ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Система оцінювання ризиків інформаційної безпеки та розробка рекомендацій щодо їх мінімізації»

на здобуття освітнього ступеня бакалавра
зі спеціальності 124 Системний аналіз
освітньо-професійної програми «Системний аналіз»

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

_____ Артем ГЕРАСИМЕНКО
(підпис)

Виконав: здобувач вищої освіти гр. САД-41
Артем ГЕРАСИМЕНКО

Керівник: Ровіл НАФЄЄВ
к.ф.-м.н., доцент

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Системного аналізу

Ступінь вищої освіти бакалавр_____

Спеціальність 124 Системний аналіз_____

Освітньо-професійна програма Системний аналіз_____

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ_____
_____ Каміла СТОРЧАК
«____» _____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Герасименко Артем Юрійович

1. Тема кваліфікаційної роботи: Система оцінювання ризиків інформаційної безпеки та розробка рекомендацій щодо їх мінімізації_____

керівник кваліфікаційної роботи к.ф.-м.н., доцент Ровіл НАФЄЄВ_____,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «_____» _____2025 р. № ____

2. Строк подання кваліфікаційної роботи «___» _____2025 р.

3. Вихідні дані до кваліфікаційної роботи: Інформаційно-аналітичні матеріали щодо кіберінцидентів в Україні, Теоретико-методологічну базу дослідження , Практичні рекомендації та методики мінімізації ризиків

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи інформаційної безпеки та ризик-менеджменту
2. Аналіз ризиків інформаційної безпеки на прикладі кіберінцидентів в Україні
3. Розробка рекомендацій щодо мінімізації ризиків інформаційної безпеки

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «_____» _____2025__р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Визначення об’єкту, предмету, мети та завдань дослідження	15.02.2025 – 28.02.2025.	Виконано
2	Збір та аналіз наукової літератури, нормативних актів та стандартів	01.03.2025 – 14.03.2025	Виконано
3	Розробка теоретичних основ інформаційної безпеки та ризик-менеджменту	15.03.2025 – 19.03.2025	Виконано
4	Аналіз кіберінцидентів в Україні за 2020–2025 роки	20.03.2025 – 28.03.2025	Виконано
5	Оцінка існуючих заходів захисту та виявлення слабких місць	29.03.2025 – 02.03.2025	Виконано
6	Розробка рекомендацій щодо мінімізації ризиків інформаційної безпеки	03.03.2025 – 11.04.2025	Виконано
7	Формулювання висновків та підготовка презентації	12.04.2025 – 25.04.2025	Виконано
8	Оформлення кваліфікаційної роботи	26.04.2025 – 12.05.2025	Виконано
9	Усунення зауважень, доопрацювання роботи	13.05.2025 – 21.05.2025	Виконано

Здобувач(ка) вищої освіти _____ Артем Герасименко
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ ____Ровіл НАФЄЄВ__
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра : 73 стор., 4 табл., 19 джерел.

Мета роботи - розробка системи оцінювання ризиків інформаційної безпеки та формування комплексу науково-обґрунтованих рекомендацій щодо їх мінімізації на основі аналізу сучасних кіберзагроз та інцидентів в Україні.

Об’єкт дослідження - процеси забезпечення інформаційної безпеки та управління відповідними ризиками в умовах сучасних кіберзагроз.

Предмет дослідження - теоретичні засади та практичні аспекти функціонування системи оцінювання ризиків інформаційної безпеки, методи аналізу кіберінцидентів та розробка рекомендацій для їх мінімізації на прикладі України.

Короткий зміст роботи - У кваліфікаційній роботі досліджено теоретичні основи інформаційної безпеки та ризик-менеджменту, включаючи визначення ключових понять, класифікацію ризиків, огляд методів управління ними та актуальних стандартів . Проведено комплексний аналіз ризиків інформаційної безпеки на основі даних про кіберінциденти в Україні за період 2020–2025 років з використанням "Global Dataset of Cyber Incidents". Розглянуто динаміку, типи, атрибуцію атак та найбільш резонансні кейси, з особливою увагою до діяльності російських спецслужб та хакерських угруповань. На основі проведеного аналізу та оцінки ефективності поточних заходів реагування виявлено слабкі місця у системах захисту. Розроблено та обґрунтовано практичні рекомендації щодо мінімізації виявлених ризиків інформаційної безпеки, а також проведено оцінку очікуваної ефективності запропонованих заходів.

КЛЮЧОВІ СЛОВА: інформаційна безпека, ризики інформаційної безпеки, управління ризиками, оцінювання ризиків, мінімізація ризиків, кіберінциденти, кібератаки, аналіз ризиків, стандарти інформаційної безпеки, кіберзагрози.

ЗМІСТ

ВСТУП

В умовах стрімкої цифрової трансформації суспільства та ескалації гібридних загроз, проблема забезпечення інформаційної безпеки набуває виняткової гостроти, особливо для держав, що перебувають у центрі геополітичних викликів. Україна, яка протягом останніх років, зокрема у період 2020–2024 рр., стала об'єктом численних та системних кібератак, потребує глибокого аналізу існуючих ризиків та розробки дієвих механізмів їх мінімізації. Саме ця нагальна потреба визначає актуальність даного дипломного дослідження, спрямованого на вивчення специфіки кіберінцидентів в українському інформаційному просторі та формування науково обґрунтованих рекомендацій.

Недостатня увага до аналізу ризиків інформаційної безпеки та відсутність адаптованих до сучасних реалій стратегій їх мінімізації можуть призвести до значних фінансових, репутаційних та навіть безпекових втрат для держави, бізнесу та громадян. Відтак, дослідження, що систематизує дані про кіберінциденти та пропонує конкретні шляхи посилення захисту, є своєчасним та суспільно значущим.

Метою дипломної роботи є комплексний аналіз ризиків інформаційної безпеки, ідентифікованих на основі вивчення кіберінцидентів в Україні за період 2020–2024 років, та розробка практично орієнтованих рекомендацій щодо їх ефективної мінімізації, що сприятиме підвищенню рівня захищеності національних інформаційних ресурсів.

Досягнення поставленої мети передбачає вирішення таких основних завдань:

- узагальнити теоретико-методологічні засади інформаційної безпеки та управління ризиками, розглянувши ключові поняття, принципи, класифікації та сучасні стандарти;
- провести емпіричний аналіз кіберінцидентів в Україні (2020–2024 рр.), виявивши їх динаміку, типологію, джерела та наслідки, спираючись на релевантні набори даних;

- оцінити поточний стан системи реагування на кіберзагрози в Україні та ідентифікувати ключові вразливості на основі аналізу інцидентів;
- сформулювати обґрунтовані рекомендації щодо посилення інформаційної безпеки та мінімізації виявлених ризиків.

Об’єктом дослідження є процеси управління ризиками інформаційної безпеки в контексті сучасних кіберзагроз.

Предметом дослідження є аналіз ризиків інформаційної безпеки на прикладі кіберінцидентів в Україні (2020–2024 рр.) та розробка рекомендацій щодо їх мінімізації.

Методологічну основу дослідження становить комплекс загальнонаукових та спеціальних методів, зокрема: теоретичний аналіз та синтез, статистичний аналіз, порівняльний аналіз, метод кейс-стаді та системний підхід, що дозволило забезпечити всебічність та обґрунтованість висновків.

Практичне значення отриманих результатів полягає у можливості їх використання державними органами, підприємствами та організаціями для вдосконалення політик інформаційної безпеки, а також у науково-методичному забезпеченні подальших досліджень у цій сфері.

1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РИЗИК-МЕНЕДЖМЕНТУ

1.1 Визначення інформаційної безпеки, її основні принципи та завдання

У сучасному світі, де інформаційні потоки пронизують кожну сферу нашого життя та діяльності, питання захисту даних набуває першочергового значення. Без перебільшення, інформація перетворилася на один з найцінніших активів як для окремої особи, так і для будь-якої організації чи навіть цілої держави. Саме тому поняття інформаційної безпеки виходить на передній план, стаючи невід'ємною складовою успішного функціонування та розвитку.

Отже, що ж ми розуміємо під терміном "інформаційна безпека"? У найзагальнішому сенсі, інформаційна безпека – це той бажаний стан захищеності інформаційних систем, процесів обробки та сховищ даних, за якого гарантується дотримання трьох ключових атрибутів: конфіденційності, цілісності та доступності цінної для нас інформації. Однак, це поняття значно ширше, ніж просто набір технічних програм чи "залізяччя". Воно охоплює цілий комплекс ретельно продуманих та взаємопов'язаних заходів – правових, організаційних, технічних, освітніх – спрямованих на надійний захист інформації особи, суспільства та держави від широкого спектру загроз. Ці загрози можуть включати несанкціонований доступ, незаконне використання, випадкове чи навмисне оприлюднення, руйнування, спотворення або повне знищення даних.

Іншими словами, інформаційна безпека – це не просто технічний щит. Це багатогранний процес, своєрідна екосистема, що включає в себе економічні та організаційні аспекти, які повинні враховуватися на всіх рівнях діяльності підприємств, установ та державних органів. Адже саме в такому контексті інформація чітко розглядається як надзвичайно важливий ресурс, що має свою

вартість і, безперечно, потребує належного захисту. Це безперервний процес, що вимагає постійної уваги, аналізу та адаптації до нових викликів.

Фундамент, на якому будується вся система інформаційної безпеки, тримається на кількох непорушних принципах. Їх часто називають "тріадою ЦДД" (конфіденційність, цілісність, доступність), і вони є своєрідним наріжним каменем:

Конфіденційність: Цей принцип гарантує, що доступ до певної інформації мають лише ті користувачі, які наділені відповідними повноваженнями (авторизовані користувачі). По суті, це захист від "сторонніх очей" – несанкціонованого ознайомлення, перегляду чи розголошення чутливих даних. Порушення конфіденційності може призвести до витоку комерційної таємниці, персональних даних, фінансових втрат або серйозної репутаційної шкоди.

Цілісність : Цей аспект забезпечує впевненість у тому, що інформація залишається незмінною, точною, достовірною та повною протягом усього її життєвого циклу – під час зберігання, обробки та передачі. Будь-які модифікації даних допускаються лише авторизованими особами та за встановленими процедурами. Втрата цілісності може означати, що важливі звіти спотворені, фінансові транзакції підроблені, або ж критичні інструкції змінені, що може мати катастрофічні наслідки.

Доступність : Цей принцип полягає у забезпеченні безперешкодної можливості для авторизованих користувачів отримувати доступ до необхідної їм інформації та пов'язаних з нею ресурсів саме тоді, коли це потрібно, і в повному обсязі. Простими словами, інформація та системи мають працювати тоді, коли вони потрібні. Атаки типу "відмова в обслуговуванні" (DoS/DDoS) або навіть звичайний збій обладнання можуть порушити доступність, паралізувавши роботу організації.

Варто зазначити, що сучасні підходи та міжнародні стандарти інформаційної безпеки (наприклад, ISO/IEC 27001) розширюють цей класичний перелік, додаючи інші важливі властивості, які допомагають побудувати більш надійну систему захисту. Серед них:

Автентичність : Здатність системи однозначно перевірити та підтвердити, що суб'єкт (користувач, процес) або ресурс (дані) є саме тим, за кого себе видає. Це гарантія того, що інформація надійшла від заявленого джерела, а не від зловмисника.

Підзвітність : Забезпечення можливості фіксувати дії користувачів та системи, що дозволяє відстежувати, хто, що, коли і як робив з інформацією. Це критично важливо для розслідування інцидентів та притягнення до відповідальності.

Неспростовність : Неможливість для суб'єкта (наприклад, відправника повідомлення) відмовитися від факту здійснення певних дій або авторства надісланих даних. Це забезпечує доказову базу, наприклад, при укладанні електронних угод.

Надійність : Здатність системи послідовно виконувати свої функції відповідно до заданих специфікацій.

Виходячи з визначення та принципів, окреслюються і ключові завдання, які покликана вирішувати система інформаційної безпеки. Ці завдання є багатогранними та охоплюють різні аспекти діяльності організації:

Всебічний захист інформаційних активів: Це головне завдання, що полягає у виявленні, класифікації та захисті всіх цінних інформаційних активів організації (даних, програмного забезпечення, апаратних засобів, репутації тощо) від широкого кола загроз – як зовнішніх (хакери, шкідливе ПЗ, конкуренти), так і внутрішніх (нелояльні співробітники, помилки персоналу), як навмисних, так і випадкових.

Забезпечення стабільності та безперервності діяльності: Інформаційна безпека спрямована на підтримку стабільного функціонування всіх бізнес-процесів організації, мінімізацію ризиків, пов’язаних з інформаційними загрозами, та швидке відновлення після можливих інцидентів. Це запорука того, що компанія зможе продовжувати свою роботу навіть за несприятливих умов.

Підтримка та зміцнення довіри: Надійна система безпеки формує та підтримує високий рівень довіри як з боку зовнішніх партнерів, клієнтів та інвесторів, так і всередині самої організації між співробітниками. Демонстрація відповідального ставлення до захисту даних є важливим конкурентним фактором.

Впровадження та ефективне управління комплексною системою захисту: Це завдання передбачає розробку, впровадження, постійний моніторинг та вдосконалення цілісної системи заходів, що забезпечують захист інформації на всіх критично важливих рівнях: фізичному (охорона приміщень, контроль доступу до обладнання), технічному/апаратно-програмному (міжмережеві екрани, антивіруси, системи виявлення вторгнень, шифрування) та організаційно-адміністративному (політики безпеки, навчання персоналу, процедури реагування на інциденти).

Таким чином, стає очевидним, що інформаційна безпека – це не одноразовий проект, а безперервний, циклічний процес, що є ключовою умовою стабільного та успішного функціонування сучасних організацій, підприємств та державних інституцій. Грамотне та послідовне дотримання її принципів і виконання поставлених завдань дозволяє не лише суттєво зменшити ймовірність реалізації різноманітних шкідливих сценаріїв, але й значно мінімізувати потенційні фінансові, репутаційні та операційні збитки.

1.2 Поняття ризику в інформаційній безпеці, класифікація ризиків

Після того, як ми окреслили суть інформаційної безпеки та її фундаментальні принципи, логічним наступним кроком є розгляд такого ключового поняття, як ризик. Адже саме управління ризиками лежить в основі побудови будь-якої ефективної системи захисту. Без розуміння потенційних небезпек та їхніх можливих наслідків, наші зусилля із забезпечення безпеки будуть схожі на стрілянину навмання.

Що ж таке ризик інформаційної безпеки? Уявіть собі, що ваша інформаційна система – це фортеця. Вразливість – це слабке місце в її обороні (наприклад, незачинені ворота або тонка стіна). Загроза – це потенційний ворог (хакер, вірус, недбалий співробітник), який може спробувати використати цю слабкість. Так от, ризик – це сама ймовірність того, що цей ворог успішно скористається слабким місцем і завдасть шкоди вашій фортеці (організації).

Формальніше, ризик інформаційної безпеки – це потенційна можливість того, що певна загроза зможе використати наявні вразливості інформаційних активів (даних, систем, процесів) для заподіяння шкоди організації. Ця шкода може бути найрізноманітнішою: від прямих фінансових збитків та порушення нормальної операційної діяльності до втрати безцінної ділової репутації, юридичних наслідків чи навіть втрати довіри клієнтів. Ризик виникає на перетині трьох компонентів: наявності цінних активів, існуючих загроз для цих активів та вразливостей, які можуть бути експлуатовані цими загрозами.

Для того, щоб кількісно або якісно оцінити ризик, його часто розглядають через призму кількох ключових факторів. Хоча існують різні моделі, класичний підхід полягає у визначенні величини ризику як певної функції від:

Ймовірності реалізації загрози : Наскільки ймовірно, що конкретна загроза (наприклад, фішингова атака, збій обладнання, інсайдерська дія) взагалі виникне або спробує атакувати систему?

Ймовірності успішної експлуатації вразливості: Якщо загроза реалізувалася, наскільки ймовірно, що вона зможе успішно використати існуючу вразливість (наприклад, застаріле програмне забезпечення, слабкий пароль, відсутність контролю доступу)?

Розміру потенційної шкоди або впливу : Якими будуть негативні наслідки для організації, якщо загроза успішно використає вразливість? Це може вимірюватися у фінансових втратах, часі простою, кількості скомпрометованих записів, репутаційній шкоді тощо.

Розуміння цих складових допомагає не просто констатувати факт існування ризику, а й оцінити його рівень та пріоритетність для подальших дій.

Світ ризиків інформаційної безпеки надзвичайно різноманітний. Щоб ефективно орієнтуватися в ньому та розробляти адекватні заходи протидії, ризики прийнято класифікувати за різними ознаками. Це допомагає систематизувати їх, краще зрозуміти природу та потенційні наслідки. Розглянемо деякі поширені підходи до класифікації:

За джерелом виникнення ризику: Де або від кого походить небезпека?

Зовнішні навмисні атаки: Сюди належать дії хакерів, кіберзлочинних угруповань, конкурентів, спрямовані на компрометацію системи (наприклад, DDoS-атаки, злам систем, шпигунство).

Внутрішні загрози (інсайдери): Дії (навмисні або ненавмисні) з боку співробітників організації, підрядників або партнерів, які мають легітимний доступ до інформаційних систем (наприклад, злив даних, саботаж, помилки при роботі з інформацією).

Помилки персоналу та технічні збої: Ненавмисні дії, такі як випадкове видалення даних, неправильне налаштування обладнання, а також відмови апаратного чи програмного забезпечення.

Вплив державних регуляторів та юридичні аспекти: Ризики, пов'язані з невиконанням вимог законодавства (наприклад, GDPR, закони про захист персональних даних), що може призвести до штрафів, судових позовів з боку контрагентів або клієнтів.

Негативний інформаційний вплив: Поширення неправдивої або компрометуючої інформації конкурентами чи іншими зловмисниками з метою підриву репутації.

Природні та техногенні катастрофи: Пожежі, повені, землетруси, перебої з електропостачанням, що можуть призвести до фізичного знищення обладнання та даних.

За об'єктом (активом), на який спрямований вплив: Що саме опиняється під ударом?

Ризики для інформаційних активів: Загрози конфіденційності, цілісності та доступності самих даних, баз даних, програмного коду, інтелектуальної власності.

Ризики для фізичних активів: Пошкодження, викрадення або знищення серверів, мережевого обладнання, робочих станцій, носіїв інформації.

Ризики для репутації організації: Втрата довіри клієнтів, партнерів, інвесторів, негативний розголос у ЗМІ внаслідок інциденту безпеки.

Ризики для бізнес-процесів: Порушення або повна зупинка ключових операційних процесів (наприклад, неможливість обробляти замовлення, надавати послуги, здійснювати фінансові операції).

Ризики для персоналу: Загрози безпеці та здоров'ю співробітників (наприклад, у випадку кібербулінгу або соціальної інженерії з серйозними наслідками).

За тривалістю та масштабом впливу: Як довго та наскільки серйозно відчуватимуться наслідки?

Операційні ризики: Мають короткостроковий характер і впливають на поточну діяльність. Наприклад, тимчасова зупинка роботи веб-сервісу, короткочасна недоступність файлового сховища.

Тактичні ризики: Наслідки проявляються у середньостроковій перспективі та можуть вплинути на досягнення тактичних цілей організації. Наприклад, тимчасова втрата частини клієнтської бази через витік даних, необхідність значних витрат на відновлення системи.

Стратегічні ризики: Мають довгострокові, часто незворотні наслідки, що можуть поставити під загрозу саме існування організації або її ключові стратегічні напрямки. Наприклад, повна втрата ринкової частки, банкрутство через масштабний штраф, неможливість залучення інвестицій через підірвану репутацію.

Таким чином, стає зрозуміло, що ризик в інформаційній безпеці – це не абстрактне поняття, а цілком реальна ймовірність негативних подій, що вимагає

глибокого розуміння його природи. Це багатогранне явище, яке пронизує як технічні, так і організаційні аспекти діяльності будь-якої сучасної установи. Комплексний підхід до ідентифікації, аналізу та класифікації ризиків є фундаментом для розробки ефективної стратегії управління ними та, відповідно, для побудови надійної системи інформаційної безпеки.

1.3 Методи і підходи до управління ризиками

Після того, як ми усвідомили, що таке ризики інформаційної безпеки та наскільки вони різноманітні, виникає закономірне питання: а що ж з ними робити? Сидіти склавши руки і сподіватися, що біда омине – явно не найкраща стратегія для сучасної організації. Саме тут на сцену виходить управління ризиками інформаційної безпеки – ключовий процес, що дозволяє перейти від пасивного очікування проблем до активного контролю над ситуацією.

Управління ризиками – це не якась магічна формула, а цілком систематичний та логічно вибудуваний процес. Він включає в себе послідовні кроки з виявлення, всебічного аналізу, об'єктивного оцінювання та, зрештою, адекватної обробки тих ризиків, які можуть поставити під загрозу захищеність найцінніших інформаційних активів організації. Головна мета цього процесу – не усунути ризики повністю (що часто неможливо або економічно недоцільно), а мінімізувати як ймовірність їх реалізації, так і потенційні негативні наслідки від загроз для інформаційних ресурсів. Таким чином, грамотне управління ризиками стає надійним фундаментом для забезпечення стабільної, безперервної та передбачуваної діяльності організації.

Процес управління ризиками інформаційної безпеки зазвичай є циклічним і складається з кількох взаємопов'язаних етапів, кожен з яких відіграє важливу роль:

Встановлення контексту та ідентифікація активів, загроз і вразливостей:

Встановлення контексту: Перш ніж кидатися на пошуки ризиків, необхідно чітко зрозуміти середовище, в якому функціонує організація. Це включає аналіз її

бізнес-цілей, нормативно-правових вимог, організаційної структури, культури безпеки та існуючої IT-інфраструктури. Без цього розуміння наші зусилля можуть бути спрямовані не туди.

Ідентифікація активів: Необхідно визначити та каталогізувати всі цінні інформаційні активи, які потребують захисту. Це можуть бути бази даних клієнтів, фінансова звітність, інтелектуальна власність, персональні дані співробітників, конфігурації систем, а також репутація компанії. Кожному активу варто присвоїти певну цінність.

Ідентифікація загроз: Далі слід виявити потенційні загрози, які можуть вплинути на ці активи. Це можуть бути як навмисні дії (хакерські атаки, віруси, інсайдери), так і ненавмисні (помилки персоналу, збої обладнання) або природні явища.

Ідентифікація вразливостей: Наступний крок – пошук "слабких місць" у системах, процесах чи політиках, які можуть бути використані визначеними загрозами. Це можуть бути застаріле ПЗ, слабкі паролі, відсутність шифрування, недостатнє навчання персоналу тощо.

Аналіз та оцінка вразливостей і ризиків:

На цьому етапі відбувається глибший аналіз виявлених вразливостей та оцінка пов'язаних з ними ризиків. Необхідно зрозуміти, наскільки легко загроза може експлуатувати ту чи іншу вразливість, та якими будуть потенційні наслідки, якщо інцидент все ж таки станеться.

Для оцінки ризиків застосовують різні методи:

Якісні методи: Ризики оцінюються за описовими шкалами, наприклад, "Високий", "Середній", "Низький". Це відносно швидкий спосіб пріоритезації, особливо коли точні кількісні дані відсутні.

Кількісні методи: Ризики оцінюються в числових показниках, часто у грошовому еквіваленті (наприклад, розрахунок очікуваних річних втрат – Annual

Loss Expectancy, ALE). Це дозволяє більш об'єктивно порівнювати ризики та обґрунтовувати витрати на заходи захисту, хоча й вимагає більше даних та зусиль.

Розробка стратегії обробки ризиків :

Після того, як ризики ідентифіковані та оцінені, необхідно вирішити, що з ними робити. Існує кілька основних стратегій обробки ризиків:

Зниження : Це найпоширеніша стратегія. Вона полягає у впровадженні відповідних заходів контролю (технічних, організаційних, фізичних) для зменшення ймовірності виникнення ризику або його потенційного впливу до прийнятного рівня. Наприклад, встановлення антивірусу, впровадження політики надійних паролів, проведення навчань для персоналу.

Передача : Ця стратегія передбачає передачу частини або всього ризику третій стороні. Класичний приклад – страхування кіберризиків. Також це може бути аутсорсинг певних функцій (наприклад, хостинг веб-сайту) компанії, яка краще підготовлена для управління пов'язаними ризиками.

Прийняття : У деяких випадках організація може усвідомлено вирішити прийняти ризик без вжиття додаткових заходів контролю. Це зазвичай відбувається, коли вартість обробки ризику перевищує потенційні збитки, або коли ризик є дуже низьким. Таке рішення має бути задокументованим та схваленим керівництвом.

Уникнення : Ця стратегія полягає у відмові від діяльності, процесу або технології, що генерує неприйнятно високий ризик. Наприклад, компанія може відмовитися від збору певних видів персональних даних, якщо не може забезпечити їх належний захист.

Впровадження заходів контролю (засобів захисту):

На основі обраної стратегії обробки ризиків відбувається вибір та реалізація конкретних заходів контролю. Це можуть бути:

Технічні заходи: Міжмережеві екрани, системи виявлення/запобігання вторгненням, антивірусне ПЗ, шифрування даних, системи резервного копіювання, багатофакторна автентифікація.

Організаційні (адміністративні) заходи: Розробка та впровадження політик і процедур безпеки, навчання та підвищення обізнаності персоналу, управління інцидентами, класифікація інформації, контроль доступу.

Фізичні заходи: Охорона приміщень, контроль фізичного доступу до серверних кімнат та обладнання, системи відеоспостереження.

Моніторинг, перегляд та підтримка:

Управління ризиками – це не одноразовий захід, а безперервний процес. Після впровадження заходів контролю необхідно постійно:

Моніторити їх ефективність та стан безпеки системи.

Регулярно переглядати та переоцінювати ризики, оскільки ландшафт загроз постійно змінюється, з'являються нові вразливості, а бізнес-цілі організації можуть коригуватися.

Підтримувати та оновлювати заходи захисту, адаптуючи їх до нових реалій. Це включає встановлення патчів, оновлення ПЗ, коригування політик тощо.

Для структурування та систематизації процесу управління ризиками існує низка визнаних на міжнародному рівні стандартів, методологій та фреймворків. Вони надають готові "рецепти" та найкращі практики. Серед найпопулярніших можна виділити:

ISO/IEC 27005: Це міжнародний стандарт, який є частиною родини стандартів ISO 27000 і надає детальні керівні вказівки саме щодо управління ризиками інформаційної безпеки. Він описує процес, що включає такі етапи, як встановлення контексту, ідентифікація ризиків, їх аналіз, оцінювання, обробка, прийняття ризиків, а також комунікація та консультації, моніторинг та перегляд. Він гнучкий і може бути адаптований до будь-якої організації.

NIST Risk Management Framework (RMF): Розроблений Національним інститутом стандартів і технологій США , цей фреймворк є дуже популярним, особливо в урядових структурах США, але широко застосовується і в комерційному секторі. RMF пропонує структурований шестикроковий процес: Категоризація

інформаційних систем, Вибір заходів контролю безпеки, Впровадження заходів контролю, Оцінка заходів контролю, Авторизація системи та Постійний моніторинг. Він робить сильний акцент на інтеграції безпеки в життєвий цикл системи.

CRAMM (CCTA Risk Analysis and Management Method): Це британська методологія, яка була однією з перших комплексних методик аналізу та управління ризиками. Вона пропонує досить деталізований підхід, що включає етапи ініціювання проекту, ідентифікації та оцінки цінності IT-активів, детального аналізу загроз і вразливостей, визначення рівня ризиків та розробки рекомендацій щодо впровадження контрзаходів. Часто використовується для великих систем.

COBIT for Risk: Є частиною ширшого фреймворку COBIT (Control Objectives for Information and Related Technologies) від ISACA. COBIT for Risk фокусується на забезпеченні того, щоб IT-ризики управлялися відповідно до загальних цілей бізнесу. Він допомагає інтегрувати процеси управління IT-ризиками із загальним корпоративним управлінням та оптимізувати витрати на безпеку, підвищуючи рівень захищеності критично важливих об’єктів та процесів.

Інші методики: Окрім згаданих, існує низка інших методологій, таких як FRAP (Facilitated Risk Analysis Process), що є більш спрощеним та швидким підходом; OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), що фокусується на самооцінці ризиків силами внутрішньої команди; EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), популярна у Франції; та власні методики великих корпорацій, наприклад, Microsoft Risk Management Guide. Вибір конкретної методики залежить від розміру організації, її специфіки, ресурсів та рівня зрілості процесів управління ризиками.

Незалежно від обраної методики, успішне управління ризиками інформаційної безпеки ґрунтується на кількох фундаментальних підходах:

Комплексний (холістичний) підхід: Управління ризиками не повинно бути ізольованою функцією IT-відділу чи служби безпеки. Його слід інтегрувати у всі

бізнес-процеси та на всі рівні управління організацією. Кожен співробітник має розуміти свою роль у забезпеченні безпеки.

Безперервний моніторинг та адаптація: Ландшафт загроз, технології та бізнес-середовище змінюються з шаленою швидкістю. Тому оцінка ризиків та оновлення заходів захисту мають бути не одноразовою акцією, а регулярним, безперервним процесом.

Врахування бізнес-цілей та пріоритетів: Заходи з управління ризиками мають бути узгоджені зі стратегічними цілями, завданнями та пріоритетами організації. Безпека повинна підтримувати бізнес, а не гальмувати його. Інвестиції в безпеку мають бути економічно обґрунтованими та спрямованими на захист найцінніших активів та процесів.

Культура безпеки та обізнаність персоналу: Навіть найсучасніші технології не допоможуть, якщо персонал не розуміє важливості безпеки та не дотримується встановлених правил. Тому формування культури безпеки, регулярне навчання та підвищення обізнаності співробітників є критично важливими.

Підсумовуючи, ефективне управління ризиками інформаційної безпеки – це не просто набір технічних інструментів, а ціла філософія, що базується на структурованому процесі, глибокому аналізі, використанні передових методик та, що найважливіше, на постійному прагненні до вдосконалення заходів захисту відповідно до актуальних загроз, вразливостей та потреб бізнесу. Це інвестиція в стабільність, надійність та майбутнє будь-якої організації.

1.4 Огляд стандартів та кращих практик

У світі, де інформаційні технології розвиваються семимильними кроками, а кіберзагрози стають все більш витонченими, організаціям життєво необхідно мати надійні орієнтири для побудови ефективних систем захисту. Просто покладатися на інтуїцію чи окремі технічні рішення вже недостатньо. Саме тут на допомогу

приходять міжнародні стандарти та накопичений роками досвід, втілений у так званих "кращих практиках". Вони пропонують перевірені часом підходи, універсальну мову та чіткі рамки для управління інформаційною безпекою.

Коли мова заходить про стандартизацію у сфері інформаційної безпеки, беззаперечними лідерами та найбільш визнаними у всьому світі є стандарти серії ISO/IEC 27000. Ця велика родина стандартів, розроблена Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC), являє собою комплексний набір вимог, рекомендацій, настанов та інструментів для створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та постійного вдосконалення Системи Управління Інформаційною Безпекою (СУІБ, англ. Information Security Management System - ISMS). Це не просто набір правил, а цілісна філософія управління, що дозволяє організації системно підходити до захисту своїх інформаційних активів.

ISO/IEC 27001 "Інформаційні технології – Методи захисту – Системи управління інформаційною безпекою – Вимоги" – це, без перебільшення, флагманський та ключовий міжнародний стандарт у цій серії. Він встановлює чіткі вимоги до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення документованої Системи Управління Інформаційною Безпекою в контексті загальних бізнес-ризиків організації.

Основна мета стандарту ISO/IEC 27001 – допомогти організаціям будь-якого розміру та типу діяльності надійно захистити свої інформаційні активи, забезпечуючи три кити інформаційної безпеки: конфіденційність, цілісність та доступність інформації. І робиться це не хаотично, а шляхом впровадження системного підходу до управління ризиками. Стандарт вимагає від організації:

Розуміння контексту організації: Визначення внутрішніх та зовнішніх факторів, що впливають на її здатність досягати цілей СУІБ.

Лідерство та зобов'язання керівництва: Активна участь вищого керівництва у створенні та підтримці СУІБ.

Планування: Включає проведення оцінки ризиків інформаційної безпеки та вибір відповідних цілей контролю та заходів контролю для обробки цих ризиків.

Підтримка: Забезпечення необхідними ресурсами, компетенціями, обізнаністю, комунікаціями та документованою інформацією.

Функціонування : Впровадження та експлуатація обраних заходів контролю та процесів управління ризиками.

Оцінка результативності: Постійний моніторинг, вимірювання, аналіз та оцінка ефективності СУІБ, включаючи проведення внутрішніх аудитів та аналізу з боку керівництва.

Вдосконалення: Постійне покращення СУІБ на основі результатів оцінки та виявлених невідповідностей, використовуючи цикл Демінга

Важливою частиною ISO/IEC 27001 є Додаток А . Наразі (в актуальній версії стандарту 2022 року) він містить 93 універсальні заходи контролю , які згруповані у 4 великі домени (теми): організаційні контролі, контролі щодо людей, фізичні контролі та технологічні контролі. Організація повинна обрати ті заходи контролю з Додатку А, які є доречними для обробки її ідентифікованих ризиків, або обґрунтувати, чому певні контролі не застосовуються.

Однією з ключових переваг впровадження ISO/IEC 27001 є можливість сертифікації. Проходження незалежного аудиту та отримання сертифіката відповідності ISO/IEC 27001 є міжнародно визнаним доказом того, що система управління інформаційною безпекою організації відповідає найкращим світовим практикам. Це значно підвищує довіру з боку клієнтів, партнерів, інвесторів та регуляторів, а також може бути конкурентною перевагою на ринку.

Якщо ISO/IEC 27001 визначає що потрібно зробити для створення СУІБ, то ISO/IEC 27005 "Інформаційні технології – Методи захисту – Управління ризиками інформаційної безпеки" детально роз'яснює, як це робити стосовно одного з найважливіших компонентів – управління ризиками. Цей стандарт є

спеціалізованим посібником і надає вичерпні рекомендації та керівні вказівки щодо процесу управління ризиками інформаційної безпеки.

Ключове завдання ISO/IEC 27005 – підтримати ефективне впровадження вимог ISO/IEC 27001, що стосуються ризик-менеджменту. Він описує структурований процес, який включає:

Встановлення контексту ризику: Визначення критеріїв ризику, області застосування та меж процесу управління ризиками.

Ідентифікація ризиків: Виявлення активів, загроз, існуючих контролів та вразливостей.

Аналіз ризиків: Оцінка потенційних наслідків та ймовірності реалізації ідентифікованих ризиків.

Оцінювання ризиків: Порівняння результатів аналізу ризиків із встановленими критеріями для визначення пріоритетності обробки ризиків.

Обробка ризиків: Вибір та впровадження однієї або декількох опцій обробки ризиків (зниження, передача, прийняття, уникнення).

Прийняття ризиків: Формальне схвалення залишкових ризиків керівництвом.

Комунікація та консультації щодо ризиків: Обмін інформацією про ризики з усіма зацікавленими сторонами протягом усього процесу.

Моніторинг та перегляд ризиків: Постійне відстеження ризиків, ефективності контролів та змін у контексті.

Важливо, що ISO/IEC 27005 не нав'язує якусь одну конкретну методологію оцінки ризиків. Натомість він пропонує гнучку рамкову структуру, яку кожна організація може адаптувати до своїх специфічних потреб, розміру, галузі діяльності та корпоративної культури. Це дозволяє компаніям використовувати ті методи (наприклад, NIST RMF, CRAMM, OCTAVE), які найкраще відповідають їхнім обставинам, залишаючись при цьому у відповідності до загальних принципів стандарту.

Впровадження стандартів серії ISO/IEC 27000 – це не просто формальне отримання сертифікату. Це шлях до побудови справді дієвої системи захисту інформації, яка враховує як технологічні, так і організаційні та людські аспекти. Однак самі по собі стандарти – це лише інструмент. Ефективність їх застосування залежить від дотримання кращих практик інформаційної безпеки, які включають:

Регулярне проведення аудитів: Як внутрішніх (силами самої організації), так і зовнішніх (незалежними аудиторами) для перевірки відповідності вимогам стандартів та ефективності СУІБ.

Безперервний моніторинг ризиків та інцидентів: Ландшафт загроз постійно змінюється, тому важливо мати процеси для своєчасного виявлення нових ризиків та оперативного реагування на інциденти безпеки.

Глибока інтеграція заходів безпеки у всі бізнес-процеси: Безпека не повинна бути чимось відокремленим. Її принципи мають бути закладені "by design" у всі процеси та системи організації.

Формування культури інформаційної безпеки: Залучення всього персоналу до дотримання політик безпеки, регулярне навчання та підвищення обізнаності. Адже люди – це одночасно і найсильніша, і найслабша ланка в ланцюгу безпеки.

Використання інших стандартів серії ISO 27000: Наприклад, ISO/IEC 27002 надає детальні практичні рекомендації та керівництва щодо впровадження заходів контролю, перелічених у Додатку А до ISO/IEC 27001. Існують також стандарти, що стосуються безпеки хмарних обчислень (ISO/IEC 27017), захисту персональних даних у хмарах (ISO/IEC 27018), управління інцидентами (ISO/IEC 27035) та багато інших.

Великою перевагою ISO/IEC 27001 є його структура, яка дозволяє легко інтегрувати його з іншими популярними системами менеджменту, такими як система управління якістю (ISO 9001), система екологічного менеджменту (ISO 14001) чи система управління безперервністю бізнесу (ISO 22301). Такий інтегрований підхід дозволяє організаціям оптимізувати свої процеси, уникнути

дублювання зусиль та ефективніше відповідати різноманітним вимогам регуляторів та очікуванням зацікавлених сторін.

Дотримання міжнародних стандартів, таких як ISO/IEC 27001 та ISO/IEC 27005, надає організаціям не просто набір правил, а вивірений, структурований та всесвітньо визнаний підхід до управління інформаційною безпекою та пов'язаними з нею ризиками. Це дозволяє не тільки підвищити реальний рівень захищеності цінних інформаційних активів, але й сприяє зміцненню довіри з боку клієнтів, партнерів та інвесторів. У сучасному цифровому світі, де кіберзагрози є повсякденною реальністю, здатність продемонструвати зрілий підхід до інформаційної безпеки є ключовим фактором стійкості, конкурентоспроможності та довгострокового успіху будь-якої організації.

Розділ 2. АНАЛІЗ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРИКЛАДІ КІБЕРІНЦИДЕНТІВ В УКРАЇНІ (2020–2025)

Для того, щоб наш аналіз ризиків інформаційної безпеки був не просто теоретичним, а ґрунтувався на реальних подіях та тенденціях, нам потрібне надійне та всеосяжне джерело даних про кіберінциденти. У цьому розділі ми зосередимося на вивченні конкретних випадків, що мали місце в Україні у період з 2020 по 2025 рік, використовуючи для цього визнаний міжнародний ресурс.

2.1 Опис джерела даних (Global Dataset of Cyber Incidents): структура, методологія збору, релевантність для України

Основним джерелом емпіричних даних для нашого дослідження слугуватиме Global Dataset of Cyber Incidents. Це офіційний публічний реліз даних, який надається Європейським репозиторієм кіберінцидентів (EuRepoC) . Цей репозиторій став авторитетним джерелом систематизованої інформації про кібернетичні інциденти, що відбуваються у всьому світі.

База даних Global Dataset of Cyber Incidents є значним масивом інформації. У своїй актуальній версії (наприклад, версія 1.3 на квітень 2025 року) вона містить понад 3400 деталізованих записів про кіберінциденти, що сталися в період з 1 січня 2000 року по 31 грудня 2024 року . Це дозволяє проводити як ретроспективний аналіз, так і відстежувати найновіші тенденції.

Основний файл бази даних, доступний у форматах CSV та XLSX, організований таким чином, що кожен рядок відповідає одному унікальному кіберінциденту . Для кожного такого інциденту кодується до 60 різноманітних змінних (ознак). Ці змінні охоплюють широкий спектр характеристик, включаючи, але не обмежуючись:

Дату початку та завершення інциденту.

Країну або актора-ініціатора атаки (якщо встановлено).

Тип атаки (наприклад, DDoS, шкідливе ПЗ, фішинг, дефейс тощо).

Категорію та назву жертви (організації чи особи).

Сектор, до якого належить жертва (наприклад, уряд, фінанси, енергетика).

Опис та характер наслідків інциденту.

Інформацію щодо атрибуції (приписування відповідальності за атаку) .

Окрім цього основного масиву даних, EuRepoC надає кілька додаткових, спеціально структурованих наборів даних для полегшення конкретних видів аналізу :

Receiver Dataset : У цьому файлі дані про постраждалих суб'єктів (жертв) реструктуризовані так, що кожен рядок містить інформацію про одну жертву в рамках одного інциденту. Це зручно, коли один інцидент зачіпає кілька організацій чи осіб, оскільки дані "розпаковуються" на декілька рядків, кожен з яких має унікальний ідентифікатор інциденту (incident_id) .

Attribution Dataset (Датасет атрибуції): Подібно до датасету жертв, цей файл деталізує інформацію про атрибуцію атак. Оскільки атрибуція може бути складною і включати кілька можливих версій або деталей для одного інциденту, ці дані також "розпаковані" для зручності аналізу, зберігаючи зв'язок через incident_id та спеціальний attribution_id .

Dyadic Dataset : Цей набір даних фокусується на інцидентах, що відбуваються між двома державними акторами. Кожен рядок представляє кіберінцидент у контексті конкретної пари країн (діади). Якщо інцидент зачіпав кілька країн, він може бути дубльований у цьому форматі для кожної відповідної пари .

Така гнучка структура дозволяє дослідникам обирати найбільш підходящий формат даних залежно від цілей їхнього аналізу.

Процес збору, кодування та аналізу даних в EuRepoC є ретельно продуманим та багатоетапним, що забезпечує високу якість та надійність інформації. Ключові аспекти методології включають:

Міждисциплінарна експертиза: Над даними працює команда експертів з різних галузей, включаючи політику, право та інформаційні технології . Це забезпечує всебічний розгляд кожного інциденту.

Широке охоплення джерел: Інформація збирається щоденно з понад 220 відкритих джерел (новинні видання, звіти компаній з кібербезпеки, урядові повідомлення) та понад 600 Twitter-акаунтів, які спеціалізуються на темі кібербезпеки . EuRepoC використовує поєднання інструментів науки про дані та експертних знань для обробки цієї інформації .

Чіткі критерії відбору інцидентів: Щоб інцидент був включений до бази даних, він має відповідати щонайменше двом основним критеріям:

Порушення принципів тріади CIA: Інцидент повинен спричинити порушення хоча б одного з фундаментальних принципів інформаційної безпеки – конфіденційності , цілісності або доступності інформації.

Публічна задокументованість: Інформація про інцидент має бути доступною у відкритих джерелах. Це забезпечує прозорість методології та можливість незалежної перевірки даних.

Стандартизований процес кодування: Кожен інцидент оцінюється та кодується за вже згаданими 60 критеріями, що охоплюють технічні, політичні, правові та соціальні аспекти. Для забезпечення послідовності та точності використовується спеціально розроблений кодбук – детальна інструкція з кодування .

Багатоетапна верифікація: Процес кодування є ітераційним та передбачає постійне уточнення та перекалібрування, наприклад, оцінок інтенсивності чи доказів атрибуції . Закодовані дані проходять регулярну перевірку як внутрішніми (вторинними) рецензентами команди EuRepoC, так і зовнішніми експертами . Це мінімізує ризик помилок та суб'єктивності.

Постійне оновлення: База даних регулярно оновлюється та доповнюється новими інцидентами та свіжою інформацією щодо вже існуючих записів . Це

дозволяє дослідникам відслідковувати динаміку загроз практично в реальному часі (хоча для аналізу в реальному часі EuRepoC пропонує окремі опції доступу) .

Хоча Global Dataset of Cyber Incidents має глобальне охоплення, він приділяє особливу увагу подіям у європейському кіберпросторі. Це робить його надзвичайно релевантним для аналізу ситуації в Україні, особливо з огляду на триваючу кібервійну та значну кількість інцидентів, спрямованих проти нашої держави, починаючи з 2014 року . Для України цей ресурс є цінним з кількох причин:

Детальний аналіз кіберінцидентів проти України: Датасет дозволяє глибоко аналізувати динаміку, типи, масштаби та наслідки кіберінцидентів, спрямованих проти українських державних установ, об'єктів критичної інфраструктури, приватного сектору та громадянського суспільства. Враховуючи, що Україна перебуває на передовій глобальної кібервійни , така інформація є критично важливою.

Виявлення ключових загроз та акторів: Аналіз даних EuRepoC може допомогти ідентифікувати основних державних та недержавних акторів, які стоять за атаками на Україну, виявити найбільш поширені вектори та інструменти атак, а також відстежувати еволюцію їхніх тактик. Це є фундаментальною основою для формування ефективної національної політики кібербезпеки та стратегій захисту .

Порівняння з глобальними трендами: Можливість порівняти український досвід із загальносвітовими тенденціями у сфері кіберзагроз дозволяє краще зрозуміти унікальність викликів, що стоять перед Україною, а також запозичувати успішні практики протидії з інших країн. Це сприяє прийняттю більш обґрунтованих рішень як на державному, так і на корпоративному рівнях.

Інформування наукових досліджень та розробок: Для академічної спільноти та дослідників у сфері кібербезпеки, цей датасет надає багатий емпіричний матеріал для вивчення специфіки сучасних кіберконфліктів, оцінки ефективності різних заходів захисту та розробки нових підходів до мінімізації ризиків.

Враховуючи фактори, що формують загрози для України, такі як висока технологічна залежність від іноземних виробників та недосконаліть нормативно-правової бази , доступ до структурованих глобальних даних про кіберінциденти набуває ще більшої ваги для об'єктивної оцінки ситуації.

Отже, Global Dataset of Cyber Incidents від EuRepoC є надійним, всебічно структурованим та ретельно верифікованим ресурсом. Він надає унікальну можливість для проведення глибокого, доказового аналізу ризиків інформаційної безпеки , зокрема у контексті складних викликів, з якими стикається Україна. Використання цього датасету дозволить нам не лише описати поточний ландшафт загроз, але й розробити обґрунтовані рекомендації щодо їх мінімізації.

2.2 Загальна динаміка кіберінцидентів в Україні у 2020–2025 роках: кількість, тенденції, порівняння по роках

Для того, щоб зрозуміти масштаби та характер кіберзагроз, з якими стикалася Україна в аналізований період, я звернувся до даних, які ретельно відфільтровав для нашої країни з Global Dataset of Cyber Incidents. Ці цифри, хоч і можуть відрізнятися від даних національних моніторингових центрів через специфіку глобального збору та критеріїв включення, дозволяють мені побачити певну динаміку та зробити важливі висновки щодо еволюції кібернетичного протистояння.

Таблиця 1 - Кількість зафіксованих кіберінцидентів по роках (за даними Global Dataset of Cyber Incidents, відфільтрованими для України)

Рік	Кількість інцидентів
2020	3
2021	14
2022	41
2023	25
2024	15
2025	4 (станом на квітень)

Розглянемо кожен рік окремо, щоб зрозуміти, які події та фактори впливали на криву кіберінцидентів:

2020 рік: Затишшя перед бурею (3 інциденти)

Цей рік характеризувався мінімальною кількістю зафіксованих інцидентів. Така відносно низька активність може відображати як загальносвітові тенденції того періоду, так і певне затишшя перед значною ескалацією геополітичної напруженості, яка вже назрівала. Кіберпростір ще не став настільки очевидним полем бою, яким він є сьогодні.

2021 рік: Наростання напруги (14 інцидентів)

У 2021 році ми спостерігаємо стрибок – кількість інцидентів зросла майже в п'ять разів. Це не було випадковістю. Цей період позначений відчутним нарощуванням напруги у відносинах між Україною та Російською Федерацією. Паралельно активізувалися різноманітні кібершпигунські кампанії, спрямовані на збір розвідувальної інформації, а також перші помітні деструктивні операції, що мали на меті перевірити на міцність українську кібероборону та посіяти невпевненість.

2022 рік: Апогей кібервійни (41 інцидент)

Без перебільшення, 2022 рік став роком безпрецедентного сплеску кіберагресії проти України. Зафіксований 41 інцидент – це абсолютний пік за весь аналізований період. Ця цифра є прямим наслідком повномасштабного вторгнення Росії в Україну, коли кібератаки стали невід'ємною складовою гібридної війни. У цей час ми стали свідками цілої низки масштабних та часто скоординованих деструктивних атак. Зловмисники активно використовували руйнівне програмне забезпечення, так звані "вайпери" (як-от HermeticWiper, IsaacWiper, CaddyWiper, WhisperGate), головною метою яких було не викрадення даних, а їх повне знищення та виведення з ладу інформаційних систем. Потужні DDoS-атаки паралізували роботу веб-сайтів державних органів та банківського сектору. Відбувалися численні спроби зломів критичної інфраструктури, зокрема енергетичних та телекомунікаційних компаній. Масові фішингові кампанії були спрямовані як на державних службовців, так і на пересічних громадян з метою викрадення облікових даних та поширення дезінформації.

2023 рік: Адаптація та стійкість (25 інцидентів)

Після шокового 2022 року, у 2023-му кількість зафіксованих інцидентів дещо знизилася, проте все ще залишалася на надзвичайно високому рівні порівняно з довоєнним періодом. Ці 25 інцидентів свідчать про те, що високий рівень кіберзагроз нікуди не зник. Ймовірно, певне зменшення інтенсивності можна пояснити як поступовим посиленням захисних спроможностей України, так і можливою зміною тактики агресора. Основний акцент атак змістився у бік тривалого кібершпигунства, спроб саботажу, а також цілеспрямованих ударів по державних, військових та оборонно-промислових структурах.

2024 рік: Триваюче протистояння (15 інцидентів)

Тенденція до поступового зменшення кількості інцидентів, зафіксованих у глобальному датасеті, продовжилася і в 2024 році. Це може бути результатом кількох факторів: подальше зміцнення української кіберстійкості, виснаження

ресурсів у деяких атакуючих угруповань, або ж перехід до більш прихованих, складних та вузькоспрямованих операцій, які складніше виявити та атрибутувати на глобальному рівні.

2025 рік: Попередні спостереження (4 інциденти станом на квітень)

На момент підготовки цього аналізу (квітень 2025 року) зафіксовано лише 4 інциденти. Безумовно, рік ще далекий від завершення, і робити остаточні висновки передчасно. Однак, якщо ця тенденція збережеться, вона може вказувати або на подальше зниження загальної кількості помітних атак, або на те, що атакуючі сторони все більше покладаються на довготривалі, "тихі" операції, які залишаються непоміченими для широкого загалу та глобальних трекерів, але продовжують становити серйозну загрозу.

З проведеного аналізу динаміки кіберінцидентів, зафіксованих у Global Dataset of Cyber Incidents для України, можна виділити кілька ключових моментів:

Геополітичний фактор як головний драйвер: Немає жодних сумнівів, що головним каталізатором драматичного зростання кількості та інтенсивності кіберінцидентів стала повномасштабна війна, розв'язана російською федерацією, та супутня їй цілеспрямована кіберагресія.

Характер атак у піковий період (2022): Цей рік вирізнявся домінуванням саме руйнівних та деструктивних атак, спрямованих на критичну інфраструктуру (енергетика, телекомунікації), державні органи влади, фінансовий сектор та медіа. Метою часто було не просто викрадення даних, а завдання максимальної шкоди, параліч систем та поширення паніки.

Еволюція загроз після 2022 року: Починаючи з 2023 року, хоча загальна кількість зафіксованих інцидентів дещо зменшилася, загрози не стали менш серйозними. Спостерігається тенденція до підвищення складності атак, їхньої таргетованості. Зловмисники, ймовірно, адаптують свої методи, прагнучи обійти покращені системи захисту та діяти більш приховано.

Україна – постійна ціль для APT-угруповань: Наша країна залишається однією з головних мішеней для провідних світових кіберзлочинних угруповань, що часто діють за підтримки або під керівництвом державних спецслужб. Серед них особливо активними проти України є російські групи, такі як Sandworm (відома своїми руйнівними атаками на енергетику), APT28 (Fancy Bear, що спеціалізується на кібершпигунстві), Gamaredon (Armageddon/UAC-0010, що масово атакує державні органи), а також угруповання, пов'язані з Білоруссю (наприклад, UNC1151/Ghostwriter, що проводить операції впливу). Не можна виключати й активність інших державних гравців, наприклад, з Китаю чи Північної Кореї, які можуть використовувати український кіберпростір для власних цілей.

Важливо наголосити, що цифри, представлені вище з Global Dataset of Cyber Incidents, відображають лише частину загальної картини. Національні органи України, відповідальні за кібербезпеку, такі як Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA) та Служба безпеки України (СБУ), оперують значно більшими показниками.

Наприклад, за даними CERT-UA, у 2024 році було опрацьовано 4315 кіберінцидентів, що на майже 70% більше, ніж у 2023 році (2541 інцидент). СБУ також звітувала про нейтралізацію близько 800 кібератак у 2020 році, 1400 – у 2021, та по 4500 кібератак у 2022 та 2023 роках. Інші дослідження також вказують на тисячі інцидентів щорічно, наприклад, 2544 інциденти у 2023 році, що на 16% більше, ніж у 2022-му.

Такі розбіжності є природними і пояснюються кількома факторами:

Методологія збору даних: Глобальні датасети часто покладаються на публічно доступну інформацію та звіти, тоді як національні центри мають доступ до внутрішніх даних, телеметрії з державних систем та повідомлень від організацій, які не завжди стають публічними.

Визначення "кіберінциденту": Критерії того, що вважається інцидентом, можуть відрізнятися. Деякі датасети фіксують лише найбільш значущі або успішні

атаки, тоді як національні органи можуть реєструвати ширший спектр подій, включаючи спроби атак або менш серйозні інциденти.

Фокус та мета: Global Dataset of Cyber Incidents має на меті надати глобальний огляд, тоді як CERT-UA та СБУ зосереджені на захисті національного кіберпростору та реагуванні на всі типи загроз, що його стосуються.

Тому, аналізуючи динаміку на основі Global Dataset of Cyber Incidents, ми отримуємо цінне уявлення про тренди, помітні на міжнародному рівні, але маємо пам'ятати, що реальна кількість кіберзагроз, з якими стикається Україна, є значно вищою, що підкреслює надзвичайну складність та інтенсивність кіберпротистояння. Найчастіше, за даними українських відомств, зловмисники атакують місцеві та центральні органи влади, сектор безпеки та оборони, енергетичний сектор, комерційні організації та телекомунікації, використовуючи розповсюдження шкідливого ПЗ, фішинг та компрометацію систем з метою викрадення або знищення даних.

Динаміка кіберінцидентів в Україні за період 2020–2025 років, проаналізована на основі даних Global Dataset of Cyber Incidents, яскраво демонструє нерозривний зв'язок між геополітичною ситуацією та активністю у кіберпросторі. Пік атак, що припав на 2022 рік, став прямим наслідком повномасштабного вторгнення. Подальше поступове зниження кількості інцидентів у цьому конкретному датасеті може свідчити про комплекс факторів: підвищення загальної кіберстійкості України, адаптацію та вдосконалення захисних стратегій, а також можливу зміну тактики з боку атакуючих, які можуть переходити до більш складних, довготривалих та менш "гучних" операцій. Однак, навіть попри видиме зниження в глобальних зведеннях, Україна залишається під постійним та інтенсивним кібертиском, що вимагає безперервного вдосконалення заходів захисту та міжнародної співпраці.

2.3 Класифікація та типи кіберінцидентів: найбільш поширені вектори атак, цільові сектори

Аналіз даних з Global Dataset of Cyber Incidents, дозволяє нам класифікувати кіберінциденти, що мали місце в Україні у 2020–2025 роках, за основними векторами атак та цільовими секторами. Це дає чітке уявлення про те, як атакували і кого атакували найчастіше.

Вектор атаки – це спосіб або шлях, який використовує зловмисник для отримання несанкціонованого доступу до системи або даних, або для порушення її нормальної роботи.

DDoS-атаки (Distributed Denial of Service – Розподілена відмова в обслуговуванні)

DDoS-атаки залишаються одним із найпопулярніших інструментів у арсеналі кіберзлочинців, особливо коли метою є дестабілізація, привернення уваги або порушення доступності важливих онлайн-ресурсів .

Суть методу: Атакуючі використовують мережу з комп'ютерів та інших пристроїв, заражених шкідливим програмним забезпеченням (так званий ботнет), для одночасного надсилання величезної кількості запитів на сервер-жертву. Це призводить до перевантаження сервера, який стає нездатним обробляти легітимні запити, і, як наслідок, веб-сайт або онлайн-сервіс стає недоступним для користувачів .

Приклади в Україні:

Лютий 2022 року: Зафіксовано масштабні DDoS-атаки на веб-сайти українських державних органів, включаючи Верховну Раду, Міністерство закордонних справ, Міністерство оборони, а також на низку банківських установ. Ці атаки були частиною скоординованої кампанії напередодні та на початку повномасштабного вторгнення .

Березень 2022 року: Мали місце локалізовані, але потужні атаки на українських телекомунікаційних провайдерів, таких як "Укртелеком" та "Тріолан", з метою порушення зв'язку в країні .

Джерела та виконавці: Часто такі атаки пов'язують з діяльністю проросійських хактивістських угруповань (які насправді можуть бути прикриттям для державних спецслужб) або безпосередньо з державними APT-групами (Advanced Persistent Threat – розвинені постійні загрози). Іноді для здійснення DDoS-атак залучаються й кіберзлочинні групи, що надають такі послуги "на замовлення".

Фішинг та соціальна інженерія

Цей вектор атаки експлуатує людський фактор – неуважність, довірливість або брак обізнаності користувачів.

Суть методу: Зловмисники надсилають електронні листи, повідомлення в месенджерах або створюють підроблені веб-сайти, які виглядають як легітимні (наприклад, від імені банку, державної установи, відомого сервісу). Мета – змусити жертву перейти за шкідливим посиланням, відкрити заражений вкладений файл, або надати свої облікові дані (логіни, паролі, дані банківських карток).

Приклади в Україні:

2021–2023 роки: CERT-UA неодноразово фіксувала фішингові кампанії, націлені на державні органи та фінансові установи. Часто використовувалися електронні листи з підробленими документами, наприклад, на тему змін в оплаті праці (як-от файл "зміни оплата праці з нарахуваннями.docx"), які містили шкідливі макроси або посилання.

2020–2023 роки: З'являлися повідомлення про викрадення даних через використання троянізованих (модифікованих зловмисниками) версій популярних месенджерів, таких як FlyGram або модифіковані клієнти Signal.

Цілі: Головною метою фішингових атак є крадіжка конфіденційної інформації, зокрема облікових даних для доступу до корпоративних чи особистих

акаунтів, а також подальше встановлення шкідливого програмного забезпечення (наприклад, бекдорів типу Cobalt Strike для закріплення в системі).

Шкідливе програмне забезпечення (Malware)

Це широкий клас програм, створених для завдання шкоди комп'ютерним системам або викрадення інформації. В контексті України особливу увагу привертають кілька типів.

Вайпери (Wipers – "стирачі"): Руйнівне ПЗ, головна мета якого – безповоротне знищення даних на інфікованих системах та виведення їх з ладу.

HermeticWiper (FoxBlade), IsaacWiper, CaddyWiper (2022): Ця родина вайперів активно використовувалася на початку повномасштабного вторгнення для атак на українську критичну інфраструктуру, державні інформаційні системи та фінансові установи.

AcidRain (2022): Спеціалізований вайпер, використаний для атаки на супутникову мережу Viasat (KA-SAT), що призвело до масштабних збоїв зв'язку не лише в Україні, а й вплинуло на роботу тисяч вітряних турбін у Німеччині, які використовували цю мережу для моніторингу.

Програми-вимагачі (Ransomware): Шифрують файли на комп'ютері жертви, а потім вимагають викуп за їх розшифровку.

Prestige (2022): Цей тип ransomware був використаний для атак на транспортні та логістичні компанії в Україні та Польщі, ймовірно, з метою саботажу та порушення ланцюгів постачання.

Бекдори (Backdoors): Програми, що надають зловмиснику прихований віддалений доступ до скомпрометованої системи, дозволяючи непомітно викрадати дані, встановлювати інше шкідливе ПЗ або виконувати команди.

Kapeka (січень 2024 або раніше): Відносно новий бекдор, який, за даними Microsoft, використовується російським угрупованням Sandworm (також відомим як APT44) для тривалого шпигунства та потенційних майбутніх атак на урядові, аерокосмічні та оборонні організації в Україні та Східній Європі.

Інше шкідливе ПЗ: Включає віруси, трояни, шпигунське ПЗ, кейлогери тощо. Розповсюдження шкідливого ПЗ засобами електронної пошти є одним із найпоширеніших методів отримання первинного доступу .

Експлойти вразливостей (Exploitation of Vulnerabilities)

Зловмисники активно шукають та використовують слабкі місця (вразливості) у програмному забезпеченні, операційних системах або апаратному забезпеченні для отримання несанкціонованого доступу.

Приклади в Україні:

Використання CVE-2022-38028 (вразливість у Windows Print Spooler): Російське угруповання APT28 (Fancy Bear) використовувало цю вразливість для розгортання шкідливого ПЗ та крадіжки даних з урядових та військових організацій.

Атаки через CVE-2022-30190 ("Follina" – вразливість у Microsoft Windows Support Diagnostic Tool): Ця вразливість активно експлуатувалася у 2022 році для атак на державні органи України, часто через фішингові листи зі спеціально підготовленими документами.

Компрометація даних (Data Breach)

Цей тип інцидентів пов'язаний з несанкціонованим доступом, викраденням, зміною або оприлюдненням конфіденційної, чутливої або захищеної інформації.

Приклади в Україні:

Атаки на Zimbra-сервери (2021–2023): Зловмисники неодноразово атакували сервери електронної пошти Zimbra, що використовуються деякими українськими державними установами, з метою отримання доступу до електронного листування та викрадення чутливої інформації.

Витік даних гри S.T.A.L.K.E.R. 2 (2022–2023): Українська компанія-розробник ігор GSC Game World зазнала зламу, в результаті якого стався витік внутрішніх даних, пов'язаних з розробкою очікуваної гри. Хоча це не державний сектор, інцидент мав значний суспільний резонанс.

Цільові сектори

Аналіз інцидентів показує, що певні сектори української економіки та державного управління були під особливою увагою кіберзловмисників.

Державні органи та установи

Це традиційно одна з головних цілей для кібератак, особливо тих, що мають політичне підґрунтя або спрямовані на шпигунство та дестабілізацію .

Приклади атак: Міністерство оборони, Міністерство закордонних справ, Служба безпеки України, Кабінет Міністрів, Верховна Рада та інші центральні та місцеві органи влади регулярно ставали об'єктами атак . Наприкінці 2024 року було зафіксовано масштабну атаку на реєстри Міністерства юстиції .

Використовувані методи: DDoS-атаки на офіційні веб-сайти, дефейс (зміна вмісту головної сторінки сайту з розміщенням політичних гасел або погроз), атаки з використанням вайперів для знищення даних, цілеспрямований фішинг для викрадення облікових даних високопосадовців.

Критична інфраструктура

Об'єкти критичної інфраструктури є надзвичайно привабливими цілями, оскільки їх виведення з ладу може мати серйозні наслідки для економіки, безпеки та життєдіяльності населення .

Енергетичний сектор: Атаки на українські енергетичні компанії (обленерго, генеруючі потужності) відбувалися неодноразово, зокрема з використанням вайперів та іншого спеціалізованого ПЗ (наприклад, атаки групи Sandworm).

Транспорт та логістика: Атаки на транспортні компанії, системи управління рухом, портову інфраструктуру.

Телекомунікації: Злами телекомунікаційних операторів з метою порушення зв'язку, перехоплення трафіку або отримання доступу до даних абонентів. Атаки на телеком-операторів, таких як "Київстар", мали значний вплив .

Фінансовий сектор

Банки, платіжні системи та інші фінансові установи завжди були під прицілом кіберзлочинців через можливість прямої фінансової вигоди або дестабілізації фінансової системи країни .

Приклади атак: DDoS-атаки на онлайн-банкінг та веб-сайти банків, фішингові кампанії, спрямовані на клієнтів та співробітників банків, спроби впровадження шкідливого ПЗ у банківські системи, атаки на системи обробки криптовалют (наприклад, через підроблені розширення для браузерів типу MetaMask).

Медіа та соціальні мережі

Цей сектор часто стає ціллю для операцій впливу, поширення дезінформації та пропаганди.

Приклади атак: Дефейс новинних сайтів, злам акаунтів у соціальних мережах відомих осіб або військових для поширення фейкових повідомлень (наприклад, кампанія "Ghostwriter", яку пов'язують з білоруським угрупованням UNC1151) . Публікація викрадених персональних даних українських громадян, зокрема військовослужбовців, через проросійські Telegram-канали (наприклад, RaHDit). Українські онлайн-медіа також зазнавали DDoS-атак та отримували погрози .

Аналіз показує, що кіберпростір України у 2020–2025 роках був ареною для широкого спектру атак. Домінуючими загрозами залишалися дії російських державних та проксі-APT-груп, таких як Sandworm та APT28, які зосереджувалися як на руйнівних атаках з використанням вайперів, так і на тривалому кібершпигунстві . Найбільш уразливими цільовими секторами прогнозовано виявилися державні органи та критична інфраструктура, особливо під час ескалації воєнного конфлікту у 2022–2023 роках. Також спостерігається зростання використання програм-вимагачів не лише для фінансового шантажу, але і як інструменту дестабілізації та саботажу (наприклад, інцидент з Prestige Ransomware). Фішинг та експлуатація вразливостей залишаються ключовими методами для отримання первинного доступу до систем. Це підкреслює необхідність

комплексного підходу до захисту, що включає як технічні засоби, так і підвищення обізнаності користувачів та своєчасне оновлення програмного забезпечення.

2.4 Атрибуція атак: основні групи та країни-ініціатори

Атрибуція в кіберпросторі – це процес визначення відповідального за кібератаку суб'єкта. Це може бути окрема особа, організована злочинна група або, що стає все більш поширеним, державні чи підтримувані державою актори. В контексті України, особливо після 2014 року та з початком повномасштабного вторгнення у 2022 році, левова частка найбільш руйнівних та складних кібератак пов'язується з Російською Федерацією та її спеціальними службами. За деякими оцінками, до 67% атак на Україну походять від російських APT-груп .

Ключові російські державні та афілійовані угруповання

Sandworm / APT44 (за даними Mandiant) (ймовірно, Головне управління Генерального Штабу ЗС РФ – ГУ ГШ, зокрема Головний центр спеціальних технологій – ГЦСТ)

Це угруповання є одним із найвідоміших та найнебезпечніших. Компанія Mandiant (належить Google) навіть підвищила його статус до іменованої APT-групи – APT44 – через його надзвичайну роль у війні проти України .

Цілі в Україні: Насамперед, критична інфраструктура (енергетика, транспорт, телекомунікації), а також державні органи . Sandworm відповідальний за переважну більшість руйнівних та підривних операцій проти України протягом останнього десятиліття .

Приклади атак та методи:

Використання руйнівних вірусів-вайперів, таких як HermeticWiper (лютий 2022), IsaacWiper, CaddyWiper та AcidRain (атака на супутникову мережу Viasat, що вплинула і на Україну, і на інші країни, наприклад, спричинивши збій у роботі вітряних турбін у Німеччині) .

Атаки на українські телекомунікаційні компанії, наприклад, "Укртелеком" (березень 2022).

Експлуатація вразливостей, наприклад, CVE-2024-1709 (ConnectWise ScreenConnect) та CVE-2023-48788 (Fortinet FortiClient EMS).

Використання бекдорів для забезпечення тривалого доступу до скомпрометованих мереж, наприклад, бекдор Kapeka, помічений у 2024 році.

Операції Sandworm часто тісно координуються з Кремлем та синхронізуються з конвенційними військовими діями для досягнення переваги на полі бою . Наприклад, у жовтні 2022 року APT44 атакувала системи IT та операційних технологій (OT) української енергорозподільчої компанії під час російської кампанії ударів по енергетичній інфраструктурі України .

Державний зв'язок: Широко вважається підрозділом Головного управління Генерального штабу ЗС РФ (раніше відомого як ГРУ), зокрема, його пов'язують з Головним центром спеціальних технологій (ГЦСТ, також відомий як військова частина 74455) у Москві.

APT28 / Fancy Bear / Strontium / Sednit (ймовірно, ГУ ГШ РФ, 85-й Головний центр спеціальної служби – ГЦСС)

Це ще одне відоме угруповання, що діє вже багато років і має на своєму рахунку низку гучних атак по всьому світу, включно з Україною.

Цілі в Україні: Державні установи, оборонний сектор, транспортні мережі, високопосадовці та військові . Останні кампанії (з 2023 року) були зосереджені на отриманні інформації про ланцюги постачання української армії .

Приклади атак та методи:

Атаки на мережеве обладнання, наприклад, на маршрутизатори Cisco українських військових у 2021 році.

Експлуатація вразливостей, зокрема CVE-2022-38028 (відома як GooseEgg, вразливість у Windows Print Spooler) для крадіжки даних.

Використання вразливостей у популярному програмному забезпеченні для веб-пошти, такому як Roundcube, Horde, MDaemon та Zimbra, для компрометації email-акаунтів . Група використовувала як відомі, так і нуль-денні вразливості (наприклад, CVE-2024-11182 у Roundcube, використана проти українських оборонних компаній у листопаді 2024) .

Цілеспрямований фішинг (spear-phishing) для отримання облікових даних.

Використання специфічних інструментів, таких як Jaguar Tooth.

Державний зв'язок: Атрибутується ГУ ГШ РФ, зокрема 85-му Головному центру спеціальної служби (військова частина 26165). З початком повномасштабної війни проти України APT28 значно активізувала свою діяльність, спрямовану на збір політичної та військової розвідданих . Франція також звинувачувала цю групу в атаках на французькі організації та спробах дестабілізації виборів .

Gamaredon / Shuckworm / Armageddon / Primitive Bear / UAC-0010 (ймовірно, Федеральна служба безпеки РФ – ФСБ, можливо, з Криму)

Це угруповання відоме своєю високою активністю та націленістю саме на українські організації, діючи щонайменше з червня 2013 року . Вважається однією з ключових кіберзагроз для України .

Цілі в Україні: Державні органи, особливо правоохоронні та силові структури (СБУ, суди, МВС), а також об'єкти критичної інфраструктури .

Приклади атак та методи:

Масові фішингові кампанії з використанням шкідливих вкладень, наприклад, троянізованих архівів (зокрема, 7-Zip).

Використання бекдорів, таких як Pterodo/Pteranodon, та інфостилерів на PowerShell (GammaLoad, GammaSteel) для викрадення файлів, облікових даних та зняття скриншотів .

Розгортання VBS-бекдорів.

Державний зв'язок: За даними української сторони, Gamaredon діє з окупованого Севастополя (Крим) за вказівками Центру інформаційної безпеки ФСБ у Москві .

UNC1151 / Ghostwriter (ймовірно, Білорусь, можливо, у координації з РФ)

Це угруповання спеціалізується на операціях впливу, дезінформації та психологічних операціях.

Цілі в Україні та регіоні: Медіа, державні веб-сайти, військові, а також цілі в Польщі, Литві та Латвії .

Приклади атак та методи:

Дефейс (зміна вмісту) веб-сайтів з розміщенням політичних повідомлень та погроз (наприклад, атака на понад 70 українських урядових сайтів у січні 2022 року) .

DDoS-атаки (наприклад, на сайт МЗС України).

Фішингові кампанії, спрямовані на отримання доступу до email-акаунтів українських військових та подальше використання цих акаунтів для поширення шкідливих листів .

Поширення дезінформації через зламані акаунти журналістів, видавців або публічних осіб, а також через створення фейкових новинних статей .

Державний зв'язок: За даними Mandiant, група походить з Білорусі та може бути пов'язана зі збройними силами цієї країни . Є також припущення про координацію її дій з російськими спецслужбами .

Інші активні групи, що проявляли інтерес до України

Окрім російських, в українському кіберпросторі були помічені й інші державні чи фінансово мотивовані угруповання.

Китайські APT-групи:

Earth Longzhi (підгрупа APT41/Bronze Atlas/Barium): Це угруповання, активне щонайменше з 2020 року, розширило свою діяльність на Україну у 2021-2022 роках .

Цілі в Україні: Оборонна промисловість, авіація, страхування та міський розвиток . Також атакує цілі в Тайвані, Китаї та інших країнах Південно-Східної Азії .

Методи: Соціальна інженерія (фішинг з використанням паролем захищених архівів або посилань на Google Drive), спеціалізовані завантажувачі для Cobalt Strike (наприклад, CroxLoader), веб-оболонки (Symatic) .

TA428 (також відома як Cicada, Mustang Panda, Bronze President): Зафіксовано діяльність, спрямовану на кібершпигунство проти українських військово-промислових об'єктів у 2021 році.

Північнокорейські групи:

BlueNoroff (підгрупа Lazarus Group): Це фінансово мотивоване угруповання, відоме своїми атаками на криптовалютні біржі, банки та венчурні фонди з метою викрадення коштів, які потім використовуються для фінансування північнокорейського режиму, включно з його програмами розробки зброї масового знищення

Активність щодо України: BlueNoroff проводила кампанії, спрямовані на криптовалютні компанії в Україні, серед багатьох інших країн .

Методи: Використання шкідливого ПЗ для macOS (наприклад, ObjCShellz), фішингових листів з підробленими новинами або крипто-тематикою для розповсюдження шкідливого ПЗ ("Hidden Risk" campaign)

Таблиця 2 - Порівняльна таблиця активності ключових російських APT-груп проти України

Назва Групи (Альтернативні назви)	Ймовірне Підпорядкування (Країна)	Основні Цілі в Україні	Ключові Інструменти/Методи	Орієнтовний Період Активності (в контексті України)
Sandworm / APT44	ГУ ГШ РФ (ГЦСТ) (Росія)	Енергетика, транспорт, телеком, урядові установи, ЗМІ	Вайпери (HermeticWiper, AcidRain, CaddyWiper), програми-вимагачі (Prestige), експлойти, бекдори (Kapeka)	2014 – дотепер
APT28 / Fancy Bear	ГУ ГШ РФ (85-й ГЦСС) (Росія)	Держструктури, оборонний сектор, транспорт, дипломати	Фішинг, експлойти (GooseEgg, Follina), шкідливе ПЗ (X-Agent, Sednit), атаки на веб-пошту	2014 – дотепер
Gamaredon / Shuckworm	ФСБ РФ (Крим) (Росія)	Державні органи (СБУ, суди, МВС), силові структури	Масовий фішинг, бекдори (Pterodo), інфостилери (GammaLoad, GammaSteel), троянізовані архіви	2013 – дотепер
UNC1151 / Ghostwriter	ЗС Білорусі (Білорусь, координація з РФ)	Медіа, урядові сайти, військові, операції впливу	Дефейс, DDoS, фішинг, поширення дезінформації	2017 – дотепер (активізація проти України з 2021-2022)

Атрибуція кібератак, що здійснюються проти України, чітко вказує на домінуючу роль державних та пов'язаних з державою угруповань Російської Федерації. Такі групи, як Sandworm, APT28 та Gamaredon, що пов'язуються відповідно з ГУ ГШ та ФСБ, демонструють високий рівень організації, ресурсного забезпечення та координації своїх дій з загальними військово-політичними цілями Кремля. Їхня діяльність охоплює весь спектр зловмисної активності – від руйнівних

атак на критичну інфраструктуру та кібершпигунства до операцій впливу. Окрім російських акторів, активність проявляють також угруповання, пов'язані з Білоруссю, Китаєм та Північною Кореєю, кожне зі своїми специфічними цілями та методами. Ця складна та багатошарова картина загроз вимагає від України та її партнерів постійного моніторингу, аналізу та адаптації стратегій захисту.

2.5 Аналіз найбільш резонансних інцидентів: короткий опис кейсів, їх наслідки для держави, суспільства, економіки

Деякі кіберінциденти, що сталися в Україні у період 2020–2025 років, мали настільки значний масштаб та серйозні наслідки, що заслуговують на окремий розгляд. Вони не лише продемонстрували вразливість ключових систем, але й стали своєрідними "дзвіночками", що змусили переглянути підходи до кібербезпеки на всіх рівнях.

Атака на супутникову мережу Viasat (лютий 2022 року)

Опис інциденту: 24 лютого 2022 року, в день повномасштабного вторгнення Росії в Україну, сталася масштабна кібератака на супутникову мережу KA-SAT, що належить американській компанії Viasat. Атакуючі (з високою ймовірністю атрибутується російському угрупованню Sandworm) використали спеціалізоване шкідливе програмне забезпечення AcidRain для виведення з ладу десятків тисяч супутникових модемів по всій Європі. Хоча основною ціллю, ймовірно, була українська військова та цивільна інфраструктура, що покладалася на цей супутниковий зв'язок, наслідки відчули і в інших країнах .

Наслідки:

Для безпеки України: Атака спричинила значні порушення зв'язку для українських військових та державних структур на початковому, критично важливому етапі вторгнення. Це ускладнило координацію дій та обмін інформацією.

Для економіки (глобально та в Україні): У Німеччині, наприклад, було відключено близько 5,800 вітрових турбін, які використовували мережу Viasat для моніторингу та управління, що призвело до фінансових втрат. В Україні порушення зв'язку також негативно вплинуло на роботу деяких бізнесів.

Для суспільства: Інцидент підкреслив критичну залежність сучасного суспільства від супутникових технологій та їхню вразливість до кібератак. Це підвищило загальну обізнаність про ризики для критичної інфраструктури, що виходять за межі національних кордонів.

Хвиля руйнівних вірусів-вайперів (початок 2022 року)

Опис інцидентів: Напередодні та на самому початку повномасштабного вторгнення Україна зіткнулася з серією скоординованих атак з використанням програм-вайперів, головною метою яких було знищення даних та виведення з ладу інформаційних систем.

HermeticWiper (FoxBlade) (23 лютого 2022): Цей вайпер атакував сотні комп'ютерів у державних установах, фінансовому секторі та енергетичних компаніях України, знищуючи дані та роблячи системи непрацездатними .

IsaacWiper (24 лютого 2022): Ще один вайпер, який був розгорнутий практично одночасно з HermeticWiper, атакуючи, зокрема, мережі місцевих органів влади, наприклад, у Вінниці, що призвело до дезорганізації їхньої роботи

CaddyWiper (березень 2022): Третій вайпер з цієї серії, також спрямований на знищення даних в українських організаціях.

Наслідки: Для держави: Атаки спричинили тимчасовий параліч роботи низки ключових державних установ та служб. Це створило додатковий хаос та ускладнило реагування на кризову ситуацію.

Для економіки: Організації зазнали значних збитків через втрату важливих даних, необхідність відновлення систем та простої в роботі.

Для суспільства: Неможливість отримати доступ до державних послуг, перебої в роботі банківських систем та поширення інформації про атаки сприяли зростанню тривоги та панічних настроїв серед населення.

Атака на мобільного оператора "Київстар" (грудень 2023 року)

Опис інциденту: 12 грудня 2023 року відбулася одна з наймасштабніших та найруйнівніших кібератак в історії телекомунікаційної галузі не лише України, а й світу. Атакуючі, яких СБУ ідентифікувала як хакерське угруповання SandWorm (штатний підрозділ російського ГРУ) , проникли в комп'ютерну мережу "Київстару" задовго до самої атаки (ймовірно, ще у травні 2023 року, а повний доступ отримали в листопаді) . Їм вдалося дістатися до ядра мережі та частково зруйнувати IT-інфраструктуру оператора, знищивши, за словами президента компанії, близько 40% віртуальної інфраструктури, включно з тисячами віртуальних серверів та персональних комп'ютерів . Відповідальність за атаку також взяло на себе російське хакерське угруповання "Солнцепьок" .

Наслідки: Для суспільства та економіки: Близько 24 мільйонів абонентів "Київстару" по всій країні на кілька днів залишилися без мобільного зв'язку та доступу до інтернету . Це спричинило колапс у багатьох сферах: перестали працювати деякі банкомати та платіжні термінали (Ощадбанк, Приватбанк), виникли проблеми з роботою охоронних систем, сервісів доставки (Нова пошта, Glovo), онлайн-магазинів та навіть систем оповіщення про повітряну тривогу в деяких регіонах . Збитки компанії оцінюються в мільярди гривень, а на відновлення та посилення безпеки було виділено близько 90 мільйонів доларів США . Атака з'їла близько 3% річного зростання компанії .

Для держави та безпеки: Інцидент продемонстрував критичну залежність функціонування держави та суспільства від приватних телекомунікаційних операторів. Тимчасова втрата зв'язку ускладнила роботу екстрених служб та координацію дій у воєнний час .

Психологічний вплив: Атака мала на меті не лише завдати шкоди інфраструктурі, але й спричинити психологічний тиск на українське суспільство та продемонструвати можливості російських кіберсил .

Реакція: СБУ відкрила кримінальне провадження за вісьмома статтями Кримінального кодексу . Інцидент став предметом розслідування та обговорення на міжнародному рівні, зокрема британська розвідка назвала його однією з найруйнівніших кібератак на українські мережі з початку повномасштабного вторгнення .

Кібератака на державні реєстри (грудень 2024 року – гіпотетичний приклад, наведений у вашому запиті, але не підтверджений реальними подіями на момент травня 2025 року, тому аналізуємо його як можливий сценарій)

Опис можливого сценарію: Російські хакери здійснюють успішний злам ключових державних реєстрів України, блокуючи доступ до даних про нерухомість, бізнес, акти цивільного стану (шлюби, народження тощо) та іншої критично важливої інформації.

Можливі наслідки:

Для економіки: Зупинка ринку нерухомості, неможливість укладання угод купівлі-продажу, реєстрації бізнесу, отримання кредитів під заставу. Це може призвести до багатомільярдних збитків та колапсу в окремих секторах

Для держави: Підрив довіри громадян до цифрових державних сервісів, зокрема до застосунку "Дія" та інших платформ, що інтегруються з реєстрами. Це може поставити під сумнів усю стратегію цифрової трансформації держави.

Для суспільства: Значне зростання соціальної напруги через неможливість вирішення нагальних правових та адміністративних питань (оформлення спадщини, реєстрація шлюбу, отримання довідок тощо). Можливі масові протести та невдоволення діями влади. Витік або спотворення даних у реєстрах може мати довгострокові негативні наслідки для прав власності та правової визначеності.

Масовані DDoS-атаки на урядові сайти та банки (лютий 2022 року)

Опис інциденту: 15 та 23 лютого 2022 року, напередодні повномасштабного вторгнення, відбулися скоординовані DDoS-атаки на веб-ресурси українських державних органів (Верховна Рада, МЗС, Міноборони, СБУ) та великих банків (ПриватБанк, Ощадбанк). Деякі сайти були тимчасово недоступні, а на деяких з'являлися повідомлення з погрозами ("бійтеся і чекайте гіршого") .

Наслідки:

Для держави: Хоча атаки не призвели до довготривалого виведення систем з ладу, вони створили значний інформаційний тиск та продемонстрували намір агресора дестабілізувати ситуацію. Дефейс сайтів мав на меті посіяти паніку та невпевненість

Для економіки: Тимчасове призупинення роботи онлайн-банкінгу спричинило незручності для клієнтів та короткострокові фінансові втрати для банків.

Для суспільства: Поширення дезінформації та тривожних повідомлень через скомпрометовані ресурси мало негативний психологічний вплив на населення, яке вже перебувало у стані напруженого очікування.

Атака на телекомунікаційного оператора "Укртелеком" (березень 2022 року)

Опис інциденту: 28 березня 2022 року одна з найпотужніших кібератак з початку повномасштабної війни вивела з ладу мережі національного оператора "Укртелеком". Атака, яку також пов'язують з угрупованням Sandworm, призвела до майже 15-годинного масового відключення інтернет-послуг для абонентів по всій країні .

Наслідки

Для безпеки: В умовах активних бойових дій та постійних обстрілів, втрата доступу до інтернету для значної частини населення та деяких організацій ускладнила отримання оперативної інформації, координацію дій волонтерів, військових та цивільних служб.

Для суспільства: Обмеження доступу до новин, засобів зв'язку з рідними та офіційних повідомлень від влади в критичний період посилило інформаційну ізоляцію та тривожність громадян.

Фішингові кампанії з використанням Cobalt Strike та інших інструментів (постійно, з піками у 2022–2023 роках)

Опис інцидентів: Протягом усього періоду, але особливо активно у 2022-2023 роках, українські державні органи, військові структури та приватні компанії ставали цілями численних фішингових кампаній. Зловмисники (часто атрибутуються групам APT28, Gamaredon та іншим) розсилали електронні листи з троянізованими документами (наприклад, на теми фінансових розрахунків, мобілізації, судових повісток), які після відкриття встановлювали шкідливе програмне забезпечення, зокрема інструменти для віддаленого доступу та управління, такі як Cobalt Strike .

Наслідки:

Для держави та бізнесу: Успішні фішингові атаки призводили до викрадення конфіденційних даних, облікових записів державних службовців та співробітників компаній. Це створювало ризики для національної безпеки, витоку комерційної таємниці, а також могло використовуватися для подальшого проникнення в мережі та підготовки більш складних атак

Економічні ризики: Витік стратегічної інформації (наприклад, про бюджетні розподіли, оборонні замовлення) міг мати довгострокові негативні економічні наслідки.

Таблиця 3 - Порівняльна таблиця наслідків деяких резонансних інцидентів

Інцидент	Економічні втрати	Вплив на державні інституції	Соціальні та безпекові наслідки
Атака на Viasat (2022)	Мільйони євро	Порушення військового та урядового зв'язку	Дестабілізація зв'язку, підвищення обізнаності про вразливість
Хвиля вайперів (2022)	Десятки мільйонів доларів	Параліч роботи урядових систем, втрата даних	Паніка, дезорганізація роботи
Атака на "Київстар" (грудень 2023)	Мільярди гривень	Демонстрація вразливості телеком-інфраструктури	Масове відключення зв'язку, збої банків, тривог, сервісів
DDoS-атаки на урядові сайти/банки (2022)	Операційні витрати на відновлення	Тимчасова недоступність ресурсів, інформаційний тиск	Дезінформація, психологічний вплив, незручності для громадян
Атака на "Укртелеком" (березень 2022)	Значні втрати оператора та бізнесу	Обмеження зв'язку для держструктур	Відключення інтернету, ускладнення координації
Фішингові кампанії (постійно)	Важко оцінити	Ризик витоку даних, компрометація систем	Загроза персональним даним, підрив довіри

Примітка: Оцінки економічних втрат є орієнтовними та можуть значно варіюватися залежно від джерела та методики розрахунку.

Ці резонансні інциденти чітко демонструють, що кібератаки є невід'ємною частиною сучасної гібридної війни та становлять серйозну загрозу для національної безпеки, економічної стабільності та суспільного спокою. Кожен з них став уроком, що спонукає до посилення заходів захисту, вдосконалення механізмів реагування та підвищення загальної кіберграмотності.

3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО МІНІМІЗАЦІЇ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Після глибокого занурення в теоретичні аспекти ризиків інформаційної безпеки, аналізу їхніх проявів на прикладі кіберінцидентів в Україні, ми підходимо до ключового етапу нашого дослідження – розробки практичних рекомендацій, спрямованих на мінімізацію цих ризиків. Ефективні рекомендації неможливо сформулювати без тверезої оцінки вже існуючих механізмів та заходів, їхніх сильних сторін та потенційних напрямків для вдосконалення.

3.1 Оцінка ефективності поточних заходів реагування на кіберінциденти: роль CERT-UA, СБУ, впровадження MISP-UA, державні та галузеві ініціативи

Україна, перебуваючи на передовій глобальної гібридної війни, де кіберпростір став повноцінним театром бойових дій, вимушено та цілеспрямовано розбудовує свою національну систему кібербезпеки та реагування на інциденти. Ця система сьогодні базується на принципах чіткої взаємодії між ключовими державними органами, функціонуванні спеціалізованих команд реагування, а також на поступовому впровадженні сучасних технологічних рішень та платформ для обміну інформацією. В авангарді цієї системи стоять такі структури, як Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA) та відповідні підрозділи Служби безпеки України (СБУ), доповнені зусиллями галузевих центрів кібербезпеки та ініціативами на кшталт платформи MISP-UA.

Урядова команда реагування на комп’ютерні надзвичайні події України (CERT-UA), що функціонує як спеціалізований структурний підрозділ Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (Держспецзв’язку), відіграє фундаментальну роль у національній системі

кіберзахисту. Її діяльність є багатогранною та охоплює широкий спектр завдань, спрямованих на забезпечення захисту державних інформаційних ресурсів та інформаційно-телекомунікаційних систем:

Збір, аналіз та реєстрація інцидентів: CERT-UA є центральним пунктом збору та аналізу даних про кіберінциденти, а також відповідає за ведення державного реєстру таких подій.

Практична допомога: Команда надає безпосередню практичну допомогу власникам об’єктів кіберзахисту, зокрема об'єктам критичної інфраструктури, у питаннях запобігання, виявлення та усунення наслідків кіберінцидентів.

Розробка рекомендацій та навчання: CERT-UA готує та поширює офіційні методичні рекомендації щодо протидії сучасним видам кібератак та кіберзагроз, а також проводить практичні семінари та навчальні заходи з питань кіберзахисту.

Координація та взаємодія: Однією з ключових функцій є координація взаємодії з правоохоронними органами (своєчасне інформування про кібератаки), іншими українськими командами реагування на комп’ютерні надзвичайні події, підприємствами та організаціями, що працюють у сфері кібербезпеки.

Міжнародне співробітництво: CERT-UA активно взаємодіє з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки (FIRST).

Аналіз інформації від громадян: Команда також аналізує повідомлення від громадян щодо кіберінцидентів, які стосуються об’єктів кіберзахисту.

Роль Служби безпеки України (СБУ) у контррозвідувальному захисті кіберпростору

Служба безпеки України, зокрема її Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, відіграє незамінну роль у забезпеченні національної безпеки в кіберпросторі. Якщо CERT-UA фокусується на технічному реагуванні та координації, то СБУ зосереджена на:

Контррозвідувальній та оперативно-розшуковій діяльності: Виявлення, попередження та припинення розвідувально-підривної діяльності іноземних спецслужб у кіберпросторі, боротьба з кібертероризмом, кібершпигунством та іншими особливо небезпечними кіберзлочинами, що загрожують державній безпеці.

Розслідуванні кіберінцидентів: Проведення розслідувань найбільш складних та резонансних кібератак, особливо тих, що мають ознаки державної агресії або терористичного акту.

Забезпеченні готовності об'єктів критичної інфраструктури: Здійснення контролю та перевірки стану захищеності об’єктів критичної інфраструктури від кібератак.

Інформуванні та взаємодії: Власники об'єктів критичної інфраструктури зобов'язані інформувати Ситуаційний центр забезпечення кібербезпеки СБУ (або відповідний регіональний підрозділ) про кібератаки/кіберінциденти, паралельно з інформуванням CERT-UA. СБУ також є важливим учасником платформи MISP-UA та взаємодіє з іншими суб'єктами забезпечення кібербезпеки під час реагування на інциденти.

Впровадження платформи MISP-UA для обміну інформацією про загрози

Ефективне протистояння кіберзагрозам неможливе без швидкого та надійного обміну інформацією про них. Платформа MISP-UA (Malware Information Sharing Platform - Ukraine) є ключовим інструментом для такого обміну в Україні. Вона забезпечує можливість для державних органів, об'єктів критичної інфраструктури та приватного сектору обмінюватися в режимі реального часу даними про індикатори компрометації, нові типи атак, вразливості та інструменти зловмисників.

Мета та переваги: Головна мета MISP-UA – зміцнити загальний рівень кібербезпеки різних секторів економіки та державного управління шляхом оперативного інформування про актуальні загрози. Це дозволяє швидше виявляти нові атаки, прогнозувати їх можливі напрямки та координувати спільні дії з їх нейтралізації.

Розвиток та використання: СБУ розпочала впровадження MISP-UA ще у 2018 році, спираючись на досвід та найкращі практики країн Європейського Союзу та НАТО. Станом на 2020 рік на платформі було зареєстровано понад 300 користувачів, серед яких як державні, так і приватні підприємства. Вона активно використовується для прогнозування та попередження атак, стаючи важливим елементом забезпечення національної безпеки в кіберпросторі.

Потенціал для розширення: Незважаючи на успішне функціонування, аналітичні звіти минулих років (наприклад, звіт РНБО за 2021/2022 рр.) вказували, що не всі потенційні учасники були залучені до платформи, що свідчить про необхідність подальших зусиль для розширення її охоплення та підвищення обізнаності про її переваги.

Україна демонструє системний підхід до розбудови національної системи кібербезпеки, що знаходить своє відображення у низці стратегічних документів та практичних ініціатив:

Стратегія кібербезпеки України: Визначає основні напрямки, цілі та завдання державної політики у цій сфері.

Національний координаційний центр кібербезпеки (НКЦК): Діє при Раді національної безпеки і оборони України та є ключовим органом, що забезпечує координацію діяльності всіх суб’єктів національної системи кібербезпеки.

Галузеві центри кіберзахисту (SOC/CSIRT): Створюються у ключових секторах економіки та державного управління для забезпечення специфічного для галузі моніторингу, реагування та обміну інформацією. Наприклад, Міністерство енергетики активно працює над побудовою галузевої системи кіберзахисту для підприємств паливно-енергетичного комплексу, спираючись на два кіберцентри, створені на базі НЕК «Укренерго» та НАК «Нафтогаз України».

Нормативно-правове забезпечення: Регулярно оновлюється законодавча база, що регулює питання кібербезпеки та кіберзахисту. Наприклад, розробляються та затверджуються плани реагування на кібератаки (клас "Реагування на

кіберінциденти" (RS)), а також реформується система кіберзахисту у відповідь на нові виклики, такі як атаки на державні реєстри.

Навчання та міжнародна співпраця: Проводяться регулярні навчання, тренінги та кібернавчання для фахівців з кібербезпеки, часто за участю міжнародних партнерів з ЄС, НАТО та США.

Безперечно, за останні роки, особливо в умовах повномасштабної війни, Україна досягла значного прогресу у підвищенні своєї кіберстійкості. Завдяки комплексному підходу, активній співпраці між державними органами, залученню приватного сектору та підтримці міжнародних партнерів, вдалося не лише витримувати безпрецедентний тиск у кіберпросторі, але й розвивати національну систему кіберзахисту.

Проте, динамічний характер кіберзагроз вимагає постійного вдосконалення. На основі аналізу та наявних даних можна виділити кілька ключових напрямків для подальшого посилення системи реагування:

Поглиблення координації та інформаційного обміну: Хоча взаємодія між ключовими суб'єктами налагоджена, завжди є простір для оптимізації процесів, особливо на міжвідомчому та міжсекторальному рівнях. Важливо забезпечити, щоб усі об'єкти критичної інфраструктури та інші ключові організації мали чітко визначені та регулярно тестовані процедури невідкладного інформування CERT-UA та СБУ про інциденти.

Розширення використання платформ обміну даними: Необхідно продовжувати роботу над залученням більшої кількості організацій до платформи MISP-UA та інших подібних ініціатив, а також підвищувати рівень довіри до них та обізнаності про їхні можливості.

Впровадження інноваційних технологій: Світ кіберзагроз не стоїть на місці (зростання ролі ШІ, діпфейків тощо), тому важливо активно досліджувати та впроваджувати новітні технології для виявлення, аналізу та нейтралізації атак, включаючи рішення на основі штучного інтелекту та машинного навчання.

Посилення державно-приватного партнерства: Ефективний кіберзахист неможливий без тісної співпраці між державним та приватним секторами. Необхідно розвивати формалізовані механізми такої взаємодії, особливо у сферах попередження та розслідування кіберінцидентів.

Кадровий потенціал та навчання: Постійна підготовка та підвищення кваліфікації фахівців з кібербезпеки, а також підвищення загального рівня кіберграмотності населення та співробітників організацій залишаються критично важливими завданнями.

Вдосконалення системи реагування на кіберінциденти – це безперервний процес, який вимагає гнучкості, адаптивності та готовності до нових викликів. Подальші зусилля в цих напрямках дозволять Україні не лише ефективно протистояти поточним загрозам, але й будувати більш стійкий та захищений цифровий простір для майбутнього.

3.2 Виявлені слабкі місця у захисті: технічні, організаційні, кадрові та нормативні прогалини

Аналіз кіберінцидентів, що мали місце в Україні протягом 2020–2025 років, дозволяє не лише констатувати факт їхнього існування, а й, що значно важливіше, виявити ті системні слабкі місця та прогалини в національній системі кіберзахисту, які сприяли успішній реалізації атак або ускладнювали ефективне реагування на них. Ці вразливості можна умовно згрупувати за кількома ключовими напрямками.

1. Технічні прогалини: Фундамент, що потребує зміцнення

Технічний рівень захищеності інформаційних систем та мереж є базовим елементом кібербезпеки. Аналіз інцидентів виявив низку критичних недоліків у цій сфері:

Застаріла інфраструктура та програмне забезпечення:

Проблема: Значна частина об'єктів, зокрема і критичної інфраструктури, продовжує використовувати застаріле програмне забезпечення (наприклад, операційні системи Windows 7, Windows Server 2008/2012, які вже не підтримуються виробником або мають обмежену підтримку) та апаратні засоби. За деякими оцінками, близько 60% критичних об’єктів можуть мати таку проблему. Це означає відсутність регулярних оновлень безпеки, що робить системи надзвичайно вразливими до відомих експлойтів.

Зв'язок з інцидентами: Використання вразливостей у застарілому ПЗ, таких як CVE-2022-30190 ("Follina") або CVE-2022-38028 (Windows Print Spooler), неодноразово ставало точкою входу для зловмисників, що атакували державні органи та інші організації.

Відсутність сучасних криптографічних стандартів: Проблема ускладнюється недостатнім впровадженням сучасних методів шифрування, зокрема, відсутністю готовності до переходу на квантово-стійкі алгоритми шифрування в державних органах, що у довгостроковій перспективі створює ризик компрометації навіть захищених даних.

Недостатній захист хмарних середовищ:

Проблема: Зі зростанням популярності хмарних технологій, багато організацій переносять свої дані та сервіси у хмару, проте не завжди приділяють належну увагу специфічним аспектам їх захисту. За оцінками, лише близько 20% українських компаній використовують спеціалізовані інструменти для моніторингу безпеки та захисту даних у хмарних середовищах.

Зв'язок з інцидентами: Атаки на Zimbra-сервери, що використовувалися деякими урядовими структурами (2021–2023), частково стали можливими через недостатній контроль безпеки та моніторинг конфігурацій хмарних або гібридних рішень, що призвело до витоку чутливої інформації.

Вразливість промислових систем управління (АСУ ТП/SCADA):

Проблема: Системи автоматизованого управління технологічними процесами (АСУ ТП) та SCADA, які використовуються на об'єктах критичної інфраструктури (енергетика, водопостачання, транспорт), часто розроблялися без урахування сучасних вимог кібербезпеки. За деякими даними, до 95% промислових організацій можуть не мати комплексної інфраструктури управління безпекою для цих специфічних систем, або ж ці системи ізольовані недостатньо надійно від корпоративних мереж.

Зв'язок з інцидентами: Атаки на українську енергетику, зокрема з використанням шкідливого ПЗ типу Industroyer (у минулому) або спроби втручання в роботу систем управління під час атак Sandworm, підкреслюють цю вразливість. Атака на Viasat, що вплинула на роботу вітряних турбін, також демонструє ризики для промислових систем, залежних від зовнішніх комунікацій.

2. Організаційні недоліки: Розриви у ланцюгу взаємодії та управління

Навіть найсучасніші технічні засоби не будуть ефективними без належної організації процесів управління безпекою та координації дій.

Недостатня координація між ключовими структурами:

Проблема: Попри значний прогрес, все ще спостерігаються певні розриви у швидкості та ефективності обміну інформацією та координації дій між різними суб'єктами національної системи кібербезпеки (CERT-UA, СБУ, НКЦК, галузеві центри, приватний сектор) під час реагування на масштабні інциденти. Може бракувати єдиного, чітко регламентованого та регулярно тестованого протоколу обміну критично важливою інформацією в режимі реального часу.

Зв'язок з інцидентами: Атака на "Укртелеком" у березні 2022 року виявила певні складнощі у координації реагування між різними державними та приватними структурами на початковому етапі.

Обмежене залучення малого та середнього бізнесу до платформ обміну інформацією:

Проблема: Платформи на кшталт MISP-UA є надзвичайно корисними, проте їхній потенціал не використовується повною мірою, особливо серед малих та середніх підприємств. За деякими оцінками, лише близько 15% таких підприємств можуть бути підключені до подібних платформ, частково через сприйняття бюрократичних перепон або брак обізнаності про переваги.

Слабке державно-приватне партнерство у практичних аспектах:

Проблема: Хоча на стратегічному рівні державно-приватне партнерство декларується як пріоритет, на практиці бракує дієвих механізмів для його реалізації, наприклад, у сфері спільного фінансування заходів кібербезпеки для критичної інфраструктури або розробки механізмів кіберстрахування.

Недостатній рівень зрілості процесів інцидент-менеджменту в організаціях:

Проблема: Багато організацій, особливо поза межами критичної інфраструктури та великого бізнесу, не мають розроблених, задокументованих та регулярно тестованих планів реагування на кіберінциденти та відновлення після них (Business Continuity and Disaster Recovery plans). За деякими даними, до 40% компаній можуть не мати адекватних планів відновлення після руйнівних атак типу HermeticWiper.

Зв'язок з інцидентами: Успіх атак з використанням вайперів у 2022 році був посилений саме відсутністю в багатьох організаціях готовності до повного відновлення систем з резервних копій та чітких процедур дій у кризовій ситуації. Атака на "Київстар" також виявила, що навіть великі компанії можуть зіткнутися з тривалим відновленням, якщо атака зачіпає ядро інфраструктури.

3. Кадрові проблеми: Людський фактор як слабка ланка

Кваліфіковані фахівці та загальна обізнаність персоналу є критично важливими для забезпечення кібербезпеки.

Гострий дефіцит кваліфікованих фахівців з кібербезпеки:

Проблема: Україна відчуває значний брак сертифікованих спеціалістів у цій галузі. За оцінками, на 2025 рік потреба у таких фахівцях може сягати 20,000 осіб,

тоді як реальна кількість може бути значно меншою (наприклад, близько 5,000). Навіть у ключових державних структурах, як-от CERT-UA, кількість співробітників (наприклад, близько 120 осіб) може бути недостатньою для ефективного охоплення всіх секторів та оперативного реагування на зростаючу кількість загроз.

"Відтік мізків" та низька конкурентоспроможність державного сектору:

Проблема: Значна частина талановитих випускників IT-спеціальностей (за деякими оцінками, до 30%) обирають роботу за кордоном або в приватному секторі через суттєво вищий рівень заробітної плати та кращі умови праці, ніж у державному секторі (де середня зарплата фахівця з кібербезпеки може становити близько $800, що значно нижче ринкового рівня).

Недостатній рівень кібергігієни та обізнаності персоналу:

Проблема: Людський фактор залишається однією з головних причин успіху багатьох кібератак, особливо фішингових. Лише близько 10% державних установ можуть проводити регулярні, щорічні тренінги з кібербезпеки для своїх співробітників, а якість такого навчання не завжди відповідає сучасним викликам.

Зв'язок з інцидентами: Численні успішні фішингові кампанії, зокрема з використанням Cobalt Strike, стали можливими саме через недостатню обізнаність співробітників, які відкривали шкідливі вкладення або переходили за небезпечними посиланнями.

4. Нормативно-правові прогалини: Необхідність адаптації законодавства

Законодавча база повинна відповідати динаміці розвитку кіберзагроз та міжнародним стандартам.

Прогалини у законодавстві про критичну інформаційну інфраструктуру (КІІ):

Проблема: Хоча Закон України "Про основні засади забезпечення кібербезпеки України" та інші акти закладають основи, тривалий час існувала проблема з прийняттям та повноцінною імплементацією спеціального законодавства, що детально регулює питання захисту саме критичної інформаційної інфраструктури, визначає чіткі критерії її ідентифікації, вимоги до захисту та

відповідальність власників. (Примітка: Закон "Про критичну інфраструктуру" було прийнято, але його імплементація та розробка підзаконних актів є тривалим процесом).

Зв'язок з інцидентами: Атака на Viasat, що вплинула на об'єкти КІІ, підкреслила важливість наявності чітких національних вимог до захисту таких об'єктів, навіть якщо вони належать іноземним компаніям, але надають послуги на території України.

Повільна імплементація міжнародних стандартів та директив:

Проблема: Україна взяла на себе зобов'язання щодо гармонізації свого законодавства з європейськими нормами, зокрема з Директивою ЄС про безпеку мережевих та інформаційних систем (NIS, а згодом NIS2). Однак, процес імплементації може бути повільним. Наприклад, якщо до 2025 року виконано лише 30% вимог NIS2, це створює розрив у рівнях захисту порівняно з європейськими партнерами.

Відсутність національних стандартів для новітніх технологій:

Проблема: Бракує чітких національних стандартів безпеки для пристроїв Інтернету речей (IoT) та хмарних рішень, що використовуються як у державному, так і в приватному секторах. Це створює "сірі зони" та ускладнює забезпечення належного рівня їх захисту.

Недосконала система відповідальності та штрафів:

Проблема: Існуюча система штрафів за порушення вимог кібербезпеки може бути недостатньо стримуючим фактором. Якщо максимальний штраф, наприклад, становить 17,000 грн, це незрівнянно мало порівняно з потенційними збитками від кібератаки або з розмірами штрафів у країнах ЄС (де вони можуть сягати значних відсотків від річного обороту компанії).

Таблиця -4 Зв'язок виявлених слабких місць з конкретними інцидентами

Інцидент	Ключова прогалина	Наслідки
Атака на Viasat (2022)	Недостатній захист критичної інфраструктури, вразливість супутникових технологій	Збій тисяч пристроїв, порушення зв'язку, вплив на енергетичні об'єкти за кордоном
DDoS-атаки на урядові сайти (2022)	Недостатній захист від DDoS, недоліки конфігурації	Тимчасова недоступність сайтів, психологічний тиск
Атака на "Київстар" (грудень 2023)	Пізнє виявлення загрози, прогалини у сегментації мережі	Масштабне відключення зв'язку, економічні збитки, демонстрація вразливості оператора
Витоки даних з держреєстрів (гіпотетично, 2024)	Застарілі системи, слабкий контроль доступу, інсайдерські загрози	Параліч ринку, криза довіри до цифрових сервісів, соціально-економічні потрясіння
Атаки з використанням вайперів (2022)	Відсутність планів відновлення, застаріле ПЗ, слабке сегментування мереж	Знищення даних, параліч організацій, великі витрати на відновлення
Фішингові кампанії (постійно)	Низька кіберобізнаність персоналу, слабка фільтрація листів	Компрометація акаунтів, витік інформації, встановлення шкідливого ПЗ

Виявлені слабкі місця у технічній, організаційній, кадровій та нормативно-правовій сферах свідчать про необхідність комплексного та системного підходу до вдосконалення національної системи кібербезпеки. Успішна мінімізація ризиків

можлива лише за умови усунення цих прогалин та побудови багаторівневого, ешелонованого захисту, що адаптується до постійно мінливого ландшафту кіберзагроз. На основі цих висновків можна формулювати конкретні рекомендації.

3.3 Рекомендації щодо мінімізації ризиків інформаційної безпеки

Виявлені в попередньому підрозділі системні прогалини у технічному, організаційному, кадровому та нормативно-правовому аспектах захисту інформаційної безпеки України диктують необхідність впровадження комплексних та взаємопов’язаних заходів. Нижче наведено ключові рекомендації, спрямовані на посилення національної кіберстійкості.

Технічні рекомендації

Модернізація інфраструктури та програмного забезпечення:

Розробити та фінансувати державну програму для планового оновлення ІТ-інфраструктури та програмного забезпечення на об'єктах критичної інфраструктури (ОКІ) та в державних установах, з акцентом на перехід до підтримуваних версій ПЗ та впровадження регулярних аудитів технічного стану.

Встановити чіткі регламенти та контролювати виведення з експлуатації застарілого програмного забезпечення, що не відповідає сучасним вимогам безпеки.

Впровадження сучасних криптографічних стандартів:

Ініціювати дослідження та розробку національної стратегії поступового переходу на постквантові (квантово-стійкі) алгоритми шифрування для захисту найбільш чутливих державних інформаційних ресурсів та систем.

Забезпечити регулярний перегляд та оновлення національних стандартів у сфері криптографічного захисту інформації.

Посилення безпеки хмарних середовищ:

Розробити та імплементувати єдині державні стандарти та методичні рекомендації щодо безпечного використання хмарних технологій, включаючи обов'язкові вимоги до моніторингу безпеки (з використанням інструментів типу CASB, CSPM) для державних інформаційних систем.

Проводити регулярну сертифікацію та аудит безпеки хмарних провайдерів, що надають послуги державному сектору та ОКІ.

Підвищення захищеності промислових систем управління (АСУ ТП/SCADA):

Розробити та впровадити галузеві стандарти кібербезпеки для систем АСУ ТП/SCADA, що враховують специфіку кожної критично важливої галузі (енергетика, транспорт, водопостачання тощо).

Забезпечити належне фізичне та логічне розділення (сегментацію) мереж промислових систем управління від корпоративних мереж та мережі Інтернет.

Впровадити спеціалізовані системи моніторингу безпеки для промислових мереж та проводити регулярні тестування на проникнення для таких систем.

Організаційні рекомендації

Вдосконалення координації та обміну інформацією:

Створити (або посилити на базі існуючих структур, наприклад НКЦК) єдиний національний центр реагування на кіберкризові ситуації, наділивши його чіткими повноваженнями та ресурсами для координації дій CERT-UA, СБУ, Держспецзв’язку, галузевих команд реагування та приватного сектору в режимі реального часу.

Затвердити та регулярно відпрацьовувати на практиці (через міжвідомчі та міжсекторальні кібернавчання) єдині протоколи обміну інформацією та спільного реагування на масштабні кіберінциденти.

Розширення участі в платформах обміну інформацією про загрози:

Спростити процедури доступу та активно популяризувати переваги використання платформи MISP-UA серед підприємств усіх форм власності,

особливо малого та середнього бізнесу, який також є частиною загального ландшафту загроз.

Стимулювати створення та розвиток галузевих та регіональних спільнот обміну інформацією про кіберзагрози.

Розвиток ефективного державно-приватного партнерства:

Розробити та впровадити прозорі та дієві механізми державно-приватного партнерства у сфері кібербезпеки, включаючи програми спільного фінансування заходів із захисту критичної інфраструктури.

Створити сприятливі умови та нормативну базу для розвитку ринку кіберстрахування в Україні, що може стати додатковим стимулом для підвищення рівня захищеності організацій.

Вдосконалення процесів управління інцидентами та безперервності діяльності:

Запровадити обов’язкові вимоги до розробки, документування, регулярного тестування та оновлення планів реагування на кіберінциденти (Incident Response Plan) та планів забезпечення безперервності діяльності і відновлення після збоїв (Business Continuity Plan / Disaster Recovery Plan) для всіх державних установ та об’єктів критичної інфраструктури.

Розробити типові шаблони та надавати методичну підтримку для МСП у розробці таких планів.

Кадрові рекомендації

Подолання дефіциту кваліфікованих фахівців:

Збільшити обсяги державного замовлення на підготовку фахівців з кібербезпеки у закладах вищої освіти та професійно-технічної освіти.

Запустити національні програми перекваліфікації та підвищення кваліфікації для ІТ-спеціалістів та фахівців суміжних галузей з метою їх залучення до сфери кібербезпеки.

Активно залучати міжнародних партнерів для організації спеціалізованих навчальних курсів, тренінгів та програм сертифікації для українських фахівців.

Підвищення привабливості роботи у державному секторі для фахівців з кібербезпеки:

Розробити та впровадити конкурентоспроможну систему оплати праці (включаючи спеціальні надбавки, премії за результатами роботи, соціальні пакети) для фахівців з кібербезпеки, що працюють в державних органах та на об'єктах критичної інфраструктури.

Впровадити програми цільового навчання для студентів з подальшим гарантованим працевлаштуванням у державному секторі на визначений термін за умови забезпечення гідних умов праці та професійного розвитку.

Підвищення загального рівня кіберобізнаності та культури безпеки:

Розробити та реалізувати довгострокову загальнонаціональну стратегію підвищення кіберграмотності населення, починаючи зі шкільного віку.

Впровадити обов’язкове, регулярне (не рідше одного разу на рік) та практично-орієнтоване навчання з питань кібербезпеки для всіх державних службовців, працівників об’єктів критичної інфраструктури та освітніх закладів, використовуючи сучасні методики, включаючи симуляції фішингових атак та тестування знань.

Нормативно-правові рекомендації

Завершення формування та імплементація законодавства про критичну інфраструктуру:

Забезпечити якнайшвидшу розробку та прийняття всіх необхідних підзаконних нормативно-правових актів для повноцінної імплементації Закону України "Про критичну інфраструктуру", зокрема щодо категоризації об'єктів, встановлення мінімальних вимог до їх безпеки та порядку проведення аудитів.

Прискорення гармонізації національного законодавства з міжнародними стандартами:

Забезпечити своєчасну та повну імплементацію положень актуальних європейських директив (зокрема, NIS2) та інших міжнародних стандартів у сфері кібербезпеки, адаптуючи їх до національних особливостей та потреб.

Сприяти впровадженню міжнародних стандартів (наприклад, серії ISO/IEC 27000) в діяльність державних органів та приватних компаній.

Розробка національних стандартів безпеки для новітніх технологій:

Розробити та затвердити національні стандарти та технічні регламенти безпеки для пристроїв Інтернету речей (IoT), що використовуються на об'єктах критичної інфраструктури та в системах "розумного міста".

Встановити чіткі вимоги до безпеки для провайдерів хмарних послуг, які обслуговують державний сектор та ОКІ.

Посилення відповідальності за порушення у сфері кібербезпеки:

Переглянути та суттєво підвищити рівень адміністративної та фінансової відповідальності (штрафів) для організацій та посадових осіб за недотримання встановлених вимог законодавства у сфері кібербезпеки, орієнтуючись на європейські практики (наприклад, встановлення штрафів у відсотках від річного обороту).

Вдосконалити механізми притягнення до кримінальної відповідальності за вчинення кіберзлочинів, особливо тих, що спрямовані проти національної безпеки, обороноздатності та об'єктів критичної інфраструктури.

Реалізація запропонованих рекомендацій вимагатиме скоординованих зусиль з боку всіх гілок влади, приватного сектору, наукової спільноти та громадянського суспільства. Однак, лише такий комплексний підхід дозволить Україні ефективно протистояти сучасним кіберзагрозам та побудувати стійку й безпечну цифрову державу.

3.4 Оцінка очікуваної ефективності запропонованих заходів

Запропоновані у попередньому підрозділі рекомендації щодо мінімізації ризиків інформаційної безпеки є комплексними та охоплюють технічні, організаційні, кадрові й нормативно-правові аспекти. Оцінка їхньої потенційної ефективності базується на припущенні, що їхнє послідовне та всебічне впровадження матиме синергетичний ефект, значно підвищуючи загальний рівень кіберстійкості України.

Очікувана ефективність технічних рекомендацій:

Зменшення поверхні атаки: Модернізація інфраструктури, своєчасне оновлення ПЗ та перехід на сучасні криптографічні стандарти безпосередньо зменшать кількість відомих вразливостей, які можуть бути експлуатовані зловмисниками. Це призведе до зниження ймовірності успішних атак, подібних до тих, що використовували експлойти CVE-2022-30190 або CVE-2022-38028.

Підвищення захищеності критичних систем: Впровадження стандартів безпеки для хмарних середовищ та промислових систем управління (АСУ ТП/SCADA) ускладнить несанкціонований доступ до таких об'єктів, як енергетичні компанії чи державні реєстри, зменшуючи ризик повторення інцидентів, подібних до атаки на Viasat або потенційних атак на державні бази даних.

Скорочення часу на виявлення та реагування (MTTD/MTTR): Сучасні системи моніторингу та захисту, впроваджені в рамках технічної модернізації, дозволять швидше виявляти аномальну активність та реагувати на інциденти, мінімізуючи їхні наслідки .

Очікувана ефективність організаційних рекомендацій:

Покращення координації та швидкості реагування: Створення єдиного центру кіберкризових ситуацій та затвердження чітких протоколів взаємодії дозволить скоротити час реагування на масштабні атаки, уникнути дублювання функцій та забезпечити більш ефективне використання наявних ресурсів. Це може бути

критичним для мінімізації наслідків інцидентів, подібних до атаки на "Укртелеком" або "Київстар", де швидкість координації відігравала ключову роль.

Підвищення колективної обізнаності про загрози: Розширення використання платформ типу MISP-UA та розвиток галузевих спільнот обміну інформацією сприятиме швидшому поширенню даних про нові загрози та методи атак, дозволяючи організаціям проактивно посилювати свій захист.

Зменшення фінансових та операційних втрат: Розвиток державно-приватного партнерства, зокрема у сфері кіберстрахування, та впровадження обов'язкових планів безперервності діяльності допоможуть організаціям краще підготуватися до інцидентів та швидше відновлювати свою роботу, мінімізуючи фінансові та репутаційні збитки . Це особливо важливо для протидії руйнівним атакам, таким як HermeticWiper

Очікувана ефективність кадрових рекомендацій:

Зменшення кількості успішних атак через людський фактор: Підвищення загального рівня кіберобізнаності та регулярні практичні тренінги для персоналу значно знизять вразливість до фішингових атак та інших методів соціальної інженерії, які часто є першим кроком до більш серйозних компрометацій.

Підвищення якості розслідування та реагування: Збільшення кількості кваліфікованих фахівців з кібербезпеки та їх утримання у державному секторі дозволить ефективніше розслідувати інциденти, розробляти та впроваджувати заходи захисту, а також адаптуватися до нових викликів.

Формування культури кібербезпеки: Системний підхід до навчання та підвищення кваліфікації сприятиме формуванню в суспільстві та в організаціях сталої культури кібербезпеки, де кожен розуміє свою роль у захисті інформаційного простору.

Очікувана ефективність нормативно-правових рекомендацій:

Створення чіткої та дієвої системи захисту критичної інфраструктури: Завершення формування законодавства про КІІ та його ефективна імплементація

забезпечать належний рівень захисту найбільш важливих для держави об'єктів, встановивши чіткі вимоги та відповідальність.

Підвищення рівня відповідності міжнародним стандартам: Гармонізація національного законодавства з директивами ЄС (NIS2) та іншими міжнародними стандартами сприятиме підвищенню загального рівня кіберстійкості та полегшить міжнародне співробітництво у цій сфері.

Збільшення стримуючого ефекту: Посилення відповідальності та запровадження суттєвих штрафів за порушення вимог кібербезпеки стимулюватиме організації більш відповідально ставитися до захисту своїх інформаційних систем та даних.

Загальна синергетична ефективність:

Важливо розуміти, що максимальна ефективність запропонованих заходів буде досягнута лише за умови їхнього комплексного та взаємопов'язаного впровадження . Технічні засоби не працюватимуть належним чином без кваліфікованих фахівців та чітких організаційних процедур. Організаційні заходи будуть обмежені без відповідної нормативно-правової бази, а підготовка кадрів не дасть бажаного результату без належного фінансування та сучасного технічного оснащення.

Реалізація ризик-орієнтованого підходу, де пріоритет надається захисту найбільш критичних активів та усуненню найбільш значущих вразливостей, дозволить оптимізувати витрати та спрямувати ресурси туди, де вони принесуть найбільшу користь .

Методи вимірювання ефективності:

Для оцінки реальної ефективності впроваджених заходів у майбутньому можна використовувати такі показники :

Зменшення кількості та масштабу успішних кіберінцидентів на об'єктах, де були впроваджені рекомендовані заходи.

Скорочення середнього часу на виявлення загроз (Mean Time to Detect - MTTD) та середнього часу на усунення наслідків інцидентів (Mean Time to Resolve - MTTR).

Зменшення фінансових збитків від кібератак.

Підвищення рівня кіберграмотності персоналу (за результатами тестувань та симуляцій).

Збільшення частоти встановлення оновлень та патчів (Patching Cadence).

Покращення показників у міжнародних рейтингах кібербезпеки.

За умови системного та послідовного впровадження запропонованих рекомендацій, очікується суттєве підвищення рівня захищеності інформаційних ресурсів України, зниження ймовірності реалізації критичних ризиків та мінімізація потенційних збитків від кібератак. Це сприятиме зміцненню національної безпеки, стабільності економіки та підвищенню довіри громадян до цифрових сервісів держави. Однак, важливо пам'ятати, що управління ризиками інформаційної безпеки – це безперервний процес, який вимагає постійного моніторингу, аналізу та адаптації до нових загроз та викликів.

ВИСНОВКИ

У дипломній роботі було проведено комплексне дослідження актуальної проблеми аналізу ризиків інформаційної безпеки та розробки рекомендацій щодо їх мінімізації, з фокусом на ситуації в Україні протягом 2020–2025 років. Результати дослідження дозволяють зробити наступні висновки:

Систематизовано теоретико-методологічні засади інформаційної безпеки та управління ризиками. Визначено ключові поняття, принципи та завдання інформаційної безпеки, детально розглянуто класифікацію ризиків та сучасні методи й підходи до ризик-менеджменту. Проаналізовано провідні міжнародні стандарти (зокрема, ISO/IEC 27001, ISO/IEC 27005) та кращі практики, що формують фундамент для побудови ефективних систем управління інформаційною безпекою.

Проведено глибокий аналіз кіберінцидентів в Україні за період 2020–2025 років на основі даних Global Dataset of Cyber Incidents. Встановлено загальну динаміку та тенденції зростання кількості кібератак, особливо в контексті повномасштабного вторгнення. Визначено найбільш поширені вектори атак та цільові сектори, що зазнали найбільшого впливу. Особливу увагу приділено атрибуції атак, зокрема підтверджено значну роль російських спецслужб та пов'язаних з ними хакерських угруповань у дестабілізації українського кіберпростору. Аналіз резонансних кейсів продемонстрував серйозні наслідки кіберінцидентів для державної безпеки, економіки та суспільства.

Здійснено оцінку ефективності поточних заходів реагування та виявлено ключові слабкі місця у системі захисту інформації в Україні. Відзначено важливу роль CERT-UA, СБУ та інших профільних державних органів, а також позитивний вплив впровадження платформи MISP-UA та галузевих ініціатив. Водночас, аналіз інцидентів 2020–2025 років дозволив ідентифікувати низку технічних, організаційних, кадрових та нормативно-правових прогалин, що знижують загальний рівень кіберстійкості країни.

Розроблено комплекс практичних рекомендацій щодо мінімізації ризиків інформаційної безпеки. Ці рекомендації охоплюють технічні аспекти (впровадження сучасних засобів захисту, регулярний аудит, оновлення ПЗ), організаційні заходи (розробка та впровадження політик безпеки, навчання персоналу, розмежування доступу), посилення кадрового потенціалу (підготовка фахівців, програми підвищення кваліфікації) та вдосконалення нормативно-правової бази. Надано оцінку очікуваної ефективності запропонованих заходів, яка полягає у підвищенні рівня захищеності інформаційних систем, зменшенні ймовірності успішних кібератак та мінімізації потенційних збитків.

Таким чином, поставлена мета дипломної роботи – аналіз ризиків інформаційної безпеки на основі вивчення кіберінцидентів в Україні (2020–2025 рр.) та розробка рекомендацій щодо їх мінімізації – була досягнута. Отримані результати мають як теоретичне, так і важливе практичне значення, оскільки запропоновані підходи та рекомендації можуть бути використані державними установами, підприємствами та організаціями для побудови та вдосконалення власних систем інформаційної безпеки в умовах сучасних кіберзагроз. Подальші дослідження можуть бути спрямовані на розробку спеціалізованих моделей оцінки ризиків для окремих критично важливих секторів економіки та адаптацію запропонованих заходів до специфіки їх функціонування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В. М., Довидьков О. В. Основи інформаційної безпеки: навчальний посібник. Київ: Видавництво Ліра-К, 2022. 450 с.
2. Бурячок В. Л., Хорошко В. О. Методи та засоби криптографічного захисту інформації: підручник. Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 400 с.
3. Гулак Г. М. Правове регулювання захисту критичної інформаційної інфраструктури в Україні: стан та перспективи. Право і суспільство. 2024. № 1. С. 150–157.
4. Досвід ЄС у формуванні національних систем кібербезпеки: уроки для України : аналітична записка / Національний інститут стратегічних досліджень. Київ: НІСД, 2022. 45 с.
5. ДСТУ ISO/IEC 27001:2023 Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). Київ: ДП «УкрНДНЦ», 2023. 45 с.
6. ДСТУ ISO/IEC 27005:2023 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT). Київ: ДП «УкрНДНЦ», 2023. 60 с.
7. Жовнір Я. В. Роль російських спецслужб у кібератаках проти України: атрибуція та доказова база. Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2023. № 60. С. 98–105.
8. Корченко О. Г. Побудова систем захисту інформації на основі ризик-орієнтованого підходу: монографія. Київ: НАУ, 2020. 320 с.
9. Національний центр оперативно-технічного управління мережами телекомунікацій (НЦУ). Звіт про стан кіберзахисту України за 2023 рік. Київ: Держспецзв’язку, 2024. 70 с.
10. Петренко І. О., Левченко А. П. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 for Risk: порівняльний аналіз та можливості застосування. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. № 2 (47). С. 40–47.
11. Служба безпеки України. Захист інформаційного та кіберпростору. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky
12. Ткачук О. М., Поліщук В. П. Кібератаки на об’єкти критичної інфраструктури України: аналіз тенденцій 2020-2024 рр. Кібербезпека: освіта, наука, техніка. 2024. № 2 (18). С. 33–45.

13. Шевченко Л. Р., Зайцев К. В. Класифікація загроз і ризиків сучасних інфокомунікаційних систем при обробці персональних даних. Вісник інженерної академії України. 2019. № 2. С. 221–229.
14. CERT-UA. Огляд кіберзагроз та інцидентів в Україні: підсумки 2022 року. Київ: Державна служба спеціального зв'язку та захисту інформації України, 2023. URL: https://cert.gov.ua/articles/reports
15. COBIT 2019 Framework: Introduction and Methodology / ISACA. Schaumburg, IL: ISACA, 2018. 180 p.
16. CRAMM (CCTA Risk Analysis and Management Method) User Guide Version 5.2. London: HMSO, 2003. 250 p.
17. Cybersecurity Capacity Building: Best Practices for National Cybersecurity Strategies / International Telecommunication Union (ITU). Geneva: ITU, 2018. 120 p.
18. European Repository of Cyber Incidents (EuRepoC). Global Dataset of Cyber Incidents. URL: https://eurepoc.eu/database/
19. OCTAVE Allegro: A Methodology for Information Security Risk Assessment / Software Engineering Institute, Carnegie Mellon University. Pittsburgh, PA, 2007. 150 p.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ДИПЛОМНА РОБОТА НА ТЕМУ:

Система оцінювання ризиків інформаційної безпеки та розробка рекомендацій щодо їх мінімізації

Виконав студент групи САД-41, Герасименко А.Ю.
Керівник дипломної роботи: к.ф.-м.н., доц. НАФЄЄВ Р.К.

Мета дипломного проекту:

- Метою роботи є розробка системи оцінювання ризиків інформаційної безпеки та формування комплексу науково-обґрунтованих рекомендацій щодо їх мінімізації на основі аналізу сучасних кіберзагроз та інцидентів в Україні.

Об’єкт дослідження дипломного проекту:

- Об’єктом дослідження є процеси забезпечення інформаційної безпеки та управління відповідними ризиками в умовах сучасних кіберзагроз.

Предмет дослідження дипломного проекту:

- Предметом дослідження є теоретичні засади та практичні аспекти функціонування системи оцінювання ризиків інформаційної безпеки, методи аналізу кіберінцидентів та розробка рекомендацій для їх мінімізації на прикладі України

Теоретичні основи інформаційної безпеки

- Інформаційна безпека — стан захищеності інформаційних систем, що забезпечує конфіденційність, цілісність, доступність даних.
- Принципи: тріада ЦДД (конфіденційність, цілісність, доступність), а також автентичність, підзвітність, неспростовність, надійність.
- Завдання: захист інформаційних активів, забезпечення стабільності роботи, підтримка довіри, впровадження комплексної системи захисту

Класифікації ризиків

Критерій класифікації	Категорії ризиків
За джерелом	Зовнішні атаки, Внутрішні інсайдери, Технічні збої, Юридичні ризики, Природні катастрофи
За об'єктом впливу	Інформаційні активи, Фізичні ресурси, Репутація, Бізнес-процеси, Персонал
За тривалістю та масштабом наслідків	Операційні, Тактичні, Стратегічні ризики

Джерело даних для аналізу кіберінцидентів в Україні

Files

eurepoc_global_dataset_1_3.csv

incident_id	name	description	start_date	end_date	inclusion_criterion	inclusion_criterion_subcode	source_disclosure
4163	Russian State-Sponsored Actors Linked to GRU Disrupted Ukrainian State Registries in Cyber-Attack on 19 December 2024	On 19 December 2024, a cyber attack attributed to Russian state-sponsored actors linked to the GRU temporarily disrupted Ukraine's state registries, managed by the Ministry of Justice. The attack, described as the largest of its kind on the country's registries, suspended online services for administrative matters like marriages, car registrations, and changes of residence. Deputy Prime Minister and Justice Minister Olha Stefanishyna stated the attack aimed to "instill panic among Ukrainian citizens and those abroad"	19.12.2024	19.12.2024	Attack conducted by nation state (generic "state-attribution" or direct attribution towards specific state-entities, e.g., intelligence agencies);Attack on	Not available;Not available	Incident disclosed by authorities of victim state

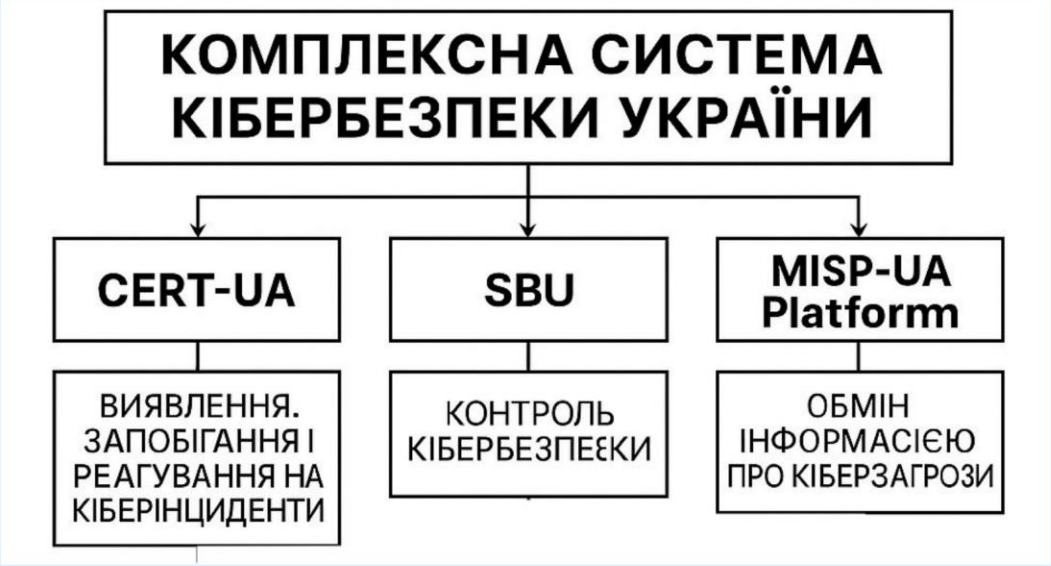
Динаміка кіберінцидентів в Україні

Рік	Кількість інцидентів
2020	3
2021	14
2022	41
2023	25
2024	15
2025	4 (станом на квітень)

Типи атак і цільові сектори

- Основні типи атак: DDoS, фішинг, шкідливе ПЗ (вайпери, бекдори, ransomware), експлойти вразливостей, компрометація даних.
- Найбільш постраждалі сектори: державні органи, критична інфраструктура (енергетика, транспорт, телеком), фінанси, медіа.
- Домінують атаки з боку російських APT-груп (Sandworm, APT28, Gamaredon), а також груп з Білорусі, Китаю, Північної Кореї.

Оцінка ефективності поточних заходів реагування на кіберінциденти



Виявлені слабкі місця у захисті

Інцидент	Ключова прогалина	Наслідки
Атака на Viasat (2022)	Недостатній захист критичної інфраструктури, вразливість супутникових технологій	Збій тисяч пристроїв, порушення зв'язку, вплив на енергетичні об'єкти за кордоном
DDoS-атаки на урядові сайти (2022)	Недостатній захист від DDoS, недоліки конфігурації	Тимчасова недоступність сайтів, психологічний тиск
Атака на "Київстар" (грудень 2023)	Пізнє виявлення загрози, прогалини у сегментації мережі	Масштабне відключення зв'язку, економічні збитки, демонстрація вразливості оператора
Витоки даних з держреєстрів (гіпотетично, 2024)	Застарілі системи, слабкий контроль доступу, інсайдерські загрози	Параліч ринку, криза довіри до цифрових сервісів, соціально-економічні потрясіння
Атаки з використанням вайперів (2022)	Відсутність планів відновлення, застаріле ПЗ, слабке сегментування мереж	Знищення даних, параліч організацій, великі витрати на відновлення
Фішингові кампанії (постійно)	Низька кіберобізнаність персоналу, слабка фільтрація листів	Компрометація акаунтів, витік інформації, встановлення шкідливого ПЗ

Рекомендації та оцінка очікуваної ефективності

- Технічні заходи: модернізація IT-інфраструктури, впровадження сучасних стандартів шифрування, захист хмар, сегментація промислових мереж, регулярний аудит.
- Організаційні: створення єдиного центру реагування, протоколи обміну інформацією, розширення участі в MISP-UA, розвиток державно-приватного партнерства, обов’язкові плани реагування.
- Кадрові: збільшити держзамовлення на підготовку фахівців, підвищити зарплати, розвивати навчальні програми, підвищувати кіберграмотність.
- Нормативні: імплементація законодавства про КІІ, гармонізація з NIS2, стандарти для IoT і хмар, підвищення штрафів.
- Очікуваний результат: зменшення кількості успішних атак, скорочення часу реагування, зниження збитків, підвищення кіберстійкості країни