**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

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

# КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ОПТИМІЗАЦІЯ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ НА ОСНОВІ АНАЛІЗУ РИЗИКІВ ТА ЗАГРОЗ»

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

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

_____ Борщ Владислав
*(підпис)* *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-42

Владислав БОРЩ
Ім'я, ПРІЗВИЩЕ

Керівник: Діана ПРИМАЧЕНКО
Ім'я, ПРІЗВИЩЕ

Рецензент:
Ім'я, ПРІЗВИЩЕ

**Київ 2026**

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ**
**ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**Навчально-науковий інститут кібербезпеки та захисту інформації**

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

**ЗАТВЕРДЖУЮ**
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2026 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ

Борщу Владиславу Сергійовичу
*(прізвище, ім’я, по батькові здобувача)*

1. Тема кваліфікаційної роботи “Оптимізація політик інформаційної безпеки організації на основі аналізу ризиків та загроз”,
керівник кваліфікаційної роботи ПРИМАЧЕНКО Діана.
*(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)*

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

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

3. Вихідні дані до кваліфікаційної роботи: *політики інформаційної безпеки, ризики та загрози організації, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Вивчити теоретичні основи інформаційної безпеки організації.
   4.2. Проаналізувати сучасний стан політик інформаційної безпеки.
   4.3. Дослідити пропозиції щодо оптимізації політик інформаційної безпеки організацій на основі аналізу ризиків.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “05“ березня 2026 р.

# КАЛЕНДАРНИЙ ПЛАН

| № з/п | Етапи кваліфікаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Визначення об’єкту, предмету, мети та завдань дослідження. | 18.03.2026 | |
| 2. | Збір та аналіз літератури. | 30.03.2026 | |
| 3. | Аналіз теоретичних основ інформаційної безпеки організації | 08.04.2026 | |
| 4. | Вивчення аналізу сучасного стану політик інформаційної безпеки | 15.04.2026 | |
| 5. | Аналіз пропозицій щодо оптимізації політик інформаційної безпеки організаций на основі аналізу ризиків | 22.04.2026 | |
| 6. | Формулювання висновків за результатами проведеного дослідження. | 29.04.2026 | |
| 7. | Оформлення роботи. | 06.05.2026 | |
| 8. | Оформлення презентації. | 11.05.2026 | |
| 9. | Отримання рецензії на роботу. | 10.06.2026 | |
| 10. | Захист в ЕК. | __.06.2026 | |

Здобувач вищої освіти _____ Владислав БОРЩ
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

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

**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**
**на здобуття освітнього ступеня бакалавра**

Направляється здобувачка Борщ В.С. до захисту кваліфікаційної роботи
*(прізвище та ініціали)*
за спеціальністю 125 Кібербезпека
*(код, найменування спеціальності)*
освітньої програми Управління інформаційною та кібернетичною безпекою
*(назва)*
на тему: “ Оптимізація політик інформаційної безпеки організації на основі аналізу ризиків та загроз ”

Кваліфікаційна робота і рецензія додаються.

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

**Висновок керівника кваліфікаційної роботи**

Здобувач БОРЩ Владислав у кваліфікаційній роботі вивчив теоретичні основи інформаційної безпеки організації, проаналізував сучасний стан політик інформаційної безпеки, дослідив пропозиції щодо оптимізації політик інформаційної безпеки організацій на основі аналізу ризиків, розробила практичні рекомендації за темою дослідження.

БОРЩ Владислав показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований та відповідальний виконавець.

Все це дозволяє оцінити кваліфікаційну роботу здобувача БОРЩА Владислава на оцінку “добре” та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Діана ПРИМАЧЕНКО
*(підпис)* *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2026 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач Борщ В.С. допускається до захисту даної роботи в Екзаменаційній комісії.

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

# ВІДГУК РЕЦЕНЗЕНТА
## на кваліфікаційну бакалаврську роботу

здобувача вищої освіти БОРЩА Владислава
на тему “Оптимізація політик інформаційної безпеки організації на основі аналізу ризиків та загроз ”

**Актуальність.** Інформаційні ресурси є ключовим активом як бізнесу, так і державних структур, а їх втрата або компрометація може спричинити суттєві фінансові та репутаційні наслідки. Традиційні підходи до захисту інформації виявляються недостатніми перед обличчям сучасних багатовекторних атак, що поєднують технологічні та соціальні інструменти. Оптимізація політик інформаційної безпеки на основі систематичного аналізу ризиків та загроз дозволяє організаціям формувати адаптивні стратегії захисту, що відповідають вимогам міжнародних стандартів.

З огляду на зазначене, дослідження проблеми оптимізації політик інформаційної безпеки організацій на основі аналізу ризиків та загроз є актуальним науковим завданням.

**Позитивні сторони.**

1. У роботі досліджено теоретичні основи та методологічні підходи до формування й оптимізації політик інформаційної безпеки організацій.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.
3. Автор опрацював значну джерельну базу: близько 50 публікацій, в тому числі англомовних.
4. За результатами дослідження запропоновано практичні рекомендації щодо вдосконалення політик інформаційної безпеки та адаптації їх до нових загроз.

**Недоліки.**

Доцільно було б приділити більше уваги порівняльному аналізу сучасних програмних інструментів для автоматизованої оцінки ризиків та моніторингу ефективності впроваджених політик інформаційної безпеки в організаціях.

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

**Висновок:** Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "добре", а здобувач БОРЩ Владислав заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:

_____
*підпис* Ім’я, ПРІЗВИЩЕ

# РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню оптимізації політик інформаційної безпеки організації на основі аналізу ризиків та загроз. Робота складається зі вступу, трьох розділів, що містять 11 рисунків та 12 таблиць, висновків та списку використаних джерел, що містить 61 найменування. Загальний обсяг роботи становить 90 аркушів, з яких 7 аркушів займає список використаних джерел.

***Метою роботи*** є теоретичне обґрунтування основ інформаційної безпеки організації, аналіз сучасного стану політик інформаційної безпеки із практичними прикладами та проблемами їхньої реалізації, а також у розробка пропозицій щодо оптимізації політик інформаційної безпеки на основі аналізу ризиків і загроз.

***Об'єктом дослідження*** є політики інформаційної безпеки організацій як складова системи управління ризиками та захисту інформаційних ресурсів.

***Предмет дослідження*** – процеси оптимізації політик інформаційної безпеки на основі аналізу ризиків і загроз.

***Методи дослідження.*** Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки, системного підходу до управління інформаційною безпекою.

Як результат, у роботі проведено аналіз основних ризиків та загроз інформаційній безпеці організації; досліджено особливості управління політиками безпеки в умовах сучасного кіберсередовища; визначено напрями та методи оптимізації політик інформаційної безпеки на основі аналізу ризиків, міжнародних стандартів, практичних прикладів їх реалізації та рекомендацій провідних дослідників у сфері кіберзахисту

***Галузь застосування*** охоплює державні установи, комерційні підприємства та освітні заклади, що потребують ефективних політик інформаційної безпеки.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКИ БЕЗПЕКИ, РИЗИКИ ТА ЗАГРОЗИ, ОПТИМІЗАЦІЯ, ОРГАНІЗАЦІЯ.

# ABSTRACT

The qualification work is devoted to the study of information security awareness and training technologies for personnel. The work consists of an introduction, three chapters containing 11 figures and 12 tables, conclusions, and a list of references comprising 61 sources. The total volume of the thesis is 90 pages, of which 7 pages are occupied by the list of references.

***The purpose*** of the thesis is to provide a theoretical justification of the fundamentals of organizational information security, to analyze the current state of information security policies with practical examples and implementation challenges, and to develop proposals for optimizing these policies based on risk and threat analysis.

***The object*** of the study is organizational information security policies as a component of risk management and protection of information resources.

***The subject*** of the study is the processes of optimizing information security policies based on risk and threat analysis.

***Research methods.*** In order to solve the mentioned higher scientific task, the methods of analysis and synthesis, comparison, classification, expert assessment, systematic approach to information security management were used in the work.

As a result, the thesis analyzes the main risks and threats to organizational information security; examines the specifics of managing security policies in the modern cyber environment; and identifies directions and methods for optimizing information security policies based on risk analysis, international standards, practical implementation examples, and recommendations of leading cybersecurity researchers.

***The scope*** of application includes government institutions, commercial enterprises, and educational establishments requiring effective information security policies.

Keywords: INFORMATION SECURITY, SECURITY POLICIES, RISKS AND THREATS, OPTIMIZATION, ORGANIZATION.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

| | |
|---|---|
| AI | Штучний інтелект (Artificial Intelligence) |
| AWS | Хмарна платформа Amazon Web Services |
| BCP | План забезпечення безперервності бізнесу (Business Continuity Plan) |
| COBIT | Система управління IT та інформаційною безпекою (Control Objectives for Information and Related Technologies) |
| CSF | Система кібербезпеки NIST (Cybersecurity Framework) |
| DLP | Система запобігання витоку даних (Data Loss Prevention) |
| ENISA | Агентство Європейського Союзу з кібербезпеки |
| GDPR | Загальний регламент захисту персональних даних ЄС |
| IBM | Міжнародна корпорація бізнес-машин (International Business Machines) |
| IEC | Міжнародна електротехнічна комісія |
| ISO | Міжнародна організація зі стандартизації |
| MDM | Управління мобільними пристроями (Mobile Device Management) |
| NIST | Національний інститут стандартів і технологій (США) |
| SIEM | Система управління подіями безпеки (Security Information and Event Management) |
| SOC | Центр операцій безпеки (Security Operations Center) |
| SWOT | Метод стратегічного аналізу (Strengths, Weaknesses, Opportunities, Threats) |
| UBA | Аналітика поведінки користувачів (User Behavior Analytics) |
| URL | Уніфікований локатор ресурсу (Uniform Resource Locator) |
| IT | Інформаційні технології |

# ВСТУП

**Актуальність теми.** Оптимізація політик інформаційної безпеки організації на основі аналізу ризиків та загроз є надзвичайно актуальною у сучасних умовах стрімкої цифровізації та зростання кіберзагроз. Сьогодні інформаційні ресурси виступають ключовим активом бізнесу та державних структур, а їхня втрата чи компрометація може призвести до значних фінансових, репутаційних та соціальних наслідків. Традиційні підходи до безпеки, що ґрунтуються лише на технічних засобах, виявляються недостатніми, адже нові методи атак поєднують технологічні та соціальні інструменти, використовуючи штучний інтелект, багатоканальні стратегії та маніпуляції людським фактором.

Аналіз ризиків та загроз дозволяє організаціям формувати адаптивні політики, які враховують специфіку бізнес-процесів, рівень цифрової грамотності персоналу та вимоги міжнародних стандартів. Це забезпечує не лише технічний захист, але й створення культури безпеки, де кожен співробітник усвідомлює свою роль у захисті даних. В умовах глобалізації та залежності від сторонніх постачальників прозорість і системність політик стають критично важливими. Таким чином, дослідження оптимізації політик інформаційної безпеки є необхідним для підвищення стійкості організацій, їхньої конкурентоспроможності та довіри з боку клієнтів і партнерів.

**Мета дослідження** полягає у теоретичному обґрунтуванні основ інформаційної безпеки організації, аналізі сучасного стану політик інформаційної безпеки із практичними прикладами та проблемами їхньої реалізації, а також у розробці пропозицій щодо оптимізації політик інформаційної безпеки на основі аналізу ризиків і загроз.

Відповідно до мети **завдання дослідження** наступні:

1. Дослідити теоретичні основи інформаційної безпеки організації, зокрема сутність політик інформаційної безпеки та методологічні підходи до аналізу ризиків і загроз.

2. Проаналізувати сучасний стан політик інформаційної безпеки в організаціях, виявити ключові ризики, загрози та проблеми їхньої реалізації.

3. Розробити пропозиції щодо оптимізації політик інформаційної безпеки організацій на основі аналізу ризиків із використанням сучасних цифрових інструментів.

**Об'єкт дослідження** – політики інформаційної безпеки організацій як складова системи управління ризиками та захисту інформаційних ресурсів.

**Предмет дослідження** – процеси оптимізації політик інформаційної безпеки на основі аналізу ризиків і загроз.

**Методи дослідження.** У дослідженні використано теоретичні методи (аналіз, синтез, індукція та дедукція, узагальнення та систематизація наукових джерел) для розкриття сутності політик інформаційної безпеки. Також застосовано практичні методи (аналіз ризиків, вивчення прикладів реалізації та порівняння з міжнародними стандартами) для оцінки ефективності та розробки пропозицій щодо їх оптимізації.

**Інформаційна база дослідження** сформована на основі наукових праць українських та зарубіжних авторів, навчальних посібників і підручників, що висвітлюють теоретичні та практичні аспекти інформаційної безпеки. Вона включає офіційні документи, міжнародні стандарти (ISO/IEC 27001, NIST CSF), аналітичні огляди CERT-UA та матеріали міжнародних організацій, що відображають сучасні тенденції та виклики у сфері кіберзахисту.

Окреме місце займають публікації про актуальні загрози – витоки даних, інсайдерські ризики, атаки на ланцюги постачання та використання штучного інтелекту у кіберзлочинності, що забезпечує комплексність та практичну значущість дослідження.

**Наукова новизна одержаних результатів** полягає у комплексному поєднанні теоретичних засад інформаційної безпеки з практичним аналізом сучасних ризиків та загроз, що дозволяє сформувати адаптивну модель політик безпеки. У роботі вперше систематизовано проблеми реалізації політик на прикладах українських та міжнародних організацій, що забезпечує практичну

значущість висновків. Запропоновані рекомендації щодо оптимізації політик базуються на ризик-орієнтованому підході та інтеграції сучасних цифрових інструментів, що розширює можливості їх застосування в умовах динамічного кіберсередовища.

**Практичне значення одержаних результатів** полягає у можливості використання запропонованих рекомендацій для вдосконалення політик інформаційної безпеки в організаціях різних галузей. Розроблені підходи сприяють підвищенню ефективності управління ризиками та мінімізації загроз, що забезпечує стабільність бізнес-процесів і захист критичних даних. Отримані результати можуть бути інтегровані у корпоративні стандарти та навчальні програми, формуючи культуру безпеки серед працівників.

**Галузь застосування одержаних результатів** охоплює державні установи, комерційні підприємства та освітні заклади, що потребують ефективних політик інформаційної безпеки.

# Розділ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

## 1.1. Поняття, сутність та значення політик інформаційної безпеки

Політика інформаційної безпеки у сучасному науковому дискурсі розглядається як багатовимірний інструмент управління, що поєднує правові, організаційні та технологічні аспекти захисту даних. Вона визначає правила доступу до інформаційних систем, порядок їх використання, відповідальність користувачів та процедури реагування на інциденти. Саме тому зарубіжні дослідники приділяють значну увагу формуванню концептуальних основ цього поняття, підкреслюючи його стратегічне значення для організацій різних рівнів.

Так, Дж. Вітман та Г. Маттord у праці «Принципи інформаційної безпеки» наголошують, що політика інформаційної безпеки є «основним документом [31], який визначає правила доступу до інформаційних систем та відповідальність користувачів». Вони підкреслюють, що без чітко сформульованої політики будь-які технічні засоби захисту залишаються фрагментарними та неефективними. Цей підхід акцентує увагу на тому, що політика виступає не лише регламентом, але й основою для формування системного мислення у сфері безпеки.

Р. Андерсон у монографії «Інженерія безпеки» розглядає політику інформаційної безпеки як «інституційний каркас», що поєднує правові, організаційні та технологічні аспекти [55]. Він зазначає, що політика має бути адаптивною, здатною враховувати нові типи загроз, зокрема кібершпигунство та атаки на критичну інфраструктуру. Андерсон підкреслює, що політика не може бути статичною, адже інформаційне середовище змінюється надзвичайно швидко, і лише гнучкі механізми дозволяють організаціям залишатися захищеними.

Сутність політики інформаційної безпеки полягає у створенні системи правил, які регулюють доступ до інформаційних ресурсів, порядок їх використання, відповідальність за порушення встановлених норм та процедури

реагування на інциденти. На думку Б. фон Солмса та Л. ван Нієрк, політика інформаційної безпеки є «живим документом», який постійно оновлюється відповідно до змін у технологічному та правовому середовищі [31]. Вони підкреслюють, що політика не може бути статичною, адже загрози еволюціонують швидше, ніж організаційні структури, і тому потребують постійного перегляду та вдосконалення.

Значення політики інформаційної безпеки виходить за межі технічного захисту. Вона виконує стратегічну функцію, інтегруючи безпеку у загальну систему управління. Міжнародний стандарт ISO/IEC 27001 визначає політику інформаційної безпеки як основу системи менеджменту безпеки, що забезпечує узгодженість дій усіх працівників та підрозділів [34]. Це означає, що політика стає не лише внутрішнім документом, а й інструментом міжнародної інтеграції, який дозволяє організаціям відповідати глобальним вимогам.

Г. Пелтьє у праці «Політики, процедури та стандарти інформаційної безпеки» наголошує, що політика є «першим кроком до формування зрілої системи управління ризиками» [42]. Він підкреслює, що саме політика створює основу для розробки процедур, інструкцій та технічних рішень. Без неї будь-які заходи залишаються хаотичними та неузгодженими. Пелтьє також звертає увагу на те, що політика повинна бути зрозумілою для всіх співробітників, незалежно від їхнього рівня технічної підготовки, адже лише тоді вона може стати дієвим інструментом управління.

У практичному вимірі політика інформаційної безпеки визначає правила автентифікації та авторизації користувачів, порядок резервного копіювання та відновлення даних, вимоги до використання мобільних пристроїв та хмарних сервісів, стандарти реагування на інциденти та управління кризовими ситуаціями. Вона формує культуру безпеки, де кожен працівник усвідомлює свою роль у захисті інформаційних активів.

Б. Дхіллон у дослідженні «Управління інформаційною безпекою» зазначає, що політика має бути зрозумілою та доступною, а її положення повинні інтегруватися у щоденну діяльність організації [28]. Він підкреслює, що політика

не може бути лише формальним документом – вона має стати частиною корпоративної культури.

Б. Шнайєр у книзі «Дані та Голіаф» підкреслює, що «безпека – це не лише технологія, а й поведінка» [55]. Тому політика інформаційної безпеки повинна формувати у співробітників відповідальне ставлення до інформації, стимулювати дотримання правил та створювати атмосферу довіри.

В українській науковій традиції питання політики інформаційної безпеки досліджується як важливий елемент державної та корпоративної стратегії. Серед сучасних дослідників варто виділити Т. Каменчук, О. Скочиляс-Павлів та С. Гнатюка, які зробили вагомий внесок у формування концептуальних основ цього напряму.

Т. Каменчук у своїх працях аналізує державну політику України у сфері інформаційної безпеки, наголошуючи на її багаторівневому характері [12]. Вона підкреслює, що ефективність політики залежить від узгодженості правових норм, організаційних процедур та технічних стандартів. Каменчук вважає, що політика має бути динамічною та враховувати як внутрішні, так і зовнішні виклики, зокрема інформаційні війни та кіберзагрози.

О. Скочиляс-Павлів досліджує правові механізми забезпечення інформаційної безпеки, акцентуючи увагу на тому, що інформаційний простір України став одним із ключових полів сучасних конфліктів [5]. Вона пропонує авторське визначення інформаційної безпеки як стану захищеності ресурсів, що гарантує їхню конфіденційність, цілісність та доступність. На її думку, політика має поєднувати технічні, політичні та правові інструменти.

С. Гнатюк зосереджується на впровадженні міжнародних стандартів, зокрема ISO/IEC 27001, у практику українських організацій [3]. Він доводить, що політика інформаційної безпеки повинна бути узгоджена з глобальними практиками, адже лише так можна забезпечити ефективний захист у міжнародному інформаційному просторі.

Ключові функції політики інформаційної безпеки організації (рис.1.1) відображають її багатогранний характер та стратегічне значення для захисту

даних. Передусім варто виділити нормативну функцію, яка встановлює правила, стандарти та процедури роботи з інформаційними ресурсами [21]. Вона забезпечує єдиний підхід до використання інформаційних систем і створює основу для узгодженості дій усіх працівників.


Рис.1.1. Ключові функції політики інформаційної безпеки організації

Організаційна функція доповнює цей процес, адже саме вона визначає ролі та відповідальність між керівництвом, адміністраторами та користувачами, формуючи чітку структуру управління безпекою [3]. Захисна функція реалізується через технічні та процедурні заходи, що протидіють внутрішнім і зовнішнім загрозам, включаючи кіберінциденти.

Не менш важливими є превентивна та стратегічна функції. Превентивна спрямована на попередження інцидентів шляхом аналізу ризиків, прогнозування можливих атак та мінімізації їхніх наслідків. Стратегічна інтегрує інформаційну безпеку у загальну систему управління організацією, визначаючи її як складову корпоративної стратегії. Водночас культурно-виховна функція формує корпоративну культуру безпеки, підвищує обізнаність співробітників та їхню відповідальність за захист даних [42]. Контрольна функція забезпечує моніторинг дотримання політики, проведення аудиту та оцінку ефективності заходів безпеки, що дозволяє своєчасно виявляти слабкі місця та вдосконалювати систему.

Адаптивна та кризова функції підкреслюють гнучкість і практичність політики. Адаптивна передбачає постійне оновлення положень відповідно до нових технологій, стандартів та загроз, що виникають у цифровому середовищі. Кризова функція визначає порядок дій у випадку інцидентів, аварій чи атак,

забезпечуючи швидке відновлення працездатності систем та мінімізацію негативних наслідків [12]. У сукупності всі ці функції формують комплексний інструмент управління, який дозволяє організації не лише захищати свої інформаційні ресурси, а й інтегрувати безпеку у стратегічний розвиток та корпоративну культуру.

Основні елементи політики інформаційної безпеки організації (рис.1.2) формують її зміст та структуру, забезпечуючи комплексний підхід до захисту інформаційних ресурсів. Передусім варто виділити мету та завдання політики, які визначають стратегічні цілі та пріоритети у сфері інформаційної безпеки. Важливим є також окреслення сфери застосування, де зазначається, які інформаційні системи, процеси та користувачі підпадають під дію політики.


Рис.1.2. Основні елементи політики інформаційної безпеки організації

Другим ключовим елементом є принципи та базові положення, що закріплюють фундаментальні правила: конфіденційність, цілісність та доступність інформації. Не менш значущим є визначення ролей та відповідальності, адже саме чіткий розподіл обов’язків між керівництвом, адміністраторами та користувачами дозволяє уникнути хаосу та забезпечити узгодженість дій [31]. До структури політики входять також механізми контролю та моніторингу, які регламентують порядок перевірки дотримання правил, проведення аудиту та реагування на інциденти.

Окремо слід виділити процедури оновлення та перегляду політики, що забезпечують її актуальність відповідно до нових технологій, стандартів та загроз [40]. У практичному вимірі політика включає технічні заходи

(автентифікація, авторизація, резервне копіювання, захист мереж), а також організаційні заходи (регламентація доступу, порядок використання мобільних пристроїв та хмарних сервісів). Завершальним елементом є заключні положення, які визначають відповідальність за порушення та порядок внесення змін.

Політика інформаційної безпеки відіграє ключову роль у створенні системи захисту даних та інформаційних ресурсів організації. Вона виступає нормативним фундаментом, який визначає правила доступу, використання та збереження інформації, а також встановлює відповідальність за порушення встановлених норм. Завдяки політиці формується єдиний підхід до управління безпекою, що дозволяє уникнути хаотичних дій та забезпечити узгодженість між різними підрозділами [36]. Крім того, політика створює основу для впровадження технічних та організаційних заходів, таких як автентифікація, резервне копіювання, моніторинг систем та реагування на інциденти.

Політика інформаційної безпеки не існує ізольовано, а інтегрується у загальну стратегію розвитку організації. Вона визначається як стратегічний інструмент, що забезпечує стійкість бізнес-процесів та захист критично важливих активів [47]. У сучасних умовах цифровізації та глобальної конкуренції інформаційна безпека стає частиною корпоративної стратегії, адже від її ефективності залежить репутація, фінансова стабільність та конкурентоспроможність компанії.

Політика узгоджується з іншими управлінськими документами, такими як стратегія ризик-менеджменту, план розвитку IT-інфраструктури чи корпоративна стратегія інновацій. Вона забезпечує гармонійне поєднання технічних рішень із бізнес-цілями, дозволяючи організації не лише захищати дані, а й ефективно використовувати інформаційні ресурси для досягнення стратегічних результатів.

Політика інформаційної безпеки безпосередньо впливає на ефективність управління ризиками в організації. Вона визначає порядок і методи аналізу ризиків, встановлює процедури їхнього моніторингу та мінімізації. Завдяки політиці створюється система превентивних заходів, яка дозволяє своєчасно

виявляти потенційні загрози та розробляти механізми реагування [55]. Політика також забезпечує узгодженість між різними рівнями управління ризиками – від стратегічного до операційного, що дозволяє організації діяти системно та ефективно. У результаті вона сприяє зниженню ймовірності інцидентів, мінімізації фінансових втрат та збереженню репутації компанії [5]. Таким чином, політика інформаційної безпеки є не лише регламентом, а й дієвим інструментом управління ризиками, який забезпечує стійкість та стабільність організації в умовах сучасних викликів.

Отож, політика інформаційної безпеки організації є багатовимірним інструментом управління, що поєднує правові, організаційні та технологічні аспекти захисту даних і формує основу для комплексного управління ризиками. Вона інтегрується у загальну стратегію організації, забезпечуючи стійкість бізнес-процесів, узгодженість дій працівників та відповідність міжнародним стандартам. Її значення виходить за межі технічного регламенту, адже політика формує корпоративну культуру безпеки, підвищує відповідальність персоналу та сприяє стабільному розвитку організації в умовах сучасних викликів.

## 1.2. Класифікація ризиків та загроз у сфері інформаційної безпеки

Загальні підходи до визначення ризиків та загроз у сфері інформаційної безпеки організації базуються на системному аналізі факторів, що можуть впливати на стабільність функціонування інформаційних систем та захищеність даних [3]. У сучасному науковому дискурсі ризик трактується як ймовірність виникнення події, що може завдати шкоди інформаційним ресурсам, тоді як загроза розглядається як конкретний чинник чи дія, здатна реалізувати цей ризик. Важливою особливістю є те, що ризики та загрози не існують у вакуумі: вони формуються під впливом технологічного середовища, правових норм, організаційних процесів та людського фактору. Саме тому визначення ризиків потребує комплексного підходу, який враховує як внутрішні, так і зовнішні умови функціонування організації.

Науковці, серед яких Р. Андерсон та Б. Шнайєр у праці, наголошують, що ризики в інформаційній сфері слід розглядати не лише як технічні проблеми, а як багатовимірні явища, що охоплюють організаційні та поведінкові аспекти. Андерсон підкреслює, що політика безпеки має бути адаптивною, здатною враховувати нові типи загроз, зокрема кібершпигунство чи атаки на критичну інфраструктуру [55]. Шнайєр, своєю чергою, акцентує увагу на тому, що безпека – це не лише технологія, а й поведінка, отже ризики часто виникають через недотримання правил співробітниками. Такий підхід дозволяє зрозуміти, що визначення ризиків має включати аналіз людського фактору, корпоративної культури та рівня обізнаності персоналу.

Загальні методологічні підходи до визначення ризиків у сфері інформаційної безпеки передбачають використання як кількісних, так і якісних інструментів [42]. Кількісні методи базуються на розрахунку ймовірності виникнення загрози та оцінці можливих фінансових втрат. Це дає змогу організації визначати пріоритети у сфері захисту та оптимально розподіляти ресурси. Якісні методи, які активно застосовуються у працях Г. Пелтьє, орієнтовані на експертні оцінки, моделювання сценаріїв та аналіз можливих наслідків. Вони дозволяють враховувати специфіку діяльності організації та особливості її інформаційного середовища. Поєднання цих підходів забезпечує більш точне та комплексне визначення ризиків, що є основою для ефективного управління ними.

Важливим аспектом є також інтеграція процесу визначення ризиків у загальну стратегію організації. Як зазначає Б. Дхіллон у дослідженні «Information Security Management», ризики повинні розглядатися у контексті бізнес-цілей та стратегічних пріоритетів [28]. Це означає, що оцінка загроз має бути спрямована не лише на технічний захист, а й на забезпечення стійкості бізнес-процесів, збереження репутації та конкурентоспроможності організації.

Внутрішні загрози інформаційної безпеки організації (рис.1.3) становлять одну з найбільш небезпечних категорій ризиків, адже вони походять від осіб, які мають легальний доступ до інформаційних ресурсів. Основними групами таких

загроз є халатність та помилки персоналу, недобросовісні дії співробітників, маніпульовані працівники, нелояльні чи скривджені співробітники, впроваджені особи та технічна недбалість [9]. Халатність проявляється у випадковому видаленні даних, використанні слабких паролів, ігноруванні процедур резервного копіювання чи недотриманні правил доступу. Ці дії не завжди мають навмисний характер, проте їхні наслідки можуть бути критичними для організації. Недобросовісні дії співробітників, навпаки, мають умисний характер і включають розголошення конфіденційної інформації, продаж даних конкурентам або саботаж роботи систем.

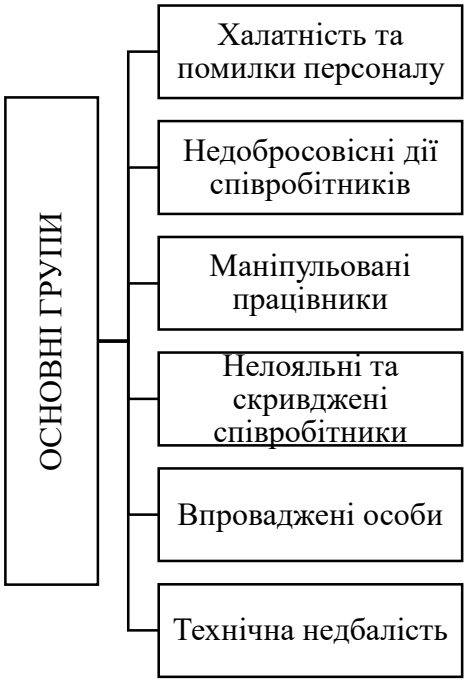


Рис.1.3. Внутрішні загрози інформаційної безпеки організації

Окрему групу становлять маніпульовані працівники, яких сторонні особи змушують або переконують передати доступ до систем чи інформації. Це може відбуватися через соціальну інженерію, психологічний тиск або інші методи впливу. Нелояльні та скривджені співробітники також становлять серйозну загрозу, адже особисті конфлікти з керівництвом чи організацією можуть спонукати їх до використання доступу з метою нанесення шкоди [17]. Впроваджені особи – це працівники, які були спеціально найняті або завербовані для здійснення витоку чи модифікації даних, і їхня діяльність часто має прихований та довготривалий характер.

Не менш небезпечним є фактор технічної недбалості, що проявляється у відсутності контролю за використанням мобільних пристроїв, хмарних сервісів чи незахищених носіїв інформації. Такі дії створюють умови для несанкціонованого доступу та втрати даних. Усі зазначені групи внутрішніх загроз демонструють, що найбільша небезпека може походити не від зовнішніх атак, а від власних співробітників організації [20]. Саме тому політика інформаційної безпеки повинна враховувати ці ризики, передбачати механізми контролю, моніторингу та формування корпоративної культури безпеки, яка мінімізує як ненавмисні помилки, так і навмисні дії персоналу. Такий підхід дозволяє організації забезпечити цілісність, конфіденційність та доступність своїх інформаційних ресурсів навіть у найскладніших умовах.

Зовнішні загрози інформаційної безпеки організації (рис.1.4) є багатогранним явищем, що охоплює як технологічні, так і соціально-політичні фактори [6]. Вони формуються поза межами організації та часто мають неконтрольований характер, що робить їх особливо небезпечними.

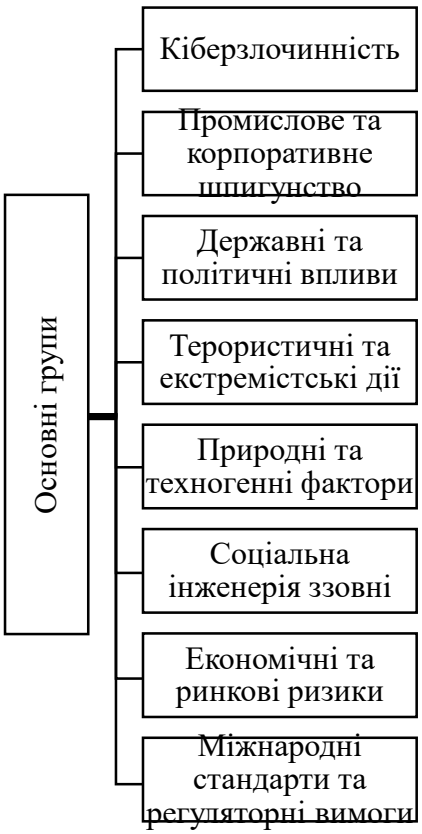


Рис.1.4. Класифікація зовнішніх загроз інформаційної безпеки організації

Однією з найпоширеніших груп зовнішніх загроз є кіберзлочинність, яка включає хакерські атаки, фішинг, поширення шкідливого програмного забезпечення та DDoS-атаки [10]. Ці дії спрямовані на отримання конфіденційної інформації, фінансових ресурсів або порушення роботи систем. Кіберзлочинність постійно еволюціонує, використовуючи нові методи проникнення та обходу захисних механізмів, що потребує від організацій постійного вдосконалення систем безпеки.

Не менш небезпечним є промислове та корпоративне шпигунство, яке полягає у незаконному отриманні комерційної інформації конкурентами чи сторонніми структурами [4]. Такі загрози можуть реалізовуватися через підкуп співробітників, використання спеціальних технічних засобів або кібератаки на корпоративні системи. Втрата комерційних таємниць здатна завдати значних фінансових збитків та підірвати конкурентоспроможність компанії. Окрему категорію становлять державні та політичні впливи, що проявляються у вигляді кібератак з боку спецслужб, інформаційних війн чи кампаній дезінформації. Такі загрози мають стратегічний характер і можуть бути спрямовані на дестабілізацію діяльності організації або навіть цілих секторів економіки.

Особливу небезпеку становлять терористичні та екстремістські дії, які можуть бути спрямовані на атаки проти критичної інфраструктури, паралізацію роботи систем чи створення паніки серед населення. Вони часто мають політичну або ідеологічну мотивацію і здатні спричинити масштабні наслідки. До зовнішніх загроз належать також природні та техногенні фактори – стихійні лиха, аварії обладнання, перебої в енергопостачанні [15]. Хоча вони не мають навмисного характеру, їхній вплив може бути не менш руйнівним, адже створює умови для втрати даних та порушення роботи інформаційних систем.

Важливим різновидом є соціальна інженерія ззовні, коли сторонні особи маніпулюють співробітниками організації через телефонні дзвінки, електронні листи чи інші методи психологічного впливу [60]. Це дозволяє отримати доступ до конфіденційної інформації без застосування складних технічних засобів. Додатковим чинником виступають економічні та ринкові ризики, такі як

коливання валют чи фінансові кризи, що можуть впливати на стабільність роботи інформаційних систем та інвестиційні можливості організації. Нарешті, значну роль відіграють міжнародні стандарти та регуляторні вимоги. Невідповідність глобальним нормам може призвести до санкцій, обмежень у співпраці та втрати довіри з боку партнерів.

Технологічні зміни та інновації у сфері інформаційної безпеки створюють не лише нові можливості, а й нові ризики. Кожна організація, яка впроваджує сучасні цифрові рішення, стикається з проблемою їхньої адаптації до існуючої інфраструктури та забезпечення належного рівня захисту [61]. Інноваційні технології, такі як хмарні сервіси, штучний інтелект чи блокчейн, відкривають нові горизонти для бізнесу, але водночас стають джерелом потенційних загроз.

Наприклад, використання хмарних платформ потребує чіткої регламентації доступу та контролю за збереженням даних, адже їхня вразливість може призвести до масштабних витоків інформації. Штучний інтелект, який активно застосовується для автоматизації процесів, може бути використаний і зловмисниками для створення складних атак, що важко виявити традиційними методами. Тому, технологічні інновації створюють подвійний ефект: вони підвищують ефективність організації, але водночас збільшують спектр ризиків, які необхідно враховувати у політиці безпеки.

Класифікація ризиків та загроз має практичне значення для управління інформаційною безпекою, оскільки дозволяє систематизувати потенційні небезпеки та визначити пріоритети у їхньому подоланні [13]. Завдяки класифікації організація отримує можливість створити цілісну картину ризиків, розподілити ресурси відповідно до рівня небезпеки та розробити ефективні заходи реагування. Вона допомагає відокремити технологічні ризики від соціальних чи організаційних, що дає змогу застосовувати різні інструменти управління.

Наприклад, для технологічних загроз доцільно використовувати сучасні технічні рішення – системи моніторингу, резервне копіювання, багаторівневу автентифікацію. Для соціальних ризиків ефективними є навчання персоналу,

формування корпоративної культури безпеки та регулярні інструктажі. Організаційні ризики можна мінімізувати завдяки чіткому розподілу ролей, створенню внутрішніх регламентів та проведенню аудитів [30].

Практична цінність класифікації полягає також у можливості прогнозування та попередження інцидентів. Вона дозволяє організації не лише реагувати на вже реалізовані загрози, а й передбачати їхнє виникнення. Це особливо важливо в умовах швидких технологічних змін, коли нові ризики з'являються майже щодня [42]. Класифікація стає інструментом стратегічного управління, який інтегрує інформаційну безпеку у загальну систему розвитку організації. У результаті вона сприяє підвищенню стійкості бізнес-процесів, збереженню репутації та конкурентоспроможності.

Таким чином, класифікація ризиків та загроз у сфері інформаційної безпеки є необхідною умовою для ефективного управління захистом даних та стабільністю бізнес-процесів. Вона дозволяє системно враховувати як внутрішні, так і зовнішні чинники, включаючи технологічні зміни, соціальні та організаційні аспекти. Завдяки цьому організація отримує можливість не лише реагувати на інциденти, а й прогнозувати їх, формуючи комплексну стратегію безпеки та підвищуючи свою конкурентоспроможність.

## 1.3. Методологічні підходи до аналізу ризиків та управління загрозами

Методологічні підходи до аналізу ризиків та управління загрозами у сфері інформаційної безпеки формують основу для створення ефективної системи захисту даних та інформаційних ресурсів. Вони поєднують теоретичні концепції та практичні інструменти, що дозволяють організації своєчасно виявляти потенційні небезпеки, оцінювати їхній вплив та розробляти механізми реагування [31]. У сучасному науковому дискурсі аналіз ризиків розглядається як багатовимірний процес, що охоплює технологічні, організаційні, правові та соціальні аспекти. Саме методологія визначає, які методи будуть застосовані – кількісні чи якісні – та як результати інтегруватимуться у загальну стратегію

управління. Важливим є те, що підходи до аналізу ризиків не можуть бути статичними: вони мають враховувати динаміку розвитку технологій, появу нових типів загроз та зміну поведінкових моделей користувачів.

Якісний аналіз ризиків у сфері інформаційної безпеки організації базуються на використанні методів, що дозволяють оцінити потенційні загрози без складних математичних розрахунків, спираючись на досвід, експертні знання та практичні інструменти [42]. Одним із найпоширеніших методів якісного аналізу ризиків (рис.1.5) є метод експертних оцінок, який передбачає залучення фахівців для визначення ймовірності та наслідків реалізації загроз. Його перевага полягає у тому, що він базується на професійних знаннях та практичному досвіді експертів, які здатні врахувати специфіку діяльності організації, особливості її інформаційного середовища та можливі слабкі місця системи захисту. Експертні оцінки дозволяють отримати глибоке розуміння ризиків навіть у тих випадках, коли кількісні дані є обмеженими або недоступними.


Рис.1.5. Методи якісного аналізу ризиків у сфері інформаційної безпеки організації

Метод сценаріїв передбачає моделювання можливих подій та аналіз їхнього впливу на інформаційні ресурси. Організація створює кілька сценаріїв розвитку ситуацій – від оптимістичних до кризових. Це дозволяє підготуватися до різних варіантів та розробити плани реагування [12]. Метод допомагає зрозуміти, які загрози є найбільш критичними та які наслідки вони можуть спричинити. Його застосування підвищує готовність організації до непередбачуваних обставин.

Метод мозкового штурму використовується для колективного генерування ідей щодо потенційних ризиків та шляхів їх мінімізації. У процесі беруть участь співробітники з різних підрозділів, що забезпечує різноманітність поглядів. Метод сприяє пошуку нестандартних рішень та формуванню комплексних підходів. Його перевага полягає у швидкому отриманні великої кількості ідей. Недоліком може бути хаотичність пропозицій, проте їхня систематизація дає цінний результат.

Метод Делфі базується на багатоетапному опитуванні експертів із метою досягнення узгодженої думки. Кожен експерт надає незалежну оцінку, яка узагальнюється та аналізується [13]. Після кількох раундів формується спільна позиція щодо ризиків. Метод дозволяє уникнути впливу авторитетів чи групового тиску. Його результатом є більш об’єктивна та збалансована оцінка загроз.

SWOT-аналіз застосовується для оцінки сильних і слабких сторін системи безпеки, а також можливостей і загроз зовнішнього середовища. Він допомагає визначити стратегічні пріоритети організації. SWOT-аналіз дозволяє поєднати внутрішні та зовнішні фактори у єдиній структурі. Це сприяє формуванню плану дій, спрямованого на посилення сильних сторін та мінімізацію слабких. Метод є універсальним і широко використовується у стратегічному плануванні.

Аналіз витрат і вигод (Cost-Benefit Analysis) співставляє можливі втрати від реалізації ризику з витратами на його попередження. Він дозволяє приймати економічно обґрунтовані рішення. Організація може визначити, які заходи є доцільними з точки зору фінансів. Метод допомагає оптимально розподіляти ресурси [42]. Його застосування забезпечує баланс між безпекою та економічною ефективністю.

Метод порівняльних таблиць передбачає зіставлення різних ризиків за критеріями ймовірності та впливу. Це дозволяє визначити пріоритетність загроз. Метод є простим у застосуванні та зрозумілим для керівництва [3]. Він допомагає концентрувати зусилля на найбільш небезпечних ризиках. У результаті організація отримує чітку картину для прийняття рішень.

Метод інтерв'ю та анкетування (табл.1.2) забезпечує збір інформації від співробітників щодо потенційних проблем у сфері безпеки. Він дозволяє врахувати думку персоналу, який безпосередньо працює з інформаційними системами. Інтерв'ю та анкети допомагають виявити слабкі місця, які можуть залишатися непоміченими керівництвом. Метод сприяє формуванню культури безпеки в організації. Його результатом є практичні дані для подальшого аналізу.

Аналіз історичних даних базується на використанні попереднього досвіду організації для прогнозування майбутніх ризиків. Він дозволяє враховувати вже реалізовані загрози та їхні наслідки. Аналіз історії інцидентів допомагає уникати повторення помилок [42]. Метод є ефективним для організацій із багатим досвідом роботи. Його застосування підвищує точність прогнозування ризиків.

Метод контрольних списків (Checklists) передбачає перевірку відповідності системи безпеки встановленим стандартам та вимогам. Контрольні списки забезпечують системність та повноту аналізу. Вони дозволяють швидко виявити недоліки та прогалини. Метод є простим у застосуванні та зрозумілим для всіх рівнів персоналу. Його використання сприяє підвищенню дисципліни та відповідальності у сфері безпеки.

Кількісний аналіз ризиків у сфері інформаційної безпеки є важливим інструментом для точного прогнозування можливих загроз та визначення їхнього впливу на діяльність організації. Він дозволяє отримати числові показники, які стають основою для прийняття обґрунтованих управлінських рішень [31]. Серед найбільш поширених і ключових методів кількісного аналізу ризиків у сфері інформаційної безпеки організації виділяють ті, які представлені на рис.1.6.

Першим є метод очікуваних втрат, який полягає у визначенні середнього значення можливих фінансових втрат з урахуванням ймовірності реалізації загрози. Цей метод дозволяє організації оцінити потенційні збитки та визначити, чи варто інвестувати у додаткові заходи безпеки [3]. Він є простим у застосуванні та зрозумілим для керівництва, адже результати виражаються у конкретних цифрах.

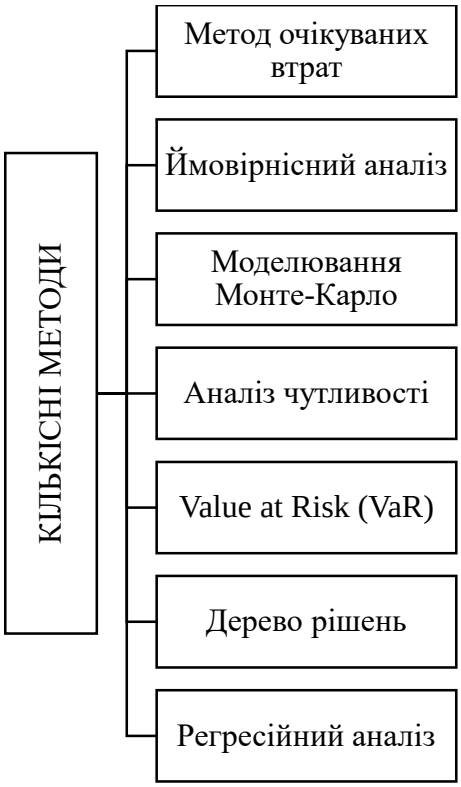


Рис.1.6. Методи кількісного аналізу ризиків у сфері інформаційної безпеки організації

Другим методом кількісного аналізу ризиків у сфері інформаційної безпеки організації виступає ймовірнісний аналіз, що базується на використанні статистичних даних та математичних моделей для оцінки ймовірності виникнення ризику. Цей метод дозволяє враховувати історичні дані та робити прогнози щодо майбутніх загроз. Його перевага полягає у можливості застосування до різних типів ризиків, від технічних до організаційних.

Третім методом є моделювання Монте-Карло, яке передбачає створення великої кількості сценаріїв для прогнозування розподілу можливих результатів. Завдяки цьому методу можна оцінити широкий спектр варіантів розвитку подій та визначити найбільш ймовірні наслідки [19]. Він особливо корисний у складних системах, де взаємодіють численні фактори.

Четвертий метод кількісного аналізу ризиків у сфері інформаційної безпеки організації – аналіз чутливості, який досліджує вплив зміни окремих параметрів на рівень ризику та кінцеві результати. Це дозволяє зрозуміти, які

фактори є найбільш критичними для безпеки організації. Метод допомагає визначити пріоритети у захисті та оптимізувати використання ресурсів.

П’ятим є – метод оцінки максимально можливих фінансових втрат у визначений період часу з певним рівнем довіри. Він широко застосовується у фінансовій сфері, але може бути корисним і для інформаційної безпеки. VaR дозволяє організації оцінити ризики у грошовому вимірі та приймати стратегічні рішення щодо їхнього управління [12].

Шостий метод – дерево рішень, що передбачає побудову дерева варіантів розвитку подій із розрахунком ймовірностей та очікуваних результатів. Це дає змогу візуалізувати можливі сценарії та оцінити їхні наслідки. Метод є ефективним для прийняття рішень у ситуаціях невизначеності.

Сьомим  методом кількісного аналізу ризиків у сфері інформаційної безпеки організації виступає регресійний аналіз, який використовує статистичні залежності для прогнозування ризиків на основі історичних даних [49]. Він дозволяє виявити закономірності та тенденції, що впливають на рівень ризику. Регресійний аналіз є потужним інструментом для довгострокового планування та прогнозування.

Управління інформаційною безпекою неможливе без використання міжнародних методологій, які забезпечують системність, стандартизацію та узгодженість процесів. Найбільш поширеними є ISO/IEC, NIST та COBIT, адже вони пропонують комплексні підходи до оцінки ризиків, розробки політик безпеки та інтеграції захисних заходів у бізнес-процеси [47; 48]. Використання цих методологій дозволяє організаціям не лише відповідати міжнародним вимогам, але й підвищувати рівень довіри з боку партнерів та клієнтів.

Наведена нижче табл.1.3 узагальнює ключові характеристики та приклади застосування зазначених методологій у практиці управління загрозами.

Аналіз наведеної табл.1.3 показує, що міжнародні методології ISO/IEC, NIST та COBIT забезпечують комплексний підхід до управління інформаційною безпекою в організації. Вони поєднують стандартизацію процесів, оцінку ризиків та інтеграцію безпеки у бізнес-процеси.

Таблиця 1.3

Використання міжнародних методологій управління інформаційною безпекою в організації

| № | Методологія / Стандарт | Характеристика | Приклад застосування |
|---|---|---|---|
| 1 | ISO/IEC 27001 | Міжнародний стандарт управління інформаційною безпекою, що визначає вимоги до створення, впровадження та підтримки системи менеджменту безпеки. | Впровадження політики безпеки та регулярний аудит відповідності вимогам стандарту. |
| 2 | ISO/IEC 27005 | Стандарт, що спеціалізується на управлінні ризиками інформаційної безпеки, включає методи ідентифікації, оцінки та обробки ризиків. | Використання для побудови процесу оцінки ризиків у корпоративній IT-інфраструктурі. |
| 3 | NIST Cybersecurity Framework (CSF) | Методологія, розроблена Національним інститутом стандартів і технологій США, яка включає п’ять функцій: ідентифікація, захист, виявлення, реагування та відновлення. | Використання для побудови комплексної стратегії кіберзахисту в державних і приватних організаціях. |
| 4 | NIST SP 800-30 | Документ, що описує методи кількісного та якісного аналізу ризиків у сфері інформаційної безпеки. | Застосування для оцінки ймовірності реалізації загроз та визначення рівня ризику. |
| 5 | COBIT (Control Objectives for Information and | Методологія управління IT-процесами та інформаційними ресурсами, яка поєднує контрольні | Використання для інтеграції управління ризиками у загальну |
|  | Related Technologies) | цілі, процеси та показники ефективності. | систему корпоративного управління. |
| 6 | COBIT 2019 | Оновлена версія методології, що враховує сучасні виклики цифрової трансформації та кіберзагроз. | Використання для побудови зрілої системи управління IT та інформаційною безпекою. |

ISO/IEC орієнтовані на створення системи менеджменту безпеки та управління ризиками, тоді як NIST пропонує практичні рамки для ідентифікації, захисту, реагування та відновлення після інцидентів [31]. COBIT, у свою чергу, зосереджується на управлінні IT-процесами та контролі ефективності, що дозволяє інтегрувати безпеку у корпоративне управління [55]. Використання цих методологій підвищує зрілість системи безпеки та довіру до організації.

Таким чином, методологічні підходи до аналізу ризиків формують основу для побудови ефективної системи управління загрозами та забезпечення

інформаційної безпеки. Поєднання якісних і кількісних методів дозволяє організації отримати як експертні оцінки, так і точні числові показники для прийняття рішень. Використання міжнародних стандартів ISO/IEC, NIST та COBIT забезпечує системність, стандартизацію та інтеграцію безпеки у бізнес-процеси, що підвищує зрілість системи захисту та довіру до організації з боку партнерів і клієнтів.

**Висновки до розділу 1**

Отже, політика інформаційної безпеки є ключовим інструментом управління, що поєднує правові, організаційні та технологічні аспекти захисту даних. Вона визначає правила доступу, відповідальність користувачів та порядок реагування на інциденти, формуючи основу системного мислення у сфері безпеки. Її значення виходить за межі технічного регламенту, адже політика інтегрується у корпоративну стратегію, забезпечує узгодженість дій працівників та відповідність міжнародним стандартам. Вона створює культуру безпеки, підвищує відповідальність персоналу й сприяє стійкому розвитку організації в умовах сучасних викликів.

Класифікація ризиків та загроз у сфері інформаційної безпеки є фундаментом для ефективного управління захистом даних. Вона охоплює внутрішні та зовнішні чинники, включаючи технічні, організаційні й соціальні аспекти. Внутрішні загрози пов’язані з халатністю, недобросовісними діями чи маніпуляціями співробітників, тоді як зовнішні охоплюють кіберзлочинність, шпигунство, політичні впливи, тероризм та природні фактори. Класифікація дозволяє систематизувати небезпеки, визначати пріоритети та прогнозувати інциденти. Завдяки цьому організація формує комплексну стратегію безпеки, забезпечує стійкість бізнес-процесів і зберігає конкурентоспроможність у динамічному цифровому середовищі.

Методологічні підходи до аналізу ризиків та управління загрозами у сфері інформаційної безпеки забезпечують системність і комплексність захисту даних.

Вони поєднують якісні методи (експертні оцінки, сценарії, SWOT-аналіз, мозковий штурм) та кількісні інструменти (очікувані втрати, ймовірнісний аналіз, моделювання Монте-Карло, VaR, регресійний аналіз). Це дозволяє отримати як глибоке розуміння ризиків, так і точні числові показники для прийняття рішень. Використання міжнародних стандартів ISO/IEC, NIST та COBIT інтегрує безпеку у бізнес-процеси, підвищує зрілість системи та довіру партнерів, формуючи ефективну стратегію управління загрозами.

# Розділ 2 АНАЛІЗ СУЧАСНОГО СТАНУ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

## 2.1. Оцінка ефективності існуючих політик інформаційної безпеки в організаціях

Оцінка ефективності існуючих політик інформаційної безпеки в сучасних організаціях є одним із ключових напрямів управління ризиками та забезпечення стійкості бізнес-процесів [3]. У світі, де цифрові технології стали основою економіки, а дані – стратегічним ресурсом, політики безпеки визначають рівень довіри до компанії з боку клієнтів, партнерів та регуляторів. Вони не лише формують правила доступу та використання інформаційних ресурсів, а й забезпечують відповідність міжнародним стандартам, що є важливим фактором конкурентоспроможності.

Нижче ми розглянемо стратегії провідних світових та українських компаній, які демонструють різні моделі впровадження політик інформаційної безпеки. Це дозволить оцінити не лише відповідність міжнародним стандартам, але й практичну ефективність заходів у конкретних умовах.

Так, яскравим прикладом високої ефективності політик інформаційної безпеки є Microsoft, яка системно впроваджує політики інформаційної безпеки відповідно до міжнародних стандартів. Її стратегія базується на стандартизації, регулярному аудиті та інтеграції безпеки у всі бізнес-процеси. Компанія має чинну сертифікацію ISO/IEC 27001 для ключових сервісів – Azure, Office 365 та Dynamics 365 (табл.2.1) [47; 48]. Це підтверджує, що система управління інформаційною безпекою відповідає вимогам щодо оцінки ризиків, впровадження контрольних заходів та постійного вдосконалення.

Сертифікація ISO/IEC 27001 охоплює широкий спектр процесів: управління доступом, моніторинг, реагування на інциденти та забезпечення безперервності бізнесу. Важливо, що Microsoft отримала першу сертифікацію ще у 2011 р. й з того часу щорічно проходить незалежні аудити [48]. Це свідчить про

сталість та ефективність політик, адже компанія не лише відповідає вимогам стандарту, а й постійно вдосконалює свої механізми захисту.

Таблиця 2.1

Характеристика основних сервісів Microsoft

| Сервіс | Призначення | Ключові функції | Цільова аудиторія |
|---|---|---|---|
| Azure | Хмарна платформа для зберігання та обробки даних, розгортання додатків | Масштабовані дата-центри, резервування, автоматичне виявлення аномалій, інтеграція AI | Корпоративні клієнти, державні установи, розробники |
| Office 365 | Пакет офісних та комунікаційних сервісів | Багаторівнева автентифікація, контроль доступу, регулярні аудити, захист пошти | Бізнес-користувачі, освітні заклади, державні органи |
| Dynamics 365 | CRM та ERP-система для управління бізнес-процесами | Аналітика ризиків, інтеграція безпеки у бізнес-процеси, захист клієнтських даних | Компанії середнього та великого бізнесу |

Практична реалізація політик проявляється у багаторівневих системах захисту, інтегрованих у продукти Microsoft. У хмарній платформі Azure діє комплексний моніторинг, який включає автоматичне виявлення аномалій та реагування на інциденти. Використання сервісів Microsoft Defender for Cloud та Sentinel дозволяє організаціям отримувати аналітику в реальному часі та швидко реагувати на загрози [48]. Це означає, що політики компанії не є формальними документами, а реально працюють у практичному середовищі.

Ще одним важливим аспектом є прозорість. Microsoft публікує звіти про відповідність стандартам та надає клієнтам доступ до інформації про сертифікації через портал Microsoft Trust Center [47]. Це підвищує рівень довіри, адже користувачі можуть переконатися, що їхні дані захищені відповідно до міжнародних вимог.

Ефективність політик Microsoft підтверджується також довірою клієнтів. Компанія обслуговує тисячі державних і корпоративних організацій, які покладаються на її хмарні сервіси для зберігання критично важливих даних. Регулярні аудити, багаторівневі системи захисту та прозорість у комунікації з

клієнтами створюють комплексну модель безпеки, яка відповідає сучасним викликам.

Google застосовує масштабний підхід до інформаційної безпеки, орієнтований на захист мільярдів користувачів у всьому світі. Одним із ключових елементів політики компанії є сервіс Safe Browsing (табл.2.2), який охоплює понад 5 млрд. пристроїв. Ця технологія блокує доступ до небезпечних сайтів, що містять фішингові атаки або шкідливе програмне забезпечення. Масштаб її застосування свідчить про високу ефективність політики: мільйони користувачів щодня отримують захист від потенційних загроз [5].

Таблиця 2.2

Характеристика сервісу Safe Browsing

| Параметр | Характеристика |
|---|---|
| Сервіс | Safe Browsing |
| Рік запуску | 2007 |
| Призначення | Захист користувачів від небезпечних веб-ресурсів та шкідливого контенту |
| Ключові функції | Виявлення фішингових сайтів; блокування шкідливих програм; попередження про небезпечні завантаження; оновлення бази загроз у реальному часі |
| Цільова аудиторія | Індивідуальні користувачі; освітні заклади; корпоративні клієнти; розробники браузерів та додатків |
| Рівень захисту | Високий (оновлення бази кожні 30 хвилин) |
| Особливості | Інтеграція у Chrome, Firefox, Safari та Android-додатки |

Додатковим прикладом є система безпеки Gmail, яка автоматично блокує понад 99,9 % спаму, фішингових атак та шкідливих вкладень. За оцінками самої компанії, це еквівалентно блокуванню близько 10 мільйонів небажаних листів щохвилини [37]. Такий рівень захисту демонструє практичну результативність політики та її здатність адаптуватися до нових типів атак.

Google постійно вдосконалює свої інструменти, враховуючи зміни у поведінкових моделях користувачів та появу нових загроз. Safe Browsing інтегровано у браузери Chrome та Firefox, а також у мобільні додатки, що забезпечує багаторівневий захист незалежно від платформи [38]. Це свідчить про системність політики та її орієнтацію на масове застосування.

Ефективність політик Google оцінюється через кількість інцидентів, яких вдалося уникнути. Масштабна статистика показує, що завдяки Safe Browsing та іншим інструментам компанія щодня блокує мільйони спроб фішингових атак. Це підтверджує дієвість політики та її здатність забезпечувати реальний захист користувачів у глобальному масштабі.

IBM є глобальним лідером у сфері інформаційних технологій, який активно інтегрує NIST Cybersecurity Framework (CSF) у свої корпоративні процеси [40]. Ця методологія, що включає п’ять основних функцій (ідентифікацію, захист, виявлення, реагування та відновлення) дозволяє компанії створювати комплексну систему управління ризиками. У 2024 р. було представлено NIST CSF 2.0, яка додала нову функцію «Governance» (управління), підкреслюючи роль керівництва у забезпеченні кіберстійкості [49].

За даними звіту про впровадження CSF у 2025 році, 81 % фінансових установ США застосовують цей фреймворк, тоді як у сфері охорони здоров’я його використовують понад 68 % лікарень. У секторі енергетики рівень впровадження сягає 75 %, а у виробництві – близько 57 % середніх та великих підприємств. IBM активно працює з цими галузями, пропонуючи рішення на основі CSF для оцінки ризиків, побудови стратегій кіберзахисту та відповідності регуляторним вимогам.

Практична реалізація політик IBM проявляється у використанні продуктів, таких як QRadar для моніторингу та аналізу інцидентів, а також Guardium для захисту даних (табл.2.3). Ці інструменти інтегрують принципи CSF, забезпечуючи виявлення аномалій у реальному часі та швидке реагування на загрози [52]. Таким чином, політики IBM не є формальними документами, а реально працюють у практичному середовищі.

Ефективність підходу IBM підтверджується довірою клієнтів у різних секторах – від фінансових установ до урядових організацій. Використання CSF дозволяє компанії створювати адаптивні рішення, які враховують специфіку кожної галузі та забезпечують відповідність міжнародним вимогам.

Таблиця 2.3

Характеристика продуктів IBM для реалізації політик інформаційної безпеки

| Параметр | IBM QRadar | IBM Guardium |
|---|---|---|
| Рік запуску | 2011 | 2009 |
| Сервіс | QRadar | Guardium |
| Призначення | Моніторинг та аналіз інцидентів | Захист даних та управління доступом |
| Ключові функції | Виявлення загроз у реальному часі; кореляція подій; аналітика журналів; автоматизація реагування | Захист баз даних; моніторинг транзакцій; контроль доступу; виявлення аномалій |
| Цільова аудиторія | Великі корпорації, державні установи, фінансові організації | Банки, телекомунікаційні компанії, організації з критичною інфраструктурою |
| Рівень захисту | Високий (SIEM-рішення з інтеграцією AI) | Високий (захист критичних даних у реальному часі) |
| Особливості | Інтеграція з іншими продуктами IBM Security; масштабованість | Підтримка різних типів баз даних; відповідність міжнародним стандартам |
| Сертифікація/стандарти | Відповідність ISO/IEC 27001, SOC | Відповідність ISO/IEC 27001, GDPR |

Amazon Web Services є найбільшим постачальником хмарних сервісів у світі, який системно впроваджує міжнародні стандарти інформаційної безпеки. AWS має сертифікації ISO/IEC 27001:2022, 27017:2015 та 27018:2019, що підтверджують відповідність її системи управління інформаційною безпекою найвищим міжнародним вимогам [35].

Сертифікат ISO/IEC 27018:2019, який регулює захист персональних даних у хмарних середовищах, був виданий AWS у листопаді 2022 р. та чинний до листопада 2026 р. Аудити проводить незалежна компанія EY CertifyPoint, що забезпечує об’єктивність оцінки. AWS також має сертифікацію ISO/IEC 27001:2022, яка охоплює широкий спектр сервісів, включаючи Amazon EC2, S3, RDS та інші ключові платформи [30].

Ефективність політик AWS проявляється у масштабі їхнього застосування. У 2026 р. понад 200 основних сервісів AWS перебувають у сфері дії сертифікацій ISO, що охоплює більшість критично важливих інструментів для бізнесу. Це означає, що клієнти, які використовують AWS для зберігання та обробки даних, можуть бути впевнені у відповідності сервісів міжнародним стандартам.

Практична реалізація політик включає багаторівневий захист даних у дата-центрах AWS, які розташовані у понад 30 регіонах світу [30]. Компанія застосовує контроль доступу, криптографічні засоби захисту та системи моніторингу для забезпечення безперервності бізнесу. Регулярні аудити та оновлення сертифікацій підтверджують, що політики AWS не є статичними, а постійно вдосконалюються відповідно до нових викликів.

Deutsche Bank, один із найбільших фінансових інститутів Європи з активами понад 1,45 трлн. дол. США у 2025 р., приділяє особливу увагу перевірці стійкості своїх систем до кіберзагроз [33]. Для цього банк регулярно проводить penetration testing та red team-вправи, які моделюють реальні атаки з метою виявлення слабких місць у захисті.

За даними досліджень, організації з розвиненими програмами red teaming виявляють порушення на 74% швидше (середній час – 18 днів проти 69 днів у компаній без таких програм) та знижують середню вартість інцидентів на 38 % – з 4,5 млн. до 2,8 млн. дол. США [54]. Для Deutsche Bank це критично, адже фінансовий сектор є однією з найбільш атакованих галузей.

У рамках європейського проєкту TIBER-EU, який у Німеччині реалізується як TIBER-DE, банки проходять загальноєвропейські стандартизовані тести на кіберстійкість. Deutsche Bank бере участь у цих програмах, що дозволяє не лише перевіряти власні системи, але й отримувати взаємне визнання результатів у межах ЄС. Практичні результати red team-вправ показують, що такі тести в середньому виявляють 11,4 невідомих раніше вразливостей, з яких близько 3,7 мають критичний рівень. Це дозволяє банку своєчасно усувати загрози та зменшувати ризик витоку даних.

Cisco Systems, глобальний лідер у сфері мережевих технологій, інтегрує політики інформаційної безпеки через використання COBIT та NIST Cybersecurity Framework (CSF) [41]. Ці методології дозволяють компанії поєднувати управління ризиками з корпоративним управлінням, забезпечуючи системність і прозорість процесів.

COBIT 2019 визначає контрольні цілі, процеси та показники ефективності, що дозволяє Cisco інтегрувати управління ризиками у загальну систему корпоративного управління. У свою чергу, NIST CSF 2.0, оновлений у 2024 р., включає шість функцій: Govern, Identify, Protect, Detect, Respond, Recover [40]. Це забезпечує комплексний підхід до управління ризиками та адаптацію до нових загроз.

Практична реалізація політик Cisco проявляється у продуктах, таких як Cisco Secure Firewall Management Center, які інтегрують принципи NIST CSF для моніторингу та реагування на інциденти. Використання цих інструментів дозволяє компанії забезпечувати захист клієнтів у понад 100 країнах світу, де Cisco має присутність.

За даними ISACA, компанії, що впроваджують COBIT, демонструють підвищення ефективності управління ризиками на 30-40 %, завдяки стандартизованим процесам та чітким KPI [41]. Для Cisco це означає можливість не лише відповідати міжнародним вимогам, але й забезпечувати конкурентні переваги у сфері кіберзахисту.

Meta, відома раніше як Facebook, є однією з найбільших соціальних платформ світу, яка постійно перебуває під пильною увагою регуляторів у сфері захисту даних. У 2025 р. компанія була оштрафована на 263,5 млн. євро за порушення вимог GDPR у Європейському Союзі [56]. Цей штраф став одним із найбільших у сфері захисту персональних даних і підтвердив, що політики інформаційної безпеки Meta потребують постійного вдосконалення.

У відповідь на критику та регуляторні санкції компанія оголосила про масштабну програму інвестицій у сферу приватності та безпеки. У січні 2025 р. Meta повідомила про виділення 8 млрд. дол. США на розвиток технологій захисту даних, включаючи вдосконалення систем шифрування, інструментів контролю доступу та прозорості для користувачів. Це свідчить про прагнення компанії не лише відповідати вимогам регуляторів, але й підвищити рівень довіри з боку мільярдів користувачів.

Практична реалізація політик Meta включає регулярні GDPR-аудити, які проводяться незалежними органами. Компанія також впроваджує нові інструменти для користувачів, що дозволяють контролювати, які дані збираються та як вони використовуються. Наприклад, у 2025 р. було розширено функції «Privacy Checkup», які охопили понад 2,9 млрд. активних користувачів платформи [56].

Ефективність політик Meta оцінюється через кількість інцидентів та реакцію регуляторів. Хоча компанія зазнає значних штрафів, її масштабні інвестиції у сферу безпеки свідчать про прагнення змінити ситуацію. Важливим показником є також зниження кількості витоків даних після впровадження нових систем моніторингу у 2025 р.

Apple є однією з небагатьох технологічних корпорацій, яка системно інтегрує міжнародні стандарти інформаційної безпеки у свої сервіси. Компанія має чинні сертифікації ISO/IEC 27001 та ISO/IEC 27018, що охоплюють ключові продукти – iCloud, iMessage та FaceTime [29]. Це підтверджує відповідність системи управління інформаційною безпекою Apple міжнародним вимогам щодо захисту даних, управління ризиками та конфіденційності користувачів.

Сертифікація ISO/IEC 27001 охоплює процеси управління доступом, моніторингу, реагування на інциденти та безперервного вдосконалення системи. Apple отримала першу сертифікацію ще у 2015 р., а у 2022 р. пройшла повторний аудит, підтверджений незалежною компанією Coalfire Systems Inc [3]. Це означає, що політики компанії регулярно перевіряються та відповідають сучасним вимогам.

Особливу увагу Apple приділяє захисту персональних даних у хмарних сервісах. Сертифікація ISO/IEC 27018:2019, яка регулює обробку персональної інформації у хмарних середовищах, була підтверджена у 2022 р. й чинна до 2026 р. [58]. Це свідчить про те, що компанія дотримується міжнародних правил щодо конфіденційності та прозорості у використанні даних користувачів.

Практична реалізація політик Apple проявляється у багаторівневому захисті даних. Наприклад, у iMessage та FaceTime використовується наскрізне

шифрування, яке забезпечує, що повідомлення та дзвінки можуть бути прочитані лише відправником і отримувачем. У iCloud реалізовано багатофакторну автентифікацію, яка охоплює понад 1,5 млрд. активних пристроїв Apple у світі.

Ефективність політик підтверджується також довірою користувачів: за даними Apple, у 2025 р. понад 85 % користувачів iCloud активували двофакторну автентифікацію, що значно знизило кількість інцидентів, пов’язаних із несанкціонованим доступом [29]. Крім того, компанія щорічно публікує звіти про прозорість, у яких зазначає кількість запитів від урядових органів щодо доступу до даних – у 2024 р. таких запитів було близько 156 тис., і більшість із них були відхилені або обмежені відповідно до політик конфіденційності.

В нашій країні НБУ (Національний банк України) є ключовим регулятором фінансової системи країни, який у 2025 р. ухвалив Постанову №143, що встановлює нові вимоги до кіберзахисту фінансових установ [16]. Документ визначає стандарти управління інформаційною безпекою, включаючи обов’язкове проведення аудитів, впровадження систем моніторингу та реагування на інциденти.

Згідно з постановою, банки та інші фінансові установи повинні щорічно проходити аудит відповідності вимогам НБУ. У 2025 р. було перевірено понад 60 системно важливих фінансових установ, і близько 78 % із них отримали позитивні висновки щодо рівня кіберзахисту. Це свідчить про ефективність нових політик та їхню здатність підвищувати стійкість фінансової системи.

Постанова №143 також передбачає обов’язкове впровадження багаторівневих систем автентифікації та регулярне оновлення програмного забезпечення [16]. У результаті у 2025 р. кількість інцидентів, пов’язаних із несанкціонованим доступом до фінансових систем, знизилася на 32 % порівняно з 2024 р.

Практична реалізація політик НБУ включає створення Центру кіберзахисту фінансового сектору, який координує дії банків у разі масштабних атак. У 2025 р. цей центр обробив понад 1 200 повідомлень про кіберінциденти,

з яких близько 15 % були класифіковані як критичні. Це дозволило своєчасно реагувати на загрози та мінімізувати їхні наслідки.

Яскравим прикладом успішного впровадження стратегій інформаційної безпеки в Україні є компанія «Київстар», найбільший телекомунікаційний оператор країни, який обслуговує понад 22,4 млн. мобільних абонентів та понад 1,2 млн. користувачів фіксованого інтернету [43]. Після масштабної кібератаки у грудні 2022 р., що призвела до тимчасового відключення мобільного зв'язку та інтернету для мільйонів клієнтів, компанія здійснила глибоку трансформацію своєї системи кіберзахисту.

Одним із ключових напрямів стало значне збільшення інвестицій у безпекові технології. У партнерстві з міжнародним холдингом VEON «Київстар» оголосив про програму інвестицій у розмірі 1 млрд дол. США на 2023-2027 рр., частина яких спрямована на розвиток кіберзахисту та цифрових сервісів [44]. Це включає модернізацію дата-центрів, впровадження систем моніторингу та автоматизованого реагування на інциденти.

Компанія інтегрувала багаторівневу систему захисту, що охоплює системи виявлення аномалій у трафіку, захист від DDoS-атак, посилений контроль доступу до внутрішніх систем та регулярні penetration testing для перевірки стійкості. Важливим кроком стало створення Центру реагування на кіберінциденти, який працює цілодобово. У 2025 р. цей центр обробив понад 12 тис. повідомлень про потенційні загрози, з яких близько 7 % були класифіковані як критичні [43].

Стратегія «Київстару» також передбачає відповідність міжнародним стандартам – компанія орієнтується на ISO/IEC 27001 та рекомендації NIST Cybersecurity Framework [48], що дозволяє інтегрувати управління ризиками у корпоративні процеси. Важливим елементом є прозорість: «Київстар» регулярно публікує звіти про кіберінциденти та заходи реагування, що підвищує довіру клієнтів і партнерів.

Ще одна відома українська компанія «Нова пошта», яка, будучи найбільшим оператором експрес-доставки, змушена забезпечувати захист даних

мільйонів клієнтів та безперервність роботи навіть в умовах війни. Стратегія компанії у сфері інформаційної безпеки базується на поєднанні міжнародних стандартів, інвестицій у технології та практичних заходів реагування.

Першим ключовим елементом є інвестиції у кіберзахист. З 2022 р. «Нова пошта» спрямувала понад 1 млрд. грн. [45] на розвиток систем моніторингу та штучного інтелекту для виявлення загроз. У компанії створено диспетчерський центр 24/7, який використовує акустичні сенсори та AI-алгоритми для відстеження траєкторій ракет і дронів, а також для аналізу кіберризиків. Система поширює сповіщення через 350 аудіосистем та понад 170 зашифрованих каналів, що дозволяє оперативно реагувати на небезпеку як фізичну, так і інформаційну.

Другим важливим напрямом є відповідність міжнародним стандартам. «Нова пошта» інтегрує принципи ISO/IEC 27001 у свої процеси управління інформаційною безпекою [50], що охоплює управління доступом, моніторинг, реагування на інциденти та безперервне вдосконалення системи. Це дозволяє компанії забезпечувати захист даних клієнтів на рівні провідних світових практик.

Третім елементом є практична реалізація політик. Компанія впровадила багаторівневі системи автентифікації для клієнтів та співробітників, а також регулярні penetration testing, які дозволяють виявляти слабкі місця у внутрішніх системах. У 2025 р. кількість інцидентів, пов’язаних із несанкціонованим доступом до клієнтських даних, знизилася на 27 % порівняно з 2024 р. [45].

Четвертим аспектом є прозорість та довіра. «Нова пошта» регулярно звітує про заходи безпеки та співпрацює з міжнародними партнерами у сфері кіберзахисту. Це підвищує рівень довіри клієнтів і партнерів, адже компанія демонструє готовність не лише реагувати на загрози, але й попереджати їх.

Насамкінець доцільно узагальнити наведені приклади у вигляді порівняльної табл.2.4, яка систематизує стратегії та практичну реалізацію політик інформаційної безпеки провідних світових і українських організацій. Такий формат дозволяє чітко співставити їхні підходи, рівень ефективності та особливості застосування у різних секторах.

Таблиця 2.4

Оцінка ефективності стратегій інформаційної безпеки світових та українських організацій

| Компанія / організація | Основна стратегія | Практична реалізація | Сертифікації / стандарти | Рівень ефективності |
|---|---|---|---|---|
| Microsoft | Стандартизація, аудит, інтеграція безпеки | Azure, Office 365, Dynamics 365; Defender for Cloud; Sentinel | ISO/IEC 27001 | Високий |
| Google | Масовий захист користувачів | Safe Browsing; Gmail антиспам | GDPR відповідність | Високий |
| IBM | Інтеграція NIST CSF | QRadar, Guardium | ISO/IEC 27001, SOC, GDPR | Високий |
| AWS | Масштабна сертифікація | EC2, S3, RDS; багаторівневий захист дата-центрів | ISO/IEC 27001:2022, 27017, 27018 | Високий |
| Deutsche Bank | Перевірка стійкості | Penetration testing, red teaming, TIBER-EU | Європейські стандарти | Високий |
| Cisco | COBIT + NIST CSF | Cisco Secure Firewall Management Center | COBIT 2019, NIST CSF 2.0 | Високий |
| Meta | GDPR-аудити, інвестиції у приватність | Privacy Checkup, шифрування | GDPR | Середній |
| Apple | Інтеграція ISO | iCloud, iMessage, FaceTime | ISO/IEC 27001, ISO/IEC 27018 | Високий |
| ТОВ «Нова пошта» | Захист логістичних даних та клієнтських сервісів | Власні дата-центри, системи моніторингу, кіберзахист мобільних додатків | Відповідність українським стандартам, GDPR для міжнародних операцій | Середній-високий |
| ПрАТ «Київстар» | Захист телекомунікаційних мереж | Системи моніторингу трафіку, захист персональних даних, SOC-центр | ISO/IEC 27001, відповідність GDPR | Високий |

Таким чином, ефективність політик інформаційної безпеки у провідних світових та українських організаціях підтверджується їхньою практичною реалізацією. Microsoft, Google та IBM демонструють системність і сталість підходів завдяки сертифікаціям та інтеграції безпеки у бізнес-процеси. AWS, Deutsche Bank та Cisco забезпечують адаптивність і відповідність міжнародним стандартам через масштабні аудити та тестування. Українські приклади, такі як НБУ, «Нова пошта» та «Київстар», свідчать про поступове наближення до

глобальних практик, що підвищує рівень довіри та кіберстійкості у національному контексті.

## 2.2. Виявлення ключових ризиків та загроз у сучасному інформаційному середовищі

У сучасному інформаційному середовищі дедалі очевиднішим стає той факт, що цифрові технології, які забезпечують розвиток економіки та суспільства, водночас створюють нові вразливості. Масове використання хмарних платформ, інтеграція Інтернету речей у повсякденне життя та стрімке поширення штучного інтелекту формують середовище, де ризики мають системний характер і можуть охоплювати цілі галузі чи державні інститути [2]. Особливість цієї ситуації полягає в тому, що загрози вже не обмежуються окремими інцидентами – вони стають частиною глобальних процесів, які впливають на економічну стабільність, політичну довіру та навіть фізичну безпеку людей.

Саме тому аналіз ключових ризиків і загроз (рис.2.1) є необхідним етапом для формування ефективної політики інформаційної безпеки, яка здатна поєднувати технологічні рішення з управлінням людським фактором та правовим регулюванням. Нижче ми розглянемо більш детально основні загрози, що вже проявили себе у світовій практиці та мають безпосередній вплив на стабільність корпоративних і державних систем.

Кіберзлочинність та хакерські атаки сьогодні є однією з найсерйозніших загроз для корпоративних і державних систем. Їхня небезпека полягає не лише у фінансових збитках, а й у можливості паралізувати критичну інфраструктуру. У 2024 році гучним прикладом стала атака групи BlackCat (ALPHV) на компанію Change Healthcare у США. Це підприємство обробляє мільйони страхових транзакцій у сфері охорони здоров’я, і після зараження системи програмою-вимагачем робота була фактично зупинена. Пацієнти не могли отримати ліки, лікарні втратили доступ до даних, а компанія зазнала збитків у

понад 2,8 млрд. дол. США. Відомо, що зловмисникам було сплачено викуп у розмірі 22 млн. дол. США, що лише підтверджує масштаб проблеми [58].


Рис.2.1. Ключові ризики та загрози сучасного інформаційного середовища

Інший приклад – інцидент із платформою Snowflake у травні 2024 р., коли дані понад сотні клієнтів, включно з AT&T та Santander Bank, опинилися під загрозою [46]. Це показало, що навіть найбільші хмарні провайдери не є повністю захищеними.

У 2025 р. кількість атак зросла майже на половину порівняно з попереднім роком, а новою тенденцією стали «подвійні» та «потрійні» методи шантажу: викрадення даних, блокування систем і погроза їх публікації. Особливо небезпечними стали атаки на інтегровані бізнес-екосистеми, як у випадку з Salesforce, де група Scattered Spider використала соціальну інженерію та викрадення токенів доступу для проникнення у середовище клієнтів – від авіакомпаній до брендів роздрібної торгівлі [57]. Це доводить, що

кіберзлочинність сьогодні є не лише технічною проблемою, а й глобальним викликом для економіки та безпеки держав.

Якщо розглянути окремо український кіберпростір, то у 2024-2025 рр. було зафіксовано низку інцидентів, які підтверджують високий рівень загроз для українських державних і приватних структур [18]. Особливість ситуації полягає в тому, що атаки мають як деструктивний, так і шпигунський характер, а їхня мета – дестабілізація інфраструктури та отримання конфіденційних даних. Україна залишається однією з головних мішеней для ворожих хакерських угруповань, які використовують сучасні технології та соціальну інженерію для досягнення своїх цілей.

У травні 2025 р. було здійснено масштабну атаку на українських інтернет-провайдерів. Під удар потрапили вісім компаній, серед яких Interlink, ActiveNet та SvitNet [19]. Хакери намагалися замаскувати свої дії під «боротьбу з шахрайством», проте CERT-UA класифікував інцидент як кібертерористичну атаку. Наслідком стали перебої у роботі інтернет-послуг, що вплинуло на користувачів та бізнес, а також створило додаткове навантаження на державні служби кіберзахисту. Цей випадок показав, що навіть базова інфраструктура, яка забезпечує доступ до мережі, може стати об’єктом цілеспрямованих атак.

Ще одним прикладом є кампанія кібершпигунства проти Сил оборони України, яку проводила група UAC-0010 (Gamaredon) [19]. У 2025 р. вона розсилала сотні тисяч фішингових листів із шкідливими вкладеннями, використовуючи легітимні інструменти Windows та сервіси на кшталт Cloudflare Tunnels і Telegram для приховування своєї діяльності. Масштабність була настільки значною, що інфікуванню піддалися тисячі комп’ютерів одночасно. Зловмисники також поширювали шкідливий код через USB-накопичувачі та документи Word, що створювало додаткові канали зараження. Метою було отримання доступу до військових даних та порушення роботи оборонних структур.

Фішинг та соціальна інженерія залишаються найпоширенішим способом проникнення у системи, адже вони експлуатують людський фактор. У 2025 р.

компанія Coinbase стала жертвою атаки, коли зловмисники підкупили співробітників служби підтримки [57]. Це дозволило отримати доступ до конфіденційних даних клієнтів – імен, дат народження та часткових номерів соціального страхування. Такі дані стали основою для подальших таргетованих атак.

У Японії того ж року було викрито масштабну кампанію CoGUI phishing kit, яка протягом кількох місяців розіслала понад 580 млн. листів, що імітували повідомлення від Amazon чи PayPal. Мета була проста – викрасти паролі та платіжні дані користувачів. У Великій Британії група Scattered Spider атакувала рітейлерів Marks & Spencer та Harrods, видаючи себе за IT-персонал [60]. Співробітників змусили відключити багатофакторну автентифікацію, що відкрило шлях для запуску ransomware. Збитки лише Marks & Spencer оцінюються у понад 300 млн. фунтів. Новим викликом стало використання штучного інтелекту для створення реалістичних фішингових повідомлень, deepfake-дзвінків та чат-ботів, які імітують справжніх співробітників. Це робить атаки майже непомітними для традиційних систем захисту.

Ми вважаємо що, соціальна інженерія сьогодні є не менш небезпечною, ніж технічні атаки: вона дозволяє обійти навіть найскладніші системи захисту, використовуючи слабкість людської психології.

Витоки даних сьогодні перетворилися на одну з найпоширеніших проблем цифрової економіки. У 2025 р. аналітична платформа Mixpanel допустила витік інформації про поведінку користувачів у тисячах застосунків, що викликало хвилю недовіри через непрозору комунікацію після інциденту. Ще більш масштабним став випадок із освітнім гігантом PowerSchool, який втратив дані понад 60 млн. учнів і вчителів [14], включно з медичними записами та інформацією про спеціальні освітні потреби. У сфері медицини прикладом є Blue Shield of California [23], яка роками передавала дані пацієнтів Google через неправильно налаштовані трекери, що стало предметом розслідувань.

В Україні у квітні 2025 р. стався масштабний витік, коли у відкритий доступ потрапили понад 10 млн. записів із конфіденційною інформацією: імена,

телефони, email-адреси, паролі та навіть копії документів [8]. Це спричинило хвилю шахрайських дзвінків, фішингових листів та спроб доступу до банківських акаунтів. Ще один резонансний випадок – атака на державні реєстри України у грудні 2024 р., коли хакери заявили про завантаження баз із понад мільярдом рядків даних, включно з біометрією та реєстраціями бізнесу [23].

Ці приклади доводять, що витоки даних стосуються не лише комерційних компаній, а й державних систем, і можуть мати наслідки для національної безпеки.

Інсайдерські загрози походять від співробітників або партнерів, які мають легальний доступ до систем, і часто залишаються непоміченими тривалий час. За даними IBM, середній інсайдерський інцидент залишається невиявленим 194 дні, а його усунення займає понад 260 днів, при цьому середні збитки сягають 4,92 млн. дол. США [20].

У липні 2025 р. Taiwan Semiconductor Manufacturing Company (TSMC) [9] звільнила двох інженерів, яких звинуватили у крадіжці технологій виробництва 2-нанометрових чипів. Це стало прецедентом у сфері захисту комерційної таємниці та показало, що інсайдери можуть становити стратегічну загрозу. Інший приклад – позов компанії Rippling проти Deel у березні 2025 р. [17] менеджера з комплаєнсу звинуватили у викраденні списків клієнтів та даних про персонал через Slack і Google Drive.

Відомий випадок із Tesla у 2025 р. став показовим прикладом інсайдерської загрози [9], яка може мати стратегічні наслідки для бізнесу. Колишні співробітники компанії передавали іноземним ЗМІ конфіденційну інформацію про клієнтів, включно з особистими даними, деталями замовлень та внутрішніми документами. Це поставило під сумнів здатність Tesla гарантувати захист приватності своїх користувачів і викликало хвилю критики з боку регуляторів та громадськості.

Особливість цього інциденту полягала в тому, що він не був результатом зовнішньої атаки чи технічної вразливості, а виник через дії людей, які мали легальний доступ до систем. Інсайдери використали своє службове становище

для отримання та поширення даних, що підкреслює слабкість будь-якої організації перед людським фактором. Для Tesla це стало серйозним репутаційним ударом, адже компанія позиціонує себе як інноваційного лідера у сфері електромобілів і цифрових технологій, де довіра клієнтів є критично важливою.

Розголошення даних призвело до розслідувань у США та Європі, а також до посилення вимог щодо внутрішнього контролю доступу. Tesla була змушена переглянути політику управління персоналом, запровадити додаткові механізми моніторингу та обмеження прав доступу, а також інвестувати у програми підвищення культури інформаційної безпеки серед співробітників.

Ці приклади доводять, що інсайдерські загрози можуть бути як навмисними, так і ненавмисними, але їхній вплив на бізнес є критичним. Саме тому компанії повинні впроваджувати системи моніторингу, обмежувати права доступу та створювати культуру відповідальності серед персоналу.

Дезінформація та інформаційні війни стали однією з ключових загроз сучасного інформаційного середовища. Їхня особливість полягає у використанні цифрових платформ та соціальних мереж для масового поширення неправдивих даних, які здатні впливати на політичні процеси, суспільну думку та навіть результати виборів [26]. На відміну від традиційної пропаганди, сучасна дезінформація базується на технологіях штучного інтелекту, що дозволяють створювати реалістичні аудіо- та відеоматеріали (deepfake) [10], які важко відрізнити від справжніх. Це робить маніпуляції більш переконливими та небезпечними. Важливою рисою інформаційних війн є їхня системність: вони не обмежуються окремими кампаніями, а стають частиною довготривалої стратегії впливу на суспільство та державні інститути.

Реальні приклади підтверджують масштаб проблеми. У Румунії в грудні 2024 р. Конституційний суд анулював результати першого туру президентських виборів через доведене використання AI-генерованих відео та іноземного втручання. Це був перший випадок у сучасній європейській історії, коли вибори були офіційно скасовані через дезінформацію. Інший приклад – США, січень

2024 р., коли близько 25 000 виборців у Нью-Гемпширі отримали телефонні дзвінки із синтетичним голосом Джо Байдена [26], який закликав їх не голосувати на праймеріз. Це була класична кампанія зниження явки, реалізована за допомогою технології. Обидва випадки показують, що дезінформація вже не обмежується «фейковими новинами», а використовує інноваційні технології для прямого втручання у демократичні процеси.

Вразливості хмарних сервісів є іншою критичною проблемою сучасного цифрового середовища. Хмарні платформи стали основою для зберігання та обробки даних у бізнесі, державному секторі та повсякденному житті. Їхня особливість полягає у багатокористувацькому середовищі та централізованому управлінні, що створює ризики масових витоків у випадку помилок конфігурації або успішних атак. Хоча провайдери хмарних сервісів інвестують мільярди доларів у безпеку, людський фактор та складність систем залишають їх вразливими.

Прикладом є інцидент із Snowflake у травні 2024 р. [46], коли масштабний витік даних зачепив понад 100 клієнтів, включно з AT&T, Ticketmaster та Santander Bank. Хакери використали слабкі місця у конфігурації та доступах, що дозволило їм проникнути у середовище зберігання даних. Ще більш масштабною стала атака на AWS у 2024 р. [61], яка охопила понад 230 мільйонів хмарних середовищ. Зловмисники знайшли відкриті файли «.env» із конфіденційними ключами доступу, створювали нові IAM-ролі з адміністративними правами, запускали шкідливі Lambda-функції та ексфільтрували інформацію у власні S3-сховища. Ці приклади доводять, що навіть глобальні провайдери не є повністю захищеними від помилок конфігурації та атак на багатокористувацькі середовища.

Інтернет речей (IoT) став невід’ємною частиною сучасного життя, інтегруючись у побут, бізнес та державні системи. Проте особливість цієї технології полягає в тому, що більшість пристроїв мають слабкий рівень захисту [2]. Виробники часто орієнтуються на швидкий вихід продукту на ринок,

а не на його безпеку, що призводить до використання паролів за замовчуванням, відсутності регулярних оновлень та низького рівня шифрування.

У результаті навіть звичайні побутові пристрої (камери відеоспостереження, «розумні» холодильники чи медичні сенсори) можуть стати точкою входу для хакерів у корпоративні мережі. Це створює серйозні ризики як для приватних користувачів, так і для великих компаній та державних установ. Проблема ускладнюється тим, що кількість IoT-пристроїв стрімко зростає, а їхня безпека часто залишається на другому плані.

Реальні приклади підтверджують масштаб цієї проблеми. Атака Mirai, яка вперше була зафіксована ще у 2016 році, у 2024 р. знову активізувалася у нових модифікаціях [22]. Ботнет використовував слабкі паролі IoT-пристроїв, таких як камери та маршрутизатори, щоб створювати масштабні DDoS-атаки на інтернет-сервіси. Це довело, що навіть старі методи залишаються ефективними через недбалість користувачів та виробників, які не змінюють стандартні налаштування безпеки. Масштабність атаки була настільки значною, що вона вплинула на роботу великих онлайн-платформ, показавши, наскільки небезпечними можуть бути навіть побутові пристрої, якщо їх використовувати у злочинних цілях.

Ще більш тривожним є приклад із медичними IoT-пристроями у 2025 р. [22]. Дослідження показало, що інсулінові помпи та кардіостимулятори, підключені до мережі, можуть бути зламані через відсутність належного шифрування. Це створює не лише кіберризики, а й пряму загрозу життю пацієнтів, адже зловмисники можуть змінювати параметри роботи пристроїв. Уявімо ситуацію, коли хакер отримує контроль над кардіостимулятором – це може призвести до фатальних наслідків. Подібні випадки доводять, що проблема IoT виходить далеко за межі цифрової безпеки і стає питанням фізичної безпеки та охорони здоров’я.

Штучний інтелект у руках зловмисників став однією з найновіших і найнебезпечніших тенденцій у сфері кіберзагроз. Якщо раніше атаки вимагали значних технічних знань і ресурсів, то сьогодні AI значно знижує бар’єр входу у

кіберзлочинність [27]. Зловмисники можуть використовувати генеративні моделі для створення реалістичних текстів, аудіо та відео, що робить атаки більш переконливими та важко виявними. Особливість проблеми полягає у масштабуванні: штучний інтелект дозволяє автоматизувати процеси, які раніше займали багато часу, наприклад, написання тисяч фішингових листів або створення персоналізованих повідомлень для різних груп користувачів.

Крім того, AI активно застосовується для клонування голосів, створення deepfake-контенту та навіть розробки спеціалізованих «темних» моделей (Dark LLMs), які обходять етичні обмеження й генерують шкідливий код чи інструкції для атак. Це означає, що навіть недосвідчені злочинці можуть отримати доступ до інструментів високого рівня, що значно підвищує ризики для бізнесу, державних структур і громадян.

Реальні приклади підтверджують масштаб цієї проблеми. У США у 2024 році було зафіксовано випадки використання голосового клонування для шахрайських дзвінків [10]. Зловмисники імітували голоси керівників компаній, щоб переконати співробітників здійснити термінові фінансові перекази. У кількох випадках компанії втратили мільйони доларів, адже дзвінки звучали настільки переконливо, що працівники не запідозрили обману. Це доводить, що навіть традиційні методи соціальної інженерії стають значно ефективнішими завдяки AI.

Інший приклад – поява у 2025 р. спеціалізованих Dark LLMs у «даркнеті». Це мовні моделі, які не мають обмежень і здатні генерувати фішингові набори, сценарії шахрайських дзвінків та шкідливий код [27]. Такі інструменти продаються як готові «пакети атак», що дозволяє навіть малодосвідченим злочинцям запускати масштабні кампанії. Фактично, AI перетворився на «зброю», яка робить кіберзлочинність доступною для широкого кола осіб.

Отож, сучасне інформаційне середовище характеризується системними ризиками, які охоплюють як державні, так і корпоративні структури. Реальні приклади 2024-2025 рр. доводять, що загрози мають глобальний масштаб і можуть паралізувати критичну інфраструктуру, спричиняти витоки даних та

підривати довіру суспільства. Особливу небезпеку становить поєднання технічних атак із соціальною інженерією та використанням штучного інтелекту, що робить їх майже непомітними для традиційних систем захисту.

## 2.3. Практичні приклади та проблеми реалізації політик інформаційної безпеки

У сучасному цифровому середовищі інформаційна безпека є ключовим чинником стабільності бізнесу та державних структур. Проте на практиці політики безпеки часто залишаються формальними документами, які не реалізуються належним чином. Це призводить до серйозних наслідків: від фінансових втрат і репутаційних криз до загроз життю людей.

Організації нерідко віддають пріоритет комерційним цілям, залишаючи безпеку на другому плані [18]. Це створює умови для масштабних атак і витоків даних. Коли компанії не інвестують у сучасні технології захисту, вони фактично відкривають двері для зловмисників.

Недостатнє фінансування (рис.2.2) проявляється у відсутності регулярного аудиту, використанні застарілих систем та слабкому контролі доступу. У багатьох випадках керівництво вважає, що витрати на кіберзахист не є пріоритетними, особливо якщо компанія не має історії великих інцидентів. Проте саме така позиція створює ілюзію безпеки, яка руйнується після першої масштабної атаки [15].

Наслідки недофінансування можуть бути катастрофічними. Витрати на відновлення систем, компенсації клієнтам та виплати викупів часто перевищують потенційні інвестиції у безпеку. Крім того, компанії стикаються з репутаційними ризиками, адже клієнти втрачають довіру до організації, яка не змогла захистити їхні дані.


Рис.2.2. Основні проблеми реалізації політик інформаційної безпеки в організаціях

Навіть найкращі політики інформаційної безпеки залишаються неефективними, якщо працівники не готові їх дотримуватися. Людський фактор є одним із головних каналів проникнення для атак [21]. Опір персоналу часто проявляється у небажанні використовувати багатофакторну автентифікацію, регулярні оновлення паролів чи дотримання правил роботи з конфіденційними даними.

Низька цифрова грамотність працівників створює додаткові ризики. Співробітники можуть не розпізнати фішингові листи, відкрити шкідливі вкладення або передати конфіденційну інформацію стороннім особам. У багатьох випадках саме соціальна інженерія стає ключовим інструментом для зловмисників, адже вона дозволяє обійти навіть найскладніші технічні системи захисту.

Опір персоналу також проявляється у небажанні змінювати звичні робочі процеси. Працівники часто сприймають нові правила як перешкоду у роботі, що знижує ефективність політик [28]. Це створює ситуацію, коли навіть добре розроблені системи безпеки залишаються формальними, адже їх не дотримуються на практиці.

Нехтування інформаційною безпекою призводить до комплексних наслідків, представлених у табл.2.5.

Таблиця 2.5

Основні наслідки нехтування політикою інформаційної безпеки в організаціях

| Категорія наслідків | Суть проблеми | Потенційні приклади наслідків |
|---|---|---|
| Фінансові втрати | Витрати на відновлення систем, виплати викупів та компенсації клієнтам часто перевищують потенційні інвестиції у безпеку. | Мільярдні збитки компаній після атак програм-вимагачів; додаткові витрати на відновлення баз даних та інфраструктури. |
| Репутаційні ризики | Витоки даних чи успішні атаки підривають довіру клієнтів і партнерів, що може мати довготривалі наслідки для бізнесу. | Втрата клієнтів через недовіру; падіння вартості акцій; негативні публікації у ЗМІ. |
| Соціальні та політичні наслідки | У випадку державних структур атаки можуть впливати на національну безпеку, політичну стабільність та довіру громадян до інституцій. | Масові витоки даних із державних реєстрів; використання інформації для дезінформаційних кампаній; підрив довіри до виборчих процесів. |
| Загроза життю та здоров'ю | У сфері медицини чи критичної інфраструктури атаки можуть призвести до реальних фізичних наслідків для людей. | Блокування доступу до медичних карток; збої у роботі лікарень; маніпуляції з IoT-медичними пристроями (кардіостимулятори, інсулінові помпи). |

Реальні приклади лише підтверджують ці висновки. У 2024 р. атака на AWS показала, що відсутність належного фінансування моніторингу може призвести до масштабних витоків. У 2025 р. витік даних у PowerSchool довів, що недофінансування систем захисту має наслідки для мільйонів користувачів. Кампанія CoGUI phishing kit у Японії засвідчила, що низька цифрова грамотність працівників і користувачів відкриває шлях для масових крадіжок даних [57]. А

випадок із Tesla у 2025 р. показав, що відсутність культури інформаційної безпеки серед персоналу може призвести до серйозних репутаційних втрат.

Інформаційна безпека часто конфліктує з вимогами швидкості та гнучкості бізнесу. Компанії прагнуть забезпечити клієнтам максимально зручний доступ до сервісів, але це нерідко суперечить суворим правилам захисту. Наприклад, багатофакторна автентифікація може уповільнити процес входу, а шифрування даних – збільшити час обробки транзакцій.

Проблема інтеграції полягає у тому, що політики безпеки не завжди узгоджуються з бізнес-моделлю компанії. У великих корпораціях це може призводити до конфлікту між різними відділами, а у малих підприємствах – до відсутності ресурсів для масштабних змін. Крім того, міжнародні стандарти (ISO/IEC 27001, GDPR, NIST) вимагають адаптації [49], яка часто є дорогою та складною.

Наслідки такої ситуації очевидні: зниження ефективності роботи, затримки у транзакціях, відтік клієнтів через незручність користування сервісами. У результаті організації опиняються перед дилемою: або забезпечити максимальну безпеку, або зберегти швидкість і гнучкість бізнес-процесів.

Інша проблема полягає у тому, що політики інформаційної безпеки часто впроваджуються формально, без системних перевірок їхньої дієвості. Це створює ілюзію захищеності, яка руйнується після першої серйозної атаки.

Регулярний аудит дозволяє оцінити поточний стан безпеки, виявити вразливості та скоригувати політики відповідно до нових загроз. Проте багато компаній нехтують цим процесом, обмежуючись внутрішніми перевірками або взагалі не проводячи тестування. У результаті системи залишаються застарілими, а вразливості – невиявленими.

Відсутність аудиту призводить до того, що організації не готові до нових типів атак, зокрема до використання штучного інтелекту у фішингових кампаніях чи до атак через ланцюг постачання [27]. Це створює серйозні ризики як для бізнесу, так і для клієнтів.

Реальні кейси лише підтверджують ці проблеми. У 2024 р. British Airways зіткнулася з труднощами інтеграції нових політик безпеки у систему бронювання, що призвело до збоїв та скарг клієнтів. А у 2025 р. Uber мав проблеми з інтеграцією правил захисту даних у мобільний додаток, що викликало критику користувачів через складність автентифікації [58].

Щодо аудиту, у 2024 р. Zoom став об'єктом критики через «Zoom-bombing», коли сторонні користувачі проникали у конференції. Причиною була відсутність належного тестування нових функцій безпеки. А у 2025 р. Slack зазнав витоку внутрішніх повідомлень через слабкі системи доступу, які не перевірялися належним чином [35].

Зараз кіберзагрози змінюються надзвичайно швидко (табл.2.6). Якщо ще кілька років тому основними методами атак були класичний фішинг чи віруси, то сьогодні зловмисники активно застосовують штучний інтелект, deepfake-технології та багатоканальні методи шантажу [53]. Використання AI-генерованих фішингових повідомлень робить їх максимально правдоподібними, а deepfake-дзвінки дозволяють імітувати голоси керівників компаній, змушуючи співробітників виконувати шахрайські інструкції.

Ці нові методи атак поєднують технічні злами з інформаційними кампаніями, створюючи комбіновані загрози, які важко виявити традиційними інструментами. Багатоканальні атаки одночасно охоплюють електронну пошту, соціальні мережі та корпоративні системи, що робить їх особливо небезпечними. Організації часто не встигають адаптувати свої політики до таких нових форм атак, і це створює критичні вразливості.

Таблиця 2.6

Нові види кіберзагроз у сучасному цифровому середовищі

| № | Вид кіберзагрози | Характеристика | Потенційні наслідки |
|---|---|---|---|
| 1 | Deepfake-атаки | Використання штучного інтелекту для створення підроблених аудіо та відео | Шахрайство, маніпуляція керівниками, підрив довіри до комунікацій |

| | | | |
|---|---|---|---|
| 2 | AI-генерований фішинг | Автоматизовані листи, що імітують стиль реальних компаній | Масові крадіжки даних, складність виявлення атак |
| 3 | Багатоканальний шантаж | Одночасні атаки через пошту, соцмережі та корпоративні системи | Параліч бізнес-процесів, фінансові втрати, репутаційні кризи |
| 4 | Ransomware-атаки нового покоління | Використання програм-вимагачів із функціями шифрування та крадіжки даних | Втрата доступу до систем, витоки конфіденційної інформації, великі фінансові збитки |
| 5 | Атаки на критичну інфраструктуру | Зловмисники спрямовують атаки на енергетику, транспорт чи медичні системи | Збої у роботі державних служб, загроза життю та здоров'ю населення |
| 6 | Кіберзагрози через квантові обчислення | Використання квантових технологій для зламу сучасних алгоритмів шифрування | Компрометація криптографії, загроза фінансовим транзакціям та державним системам |

Як доказ вищенаведеній інформації, у 2025 р. було зафіксовано хвилю AI-фішингових атак, коли зловмисники використовували алгоритми машинного навчання для створення персоналізованих листів, що імітували стиль реальних компаній. Це значно ускладнило виявлення шахрайства. Інший випадок – використання deepfake-дзвінків для бізнес-шахрайств: злочинці імітували голоси керівників, щоб змусити співробітників переказати кошти на сторонні рахунки.

Хмарні технології та «розумні» пристрої стали невід'ємною частиною сучасного бізнесу, але вони створюють нові ризики. Централізоване зберігання даних у хмарі робить компанії залежними від сторонніх постачальників, а слабкий захист IoT-пристроїв відкриває шлях для атак на критичну інфраструктуру [61].

Основні проблеми полягають у відсутності прозорості у ланцюгах постачання хмарних сервісів, використанні застарілих або неправильно налаштованих конфігурацій, а також у слабкому захисті IoT-пристроїв, які часто не мають регулярних оновлень. Складність контролю за величезною кількістю підключених пристроїв робить традиційні методи безпеки малоефективними.

Відомі кейси доводять масштабність проблеми. У 2025 р. компанія PowerSchool втратила дані понад 60 млн. учнів і вчителів, включно з медичними записами, що показало вразливість централізованих освітніх платформ [59].

У сфері IoT також є показові випадки. У 2024 р. дослідники зафіксували атаки на медичні пристрої – інсулінові помпи та кардіостимулятори, які можна було віддалено перепрограмувати через слабкий захист. Це створює реальну загрозу життю та здоров'ю людей і доводить, що безпека IoT-середовищ має бути пріоритетом.

Непрозорість постачальників та відсутність єдиної культури інформаційної безпеки залишають організації вразливими навіть тоді, коли власні системи захищені [11].

Так, використання сторонніх сервісів і підрядників часто не супроводжується належним аудитом. Компанії покладаються на постачальників хмарних рішень, програмного забезпечення чи обладнання, але не мають повної інформації про їхні внутрішні процеси безпеки. Це відкриває шлях для атак через ланцюг постачання, коли зловмисники проникають у систему не напряму, а через менш захищеного партнера.

Глобалізація лише ускладнює ситуацію: ланцюги постачання охоплюють десятки країн, різні правові режими та стандарти. Відсутність прозорості робить неможливим повний контроль [2]. У результаті компанії можуть стати жертвами атак навіть тоді, коли їхні власні системи захищені належним чином.

Відомі приклади підтверджують масштабність проблеми. У 2024 р. вразливість Log4j (Log4Shell) знову стала предметом атак, адже бібліотека інтегрована у тисячі продуктів. Компанії, які використовували її без належного моніторингу, опинилися під загрозою масових витоків даних. А у 2025 р. було зафіксовано нові атаки на сервіс Codecov [58], коли шкідливий код інтегрували у легітимні оновлення програмного забезпечення. Це дозволило зловмисникам отримати доступ до конфігурацій і ключів клієнтів, які довіряли сервісу.

Інша проблема полягає у тому, що політики безпеки часто впроваджуються формально, без створення єдиної корпоративної культури. Працівники можуть сприймати правила як перешкоду у роботі, ігнорувати вимоги щодо паролів чи багатофакторної автентифікації. У результаті навіть сучасні системи захисту залишаються неефективними.

Єдина культура інформаційної безпеки передбачає, що всі співробітники (від керівництва до рядових працівників) усвідомлюють важливість захисту даних і дотримуються правил. Проте на практиці часто бракує навчання, мотивації та контролю [9]. Це створює ситуацію, коли людський фактор стає головним каналом проникнення для атак.

Сучасні кейси засвідчують проблеми, що виникають через відсутність єдиної культури безпеки. У 2024 р. в кількох європейських компаніях було зафіксовано випадки deepfake-шахрайств, коли співробітники виконували інструкції «керівників», імітованих за допомогою штучного інтелекту. Це стало можливим через відсутність культури перевірки автентичності комунікацій. А у 2025 р. дослідження ENISA показало, що брак навичок та людський фактор залишаються серед трьох головних кіберзагроз у Європі [2]. Працівники часто використовують застарілі системи та нехтують оновленнями, що створює критичні вразливості навіть у добре захищених організаціях.

Отож, інформаційна безпека залишається критичною сферою, де формальне впровадження політик без належного контролю створює серйозні ризики. Основними проблемами є недофінансування, людський фактор та складність інтеграції політик у бізнес-процеси. Практика доводить, що без системного аудиту й формування культури безпеки організації залишаються вразливими до сучасних кіберзагроз.

## Висновки до розділу 2

Отож, оцінка ефективності політик інформаційної безпеки демонструє, що провідні світові організації інтегрують міжнародні стандарти та практичні інструменти для забезпечення стійкості бізнес-процесів. Microsoft, Google, IBM, AWS, Cisco та Apple підтверджують дієвість своїх політик завдяки сертифікаціям ISO/IEC, NIST та COBIT, регулярним аудитам і багаторівневим системам захисту. Їхні стратегії поєднують прозорість, адаптивність та орієнтацію на клієнтів. Водночас приклади Deutsche Bank і Meta показують

важливість тестування та вдосконалення політик у відповідь на регуляторні вимоги. Загалом ефективність політик визначається їхньою здатністю інтегрувати безпеку у корпоративну культуру та глобальні стандарти.

Ключові ризики сучасного інформаційного середовища охоплюють кіберзлочинність, витоки даних, інсайдерські загрози, дезінформацію, вразливості хмарних сервісів, небезпеки Інтернету речей та використання штучного інтелекту зловмисниками. Масштабні атаки на критичну інфраструктуру, фінансові установи й державні системи доводять, що загрози мають глобальний характер і впливають на економічну стабільність та національну безпеку. Особливу небезпеку становить соціальна інженерія, яка експлуатує людський фактор. Виявлення цих ризиків дозволяє організаціям формувати комплексні політики безпеки, інтегрувати технологічні та організаційні заходи й підвищувати стійкість бізнес-процесів.

Практичні приклади реалізації політик інформаційної безпеки показують, що їхня ефективність часто обмежується формальним впровадженням без належного контролю. Основними проблемами є недофінансування, опір персоналу та низька цифрова грамотність, що відкриває шлях для соціальної інженерії та масштабних атак. Конфлікт між вимогами безпеки та швидкістю бізнес-процесів ускладнює інтеграцію політик, а відсутність регулярного аудиту створює ілюзію захищеності. Нові загрози, зокрема deepfake-атаки та AI-фішинг, доводять необхідність постійного оновлення систем. Лише формування єдиної культури безпеки та системний аудит можуть забезпечити реальний захист.

# Розділ 3 ПРОПОЗИЦІЇ ЩОДО ОПТИМІЗАЦІЇ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЙ НА ОСНОВІ АНАЛІЗУ РИЗИКІВ

## 3.1. Розробка рекомендацій щодо вдосконалення політик інформаційної безпеки

У сучасних умовах стрімкого розвитку цифрових технологій питання інформаційної безпеки набуває особливої актуальності для організацій різних сфер діяльності. Постійне зростання кількості кіберзагроз вимагає від керівництва організацій системного підходу до формування та вдосконалення політик захисту даних. Виявлені проблеми у функціонуванні існуючих політик свідчать про необхідність їх адаптації до нових викликів та інтеграції міжнародних стандартів. На рис. 3.1 відображено основні рекомендації щодо вдосконалення політик інформаційної безпеки організацій.

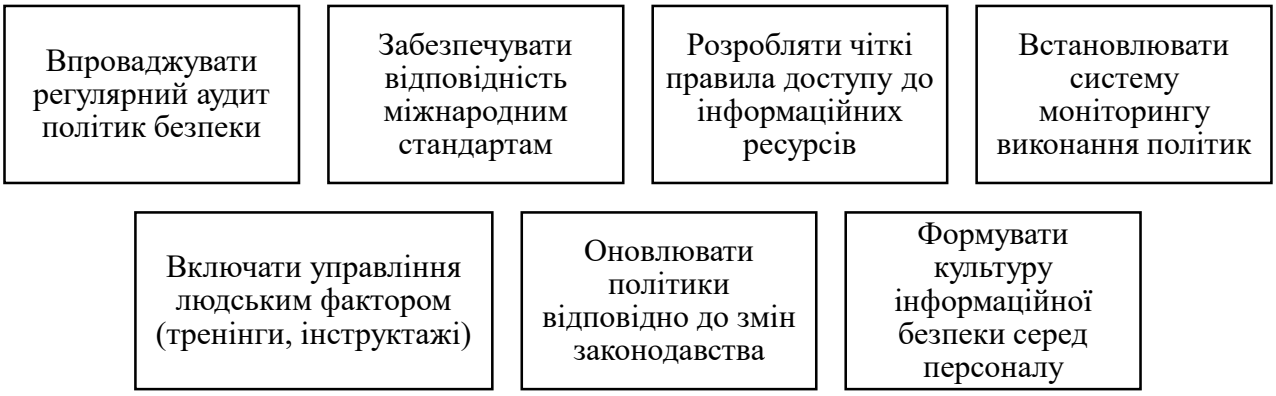


Рис.3.1. Ключові рекомендації щодо вдосконалення політик інформаційної безпеки організацій

Регулярний аудит політик інформаційної безпеки є ключовим інструментом для підтримання їхньої актуальності та ефективності. Він дозволяє систематично перевіряти відповідність внутрішніх правил сучасним стандартам, законодавчим вимогам та реальним загрозам [22]. Аудит має охоплювати як

технічні аспекти (захист даних, доступ до систем), так і організаційні (навчання персоналу, дотримання процедур). Важливо, щоб перевірки проводилися незалежними експертами або внутрішніми аудиторами, які мають достатній рівень компетенції. Результати аудиту повинні оформлюватися у вигляді звітів із конкретними рекомендаціями щодо усунення виявлених недоліків.

Регулярність таких перевірок (наприклад, щоквартально чи щорічно) забезпечує своєчасне реагування на нові виклики та мінімізує ризики інцидентів. Крім того, аудит сприяє формуванню культури прозорості та відповідальності в організації, адже кожен співробітник розуміє, що його дії можуть бути перевірені. У результаті організація отримує не лише підвищений рівень захисту, але й довіру клієнтів та партнерів, які бачать системний підхід до безпеки.

Відповідність міжнародним стандартам інформаційної безпеки є важливим фактором для підвищення конкурентоспроможності та довіри до організації. ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою, включаючи політики, процедури та контрольні механізми. NIST Cybersecurity Framework (CSF) пропонує гнучку модель оцінки ризиків і реагування на загрози [40]. Інтеграція цих стандартів у діяльність організації дозволяє створити структуровану систему захисту, яка враховує як технічні, так і організаційні аспекти. Важливо не лише формально задекларувати відповідність, а й реально впровадити практики, передбачені стандартами: управління доступом, резервне копіювання, реагування на інциденти, навчання персоналу.

Сертифікація за ISO/IEC 27001 може стати додатковою перевагою для бізнесу, адже підтверджує високий рівень захисту даних [47]. Відповідність міжнародним стандартам також полегшує співпрацю з іноземними партнерами та вихід на глобальні ринки. Таким чином, організація отримує не лише захист від загроз, але й стратегічні можливості для розвитку.

Одним із найважливіших елементів політики інформаційної безпеки є правила доступу до інформаційних ресурсів. Вони визначають, хто, коли і на яких умовах може отримати доступ до даних та систем. Чіткі правила

дозволяють мінімізувати ризики несанкціонованого використання інформації та інсайдерських загроз [20]. Для цього необхідно впровадити принцип мінімальних привілеїв: кожен співробітник отримує лише ті права, які потрібні для виконання його функцій. Важливо також передбачити процедури надання та відкликання доступу, особливо при зміні посад чи звільненні працівників. Технічна реалізація може включати багатофакторну автентифікацію, контроль паролів, використання систем управління ідентифікацією (IAM).

Крім того, правила доступу повинні бути чітко задокументовані та доведені до відома всіх співробітників. Регулярний перегляд і оновлення цих правил забезпечує їхню актуальність у контексті нових загроз. У результаті організація отримує контрольоване середовище, де доступ до критичних ресурсів здійснюється прозоро та безпечно.

Моніторинг виконання політик інформаційної безпеки є необхідним для забезпечення їхньої реальної ефективності. Навіть найкращі правила залишаються формальністю, якщо немає механізму контролю їх дотримання. Система моніторингу повинна включати автоматизовані інструменти, які відстежують дії користувачів, доступ до даних, спроби порушення політик. Це можуть бути SIEM-системи (табл.3.1), які збирають та аналізують журнали подій у режимі реального часу [52]. Важливо також передбачити механізми сповіщення про інциденти та швидке реагування на них. Моніторинг має охоплювати не лише технічні аспекти, а й організаційні: виконання процедур, проходження навчань, дотримання регламентів.

Регулярні звіти про результати моніторингу дозволяють керівництву оцінювати рівень безпеки та приймати обґрунтовані рішення [19]. Окрім цього, система моніторингу сприяє формуванню дисципліни серед співробітників, адже вони усвідомлюють, що їхні дії контролюються. У результаті організація отримує не лише захист від загроз, але й інструмент для постійного вдосконалення політик.

Людський фактор залишається одним із найслабших місць у системі інформаційної безпеки, адже навіть найсучасніші технології не здатні повністю

захистити організацію від помилок чи недбалості персоналу. Саме тому важливо включити управління людським фактором у політику безпеки. Це передбачає регулярні тренінги, інструктажі та практичні навчання, спрямовані на підвищення обізнаності співробітників щодо актуальних кіберзагроз [2]. Працівники повинні знати, як розпізнавати фішингові листи, уникати небезпечних посилань, правильно працювати з конфіденційними даними та дотримуватися правил доступу.

Таблиця 3.1

Характеристика основних SIEM-систем

| № | Система / Продукт | Основні функції | Переваги | Приклад використання |
|---|---|---|---|---|
| 1 | IBM QRadar | Збір та аналіз журналів подій, кореляція інцидентів | Висока масштабованість, інтеграція з іншими продуктами IBM | Використання у великих корпораціях для моніторингу мережевих атак |
| 2 | Splunk Enterprise Security | Аналіз великих обсягів даних, візуалізація загроз | Гнучкість налаштувань, потужна аналітика | Виявлення аномалій у фінансових транзакціях |
| 3 | ArcSight (Micro Focus) | Централізований збір логів, кореляція подій | Підтримка складних сценаріїв безпеки | Використання у державних установах для контролю доступу |
| 4 | LogRhythm | Моніторинг, управління інцидентами, автоматизація | Інтеграція з інструментами реагування | Захист критичної інфраструктури (енергетика, транспорт) |
| 5 | AlienVault (AT&T Cybersecurity) | SIEM + IDS/IPS, управління вразливостями | Комплексний підхід «все в одному» | Використання у середніх компаніях для швидкого впровадження |
| 6 | Microsoft Sentinel | Хмарна SIEM-платформа, інтеграція з Azure | Масштабованість, використання ШІ для аналізу | Захист корпоративних даних у хмарних середовищах |

Організаціям варто проводити моделювання інцидентів (табл.3.2), щоб персонал міг відпрацювати алгоритми реагування у реальних умовах. Управління людським фактором також включає створення системи мотивації та відповідальності: співробітники мають розуміти, що їхня поведінка

безпосередньо впливає на рівень захисту організації. Тому, тренінги та інструктажі стають не просто формальністю, а дієвим інструментом формування культури безпеки.

Таблиця 3.2

Моделювання інцидентів інформаційної безпеки

| № | Тип інциденту | Сценарій моделювання | Очікувані наслідки | Алгоритм реагування |
|---|---|---|---|---|
| 1 | Фішинг | Працівник отримує лист із шкідливим посиланням | Викрадення облікових даних, доступ до внутрішніх систем | Навчання персоналу, блокування домену, зміна паролів |
| 2 | Витік даних | Несанкціоноване копіювання файлів співробітником | Розголошення конфіденційної інформації | Виявлення через DLP-системи, дисциплінарні заходи |
| 3 | Атака на ланцюг постачання | Інсталяція зараженого оновлення ПЗ | Компрометація корпоративних систем | Перевірка джерел оновлень, ізоляція заражених вузлів |
| 4 | Ransomware | Шкідливе ПЗ блокує доступ до даних | Зупинка бізнес-процесів, фінансові втрати | Використання резервних копій, повідомлення CERT-UA |
| 5 | Інсайдерська загроза | Співробітник навмисно передає дані конкурентам | Репутаційні та фінансові втрати | Моніторинг дій користувачів, обмеження доступу, юридичні дії |

Законодавство у сфері інформаційної безпеки постійно змінюється, реагуючи на нові виклики та технологічні тенденції. Тому політики організації повинні регулярно оновлюватися відповідно до цих змін. Це стосується як національних нормативних актів, так і міжнародних регламентів, що визначають правила обробки та захисту даних [49]. Вчасне оновлення політик дозволяє уникнути юридичних ризиків, штрафів та репутаційних втрат. Організація повинна створити механізм моніторингу законодавчих змін, призначити відповідальних осіб та забезпечити їхню взаємодію з юридичним відділом.

Важливо проводити роз’яснювальну роботу серед персоналу, щоб співробітники розуміли нові вимоги та могли їх виконувати. Оновлення політик має бути не формальним, а практичним – із внесенням змін у процедури доступу,

обробки даних, реагування на інциденти. Це забезпечує відповідність діяльності організації правовим нормам і підвищує довіру клієнтів та партнерів.

Культура інформаційної безпеки – це система цінностей, норм і поведінкових моделей, яка визначає ставлення співробітників до захисту даних. Формування такої культури є стратегічним завданням, адже саме від щоденних дій персоналу залежить ефективність політик безпеки [17]. Для цього необхідно поєднувати навчання, мотивацію та контроль. Працівники повинні усвідомлювати, що інформаційна безпека – це не лише технічне питання, а й частина корпоративної етики.

Важливо створювати середовище, де дотримання правил безпеки сприймається як норма, а порушення – як загроза для всієї організації. Це можна досягти через регулярні комунікації, внутрішні кампанії, інтеграцію теми безпеки у корпоративні заходи [13]. Культура безпеки також передбачає відкритість: співробітники мають можливість повідомляти про інциденти без страху покарання. У результаті формується відповідальне ставлення до інформації, що знижує ризики та підвищує стійкість організації до загроз.

Отож, розробка рекомендацій щодо вдосконалення політик інформаційної безпеки організацій показала, що ефективний захист даних потребує комплексного підходу, який поєднує аудит, стандартизацію та управління доступом. Важливим є не лише створення правил, а й постійний моніторинг їх виконання та робота з людським фактором, що забезпечує реальну дієвість політик. У результаті організація отримує адаптивну систему безпеки, здатну реагувати на нові загрози та формувати довіру клієнтів і партнерів.

## 3.2. Використання сучасних цифрових інструментів для управління ризиками

Організації, що прагнуть підвищити ефективність управління ризиками в інформаційному просторі, мають орієнтуватися на впровадження сучасних цифрових інструментів у своїй діяльності. Такі рішення забезпечують не лише

захист даних, але й створюють основу для стабільності та прозорості бізнес-процесів. Особливе значення має інтеграція автоматизованих технологій, здатних оптимізувати контроль і своєчасно реагувати на потенційні проблеми. На рис. 3.2 відображено ключові рекомендації щодо використання сучасних цифрових інструментів для управління ризиками в інформаційному середовищі.


Рис.3.2. Ключові рекомендації щодо використання сучасних цифрових інструментів для управління ризиками в інформаційному просторі

Системи управління вразливостями є ключовим інструментом для своєчасного виявлення та усунення слабких місць у програмному забезпеченні та інфраструктурі організації. Вони дозволяють автоматично сканувати мережу, сервери та робочі станції, визначати відомі вразливості та формувати звіти з пріоритетами їх усунення [27]. Це забезпечує проактивний захист, адже організація може випереджати потенційні атаки, закриваючи критичні «дірки» ще до того, як ними скористаються зловмисники.

Важливо, щоб процес управління вразливостями був інтегрований у загальну політику безпеки та включав регулярні перевірки, оновлення баз даних та контроль виконання рекомендацій. Окрім цього, системи управління вразливостями допомагають відповідати міжнародним стандартам, які вимагають документованого процесу оцінки ризиків. У результаті організація отримує не лише технічний захист, але й стратегічну перевагу – можливість

демонструвати партнерам і клієнтам високий рівень зрілості у сфері кібербезпеки [53].

Багатофакторна автентифікація (MFA) є одним із найефективніших способів захисту доступу до інформаційних систем. Вона передбачає використання кількох рівнів перевірки особи: пароль, одноразовий код, біометричні дані чи апаратний токен. Це значно знижує ризик компрометації облікових записів, адже навіть у випадку викрадення пароля зловмисник не зможе отримати доступ без додаткового фактору. Інтеграція MFA повинна охоплювати всі критичні системи організації, включаючи корпоративну пошту, бази даних та хмарні сервіси.

Необхідно також забезпечити зручність для користувачів, щоб додаткові кроки автентифікації не перетворювалися на бар'єр у роботі [20]. Сучасні рішення дозволяють використовувати мобільні додатки, push-повідомлення чи біометрію, що робить процес швидким і безпечним. У результаті організація отримує значно вищий рівень захисту від фішингових атак, інсайдерських загроз та несанкціонованого доступу.

Інструменти Data Loss Prevention (DLP) призначені для контролю руху конфіденційної інформації та запобігання її несанкціонованому поширенню [7]. Вони дозволяють відстежувати, які дані копіюються, пересилаються чи завантажуються користувачами, і блокувати небезпечні дії. DLP-системи (табл.3.3) особливо актуальні для організацій, що працюють із персональними даними клієнтів, фінансовою інформацією чи комерційними секретами. Важливо, щоб політики DLP були налаштовані відповідно до специфіки бізнесу: наприклад, заборона пересилання файлів із певними ключовими словами або блокування копіювання даних на зовнішні носії.

Крім того, DLP-системи можуть інтегруватися з SIEM-рішеннями, що забезпечує комплексний контроль за інформаційними потоками [52]. Використання таких інструментів не лише знижує ризик витоків, але й допомагає організації відповідати вимогам законодавства щодо захисту персональних

даних. У результаті формується прозора система контролю, яка підвищує довіру клієнтів та партнерів.

Таблиця 3.3

Інструменти Data Loss Prevention (DLP)

| № | Інструмент | Основне призначення | Ключові функції | Цільова аудиторія |
|---|---|---|---|---|
| 1 | Symantec DLP | Захист конфіденційних даних у корпоративних системах | Контроль електронної пошти, файлів, веб-трафіку; політики відповідності | Великі корпорації, фінансові установи |
| 2 | McAfee Total Protection for DLP | Запобігання витокам даних через різні канали | Моніторинг USB-носіїв, хмарних сервісів, мобільних пристроїв | Бізнес середнього та великого масштабу |
| 3 | Digital Guardian DLP | Захист інтелектуальної власності та критичних даних | Контроль кінцевих точок, шифрування, аналітика поведінки | Виробничі компанії, R&D-центри |
| 4 | Forcepoint DLP | Комплексний контроль інформаційних потоків | Інтеграція з SIEM, аналіз контенту, адаптивні політики | Державні установи, освітні заклади |
| 5 | Trend Micro DLP | Захист даних у хмарних та локальних середовищах | Виявлення конфіденційної інформації, інтеграція з Office 365 | Компанії, що використовують хмарні сервіси |

Хмарні технології стали невід’ємною частиною сучасного бізнесу, проте їх використання потребує особливої уваги до питань безпеки [10]. Використання хмарних сервісів із сертифікованою безпекою (наприклад, відповідність ISO/IEC 27017, SOC 2 чи GDPR) гарантує, що дані організації зберігаються та обробляються відповідно до міжнародних стандартів. Такі сервіси забезпечують шифрування даних, багаторівневу автентифікацію, резервне копіювання та постійний моніторинг інцидентів.

Ключове значення має те, щоб організація ретельно обирала постачальника хмарних послуг, враховуючи його репутацію, сертифікацію та можливості інтеграції з внутрішніми системами. Варто передбачити політики розмежування доступу та контроль за діями користувачів у хмарному середовищі. Використання сертифікованих хмарних сервісів дозволяє не лише знизити

витрати на інфраструктуру, але й підвищити рівень захисту даних, що особливо важливо для організацій, які працюють із критичною інформацією. У результаті бізнес отримує гнучке та безпечне середовище для розвитку.

Автоматизовані системи резервного копіювання є одним із найважливіших інструментів для забезпечення безперервності бізнес-процесів та захисту критичних даних [22]. Вони дозволяють організації створювати копії інформації у визначені проміжки часу без участі користувачів, що мінімізує ризик людських помилок. Такі системи можуть працювати як у локальному середовищі, так і в хмарних сервісах, забезпечуючи багаторівневий захист. Необхідно налаштувати політику резервного копіювання так, щоб вона охоплювала всі ключові ресурси: бази даних, документи, електронну пошту та конфігурації систем.

Необхідно передбачити регулярне тестування відновлення даних, адже сам факт наявності копій не гарантує їхньої працездатності. Автоматизація процесу дозволяє зменшити витрати часу та ресурсів, а також забезпечує швидке відновлення після інцидентів, таких як атаки ransomware чи технічні збої. У результаті організація отримує стабільність роботи та впевненість у тому, що навіть у кризових ситуаціях вона зможе зберегти ключову інформацію.

Інструменти User Behavior Analytics (UBA) призначені для виявлення аномалій у діях співробітників та користувачів системи (табл.3.4). Вони аналізують звичні шаблони поведінки (час входу, використання ресурсів, обсяг переданих даних) і сигналізують про відхилення, які можуть свідчити про загрозу [3]. Наприклад, якщо працівник раптово починає завантажувати великі обсяги конфіденційної інформації або входить у систему в незвичний час, UBA-система може автоматично повідомити службу безпеки. Це дозволяє виявляти як зовнішні атаки, так і інсайдерські загрози.

Необхідно інтегрувати UBA з іншими інструментами, такими як SIEM чи DLP, щоб отримати комплексну картину ризиків. Використання UBA сприяє формуванню культури відповідальності серед персоналу, адже співробітники усвідомлюють, що їхні дії відстежуються [9]. У результаті організація отримує

потужний інструмент для раннього виявлення загроз, що значно знижує ймовірність серйозних інцидентів.

Таблиця 3.4

Інструменти User Behavior Analytics (UBA)

| № | Інструмент | Основне призначення | Ключові функції | Цільова аудиторія |
|---|---|---|---|---|
| 1 | Splunk UBA | Виявлення аномалій у поведінці користувачів | Машинне навчання, аналіз шаблонів доступу, інтеграція з SIEM | Великі корпорації, фінансові установи |
| 2 | Exabeam Advanced Analytics | Автоматизація аналізу поведінки | Виявлення інсайдерських загроз, побудова профілів користувачів | Бізнес середнього та великого масштабу |
| 3 | Securonix UBA | Захист від складних атак | Кореляція подій, поведінковий аналіз, прогнозування ризиків | Державні установи, критична інфраструктура |
| 4 | Varonis UBA | Контроль доступу до даних | Моніторинг файлових систем, аналіз прав доступу, виявлення підозрілих дій | Компанії, що працюють із конфіденційними даними |
| 5 | Microsoft Defender for Identity (UBA) | Виявлення аномалій у корпоративних мережах | Аналіз дій користувачів у Active Directory, виявлення компрометації | Організації, що використовують Microsoft 365 та Azure |

Штучний інтелект (ШІ) відкриває нові можливості у сфері інформаційної безпеки, особливо для прогнозування потенційних загроз. Використання алгоритмів машинного навчання дозволяє аналізувати великі масиви даних, виявляти приховані закономірності та передбачати ймовірність атак ще до їхнього здійснення. Наприклад, ШІ може визначати тенденції у фішингових кампаніях, прогнозувати появу нових шкідливих програм або оцінювати ризики інсайдерських дій [10]. Інтеграція таких технологій у політику безпеки забезпечує проактивний підхід: організація не лише реагує на інциденти, а й готується до них заздалегідь.

Важливо, щоб системи на основі ШІ працювали у зв’язці з іншими інструментами (SIEM, UBA, DLP) створюючи єдину екосистему захисту. Використання ШІ дозволяє оптимізувати ресурси служби безпеки, адже

автоматизований аналіз зменшує навантаження на фахівців [40]. У результаті організація отримує гнучку та інтелектуальну систему, здатну адаптуватися до нових викликів і забезпечувати високий рівень захисту даних.

Таким чином, використання сучасних цифрових інструментів для управління ризиками формує основу для підвищення ефективності інформаційної безпеки організацій. Інтеграція таких рішень забезпечує комплексний контроль за даними та процесами, зменшуючи ймовірність критичних інцидентів. Цифрові інструменти стають ключовим елементом стабільності та прозорості бізнес-процесів.

## 3.3. Практичні кроки адаптації політик інформаційної безпеки до нових загроз

Практичні кроки адаптації політик інформаційної безпеки до нових загроз є важливим елементом формування стійкої системи захисту організації. Вони дозволяють враховувати динаміку кіберзагроз та забезпечувати відповідність сучасним стандартам безпеки. Кожен із запропонованих заходів спрямований на зниження ризиків та підвищення ефективності управління інформаційними ресурсами. На рис. 3.3 відображено основні практичні кроки адаптації політик інформаційної безпеки до нових загроз.

Регулярне оновлення політик інформаційної безпеки є фундаментальним елементом ефективного управління ризиками. У сучасному цифровому середовищі загрози постійно змінюються: з’являються нові методи атак, уразливості програмного забезпечення та інструменти соціальної інженерії. Якщо політика безпеки залишається статичною, вона швидко втрачає актуальність і перестає виконувати свою захисну функцію. Тому організація повинна передбачати механізм постійного перегляду та коригування документів, що регламентують роботу з інформаційними ресурсами [21]. Це включає аналіз нових ризиків, врахування міжнародних стандартів та рекомендацій галузевих експертів.


Рис.3.3. Основні практичні кроки адаптації політик інформаційної безпеки до нових загроз

Потрібно також інтегрувати результати внутрішніх аудитів і тестів на проникнення, які дозволяють виявити слабкі місця у системі. Регулярне оновлення політик забезпечує не лише технічний захист, але й формує довіру клієнтів та партнерів, адже демонструє зрілість організації у сфері кібербезпеки. У результаті організація отримує адаптивну систему, здатну реагувати на нові виклики та підтримувати стабільність бізнес-процесів.

План безперервності бізнесу (Business Continuity Plan, BCP) є ключовим інструментом для забезпечення стійкості організації у випадку кризових ситуацій [3]. Його мета полягає у визначенні процедур, які дозволяють підтримувати критичні бізнес-процеси навіть під час інцидентів, технічних збоїв чи атак. Розробка BCP повинна враховувати всі основні ресурси: інформаційні системи, персонал, інфраструктуру та постачальників. Важливо не лише створити документ, але й регулярно тестувати його на практиці. Тестування дозволяє виявити слабкі місця та вдосконалити процедури реагування.

Окрім цього, BCP має бути інтегрований у загальну політику безпеки та узгоджений із планами відновлення після інцидентів (Disaster Recovery Plans). Наявність ефективного BCP підвищує довіру клієнтів і партнерів, адже демонструє готовність організації до непередбачуваних подій [49]. У результаті компанія отримує стратегічну перевагу – здатність швидко відновлювати роботу та мінімізувати фінансові й репутаційні втрати.

Гнучкість політик інформаційної безпеки є необхідною умовою їхньої ефективності. Організації працюють у різних сферах, мають різні масштаби та специфіку бізнес-процесів, тому універсальні підходи часто виявляються недостатніми [12]. Політика має враховувати особливості кожного підрозділу: наприклад, вимоги до фінансового відділу будуть відрізнятися від потреб виробничого чи маркетингового. Гнучкість означає можливість адаптації правил до конкретних умов, зберігаючи при цьому загальні стандарти безпеки. Це може включати різні рівні доступу, специфічні процедури контролю або індивідуальні сценарії реагування на інциденти.

Важливо, щоб політика не перетворювалася на бюрократичний бар'єр, а залишалася практичним інструментом, який підтримує ефективність роботи [13]. Для цього необхідно регулярно переглядати її положення, враховувати зміни у бізнес-моделі та технологічному середовищі. Гнучкі політики дозволяють організації швидко реагувати на нові виклики, мінімізувати ризики та забезпечувати стабільність бізнес-процесів без шкоди для продуктивності.

Інсайдерські загрози залишаються одними з найскладніших для виявлення, адже вони походять від співробітників чи партнерів, які мають легальний доступ до систем. Політики інформаційної безпеки повинні враховувати цей фактор, створюючи механізми контролю та моніторингу дій користувачів [25]. Це може включати обмеження прав доступу, використання систем аналізу поведінки (UBA) та регулярні перевірки журналів активності. Важливо також формувати культуру відповідальності серед персоналу, адже усвідомлення наслідків порушень знижує ймовірність зловживань. Політики мають передбачати чіткі процедури реагування на підозрілі дії, включаючи тимчасове блокування доступу та проведення внутрішніх розслідувань.

Слід враховувати психологічні та соціальні чинники, які можуть спонукати працівників до неправомірних дій, наприклад, конфлікти чи незадоволення умовами праці [39]. У результаті організація отримує комплексний підхід, що поєднує технічні, організаційні та людські аспекти, зменшуючи ризик витоку даних чи саботажу.

Співпраця з державними та міжнародними центрами кіберзахисту (табл.3.5) є важливим елементом сучасної політики інформаційної безпеки. Такі структури забезпечують обмін актуальною інформацією про нові загрози, надають рекомендації щодо реагування та допомагають координувати дії під час масштабних інцидентів [22]. Організація, яка активно взаємодіє з цими центрами, отримує доступ до баз знань, аналітичних звітів та інструментів раннього попередження. Це дозволяє швидше адаптувати політики безпеки та підвищувати їхню ефективність.

Таблиця 3.5

Міжнародні центри кіберзахисту

| № | Центр | Країна / Організація | Основне призначення | Ключові функції |
|---|---|---|---|---|
| 1 | NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) | Естонія (НАТО) | Дослідження та навчання у сфері кібероборони | Розробка стратегій, проведення навчань, аналітика кіберзагроз |
| 2 | European Union Agency for Cybersecurity (ENISA) | ЄС | Координація кіберзахисту в країнах ЄС | Розробка стандартів, підтримка CERT-ів, рекомендації для урядів та бізнесу |
| 3 | FIRST (Forum of Incident Response and Security Teams) | Глобальна мережа | Об’єднання команд реагування на інциденти | Обмін інформацією, стандартизація процесів реагування, міжнародна співпраця |
| 4 | Global Forum on Cyber Expertise (GFCE) | Міжнародна платформа | Підвищення кіберстійкості через обмін знаннями | Освітні програми, підтримка країн, розвиток політик кіберзахисту |
| 5 | APCERT (Asia Pacific Computer Emergency Response Team) | Азійсько-Тихоокеанський регіон | Координація реагування на інциденти в регіоні | Спільні тренінги, обмін інформацією, підтримка національних CERT-ів |

Співпраця сприяє відповідності міжнародним стандартам і демонструє партнерам високий рівень зрілості у сфері кіберзахисту. Важливе значення має те, щоб політики організації передбачали механізми обміну даними та участь у спільних навчаннях чи тренінгах [19]. Такий підхід формує глобальну екосистему безпеки, де кожна компанія є частиною ширшої мережі захисту. У

результаті організація отримує стратегічну перевагу – можливість оперативно реагувати на нові виклики та зменшувати ризики масштабних інцидентів.

Розробка та впровадження політик управління мобільними пристроями (Mobile Device Management, MDM) є критично важливим завданням для сучасних організацій, які активно використовують смартфони, планшети та інші мобільні засоби у своїй діяльності [55]. Зростання мобільності персоналу та поширення концепції BYOD (Bring Your Own Device) створюють додаткові ризики витоку даних, несанкціонованого доступу та зараження корпоративних систем шкідливим програмним забезпеченням.

Політики інформаційної безпеки MDM повинні визначати правила використання мобільних пристроїв, включаючи вимоги до шифрування даних, встановлення лише перевірених додатків, регулярне оновлення операційних систем та антивірусного захисту. Ключовим елементом є централізоване адміністрування, яке дозволяє службі безпеки віддалено блокувати або видаляти дані з пристроїв у випадку їхньої втрати чи компрометації.

Крім того, політики інформаційної безпеки мають передбачати контроль доступу до корпоративних ресурсів через багатофакторну автентифікацію та VPN-з’єднання [3]. Ефективне впровадження MDM сприяє зниженню ризиків, пов’язаних із мобільними технологіями, та забезпечує баланс між безпекою і зручністю роботи персоналу.

Таким чином, практичні кроки адаптації політик інформаційної безпеки до нових загроз забезпечують організаціям здатність оперативно реагувати на динамічні виклики кіберпростору. Вони формують комплексний підхід, що поєднує технічні, організаційні та людські аспекти захисту. У підсумку це створює адаптивну систему кібербезпеки, здатну мінімізувати ризики та підтримувати високий рівень стійкості інформаційної інфраструктури.

## Висновки до розділу 3

Отже, розробка рекомендацій щодо вдосконалення політик інформаційної безпеки доводить, що ефективний захист даних потребує комплексного підходу. Ключовими напрямами є регулярний аудит, який забезпечує актуальність правил, та інтеграція міжнародних стандартів ISO/IEC і NIST, що підвищує довіру й конкурентоспроможність організації. Важливим є впровадження чітких правил доступу, багатофакторної автентифікації та систем моніторингу, зокрема SIEM-рішень. Особливу увагу слід приділяти людському фактору через навчання, моделювання інцидентів і формування культури безпеки.

Використання сучасних цифрових інструментів для управління ризиками формує основу ефективної системи інформаційної безпеки. Ключовими напрямами є впровадження систем управління вразливостями, що забезпечують проактивний захист, та багатофакторної автентифікації, яка мінімізує ризик несанкціонованого доступу. Інструменти DLP контролюють рух конфіденційної інформації, а сертифіковані хмарні сервіси гарантують відповідність міжнародним стандартам. Автоматизоване резервне копіювання забезпечує безперервність бізнес-процесів, тоді як UBA-системи виявляють інсайдерські загрози. Інтеграція штучного інтелекту дозволяє прогнозувати атаки та оптимізувати ресурси.

Практичні кроки адаптації політик інформаційної безпеки до нових загроз забезпечують організаціям здатність оперативно реагувати на динамічні виклики кіберпростору. Регулярне оновлення політик та інтеграція результатів аудитів і тестів на проникнення підтримують їхню актуальність і ефективність. План безперервності бізнесу гарантує стійкість критичних процесів навіть у кризових умовах. Гнучкість політик дозволяє враховувати специфіку різних підрозділів, а механізми контролю інсайдерських загроз знижують ризик витоків даних. Співпраця з міжнародними центрами кіберзахисту та впровадження MDM-рішень формують комплексний підхід, що поєднує технічні, організаційні та людські аспекти захисту.

# ВИСНОВКИ

На основі одержаних результатів дослідження можна сформулювати наступні висновки, які відображають сутність, проблеми та практичні аспекти оптимізації політики інформаційної безпеки організації на основі аналізу ризиків та загроз:

1. Політика інформаційної безпеки є стратегічним документом, що визначає принципи, правила та механізми захисту інформаційних активів. Її значення полягає у створенні системного підходу до управління ризиками, формуванні культури відповідальності серед персоналу та забезпеченні відповідності міжнародним стандартам і законодавчим вимогам. Вона координує дії співробітників, технічних засобів та управлінських рішень, спрямованих на збереження конфіденційності, цілісності та доступності даних. У підсумку політика виступає не лише регламентом, а й стратегічним ресурсом, що підтримує здатність організації протидіяти сучасним кіберзагрозам.

2. Класифікація ризиків та загроз у сфері інформаційної безпеки дозволяє систематизувати потенційні небезпеки за джерелами, рівнем впливу та ймовірністю реалізації. Вона охоплює технічні, організаційні, людські та зовнішні фактори, що формують комплексну картину ризиків. Методи аналізу, такі як SWOT, OCTAVE чи ISO-базовані підходи, забезпечують можливість якісної та кількісної оцінки загроз. Це дозволяє визначати пріоритети у захисті, оптимізувати використання ресурсів, формувати ефективні стратегії реагування.

3. Ефективність політик інформаційної безпеки визначається їхньою здатністю знижувати ризики та забезпечувати стабільність роботи інформаційних систем. Наприклад, у компанії Microsoft політика безпеки інтегрована з міжнародними стандартами ISO/IEC 27001, що дозволяє підтримувати високий рівень захисту даних клієнтів. У банківській сфері, зокрема в Deutsche Bank, політики безпеки регулярно перевіряються аудитами та тестами на проникнення, що забезпечує їхню актуальність. Важливим є врахування рівня обізнаності персоналу та наявності механізмів контролю. Якщо

політики залишаються статичними або не оновлюються, вони швидко втрачають ефективність.

4. Реалізація інформаційної політики на практиці часто стикається з проблемами, що підтверджуються реальними інцидентами у світовій та українській практиці. Серед ключових ризиків, які ми розглядали, варто виділити кіберзлочинність та хакерські атаки, що можуть паралізувати критичну інфраструктуру, як у випадку BlackCat проти Change Healthcare. Вразливості хмарних сервісів, продемонстровані інцидентом Snowflake, доводять, що навіть великі провайдери не є повністю захищеними. Фішинг і соціальна інженерія, як атаки на Coinbase чи Marks & Spencer, показують слабкість людського фактора. Усі ці приклади доводять, що політика безпеки без постійного оновлення та практичного контролю залишається формальною і неефективною.

5. Рекомендації щодо вдосконалення політики інформаційної безпеки повинні враховувати сучасні тенденції та практичні потреби організації. Серед ключових напрямів – регулярне оновлення документів, інтеграція міжнародних стандартів, впровадження систем моніторингу та аналізу поведінки користувачів. Необхідно забезпечити навчання персоналу та формування культури відповідальності. Доцільно також передбачити механізми реагування на інциденти та процедури відновлення після кризових ситуацій. Використання цифрових інструментів, таких як SIEM чи DLP, дозволяє підвищити ефективність контролю.

Практичні кроки адаптації політик інформаційної безпеки до нових загроз формують основу гнучкої та стійкої системи захисту. Їхня мета полягає у забезпеченні постійного оновлення документів, інтеграції сучасних технологій та врахуванні людського фактора. Важливим є використання результатів внутрішніх аудитів, тестів на проникнення та співпраця з міжнародними центрами кіберзахисту. Політики мають передбачати механізми реагування на інсайдерські ризики, соціальну інженерію та витоки даних. У підсумку організація отримує адаптивну систему кібербезпеки, здатну оперативно реагувати на нові виклики та мінімізувати ймовірність критичних інцидентів.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ананьїн В. О., Горлинський В. В., Гангал А. В. Інформаційна безпека. Менеджмент інформаційної безпеки держави [Електронний ресурс]: курс лекцій: навч. посіб. для здобувачів ступеня магістра за освітніми програмами «Комп'ютерні системи і технології спеціального зв'язку» та «Спеціальні системи електронних комунікацій» спец. 122 «Комп'ютерні науки», 172 «Електронні комунікації та радіотехніка» / ІСЗЗІ КПІ ім. Ігоря Сікорського. Електронні текстові дані (1 файл: 2,73 Мбайт). Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. URL: https://ela.kpi.ua/server/api/core/bitstreams/c4ad5148-9e04-4979-9ef7-0fec3a385650/content (дата звернення: 07.05.2026).

2. Атаки на ланцюги постачання є головною кіберзагрозою до 2030 року – ENISA. URL: https://10guards.com/ua/blog/2024/05/28/supply-chain-attacks-top-cyber-threat-for-2030-enisa/ (дата звернення: 07.05.2026).

3. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посібник. Київ: Юрінком Інтер, 2025. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/25701/3/0061692m.pdf (дата звернення: 07.05.2026).

4. Буряченко О. Сучасні виклики глобальної інформаційної безпеки. URL: https://fps-visnyk.lnu.lviv.ua/archive/55_2024/32.pdf (дата звернення: 07.05.2026).

5. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ: ДУТ, 2015. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 07.05.2026).

6. Великий куш: чому стаються витоки даних? URL: https://www.kunsht.com.ua/articles/velykyy-kush-chomu-staiutsia-vytoky-danykh (дата звернення: 07.05.2026).

7. Витоки даних: як їм запобігти та що робити у разі порушення. URL: https://www.hostragons.com/uk/%D0%B1%D0%BB%D0%BE%D0%B3/%D1%8F%D0%BA-

%D0%B7%D0%B0%D0%BF%D0%BE%D0%B1%D1%96%D0%B3%D1%82%D0%B8-%D0%B2%D0%B8%D1%82%D0%BE%D0%BA%D0%B0%D0%BC-%D0%B4%D0%B0%D0%BD%D0%B8%D1%85-%D1%96-%D1%89%D0%BE-%D1%80%D0%BE%D0%B1%D0%B8%D1%82%D0%B8/ (дата звернення: 07.05.2026).

8. Витоки персональних даних 2025. URL: https://avitar.legal/post/2025-rik-koli-vitoki-danih-stali-novoyu-normoyu (дата звернення: 07.05.2026).

9. Ворог всередині: інсайдерські загрози, що чатують у 2025 році. URL: https://ua.linkedin.com/pulse/nsbcs086-enemy-within-insider-threats-lurking-2025-nsb-cyber-3qyhc (дата звернення: 07.05.2026).

10. Дипфейки: як працює технологія обману та які загрози несе. URL: https://zaxid.net/dipfeyki_yak_pratsyuye_tehnologiya_obmanu_ta_yaki_zagrozi_nese_n1614984 (дата звернення: 07.05.2026).

11. Зростання загрози атак на ланцюги постачання ПЗ. URL: https://corewin.ua/blog/growing-threat-of-supply-chain-attacks/ (дата звернення: 07.05.2026).

12. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В. І. Вернадського. Київ, 2026. № 1 (січень). 139 с. URL: https://ippi.org.ua/sites/default/files/2026-1.pdf (дата звернення: 07.05.2026).

13. Костюк Ю. В. Безпека інформаційно-комунікаційних систем: підручник / Ю.В. Костюк, П.М. Складанний, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва, М.В. Ворохоб. Київ: Київський столичний університет імені Бориса Грінченка, 2025. URL: https://elibrary.kubg.edu.ua/id/eprint/51358/1/Kostiuk_Y_Skladannyi_P_Bebeshko_B_Khorolska_K_Rzaieva_S_Vorokhob_M_BIKS_2025_FITM.pdf (дата звернення: 07.05.2026).

14. Масштабний витік даних – чи є там ваші? URL: https://znayemo.com.ua/masshtabnyj-vytik-danyh-chy-ye-tam-vashi/ (дата звернення: 07.05.2026).

15. Мухін В. Є., Завгородній В. В., Завгородня Г. А. Інформаційна безпека та гібридні загрози: навчальний посібник / укл. В. Є. Мухін, В. В. Завгородній, Г. А. Завгородня. – Київ: ТОВ «ТРОПЕА», 2024. DOI: https://doi.org/10.32703/978-617-8268-36-7 (дата звернення: 07.05.2026).

16. НБУ Regulation. Постанова НБУ № 143 – Інформаційна безпека та кіберзахист. URL: https://secboard.online/about/knowledge-base/nbu-regulation-no-143-information-security-cyber-protection/ (дата звернення: 07.05.2026).

17. Небезпека ближче, ніж ви думаєте: як компанії захиститися від інсайдерських загроз. URL: https://www.eset.com/ua/about/newsroom/blog/business-security/nebezpeka-blyzhche-nizh-vy-vvazhayete-yak-kompaniyi-zakhystytsya-vid-insayderskykh-zahroz/ (дата звернення: 07.05.2026).

18. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. URL: https://duikt.edu.ua/uploads/l_1426_56444238.pdf (дата звернення: 07.05.2026).

19. Огляд кіберзагроз та стратегій захисту в 2025 році: досвід CERT-UA. URL: https://cip.gov.ua/ua/news/cyber-threat-overview-and-defense-strategies-in-2025-cert-ua-s-experience (дата звернення: 07.05.2026).

20. Повний гайд з керування інсайдерськими ризиками. URL: https://corewin.ua/blog/insider-threat/ (дата звернення: 07.05.2026).

21. Розробка та реалізація політик безпеки. URL: https://softtim.com.ua/rishennya/informatsijna-bezpeka/rozrobka-ta-realizatsiya-politik-bezpeki (дата звернення: 07.05.2026).

22. Сучасні кіберзагрози: виклики 2025 року. URL: https://proit.com.ua/news/suchasni-kiberzagrozy-vyklyky-2025-roku/ (дата звернення: 07.05.2026).

23. Топ-10 витоків даних, що зачепили українців (2024-2026). URL: https://cyberpeople.tech/blog/ua/top-10-vytokiv-danykh-shcho-zachepyly-ukraintsiv (дата звернення: 07.05.2026).

24. Що таке витік даних? Визначення і приклади. URL: https://gridinsoft.ua/data-breaches (дата звернення: 07.05.2026).

25. Як запобігти чотирьом поширеним інсайдерським загрозам. URL: https://eska.global/blog/4-prikladi-insajderskih-zagroz-ta-yak-yih-zapobigti (дата звернення: 07.05.2026).

26. AI and Election Disinformation. URL: https://stateofsurveillance.org/articles/surveillance/ai-election-disinformation-2024-2025/ (дата звернення: 07.05.2026).

27. AI-Powered Cyberattacks: How Artificial Intelligence Is Changing the Threat Landscape. URL: https://www.techprescient.com/blogs/ai-powered-cyberattacks/ (дата звернення: 07.05.2026).

28. Ali Ismail Awad. Introduction to information security foundations and applications. URL: https://www.diva-portal.org/smash/get/diva2:1204986/FULLTEXT01.pdf (дата звернення: 07.05.2026).

29. Apple Platform Certifications. Intro to Apple security assurance. URL: https://support.apple.com/uk-ua/guide/certifications/apc3cea61877b/web (дата звернення: 07.05.2026).

30. AWS Services in Scope by Compliance Program. URL: https://aws.amazon.com/compliance/iso-certified/ (дата звернення: 07.05.2026).

31. Bjorn Lundgren, Niklas Moller. Defining Information Security. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6450831/pdf/11948_2017_Article_9992.pdf (дата звернення: 07.05.2026).

32. Cyberwiderstandsfähigkeit des Finanzsystems. URL: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/tiber-de/tiber-de-816986 (дата звернення: 07.05.2026).

33. Deutsche Bank – statistics & facts. URL: https://www.statista.com/topics/1350/deutsche-bank/ (дата звернення: 07.05.2026).

34. Diana Rusu and Marius Mantulescu. Development of an Application-Based Framework for Information Security Management in SMEs. URL: https://www.mdpi.com/2071-1050/17/18/8314 (дата звернення: 07.05.2026).

35. Docusign Envelope Certificate. URL: https://d1.awsstatic.com/certifications/iso_27018_certification.pdf (дата звернення: 07.05.2026).

36. Framework Mapping: Cisco Firewalls + NIST CSF 2.0. URL: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/fm-firewalls-nist-csf-wp.html (дата звернення: 07.05.2026).

37. Gmail Email Security & Privacy Settings – Google Safety Center. URL: https://safety.google/intl/en_us/products/gmail/ (дата звернення: 07.05.2026).

38. Google. Keeping over five billion devices safer. URL: https://safebrowsing.google.com/ (дата звернення: 07.05.2026).

39. How to Prevent Insider Threats in Website Security? URL: https://www.linkedin.com/pulse/how-prevent-insider-threats-website-security-teknologiia-rdqpf/ (дата звернення: 07.05.2026).

40. IBM. What is the NIST Cybersecurity Framework? URL: https://www.ibm.com/think/topics/nist (дата звернення: 07.05.2026).

41. ISACA / Cisco. Why COBIT. URL: https://www.isaca.org/resources/cobit (дата звернення: 07.05.2026).

42. Joseph R. Laracy, Thomas Marlowe. Systems Theory and Information Security: Foundations for a New Educational Approach. URL: https://www.dline.info/isej/fulltext/v5n2/isejv5n2_1.pdf (дата звернення: 07.05.2026).

43. Kyivstar Cyber Attack: A Deep Dive Into Cyber Warfare in Ukraine. URL: https://www.afcea.org/signal-media/cyber-edge/kyivstar-cyber-attack-deep-dive-cyber-warfare-ukraine (дата звернення: 07.05.2026).

44. Kyivstar Files its 2025 Annual Report on Form 20-F. URL: https://investors.kyivstar.ua/news-releases/news-release-details/kyivstar-files-its-2025-annual-report-form-20-f (дата звернення: 07.05.2026).

45. Logistics Giant Nova Poshta Invests Over 1 Billion Hryvnia to Shield Ukrainian Supply Chains Amid Persistent Aerial Threats. URL: https://axlnews.com/article/logistics-giant-nova-poshta-invests-over-1-billion-hryvnia-to-shield-ukrainian-supply-chains-amid-persistent-aerial-threats (дата звернення: 07.05.2026).

46. Massive Cloud Provider Cyberattacks in 2024: Examples and Prevention Strategies. URL: https://www.blackfog.com/cloud-provider-cyberattacks-2024/ (дата звернення: 07.05.2026).

47. Microsoft Corporation. CERTIFICATE OF REGISTRATION Information Security Management System – ISO/IEC 27001:2022. URL: https://trh-data.com/wp-content/uploads/2025/01/Azure-Dynamics-365-Online-Services-ISO-27001-and-ISO-27701-Certificate-12.16.2024.pdf (дата звернення: 07.05.2026).

48. Microsoft. ISO/IEC 27001:2013 Information Security Management Standards. URL: https://learn.microsoft.com/en-us/compliance/regulatory/offering-ISO-27001 (дата звернення: 07.05.2026).

49. NIST Cybersecurity Framework Adoption & Industry Analysis. URL: https://acsmi.org/blogs/nist-cybersecurity-framework-adoption-original-data-amp-industry-analysis-2025 (дата звернення: 07.05.2026).

50. Nova Poshta invests over UAH 1 bln in security since invasion. URL: https://en.interfax.com.ua/news/economic/1153556.html (дата звернення: 07.05.2026).

51. Protecting the confidentiality, integrity and availability of customer and bank details is a key priority at Deutsche Bank. Find out here what we are doing to combat cyber crime. URL: https://corporates.db.com/in-focus/focus-topics/cyber-security/security-at-deutsche-bank (дата звернення: 07.05.2026).

52. QRadar and Guardium integration. URL: https://www.ibm.com/docs/en/gdp/11.4.0?topic=integration-qradar-guardium (дата звернення: 07.05.2026).

53. Ransomware Attack 2025 Recap – From Critical Data Extortion to Operational Disruption. URL: https://cybersecuritynews.com/ransomware-attack-2025-recap/ (дата звернення: 07.05.2026).

54. Red Team Statistics 2026: 50+ Key Facts and Figures. URL: https://cybersecurityswitzerland.com/research/red-team-statistics-2026/ (дата звернення: 07.05.2026).

55. Shafag Ahmedova, Azer Shirinov. Political and legal foundations of information security in the modern world. URL: https://www.periodicojs.com.br/index.php/gei/article/view/50 (дата звернення: 07.05.2026).

56. Security Spotlight. Meta Fined $263.5m Over Data Breach in Europe. URL: https://dailysecurityreview.com/security-spotlight/meta-fined-263-5m-over-data-breach-in-europe/ (дата звернення: 07.05.2026).

57. Social Engineering Attacks Surge in 2025, Becoming Top Cybersecurity Threat. URL: https://www.techrepublic.com/article/news-social-engineering-top-cyber-threat-2025/ (дата звернення: 07.05.2026).

58. Top 10 Biggest Cyber Attacks of 2024 & 25 Other Attacks to Know About! URL: https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about (дата звернення: 07.05.2026).

59. Top 10 Ransomware Attacks of 2025. URL: https://socradar.io/blog/top-10-ransomware-attacks-2025/ (дата звернення: 07.05.2026).

60. Top Social Engineering Attacks in 2025. URL: https://www.mitnicksecurity.com/blog/top-social-engineering-attacks (дата звернення: 07.05.2026).

61. Top Threats to Cloud Computing – Deep Dive 2025. URL: https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2025 (дата звернення: 07.05.2026).