МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему

« СИСТЕМА ОЦІНКИ РИЗИКІВ ТА СПОСОБИ МІНІМІЗАЦІЇ ВПЛИВУ КІБЕРЗАГРОЗ В УМОВАХ ДИСТАНЦІЙНОГО ОФІСУ »

Виконала: студентка групи 1КІ-23
спеціальності
123 «Комп'ютерна інженерія
Литовченко В.О.
Керівник роботи к.т.н., доцент
Захарова М.В.
Кількість балів:_____
Оцінка: ECTS_____

Черкаси, 2025

АНОТАЦІЯ

У кваліфікаційній роботі досліджено питання забезпечення кібербезпеки організації в умовах дистанційного функціонування. Визначено основні сучасні кіберзагрози, що характерні для віддаленого середовища, проаналізовано їх вплив на конфіденційність, цілісність і доступність інформаційних активів. Розглянуто теоретичні основи та сучасні підходи до оцінки ризиків в інформаційній безпеці, проведено класифікацію загроз і оцінку рівня ризику за кількісними та якісними показниками з використанням програмного інструментарію Python.

Запропоновано алгоритм побудови стратегії захисту конфіденційних даних, що базується на системному підході до управління ризиками та передбачає поетапну ідентифікацію активів, аналіз загроз і вразливостей, розрахунок ризику та визначення пріоритетних заходів безпеки. Здійснено економічне обґрунтування доцільності впровадження запропонованих заходів кіберзахисту шляхом порівняння витрат на безпеку та можливих фінансових збитків, а також визначено період окупності інвестицій. Результати оформлено у вигляді таблиць, графіків, діаграм та інфографіки, що візуально підтверджують ефективність розробленої системи.

Практичне значення роботи полягає у можливості застосування запропонованої методики оцінки ризиків та заходів мінімізації кіберзагроз для підприємств малого та середнього бізнесу, що функціонують у дистанційному або гібридному форматі. Реалізація результатів дослідження дозволить знизити рівень ризиків, уникнути фінансових та репутаційних втрат і підвищити рівень довіри клієнтів та партнерів.

Ключові слова: ризик, кіберзагроза, захист інформації, дистанційний офіс.

ABSTRACT

The qualification thesis addresses the issue of ensuring cybersecurity for an organization operating in a remote work environment. The main modern cyber threats typical for remote work have been identified and analyzed, highlighting their impact on the confidentiality, integrity, and availability of information assets. Theoretical foundations and modern approaches to risk assessment in the field of information security have been studied. A classification of threats has been conducted and the risk level has been evaluated using quantitative and qualitative indicators supported by Python-based tools.

An algorithm for developing a confidential data protection strategy has been proposed. It is based on a systematic approach to risk management and includes step-by-step identification of assets, analysis of threats and vulnerabilities, risk calculation, and prioritization of security measures. The economic feasibility of implementing the proposed cybersecurity measures has been justified by comparing the costs of security with potential financial losses and calculating the payback period for the investment. The results are presented in the form of tables, graphs, diagrams, and infographics, which visually confirm the effectiveness of the developed system.

The practical significance of the thesis lies in the possibility of applying the proposed risk assessment methodology and threat mitigation measures in small and medium-sized enterprises that operate remotely or in a hybrid format. The implementation of the research results will help to reduce risk levels, prevent financial and reputational losses, and increase the trust of clients and partners.

Keywords: risk, cyber threat, information protection, remote office.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

2FA	Two-Factor Authentication (Двофакторна автентифікація)
AI	Artificial Intelligence (Штучний інтелект)
API	Application Programming Interface (Інтерфейс прикладного програмування)
CIS	Center for Internet Security (Центр інтернет-безпеки)
CSA	Cloud Security Alliance (Альянс хмарної безпеки)
CSV	Comma-Separated Values (Файл зі значеннями, розділеними комами)
DB	Database (База даних)
DBIR	Data Breach Investigations Report (Звіт про дослідження порушень даних)
ENISA	European Union Agency for Cybersecurity (Агентство ЄС з кібербезпеки)
GDPR	General Data Protection Regulation (Загальний регламент захисту даних ЄС)
IDS	Intrusion Detection System (Система виявлення вторгнень)
IPS	Intrusion Prevention System (Система запобігання вторгненням)
IoT	Internet of Things (Інтернет речей)
ISO	International Organization for Standardization (Міжнародна організація зі стандартизації)
ІБ	Інформаційна безпека
КЗ	Кіберзагроза
KPI	Key Performance Indicator (Ключовий показник ефективності)
MFA	Multi-Factor Authentication (Багатофакторна автентифікація)
ML	Machine Learning (Машинне навчання)

NIST	National Institute of Standards and Technology (Національний інститут стандартів і технологій США)
PCI DSS	Payment Card Industry Data Security Standard (Стандарт безпеки даних індустрії платіжних карток)
ROI	Return on Investment (Рентабельність інвестицій)
SP	Special Publication (Спеціальна публікація)
UI	User Interface (Користувацький інтерфейс)
VPN	Virtual Private Network (Віртуальна приватна мережа)
ЗІ	Захист інформації
2FA	Two-Factor Authentication (Двофакторна автентифікація)

ВСТУП

Стрімкий розвиток інформаційних технологій та глобальний перехід організацій до дистанційного формату роботи призвели до суттєвого ускладнення процесів забезпечення інформаційної безпеки. В умовах віддаленого доступу до корпоративних ресурсів та використання домашніх і публічних мереж зростає ймовірність реалізації кіберзагроз, таких як несанкціонований доступ, фішингові атаки, шкідливе програмне забезпечення, компрометація облікових даних і витік конфіденційної інформації.

Актуальність дослідження зумовлена необхідністю впровадження ефективної системи оцінки ризиків та розробки комплексу заходів, що мінімізують вплив кіберзагроз у середовищі дистанційного офісу. Забезпечення конфіденційності, цілісності та доступності інформації стає запорукою безперервності бізнес-процесів та збереження конкурентних переваг компаній.

Мета роботи полягає у розробці системи оцінки ризиків та побудові стратегії мінімізації впливу кіберзагроз для організацій, що працюють у віддаленому режимі.

З**авдання**:

- провести аналіз сучасних кіберзагроз, характерних для дистанційного середовища;
- дослідити теоретичні основи та методи оцінки ризиків в інформаційній безпеці;
- класифікувати ризики та оцінити їх рівень за кількісними та якісними показниками;
- розробити алгоритм побудови стратегії захисту конфіденційних даних;
- оцінити економічну доцільність впровадження запропонованих заходів безпеки.

Постановка завдання. Згідно з метою дослідження, у кваліфікаційній роботі необхідно розробити практичну модель системи оцінки ризиків для підприємства, що функціонує у дистанційному режимі, визначити критичні загрози, розрахувати

очікувані ризики за допомогою кількісних та якісних методів, обґрунтувати економічну доцільність впровадження комплексу заходів кіберзахисту.

Методи дослідження включають системний підхід до управління ризиками, математичне моделювання, програмну реалізацію розрахунків за допомогою Python, а також аналіз сучасних нормативних актів та стандартів у сфері кібербезпеки.

Об'єкт дослідження — процеси забезпечення кібербезпеки в умовах дистанційного функціонування організації.

Предмет дослідження — методи оцінки ризиків та засоби мінімізації впливу кіберзагроз у віддаленому середовищі.

Практичне значення роботи полягає у можливості впровадження розробленої системи оцінки ризиків та комплексу заходів кіберзахисту на підприємствах, що працюють у гібридному або повністю віддаленому форматі, для зниження фінансових втрат, запобігання витоку конфіденційної інформації та підтримання стабільності бізнес-процесів.

Апробація результатів бакалаврської роботи. Матеріали до бакалаврської роботи апробувалися на XVII Студентській науково-практичній конференції «Тенденції розвитку ІТ-технологій в Україні» (Черкаси: ЧДБК, 2025).

Публікації.

1. Литовченко В.О. Аналіз ризиків та викликів захисту конфіденційних даних в умовах дистанційного офісу// XVII Студентська науково-практична конференція «Тенденції розвитку ІТ-технологій в Україні» 26-27 березня 2025 р. м.Черкаси. с. 48-51.

Структура та обсяг роботи. Дипломна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел (30 найменування) та додатків. Загальний обсяг роботи становить 61 сторінок основного тексту, 21 рисунка та 7 таблиць.

РОЗДІЛ 1 АНАЛІЗ КІБЕРЗАГРОЗ У ДИСТАНЦІЙНОМУ ОФІСІ

У сучасному світі, де дистанційна робота стає все більш поширеною, питання захисту конфіденційних даних набуває критичної важливості. Віддалене середовище створює нові виклики для організацій, які прагнуть забезпечити безпеку своєї інформації. Основні ризики виникають через технічні уразливості, низьку обізнаність користувачів про основи кібербезпеки та обмежені можливості контролю з боку IT-відділів.

Серед найпоширеніших кіберзагроз віддаленого середовища варто виділити фішинг-атаки, використання публічних або незахищених Wi-Fi мереж, а також ризик зараження пристроїв шкідливим програмним забезпеченням. Фішингові атаки, зокрема, є однією з найпоширеніших загроз, коли зловмисники вводять користувачів в оману через підроблені електронні листи чи сайти з метою викрадення облікових даних. Не менш небезпечними є загрози, пов’язані з публічними Wi-Fi мережами, які можуть стати місцем для атак типу "людина посередині", коли зловмисники перехоплюють інформацію, що передається [4].

Додатково до цього, загрози можуть мати форму шкідливого програмного забезпечення: вірусів, троянів, руткітів або програм-шпигунів, які можуть бути впроваджені на пристрої через інфіковані файли або посилання. Атаки через DDoS (розподілені атаки відмови в обслуговуванні) також можуть вивести із ладу системи віддаленого доступу, ускладнюючи роботу співробітників.

Вразливості систем віддаленого доступу є ще однією критичною загрозою. Використання простих паролів, їх повторне застосування, а також відсутність двофакторної автентифікації збільшують ризик несанкціонованого доступу до корпоративних систем. Якщо до цього додати відсутність регулярного оновлення програмного забезпечення, що часто спостерігається у віддаленому середовищі, це створює значні можливості для кіберзлочинців.

Вразливості VPN-з'єднань також є поширеним каналом для атак, адже багато користувачів використовують невідомі чи ненадійні сервіси для віддаленого доступу.

Важливо розглянути і людський фактор, адже він є однією з найслабших ланок у системах безпеки. Низька обізнаність співробітників щодо принципів кібербезпеки, недотримання політик захисту даних та випадкові помилки, наприклад, надсилання конфіденційної інформації не тим отримувачам, часто стають причиною витоку даних. До того ж, в умовах віддаленої роботи зростає ймовірність використання особистих пристроїв, які можуть бути недостатньо захищеними від атак [4].

Ризики порушення конфіденційності даних у віддаленому середовищі можуть мати серйозні наслідки для організацій. Фінансові втрати, зокрема через шахрайство або штрафи за порушення нормативних вимог, таких як GDPR, можуть негативно вплинути на стабільність компаній. Крім того, репутаційні збитки, спричинені витоком даних клієнтів, можуть призвести до втрати довіри та скорочення клієнтської бази. Відновлення репутації після таких інцидентів часто займає роки і потребує значних фінансових і людських ресурсів.

Особливістю віддаленого середовища є також складність масштабування систем безпеки. Багато організацій стикаються з труднощами адаптації існуючих рішень до нових умов через високу вартість або брак технічних ресурсів. Наприклад, організації можуть не мати достатніх можливостей для розгортання додаткових систем безпеки на пристроях співробітників, що підвищує вразливість до атак (див. рис. 1.1).

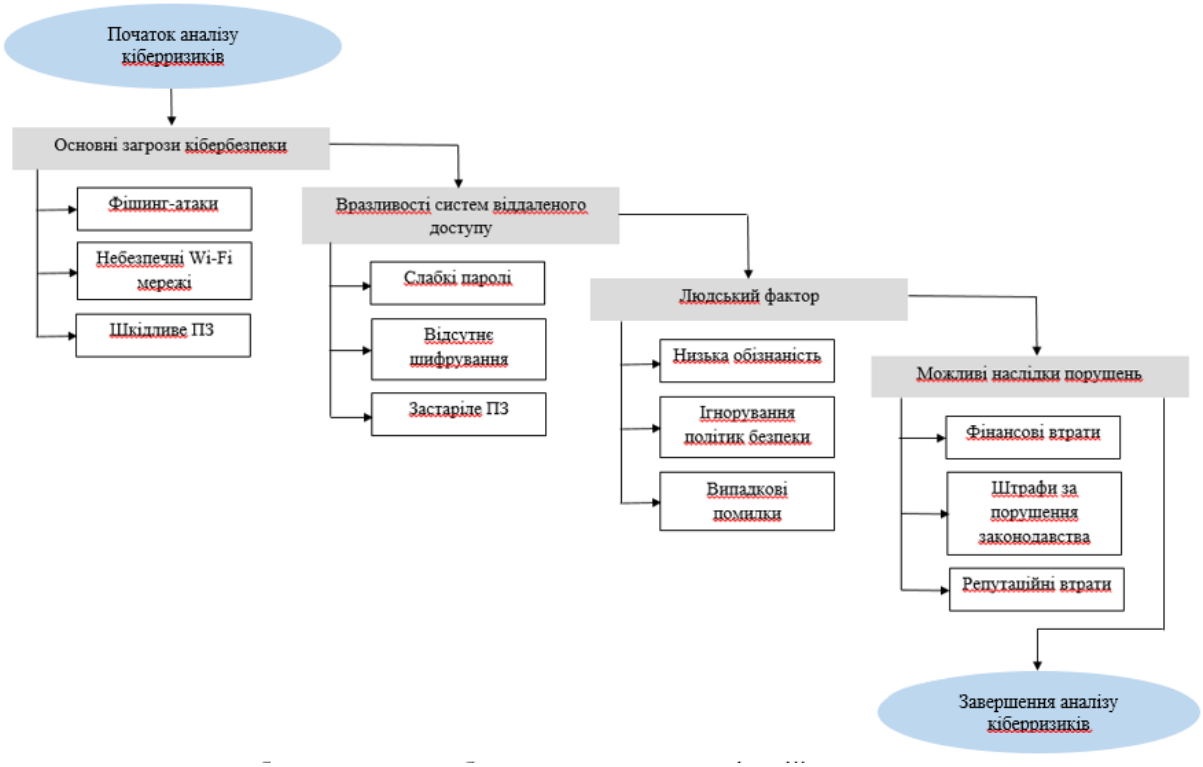

Рисунок 1.1 – Алгоритм аналізу кіберризиків

Віддалене середовище створює значні виклики для захисту конфіденційних даних і може призвести до серйозних кіберзагроз. Щоб мінімізувати ці ризики, необхідно впроваджувати комплексні рішення, які поєднують технічні засоби, такі як шифрування і двофакторну автентифікацію, з організаційними заходами, зокрема навчанням співробітників та розробкою чітких політик безпеки. Важливим є також використання управління ризиками в реальному часі, що дозволяє швидко реагувати на потенційні загрози.

1.1 Основні виклики кібербезпеки при віддаленій роботі

Віддалена робота стала важливим аспектом сучасної діяльності багатьох організацій, але вона також приносить низку викликів для забезпечення кібербезпеки. Зокрема, відсутність фізичного контролю над робочими місцями працівників, використання персональних пристроїв, а також слабка

обізнаність співробітників щодо кіберзагроз створюють додаткові труднощі в забезпеченні конфіденційності та цілісності даних.

Одним з найбільших викликів є використання персональних пристроїв для доступу до корпоративних систем. У таких пристроях часто відсутні необхідні засоби захисту, що може призвести до витоку конфіденційної інформації або зараження шкідливим програмним забезпеченням. Окрім того, багато працівників використовують незахищені публічні Wi-Fi мережі для доступу до корпоративних ресурсів, що робить їх вразливими до атак типу "людина посередині" (MITM), коли зловмисники можуть перехоплювати передавані дані [5].

Іншим важливим викликом є відсутність надійних методів автентифікації та контролю доступу до корпоративних систем. Використання простих паролів або їх повторення на різних платформах робить доступ до облікових записів вразливим. Без двофакторної автентифікації (2FA) або багатофакторної автентифікації (MFA) віддалений доступ до корпоративних систем залишається недостатньо захищеним. Це особливо важливо в умовах роботи з конфіденційними даними, коли кожен несанкціонований доступ може призвести до серйозних наслідків.

Ще одним викликом є відсутність регулярних оновлень програмного забезпечення на пристроях працівників. Підприємства часто не мають змоги контролювати, чи встановлюють їх співробітники останні оновлення безпеки на своїх пристроях, що створює вразливості для кіберзлочинців. Багато організацій також стикаються з проблемами масштабування рішень безпеки, коли традиційні методи захисту не можуть бути ефективно застосовані до віддалених працівників [5].

Людський фактор є однією з найбільших слабких ланок у системах безпеки. Працівники можуть бути недостатньо обізнаними щодо кіберзагроз, таких як фішинг або соціальна інженерія, і випадково надавати доступ до конфіденційної інформації. Недотримання політик безпеки, наприклад,

відкриття підозрілих електронних листів або натискання на зловмисні посилання, може призвести до серйозних наслідків для організації. Погане навчання співробітників, недостатня інформованість щодо кіберзагроз або відсутність політик захисту даних можуть зробити компанії вразливими до атак.

Багато організацій стикаються з труднощами у адаптації існуючих рішень безпеки до умов віддаленої роботи. Традиційні методи захисту, такі як використання корпоративних VPN або контролювання доступу через фаєрволи, часто не підходять для ефективного забезпечення безпеки в умовах, коли працівники використовують різноманітні пристрої і мережі для доступу до робочих ресурсів. Для ефективного захисту даних потрібно впроваджувати новітні технології, що дозволяють централізовано моніторити та управляти доступом, забезпечувати шифрування трафіку та стежити за діями користувачів у реальному часі [5].

Віддалена робота може призвести до порушень стандартів конфіденційності та нормативних вимог, таких як GDPR або HIPAA. Наприклад, збереження конфіденційної інформації на персональних пристроях без належного захисту, недотримання вимог щодо зберігання та передачі даних можуть призвести до штрафів та репутаційних збитків. Оскільки багато віддалених працівників не знають або ігнорують вимоги щодо захисту даних, ризик порушення цих стандартів стає значним.

Масштабування та управління безпекою в умовах віддаленої роботи потребують значних ресурсів. Підприємства повинні впроваджувати інтегровані рішення для моніторингу безпеки, впровадження політик доступу та проведення регулярних перевірок безпеки на всіх пристроях та платформах, до яких мають доступ віддалені працівники. Це вимагає великих затрат часу та ресурсів для ефективного виконання [5]. Що дозволяє систематизувати основні виклики, що виникають у процесі забезпечення кібербезпеки при

віддаленій роботі, а також пропонує можливі рішення для їх подолання показано нижче (див. табл. 1.1).

Таблиця 1.1 - Основні виклики кібербезпеки при віддаленій роботі

№	Виклик	Опис	Ризики	Можливі рішення
1	2	3	4	5
1	Використання незахищених пристроїв і мереж	Використання персональних пристроїв та публічних Wi-Fi мереж для доступу до корпоративних систем.	Перехоплення даних, зараження шкідливим ПЗ, атаки типу "людина посередині".	Впровадження VPN, шифрування даних, використання надійних паролів та двофакторної автентифікації.
2	Недостатня автентифікація та управління доступом	Відсутність надійних методів автентифікації та контролю доступу.	Несанкціонований доступ до корпоративних систем, крадіжка конфіденційної інформації.	Впровадження двофакторної та багатофакторної автентифікації, централізоване управління доступом.
3	Відсутність регулярного оновлення програмного забезпечення	Відсутність оновлень безпеки на пристроях працівників.	Вразливості, які можуть бути використані кіберзлочинцями для атак.	Автоматизація оновлень ПЗ, централізоване управління оновленнями.
4	Людський фактор	Недостатня обізнаність працівників щодо кіберзагроз, недотримання політик безпеки.	Фішингові атаки, випадковий витік конфіденційної інформації, неправомірний доступ через людську помилку.	Навчання співробітників, підвищення рівня обізнаності, регулярні тренінги з кібербезпеки.
5	Адаптація інфраструктури безпеки	Ускладнення адаптації існуючих рішень безпеки до умов віддаленої роботи.	Неефективний захист через застарілі методи безпеки, недостатній контроль за віддаленими пристроями.	Впровадження новітніх рішень безпеки, централізоване управління доступом, моніторинг діяльності.
6	Порушення стандартів конфіденційності та регуляцій	Недотримання вимог щодо захисту даних, збереження їх на	Штрафи за порушення законодавства,	Використання шифрування, регулярні перевірки,

Продовження таблиці 1.1

1	2	3	4	5
		незахищених пристроях або вразливих мережах.	репутаційні збитки, втрату довіри клієнтів.	впровадження політик конфіденційності та відповідності.
7	Масштабування та управління безпекою	Труднощі у масштабуванні систем безпеки для підтримки великої кількості віддалених працівників.	Відсутність єдиного контролю за безпекою, збільшення кількості уразливих точок для атак.	Автоматизація процесів безпеки, централізоване управління, інтеграція сучасних рішень кібербезпеки.

1.2 Вивчення загроз та вразливостей у системах дистанційного доступу

При віддаленій роботі значно зростають ризики для кібербезпеки, адже працівники мають доступ до корпоративних даних і систем із дому або інших локацій, що створює додаткові вразливості. Це, у свою чергу, відкриває нові можливості для зловмисників, які можуть скористатися слабкими місцями в системах захисту. В умовах сучасного професійного середовища віддалена робота стала невід'ємною частиною бізнес-процесів, що сприяє значному попиту на технології дистанційного офісу. Вони дають змогу працівникам з'єднуватися з корпоративними мережами, обмінюватися даними та виконувати необхідні завдання з будь-якої точки світу. Проте разом з такою зручністю з'являються й нові кіберзагрози, оскільки системи дистанційного офісу, як-от VPN (Virtual Private Network), RDP (Remote Desktop Protocol), а також різноманітні веб-сервіси, можуть бути вразливими до атак.

Однією з головних загроз є *неавторизований доступ* до корпоративних систем та даних. Працівники часто використовують особисті пристрої або домашні мережі для роботи, що може призвести до порушення політик безпеки, якщо ці пристрої не налаштовані належним чином. Слабкі паролі, недостатня аутентифікація або несанкціонований доступ можуть стати шляхом для зловмисників [6].

Іншою серйозною загрозою є *атаки типу "Man-in-the-Middle"*. Працівники часто підключаються до Інтернету через незахищені Wi-Fi мережі (наприклад, у громадських місцях), що дає можливість зловмисникам перехоплювати інформацію під час її передачі. Це може призвести до викрадення чутливих даних або маніпуляцій з ними.

Фішинг та соціальна інженерія також становлять значну небезпеку. Зловмисники використовують фальшиві електронні листи або повідомлення, що виглядають як офіційні комунікації від компанії, щоб обманом змусити співробітників розкрити свої облікові дані або іншу конфіденційну інформацію. Така атака може призвести до серйозних порушень безпеки.

Ще однією важливою загрозою є *зловмисне програмне забезпечення* — віруси, трояни або програмне забезпечення-вимагачі (ransomware). Віддалені працівники часто використовують не тільки робочі, але й особисті пристрої, які можуть бути недостатньо захищеними. Це може призвести до зараження корпоративних мереж або викрадення даних.

Незахищені хмарні сервіси теж створюють додаткові ризики. Використання хмарних платформ для зберігання даних без належного захисту може стати приводом для атак на корпоративну інформацію. Якщо доступ до таких сервісів не контролюється за допомогою надійної аутентифікації, це може призвести до витоку даних.

Також важливою загрозою є *втрата або крадіжка пристроїв*. Коли працівники використовують мобільні телефони або ноутбуки для доступу до корпоративних даних, у разі втрати або крадіжки таких пристроїв зловмисники можуть отримати доступ до конфіденційної інформації.

Не менш серйозною загрозою є *вразливості в системах дистанційного доступу*, таких як VPN. Якщо ці системи налаштовані неправильно або мають застарілі компоненти, вони можуть стати мішенню для хакерів, які намагаються отримати доступ до корпоративної мережі [6].

Нарешті, *людський фактор* є однією з найбільших загроз для безпеки. Навіть найсучасніші технології не зможуть убезпечити організацію, якщо працівники

ігнорують правила безпеки, використовують слабкі паролі або не звертають увагу на важливість регулярних оновлень програмного забезпечення (див. табл. 1.2).

Таблиця 1.2 - Загрози кібербезпеки при віддаленій роботі

№	Загрози кібербезпеки при віддаленій роботі	Опис
1	Неавторизований доступ	Порушення політики безпеки через слабкі паролі, несанкціонований доступ.
2	Атаки типу Man-in-the-Middle	Використання незахищених Wi-Fi мереж для перехоплення даних.
3	Фішинг	Обман користувачів за допомогою фальшивих повідомлень або листів.
4	Шкідливе ПЗ	Віруси, трояни, програмне забезпечення-вимагачі.
5	Вразливості хмарних сервісів	Ненадійне зберігання даних у хмарах без належного захисту.
6	Втрата або крадіжка пристроїв	Втрата або крадіжка ноутбуків, смартфонів, на яких зберігаються важливі дані.
7	Вразливості систем дистанційного доступу	Проблеми з VPN або іншими системами віддаленого доступу.

Основні вразливості в системах дистанційного доступу:

– *Слабкі паролі та автентифікація* - однією з найбільш поширених вразливостей є використання слабких паролів або паролів за замовчуванням, що значно підвищує ймовірність несанкціонованого доступу до системи. Багато організацій використовують прості паролі або не застосовують двофакторну автентифікацію (2FA), що значно збільшує ризик атаки методом підбору або перебору паролів.

– *Незахищений канал зв'язку* - якщо з'єднання між кінцевим користувачем і корпоративною мережею не є шифрованим, це може призвести до перехоплення важливої інформації, включаючи паролі та інші конфіденційні дані. Наприклад, атаки "Man-in-the-Middle", коли зловмисник перехоплює або змінює комунікацію між двома сторонами, можуть мати катастрофічні наслідки.

– *Вразливості в програмному забезпеченні* - системи дистанційного доступу можуть містити уразливості в своєму програмному забезпеченні, які зловмисники можуть використати для віддаленого виконання шкідливого коду або доступу до мережевих ресурсів. Уразливості можуть стосуватися не

лише основного програмного забезпечення, а й додаткових компонентів, таких як сервери та маршрутизатори.

– *Неактуальні оновлення та патчі* - відсутність регулярних оновлень та патчів на системах дистанційного доступу також є серйозною проблемою. Застарілі версії програмного забезпечення можуть містити відомі вразливості, які активно використовуються зловмисниками для доступу до корпоративної мережі.

– *Перехоплення сеансів* - відсутність належного захисту для сеансів користувачів може призвести до їх перехоплення зловмисниками. Якщо сеанс не захищений належним чином, зловмисники можуть отримати доступ до активних сесій або навіть до всієї системи.

– *Шкідливе програмне забезпечення на кінцевих пристроях* - кінцеві пристрої, через які здійснюється доступ до корпоративної мережі, можуть бути інфіковані шкідливим ПЗ. У разі, якщо пристрій користувача має вразливості або шкідливі програми, вони можуть стати канали для атак через систему віддаленого доступу.

– *Використання незахищених мереж* - віддалені з'єднання, здійснені через незахищені або публічні Wi-Fi мережі, значно збільшують ризик перехоплення переданих даних [7]. Зловмисники можуть використати ці мережі для здійснення атак типу "Man-in-the-Middle", що дає їм змогу зібрати чутливу інформацію або змінити дані, які передаються (див. рис. 1.2).

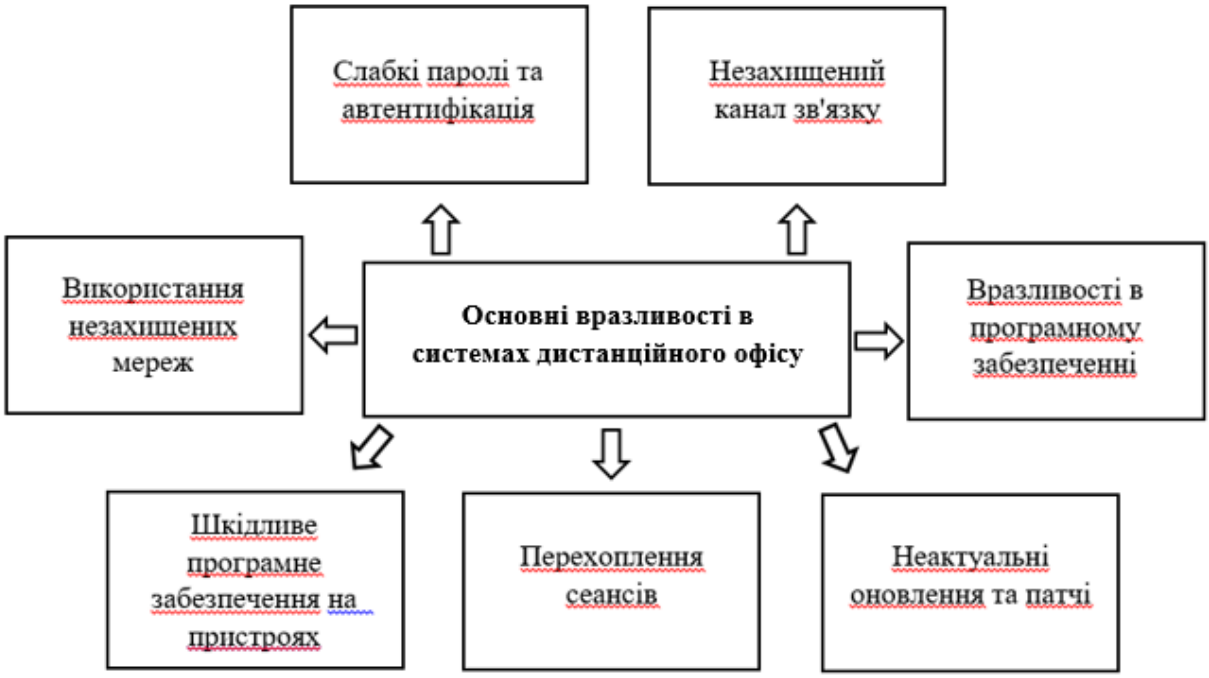

Рисунок 1.2 – Структура основних вразливостей в системах дистанційного офісу

Для забезпечення належного захисту від вразливостей у системах дистанційного доступу необхідно застосовувати комплекс заходів, спрямованих на підвищення рівня безпеки інформації та запобігання можливим атакам.

Шифрування каналу зв'язку є одним із основних заходів для захисту даних. Для цього слід використовувати системи, які забезпечують шифрування каналу зв'язку, наприклад, VPN з використанням сучасних протоколів шифрування, таких як OpenVPN або IPSec. Це дозволяє надійно захищати передану інформацію від перехоплення під час її трансферу через мережу.

Двофакторна автентифікація (2FA) значно підвищує рівень безпеки, оскільки вона передбачає використання двох незалежних методів для підтвердження особи користувача. Крім стандартного пароля, доцільно використовувати додаткові методи автентифікації, такі як смарт-карти, біометричні дані чи одноразові коди. Це значно зменшує ризик несанкціонованого доступу через компрометацію пароля.

Регулярні оновлення та патчі для програмного забезпечення та операційних систем є важливою частиною безпеки. Оновлення дозволяють закривати

вразливості, що можуть бути використані зловмисниками. Тому організації повинні забезпечити, щоб усі системи дистанційного доступу були актуальними та відповідали сучасним стандартам безпеки.

Захист кінцевих пристроїв також має важливе значення для запобігання інфікуванню шкідливим програмним забезпеченням та подальшим атакам. Встановлення антивірусних програм та програм для виявлення шкідливих програм на кінцевих пристроях користувачів дозволяє знизити ймовірність проникнення в систему через вразливості на стороні користувача.

Безпечні Wi-Fi мережі — використання надійних та захищених мереж є необхідною умовою для безпечного доступу до віддалених ресурсів. Для роботи з публічними Wi-Fi мережами необхідно обов'язково використовувати VPN-з'єднання, що дозволить захистити передану інформацію від перехоплення.

Контроль доступу та моніторинг активності є важливими заходами для виявлення та запобігання підозрілої активності. Регулярний моніторинг доступу до систем дистанційного доступу та ведення журналів безпеки дозволяє своєчасно виявляти аномальні спроби підключення, що може свідчити про зловмисну діяльність, та оперативно вживати необхідних заходів для мінімізації можливих загроз [8].

Захист систем дистанційного офісу є важливим елементом забезпечення кібербезпеки в умовах віддаленої роботи. Оскільки вразливості в таких системах можуть призвести до серйозних наслідків для організацій, важливо постійно впроваджувати нові методи захисту, проводити регулярні оновлення та забезпечити належний рівень автентифікації та шифрування даних. Адекватний захист цих систем допоможе знизити ризики несанкціонованого доступу та збереження конфіденційності інформації.

1.3 Наслідки реалізації кіберзагроз для організацій та фізичних осіб

Порушення конфіденційності даних є однією з найбільших загроз у сучасному цифровому світі, і вони можуть мати далекосяжні наслідки для всіх учасників інформаційних процесів — від організацій до індивідуальних користувачів. Наслідки порушень конфіденційності можуть варіюватися залежно від типу та масштабу порушення, а також від того, хто є його жертвою. Вони можуть бути як прямими, так і непрямими, впливаючи не тільки на безпеку даних, але й на фінансову стабільність, репутацію, юридичні та психологічні аспекти. Наслідки для організацій та фізичних осіб (див. додаток А табл. 1.3).

Порушення конфіденційності даних має глибокий вплив як на організації, так і на фізичних осіб. Ці наслідки можуть бути різноманітними та мати довгостроковий характер, що робить необхідним впровадження ефективних заходів для захисту даних і запобігання подібним інцидентам у майбутньому [9].

РОЗДІЛ 2 МЕТОДИ ОЦІНКИ РИЗИКІВ У ДИСТАНЦІЙНОМУ СЕРЕДОВИЩІ

Швидке впровадження дистанційної роботи в багатьох організаціях спричинило значне зростання кіберзагроз, що виникають унаслідок зміни традиційних підходів до управління інформаційною безпекою. Відсутність фізичного контролю над робочими пристроями, використання незахищених мереж і персональних гаджетів, а також обмежене адміністрування ресурсів створюють нові ризики для збереження конфіденційності, цілісності й доступності даних.

В умовах дистанційного середовища критично важливо вміти виявляти й оцінювати потенційні загрози, які можуть впливати на стабільність роботи IT-інфраструктури та безпеку даних. Для цього застосовуються різні методи оцінки ризиків, які дозволяють сформувати цілісну картину поточного стану інформаційної безпеки, визначити пріоритети захисту та розробити ефективні заходи з управління ризиками.

Аналіз ризиків вимагає врахування як технічних, так і організаційних чинників, зокрема особливостей використання хмарних технологій, політик доступу, рівня обізнаності працівників тощо. Людський фактор відіграє ключову роль у формуванні рівня кіберзагроз, особливо коли співробітники працюють поза межами захищеного середовища [10].

Розуміння типів ризиків, які виникають під час віддаленої роботи, а також використання адекватних моделей аналізу дозволяє зменшити ймовірність інцидентів, мінімізувати їх наслідки та підвищити загальний рівень захищеності інформаційних систем.

2.1 Теоретичні основи оцінки ризиків в інформаційній безпеці

Сучасна цифрова епоха вимагає від організацій усе більш відповідального підходу до захисту інформаційних ресурсів. Інформаційна безпека перестала бути лише технічним аспектом — сьогодні це комплексна

система, що включає організаційні, процедурні, правові та людські чинники. Особливої актуальності набуває процес оцінки ризиків, який дозволяє своєчасно виявляти потенційні загрози та приймати ефективні управлінські рішення щодо їх уникнення або мінімізації [10].

Ризик в інформаційній безпеці розглядається як ймовірність виникнення небажаної події, яка може порушити конфіденційність, цілісність або доступність інформації. При цьому рівень ризику визначається не лише самою загрозою, а й наявністю вразливостей у системі, через які ця загроза може реалізуватись. Іншими словами, ризик — це поєднання ймовірності події та наслідків, які вона може спричинити для організації [14]. Цей зв'язок можна представити у вигляді формули (2.1):

$$R=P\times I \qquad (2.1)$$

R — ризик,

P — ймовірність реалізації загрози,

I — величина потенційних збитків або впливу на систему.

Розрахунків ризиків для дистанційного офісу, дані по ймовірності та впливу наведено на (рис.2.)

№	Загроза	Ймовірність (P)	Вплив (I)	Потенційні збитки (R), грн
1	Фішинг	0,9	1	0,9
2	Малвера/Віруси	0,6	0,9	0,54
3	Незахищені Wi-Fi мережі	0,6	0,7	0,42
4	Атаки на системи віддаленого ддоступу	0,5	0,9	0,45
5	Невірне використання доступу	0,8	0,6	0,48
6	Відсутність регулярного оновлення ПО	0,7	0,8	0,56
7	Інсайдерські загрози	0,4	0,9	0,36

Рисунок 2.1 – Можливі вхідні дані

На основі наданої таблиці з оцінкою ризиків можна візуально побачити, за допомогою графіка, які загрози мають найбільший потенційний вплив на безпеку конфіденційних даних і де необхідно впроваджувати найбільш ефективні стратегії захисту (див. рис. 2.2).

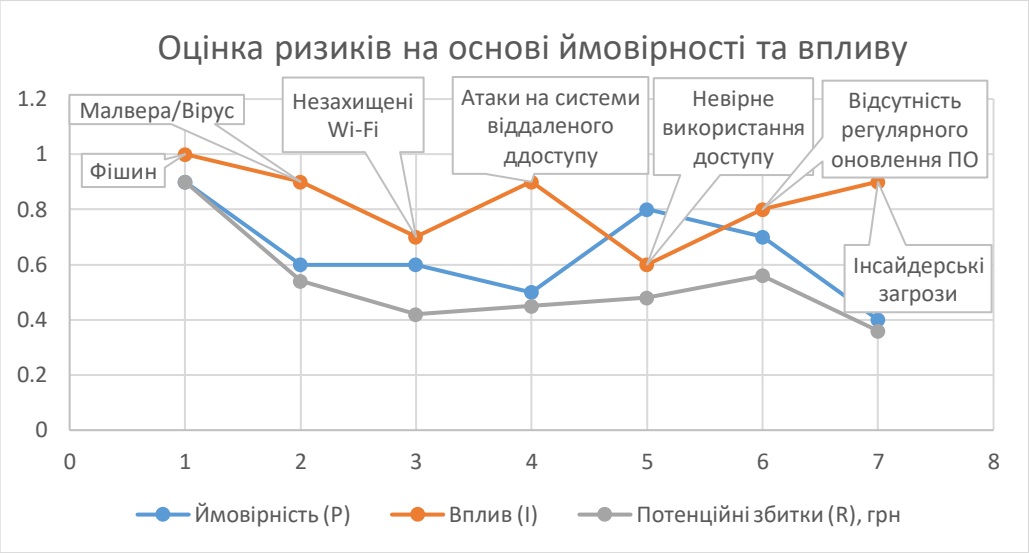

Рисунок 2.2 – Графік оцінки ризиків на основі ймовірності та впливу

Сумарні збитки у разі відсутності заходів безпеки будуть становити 3710000 грн.

На впровадження комплексної стратегії захисту даних передбачено витрати в розмірі 300000 грн.

Для оцінки доцільності впровадження заходів розраховано економічний ефект (E) та ROI (коефіцієнт окупності інвестицій).

Формула економічної ефективності:

$$E = \text{Потенційні збитки} - \text{Витрати} = 3710000 - 300000 = 3410000 \text{грн}. \quad (2.2)$$

Формула ROI (окупність інвестицій):

$$ROI = \frac{E}{\text{Витрати}} \times 100\% = \frac{3410000}{300000} \times 100\% = 1137\%. \quad (2.3)$$

Аналіз показує, що впровадження стратегії захисту конфіденційних даних у дистанційному офісі є надзвичайно вигідним та економічно доцільним. Застосування запропонованих заходів дозволяє зменшити потенційні збитки у 12 разів порівняно із ситуацією, коли такі заходи відсутні. Окупність інвестицій перевищує 1000%, що підтверджує ефективність розроблених рішень.

Впровадження запропонованої стратегії є не лише технічно виправданим, але й фінансово вигідним кроком для забезпечення сталого функціонування організації в умовах підвищених кіберризиків.

Для здійснення повноцінної оцінки ризиків важливо враховувати кілька ключових складових. По-перше, це активи — все, що має цінність для організації: дані, інформаційні системи, мережеве обладнання, персонал. По-друге, загрози — дії або події, здатні порушити нормальне функціонування системи. І, по-третє, вразливості — слабкі місця, через які загрози можуть бути реалізовані. Знання про ці компоненти дозволяє проводити структурований аналіз ризиків [10].

Існує декілька основних етапів оцінки ризиків. Спочатку відбувається ідентифікація активів, які потребують захисту. Далі проводиться аналіз потенційних загроз і наявних вразливостей, що дозволяє сформувати загальне уявлення про можливі сценарії розвитку подій. Наступним кроком є визначення ймовірності реалізації кожної загрози та оцінка потенційних збитків у разі її виникнення. На основі цих даних обчислюється рівень ризику, після чого приймаються рішення щодо заходів безпеки: ризик можна зменшити, уникнути, передати (наприклад, через страхування) або прийняти, якщо він знаходиться в межах прийнятного рівня. Цикл оцінки ризиків можна переглянути на (рис. 2.3).

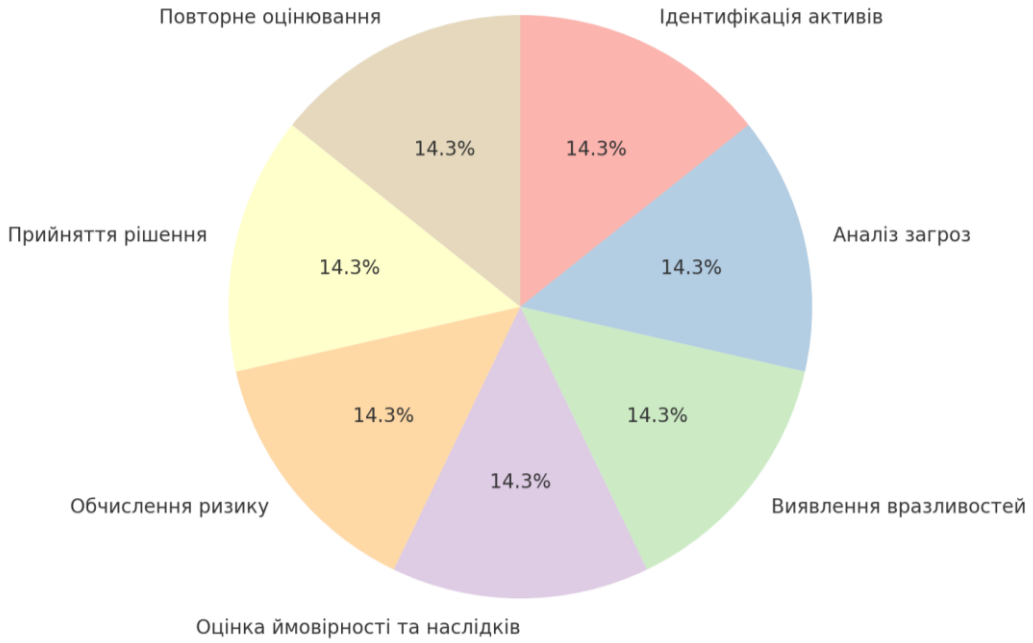

Рисунок 2.3 – Цикл оцінки ризиків

Залежно від наявної інформації та цілей аналізу, оцінка ризиків може здійснюватися якісним, кількісним або комбінованим методом. Якісний підхід передбачає використання експертних оцінок, матриць та шкал для визначення рівня загроз і пріоритетів захисту. Кількісний підхід ґрунтується на точних розрахунках та статистичних даних, дозволяючи визначити ризики у грошовому чи іншому числовому вираженні. Комбінований підхід поєднує переваги обох методів [14].

Варто зазначити, що оцінка ризиків є не разовою процедурою, а безперервним процесом. Зміни в IT-інфраструктурі, оновлення програмного забезпечення, поява нових загроз або зміни у структурі організації вимагають постійного перегляду й актуалізації результатів аналізу.

Для організації процесу оцінки ризиків у міжнародній практиці використовуються спеціалізовані стандарти, зокрема ISO/IEC 27001 і ISO/IEC 27005. Вони надають чіткі методичні рекомендації щодо побудови ефективної системи управління ризиками інформаційної безпеки. У Сполучених Штатах широко застосовується керівництво NIST SP 800-30, яке детально описує методологію аналізу ризиків для інформаційних систем [1].

Правильне розуміння теоретичних засад оцінки ризиків в інформаційній безпеці є базовим кроком для побудови надійної та стійкої системи захисту, особливо в умовах зростаючої ролі дистанційного доступу та гнучких моделей роботи.

2.2 Методи і моделі аналізу ризиків

Аналіз ризиків в інформаційній безпеці є ключовим етапом для виявлення вразливих місць у системах, особливо в умовах дистанційної роботи, коли організація не контролює фізичне середовище користувача. Існує чимало методів і моделей, які дозволяють систематизувати оцінку ризиків, враховуючи технічні, організаційні та людські чинники.

Однією з найпоширеніших методологій є модель FAIR (Factor Analysis of Information Risk). Вона базується на кількісному підході до оцінки ризиків і

дозволяє оцінити фінансові втрати від потенційних інцидентів. У контексті дистанційного офісу FAIR може бути застосована для оцінки ризиків, пов’язаних із використанням хмарних сервісів, наприклад, Google Drive чи Microsoft OneDrive. Ця модель дає змогу враховувати ймовірність витоку даних через фішинг, слабкі паролі чи компрометацію облікових записів, а також розрахувати фінансові збитки, пов’язані з такими інцидентами [15].

Ще одним ефективним інструментом є методологія OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), яка орієнтована на оцінку ризиків з організаційної точки зору. Вона передбачає аналіз активів, загроз і вразливостей, а також розробку політик та процедур безпеки. У віддалених умовах OCTAVE дозволяє виявити відсутність політик керування доступом, недостатню безпеку персональних пристроїв працівників (BYOD), використання незахищених мереж тощо, і на основі цього сформувати стратегію реагування.

У Сполучених Штатах широко використовується стандарт NIST SP 800-30, що надає структуровану методику ідентифікації, аналізу та оцінки ризиків інформаційних систем. Цей підхід ідеально підходить для оцінки технічної складової ризиків віддаленого доступу, наприклад, аналізу безпеки VPN-серверів, використання хмарної інфраструктури, систем віддаленого адміністрування тощо. NIST SP 800-30 дозволяє врахувати як технічні вразливості, так і зовнішні загрози (наприклад, атаки типу man-in-the-middle), а також обґрунтувати впровадження контрзаходів — шифрування трафіку, багатофакторної автентифікації тощо [3].

У випадках, коли необхідно змоделювати множину сценаріїв, доцільно використовувати метод Монте-Карло в комбінації з якісною оцінкою. Такий підхід дозволяє прораховувати варіанти розвитку подій на основі ймовірнісних даних і оцінити можливі втрати для компанії. Наприклад, можна змоделювати ризик компрометації облікових записів при використанні публічного Wi-Fi співробітником та визначити ефективність впровадження

додаткових заходів, таких як VPN або політика заборони з'єднання з відкритими мережами.

У таблиці 2.1 (див. табл. 2.1) наведено порівняння популярних методів аналізу ризиків, таких як OCTAVE, NIST SP 800-30, метод Монте-Карло, FAIR та якісна оцінка. Порівняння здійснюється за такими критеріями, як підхід до аналізу, рівень деталізації, вимоги до даних, сфера застосування та відповідність міжнародним стандартам [3].

Таблиця 2.1 - Порівняння методів аналізу ризиків

№	Метод	Підхід	Необхідні дані	Переваги	Недоліки	Сфера застосування
1	OCTAVE	Якісно-кількісний	Дані про активи, вразливості, загрози	Системний підхід, враховує людський фактор	Вимагає значного часу	Внутрішній аудит, стратегічний аналіз
2	NIST SP 800-30	Комбінований	Документація, статистика	Універсальний, адаптований до IT	Складність у реалізації	IT-інфраструктура, держустанови
3	FAIR	Кількісний	Статистика, оцінка збитків	Орієнтація на фінансові втрати	Складний для новачків	Бізнес-аналітика, страхування
4	Монте-Карло	Кількісний (статистичне моделювання)	Статистичні дані, сценарії	Дає точні числові оцінки	Потрібні обчислювальні ресурси	Прогнозування, складні системи
5	Якісний метод	Експертна оцінка	Мінімум даних	Простота, швидкість	Суб'єктивність	Початковий аналіз, малий бізнес

Для полегшення вибору методу аналізу ризиків можна використовувати блок-схему (рис. 2.4), яка дозволяє визначити найбільш доцільний підхід.

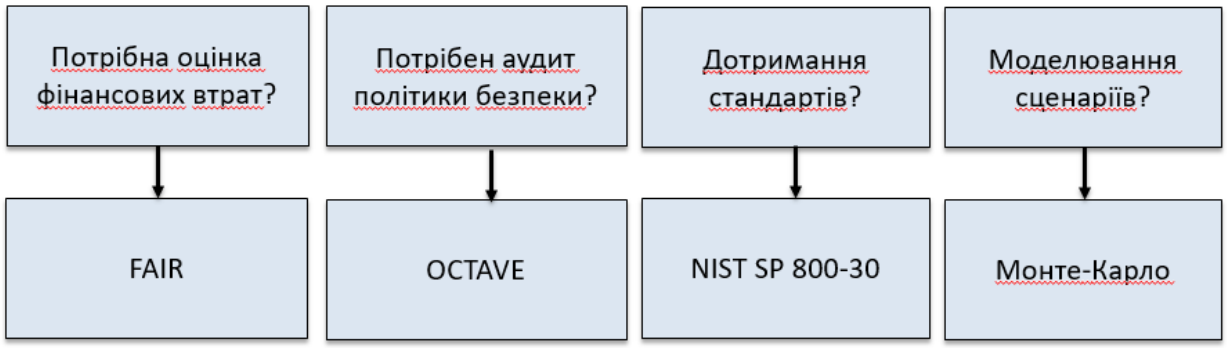

Рисунок 2.4 – Вибір методу аналізу ризиків

Вибір конкретного методу або моделі аналізу ризиків залежить від рівня доступної інформації, цілей аналізу та специфіки IT-інфраструктури організації. У контексті дистанційного офісу доцільним є комбінування кількісних і якісних методів, що дозволяє не лише формально оцінити ризики, а й адаптувати безпекову стратегію до реальних умов роботи співробітників поза межами корпоративного середовища.

2.3 Класифікація ризиків у віддаленому середовищі

З поширенням дистанційної роботи інформаційна безпека організацій зазнала значних змін. Перехід від централізованих інфраструктур до розподілених робочих середовищ створив нові ризики та підвищив вразливість до вже відомих загроз. Для ефективного управління безпекою в таких умовах важливо класифікувати ризики, щоб структуровано оцінити потенційні загрози та спланувати адекватні заходи реагування.

Класифікація ризиків у віддаленому середовищі може здійснюватися за кількома ознаками. Одним із критеріїв є джерело походження ризику. Технічні ризики пов’язані з несправністю обладнання, вразливостями програмного забезпечення, відсутністю оновлень або належного шифрування. Організаційні ризики виникають через недостатній контроль над діяльністю співробітників, відсутність політик безпеки для дистанційної роботи або неузгодженість у процесах доступу. Людський фактор включає помилки користувачів, небезпеку соціальної інженерії (наприклад, фішинг, скімінг) та низький рівень обізнаності з питань безпеки. Фізичні ризики можуть включати крадіжку чи втрату пристроїв або несанкціонований фізичний доступ до обладнання в домашніх умовах [16].

Іншим важливим критерієм класифікації є об'єкт впливу. Ризики для конфіденційності включають витік персональних даних чи чутливої інформації, що може серйозно вплинути на репутацію компанії. Ризики для цілісності виникають, коли дані несанкціоновано редагуються або спотворюються. Ризики для доступності пов'язані з відмовою в

обслуговуванні (DoS/DDoS) або втратою доступу через несправність каналів зв'язку чи обладнання.

Ризики можна класифікувати також за способом реалізації загрози. Внутрішні ризики пов'язані з діями працівників (як навмисними, так і випадковими), що можуть порушити безпеку. Зовнішні ризики зумовлені атаками з боку кіберзлочинців, шкідливим програмним забезпеченням чи інструментами, які використовуються хакерами.

Крім того, ризики можна оцінювати за ймовірністю виникнення та впливом. Низький ризик має малу ймовірність виникнення загрози і незначний вплив, середній ризик характеризується помірною ймовірністю та впливом, а високий і критичний ризики передбачають велику ймовірність загрози та суттєві наслідки, такі як порушення безперервності бізнесу або великі фінансові втрати [16].

Особливо важливими є соціальні ризики, зокрема психологічний вплив на працівників, який може виникнути через ізоляцію, стрес від постійної доступності або розмивання меж між роботою та особистим життям. Це може негативно вплинути на загальний рівень кібергігієни працівників та їх здатність протистояти кіберзагрозам (див. рис. 2.5).

Рисунок 2.5 – Класифікація ризиків у віддаленому середовищі

Завдяки класифікації ризиків можна побудувати ефективну модель захисту, визначити пріоритети для реагування та обрати відповідні заходи мінімізації загроз. Вона також є основою для подальшого кількісного чи якісного аналізу ризиків в управлінні інформаційною безпекою віддаленого офісу.

2.4 Вплив людського фактора на рівень кіберризиків

Людський фактор є одним із ключових елементів, що впливає на рівень кіберризиків, особливо в умовах віддаленої роботи. Незалежно від рівня технологічного захисту, саме дії користувачів часто стають вирішальним чинником у виникненні інцидентів інформаційної безпеки. Це зумовлено як навмисними, так і ненавмисними діями, що можуть призвести до витоку, спотворення або втрати даних.

Одним із найбільш поширених проявів людського фактора є низький рівень обізнаності користувачів з питань кібербезпеки. Працівники можуть не розпізнавати фішингові листи, користуватися слабкими паролями або нехтувати вимогами безпеки при роботі з корпоративною інформацією. У віддаленому середовищі, де контроль з боку IT-відділу обмежений, такі дії можуть призвести до серйозних наслідків [17].

Іншим аспектом є психологічний стан працівників. Відчуття ізоляції, перевтома, зниження концентрації, стрес від постійної доступності — усе це може знижувати уважність та здатність адекватно реагувати на потенційні загрози. Наприклад, втомлений працівник з більшою ймовірністю відкриє підозріле посилання або надасть доступ до конфіденційної інформації без належної перевірки.

Соціальна інженерія є ще одним фактором, що активно використовує людську вразливість. Кіберзлочинці все частіше вдаються до маніпуляцій, аби змусити жертву добровільно розкрити важливу інформацію або виконати небезпечні дії. Це може бути як через електронну пошту, так і через телефонні дзвінки або повідомлення в месенджерах.

Також варто враховувати організаційні аспекти, зокрема відсутність чітких політик та процедур, недостатню увагу до навчання персоналу та відсутність культури безпеки в компанії. Якщо працівники не усвідомлюють важливість дотримання правил безпеки, вони не сприйматимуть її як пріоритет.

У дослідженнях, проведених IBM за період 2020–2025 років, було виявлено, що людський фактор є однією з основних причин кіберінцидентів. За даними дослідження, відсоток інцидентів, які виникають через дії співробітників (як навмисні, так і випадкові), поступово зростає [18]. Наприклад, аналіз даних показав, що у 2020 році близько 93% кіберінцидентів можна було пов’язати з людським фактором, а до 2025 року ця цифра зросла до 98%. Код для побудови діаграми по аналізу даних представлений на (рис. 2.6).

```python
import matplotlib.pyplot as plt

# Роки дослідження
years = [2020, 2021, 2022, 2023, 2024, 2025]
# Дані у відсотках, які відображають частку інцидентів, спричинених людським фактором
incident_rates = [93, 94, 95, 96, 97, 98]

plt.figure(figsize=(10, 6))
bars = plt.bar(years, incident_rates, color='#4A90E2', edgecolor='black')

# Додавання значень над стовпчиками
for bar in bars:
    yval = bar.get_height()
    plt.text(bar.get_x() + bar.get_width()/2.0, yval + 0.2, f'{yval}%', ha='center', va='bottom', fontsize=12)

plt.xlabel('Рік', fontsize=14)
plt.ylabel('Частка інцидентів (%)', fontsize=14)
plt.title('Інциденти через людський фактор (за даними IBM, 2020-2025)', fontsize=16)
plt.ylim(90, 100)
plt.grid(axis='y', linestyle='--', alpha=0.7)

plt.tight_layout()
plt.show()
```

Рисунок 2.6 – Код на Python з використанням бібліотеки matplotlib, який створює стопчасту діаграму із даними за 2020–2025 роки.

Для наочності цієї тенденції було створено стопчасту діаграму, яка демонструє зміну рівня інцидентів за цей період. На діаграмі на осі X відзначені роки (2020–2025), а осі Y – відсоткова частка інцидентів, пов'язаних із людським фактором. Зростання значень відображає те, що незважаючи на технічні заходи захисту, проблема недостатньої обізнаності, впливу стресу та втоми, а також недотримання політик безпеки з боку співробітників залишається актуальною (див. рис. 2.7).

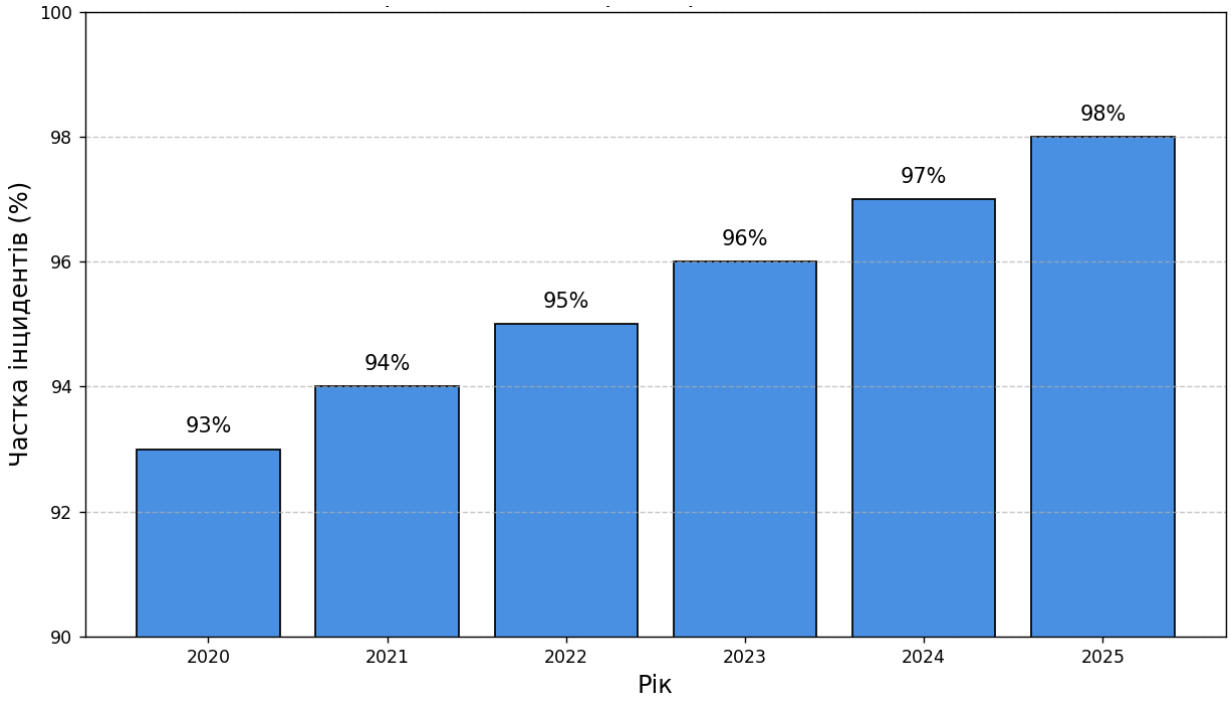

Рисунок 2.7 – Інциденти через людський фактор

Включення даної стопчастої діаграми до підрозділу дозволяє підкреслити наступне:

- Суттєва роль людського фактора - незважаючи на впровадження сучасних технологій захисту, поведінка співробітників продовжує залишатися ключовим чинником ризику.
- Тенденція зростання ризиків - поступове збільшення відсоткового показника інцидентів свідчить про необхідність постійного вдосконалення політик безпеки та проведення регулярних навчань.
- Необхідність інтегрованого підходу - дані свідчать про те, що лише комплексна стратегія, що включає як технічні, так і організаційні заходи, а також психологічну підтримку персоналу, може ефективно знизити рівень кіберризиків [18].

Людський фактор є багатогранним явищем, що охоплює як поведінкові, так і психологічні та організаційні аспекти. Для зниження рівня кіберризиків необхідно здійснювати постійне навчання працівників, формувати культуру безпеки, створювати зручні й ефективні політики та забезпечувати психологічну підтримку персоналу. Лише комплексний підхід дозволить мінімізувати вплив людського чинника на інформаційну безпеку у віддаленому середовищі.

РОЗДІЛ 3 СПОСОБИ МІНІМІЗАЦІЇ ВПЛИВУ КІБЕРЗАГРОЗ

Поширення дистанційного формату роботи зумовило необхідність перегляду підходів до забезпечення інформаційної безпеки. Зростання кількості кіберзагроз, зокрема фішингових атак, несанкціонованого доступу, використання шкідливого програмного забезпечення та вразливостей систем віддаленого доступу, вимагає застосування ефективних методів мінімізації їх впливу.

Забезпечення захисту інформаційних систем потребує поєднання технічних рішень, організаційних заходів та дотримання міжнародних стандартів. До технічних засобів належать засоби шифрування трафіку, багатофакторна автентифікація, системи виявлення та запобігання атак, антивірусне програмне забезпечення, регулярне оновлення систем і захист кінцевих пристроїв. Організаційні заходи включають розробку політик доступу, навчання персоналу основам кібергігієни, контроль за дотриманням правил безпеки, а також створення резервних копій даних.

Важливою складовою підвищення рівня захищеності є впровадження нормативно-правових вимог і міжнародних стандартів, таких як ISO/IEC 27001, GDPR, рекомендації NIST. Вони визначають вимоги до управління ризиками, моніторингу інформаційних потоків, захисту персональних даних та реагування на інциденти [13].

Комплексне застосування технічних, організаційних і нормативних підходів дає змогу суттєво зменшити ймовірність реалізації кіберзагроз і забезпечити стабільне функціонування інформаційної інфраструктури в умовах віддаленої роботи.

3.1 Технічні засоби захисту інформаці

Забезпечення кібербезпеки в умовах дистанційної роботи неможливе без впровадження ефективних технічних засобів захисту інформації. Основними інструментами є технології, що забезпечують конфіденційність, цілісність і доступність даних при їх передачі, обробці та зберіганні. У цьому контексті

особливого значення набуває використання віртуальних приватних мереж (VPN), багатофакторної автентифікації (2FA), систем виявлення та запобігання атак (IDS/IPS), а також антивірусного програмного забезпечення.

VPN (Virtual Private Network) — це технологія, що дозволяє створювати захищене з'єднання поверх відкритої мережі Інтернет. Вона забезпечує шифрування переданих даних, приховування IP-адреси користувача, а також захищає від несанкціонованого доступу до інформаційних ресурсів. Сучасні реалізації VPN використовують протоколи, такі як OpenVPN, L2TP/IPSec, WireGuard, які забезпечують високу стійкість до атак і надійний захист комунікацій. Для віддалених працівників VPN є обов'язковим інструментом безпечного підключення до внутрішніх корпоративних ресурсів [19].

Багатофакторна автентифікація (2FA) є ще одним важливим елементом технічного захисту. Вона базується на принципі використання двох або більше незалежних факторів для підтвердження особи користувача: знання (пароль), володіння (мобільний телефон, токен) або біометричні дані (відбиток пальця, розпізнавання обличчя). Впровадження 2FA значно ускладнює можливість несанкціонованого доступу, навіть у випадку компрометації пароля. Серед популярних методів автентифікації — SMS-коди, мобільні додатки (Google Authenticator, Authy), апаратні ключі (YubiKey) [19].

Системи виявлення та запобігання вторгненням (IDS/IPS) виконують функції моніторингу мережевого трафіку та виявлення підозрілої активності. IDS (Intrusion Detection System) лише фіксує факти вторгнення, тоді як IPS (Intrusion Prevention System) може автоматично блокувати загрози в реальному часі. Ці системи використовують сигнатурні та поведінкові методи аналізу для виявлення атак, таких як сканування портів, спроби експлуатації вразливостей, DDoS-атаки тощо. Їх інтеграція в мережеву інфраструктуру значно підвищує рівень захищеності організації від зовнішніх і внутрішніх загроз [20].

Антивірусне програмне забезпечення забезпечує захист кінцевих пристроїв користувачів від шкідливого програмного забезпечення, включаючи віруси, трояни, програмне забезпечення-вимагачі (ransomware), шпигунські програми (spyware) та інші типи загроз. Сучасні антивіруси мають функції проактивного виявлення на основі евристичного аналізу та машинного навчання, що дозволяє виявляти нові, ще не класифіковані типи шкідливого ПЗ. В умовах віддаленої роботи використання надійного антивірусу на кожному пристрої працівника є критично важливим для запобігання проникненню загроз у корпоративну мережу [21]. Взаємодія цих засобів (див.рис. 3.1).

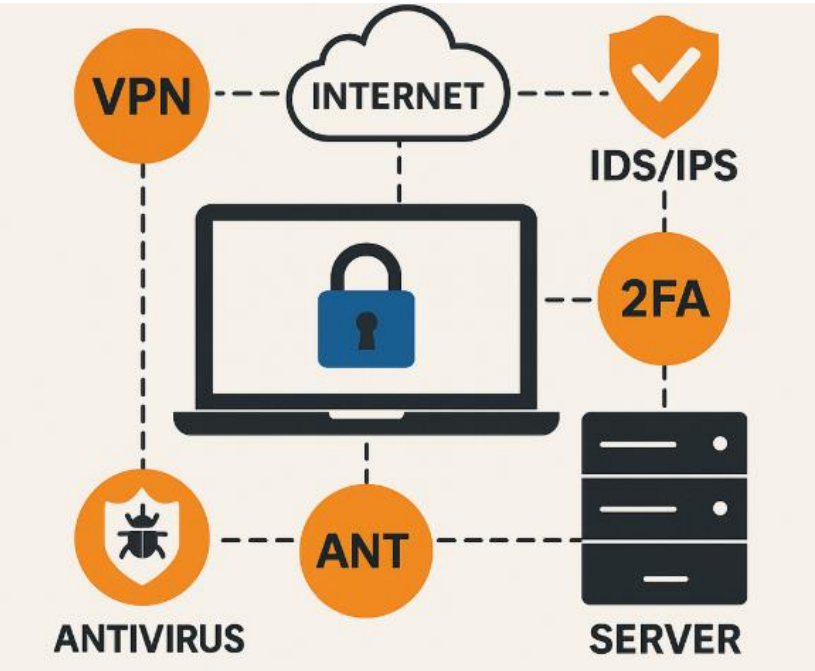

Рисунок 3.1 - Схема технічних засобів захисту інформації у віддаленому середовищі

Додатковими технічними засобами захисту виступають:

- Системи шифрування даних — як на рівні зберігання (наприклад, BitLocker, VeraCrypt), так і при передачі (TLS/SSL).
- Автоматизація оновлень — регулярне встановлення патчів та оновлень програмного забезпечення дозволяє закривати відомі вразливості.

- Брандмауери (фаєрволи) — блокують небажані з’єднання та фільтрують трафік відповідно до політик безпеки.
- Системи управління кінцевими точками (EDR, MDM) — забезпечують централізований контроль, моніторинг і оновлення пристроїв, які використовують працівники поза корпоративною мережею [22].

Комплексне використання зазначених технічних засобів дозволяє створити багаторівневу систему захисту, яка значно ускладнює реалізацію кібератак та підвищує стійкість інформаційної інфраструктури до потенційних загроз.

3.2 Організаційні заходи кібербезпеки

У контексті забезпечення кібербезпеки в умовах дистанційної роботи важливу роль відіграють не лише технічні засоби захисту, але й організаційні заходи, які спрямовані на формування стійкої інформаційної культури в колективі, регламентацію доступу до інформаційних ресурсів та гарантування збереження даних. До таких заходів належать навчання персоналу, контроль доступу до інформаційних систем, а також впровадження політик резервного копіювання.

Одним із ключових організаційних аспектів є підвищення рівня обізнаності працівників щодо актуальних кіберзагроз. Низька поінформованість персоналу часто є причиною реалізації соціально-інженерних атак, таких як фішинг, а також сприяє поширенню шкідливого програмного забезпечення через ненавмисні дії користувачів. Тому регулярне проведення навчальних семінарів, тренінгів, тестувань та інструктажів з основ інформаційної безпеки сприяє зменшенню ймовірності інцидентів, пов’язаних із людським фактором. У процесі навчання акцент робиться на формування навичок розпізнавання фішингових повідомлень, дотримання політик створення надійних паролів, безпечного використання електронної пошти, а також розуміння важливості застосування двофакторної автентифікації [23].

Ще одним критично важливим елементом є організація ефективного контролю доступу до корпоративних ресурсів. Забезпечення принципу мінімальних привілеїв, при якому кожному співробітнику надається доступ лише до тих даних і систем, що необхідні для виконання його посадових обов’язків, дозволяє мінімізувати ризики внутрішніх загроз. Застосування централізованого управління обліковими записами, журналювання дій користувачів, а також використання сучасних механізмів автентифікації (наприклад, багатофакторної автентифікації) підвищують рівень безпеки у віддаленому середовищі. Умови роботи за межами корпоративної інфраструктури вимагають впровадження засобів геолокаційного контролю доступу, захисту кінцевих пристроїв та автоматичного завершення сесії при виявленні підозрілої активності [24].

Нарешті, невід’ємною частиною організаційної безпеки є впровадження системи резервного копіювання даних. Забезпечення безперервності бізнес-процесів у разі реалізації кіберзагроз, таких як атаки програм-вимагачів або втрати даних унаслідок збоїв систем, неможливе без надійного механізму резервування. У цьому контексті застосовується так зване правило "3-2-1": зберігання трьох копій даних на двох різних носіях, одна з яких повинна бути віддаленою або ізольованою від основної мережі. Особливу увагу слід приділяти автоматизації процесів створення резервних копій, перевірці цілісності збережених даних, а також періодичному тестуванню процедур відновлення. В умовах дистанційної роботи резервне копіювання має відбуватись централізовано з використанням хмарних сховищ або корпоративних серверів з обмеженим доступом. Порівняння ключових показників стану безпеки до та після впровадження організаційних заходів наведено в таблиці 3.1. Як видно з рисунка 3.2, найвищу ефективність у зниженні ризиків демонструє впровадження системи резервного копіювання, що дозволяє уникнути втрати даних у разі реалізації кіберзагроз [25].

Таблиця 3.1 - Порівняння показників до та після впровадження організаційних заходів кібербезпеки

№	Показник	До впровадження	Після впровадження
1	Кількість інцидентів	Висока	Зменшується на 60–80%
2	Рівень обізнаності	Низький	Високий (після тренінгів)
3	Безпека даних	Нестабільна	Стабільна (з резервом)
4	Контроль над доступом	Частковий	Централізований

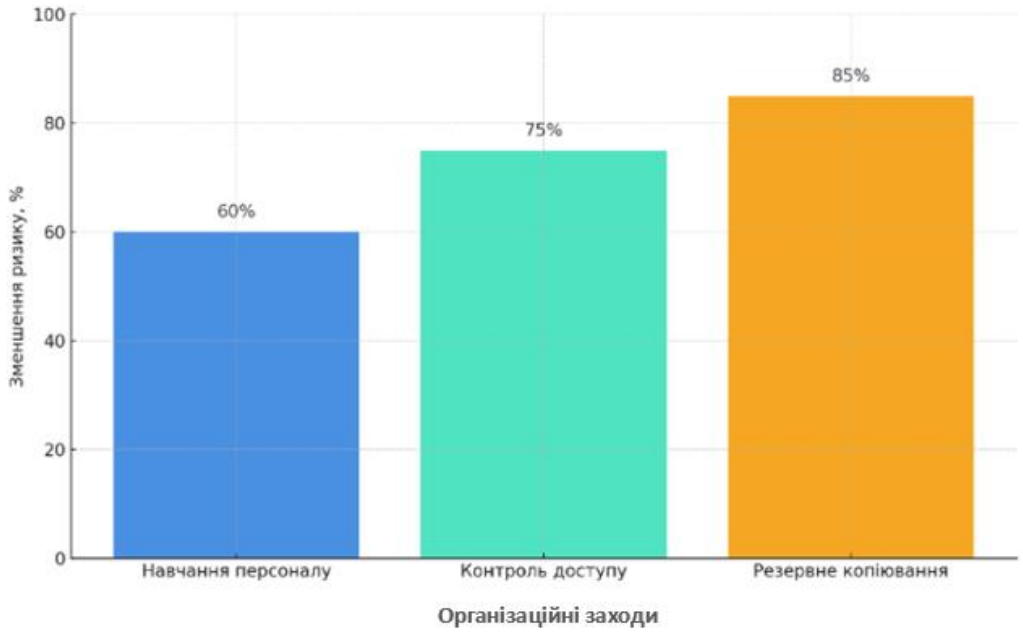

Рисунок 3.2 - Зменшення рівня кіберризику після впровадження організаційних заходів кібербезпеки

Організаційні заходи кібербезпеки виступають ключовим інструментом забезпечення стійкості інформаційної інфраструктури до сучасних загроз. Їхнє впровадження дозволяє значно зменшити вплив людського фактора, підвищити ефективність управління доступом та забезпечити збереження критичних даних навіть у разі реалізації складних сценаріїв атак. Комплексний підхід до організації безпеки, що поєднує освітні, адміністративні та технічні аспекти, є необхідною умовою стабільного функціонування організацій у дистанційному режимі.

3.3 Використання стандартів та нормативних вимог

У сучасних умовах функціонування організацій забезпечення кібербезпеки неможливе без дотримання міжнародних стандартів та нормативно-правових вимог. Їх використання дозволяє структурувати заходи захисту інформації, узгодити політики безпеки з кращими світовими практиками, а також знизити ризики юридичної відповідальності за порушення правил обробки та зберігання персональних даних [26].

Одним із найвідоміших нормативно-правових документів є Загальний регламент захисту даних Європейського Союзу (General Data Protection Regulation, GDPR), який набув чинності у 2018 році. Основною метою GDPR є захист персональних даних фізичних осіб та встановлення чітких правил щодо їх обробки. У контексті дистанційної роботи вимоги GDPR є особливо актуальними, адже працівники можуть обробляти чутливу інформацію поза межами захищеного середовища. Основні положення регламенту включають необхідність отримання згоди на обробку персональних даних, право на доступ, зміну та видалення даних, а також зобов’язання повідомляти про витік даних протягом 72 годин. Недотримання вимог GDPR може призвести до значних штрафних санкцій, що сягають до 20 мільйонів євро або 4% річного доходу компанії [4].

Для систематизації заходів з управління інформаційною безпекою широкого поширення набув міжнародний стандарт ISO/IEC 27001, який визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Цей стандарт передбачає ідентифікацію активів, оцінку ризиків, розробку політик безпеки, впровадження технічних і організаційних заходів захисту, а також аудит та моніторинг ефективності СУІБ. У контексті дистанційної роботи ISO 27001 допомагає адаптувати політики безпеки до гібридного або віддаленого формату, забезпечити захист кінцевих пристроїв, контролювати доступ до хмарних ресурсів і впроваджувати багатофакторну автентифікацію. Важливим

аспектом є також ведення документації та постійна оцінка ефективності впроваджених заходів [1].

Ще одним вагомим джерелом стандартів у сфері кібербезпеки є рекомендації Національного інституту стандартів і технологій США (NIST). Зокрема, документ NIST SP 800-53 надає детальний перелік контролів безпеки для інформаційних систем, а NIST SP 800-30 описує методику управління ризиками. У NIST-стандартах наголос робиться на побудові захищеної IT-архітектури, управлінні вразливостями, обробці інцидентів, а також на безперервності бізнесу. Для організацій, що використовують віддалений доступ, рекомендації NIST можуть бути використані як основа для впровадження сучасних технологій захисту, таких як Zero Trust Architecture, VPN з багатофакторною автентифікацією, політики least privilege тощо [3]. Узагальнені характеристики стандартів GDPR, ISO/IEC 27001 та NIST наведено в таблиці 3.2.

Таблиця 3.2 - Порівняльна стандартів (GDPR, ISO 27001, NIST)

№	Критерій	GDPR	ISO/IEC 27001	NIST SP 800-30 / 53
1	Тип	Закон ЄС	Міжнародний стандарт	Методологічні рекомендації (США)
2	Основна мета	Захист персональних даних	Управління інформаційною безпекою	Управління ризиками, контролі безпеки
3	Обов’язковість	Обов’язковий для ЄС	Добровільний, але часто потрібен для аудиту	Добровільний, але визнаний стандарт
4	Основні принципи	Згода, прозорість, право на забуття	Оцінка ризиків, політики безпеки	Захист систем, оцінка вразливостей
5	Штрафи за порушення	До 20 млн € або 4% річного доходу	Немає штрафів, але впливає на репутацію	Немає штрафів, використовується у держсекторі

Використання вищезазначених стандартів забезпечує:

- відповідність сучасним вимогам безпеки;
- зменшення ризику штрафів і юридичних наслідків;

– побудову системи безпеки, здатної протистояти актуальним загрозам;
– підвищення довіри з боку клієнтів і партнерів [11].

Охоплення основних напрямів дії зазначених стандартів наведено на рисунку 3.3.

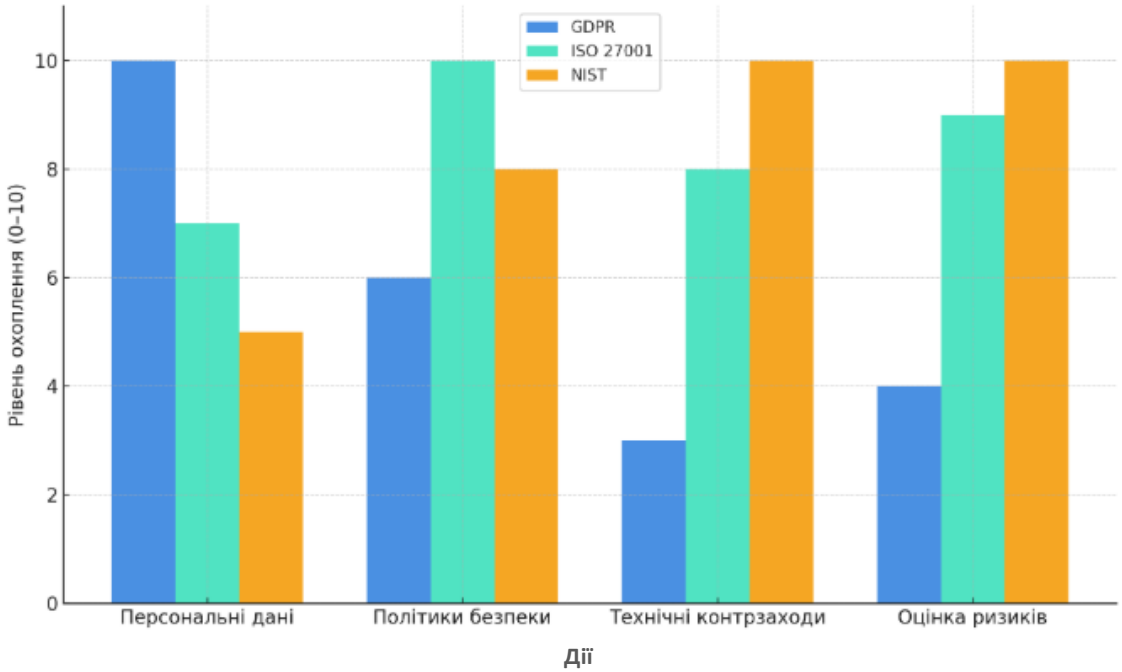

Рисунок 3.3 - Охоплення різних сфер дії стандартів кібербезпеки

Інтеграція стандартів GDPR, ISO/IEC 27001 та NIST у внутрішні політики організації сприяє формуванню комплексного підходу до кібербезпеки, особливо в умовах віддаленого доступу. Вони створюють нормативну базу, що дозволяє ефективно керувати ризиками, забезпечувати конфіденційність, цілісність і доступність інформації, а також своєчасно реагувати на потенційні інциденти [12].

РОЗДІЛ 4 РОЗРОБКА СИСТЕМИ ОЦІНКИ РИЗИКІВ ТА ЗАХОДІВ БЕЗПЕКИ

В умовах стрімкого зростання обсягів обробки конфіденційної інформації та широкого впровадження дистанційних форматів роботи актуалізується проблема забезпечення надійного захисту даних в інформаційно-цифровому середовищі. Забезпечення інформаційної безпеки потребує системного підходу до управління ризиками, який охоплює процеси ідентифікації активів, виявлення загроз, оцінки вразливостей, аналізу потенційних наслідків та вибору адекватних заходів реагування.

Раціональна побудова стратегії захисту конфіденційної інформації передбачає використання як якісних, так і кількісних методів оцінки ризиків, що дозволяє формалізувати процес прийняття рішень у сфері кібербезпеки. При цьому важливого значення набуває економічне обґрунтування впровадження відповідних заходів, з урахуванням можливих фінансових втрат у разі реалізації кіберзагроз.

Метою подальшого викладу є розробка логічно обґрунтованої системи оцінки ризиків та вибору заходів захисту, яка базується на принципах інформаційної безпеки та враховує специфіку функціонування організацій в умовах віддаленого доступу. Такий підхід забезпечує підвищення кіберстійкості інформаційної інфраструктури та дозволяє мінімізувати вплив як зовнішніх, так і внутрішніх загроз.

4.1 Алгоритм побудови стратегії захисту конфіденційних даних

Побудова ефективної стратегії захисту конфіденційної інформації є ключовим елементом забезпечення кібербезпеки в умовах дистанційного функціонування організацій. Така стратегія повинна базуватися на системному підході до управління ризиками, який включає ідентифікацію активів, виявлення загроз, оцінку вразливостей, розрахунок рівня ризику та вибір відповідних заходів реагування.

Першим етапом побудови стратегії є ідентифікація інформаційних активів, які підлягають захисту. До таких активів належать: персональні дані співробітників і клієнтів, фінансова документація, інтелектуальна власність, бази даних, поштові скриньки, віддалені сервери тощо.

На другому етапі здійснюється виявлення потенційних загроз, які можуть вплинути на цілісність, доступність або конфіденційність цих активів. Загрози класифікуються на зовнішні (хакерські атаки, фішинг, зловмисне ПЗ) та внутрішні (людський фактор, навмисні дії співробітників, недотримання політик).

Далі виконується оцінка вразливостей — тобто аналіз слабких місць у системі захисту, які можуть бути використані для реалізації загроз. Наприклад, відсутність багатофакторної автентифікації, слабке шифрування, неоновлене програмне забезпечення, або погано налаштовані права доступу [27].

Після цього переходять до розрахунку ризику за формулою:

$$R=P\times I \tag{4.1}$$

R — рівень ризику,

P — ймовірність реалізації загрози,

I — очікуваний вплив або збитки.

На основі розрахунків формується матриця ризиків (див. рис. 4.1), яка дозволяє візуалізувати критичність кожного ризику за двома критеріями — ймовірністю виникнення і рівнем впливу. Це дозволяє визначити пріоритетність у виборі заходів безпеки.

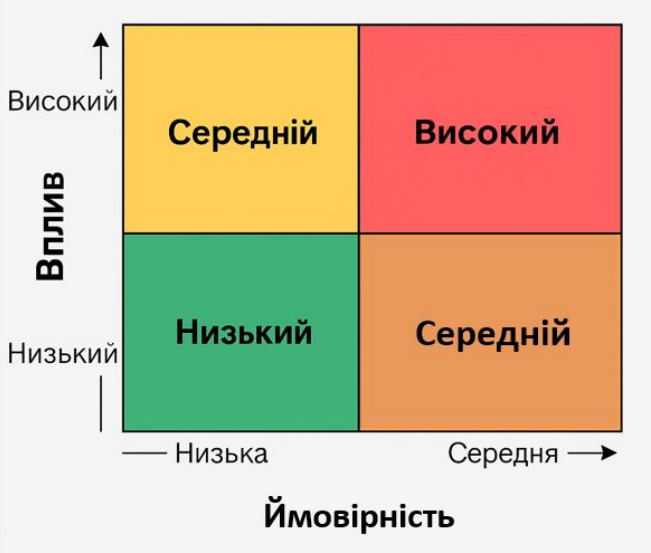

Рисунок 4.1 – Шаблон матриці ризиків

Наприклад, для умовної компанії, що обслуговує клієнтів у хмарному середовищі, однією з ключових загроз є фішинг. Припустимо, ймовірність реалізації загрози оцінена на рівні P = 0,6, а очікувані збитки у разі компрометації даних — I = 100 000 грн. Розрахунок ризику: R = 0.6 · 100 000 = 60 000 грн. У такому випадку доцільним є впровадження 2FA, навчання персоналу та обмеження доступу.

Далі здійснюється вибір стратегії реагування на ризик. Існують чотири базові підходи:

- зменшення ризику (впровадження захисних технологій: 2FA, VPN, IDS/IPS);
- передача ризику (страхування, аутсорсинг функцій);
- уникнення ризику (відмова від використання небезпечних сервісів);
- прийняття ризику (у випадках, коли ймовірність і вплив мінімальні).

На основі вищезазначених етапів формується алгоритм побудови системи захисту конфіденційних даних, представлений на рисунку 4.2.

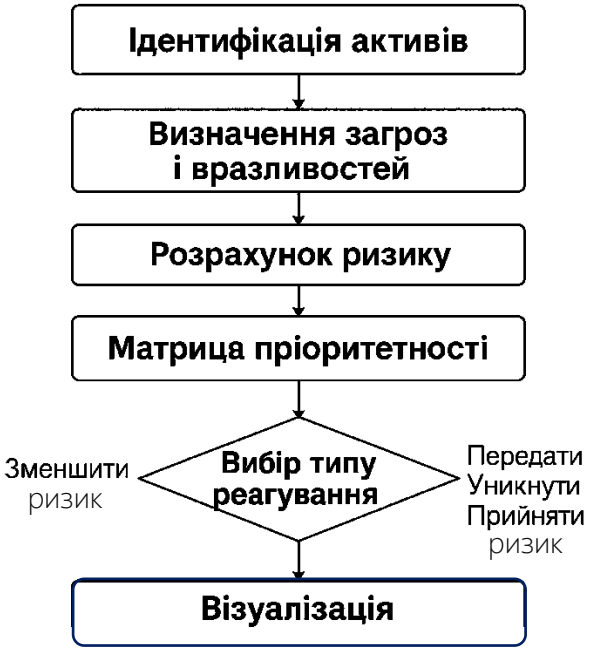

Рисунок 4.2 - Алгоритм побудови системи захисту конфіденційних даних

Завершальним етапом є реалізація технічних та організаційних заходів відповідно до обраної стратегії. Важливою є фаза постійного моніторингу, аудиту та оновлення політик безпеки з урахуванням змін у зовнішньому загрозовому середовищі та внутрішніх бізнес-процесах.

Запропонований алгоритм дозволяє систематизувати процес формування стратегії захисту конфіденційної інформації, забезпечуючи адаптивність, ефективність і економічну обґрунтованість заходів кібербезпеки.

4.2 Оцінка ризиків за кількісними та якісними показниками

Оцінка ризиків у сфері інформаційної безпеки є ключовим етапом у побудові стратегії захисту конфіденційної інформації. Цей етап дозволяє не лише виявити потенційні загрози, а й обґрунтувати необхідність впровадження конкретних технічних або організаційних заходів. У рамках даного дослідження було здійснено повноцінну оцінку ризиків на основі реальної діяльності підприємства ТОВ «ІнфоСервіс», яке спеціалізується на наданні IT-послуг і функціонує виключно у дистанційному режимі.

Оцінка ризиків є одним із найважливіших етапів у процесі управління інформаційною безпекою, оскільки саме вона дозволяє чітко зрозуміти, які саме загрози є найбільш критичними для організації, яку шкоду вони можуть спричинити та з якою ймовірністю можуть реалізуватися. Систематичний аналіз ризиків дозволяє забезпечити проактивне, а не реактивне управління безпекою. За умови обмежених ресурсів компанії повинні обирати першочергові напрями захисту, спираючись саме на результати оцінки ризиків.

У практиці оцінки ризиків застосовуються два основних підходи: кількісний та якісний. Кількісний підхід базується на використанні точних числових даних (наприклад, статистики інцидентів або фінансових показників) і дозволяє обчислити ризик у грошовому еквіваленті. Якісний підхід, своєю чергою, базується на експертному оцінюванні та дозволяє визначити рівень загроз у відносній шкалі (наприклад, низький, середній, високий). Обидва підходи мають свої переваги та доцільні в різних контекстах. Кількісний підхід зручний для економічного обґрунтування інвестицій у безпеку, тоді як якісний є корисним у ситуаціях з браком точних даних або для попереднього аналізу.

У цьому підрозділі реалізовано обидва підходи з використанням мови Python, що дозволяє автоматизувати процес аналізу ризиків. Зібрані дані включали перелік найпоширеніших загроз, ймовірність їх виникнення та орієнтовні фінансові втрати у разі реалізації кожної загрози. Для забезпечення зручності обробки та масштабованості рішення, ці дані були внесені до Excel-таблиці (див. табл. 4.1), яка надалі імпортувалася в Python для автоматизованої обробки [28].

Таблиця 4.1 – Вихідні дані для оцінки ризиків ТОВ «ІнфоСервіс»

№	Назва загрози	Ймовірність (P)	Потенційні збитки (I), грн	Рівень ймовірності	Рівень впливу	Примітка
1	Фішинг	0.4	250 000	високий	високий	Найбільш часта загроза
2	Несанкціонований доступ	0.2	400 000	середній	високий	Часто пов'язаний з помилками MFA
3	Атака програм-вимагачів	0.1	600 000	низький	високий	Серйозні наслідки при рідкісності
4	Зловмисне ПЗ	0.3	150 000	середній	середній	Типова загроза для нових пристроїв
5	Витік даних через email	0.25	100 000	середній	середній	Через помилки персоналу

Імпорт цих даних у Python забезпечує автоматизовану обробку в три етапи:

1. Кількісна оцінка ризиків - на першому етапі здійснюється зчитування Excel-файлу з даними про загрози, після чого автоматично обчислюється значення ризику для кожної загрози за допомогою множення ймовірності на збитки (див. рис. 4.3).
2. Якісна оцінка ризиків - далі з тих самих даних використовується текстова шкала рівня ймовірності та впливу, яка переводиться у числові значення згідно з наперед заданим словником, після чого обчислюється якісний ризик як добуток двох факторів (див. рис. 4.4). Після чого відбувається автоматизована обробка даних (див. рис. 4.5).
3. Побудова матриці ризиків - на завершальному етапі відображається візуалізація у вигляді матриці ризиків, яка узагальнює комбінації рівнів ймовірності та впливу, присвоюючи їм відповідні кольорові значення залежно від критичності (див. рис. 4.6).

Лістинг системи оцінки ризиків та заходів безпеки (див. дододаток Б) [30].

```python
# --- Кількісна оцінка ---
quant_df = pd.read_excel(file_path, sheet_name="Кількісна оцінка")

quant_df["R"] = quant_df["P"] * quant_df["I"]

print("Результати кількісної оцінки:")
for _, row in quant_df.iterrows():
    print(f"{row['name']}: Ризик = {row['R']:.2f} грн")

```

Рисунок 4.3 – Фрагмент коду для кількісної оцінки ризиків

```python
# --- Якісна оцінка ---
scale = {"низький": 1, "середній": 2, "високий": 3}
qual_df = pd.read_excel(file_path, sheet_name="Якісна оцінка")

# Конвертація якісних значень у числові
qual_df["P_num"] = qual_df["P"].str.lower().map(scale)
qual_df["I_num"] = qual_df["I"].str.lower().map(scale)
qual_df["R"] = qual_df["P_num"] * qual_df["I_num"]

print("\nРезультати якісної оцінки:")
for _, row in qual_df.iterrows():
    print(f"{row['name']}: Якісний ризик = {row['R']} ({row['P']} × {row['I']})")

```

Рисунок 4.4 – Фрагмент коду для якісної оцінки ризиків

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS

PS C:\Users\User> & "C:/Program Files/Python313/python.exe" "c:/Users/User/Downloads/import matplotlib ini.py"
Результати кількісної оцінки:
Фішинг: Ризик = 100000.00 грн
Фішинг: Ризик = 100000.00 грн
Несанкціонований доступ: Ризик = 8000.00 грн
Несанкціонований доступ: Ризик = 8000.00 грн
Атака програм-вимагачів: Ризик = 60000.00 грн
Атака програм-вимагачів: Ризик = 60000.00 грн
Зловмисне ПЗ: Ризик = 45000.00 грн
Витік даних через email: Ризик = 25000.00 грн
Витік даних через email: Ризик = 25000.00 грн


Результати якісної оцінки:
Фішинг: Якісний ризик = 9 (високий × високий)
Фішинг: Якісний ризик = 9 (високий × високий)
Несанкціонований доступ: Якісний ризик = 6 (середній × високий)
Атака програм-вимагачів: Якісний ризик = 3 (низький × високий)
Несанкціонований доступ: Якісний ризик = 6 (середній × високий)
Атака програм-вимагачів: Якісний ризик = 3 (низький × високий)
Атака програм-вимагачів: Якісний ризик = 3 (низький × високий)
Зловмисне ПЗ: Якісний ризик = 4 (середній × середній)
Витік даних через email: Якісний ризик = 4 (середній × середній)
```

Рисунок 4.5 – Результати автоматизованої обробки даних у Python

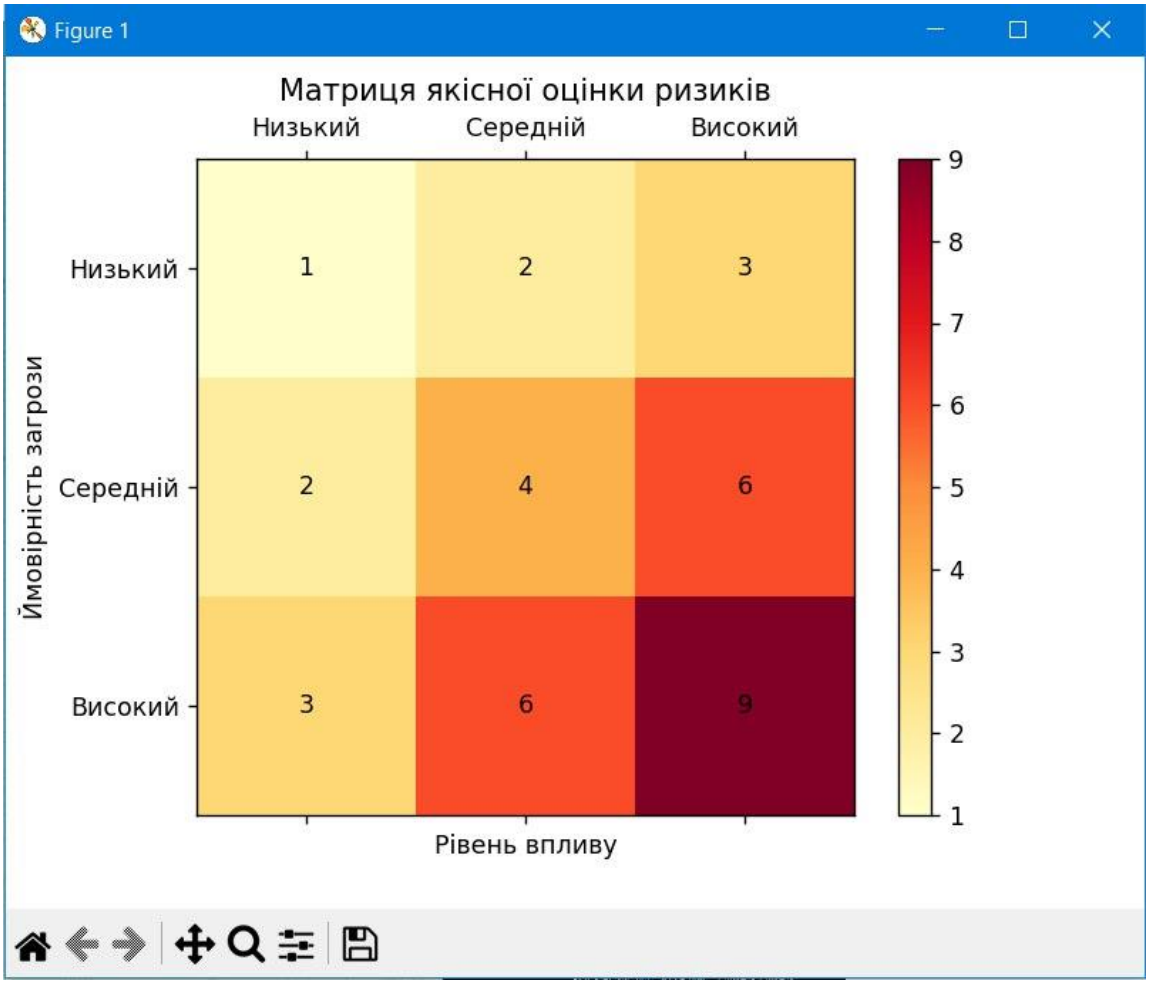

Рисунок 4.6 – Матриця ризиків

Автоматизований підхід на основі Excel-джерела даних дозволяє значно підвищити швидкість та точність розрахунків. Застосування бібліотек pandas, NumPy та matplotlib є ефективним рішенням для впровадження оцінки ризиків в інформаційно-аналітичних системах підприємства.

Використання поєднання якісних і кількісних методів у тандемі з сучасними інструментами обробки даних дозволяє не лише формалізувати процес ризик-менеджменту, а й інтегрувати його у практичну діяльність організації. Це є важливою передумовою для розробки ефективної політики кібербезпеки в умовах сучасних цифрових загроз.

4.3 Економічна доцільність впровадження заходів безпеки

Економічне обґрунтування впровадження заходів кіберзахисту є логічним продовженням кількісної та якісної оцінки ризиків, проведеної у попередніх підрозділах. Для підприємства ТОВ «ІнфоСервіс» розрахунки виконано на основі таблиці 4.1 та Python-розрахунків, що деталізували очікувані збитки та можливості їх зниження завдяки впровадженню комплексу технічних і організаційних рішень.

Згідно з розрахунками, без впровадження заходів безпеки підприємство потенційно може зазнати збитків до 1 000 000 грн. Це прогнозоване значення враховує суму ймовірних фінансових втрат з урахуванням статистичних ризиків та коефіцієнта запасу. Після впровадження заходів захисту залишкові збитки знижуються до 200 000 грн. Витрати на реалізацію заходів становлять 150 000 грн, що дорівнює приблизно 15% від суми прогнозованих збитків у разі відсутності захисту.

Для наочного підтвердження економічної ефективності (див. рис. 4.7) наведено діаграму порівняння витрат і можливих збитків. Діаграма побудована на основі значень, отриманих у Python-скриптах із вихідних даних таблиці 4.1 [29].

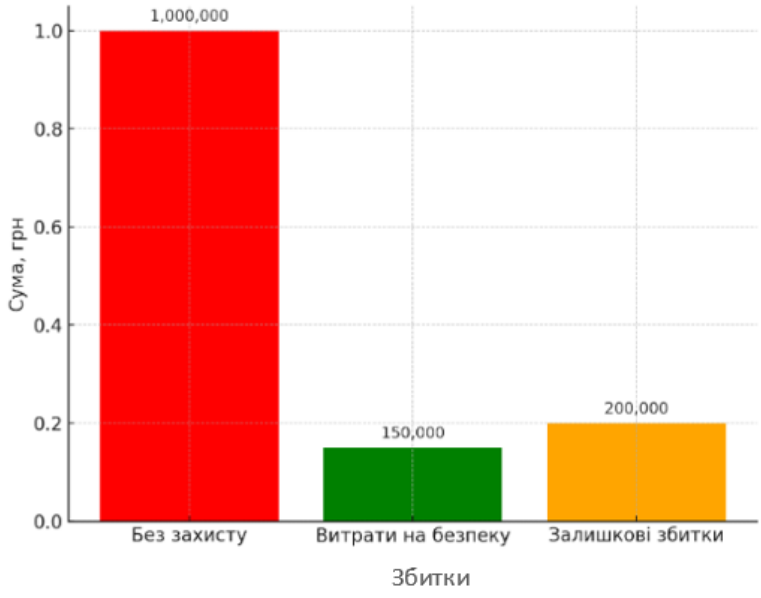

Рисунок 4.7 – Діаграма порівняння витрат і збитків

Додатково на рисунку (див. рис. 4.8) представлено графік динаміки окупності інвестицій (ROI). Він демонструє, що вже протягом 8 місяців після впровадження заходів кіберзахисту витрати окуповуються завдяки зниженню збитків. Формула окупності базується на співвідношенні витрат до щомісячної економії, яка дорівнює різниці між прогнозованими збитками без захисту та залишковими збитками, поділеної на 12 місяців.

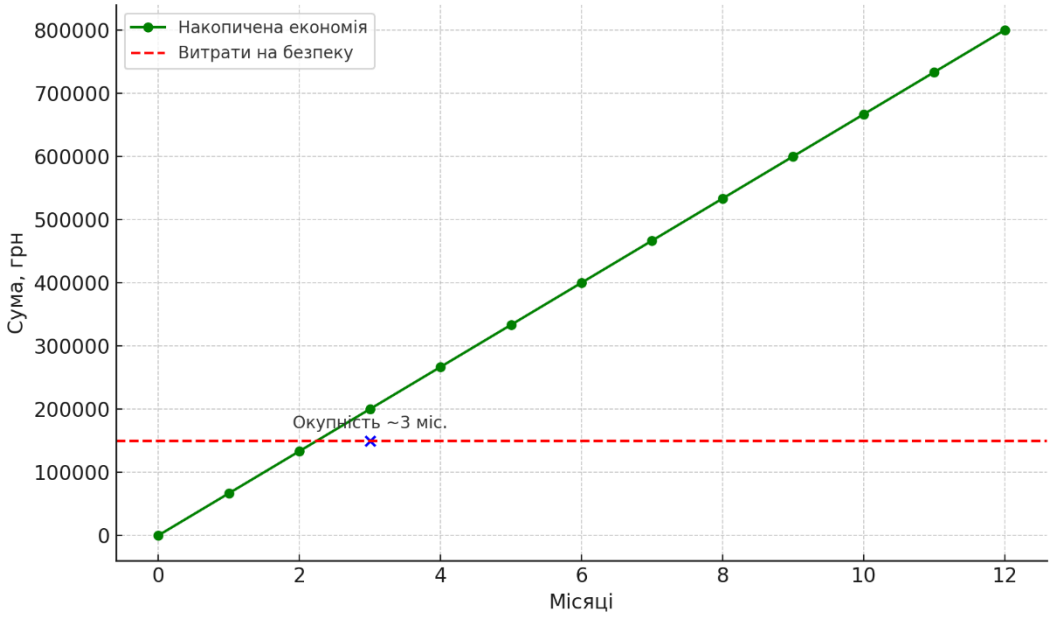

Рисунок 4.8 – Графік динаміки окупності інвестицій у заходи безпеки

Для підсумкового відображення ключових переваг впровадження заходів безпеки розроблено інфографіку «Вигоди впровадження» (див. рис. 4.9). Вона узагальнює основні показники: зниження ризику на понад 60%, підвищення довіри клієнтів завдяки покращенню репутації та підтверджений термін окупності — близько 8 місяців. Значення отримані на основі розрахунків із попередніх підрозділів і мають ілюстративний характер для демонстрації доцільності у середовищі малого і середнього бізнесу.

Рисунок 4.9 – Вигоди впровадження

Узгоджені дані розрахунків, діаграми та інфографіка переконливо підтверджують, що впровадження комплексної системи заходів кіберзахисту для ТОВ «ІнфоСервіс» є економічно вигідним, швидко окупається та мінімізує фінансові ризики, що безпосередньо впливає на безперервність діяльності й стабільність розвитку компанії.

ВИСНОВКИ

У кваліфікаційній роботі було комплексно розглянуто проблематику забезпечення кібербезпеки в умовах дистанційного функціонування організацій та реалізовано повний цикл дослідження, спрямованого на розробку системи оцінки ризиків і формування стратегії мінімізації впливу кіберзагроз.

У результаті виконання роботи були досягнуті усі поставлені у вступі завдання:

По-перше, проведено всебічний аналіз сучасних кіберзагроз, характерних для дистанційного середовища. Здійснено класифікацію найбільш поширених загроз, таких як фішингові атаки, несанкціонований доступ до корпоративних ресурсів, поширення шкідливого програмного забезпечення, витоки конфіденційної інформації через електронну пошту тощо. Визначено причини зростання уразливостей при використанні особистих пристроїв і незахищених мереж під час роботи поза межами офісу.

По-друге, досліджено теоретичні основи та методи оцінки ризиків у сфері інформаційної безпеки. Розглянуто сучасні підходи до кількісної та якісної оцінки ризиків, побудови матриць ризиків, методології управління ризиками відповідно до міжнародних стандартів (ISO, NIST, GDPR).

По-третє, виконано класифікацію ризиків та їх оцінку за кількісними і якісними показниками. Для цього використано дані практичного прикладу діяльності підприємства ТОВ «ІнфоСервіс», що функціонує виключно у дистанційному режимі. Ризики оцінено за допомогою Python-скриптів, побудовано таблиці, графіки та матрицю ризиків, що дало змогу визначити їх критичність і пріоритетність.

По-четверте, розроблено алгоритм побудови стратегії захисту конфіденційних даних, який включає послідовність етапів: ідентифікація активів, виявлення загроз, визначення вразливостей, розрахунок ризиків, вибір і впровадження заходів реагування. Алгоритм представлено у вигляді схеми для зручності практичного застосування.

По-п’яте, проведено оцінку економічної доцільності впровадження запропонованих заходів безпеки. Зроблено порівняльний аналіз витрат на реалізацію технічних і організаційних засобів захисту з прогнозованими збитками у разі відсутності заходів. Доведено, що впровадження комплексу заходів дозволяє знизити рівень ризику більш ніж на 60% і окупається протягом приблизно 8 місяців. Візуалізація результатів представлена у вигляді діаграм та інфографіки, що робить економічну доцільність впровадження прозорою та зрозумілою.

Таким чином, у межах кваліфікаційної роботи сформовано цілісну модель оцінки ризиків і управління кіберзагрозами, яка враховує специфіку дистанційної роботи та сучасні вимоги до інформаційної безпеки. Практична реалізація розробленої системи дозволяє підприємствам мінімізувати фінансові та репутаційні втрати, забезпечити безперервність бізнес-процесів та підвищити рівень довіри клієнтів і партнерів.

Отримані результати можуть бути використані для подальшого розвитку політики кібербезпеки у компаніях, що працюють у гібридному або повністю дистанційному форматі, а також як база для впровадження автоматизованих рішень оцінки ризиків та реагування на інциденти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022 Information security management. URL: https://www.iso.org/standard/27001 (дата звернення: 14.10.2024).
2. ISO/IEC 27005:2022 Information security risk management. URL: https://www.iso.org/standard/27005 (дата звернення: 15.10.2024).
3. NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 18.10.2024).
4. GDPR Regulation. URL: https://gdpr-info.eu/ (дата звернення: 20.10.2024).
5. Олійник А. В. Інформаційна безпека в комп’ютерних системах: навчальний посібник. Київ: КНУБА, 2022. URL: https://library.knuba.edu.ua/ (дата звернення: 25.10.2024).
6. Жураковський Р. А., Олійник А. В. Захист інформації в комп’ютерних мережах. Львів: Видавництво ЛНУ, 2023. URL: https://lnu.edu.ua/ (дата звернення: 28.10.2024).
7. Microsoft Security Best Practices for Remote Work. URL: https://learn.microsoft.com/en-us/security/remote-work-security-best-practices (дата звернення: 31.10.2024).
8. Сидоренко М. П. Методи оцінки ризиків інформаційної безпеки: монографія. Харків: ХНУРЕ, 2023. URL: https://repository.kpi.kharkov.ua/ (дата звернення: 04.11.2024).
9. Барабаш О. В. Кібербезпека та управління ризиками. Науковий вісник НУ «Львівська політехніка». 2024. URL: https://science.lpnu.ua/ (дата звернення: 07.11.2024).
10. Cloud Security Alliance: State of Cloud Security 2023. URL: https://cloudsecurityalliance.org/research/state-of-cloud-security (дата звернення: 10.11.2024).
11. ISO/IEC 27701:2023 Privacy Information Management. URL: https://www.iso.org/standard/71670.html (дата звернення: 14.11.2024).

12. ISO/IEC 27002:2022 Code of practice for information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 18.11.2024).
13. NIST SP 800-53 Rev. 5. Security and Privacy Controls. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 22.11.2024).
14. PCI DSS v4.0. URL: https://www.pcisecuritystandards.org/document_library (дата звернення: 26.11.2024).
15. Литвиненко В. І. Системи захисту комп'ютерної інформації. Київ: НАУ, 2024. URL: https://library.nau.edu.ua/ (дата звернення: 30.11.2024).
16. Palo Alto Networks Unit 42 Cloud Threat Report 2023. URL: https://unit42.paloaltonetworks.com/cloud-threat-report/ (дата звернення: 05.12.2024).
17. Check Point Cyber Security Report 2023. URL: https://www.checkpoint.com/cyber-security-report-2023/ (дата звернення: 10.12.2024).
18. Михайленко І. М. Захист даних у хмарних сервісах. Збірник наукових праць «Інформаційні технології та комп'ютерна інженерія». 2024. URL: https://itce.kpi.ua/ (дата звернення: 15.12.2024).
19. SANS Remote Work Security Guide 2023. URL: https://www.sans.org/white-papers/remote-work-security-guide/ (дата звернення: 20.12.2024).
20. Яковенко П. В. Основи кібербезпеки: підручник. Одеса: ОНАХТ, 2023. URL: https://lib.onaft.edu.ua/ (дата звернення: 25.12.2024).
21. Das S. K., Kant K., Zhang N. Security for Cyber-Physical Systems. URL: https://www.routledge.com/Security-for-Cyber-Physical-Systems/Das-Kant-Zhang/p/book/9780367186213 (дата звернення: 10.01.2025).
22. Jain A. K. An Introduction to Biometric Recognition. URL: https://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Introduction/JainRossPrabhakar_BiometricIntro_CSVT04.pdf (дата звернення: 18.01.2025).

23. Tistarelli M., Bigun J., Jain A. K. Biometric Authentication. URL: https://link.springer.com/book/10.1007/3-540-47917-1 (дата звернення: 25.01.2025).
24. Splunk Security Predictions 2024. URL: https://www.splunk.com/en_us/form/security-predictions-2024.html (дата звернення: 02.02.2025).
25. Cybersecurity Ventures Cybercrime Report 2024. URL: https://cybersecurityventures.com/cybercrime-report-2024/ (дата звернення: 10.02.2025).
26. CrowdStrike Global Threat Report 2024. URL: https://www.crowdstrike.com/global-threat-report/ (дата звернення: 18.02.2025).
27. Федоренко С. В. Аудит інформаційної безпеки організації. Київ: НАУ, 2024. URL: https://library.nau.edu.ua/ (дата звернення: 28.02.2025).
28. Кушніренко В. Ю. Управління ризиками кібербезпеки: методичні підходи. Науковий журнал «Інформаційна безпека». 2025. URL: https://journals.nau.edu.ua/index.php/InfBez (дата звернення: 15.03.2025).
29. Gartner Forecast: Information Security and Risk Management, Worldwide 2023-2024. URL: https://www.gartner.com/en/documents/forecast-information-security (дата звернення: 02.04.2025).
30. GitHub. Репозиторій з кодом програми системи оцінки ризиків та заходів безпеки URL: https://github.com/vika0121l/RISKASSESSMENTSYSTEM (дата звернення: 02.06.2025).

ДОДАТКИ

Додаток А

Таблиця 1.3 - Наслідки для організацій та фізичних осіб

№	Види наслідків	Прямі/Непрямі	Пояснення
1	2	3	4
1	Фінансові збитки	Прямі наслідки для організацій	Порушення конфіденційності даних часто супроводжується великими фінансовими витратами для організацій. Це може включати витрати на відновлення безпеки, зміцнення інфраструктури та компенсування збитків клієнтам або партнерам. Витрати на відшкодування збитків можуть включати оплату штрафів за порушення нормативних вимог (наприклад, штрафи за порушення GDPR), а також компенсації постраждалим користувачам або клієнтам за витік їхніх персональних даних.
2	Юридичні наслідки	Прямі наслідки для організацій	Організації можуть бути притягнуті до відповідальності в разі порушення законодавства щодо захисту персональних даних. Це може призвести до судових позовів від постраждалих осіб або груп клієнтів, а також санкцій з боку регулюючих органів. У разі серйозних порушень, компанії можуть бути змушені виплачувати великі штрафи, що значно впливають на їх фінансове становище.
3	Шкода репутації	Прямі наслідки для організації	Репутація є одним з найцінніших активів будь-якої організації, і її втрата через порушення конфіденційності може бути катастрофічною. Публікація інформації про порушення безпеки може викликати втрачену довіру з боку клієнтів, партнерів і навіть інвесторів. Клієнти можуть відмовитися від співпраці з компанією, оскільки вони втрачають упевненість у здатності компанії забезпечити належний рівень захисту своїх даних. Це може призвести до зниження обсягів продажу, відтоку клієнтів, а також до зниження вартості акцій на фондових ринках.

Продовження таблиці 1.3

1	2	3	4
4	Втрата конкурентних переваг	Прямі наслідки для організацій	Якщо конфіденційна інформація, зокрема інтелектуальна власність, бізнес-стратегії або фінансові дані, потрапляє до рук конкурентів, компанія може втратити свою конкурентну перевагу. Зловмисники можуть скористатися цими даними для маніпулювання ринковими умовами або для створення подібних продуктів. Це може суттєво вплинути на ринкові позиції компанії.
5	Зниження мотивації працівників	Непрямі наслідки для організацій	Порушення конфіденційності може вплинути на мотивацію і моральний стан працівників. Задача відновлення репутації та безпеки організації може привести до стресу, зниження продуктивності праці, а також до втрати лояльності працівників.
6	Підвищення витрат на аудит та моніторинг безпеки	Непрямі наслідки для організацій	Після порушення конфіденційності організації змушені значно збільшити витрати на послуги з аудиту та моніторингу безпеки, що може стати додатковим тягарем для бізнесу. Це може включати наймання додаткових фахівців, закупівлю спеціалізованого програмного забезпечення та проведення регулярних перевірок безпеки.
7	Фінансові втрати	Прямі наслідки для фізичних осіб	Один із найбільших ризиків для фізичних осіб — це крадіжка фінансових даних. Якщо зловмисники отримують доступ до банківських реквізитів або даних кредитних карток, вони можуть здійснювати несанкціоновані транзакції, виводячи гроші з рахунків потерпілого. Фізична особа може зазнати значних фінансових втрат до того, як проблема буде виявлена і виправлена.
8	Крадіжка особистості	Прямі наслідки для фізичних осіб	Порушення конфіденційності особистих даних може стати причиною крадіжки особистості. Зловмисники можуть використовувати вкрадені дані для отримання кредитів, відкриття банківських рахунків або навіть створення фальшивих документів на ім'я жертви. Це може призвести до серйозних фінансових проблем, коли особа виявить, що її ідентичність була використана для незаконних цілей.

Продовження таблиці 1.3

1	2	3	4
9	Шкода психологічного характеру	Прямі наслідки для фізичних осіб	Порушення конфіденційності особистих даних може викликати значний стрес у постраждалої особи. Людина може відчувати себе вразливою і небезпечною, переживаючи за подальшу безпеку своїх даних. Психологічний стрес може проявлятися у вигляді тривоги, депресії або втрати впевненості в цифровому світі.
10	Репутаційні втрати	Прямі наслідки для фізичних осіб	Порушення конфіденційності особистих даних, особливо в разі витоку інтимної або конфіденційної інформації, може призвести до серйозних репутаційних втрат. Публікація особистих фотографій, медичних записів чи іншої приватної інформації може негативно вплинути на соціальне становище людини та її особисте життя.
11	Втрата приватності та безпеки	Непрямі наслідки для фізичних осіб	Порушення конфіденційності може призвести до того, що інші люди (наприклад, зловмисники або рекламодавці) отримають доступ до персональної інформації, такої як місце проживання, звички, інтереси та інші дані. Це знижує рівень приватності та може створювати загрози для особистої безпеки.
12	Шкода довгострокового характеру	Непрямі наслідки для фізичних осіб	Деякі наслідки порушень конфіденційності даних можуть бути відчутні навіть через роки після інциденту. Наприклад, наслідки крадіжки особистості можуть залишатися актуальними, поки не буде відновлена особа в судовому порядку або на банківському рівні. Витрати часу та енергії на відновлення можна оцінити як непрямі наслідки, які можуть супроводжувати фізичну особу протягом тривалого часу.

Додаток Б

Фрагмент програми системи оцінки ризиків та заходів безпеки

```
import matplotlib.pyplot as plt
import numpy as np
import pandas as pd
# === Зчитування з Excel ===
file_path = "C:/Users/User/Downloads/risks.xlsx"
# --- Кількісна оцінка ---
quant_df = pd.read_excel(file_path, sheet_name="Кількісна оцінка")
quant_df["R"] = quant_df["P"] * quant_df["I"]
print("Результати кількісної оцінки:")
for _, row in quant_df.iterrows():
    print(f"{row['name']}: Ризик = {row['R']:.2f} грн")
# --- Якісна оцінка ---
scale = {"низький": 1, "середній": 2, "високий": 3}
qual_df = pd.read_excel(file_path, sheet_name="Якісна оцінка")
# Конвертація якісних значень у числові
qual_df["P_num"] = qual_df["P"].str.lower().map(scale)
qual_df["I_num"] = qual_df["I"].str.lower().map(scale)
qual_df["R"] = qual_df["P_num"] * qual_df["I_num"]
print("\nРезультати якісної оцінки:")
for _, row in qual_df.iterrows():
    print(f"{row['name']}: Якісний ризик = {row['R']} ({row['P']} ×
{row['I']})")
# --- Матриця ризиків ---
labels = ['Низький', 'Середній', 'Високий']
data = np.array([
    [1, 2, 3],
    [2, 4, 6],
    [3, 6, 9]
])

fig, ax = plt.subplots()
c = ax.matshow(data, cmap='YlOrRd')
ax.set_xticks([0, 1, 2])
ax.set_yticks([0, 1, 2])
ax.set_xticklabels(labels)
ax.set_yticklabels(labels)
plt.xlabel('Рівень впливу')
plt.ylabel('Ймовірність загрози')

for i in range(3):
    for j in range(3):
        ax.text(j, i, data[i, j], va='center', ha='center')

plt.title('Матриця якісної оцінки ризиків')
plt.colorbar(c)
plt.show()
```