікових записів, володіє знаннями про політику безпеки, структуру мережі, службові процедури й може обійти системи контролю, не викликаючи підозри. Саме тому, за даними звіту IBM Cost of Insider Threats Report 2024, середній час виявлення інсайдерського інциденту становить понад 85 днів, а усунення наслідків — ще близько 70 днів. При цьому 56% інцидентів пов’язані з ненавмисними діями співробітників, тоді як 44% — із навмисними порушеннями політики безпеки.

Залежно від причин і мотивації внутрішні загрози поділяються на кілька основних типів. Перший тип — навмисні загрози, що виникають унаслідок свідомих дій працівників, які з певних мотивів (матеріальна вигода, помста, політична чи ідеологічна зацікавленість) намагаються завдати шкоди організації. Такі інсайдери можуть копіювати або продавати конфіденційні дані, вносити зміни до програмного забезпечення, маніпулювати параметрами систем управління чи знищувати дані. Другий тип — ненавмисні загрози, які зумовлені некомпетентністю, помилками або необережністю персоналу. Найчастіше це відкриття фішингових листів, використання слабких паролів, порушення правил поводження з носіями інформації, випадкове розкриття службових даних. Третій тип — компрометовані інсайдери,

тобто користувачі, облікові дані яких були викрадені або підроблені, через що зовнішні зловмисники діють від їхнього імені.

Сучасна міжнародна практика передбачає використання стандартів і рекомендацій для управління ризиками внутрішніх загроз. Документи ISO/IEC 27005, NIST SP 800-53 Rev.5, а також методичні матеріали ENISA пропонують комплексний підхід, який включає політику управління привілейованими користувачами, регулярний аудит доступу, моніторинг журналів подій і впровадження систем класу DLP (Data Loss Prevention), SIEM (Security Information and Event Management) та UEBA (User and Entity Behavior Analytics).

За класифікацією загрози розрізняють як загрози від співробітників, які мають офіційний доступ до систем організації, загрози від підрядників і постачальників, які можуть виникати через недостатній контроль за їх діяльністю, а також загрози від колишніх співробітників, які зберігають доступ до інформаційних ресурсів після звільнення. Що стосується типу дій, внутрішні загрози можуть бути як навмисними, коли порушення безпеки спричиняються зловмисними намірами (наприклад, крадіжка даних або саботаж), так і ненавмисними, коли загроза виникає через помилки, недотримання правил або незнання співробітниками політик безпеки.

Мотиви загроз можуть бути різноманітними, до економічних мотивів відносяться дії, спрямовані на отримання фінансової вигоди, наприклад, крадіжка комерційної таємниці або продаж конфіденційних даних. Мотиви помсти можуть бути пов’язані з особистими неприязними стосунками співробітника до організації, а ідеологічні мотиви можуть включати здійснення атак через політичні чи соціальні переконання.

1.3. Огляд основних типів загроз інформаційній безпеці в критичних установах

Інформаційна безпека критичної інфраструктури є ключовою складовою системи національної безпеки держави, оскільки саме ці структури забезпечують стабільне функціонування життєво важливих секторів — енергетики, транспорту,

зв’язку, фінансів, медицини, оборони та державного управління. Порушення роботи таких об’єктів може мати масштабні економічні, соціальні та політичні наслідки.

Загрози інформаційній безпеці критичної інфрасруктури поділяються на зовнішні та внутрішні. Зовнішні загрози — це дії зловмисників, які не мають безпосереднього доступу до інформаційних ресурсів організації, але намагаються його отримати через мережеві або програмні вразливості. Внутрішні загрози, навпаки, походять від осіб, які мають легітимний доступ до системи.

До основних типів загроз інформаційній безпеці в критичних установах належать технічні, організаційні, людські, зовнішні та соціотехнічні. Технічні загрози пов’язані з несанкціонованим втручанням у роботу інформаційних систем, мереж або обладнання. Вони включають впровадження шкідливого програмного забезпечення (вірусів, троянів, шпигунських програм, програм-вимагачів), експлуатацію вразливостей у програмному коді, атаки типу DDoS, перехоплення мережевого трафіку та несанкціоноване підключення до мереж.

Людський фактор — ще одна критична складова загроз інформаційній безпеці. Саме помилки, недбалість або навмисні дії співробітників часто стають причиною інцидентів. Це може бути відкриття фішингових листів, використання слабких паролів, зберігання конфіденційної інформації на особистих пристроях або неналежне поводження з носіями даних.

Зовнішні загрози виникають унаслідок діяльності хакерських угруповань, державних спецслужб, терористичних організацій або конкурентів. Вони часто реалізуються через багаторівневі цілеспрямовані атаки (Advanced Persistent Threats — APT), які передбачають тривале приховане перебування зловмисника у системі, збір розвідданих і поступове порушення роботи об’єкта. Найвідомішими прикладами таких атак є NotPetya (2017), яка паралізувала роботу українських державних установ і приватних компаній, та SolarWinds (2020), коли було зламано оновлення програмного забезпечення, через що постраждали сотні організацій по всьому світу. Держава активно та постійно опікується питаннями посилення захисту об’єктів критичної інфраструктури. Повний перелік таких об’єктів ухвалює Уряд України, виходячи із таких критеріїв, як соціальна, політична, економічна

значущість для забезпечення оборони країни та безпеки суспільства, рівень уразливості таких об’єктів [3]. Соціотехнічні загрози базуються на маніпулюванні людьми для отримання доступу до конфіденційної інформації або ресурсів. Найпоширенішими є фішинг, спуфінг, телефонні шахрайства, підробка корпоративних повідомлень, а також «спуфінг довіри» — коли зловмисник видає себе за керівника чи колегу. У критичних установах такі методи часто поєднуються з психологічним впливом або інформаційно-психологічними операціями, спрямованими на дестабілізацію роботи персоналу.

За об’єктами впливу загрози поділяються на такі, що спрямовані на інформаційні ресурси (витік, модифікація чи знищення даних), на інформаційно-комунікаційні системи (пошкодження інфраструктури, знищення журналів, перехоплення даних), на персонал (маніпуляції, соціотехнічні атаки), а також на організаційні структури (підрив управлінських процесів, компрометація політик безпеки). Для кожного об’єкта характерні свої індикатори загроз, що вимагають специфічних механізмів захисту.

За даними ENISA Threat Landscape Report 2024, майже половина зареєстрованих атак на державному рівні була спрямована на енергетичний, транспортний і комунікаційний сектори. При цьому понад 60% інцидентів мали внутрішній компонент — людські помилки, витік облікових даних чи використання скомпрометованих акаунтів. В Україні, за даними CERT-UA, у 2022–2024 роках зафіксовано понад 250 спроб кібератак на об’єкти критичної інфраструктури, більшість із яких реалізовувалися через фішинг і зараження шкідливим ПЗ (Рис. 1.1).

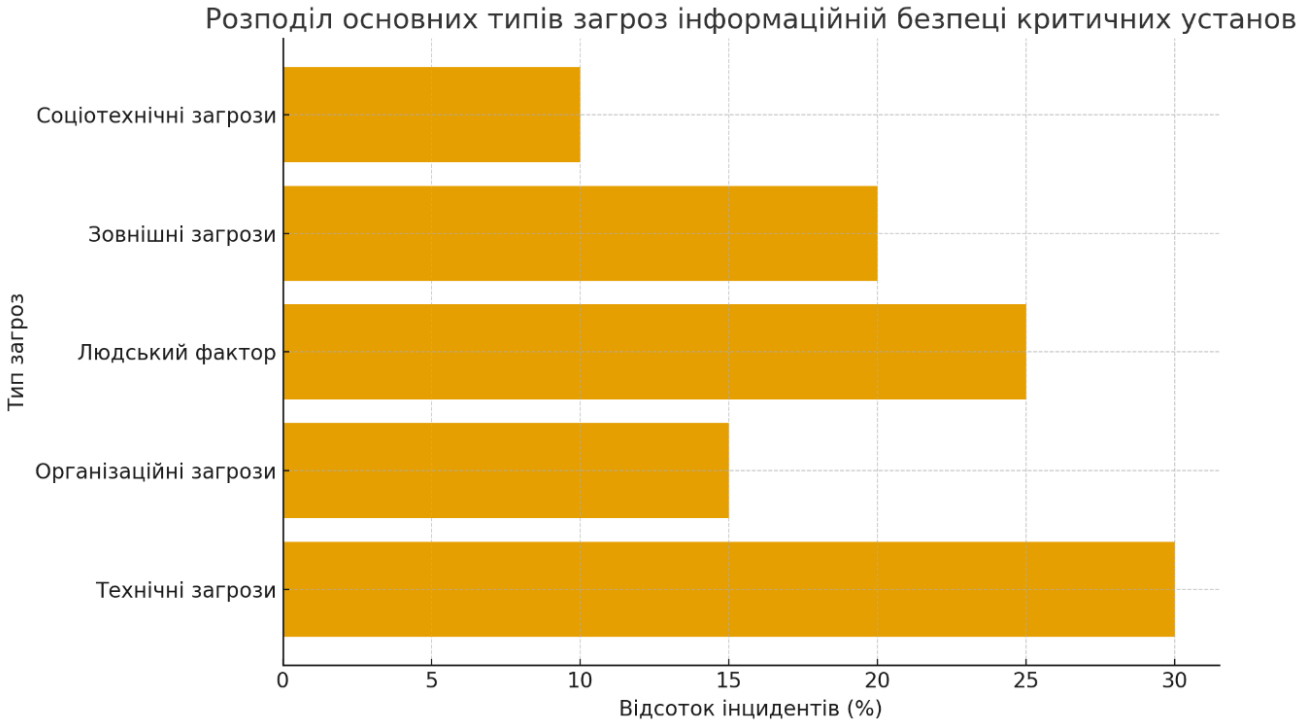

Рис. 1.1. Розподіл основних типів загроз

1.4. Особливості забезпечення інформаційної безпеки критичної інфраструктури

Забезпечення інформаційної безпеки в установах критичної інфраструктури є стратегічно важливим завданням державного рівня, оскільки ці об’єкти забезпечують безперервне функціонування енергетичних, фінансових, транспортних, комунікаційних, медичних, військових та управлінських систем. Порушення їх роботи може спричинити не лише економічні збитки, але й політичну дестабілізацію, загрозу життю людей, колапс державних сервісів. Саме тому процес побудови системи інформаційної безпеки для таких структур має комплексний і багаторівневий характер, що поєднує технічні, організаційні, кадрові, правові й навіть психологічні аспекти.

Однією з головних особливостей є високий рівень вимог до надійності та безперервності роботи систем. Будь-який інцидент, навіть короткочасне порушення доступу до даних або затримка в обробці інформації, може мати критичні наслідки. Наприклад, збій у роботі системи управління рухом на залізниці або в енергетичній

мережі може паралізувати роботу цілих регіонів. Тому системи безпеки для таких об’єктів будуються з урахуванням принципів резервування, дублювання функцій, сегментації мереж, контролю доступу та багаторівневого моніторингу. Важливою характеристикою є висока інтегрованість IT-середовища. У критичних структурах поєднуються сучасні цифрові технології, промислові системи управління (ICS, SCADA), мережеві компоненти та спеціалізоване обладнання.

Не менш важливим є людський фактор. У критичних структурах працівники мають доступ до важливої інформації та систем управління, тому саме вони часто стають об’єктами атак або джерелами внутрішніх загроз. Через це система безпеки має бути не лише технічною, а й поведінковою. Застосування технологій UEBA (User and Entity Behavior Analytics), DLP (Data Loss Prevention), PAM (Privileged Access Management) дозволяє контролювати дії користувачів, виявляти підозрілі патерни поведінки, запобігати витоку інформації та зловживанню привілеями.

Особливістю безпеки критичних структур є чітке державне регулювання та стандартизація процесів. Усі організації, віднесені до об’єктів критичної інфраструктури, зобов’язані впроваджувати системи управління інформаційною безпекою відповідно до міжнародних стандартів ISO/IEC 27001, NIST SP 800-53, а також національних вимог, зокрема Закону України «Про основні засади забезпечення кібербезпеки України» та Національної стратегії кібербезпеки. Ці документи встановлюють вимоги до управління ризиками, реагування на інциденти, обміну інформацією про загрози, проведення аудитів і сертифікації систем безпеки.

Особливе місце посідає управління ризиками та реагування на інциденти. В установах критичної інфраструктури безпека розглядається не як статичний стан, а як безперервний процес. Створюються спеціальні підрозділи — центри кібербезпеки (SOC — Security Operations Center), які цілодобово відстежують події в системі, аналізують журнали, виявляють аномалії та координують дії у разі загрози. Такі центри використовують технології SIEM (Security Information and Event Management) для автоматизованого збору даних про інциденти, а також системи реагування SOAR (Security Orchestration, Automation and Response) для оперативного усунення наслідків атак.

Ще одна важлива особливість — висока вартість і тривалість впровадження систем захисту. Будь-яке рішення має бути узгоджене з вимогами сумісності, сертифікації, безпеки та економічної доцільності. Крім того, зміна або оновлення технологічного обладнання може вимагати тривалого тестування, що уповільнює впровадження сучасних методів захисту.

Оскільки критичні структури часто є об’єктом цілеспрямованих кібератак державного рівня, їх системи безпеки повинні враховувати не лише технічні загрози, а й геополітичні фактори. Для України це питання набуває особливої актуальності у зв’язку з триваючою кібервійною, що супроводжує збройну агресію Російської Федерації.

У системі кіберзахисту важливу роль відіграє міжвідомча взаємодія та обмін інформацією між державними структурами, правоохоронними органами, приватними компаніями та міжнародними партнерами. Такий підхід дозволяє швидко реагувати на загрози, ідентифікувати нові вектори атак і запобігати поширенню шкідливих впливів (Рис. 1.2.).

Рис. 1.2. Порівняння рівня вразливості

1.5. Аналіз реальних випадків запобігання та боротьби з внутрішніми загрозами

Першим прикладом стала атака BlackEnergy (2015 р.), під час якої українські енергетичні компанії стали жертвами фішингової кампанії. Працівники несвідомо відкрили заражені електронні листи, після чого зловмисники отримали віддалений доступ до SCADA-систем і здійснили відключення електропостачання для понад 230 тисяч споживачів. Цей інцидент продемонстрував, наскільки критично важливо проводити навчання персоналу з кібергігієни та контролювати електронні комунікації. В результаті компанії запровадили системи моніторингу електронної пошти, DLP-технології та внутрішні інструкції з обробки листів.

У 2016 році Україна знову стала об’єктом кібератаки — цього разу за допомогою шкідливого ПЗ Industroyer (CrashOverride), спрямованого на енергетичні системи Києва. Експерти зазначають, що зловмисники володіли детальною інформацією про структуру промислових мереж, що могло свідчити про використання внутрішніх знань або співпраці з працівниками компаній. Після цього випадку енергетичні підприємства посилили контроль за доступом до промислових мереж, запровадили принцип мінімізації прав користувачів і перевірку надійності персоналу.

Ще одним важливим інцидентом стала атака NotPetya (2017 р.), яка почалася з компрометації програмного забезпечення «M.E.Doc» — бухгалтерської системи, якою користувалися тисячі українських організацій. Через внутрішню мережу шкідливий код швидко поширився на державні установи, банки, транспортні компанії та енергетичні підприємства.

На міжнародному рівні також є низка прикладів, які підтверджують небезпеку внутрішніх загроз. Так, у США у 2013 році співробітник Агентства національної безпеки Едвард Сноуден розголосив секретні дані, що стало поштовхом до впровадження систем PAM (Privileged Access Management) для контролю дій користувачів із підвищеними правами. У 2021 році компанія Tesla запобігла витоку

комерційної інформації завдяки аналітичній системі UEBA, яка виявила аномальну активність працівника, що намагався передати дані конкурентам.

Після 2017 року кібератаки на Україну не припинилися, а лише еволюціонували. У 2020–2021 роках зафіксовано хвилю атак із використанням шкідливих програм QUIETPLACE, WhisperGate, HermeticWiper, спрямованих на державні установи, енергетичні компанії та об’єкти оборонного сектору. Ці атаки мали характер «wiper» — тобто програм, які не шифрують дані, а безповоротно їх знищують. Метою було порушення роботи державних органів і створення хаосу в інформаційному середовищі.

Під час повномасштабного вторгнення Росії у 2022 році кібератаки стали невід’ємною складовою військової агресії. У перші дні вторгнення група Sandworm запустила атаку Industroyer2, спрямовану на українську енергосистему. Вона мала повторити ефект 2016 року, проте завдяки підготовці CERT-UA, Держспецзв’язку та партнерів із ЄС і США, атаку вдалося нейтралізувати до реалізації. Одночасно відбувалися масові DDoS-атаки на урядові сайти, банківські сервіси, системи оповіщення та медіаресурси.

Також у 2022–2024 роках фіксувалися атаки груп Gamaredon (Primitive Bear), APT28 (Fancy Bear), KillNet та NoName057(16), спрямовані на українські держустанови, телекомунікаційні мережі, транспорт і об’єкти енергетики. Основною метою таких атак було порушення стабільності державного управління, розповсюдження дезінформації, знищення даних і деморалізація населення. Україна стала прикладом для всього світу, як країна, що одночасно веде традиційну і кібервійну. Як відповідь на постійні загрози, держава створила Національний координаційний центр кібербезпеки (НКЦК) при РНБО, модернізувала CERT-UA, запровадила Закон «Про основні засади забезпечення кібербезпеки України» (2017 р.) і ухвалила Національну стратегію кібербезпеки (2021 р.).

В Україні також траплялися випадки витоку персональних даних із державних реєстрів, зокрема через недбалість співробітників або слабкий контроль за доступом до інформаційних систем. Ці інциденти показали потребу у створенні єдиної

системи моніторингу дій користувачів і посиленні дисциплінарної відповідальності за порушення політик безпеки (Рис 1.3.)

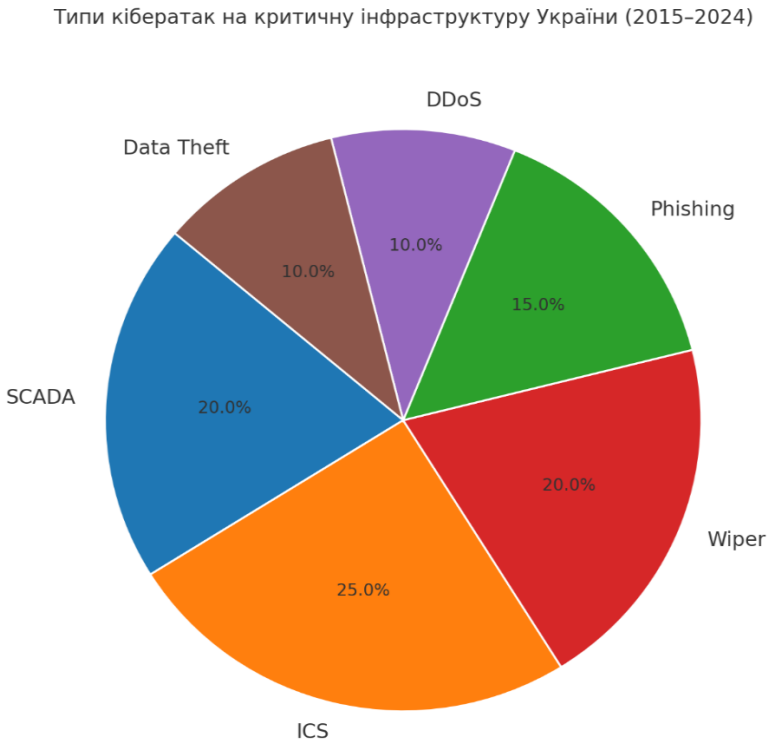

Рис. 1.3. Типи кібератак

У результаті аналізу можна визначити кілька основних напрямів протидії внутрішнім загрозам:

- Технологічні заходи: впровадження систем SIEM, DLP, UEBA, PAM для автоматичного виявлення аномалій і запобігання витоку даних.
- Організаційні заходи: проведення аудиту доступів, розмежування повноважень, створення внутрішніх регламентів і системи контролю.
- Освітні ініціативи: регулярні тренінги з кібергігієни, моделювання фішингових атак і формування навичок безпечної роботи з інформацією.
- Кадрові політики: перевірка персоналу перед працевлаштуванням, оцінка рівня благонадійності та психологічної стабільності працівників, які мають доступ до критичних даних.

- Міжвідомча взаємодія: співпраця з державними структурами, такими як CERT-UA та Держспецзв’язку, для обміну інформацією про інциденти й підвищення кіберстійкості.

Загальними особливостями об’єктів критичної інфраструктури є автоматизація процесів планування, обліку і управління основних напрямків діяльності об’єктів критичної інфраструктури. Тому загалом їх можна розглядати як інтегровану сукупність таких основних підсистем: управління фінансами, управління матеріальними потоками, управління обслуговуванням, управління якістю, управління персоналом, управління збутом, аналіз фінансів, собівартості, оборотних коштів, управління маркетингом тощо [42].

Аналіз реальних випадків свідчить, що боротьба з внутрішніми загрозами вимагає не лише впровадження технічних засобів, але й побудови цілісної системи управління безпекою, орієнтованої на людський фактор. Ефективний захист можливий лише тоді, коли поєднано технологічний контроль, грамотну організаційну політику та свідому участь кожного співробітника у забезпеченні кіберстійкості організації.

Висновки до 1 розділу

У результаті теоретичного дослідження встановлено, що інформаційна безпека об’єктів критичної інфраструктури є однією з основних складових національної безпеки, оскільки критична інфраструктура охоплює об'єкти та системи, які є критичними для стабільності функціонування держави. Ці системи включають енергетику, транспорт, зв’язок, фінанси, оборону, охорону здоров’я та інші, порушення роботи яких може призвести до значних соціальних, економічних та екологічних наслідків. Тому забезпечення інформаційної безпеки цих об'єктів має стратегічне значення для національної безпеки.

З аналізу загроз встановлено, що інформаційній безпеці критичної інфраструктури загрожують як зовнішні, так і внутрішні фактори. Внутрішні загрози, зокрема пов'язані з людським фактором, неналежним управлінням доступами або умисними діями персоналу, є особливо небезпечними, оскільки вони часто важко виявляються. Зовнішні загрози, до яких належать кібератаки, шпигунство, саботаж, технічні збої та природні катастрофи, також представляють серйозну небезпеку для критичних систем.

Дослідження показало, що для ефективного забезпечення інформаційної безпеки критичної інфраструктури необхідна системна інтеграція технічних, організаційних, правових і кадрових заходів. Це включає впровадження багаторівневих механізмів захисту, таких як системи моніторингу (SOC, SIEM), контроль доступу (IAM, PAM), запобігання витоку даних (DLP) та виявлення аномальної активності користувачів (UEBA). Водночас важливою складовою є підвищення обізнаності персоналу, розвиток корпоративної культури безпеки та суворе дотримання правил роботи з інформацією.

Аналіз реальних кібератак на Україну, таких як BlackEnergy (2015), Industroyer (2016), NotPetya (2017), а також подальші атаки у 2020–2024 роках, підтвердив, що критична інфраструктура є постійною мішенню для організованих зловмисних груп.

РОЗДІЛ 2.
ВНУТРІШНІ ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, МЕТОДИ ПРОТИДІЇ

На сьогодні високий ступінь впровадження новітніх технологій є ознакою рівня розвиненості країни, визначальним чинником її економічної конкурентоспроможності, а, отже, і необхідною умовою для досягнення цілей, які визначаються національними інтересами. В той же час, поряд з багатьма перевагами технологічний прогрес утворює умови безпрецедентної залежності як окремої людини, так і суспільства від систем, що надають інформаційні, комунікаційні, транспортні, енергетичні, фінансові та інші послуги. З руйнуванням таких систем на сьогодні пов’язують найбільш пагубні безпекові сценарії для провідних держав світу, зокрема для країн ЄС [22].

Внутрішні загрози є однією з найсерйозніших проблем для забезпечення інформаційної безпеки, оскільки вони виникають від осіб, які вже мають легітимний доступ до систем і даних організації. Це можуть бути співробітники, підрядники чи партнери, які працюють з організацією на постійній або тимчасовій основі. Внутрішні загрози включають як навмисні дії, такі як крадіжка даних чи саботаж, так і випадкові помилки, наприклад, неправильне налаштування систем чи видалення важливих файлів. Такі загрози є особливо небезпечними через те, що зловмисники, як правило, знайомі з внутрішньою структурою організації і мають доступ до критичних ресурсів.

Внутрішні загрози можна поділити на кілька основних категорій. До них відносяться злочинні дії, наприклад, крадіжка або незаконний продаж конфіденційної інформації, саботаж чи шпигунство, коли співробітник передає секретні дані конкурентам. Інший тип загроз — це випадкові дії, такі як помилки в налаштуваннях систем або невірне використання інструментів, що можуть призвести до втрати даних або зниження рівня безпеки.

Одним з ключових принципів є "найменшого привілею", який полягає в тому, щоб кожен співробітник мав доступ лише до тих даних і систем, які необхідні для

виконання його професійних обов'язків. Для керування привілеями доступу використовуються спеціалізовані системи управління привілеями (PAM), які забезпечують контроль за доступом до критичних ресурсів. Важливим елементом є також впровадження мультифакторної автентифікації (MFA), яка додає додатковий рівень захисту до облікових записів. Для забезпечення конфіденційності даних необхідно використовувати шифрування інформації, що дозволяє зберігати її в безпечному вигляді, навіть якщо дані потрапили в чужі руки.

Моніторинг та логування за допомогою систем SIEM дозволяє відстежувати дії користувачів і виявляти аномалії в їхній поведінці, що можуть свідчити про загрозу. Системи запобігання витоку даних (DLP) допомагають контролювати пересування конфіденційної інформації та блокувати несанкціоновані спроби її передачі. Важливим є також регулярне проведення аудитів прав доступу і моніторинг політик безпеки для забезпечення того, що доступ до чутливих даних є обмеженим і контрольованим.

Важливою складовою є наявність чітко визначеного плану реагування на інциденти (IRP), що дозволяє оперативно реагувати на загрози, локалізувати проблему і проводити необхідні заходи для відновлення нормальної роботи систем. Включає це і збереження доказів, проведення розслідування та, якщо потрібно, залучення фахівців з кібербезпеки для детального аналізу ситуації.

Законодавчі та правові аспекти також мають важливе значення в протидії внутрішнім загрозам. Організація повинна мати чітко визначені політики безпеки, які окреслюють відповідальність співробітників за порушення правил, і бути готовою застосовувати відповідні юридичні заходи, включаючи дисциплінарні покарання, цивільні або кримінальні санкції у разі серйозних порушень.

Для ефективної протидії внутрішнім загрозам необхідний комплексний підхід, який поєднує технічні засоби захисту, належну організаційну структуру, регулярне навчання персоналу та продумані правові механізми. Це допомагає не тільки виявляти і знижувати ризики внутрішніх загроз, але й створювати систему, яка забезпечить максимальний рівень захисту інформаційних ресурсів організації.

2.1. Характеристика та внутрішні загрози

У контексті розвитку цифрових технологій та зростання значення інформаційних систем для стабільного функціонування держави, бізнесу та критичної інфраструктури, проблема внутрішніх загроз для інформаційної безпеки набуває все більшої актуальності. Внутрішні загрози є особливо небезпечними через те, що виникають безпосередньо всередині організації, а їхніми джерелами виступають працівники, підрядники або партнери, які мають законний доступ до інформаційних ресурсів і добре знайомі з архітектурою та процесами системи. Такі загрози відрізняються високим рівнем прихованості, адже дії інсайдерів часто виглядають як звичайна робоча активність, що значно ускладнює їх виявлення. Прибрати ШІ

Під внутрішньою загрозою інформаційній безпеці розуміють потенційну або реальну можливість порушення конфіденційності, цілісності чи доступності інформації внаслідок дій осіб, які мають авторизований доступ до ресурсів організації. Вони можуть бути як навмисними, так і ненавмисними. Навмисні дії зазвичай пов’язані з бажанням завдати шкоди, отримати матеріальну вигоду або виконати завдання третьої сторони — конкурентів чи державних структур супротивника.

В Україні немає єдиного підходу до класифікації загроз критичній інфраструктурі. В Концепції створення державної системи захисту критичної інфраструктури, схваленої Розпорядження КМУ від 06.12.2017 р. № 1009-р. визначено загрози для критичної інфраструктури природного та техногенного характеру, протиправні дії та їх комбінації [31]. Класифікація внутрішніх загроз здійснюється за різними критеріями, однак найважливішим є ступінь умислу. До навмисних внутрішніх загроз належать умисні дії працівників, спрямовані на завдання шкоди організації — крадіжка або передача конфіденційних даних, саботаж, модифікація або знищення інформації, несанкціонований доступ до критичних систем. Причинами таких дій можуть бути фінансові труднощі, конфлікти всередині колективу, помста керівництву або співпраця з конкурентами.

Ненавмисні загрози, навпаки, виникають унаслідок необережності чи незнання — наприклад, коли працівник відкриває фішинговий лист, підключає заражений носій або ненавмисно розголошує службову інформацію. Окрему групу становлять комбіновані загрози, коли внутрішній користувач діє під впливом або контролем зовнішніх зловмисників, що є типовим у гібридних кібератаках.

Причини появи внутрішніх загроз мають комплексний характер і поділяються на технічні, організаційні та психологічні. До технічних належать відсутність ефективного контролю доступу, слабка система аутентифікації, неякісна сегментація мережі та недостатнє журналювання дій користувачів. Психологічні причини, своєю чергою, охоплюють незадоволеність умовами праці, конфлікти з керівництвом, відчуття несправедливості або зовнішній тиск. Саме людський фактор є найбільшою загрозою, адже, за статистикою, до 70% усіх інцидентів інформаційної безпеки пов’язані з діями працівників.

Втручання внутрішнього користувача у такі системи може призвести до порушення технологічних процесів, зупинки енергопостачання, транспортних колапсів або загроз для життя людей. Механізм реалізації інсайдерської загрози, як правило, має кілька етапів. Спочатку відбувається підготовка — зловмисник збирає інформацію про структуру системи, визначає слабкі місця, можливості для доступу. Потім здійснюється безпосереднє проникнення, зазвичай за допомогою власних або викрадених облікових даних. На етапі експлуатації інсайдер проводить операції із системами чи даними — копіює, модифікує або знищує інформацію, змінює налаштування обладнання, запускає шкідливе програмне забезпечення. Завершальним етапом є приховування слідів: видалення журналів подій, використання шифрування або тунелювання трафіку для уникнення виявлення.

2.2. Методи виявлення і попередження інсайдерських атак

Виявлення та попередження інсайдерських загроз — одна з найскладніших задач сучасної кібербезпеки, оскільки інсайдер має легальний доступ до систем, добре розуміє їхню структуру та часто діє в межах своїх службових повноважень.

Установи критичної інфраструктури, де інформаційні системи забезпечують роботу життєво важливих процесів, особливо вразливі до подібних дій. Тому розробка ефективних методів виявлення, моніторингу та профілактики інсайдерських загроз є ключовим елементом комплексного захисту.

Будь-яка система контролю інсайдерських ризиків ґрунтується на трьох головних принципах: безперервний моніторинг, поведінковий аналіз і багаторівневий захист.

- Безперервний моніторинг передбачає збір даних про всі дії користувачів у системі: вхід у мережу, копіювання файлів, доступ до серверів, пересилання листів тощо. Це дозволяє виявляти відхилення від звичайних моделей поведінки.
- Поведінковий аналіз полягає у використанні алгоритмів машинного навчання, які розпізнають аномалії у діях користувачів — наприклад, доступ до незвичних ресурсів, зміни облікових записів, великі обсяги копіювання даних.
- Багаторівневий захист означає комбінування технічних, організаційних і адміністративних методів для створення цілісної системи попередження інцидентів.

Технічні методи виявлення інсайдерських атак складаються з моніторингу активності користувачів (User Activity Monitoring, UAM) Цей підхід забезпечує постійне спостереження за діями працівників у системах, запис операцій, відвіданих ресурсів, використання зовнішніх носіїв. Він допомагає фіксувати спроби копіювання або передачі критичних даних. Приклади таких систем: Ekran System, Teramind, ObserveIT. Аналіз поведінки користувачів і сутностей (UEBA— User and Entity Behavior Analytics) UEBA-системи використовують алгоритми штучного інтелекту для створення профілів нормальної поведінки кожного користувача та виявлення аномалій. Наприклад, якщо співробітник, який зазвичай працює з одним відділом даних, раптом починає копіювати великі обсяги інформації з іншого сервера, система сигналізує про потенційну загрозу. Відомі рішення: Exabeam, Securonix, Varonis, Splunk UBA. Системи запобігання витоку даних (DLP — Data Loss Prevention) DLP-рішення контролюють переміщення інформації в межах корпоративного середовища — електронна пошта, месенджери, зовнішні носії, хмарні сервіси. У разі виявлення передачі конфіденційних файлів система

блокує дію та повідомляє адміністратора. Популярні продукти: Symantec DLP, Forcepoint, Safetica, McAfee Total Protection. Контроль доступу та привілеїв (IAM/PAM) IAM (Identity and Access Management) забезпечує управління обліковими записами, багатофакторну автентифікацію та контроль доступу до даних на основі ролей. PAM (Privileged AccessManagement) контролює дії користувачів із розширеними правами, (Рис. 2.1.).

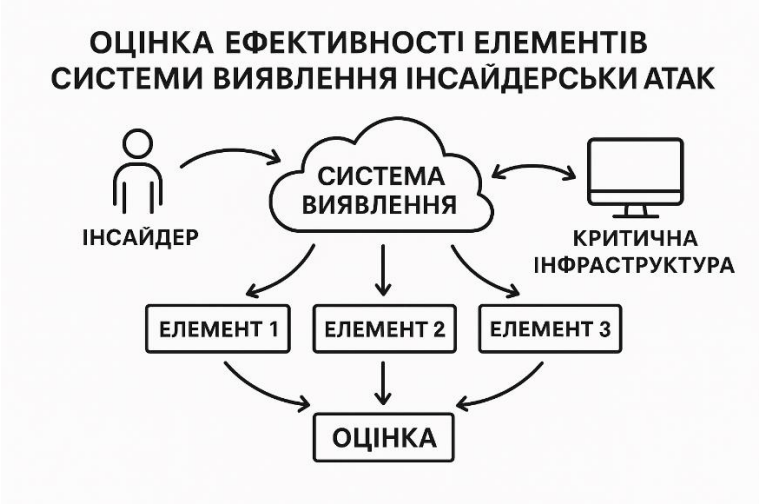

Рис. 2.1. Оцінка ефективності

SIEM-системи збирають і аналізують журнали подій з різних джерел (сервери, мережеві пристрої, робочі станції) для виявлення нетипових шаблонів активності. У поєднанні з UEBA вони дозволяють швидко реагувати на потенційні інциденти.

Технічні засоби не можуть повністю гарантувати безпеку без підтримки на організаційному рівні. Ефективне попередження інсайдерських загроз передбачає комплекс заходів, зокрема:

- Розробку політики інформаційної безпеки, що чітко визначає права доступу, правила обробки даних, процедури реагування на інциденти.
- Регулярний аудит безпеки — перевірка дотримання політик, тестування вразливостей, аналіз журналів доступу.
- Навчання персоналу — тренінги, симуляції фішингових атак, роз’яснення ризиків соціальної інженерії.

- Сегментацію інформаційних ресурсів — розмежування критичних даних за рівнями доступу, що мінімізує наслідки у разі компрометації одного користувача.
- Принцип мінімальних привілеїв (Least Privilege) — кожен працівник має доступ лише до тих даних, які необхідні для виконання його обов’язків.
- Система повідомлення про підозрілу активність (Insider Threat Reporting Program) — заохочення співробітників повідомляти про аномальні або підозрілі дії колег.

В організаціях, що працюють із критичною інфраструктурою, застосовуються:

- Періодичні перевірки лояльності персоналу, тестування на дотримання етичних стандартів;
- Програми підтримки працівників, які зменшують ризики емоційного вигорання чи конфліктів;
- Політика “zero trust”, що передбачає недовіру до будь-якої дії, доки вона не буде перевірена технічно або адміністративно.

Прикладами практичного застосування методів виявлення інсайдерів є:

- NASA впровадила систему Insider Threat Program, що поєднує технічний моніторинг і психологічний аналіз персоналу. Це дозволило виявити понад 40 потенційних інцидентів ще до їх реалізації.
- Енергетичні компанії України після атак BlackEnergy інтегрували SIEM-системи (наприклад, IBM QRadar) із UEBA-модулями, що дало змогу скоротити час виявлення внутрішніх інцидентів на 60%.
- Bank of America використовує DLP-платформу Forcepoint, що блокує передачу внутрішньої документації за межі корпоративної мережі.

2.3. Розробка системи управління інцидентами безпеки

Система управління інцидентами інформаційної безпеки (Security Incident Management System — SIMS) є фундаментальним елементом побудови ефективної стратегії кіберзахисту в сучасних умовах цифрової трансформації та зростання кіберзагроз. Її головне завдання — забезпечення безперервного циклу виявлення,

реагування, усунення, документування та вдосконалення механізмів захисту від інцидентів, що загрожують конфіденційності, цілісності або доступності інформації.

Система управління інцидентами безпеки являє собою комплекс організаційних, технічних і аналітичних заходів, спрямованих на своєчасне виявлення та усунення кіберінцидентів, а також на аналіз причин їх виникнення. У сучасному розумінні SIMS — це не лише набір інструментів моніторингу, а цілісна система управління ризиками, інтегрована з іншими елементами інформаційної безпеки, такими як SIEM, SOAR, UEBA, DLP, PAM, IDS/IPS тощо. Її функціонування базується на принципі «detect – respond – recover – learn» (виявити — відреагувати — відновити — навчитися), який забезпечує безперервний розвиток процесів кіберзахисту.

Розробка системи управління інцидентами починається з етапу підготовки, який передбачає створення політик безпеки, процедур реагування, навчання персоналу, формування спеціалізованих команд реагування на інциденти — CSIRT (Computer Security Incident Response Team) або CERT (Computer Emergency Response Team). На цьому етапі визначаються ключові ролі, відповідальність, засоби моніторингу та звітності. Дуже важливою складовою є створення каталогу типових інцидентів, який дозволяє стандартизувати реакцію на певні типи подій.

Після етапу підготовки йде виявлення та ідентифікація інцидентів, які здійснюються за допомогою систем збору та аналізу подій (SIEM — Security Information and Event Management). Такі системи збирають журнали подій із серверів, мережевих пристроїв, додатків і користувацьких станцій, корелюють ці дані та виявляють відхилення від нормальної поведінки. У сучасних рішеннях активно застосовується UEBA-аналітика (User and Entity Behavior Analytics), яка використовує машинне навчання для виявлення нетипових дій користувачів — наприклад, доступ до незвичних ресурсів, скачування великого обсягу даних чи підозрілі спроби входу в систему в неробочий час.

Наступним етапом є класифікація та оцінка інциденту, де визначається його критичність, потенційний вплив на інформаційні системи та бізнес-процеси, а також тип загрози — внутрішня (інсайдерська), зовнішня (кібератака) або комбінована.

Важливо встановити, чи це одинична подія, чи частина більш масштабної атаки. На цьому етапі застосовуються методики оцінки ризиків (Risk Assessment Frameworks), які дозволяють пріоритезувати дії команди реагування.

Після оцінки настає локалізація інциденту (Containment) — ізоляція заражених або скомпрометованих систем, блокування шкідливих процесів, обмеження доступу до уражених сегментів мережі. Локалізація може бути короткостроковою (термінові дії для запобігання поширенню загрози) або довгостроковою (глибока реконфігурація системи з метою уникнення повторного інциденту).

Коли загрозу ізольовано, здійснюється усунення (Eradication) — видалення шкідливих компонентів, очищення журналів, відновлення працездатності систем, встановлення оновлень безпеки. Після цього відбувається етап відновлення (Recovery), у межах якого системи поступово повертаються до нормального режиму роботи під контролем фахівців.

Найважливіший етап — аналіз і вдосконалення (Lessons Learned). На цьому етапі проводиться глибокий розбір інциденту: як він виник, чому не був виявлений раніше, які прогалини існують у системі безпеки, які заходи необхідно впровадити, щоб уникнути повторення. Результати документуються у звітах (Incident Reports), формуються аналітичні висновки, які використовуються для оновлення політик, процедур, конфігурацій систем. Таким чином, кожен інцидент стає навчальним матеріалом для організації, формуючи корпоративну пам’ять і культуру безпеки.

Архітектура сучасних SIMS включає кілька взаємопов’язаних рівнів. Операційний рівень відповідає за збір та обробку даних — сюди входять системи моніторингу, сенсори, агенти безпеки. Аналітичний рівень обробляє інформацію за допомогою алгоритмів кореляції, штучного інтелекту, поведінкових моделей і візуалізації даних. Рівень реагування реалізується через платформи SOAR (Security Orchestration, Automation and Response), які дозволяють автоматизувати частину процесів реагування — наприклад, блокування користувача, ізоляцію пристрою або генерацію повідомлення для команди безпеки.

Для забезпечення ефективності роботи системи необхідна спеціалізована команда реагування на інциденти (CSIRT/CERT), яка координує дії між технічними

та управлінськими підрозділами, забезпечує обмін інформацією з національними центрами кіберзахисту, проводить розслідування інцидентів, а також бере участь у розробці нових політик.

Одним із найважливіших напрямів розвитку є інтеграція штучного інтелекту та машинного навчання у процес управління інцидентами. AI-рішення дозволяють здійснювати прогностичну аналітику, автоматично класифікувати події, виявляти складні патерни атак, що не піддаються традиційним методам аналізу. AI-рішення в SIMS виконують одразу кілька критичних функцій. По-перше, вони здатні аналізувати величезні обсяги даних у реальному часі, виявляючи приховані закономірності та аномалії, які можуть свідчити про потенційні інциденти. На відміну від класичних систем моніторингу, які працюють на основі заздалегідь визначених правил або сигнатур, AI-моделі самостійно навчаються на поведінці користувачів і систем, виявляючи навіть невідомі типи атак (так звані zero-day threats).

Одним із найпоширеніших напрямів використання AI у сфері кібербезпеки є поведінковий аналіз (User and Entity Behavior Analytics — UEBA). AI-алгоритми відстежують активність користувачів, пристроїв і додатків, формуючи профілі звичної поведінки. Якщо система виявляє відхилення — наприклад, спробу входу до системи в незвичний час, доступ до нетипових файлів чи передачу великого обсягу даних на зовнішні сервери — вона автоматично генерує попередження або активує процедуру реагування. Таким чином, AI допомагає виявляти інсайдерські загрози та складні багатоступеневі атаки, які часто залишаються непоміченими традиційними методами.

Ще один важливий аспект — автоматизація реагування на інциденти. AI інтегрується з платформами SOAR (Security Orchestration, Automation and Response), що дозволяють виконувати рутинні завдання без участі людини: блокування облікових записів, ізоляцію заражених систем, оновлення політик доступу, повідомлення аналітиків. Наприклад, якщо AI-система виявляє підозрілу активність, вона може самостійно перевірити її контекст (зокрема IP-адресу, історію дій користувача, наявність відомих ознак компрометації), а потім прийняти рішення про

блокування чи ескалацію інциденту. Це значно скорочує час реагування (MTTR — Mean Time to Respond) і знижує навантаження на аналітиків SOC.

AI також активно застосовується у прогностичній аналітиці (Predictive Threat Intelligence). На основі аналізу історичних даних, відкритих джерел (OSINT), індикаторів компрометації (IoC) та загроз (TTP — Tactics, Techniques, and Procedures), AI може передбачати можливі напрямки майбутніх атак. Такі рішення дозволяють проактивно зміцнювати захист, наприклад, шляхом динамічного налаштування міжмережевих екранів або зміни політик доступу до критичних ресурсів (Рис. 2.2.).

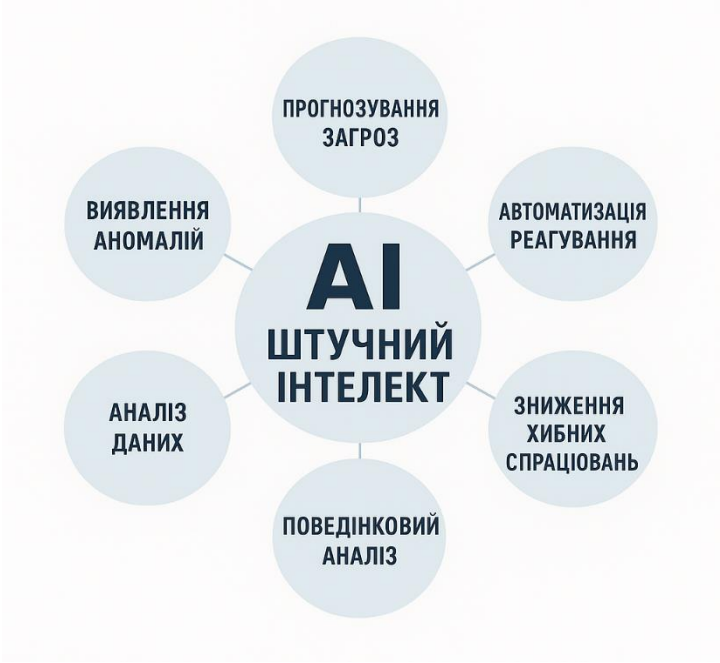

Рис 2.2. Штучний інтелект

В українських реаліях AI-рішення також поступово впроваджуються у державному секторі та критичній інфраструктурі. CERT-UA, НКЦК (Національний координаційний центр кібербезпеки) та інші структури активно досліджують можливості застосування машинного навчання для аналізу телеметричних даних і прогнозування атак, зокрема з боку державних акторів.

Перспективи розвитку AI у системах управління інцидентами безпеки полягають у переході від реактивного до проактивного та адаптивного захисту. Завдяки постійному навчанню моделі зможуть не лише реагувати на вже відомі

загрози, а й передбачати їх появу, пропонуючи оптимальні заходи безпеки в режимі реального часу. Інтеграція AI з технологіями Big Data, Blockchain і Quantum Security у майбутньому дозволить створити інтелектуальні екосистеми кіберзахисту, здатні забезпечувати стійкість критичної інфраструктури навіть у найскладніших умовах гібридних загроз.

Розробка системи управління інцидентами також передбачає впровадження національних і міжнародних стандартів. Найпоширенішими є ISO/IEC 27035 «Information Security Incident Management», NIST SP 800-61 «Computer Security Incident Handling Guide», COBIT 5 for Information Security, ITIL Incident Management. Вони визначають методологію, принципи документування, вимоги до етапів реагування, ролей і звітності. Використання таких стандартів забезпечує сумісність між різними системами та структурами, полегшуючи обмін інформацією між організаціями.

2.4. Огляд сучасних рішень та технологій безпеки на ринку

Сучасний ринок кібербезпеки пропонує широкий спектр технологій і рішень, спрямованих на забезпечення захисту інформаційних систем від зовнішніх і внутрішніх загроз. Особливу роль ці інструменти відіграють у установах критичної інфраструктури, де порушення безпеки може призвести до серйозних наслідків для держави, економіки чи життя громадян. Значна частина підприємств, установ та організацій усіх форм власності не забезпечують кіберзахист електронних інформаційних ресурсів, якими вони розпоряджаються, що призводить до порушень прав користувачів цифрових послуг та дискредитує процеси цифрової трансформації в державі [27]. Нижче наведено детальний аналіз основних категорій технологій безпеки, які сьогодні формують основу кіберзахисту.

Системи SIEM є ядром будь-якої сучасної інфраструктури безпеки. Вони забезпечують централізований збір, аналіз, збереження та кореляцію подій безпеки з усіх компонентів IT-інфраструктури — серверів, робочих станцій, мережевого обладнання, систем контролю доступу, баз даних тощо. Основна функція SIEM —

виявлення аномалій і порушень, які можуть вказувати на потенційну атаку або внутрішню загрозу. Системи аналізують тисячі логів за секунду, зіставляючи їх із шаблонами поведінки, сигнатурами атак, історичними даними та політиками безпеки.

Переваги:

- Цілодобовий моніторинг усіх подій у мережі.
- Виявлення складних багаторівневих атак завдяки кореляції подій.
- Інтеграція з іншими системами безпеки (DLP, UEBA, SOAR).
- Генерація звітів для аудиту, аналізу інцидентів та відповідності стандартам (ISO 27001, NIST, GDPR).

Найпопулярніші рішення:

- IBM QRadar — корпоративна платформа з потужним аналітичним ядром, підтримкою машинного навчання та автоматизованим реагуванням.
- Splunk Enterprise Security — високопродуктивне рішення з можливістю побудови візуальних аналітичних панелей (dashboard).
- ArcSight (Micro Focus) — класична SIEM-система з розвиненою системою правил кореляції.
- Microsoft Sentinel — хмарне SIEM-рішення з інтеграцією в Azure та Office 365.

В енергетичних компаніях SIEM використовується для моніторингу SCADA-систем, виявлення несанкціонованих змін у параметрах керування та спроб віддаленого доступу до промислових контролерів.

SOAR — це платформа для автоматизації процесів реагування на інциденти безпеки, яка поєднує дані з різних систем (SIEM, антивірус, IDS/IPS, DLP) і виконує визначені сценарії дій. SOAR дозволяє зменшити час реагування (MTTR), виключити людські помилки й оптимізувати роботу SOC-команд.

Переваги:

- Автоматичне виконання дій у разі інциденту (наприклад, блокування користувача, ізоляція пристрою).
- Централізована координація дій між різними системами безпеки.

- Можливість створення кастомних сценаріїв реагування (Playbooks).
- Підвищення ефективності роботи аналітиків безпеки.

Популярні рішення:

- Palo Alto Cortex XSOAR — одна з найвідоміших платформ, що поєднує оркестрацію, автоматизацію та аналітику інцидентів.
- Splunk Phantom — гнучке рішення з можливістю створення візуальних сценаріїв реагування.
- IBM Resilient — система для інтеграції аналітики, форензики й реагування.
- ServiceNow Security Operations — платформа з потужним управлінням інцидентами та автоматизацією процесів SOC.

У банківському секторі SOAR використовується для автоматичної обробки фішингових інцидентів: при отриманні підозрілого листа система блокує домен, повідомляє користувача, додає дані в базу IOC та створює звіт у SIEM.

UEBA-системи використовують машинне навчання для аналізу поведінки користувачів і пристроїв у мережі. Вони формують профілі звичної активності та виявляють відхилення, що можуть свідчити про зловмисні дії або інсайдерську активність.

Переваги:

- Виявлення інсайдерських загроз (навмисних або випадкових).
- Виявлення компрометації облікових записів (спроби входу в незвичний час, підозрілі запити).
- Побудова поведінкових моделей користувачів, систем, пристроїв IoT.
- Зменшення кількості хибних спрацювань у SIEM.

Відомі рішення:

- Exabeam — провідна UEBA-платформа з фокусом на поведінкову аналітику користувачів.
- Securonix — система, що поєднує AI-аналітику з інтеграцією у хмарні сервіси.
- Varonis — спеціалізується на контролі доступу до конфіденційних файлів.

- Microsoft Defender for Identity — інструмент для відстеження підозрілої поведінки в Active Directory.

У державних установах UEBA допомагає виявляти інсайдерів, які копіюють або передають секретні документи за межі дозволених каналів.

Системи DLP контролюють рух, зберігання та обробку даних, щоб запобігти їх витоку або несанкціонованому доступу. Вони відстежують передачу файлів через електронну пошту, зовнішні носії, хмарні сервіси та інші канали.

Основні переваги:

- Захист конфіденційних даних (державна таємниця, персональні дані, фінансова інформація).
- Моніторинг дій користувачів у реальному часі.
- Контроль копіювання, друку, збереження та пересилання файлів.
- Вбудована система політик доступу.

Найкращі продукти:

- Symantec DLP — комплексне рішення з підтримкою хмарних середовищ.
- Forcepoint DLP — система з глибокою контекстною аналітикою.
- Digital Guardian — забезпечує контроль дій користувачів навіть у офлайн-режимі.
- Safetica — доступне рішення для малих і середніх підприємств (Рис. 2.3.).

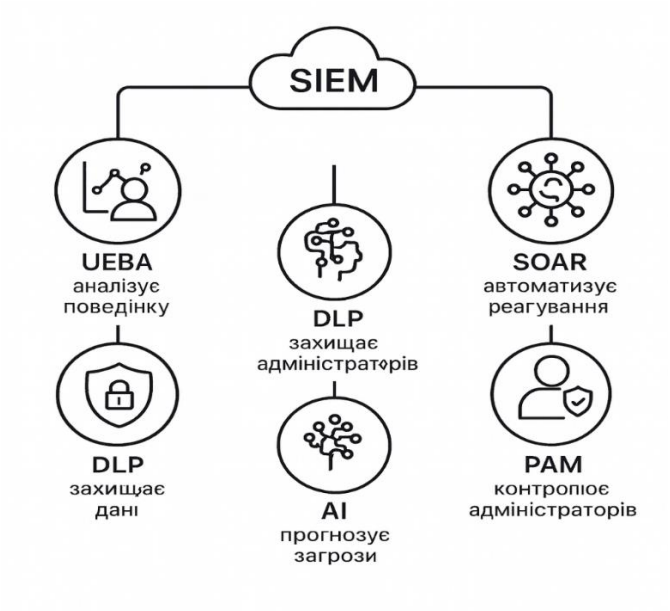

Рис. 2.3. Системи та технології

Системи PAM контролюють дії користувачів із підвищеними привілеями (адміністраторів, системних операторів, розробників). Вони дозволяють записувати сесії, обмежувати доступ і мінімізувати ризики зловживань.

Переваги:

- Повний аудит усіх дій користувачів із привілеями.
- Впровадження політики Least Privilege — мінімально необхідних прав доступу.
- Захист від компрометації облікових записів адміністраторів.
- Можливість швидкого відкликання доступу при інцидентах.

Основні продукти:

- CyberArk — флагманське рішення з розширеними можливостями контролю сесій.
- BeyondTrust — система, що підтримує гібридні та хмарні середовища.
- Thycotic/Delinea Secret Server — орієнтована на автоматизацію управління паролями.
- One Identity Safeguard — комплексне рішення для великих організацій.

У банках PAM використовується для запису дій системних адміністраторів і виявлення спроб несанкціонованого доступу до баз даних клієнтів.

Zero Trust — це концепція “не довіряй нікому”, навіть користувачам усередині мережі. Кожен запит до ресурсу вимагає перевірки автентичності, контексту, місця, часу та пристрою.

Основні принципи:

- Перевірка кожної взаємодії незалежно від місця розташування користувача.
- Динамічне управління доступом залежно від рівня ризику.
- Мікросегментація мережі — поділ системи на ізольовані зони.
- Постійна верифікація дій користувачів.

Відомі рішення:

- Microsoft Zero Trust Framework, Cisco Duo, Okta Zero Trust, Google BeyondCorp.

AI (штучний інтелект) і ML (машинне навчання) відіграють вирішальну роль у побудові інтелектуальних систем безпеки нового покоління. Вони використовуються для аналізу поведінки користувачів, прогнозування атак, автоматичного реагування й зменшення кількості хибних сповіщень.

Приклади систем:

- Darktrace — система на основі штучного інтелекту, яка самостійно виявляє невідомі загрози.
- Vectra AI — аналізує мережеву активність і виявляє аномалії в трафіку.
- Cynet 360 — платформа XDR із повною автоматизацією реагування.
- IBM Watson for Security — AI-аналізатор, що використовує когнітивні алгоритми для розслідування інцидентів.

AI-рішення можуть прогнозувати потенційні атаки на енергетичну систему, аналізуючи велику кількість телеметричних даних у режимі реального часу.

Сучасні рішення кібербезпеки формують багаторівневу, взаємопов’язану екосистему. Їхня сила полягає не лише в індивідуальній функціональності, а у взаємній інтеграції — SIEM збирає дані, UEBA аналізує поведінку, SOAR автоматизує реагування, DLP захищає дані, PAM контролює адміністраторів, а AI прогнозує загрози (Рис. 2.4.).

Рис. 2.4. Огляд сучасних рішень

2.5. Вибір і впровадження систем захисту в установах критичної інфраструктури

Захист інформаційних систем критичної інфраструктури є одним із найважливіших завдань національної безпеки, що вимагає системного підходу до вибору, впровадження та підтримки ефективних рішень з кіберзахисту. В умовах стрімкого зростання кіберзагроз, особливо з боку державних та організованих акторів, установи критичної інфраструктури повинні будувати багаторівневі системи безпеки, здатні не лише реагувати на інциденти, а й передбачати їх появу.

Критерії вибору систем безпеки охоплюють низку аспектів: відповідність нормативно-правовим вимогам України та міжнародним стандартам (ISO/IEC 27001, IEC 62443, NIST SP 800-53), масштабованість, інтеграційна сумісність, гнучкість, автоматизацію процесів і вартість володіння (TCO). Особливу увагу приділяють здатності системи функціонувати безперервно навіть під час збоїв або атак, а також можливості централізованого керування й моніторингу.

Після етапу вибору технологій здійснюється проектування архітектури інформаційної безпеки. Вона базується на принципі багаторівневого захисту (Defense in Depth), що передбачає створення кількох взаємопов’язаних бар’єрів — мережевих, прикладних, організаційних і фізичних. Проектування включає сегментацію мережі, розподіл зон довіри (DMZ, виробничий контур, адміністративна зона), впровадження засобів автентифікації, шифрування та контролю доступу. У промислових середовищах, де працюють системи керування технологічними процесами (SCADA/ICS), захист реалізується без порушення безперервності технологічних операцій, тому особливу роль відіграють пасивні методи моніторингу, мережеві шлюзи безпеки й системи аналізу аномалій.

Етап впровадження передбачає інсталяцію програмно-апаратних засобів, їх налаштування, інтеграцію між компонентами та тестування працездатності. У цей період розробляються політики доступу, створюються аналітичні правила, автоматизовані сценарії реагування (playbooks), налаштовується збір логів і формування звітів. Важливим елементом є підготовка персоналу: адміністратори,

аналітики SOC (Security Operations Center) та інженери з безпеки мають пройти навчання щодо роботи з консолями моніторингу, аналізу подій, реагування на інциденти. Після розгортання системи проводиться аудит безпеки й тестування, у тому числі пенетраційне, яке дозволяє оцінити її стійкість до атак і відповідність політикам. Для підвищення ефективності кіберзахисту установа має впровадити систему управління інформаційною безпекою (ISMS) відповідно до стандарту ISO/IEC 27001. Вона передбачає формування політик, визначення ролей і відповідальності персоналу, управління ризиками, а також безперервне вдосконалення за циклом PDCA (Plan – Do – Check – Act). Таким чином, безпека перестає бути одноразовим проектом і стає постійним процесом, інтегрованим у корпоративне управління.

На практиці українські підприємства вже демонструють приклади ефективного впровадження систем захисту. В енергетичному секторі «Укренерго» та «ДТЕК» реалізували централізовані SOC-платформи з використанням SIEM, PAM та DLP. У фінансовому секторі Національний банк України створив систему моніторингу кіберінцидентів, що об’єднує банки в єдину мережу обміну даними про загрози. У телекомунікаціях компанії «Київстар» та «Укртелеком» використовують XDR-рішення з елементами поведінкової аналітики та автоматизованого реагування. (Рис. 2.5.).

Рис. 2.5. Вибір і впровадження систем захисту

Запровадження системного підходу до розв’язання проблем захищеності критичної інфраструктури, звичайно, виходить далеко за межі лише введення відповідного терміна. На першому місці – створення дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди вуз ловим елементам критичної інфраструктури внаслідок дії негативних чинників будь-якого походження: техногенного, природного, соціальнополітичного або будь-якої їх комбінації [32].

Висновки до розділу 2

Ефективна протидія інсайдерським загрозам вимагає комплексного підходу, що передбачає інтеграцію технологічних, організаційних та людських компонентів. З технологічного погляду, важливими елементами є системи моніторингу активності користувачів, рішення для запобігання витокам інформації (DLP), платформи для збору та кореляції подій безпеки (SIEM), а також технології аналізу поведінкових аномалій (UEBA). Використання штучного інтелекту (ШІ) та машинного навчання (МН) дозволяє підвищити точність виявлення аномалій та своєчасно ідентифікувати потенційні загрози до їх реалізації.

З організаційної точки зору необхідно розробити та впровадити політику інформаційної безпеки, що регламентує права доступу до інформаційних ресурсів, порядок використання ресурсів, обов'язки співробітників та процедури реагування на інциденти. Важливими принципами є "мінімальний доступ" (Least Privilege) та "Zero Trust" — принцип недовіри до будь-якого користувача чи пристрою без постійної перевірки їх прав. Важливим аспектом є також створення системи управління інформаційною безпекою (ISMS), що забезпечує надійний контроль, аудит і постійне вдосконалення процесів.

Окрему увагу слід приділяти людському фактору. Підготовка персоналу, формування культури безпеки, навчання правилам кібергігієни та етичному поводженню з інформацією є ключовими для зменшення ризиків, пов'язаних з помилками або недбалістю співробітників. Регулярні тренінги, моделювання фішинг-атак і навчання реагуванню на інциденти дозволяють мінімізувати можливість помилок з боку персоналу.

РОЗДІЛ 3.
ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ ВНУТРІШНІХ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Цифровізації суспільства та зростання обсягів оброблюваної інформації а також питання забезпечення інформаційної безпеки набуває стратегічного значення. Якщо раніше основна увага приділялася захисту від зовнішніх кіберзагроз — хакерських атак, вірусів чи несанкціонованого втручання ззовні, то нині дедалі більшої актуальності набуває проблема внутрішніх загроз. Ці загрози пов’язані з діяльністю осіб, які мають легальний доступ до інформаційних систем — співробітників, адміністраторів, підрядників або партнерів. Саме такі інсайдерські ризики становлять особливу небезпеку, оскільки зловмисники мають глибоке знання внутрішніх процесів, прав доступу та технологічних особливостей системи. Ключовим напрямом розвитку України є імплементація міжнародних стандартів та розширення міжнародного співробітництва. Україна активно взаємодіє з Європейським Союзом, НАТО, США та іншими партнерами у сфері кіберзахисту. Важливими є проєкти, що спрямовані на обмін інформацією про кіберзагрози, навчання спеціалістів та впровадження технологічних рішень для зміцнення стійкості критичної інфраструктури [12].

Внутрішні загрози можуть мати як навмисний, так і ненавмисний характер. У першому випадку вони спрямовані на крадіжку або знищення даних, саботаж, несанкціоновану зміну інформації чи підрив репутації організації. У другому — є наслідком людської помилки, нехтування політиками безпеки або неуважності користувачів. Особливо небезпечними такі ризики є для об’єктів критичної інфраструктури, де навіть незначний інцидент може спричинити значні економічні збитки, соціальні наслідки чи порушення національної безпеки.

Метою цього розділу є комплексне дослідження технологій і методів, що дозволяють виявляти, запобігати та нейтралізувати внутрішні загрози в системах інформаційної безпеки. Розділ присвячений аналізу як організаційних, так і

технічних підходів, що у сукупності формують ефективну модель протидії інсайдерським ризикам.

Зокрема, у розділі розглянуто принципи розробки політики безпеки та нормативної документації, використання криптографічних методів для забезпечення конфіденційності та цілісності інформаційних даних, впровадження систем моніторингу та аудиту доступу, застосування біометричних технологій, які підвищують точність автентифікації та мінімізують ризик підробки облікових даних, роль антивірусних і антишпигунських засобів у боротьбі з внутрішніми кіберзагрозами, впровадження аналітичних інструментів UBA та UEBA.

Розгляд зазначених аспектів дозволяє сформувати цілісне уявлення про архітектуру сучасної системи захисту інформації, орієнтованої не лише на зовнішні загрози, а й на внутрішні ризики, які часто є найважчими для виявлення. Таким чином, розділ спрямований на обґрунтування необхідності інтеграції організаційних, програмно-технічних і поведінкових механізмів у єдину систему протидії інсайдерським загрозам, що забезпечує надійний і безперервний захист інформаційних активів організації.

Коли відбувається кризова ситуація, цілі стійкості критично важливої інфраструктури можна оцінити у двох вимірах: обмеження масштабу пошкоджень та обмеження тривалості перерви у наданні послуг, спричиненої пошкодженнями. Важливо зазначити, що відновлення не обов'язково означає повернення до попереднього стану, який існував до надзвичайної ситуації або інциденту, але може передбачати зміну, адаптацію до нових умов та покращення функціональності систем [50].

3.1. Розробка політики безпеки та нормативної документації

Розробка політики інформаційної безпеки є одним із ключових етапів створення ефективної системи захисту інформаційних ресурсів організації. Політика безпеки виступає базовим документом, який визначає мету, принципи, завдання та механізми забезпечення інформаційної безпеки. Її призначення полягає у створенні

єдиного стандарту поведінки працівників, встановленні правил доступу до інформаційних активів, а також визначенні відповідальності за порушення встановлених норм.

Першим кроком у розробці політики інформаційної безпеки є проведення аналізу ризиків, спрямованого на ідентифікацію потенційних загроз, оцінку вразливостей і визначення рівня впливу кожного ризику на бізнес-процеси організації. Аналіз дає змогу визначити найважливіші об’єкти захисту: конфіденційні дані, персональну інформацію, комерційну таємницю, корпоративну документацію, інформаційні системи, мережеві ресурси, сервери та засоби зв’язку. На основі цього формується карта ризиків, де визначаються пріоритетні напрямки для розробки заходів безпеки.

Наступним етапом є визначення цілей і принципів інформаційної безпеки. Основними принципами виступають конфіденційність, цілісність, доступність та підзвітність інформації. Принцип конфіденційності передбачає захист даних від несанкціонованого доступу або розголошення. Цілісність означає збереження достовірності та незмінності інформації в процесі її обробки, передачі та зберігання. Принцип доступності гарантує можливість легального користувача отримати доступ до потрібних даних у будь-який момент часу, коли це необхідно для виконання службових обов’язків. Підзвітність забезпечує можливість простежити всі дії користувачів, що дозволяє виявляти інциденти безпеки та визначати винних у їх виникненні.

Політика безпеки має чітку структуру, яка забезпечує системність і повноту викладення. Зазвичай документ включає такі розділи: загальні положення, цілі, область застосування, терміни та визначення, організаційну структуру управління інформаційною безпекою, політику управління доступом, правила використання паролів і засобів автентифікації, політику резервного копіювання, порядок роботи з конфіденційною інформацією, правила використання мережевих ресурсів, політику реагування на інциденти, контроль виконання та порядок внесення змін до політики.

Важливою складовою політики безпеки є розробка нормативної та розпорядчої документації, яка конкретизує та деталізує положення основного документу. До

такої документації належать: положення про інформаційну безпеку, інструкції з користування комп'ютерними системами, регламент управління доступом, політика створення та використання паролів, правила резервного копіювання і відновлення даних, порядок дій у разі виявлення інцидентів безпеки, політика щодо використання персональних пристроїв (BYOD), а також документи, які регламентують процедури реагування на надзвичайні ситуації. Ці документи формують нормативну базу, на основі якої здійснюється повсякденна робота з інформаційними ресурсами.

Організаційна структура системи управління безпекою передбачає призначення відповідальних осіб, таких як фахівець або відділ з інформаційної безпеки (CISO, Security Officer), системні адміністратори, аудитори безпеки. Вони координують впровадження політики, здійснюють контроль за її дотриманням, проводять внутрішні перевірки та навчання персоналу. Визначення зон відповідальності є необхідним для забезпечення ефективного управління інцидентами, уникнення конфлікту інтересів і зменшення ризику навмисних або випадкових порушень безпеки. Для ефективної взаємодії усіх учасників процесу запроваджується система звітності та моніторингу, яка дозволяє відслідковувати події в інформаційних системах, фіксувати порушення та оперативно реагувати на них.

Після розробки політики безпеки необхідним етапом є її впровадження. Кожен співробітник повинен бути ознайомлений із положеннями політики під підпис, а керівники підрозділів мають забезпечити контроль її виконання. Для моніторингу дотримання правил використовуються технічні засоби — системи аудиту, журналювання подій, моніторинг доступу до критичних ресурсів. У результаті впровадження політики безпеки формується чітка, контрольована система управління інформаційною безпекою, у межах якої кожен співробітник розуміє свої права, обов'язки та межі відповідальності. Такий підхід дозволяє значно знизити ризики внутрішніх загроз, мінімізувати можливість несанкціонованого доступу до інформації, а також створює правові підстави для реагування у разі інцидентів. Наявність нормативної документації забезпечує організаційний фундамент усіх

подальших заходів — від криптографічного захисту до систем моніторингу й аудиту (Рис. 3.1.).

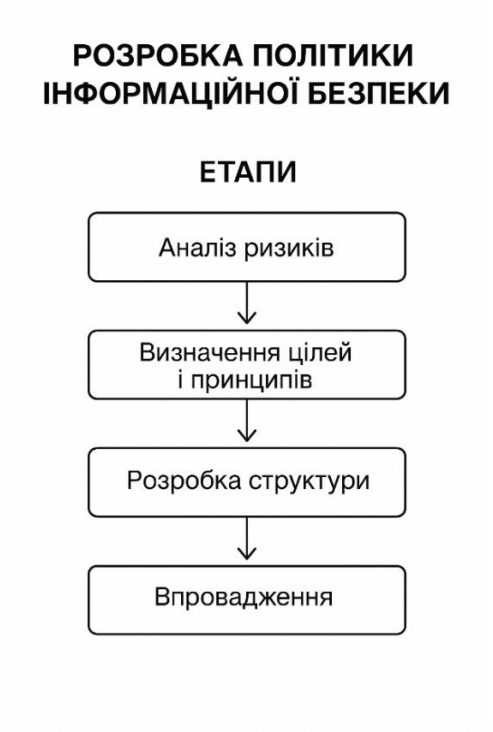

Рис. 3.1. Етапи розробки

3.2. Використання криптографії для захисту інформаційних даних

Необхідність захисту критичної інфраструктури надзвичайно важлива для нормального функціонування держави, особливо під час сучасних загроз, пов’язаних із військовими діями та постійними обстрілами цивільних міст. У зв’язку з цим, уряд нашої країни посилює заходи безпеки для об’єктів, які вважаються критичними для життєдіяльності суспільства. Нині існує цілий комплекс заходів, який складається з моніторингу та швидкого реагування на можливі загрози: терористичні атаки, кібератаки, природні катастрофи тощо [46].

Криптографія є одним із найефективніших інструментів забезпечення інформаційної безпеки. Її головне завдання полягає у захисті інформаційних ресурсів від несанкціонованого доступу, змін, підроблення чи знищення. Застосування криптографії підвищує кіберстійкість (cyber resilience) об’єктів критичної інфраструктури, тобто їх здатність протистояти, виявляти, реагувати та

відновлюватися після кіберінцидентів. Шифрування даних, контроль автентичності користувачів, перевірка підписів та захист комунікацій роблять системи значно стійкішими до атак типу man-in-the-middle, spoofing, data tampering або ransomware.

Сучасні системи управління критичними об’єктами (наприклад, SCADA, ICS, DCS) часто обмінюються величезними обсягами чутливої інформації: показниками датчиків, командами управління, телеметричними даними тощо. Якщо зловмисник отримає доступ до цих даних або змінить їх у процесі передавання, це може призвести до зупинки виробництва, пошкодження обладнання або навіть загрози для життя людей.

Ключові напрями використання криптографії в захисті критичної інфраструктури:

1. Шифрування каналів зв’язку.

Для передачі технологічних і адміністративних даних між елементами інфраструктури використовуються захищені протоколи — TLS, IPSec, SSH, VPN. Вони забезпечують конфіденційність трафіку, запобігають перехопленню або модифікації даних у процесі передавання.

2. Захист даних у стані зберігання (data at rest).

Криптографічне шифрування використовується для збереження даних на серверах, контролерах, промислових комп’ютерах і мобільних пристроях. Навіть якщо фізичний носій буде викрадений або скомпрометований, зловмисник не отримає доступу до інформації без ключів. Для цього використовуються алгоритми AES-256, ChaCha20, або системи повнодискового шифрування на кшталт BitLocker, VeraCrypt.

3. Цифрові підписи та сертифікація.

Для підтвердження справжності джерела інформації застосовується електронний цифровий підпис (ЕЦП). Він дозволяє перевірити, що дані були створені автентичним відправником і не зазнали змін після підписання сертифікатами користувачів, серверів і пристроїв. Це дозволяє гарантувати, що лише довірені елементи мають право на взаємодію в межах мережі.

4. Хешування та контроль цілісності.

Криптографічні хеш-функції (наприклад, SHA-3 або BLAKE2) використовуються

для перевірки незмінності критичних даних, програмного коду та конфігураційних файлів.

5. Захист доступу та автентифікація користувачів.

У системах КІІ впроваджується багатофакторна автентифікація (MFA), що включає криптографічні токени, смарт-карти, біометричні дані та одноразові ключі. Це запобігає несанкціонованому входу навіть у разі компрометації паролів.

6. Безпечне оновлення програмного забезпечення.

Криптографічні підписи забезпечують довіру до оновлень у промислових системах. Будь-яке оновлення має бути підписане розробником, і система перевіряє цей підпис перед встановленням, що унеможливлює встановлення шкідливого коду.

Застосування криптографії у сфері критичної інфраструктури регламентується як міжнародними, так і національними нормативно-правовими документами. Основними є:

- ISO/IEC 27001 — стандарт управління інформаційною безпекою;
- ISO/IEC 19790 — вимоги до криптографічних модулів;
- NIST FIPS 140-3 — стандарт безпеки криптографічних компонентів;

7. ДСТУ 4145-2002, ДСТУ ISO/IEC 10118-3:2019, ДСТУ 7624:2014 — українські стандарти для реалізації криптографічних алгоритмів і хеш-функцій (Рис. 3.1.).

Рис. 3.1 Використання криптографії

Використання перевірених стандартів гарантує сумісність рішень, надійність криптографічного захисту та відповідність вимогам законодавства України у сфері кібербезпеки. Захист інформації у мережах і корпоративних системах базується на стандартизованих криптографічних протоколах, які забезпечують сумісність та надійність. До них належать: SSL/TLS — протокол захисту комунікацій у мережі Інтернет, який гарантує безпечне з'єднання між клієнтом і сервером (використовується в HTTPS). IPSec — протокол безпечного обміну даними в мережах, що лежить в основі VPN-з'єднань. PGP (Pretty Good Privacy) — застосовується для шифрування електронної пошти. S/MIME (Secure/Multipurpose Internet Mail Extensions) — стандарт захищеного обміну повідомленнями. AES (FIPS 197) — стандарт симетричного шифрування, затверджений як офіційний для урядових структур США. RSA (PKCS #1) один із найпоширеніших алгоритмів асиме тричного шифрування. SHA-3 — сучасний стандарт хешування, рекомендований для перевірки цілісності даних.

3.3. Системи моніторингу та аудиту доступу до інформаційних ресурсів

Питанню захисту та моніторингу критичної інфраструктури приділяється значна увага в країнах ЄС та світу. У 2004 р. Європейська Рада висунула вимогу щодо підготовки загальної стратегії охорони та захисту критичної інфраструктури (КІ). У відповідь на це Комісія ухвалила Повідомлення про охорону та захист КІ в рамках боротьби проти тероризму, в якому було викладено пропозиції щодо можливих заходів ЄС щодо попередження, підготованості та реагування на терористичні акти, пов'язані з КІ [40].

Моніторинг у контексті критичної інфраструктури — це безперервний процес збору, фіксації та аналізу даних про події у інформаційних системах, мережах і серверах, який дає змогу виявляти ознаки несанкціонованого втручання або ненормальної активності. Аудит — це систематична перевірка відповідності дій користувачів, адміністраторів та системних процесів вимогам політики безпеки, стандартам і нормативним документам. Інформаційні ресурси критичної

інфраструктури мають підвищену цінність, а тому є основною мішенню для кібератак. За даними міжнародних звітів (ENISA, NIST, CERT-UA), саме на об’єкти КІІ припадає найбільша кількість спроб кібершпигунства, атак типу ransomware, DDoS та внутрішніх порушень. Наслідком таких атак можуть бути збої в енергопостачанні, порушення транспортних систем, банківські колапси або параліч урядових служб.

Системи моніторингу та аудиту є ключовим елементом у виявленні, аналізі та реагуванні на подібні інциденти. Вони дозволяють:

- постійно відстежувати діяльність користувачів і сервісів;
- виявляти аномальні дії, які можуть свідчити про порушення;
- контролювати спроби доступу до критичних компонентів;
- документувати всі події для подальшого розслідування;
- забезпечувати відповідність вимогам національного та міжнародного законодавства у сфері кібербезпеки.

Основні компоненти систем моніторингу в критичних системах:

1. Системи збору та централізації журналів подій (логів). Усі дії користувачів, службових процесів, мережевого обладнання й прикладних програм мають бути зафіксовані у журналах подій. Це включає: входи й виходи із системи, зміни налаштувань, спроби підключення, роботу служб керування, передачу даних через SCADA або інші технологічні мережі.

2. SIEM-системи (Security Information and Event Management).

Вони є серцем інфраструктури моніторингу. SIEM-платформи збирають, нормалізують і аналізують події з різних джерел — серверів, міжмережевих екранів, систем управління доступом, SCADA-контролерів, баз даних. За допомогою кореляційних правил SIEM виявляє підозрілі комбінації подій, що можуть вказувати на атаку або внутрішнє порушення. Для КІІ використовуються сертифіковані рішення, такі як IBM QRadar, ArcSight, Splunk, Wazuh, LogPoint, які відповідають вимогам стандартів ISO/IEC 27001 і NIST SP 800-137.

3. Системи виявлення та запобігання вторгненням (IDS/IPS). Вони здійснюють аналіз мережевого трафіку, шукають аномалії, спроби сканування портів, впровадження шкідливого коду чи витоку інформації.

4. UEBA-системи (User and Entity Behavior Analytics).

Ці системи аналізують поведінку користувачів і пристроїв, формуючи “профілі нормальної активності”. Будь-яке відхилення — наприклад, нетиповий час доступу, завантаження великих обсягів даних або спроби отримати привілеї — розглядається як потенційна загроза.

5. Інфраструктура управління обліковими записами (IAM).

Контролює надання, зміну та відкликання прав доступу користувачів до інформаційних ресурсів. Усі дії з ідентифікацією, автентифікацією та авторизацією фіксуються для подальшого аудиту (Рис. 3.2.).

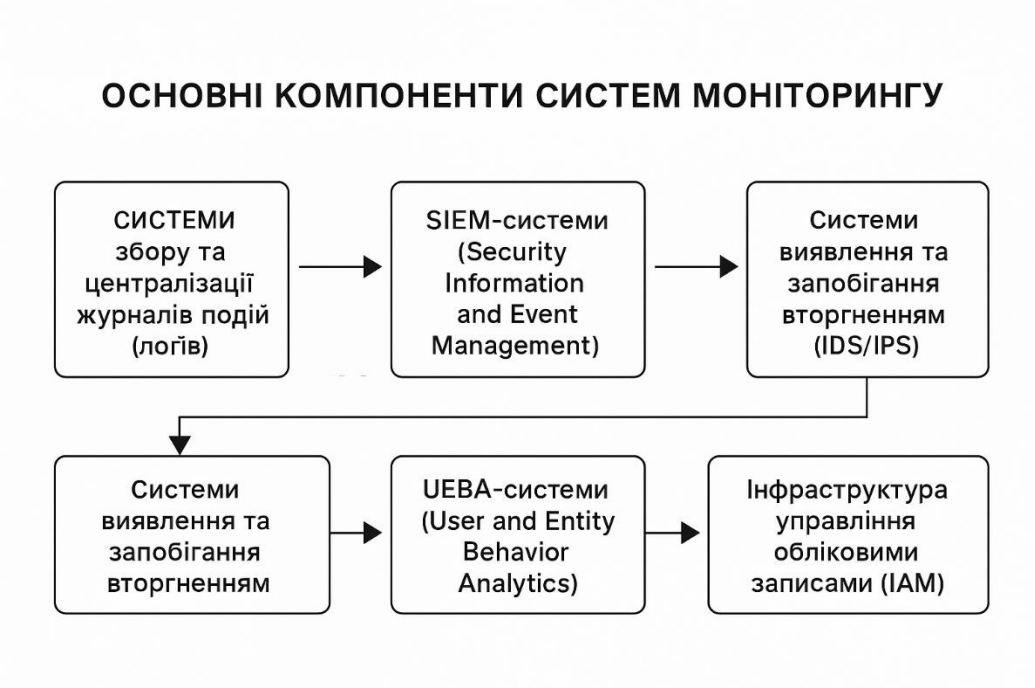

Рис. 3.2. Системи моніторингу

Аудит у системах КІІ має стратегічне значення, оскільки він дозволяє оцінити ефективність засобів захисту та виявити недоліки у процесах управління безпекою. Регулярний аудит забезпечує: перевірку дотримання політик безпеки і вимог законодавства (зокрема, Закону України «Про основні засади забезпечення кібербезпеки»); аналіз історії подій і дій користувачів; виявлення слабких місць у

конфігурації систем і мереж; документування інцидентів для подальшого розслідування. Для проведення аудиту застосовуються як автоматизовані засоби (звітність SIEM, лог-аналітика, сканери вразливостей), так і ручні перевірки, що здійснюються уповноваженими підрозділами кібербезпеки.

Важливою складовою є також реагування на інциденти. Більшість сучасних систем підтримують інтеграцію з SOAR-платформами (Security Orchestration, Automation and Response), які автоматизують процес реагування — блокування користувачів, відключення сегментів мережі, запуск процедур ізоляції або сповіщення адміністраторів.

Оскільки об’єкти критичної інфраструктури є надзвичайно важливими для безпеки держави, системи моніторингу повинні відповідати суворим вимогам:

- безперервна робота 24/7 у реальному часі;
- відмовостійкість і резервування компонентів;
- фізична та логічна сегментація мережі;
- шифрування всіх каналів передачі даних;
- збереження журналів подій протягом визначеного законом терміну (часто — не менше 1 року);
- дотримання національних і міжнародних стандартів безпеки (ISO/IEC 27035, NIST SP 800-137, ДСТУ 8302:2015 тощо).

3.4. Використання біометричних систем для контролю доступу

Біометричні системи використовують індивідуальні ознаки людини для ідентифікації (визначення особи серед зареєстрованих користувачів) або автентифікації (підтвердження, що користувач є саме тим, за кого себе видає). До основних біометричних характеристик належать відбитки пальців, форма обличчя, геометрія долоні, сітківка або райдужна оболонка ока, голос, підпис, а також поведінкові особливості, наприклад, динаміка набору тексту або рухів миші. Завдяки цим характеристикам біометричні системи забезпечують вищий рівень достовірності при перевірці особи, ніж будь-які традиційні засоби автентифікації.

Принцип роботи біометричної системи полягає у зборі, обробці, порівнянні та зберіганні біометричних даних користувачів. Спочатку спеціальний сенсор (наприклад, сканер відбитків пальців або камера розпізнавання обличчя) знімає біометричний зразок. Далі система обробляє отримане зображення, виділяючи ключові ознаки — характерні точки, контури або частотні параметри. Потім формується математичний шаблон, який зберігається у зашифрованому вигляді у базі даних. Під час спроби доступу новий зразок порівнюється з шаблоном, і система приймає рішення про дозвіл або відмову в доступі залежно від рівня збігу.

Біометричні технології поділяються на кілька типів. Найпоширенішим є дактилоскопічна ідентифікація, яка використовує відбитки пальців. Цей метод відзначається високою точністю, швидкістю та доступністю обладнання. Іншим популярним напрямом є розпізнавання обличчя, яке активно розвивається завдяки застосуванню штучного інтелекту та нейронних мереж. Такі системи здатні працювати без фізичного контакту, що робить їх зручними для масового використання. Ідентифікація за райдужною оболонкою чи сітківкою оказабезпечує найвищий рівень безпеки й застосовується у військових, енергетичних і банківських структурах, де потрібен максимальний контроль. Голосова біометрія використовується у дистанційних сервісах, наприклад у банківських контакт-центрах, тоді як поведінкова біометрія аналізує манеру взаємодії користувача з пристроєм і використовується як додатковий рівень захисту у вебсистемах.

Переваги біометричних систем контролю доступу очевидні. Насамперед, вони забезпечують високий рівень надійності, адже біометричні ознаки важко підробити або передати іншій особі. По-друге, такі системи зручні у використанні — користувачеві не потрібно запам’ятовувати складні паролі чи носити додаткові картки. Процес ідентифікації відбувається швидко і майже непомітно. По-третє, біометричні системи зменшують вплив людського фактору, оскільки усувають ризик недбалого ставлення до паролів чи передачі їх колегам. Крім того, біометрію можна інтегрувати з іншими технологіями безпеки, створюючи мультифакторну систему автентифікації, яка поєднує кілька методів перевірки особи (наприклад, біометрію +

смарт-карту + PIN-код). Це суттєво підвищує стійкість системи до несанкціонованого доступу.

Разом із тим, біометричні технології мають і низку недоліків. Найважливішим із них є питання конфіденційності. Біометричні дані є персональними, тому їхня обробка, зберігання і передавання мають здійснюватися відповідно до законодавства про захист персональних даних (GDPR, Закон України «Про захист персональних даних»). Ще одним викликом є технічна вразливість — зміни у фізіологічному стані користувача (травма пальця, зміна голосу, освітлення обличчя тощо) можуть спричинити помилки розпізнавання. У сфері критичної інфраструктури біометричні системи контролю доступу відіграють особливо важливу роль. Вони використовуються для обмеження доступу персоналу до стратегічних об’єктів — центрів обробки даних, диспетчерських пунктів, серверних кімнат, систем SCADA та інших елементів технологічних мереж.

Висока надійність біометричних систем контролю доступу забезпечується дотриманням міжнародних стандартів, серед яких: ISO/IEC 19794 (формати обміну біометричними даними), ISO/IEC 30107 (захист від підроблення), ISO/IEC 24745 (зберігання та управління шаблонами), NIST SP 800-76 (вимоги до біометричних систем у державному секторі). В Україні також діють стандарти серії ДСТУ ISO/IEC 19794, які регламентують формати даних і безпечне використання біометрії (Рис. 3.3.).

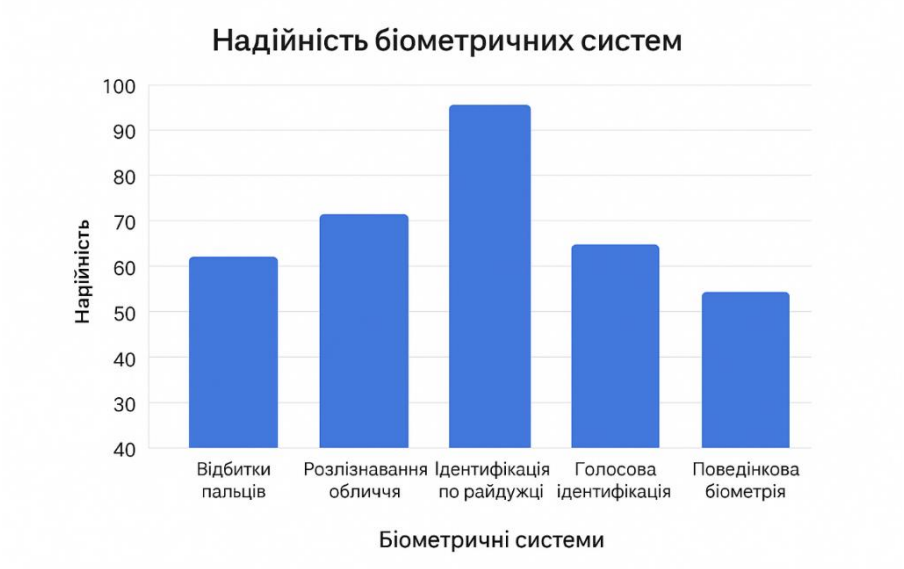

Рис. 3.3. Надійність біометричних систем

3.5. Застосування антивірусних та антишпигунських технологій для боротьби з внутрішніми загрозами

Сьогодні наша держава протистоїть найбільшому виклику у сфері забезпечення державної безпеки. Збройна агресія Російської Федерації спричинила руйнування та пошкодження численних підприємств, а також важливих інфраструктурних об’єктів. Це зумовлює актуалізацію питання захисту систем, об’єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки [34]. Критична інфраструктура держави — це сукупність об’єктів, систем і процесів, від стабільного функціонування яких залежить безпека суспільства, економічна стабільність та життєздатність країни. Одним із ключових напрямів захисту є впровадження антивірусних та антишпигунських технологій, які забезпечують виявлення, попередження та нейтралізацію шкідливих програм, а також мінімізують ризики внутрішніх загроз, пов’язаних із людським фактором.

Внутрішні загрози для систем критичної інфраструктури становлять особливу небезпеку, оскільки вони можуть виникати як ненавмисно (через помилки або необережність персоналу), так і навмисно — у результаті інсайдерської діяльності. Навіть кваліфікований співробітник із законним доступом до технологічних систем може стати причиною зараження мережі, встановлення шпигунського програмного забезпечення або витоку конфіденційних даних.

Антивірусні технології призначені для виявлення, блокування та ліквідації шкідливого програмного забезпечення, яке може бути використане для саботажу, шпигунства або порушення роботи критичних систем. Вони виконують постійний моніторинг стану файлів, процесів і мережевого трафіку, реагуючи на підозрілу активність у режимі реального часу. Основні методи, які застосовуються в антивірусних рішеннях, включають сигнатурний аналіз(виявлення відомих загроз за цифровими «відбитками»), евристичний аналіз (пошук потенційно небезпечних елементів у коді програм), поведенковий аналіз (відстеження нетипової поведінки

програм), а також хмарний моніторинг, який дозволяє отримувати оновлення про нові загрози в реальному часі з глобальних баз даних.

У контексті критичної інфраструктури антивірусні системи мають низку специфічних завдань. По-перше, вони захищають операторські станції та сервери управління, які керують технологічними процесами. Навіть незначне зараження в цих системах може спричинити відмову обладнання або порушення алгоритмів управління. По-друге, антивірусні рішення забезпечують контроль обміну даними між корпоративним і технологічним сегментами, щоб шкідливе програмне забезпечення не проникло у виробниче середовище через електронну пошту або мережеві шляхи. По-третє, вони контролюють зовнішні носії даних (флешки, диски, портативні пристрої), які часто стають джерелом інфікування у закритих мережах.

У критичних системах важливо, щоб антивірусні платформи були стабільними, сумісними з промисловими протоколами (Modbus, DNP3, IEC 104 тощо) та працювали у спеціальному режимі — без впливу на реальний час управління. Для цього використовуються сертифіковані рішення, наприклад, Kaspersky Industrial CyberSecurity, Symantec Critical System Protection, McAfee Embedded Control, Trend Micro Deep Security, Fortinet Endpoint Security, які мають спеціальні режими для SCADA-середовищ. Такі рішення здатні не лише блокувати віруси, але й ізолювати заражені вузли, переводячи їх у карантин без порушення роботи всієї системи.

Не менш важливим компонентом є антишпигунські технології, які виявляють програми, що збирають дані без згоди користувача — кейлогери, модулі прихованого спостереження, програми віддаленого доступу, а також компоненти, які передають інформацію зовні. У сфері критичної інфраструктури такі інструменти є особливо необхідними, оскільки шпигунське програмне забезпечення може бути використане для промислового шпигунства, збору технологічних даних, відстеження команд управління SCADA або підміни сигналів контролерів.

Важливо, що сучасні антивірусні та антишпигунські системи не діють ізольовано, а інтегруються у комплексну систему моніторингу подій безпеки (SIEM). Це дозволяє централізовано збирати інформацію про виявлені загрози, корелювати

події з інших джерел (IDS/IPS, UEBA, IAM) та своєчасно реагувати на інциденти. Також усе частіше такі системи поєднуються із SOAR-платформами, які автоматизують процес реагування — ізолюють заражені вузли, відключають користувачів або блокують підозрілий трафік без втручання людини.

В умовах критичної інфраструктури важливими є також організаційні аспекти використання антивірусного захисту. Кожен об’єкт має мати чітко визначену політику оновлення сигнатур, регламент сканування систем, алгоритм дій при виявленні загроз і процедуру звітування до центру кіберзахисту. Дані журналів подій повинні зберігатися тривалий час у захищеному вигляді для можливості проведення подальшого аудиту або розслідування інцидентів.

Окремо слід відзначити, що у промислових середовищах антивірусні системи повинні відповідати міжнародним стандартам, зокрема IEC 62443 (Industrial Control Systems Security), NIST SP 800-82 (Guide to Industrial Control Systems Security), ISO/IEC 27001 (Information Security Management), а також національним нормативам, які регламентують сертифікацію програмних засобів у сфері кіберзахисту. Дотримання цих стандартів гарантує, що антивірусні рішення не впливатимуть негативно на безперервність технологічних процесів і відповідатимуть вимогам до критичних об’єктів.

3.6. Інструменти для виявлення аномалій у поведінці користувачів (UBA, UEBA)

Системи моніторингу безпеки, такі як антивіруси, фаєрволи або SIEM-рішення, ефективно протидіють відомим загрозам, однак мають обмежені можливості у виявленні аномальної поведінки легітимних користувачів. Саме тому все ширшого застосування набувають UBA (User Behavior Analytics) та UEBA (User and Entity Behavior Analytics) — аналітичні системи нового покоління, що базуються на штучному інтелекті, машинному навчанні та поведінковій аналітиці.

UBA/UEBA системи — це рішення, які аналізують дії користувачів і об’єктів у мережі (пристроїв, акаунтів, додатків) з метою виявлення відхилень від звичної

поведінки. Вони створюють поведінковий профіль кожного користувача або сутності, фіксуючи типові дії: час входу, місце доступу, частоту використання програм, структуру файлів, до яких здійснюється доступ, характер команд і запитів до баз даних тощо.

Принцип роботи UEBA полягає у постійній обробці великих обсягів даних із різних джерел — журналів подій (logs), систем автентифікації, поштових серверів, систем контролю доступу, мережевих пристроїв, баз даних, а також від зовнішніх сенсорів. Використовуючи алгоритми машинного навчання, система формує динамічні моделі поведінки користувачів та пристроїв, які автоматично адаптуються до змін у середовищі. Таким чином, UEBA здатна виявляти складні та приховані інциденти, які неможливо ідентифікувати традиційними методами, наприклад:

- поступове накопичення несанкціонованого доступу до конфіденційних ресурсів;
- повільне копіювання великих обсягів даних з архівів;
- створення прихованих користувацьких акаунтів;
- передачу даних на зовнішні сервери з легальних облікових записів;
- внутрішні атаки у поєднанні з соціальною інженерією.

Важливою перевагою таких систем є те, що вони працюють без необхідності заздалегідь знати сигнатуру атаки. На відміну від антивірусів або IDS-систем, які орієнтовані на пошук відомих шаблонів шкідливої активності, UEBA аналізує поведінку в контексті — тобто визначає, чи є поточні дії користувача логічними щодо його звичного профілю.

UEBA системи базуються на кількох основних технологічних принципах:

1. Збір та агрегація даних. Система інтегрується з SIEM, Active Directory, журналами подій, системами контролю доступу, мережевими сенсорами, платформами електронної пошти та базами даних.

2. Моделювання поведінки. На основі зібраних даних будується математична модель "нормальної" поведінки користувача або пристрою.

3. Виявлення відхилень. Порівнюючи поточну активність із нормою, система виявляє аномалії, які можуть свідчити про зловмисну активність.

4. Пріоритизація ризиків. Кожна аномалія отримує рейтинг ризику (low, medium, high) залежно від її потенційного впливу.

5. Інтеграція з системами реагування. UEBA може автоматично передавати дані до SIEM або SOAR для оперативного реагування на інцидент.

Серед найвідоміших рішень на ринку UEBA — IBM QRadar UBA, Splunk User Behavior Analytics, Exabeam, Securonix, Microsoft Sentinel, ArcSight Intelligence, Varonis DatAdvantage, Rapid7 InsightIDR (Рис. 3.4.).

Рис. 3.4. Аномалії користувача

У контексті критичної інфраструктури, інструменти UEBA мають особливе значення, оскільки дозволяють відстежувати дії як звичайних працівників, так і адміністративного персоналу, який має високі привілеї доступу. Крім цього, UEBA може працювати в тісній інтеграції з антивірусними, антишпигунськими, DLP (Data Loss Prevention) та IAM (Identity and Access Management) системами, створюючи багаторівневий підхід до захисту інформаційних ресурсів.

Переваги UEBA включають:

- автоматичне виявлення аномалій без попереднього налаштування правил;
- зменшення кількості хибних спрацювань порівняно з класичними системами;

- можливість аналізу дій не лише користувачів, а й пристроїв, ботів, програм;
- підвищення прозорості дій співробітників;
- створення доказової бази для внутрішніх розслідувань.

Однак, впровадження таких технологій також має низку викликів. Найбільшими серед них є захист персональних даних, оскільки система обробляє детальну інформацію про діяльність користувачів; необхідність належної якості вихідних даних, адже некоректні журнали подій можуть спотворити аналітику; а також висока вартість і складність налаштування UEBA-систем для великих інфраструктур.

У підсумку, інструменти UBA та UEBA є одним із найефективніших засобів сучасної аналітики безпеки, які забезпечують виявлення прихованих, довготривалих і нетипових загроз усередині організації. Вони підвищують рівень довіри до користувачів, забезпечують персоніфікований контроль доступу та мінімізують ризики інсайдерських атак. У сфері критичної інфраструктури впровадження таких систем є не лише технологічною інновацією, а й необхідною умовою кіберстійкості держави, що гарантує своєчасне виявлення потенційних загроз і збереження стабільності стратегічних процесів.

Висновки до розділу 3

Було розглянуто комплекс сучасних технологій, методів і засобів, спрямованих на попередження, виявлення та нейтралізацію внутрішніх загроз інформаційній безпеці організації, зокрема об’єктів критичної інфраструктури. Проаналізовано основні напрями захисту інформаційних ресурсів, починаючи від розробки політики безпеки та нормативної документації, і завершуючи впровадженням інтелектуальних систем поведінкового аналізу користувачів (UEBA).

Розробка політики інформаційної безпеки визначена як базовий елемент системи захисту, що формує організаційно-правові та технічні основи безпечного функціонування інформаційних систем. Саме чітко сформульовані політики, регламенти та процедури доступу забезпечують єдність підходів до управління ризиками та мінімізують вплив людського фактору.

Використання криптографічних методів забезпечує конфіденційність, цілісність і достовірність інформаційних даних під час їхнього зберігання та передавання. Для систем критичної інфраструктури криптографічний захист є ключовим засобом протидії як зовнішнім, так і внутрішнім загрозам, адже він унеможливлює несанкціоноване перехоплення або модифікацію критично важливих даних.

Важливе місце посідають системи моніторингу та аудиту доступу, які дозволяють здійснювати постійне спостереження за подіями у мережі, фіксувати порушення політик безпеки та виявляти спроби несанкціонованого доступу. Їхня інтеграція із SIEM-платформами та SOC-центрами забезпечує централізований контроль, аналіз інцидентів і швидке реагування на потенційні загрози.

Використання біометричних систем контролю доступу забезпечує надійний рівень ідентифікації користувачів і практично усуває можливість підробки облікових даних. Такі системи, у поєднанні з криптографічними засобами та багатофакторною автентифікацією, формують стійку до компрометації архітектуру доступу до інформаційних ресурсів.

Антивірусні та антишпигунські технології продемонстрували свою ефективність у боротьбі як із зовнішніми, так і внутрішніми загрозами, спричиненими людськими помилками або зловмисними діями співробітників. У контексті критичної інфраструктури вони є обов’язковим компонентом комплексного кіберзахисту, що забезпечує безперервність технологічних процесів і стабільність роботи стратегічно важливих систем.

Завершальним етапом розгляду стала оцінка ролі інструментів UBA/UEBA — систем поведінкової аналітики користувачів і об’єктів. Вони дозволяють виявляти приховані, нетипові та довготривалі інциденти, які не піддаються фіксації традиційними методами. Використання машинного навчання та штучного інтелекту в таких системах відкриває новий рівень проактивного захисту від внутрішніх загроз, особливо у великих розподілених середовищах.

У розділі доведено, що ефективне попередження внутрішніх загроз інформаційній безпеці можливе лише за умови комплексного підходу, який включає поєднання організаційних, технічних і аналітичних засобів. Оптимальна система захисту повинна бути багаторівневою, адаптивною та інтегрованою — здатною не лише реагувати на вже відомі інциденти, а й передбачати потенційні ризики. Впровадження таких технологій у сфері критичної інфраструктури сприяє підвищенню рівня кіберстійкості держави, захисту інформаційних активів і гарантує безперервність функціонування стратегічних секторів.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи на тему «Технології запобігання і протидії внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури» було проведено комплексне дослідження сучасних підходів, методів і технологій, спрямованих на забезпечення надійного захисту інформаційних систем від внутрішніх загроз. Дослідження дозволило встановити, що в умовах стрімкого зростання цифровізації суспільства та поширення використання інформаційних технологій саме внутрішні загрози є одними з найскладніших і найнебезпечніших викликів для сучасної кібербезпеки. Вони виникають внаслідок дій співробітників або підрядників, які мають легальний доступ до інформаційних ресурсів і володіють знаннями про структуру інформаційної системи. Це дає їм потенційну можливість здійснювати шкідливі або ненавмисні дії, здатні порушити цілісність, конфіденційність і доступність даних, що є критичним для стабільної роботи організації.

Особливу актуальність ця проблема набуває в контексті захисту установ критичної інфраструктури, де навіть незначне порушення інформаційної безпеки може призвести до масштабних технічних збоїв, економічних втрат, соціальних наслідків або загрози національній безпеці. Тому забезпечення захисту таких систем вимагає застосування комплексних рішень, які поєднують організаційні, технічні, аналітичні та поведінкові заходи.

В рамках дослідження було визначено, що ефективна система запобігання внутрішнім загрозам повинна базуватися на кількох взаємопов'язаних складових. По-перше, важливою є розробка політики інформаційної безпеки та нормативної документації, що регламентує порядок доступу до інформаційних ресурсів, визначає права і відповідальність користувачів, а також процедури реагування на інциденти. По-друге, важливу роль у захисті інформаційних систем відіграють криптографічні методи, які забезпечують конфіденційність та цілісність даних під час їх зберігання та передачі. По-третє, значну роль у захисті організаційних систем мають системи моніторингу, аудиту та реагування (SIEM, SOC), що здійснюють постійне

спостереження за активністю користувачів і дають змогу оперативно виявляти підозрілі дії або спроби несанкціонованого доступу.

Одним з найбільш перспективних напрямків є впровадження біометричних систем аутентифікації, що дозволяють забезпечити високий рівень точності ідентифікації та мінімізувати ризики підробки облікових даних. Такі технології є ефективним інструментом контролю доступу до критичних інформаційних ресурсів і допомагають запобігати несанкціонованому доступу до системи.

Не менш важливою складовою частиною захисту інформаційних систем є використання антивірусних і антишпигунських технологій, адаптованих для промислових середовищ. Ці системи забезпечують стабільність функціонування інформаційних систем, виявляють шкідливі програми, шпигунське ПЗ та інші прояви внутрішніх загроз, що може бути критичним у випадку нападів з боку зловмисників або недбалості користувачів.

Особливу увагу було приділено сучасним аналітичним рішенням, таким як системи поведінкової аналітики (UBA/UEBA), що використовують методи штучного інтелекту та машинного навчання для виявлення аномалій у поведінці користувачів. Відмінність цих систем від традиційних інструментів полягає в тому, що вони не залежать від сигнатур загроз, а аналізують типові моделі поведінки співробітників і виявляють аномалії, характерні для інсайдерської активності. У критичних інфраструктурах такі рішення дозволяють проактивно ідентифікувати потенційні порушення ще до того, як вони призведуть до інцидентів.

Результати дослідження підтвердили, що найефективніший підхід до протидії внутрішнім загрозам полягає в створенні багаторівневої системи захисту, яка поєднує організаційні, технічні, програмні та поведінкові інструменти. Така система має забезпечувати безперервний моніторинг, своєчасне виявлення відхилень, автоматизоване реагування на інциденти та проведення аудиту безпеки. Водночас важливу роль в управлінні внутрішніми загрозами відіграє людський фактор — рівень обізнаності персоналу, дотримання політик безпеки та культура кібергігієни. Тому підвищення компетенцій співробітників є необхідною умовою ефективного функціонування будь-якої системи захисту.

У результаті проведеного дослідження було доведено, що запобігання і протидія внутрішнім загрозам інформаційної безпеки установ критичної інфраструктури можливі лише за умови системного, комплексного та проактивного підходу. Реалізація такого підходу забезпечує підвищення рівня кіберстійкості, захист конфіденційних даних і, в кінцевому рахунку, зміцнення національної безпеки держави в умовах зростання масштабів кіберзагроз.

Надалі, важливим напрямком буде розвиток технологій аналізу великих даних для виявлення нових патернів загроз і розробка інструментів для їх своєчасного прогнозування та запобігання. Зокрема, інтелектуальні системи, які використовують алгоритми штучного інтелекту для моделювання поведінки внутрішніх користувачів, зможуть виявляти нові типи загроз, які не були передбачені традиційними методами виявлення. Це дозволить не лише реагувати на інциденти, але й проактивно ідентифікувати потенційні загрози ще до того, як вони стануть реальністю.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

Законодавчі та нормативні документи

1. Закон України. Про критичну інфраструктуру. Офіційний вебпортал парламенту України. 2023 URL: https://zakon.rada.gov.ua/laws/show/1882-20#text.

2. Указ президента України «Про рішення ради національної безпеки і оборони україни від 06.05.2015 р. «Про стратегію національної безпеки України» № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#text

3. Про внесення змін до Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/rada/show/v0857519-23#Text.

4. Постанова кабінету міністрів України «Про затвердження порядку ведення реєстру об’єктів критичної інфраструктури» від 28.04.2023 № 415. URL: https://zakon.rada.gov.ua/rada/show/415-2023-%d0%bf#n15

5. Про затвердження національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: розпорядження кабінету міністрів україни № 825-р. Від 19 вересня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%d1%80#text

6. Висновок антикорупційної експертизи «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних об’єктів критичної інфраструктури». НАЗК | Національне агентство з питань запобігання корупції. URL: https://nazk.gov.ua/uk/documents/vysnovok-antykoruptsiynoi-ekspertyzy-proektu-postanovy-kabinetu-ministriv-ukrainy-pro-zatverdzhennya-poryadku-otsinyuvannya-stanu-kiberzahystu-informatsiynyh-elektronnyh-komunikatsiynyh-ta-informatsiyno-komunikatsiynyh-system-v-yakyh-obroblyayutsya-derzha/.

7. Про основні засади забезпечення кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Електронні ресурси

1. Деякі питання об'єктів критичної інформаційної інфраструктури. Офіційний вебпортал парламенту україни. 2020 URL: https://zakon.rada.gov.ua/laws/show/943-2020-п#text.

2. Шляхи забезпечення кібернетичної безпеки об’єктів критичної інформаційної інфраструктури держави у воєнній сфері | збірник наукових праць центру воєнно-стратегічних досліджень нуоу імені івана черняховського. Збірник наукових праць центру воєнно-стратегічних досліджень нуоу імені івана черняховського. 2018 URL: http://znp-cvsd.nuou.org.ua/article/view/125525.

3. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни | інформація і право. Інформація і право. 2023 url: http://il.ippi.org.ua/article/view/287780.

4. Інформаційна безпека та кіберзахист | укргідроенерго. Укргідроенерго. 2022 URL: https://uhe.gov.ua/information_security_and_cyber_protection.

5. Актуальні питання забезпечення кібербезпеки об’єктів критичної інфраструктури. Інформація про видання. 2024 URL: http://lsej.org.ua/10_2024/73.pdf.

6. Іпс ліга:закон - система пошуку, аналізу та моніторингу нормативно-правової бази. Іпс ліга:закон. 2022 URL: https://ips.ligazakon.net/document/kp190518?an=193.

7. Кібербезпека для енергетичних та промислових систем | wezom. It-компания полного цикла разработки программных продуктов wezom - Київ, Україна. 2024 url: https://wezom.com.ua/ua/blog/zahist-kritichnoyi-infrastrukturi.

8. Іпс ліга:закон - система пошуку, аналізу та моніторингу нормативно-правової бази. Іпс ліга. 2025 URL: https://ips.ligazakon.net/document/kp250447.

9. Затверджено загальні вимоги до кіберзахисту об’єктів критичної інфраструктури. Ibuhgalter.net современный бухгалтерский портал. 2019 URL: https://ibuhgalter.net/ru/news/4458.

10. Робоча програма навчальної дисципліни "захист об'єктів в критичній інфраструктурі". Entukhpiir :: головна. 2022 URL: https://repository.kpi.kharkov.ua/items/4461e78f-7abc-4d4c-8396-9a339926acfe.

11. Нормативно-правова база у сфері захисту критичної інфраструктури. Moz.gov.ua. 2025 URL: https://moz.gov.ua/uk/kritichna-infrastruktura.

12. Захист критичної інформаційної інфраструктури як національний пріоритет. Dspace :: elakpi :: репозитарій кпі ім. Ігоря сікорського. URL: https://ela.kpi.ua/items/9f9837fd-fae5-44ef-a552-cdf6ce46c184.

13. Правове та організаційне забезпечення захисту об’єктів критичної інформаційної інфраструктури від кібератак | інформація і право. Інформація і право. 2021 URL: http://il.ippi.org.ua/article/view/248832.

14. Modern approaches to critical infrastructure objects detection and identification | ukrainian scientific journal of information security. Наукові журнали державного університету “Київський авіаційний інститут”. 2015 URL: https://jrnl.nau.edu.ua/index.php/infosecurity/article/view/9690.

15. Деякі питання об'єктів критичної інформаційної інфраструктури - - закони України protocol. 2020 URL: https://protocol.ua/ua/deyaki_pitannya_ob_ektiv_kritichnoi_informatsiynoi_infrastrukturi/.

16. Інформаційна безпека: що це і навіщо вона потрібна. Останні новини херсона та херсонщини сьогодні: слідкуйте на вгору. 2023 URL: https://vgoru.org/cikavo/informaciina-bezpeka-shho-ce-i-navishho-vona-potribna?gad_source=1&gad_campaignid=23005040121&gbraid=0aaaabap6m8s4dk1agf9iccujlcbqfgxlp&gclid=eaiaiqobchmi7bhnu-3ikamviqciax1n7wgqeaayasaaegijtfd_bwe.

17. Захист критичної інформаційної інфраструктури як національний пріоритет. Researchgate. 2025 URL: https://www.researchgate.net/publication/396508840_zahist_kriticnoi_informacijnoi_infrastrukturi_ak_nacionalnij_prioritet.

18. Зеленському поклали на стіл закон щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об’єктів критичної інформаційної інфраструктури. Інтернет журнал кібербез. 2025 URL: https://cybersec.net.ua/normatyv

ni-dokumenty/839-zelenskomu-poklaly-na-stil-zakon-shchodo-zakhystu-informatsii-ta-kiberzakhystu-derzhavnykh-informatsiinykh-resursiv-obiektiv-krytychnoi-informatsiinoi-infrastruktury.html.

19. Ukrinform. Для захисту об'єктів критичної інфраструктури потрібно 1000 додаткових кіберфахівців - держспецзв'язку. Укрінформ - актуальні новини України та світу. 2025 URL: https://www.ukrinform.ua/rubric-society/4020164-dla-zahistu-obektiv-kriticnoi-infrastrukturi-potribno-1000-dodatkovih-kiberfahivciv-derzspeczvazku.html.

20. Модель оцінювання ризиків у сфері критичної інфраструктури Державної прикордонної служби України в умовах воєнного стану. Аналітичні бази даних. 2025 URL: https://perspectives.pp.ua/index.php/niu/article/view/28662/28625.

21. Безпека критичної інфраструктури: як захистити електростанції від кібератак у сучасному світі. Nozomi networks - надійне рішення в галузі безпеки та контролю ot та iot. URL: https://nozominetworks.bakotech.com/ua/security-of-critical-infrastructure.

22. "Європейський досвід розбудови системи захисту критичної інфраструктури: уроки для України". Аналітична записка. Niss.gov.ua. 2013 URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/evropeyskiy-dosvid-rozbudovi-sistemi-zakhistu-kritichnoi.

23. Дп «редакція газ. «голос україни». Міністерство енергетики оприлюднило проєкт наказу щодо профілів безпеки систем у паливно-енергетичному комплексі. Голос України - газета верховної ради україни. 2025 URL: https://www.golos.com.ua/news/6714.

24. Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів | сучасний захист інформації. Open journal systems. 2020 URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2408.

25. Що таке захист критичної інформаційної інфраструктури?. Spike. 2025 URL: https://spike.ranok.cx.ua/ukraincyam/shho-take-zakhist-kritichnoi-informaciynoi-infrastrukturi.html.

26. Стратегія кібербезпеки України // рада національної безпеки і оборони УКРАЇНИ URL: https://zakon.rada.gov.ua/laws/show/96/2016#text.

27. Стратегія кібербезпеки України (2021 – 2025 роки) // Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

28. Аналіз існуючих політик безпеки. URl: https://www.researchgate.net/publication/323728627_analiz_pobudovi_modeli_polit iki_informacijnoi_bezpeki_pidpriemstva

29. Види політик безпеки. StudFiles. URL: https://studfile.net/preview/7475501/page:18/.

30. Проблеми захисту та відновлення критичної інфраструктури із залученням приватного сектору. 2025 URL: https://boi.org.ua/wp-content/uploads/2025/03/problemy-zahystu-ta-vidnovlennya-krytychnoyi-infrastruktury.pdf.

31. Збірник «Науковий вісник УжНУ. Серія «Право». 2024 URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/41-2.pdf.

32. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. 2012 URL: https://niss.gov.ua/sites/default/files/2013-02/Sots_zahust-86178.pdf.

33. Правові проблеми захисту критичних об’єктів інфраструктури стратегічного значення в України. 2019 URL: https://environmentalscience.com.ua/web/uploads/pdf/Law.Human.Environment_2019_Vol.%2010,%20No.%203_124-131.pdf.

34. Правові умови захисту об’єктів критичної інфраструктури в Україні: проблеми та перспективи. 2021 URL: http://www.sulj.oduvs.od.ua/archive/2021/2/22.pdf.

35. Моделювання міжгалузевої економіки як критичної інфраструктури: розроблення сценаріїв розвитку економіки України в умовах війни та післявоєнного відновлення / Кулик В. В. (2023). JNAS | Journals of National Academy of Sciences of Ukraine. URL: http://jnas.nbuv.gov.ua/uk/article/UJRN-0001442971.

36. Огляд ринку кібербезпеки в Україні. 2025 URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf.

37. DSpace Repository :: Репозитарій Львівської політехніки :: Головна. 2023 URL: https://repo.btu.kharkiv.ua/server/api/core/bitstreams/71f8cbfe-bf53-4f05-bad5-ed5efd1cf113/content.

38. Ключові проблеми розвитку критичної інфраструктури в Україні у воєнний період. Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку. 2020. 3. С. 45. URL: Http://perspectives.pp.ua/public/site/conferency/conf-30.pdf#page=346

39. Головна - Запрошуємо в ДНТБ України! Завжди Вам раді. Міжнародна наукова практична конференція 2023 URL: https://dntb.gov.ua/wp-content/uploads/2023/08/Збірник-тез-МНПК_МУЕП.pdf.

40. Формування методів управління проектами та програмами безпеки об’єктів критичної інфраструктури. 2019. URL: Https://repositary.knuba.edu.ua/bitstream/987654321/3147/1/11.pdf

41. Теоретичні засади функціонування об’єктів критичної інфраструктури. Наука про цивільний захист як шлях становлення молодих вчених. 2020. URL: Https://chipb.dsns.gov.ua/upload/1/8/0/4/2/6/8/2-fomic.pdf#page=104

42. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктур. 2021 URL: https://sci.ldubgd.edu.ua/handle/123456789/9829.

43. Теоретико-ігрові та оптимізаційні моделі і методи підвищення безпеки кіберінфраструктур. 2022. URL: Https://ekmair.ukma.edu.ua/items/e5378262-0574-4f65-8b48-83b1c82ebd00

44. Актуальні проблеми об’єктів критичної інфраструктури. Радник у сфері публічних закупівель. 2023 URL: https://radnuk.com.ua/voiennyj-stan/aktualni-problemy-ob-iektiv-krytychnoi-infrastruktury/.

45. Критична інфраструктура західного регіону України в умовах війни: суспільно-географічне дослідження. Головна - Географічний факультет. 2023 URL: https://geography.lnu.edu.ua/wp-content/uploads/2023/11/Borsuk-Kryt-infrastr-Zakh-rehionu-Ukrainy-viyny-23-stattya.pdf.

46. Все, що ви повинні знати про об'єкти критичної інфраструктури в Україні. Головні новини з України сьогодні - Kyiv Post. 2024 URL: https://www.kyivpost.com/uk/post/28283.

47. Критична інфраструктура забезпечена альтернативними джерелами живлення: тернопільська ова. URL: https://suspilne.media/ternopil/917103-kriticnainfrastruktura-zabezpecena-alternativnimi-dzerelami-zivlenna-ternopilska-ova/

48. Об'єкти критичної інфраструктури: детальний аналіз та відповіді на поширені питання | Блог Smarttender. SmartTender – відкриті тендери в Україні, державні та комерційні закупівлі Prozorro. 2022 URL: https://smarttender.biz/blog/view/ob-yekti-kritichnoyi-infrastrukturi-detalniy-analiz-ta-vidpovidi-na-poshireni-pitannya/.

49. Фінансовий клуб. Збитки інфраструктурі України від агресії росії досягли $155 млрд – Фінансовий клуб. Фінансові новини України та аналітика – Фінансовий клуб. 2024 URL: https://finclub.net/news/zbytky-infrastrukturi-ukrainy-vid-ahresii-rosii-dosiahly-usd155-mlrd.html.

50. Механізми забезпечення стійкості критичної інфраструктури: європейський досвід. URL: https://ekmair.ukma.edu.ua/items/f12b475a-1742-41d8-8e32-5ce1e721f139

51. Opportunities and problems in improving the protection of critical infrastructure objects in modern conditions | Honor and Law. Honor and Law. URL: https://chiz.nangu.edu.ua/article/view/272291.

52. Українські оператори зв’язку можуть отримати статус критично важливих об’єктів.url: https://deps.ua/ua/news/novosti-rynka/10893.html

53. Загрози критичній інфраструктурі та їхвплив на стан національної безпеки (моніторинг реалізації стратегії національної безпеки). Аналітична записка.URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/zagrozi-kritichniy-infrastrukturi-ta-ikh-vpliv-na-stan-nacionalnoi

54. Офіційний веб-сайт centre for the protection of national infrastructure. URL: http://www.cpni.gov.uk/