НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Факультет адвокатури та антикорупційної діяльності
Кафедра економіки та менеджменту

БАКАЛАВРСЬКА РОБОТА

на тему: **«Ефективне управління кібербезпекою в бізнес– середовищі»**

Виконав: здобувач 4 курсу бакалаврського рівня
галузі знань
07 – Управління та адміністрування,
спеціальності
073 – Менеджмент
Єгор КРІЦЬКИЙ

Керівник: к.е.н., доц. Євгенія РЕДІНА
Рецензент: к.е.н., доц. Іван ПРІЙМАЧЕНКО

Одеса – 2025

ЗМІСТ

ВСТУП

Сучасне бізнес-середовище, що формується під впливом стрімкої цифровізації, глобалізації та зростання кіберзагроз, вимагає від організацій не лише оперативного реагування на виклики, а й стратегічного підходу до забезпечення захисту інформаційних активів. У умовах, коли інформація стала ключовим ресурсом, а кібератаки, такі як фішинг, DDoS-атаки, програми-вимагачі та витоки даних, набувають дедалі більшої складності, кібербезпека трансформується в стратегічний інструмент управління, що забезпечує стабільність бізнес-процесів, захист конфіденційних даних і збереження довіри клієнтів та партнерів.

Кібербезпека охоплює комплекс технічних, організаційних і людських заходів, спрямованих на захист комп'ютерних систем, мереж і даних від несанкціонованого доступу, пошкодження чи викрадення. Вона базується на принципах конфіденційності, цілісності та доступності інформації, які є основою для створення надійного захисту в цифровому середовищі. Інтегрований підхід до управління кібербезпекою, що включає проактивні, реактивні та адаптивні стратегії, дозволяє організаціям не лише запобігати кіберзагрозам, але й оперативно реагувати на інциденти, мінімізуючи їх наслідки. Цифрова трансформація додатково посилює актуальність цього питання, надаючи нові можливості для використання штучного інтелекту, аналітики великих даних і автоматизованих систем захисту, але водночас створюючи нові виклики через зростання складності кібератак.

Актуальність теми дослідження зумовлена зростаючою кількістю кіберзагроз, які впливають на фінансову стабільність, репутацію та конкурентоспроможність організацій. Виклики, пов'язані з фрагментарним застосуванням захисних технологій, недостатньою обізнаністю персоналу та потребою в адаптації до нових видів атак, вимагають розробки комплексних моделей управління кібербезпекою. Дослідження спирається на праці таких

вітчизняних та зарубіжних авторів, як Бурячок В.Л., Горбаченко С.А., Дикий О.В., Діордіца І.В., Рєдіна Є.В., Кібік О.М., Котлубай В.О., Муравський В.В., Ткаченко О., Rass S., Schauer S., König S., Zhu Q., а також на міжнародні стандарти, такі як ISO/IEC 27001 і NIST Cybersecurity Framework, які висвітлюють ключові аспекти управління кібербезпекою, впровадження захисних механізмів і вплив цифрових технологій на безпеку бізнесу.

Мета дослідження полягає у дослідження теоретичних та практичних аспектів управління кібербезпекою в бізнес-середовищі.

Для досягнення поставленої мети передбачено виконання наступних завдань:

- розкрити сутність кібербезпеки та її значення в сучасному бізнес-середовищі;
- охарактеризувати основні концепції та підходи до управління кібербезпекою;
- проаналізовано сучасні інструменти та технології кіберзахисту, що застосовуються в бізнес–структурах;
- провести оцінку фінансово–економічних показників організації з метою визначення можливостей для інвестування в кібербезпеку;
- виявити рівень загроз та оцінити вразливості організації;
- обгрунтувати заходи для підвищення рівня кіберзахисту організації з урахуванням виявлених проблем;
- оцінити ефективність впровадження запропонованих заходів.

Об'єкт дослідження – процеси забезпечення кібербезпеки в діяльності сучасних бізнес–структур.

Предмет дослідження – теоретичні та практичні особливості формування ефективної системи кіберзахисту організації в умовах цифрового середовища.

Методологічну базу дослідження склали системний, порівняльний і комплексний підходи, методи аналізу ризиків, контент-аналіз наукової літератури, а також емпіричне дослідження сучасних кіберзагроз і захисних технологій.

Інформаційною базою бакалаврської роботи стали нормативно–правові акти (українське законодавство, міжнародні стандарти, зокрема ISO/IEC 27001), наукові праці вітчизняних і зарубіжних авторів, монографії та підручники з кібербезпеки, фінансова звітність ТОВ «Нова пошта», а також матеріали науково–практичних конференцій, що висвітлюють теоретичні та практичні аспекти кібербезпеки.

Основні теоретичні основи роботи та її практичні результати було представлено на Всеукраїнській науково–практичній конференції здобувачів вищої освіти «Суспільство та держава: нові виміри у воєнний час» (м. Одеса, 26 травня 2025 р.).

Робота складається з вступу, трьох розділів, загальних висновків, переліку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В БІЗНЕС–СЕРЕДОВИЩІ

1.1. Поняття кібербезпеки та її значення в сучасному бізнес–середовищі

У сучасному світі інформаційні технології є невід'ємною частиною діяльності організацій, що робить захист інформації ключовим завданням. Інформація стала найціннішим ресурсом, а зростання кіберзагроз, таких як хакерські атаки, шкідливе програмне забезпечення та витоки даних, підкреслює важливість кібербезпеки. Цей напрям є стратегічно важливим для забезпечення стабільності бізнес–процесів, захисту конфіденційних даних і підтримки довіри клієнтів та партнерів.

Інформаційна безпека є комплексом заходів, спрямованих на захист всієї інформації, яка обробляється або зберігається на різних носіях [23, с. 5].

Вона охоплює всі форми збереження і передачі даних, включаючи як фізичні носії (паперові документи, архіви), так і цифрові. Основними складовими інформаційної безпеки є конфіденційність, доступність і цілісність інформації [25]. Конфіденційність передбачає захист даних від несанкціонованого доступу, що забезпечує їх збереження в межах визначеного кола осіб. Доступність забезпечує можливість доступу до інформації лише авторизованими користувачами в потрібний час, що критично важливо для ефективного функціонування інформаційних систем. Цілісність означає захист інформації від несанкціонованих змін або пошкоджень, які можуть вплинути на її достовірність. Всі ці елементи разом сприяють створенню надійного захисту інформаційних ресурсів, що зберігаються як в цифровому, так і в фізичному вигляді.

Кібербезпека, в свою чергу, є специфічним напрямком, який зосереджений на захисті комп'ютерних систем, мереж і даних від кіберзагроз. Вона включає в себе заходи, спрямовані на запобігання атак, зловмисних програм, несанкціонованого доступу і інших цифрових загроз.

Кібербезпека – це процес захисту базових систем і конфіденційної інформації від цифрових атак. Вона також відома як інформаційна безпека (ІТ–безпека), а заходи з кіберзахисту спрямовані на боротьбу з загрозами, що виникають як усередині, так і за межами організації [3].

Відповідно до Діордіца І., кібербезпека – це заходи щодо запобігання збоям в ІКТ–системах, їх некоректному використанню та відновлення після атак [10].

Білявська Ю.А. визначає кібербезпеку як здатність людини, суспільства та держави запобігати й уникати цілеспрямованого, передусім несвідомого, негативного впливу або маніпуляції інформацією [1].

Кібербезпека – це комплекс технічних і соціальних заходів, стратегій та принципів, спрямованих на захист суспільства від загроз і негативних впливів, що виникають у цифровому середовищі [13].

Кібербезпека – це одна з найважливіших складових сучасного бізнес–середовища, оскільки вона охоплює заходи щодо запобігання, виявлення та усунення кіберзагроз. У цифровому світі, де інформація стала головним ресурсом, її захист набуває критично важливого значення. Компанії будь–якого масштабу, незалежно від сфери діяльності, змушені приділяти значну увагу безпеці своїх даних, щоб уникнути фінансових втрат, репутаційних ризиків і навіть правових наслідків. У зв'язку з розвитком технологій та розширенням кіберпростору зростає кількість загроз, які можуть впливати на бізнес, що робить необхідним розгляд кібербезпеки як ключового елемента стратегічного управління [35].

Останніми роками «кібербезпека» стала широко вживаним терміном, який дедалі більше використовують фахівці та законодавці. Проте, як це часто буває з популярними поняттями, існує недостатнє розуміння його змісту. Це не є проблемою у неформальному спілкуванні, однак може викликати серйозні

труднощі в контексті стратегічного управління організацією, бізнес–цілей чи міжнародних угод.

Кібербезпека забезпечує захист веб–підключених систем, включаючи апаратне забезпечення, програмне забезпечення та дані, від цифрових загроз. У сфері комп'ютерної безпеки вона включає як мережевий, так і фізичний захист, що застосовується для запобігання несанкціонованому доступу до центрів обробки даних та інших електронних систем. Безпека, яка спрямована на підтримання конфіденційності, цілісності та доступності інформації, є підкатегорією кібербезпеки.

Кіберзагрози поділяються на зовнішні та внутрішні, кожна з яких має значний вплив на діяльність організацій. Зовнішні загрози включають хакерські атаки, такі як фішинг – обман користувачів для викрадення конфіденційних даних, DDoS–атаки – перевантаження серверів для блокування доступу до ресурсів, програми–вимагачі – шифрування даних із вимогою викупу та кібершпигунство – викрадення комерційної інформації. Наприклад, фішингова атака може призвести до компрометації даних клієнтів, а DDoS–атака – до зупинки онлайн–сервісів. Внутрішні загрози виникають через дії працівників, які можуть бути навмисними, такими як витік даних, або ненавмисними, які спричинені помилками чи недостатньою обізнаністю або вразливості в інформаційних системах, наприклад, слабкі паролі чи застаріле програмне забепечення [17]. За даними звіту IBM Security 2024, середня вартість витоку даних становить 4,45 млн доларів США, що підкреслює серйозність цих загроз для бізнесу [39].

Сучасне бізнес–середовище характеризується великою кількістю інформаційних потоків, що циркулюють у цифровому форматі. Це можуть бути фінансові дані, персональна інформація клієнтів, конфіденційні бізнес–процеси або стратегічні плани. Незахищеність цих даних може призвести до серйозних наслідків, таких як витік інформації, шахрайство, атаки на інформаційні системи або навіть зупинка діяльності компанії. Кібербезпека забезпечує захист від цих

загроз, впроваджуючи заходи безпеки, що допомагають зменшити ризики і підвищити довіру клієнтів та партнерів.

Кіберзлочинці націлюються на персональну інформацію користувачів (PII) – імена, адреси, номери ідентифікаційних документів, дані кредитних карток – і продають ці записи на підпільних цифрових ринках. Компрометація PII часто призводить до втрати довіри клієнтів, адміністративних штрафів і навіть судових позовів. Складність систем безпеки, що виникає через різноманітність технологій і брак внутрішніх фахівців, може збільшити ці витрати [6].

Сучасні кіберзагрози включають різноманітні методи атак, що розвиваються паралельно із новими технологіями. Одними з найпоширеніших є фішингові атаки, спрямовані на викрадення конфіденційних даних через обман користувачів. Використання шкідливого програмного забезпечення (вірусів, троянів, шпигунських програм) може спричинити значні втрати, порушення роботи систем і викрадення інформації. DDoS–атаки (розподілені атаки на відмову в обслуговуванні) спрямовані на перевантаження серверів і блокування доступу до ресурсів компанії. Соціальна інженерія, що базується на маніпуляції людським фактором, стає все більш витонченим методом зламування систем без необхідності використання складних технологічних засобів.

Однією з ключових складових кібербезпеки є управління ризиками, яке включає ідентифікацію, аналіз та оцінку потенційних загроз, розробку відповідних заходів та впровадження стратегій мінімізації ризиків. Бізнес повинен мати чітко визначену політику інформаційної безпеки, що охоплює правила роботи з конфіденційною інформацією, регламенти доступу до даних, процедури резервного копіювання та реагування на інциденти. Використання сучасних технологій, таких як шифрування даних, багатофакторна автентифікація, системи виявлення вторгнень, забезпечує додатковий рівень безпеки [8].

Не менш важливим аспектом кібербезпеки є підвищення обізнаності персоналу щодо можливих загроз. Людський фактор залишається одним із найслабших місць у системі безпеки, тому навчання працівників правилам

роботи з інформацією, виявлення підозрілих дій та запобігання шахрайству може значно знизити ймовірність успішних атак. Багато компаній впроваджують програми кібергігієни, що включають регулярне оновлення паролів, використання захищених мереж і уникнення підозрілих електронних листів.

Законодавче регулювання кібербезпеки також відіграє важливу роль у захисті бізнесу. Уряди різних країн ухвалюють нормативні акти, що встановлюють вимоги до зберігання, обробки та захисту персональних даних. Наприклад, Загальний регламент про захист даних (GDPR) в Європейському Союзі зобов'язує компанії забезпечувати високий рівень безпеки даних, а порушення цих вимог може призвести до значних штрафів. У США діють такі закони, як Закон про захист споживчих даних (CCPA) та інші акти, що регулюють кібербезпеку. Впровадження таких регуляцій сприяє підвищенню рівня відповідальності компаній за збереження даних клієнтів [36].

Окрім законодавчих аспектів, компанії повинні розглядати питання кіберстрахування як спосіб зменшення фінансових ризиків у разі кібератак. Кіберстрахування дозволяє покрити збитки, спричинені витоком даних, атаками на інфраструктуру та іншими кіберінцидентами. В останні роки попит на такі послуги зростає, оскільки бізнес усвідомлює важливість підготовки до можливих атак і необхідність швидкого відновлення діяльності після них.

Окремо слід згадати про роль штучного інтелекту та машинного навчання у сфері кібербезпеки. Сучасні алгоритми аналізують великі обсяги даних, виявляючи аномалії та потенційні загрози ще до того, як вони можуть завдати шкоди. Використання автоматизованих систем кіберзахисту дозволяє швидко реагувати на атаки, мінімізуючи їх наслідки [5].

Незважаючи на схожість у цілях захисту інформації, між інформаційною безпекою і кібербезпекою існують суттєві відмінності. Інформаційна безпека має більш широкий спектр застосування, оскільки вона охоплює всі аспекти захисту даних, включаючи фізичні носії та нецифрову інформацію. Вона зосереджена на створенні системи захисту даних від будь–яких загроз, незалежно від того, чи це кіберзагроза, чи фізичний доступ до документа.

Кібербезпека обмежується лише цифровим середовищем і зосереджується на захисті комп'ютерних систем, мереж і даних від атак, зловмисного програмного забезпечення і витоків інформації через інтернет. Відповідно, засоби захисту, які застосовуються в обох випадках, також мають різну специфіку. Для інформаційної безпеки використовуються як технічні, так і організаційні засоби, зокрема забезпечення фізичного доступу до документів, проведення тренінгів для персоналу з питань безпеки, створення систем резервного копіювання даних. У кібербезпеці ж основну роль відіграють технічні засоби, такі як антивірусні програми, брандмауери, шифрування даних та інші цифрові інструменти.

Отже, кібербезпека є невід'ємною частиною сучасного бізнес–середовища, яка вимагає комплексного підходу та постійного вдосконалення. Бізнес повинен адаптуватися до нових загроз, впроваджувати інноваційні рішення та підвищувати рівень обізнаності персоналу. Враховуючи швидкий розвиток цифрових технологій, безпека інформації стає ключовим фактором стабільного розвитку компаній та їх конкурентоспроможності на ринку. Впровадження ефективних механізмів захисту дозволяє не лише запобігати загрозам, а й будувати довіру клієнтів, що є основою успішного ведення бізнесу у цифрову епоху.

1.2. Основні концепції та підходи до управління кібербезпекою

У сучасному цифровому світі кібербезпека стала критично важливою складовою стабільного функціонування як державних, так і приватних структур. Зі зростанням обсягів обробки даних, інтенсивністю використання інформаційно–комунікаційних технологій та поширенням цифрових сервісів, зростає і спектр потенційних кіберзагроз. Це обумовлює необхідність глибокого

розуміння не лише технічних аспектів захисту інформаційних ресурсів, але й теоретичних засад управління кібербезпекою, зокрема концепцій та підходів, що лежать в основі цієї діяльності.

Поняття кібербезпеки охоплює комплекс заходів, спрямованих на захист комп'ютерних систем, мереж та даних від несанкціонованого доступу, пошкодження, викрадення або інших загроз, що можуть завдати шкоди конфіденційності, цілісності та доступності інформації. Управління кібербезпекою передбачає системну діяльність, спрямовану на виявлення, аналіз, попередження та реагування на кіберзагрози у рамках організаційної стратегії захисту інформаційних активів. Для ефективного захисту інформаційних систем важливо впроваджувати комплексні заходи кібербезпеки [20].

У таблиці 1.1 представлені основні концепції управління кібербезпекою у бізнес–середовищі.

Однією з основних концепцій управління кібербезпекою є ризик–орієнтований підхід, який передбачає оцінку потенційних загроз, визначення їхнього впливу на бізнес–процеси та розробку стратегій зменшення ризиків. Компанії проводять аналіз активів, визначають критичні ресурси та застосовують засоби моніторингу для виявлення вразливостей. Важливим аспектом є впровадження багаторівневого захисту інформаційних систем, що включає використання антивірусного програмного забезпечення, міжмережевих екранів, шифрування даних, багатофакторної аутентифікації та управління правами доступу.

Політики та регламенти кібербезпеки є невід'ємною частиною захисту бізнесу, оскільки вони визначають правила користування корпоративними інформаційними ресурсами, процедури обробки конфіденційних даних та заходи реагування на інциденти. Створення внутрішніх політик допомагає уніфікувати підхід до кібербезпеки, мінімізувати ризики людського фактора та забезпечити відповідність законодавчим вимогам [26].

Таблиця 1.1

Основні концепції управління кібербезпекою у бізнес–середовищі

Концепція	Опис
Ризик–орієнтований підхід	Аналіз загроз, оцінка їхнього впливу на бізнес та впровадження заходів з мінімізації кіберризиків. Використання моніторингу для виявлення вразливостей.
Багаторівневий захист інформаційних систем	Використання антивірусного ПЗ, міжмережевих екранів, шифрування даних, багатофакторної аутентифікації, систем контролю доступу.
Політики та регламенти кібербезпеки	Впровадження внутрішніх політик щодо використання інформаційних систем, обробки конфіденційних даних та реагування на кіберінциденти.
Навчання персоналу та підвищення обізнаності	Проведення тренінгів з виявлення фішингових атак, безпечного користування паролями, мінімізації ризиків людського фактора.
Оперативне реагування на інциденти	Виявлення загроз у режимі реального часу, розробка планів реагування, локалізація загрози, швидке відновлення систем.
Дотримання міжнародних стандартів	Впровадження стандартів кібербезпеки (ISO/IEC 27001, NIST Cybersecurity Framework, GDPR) для правової відповідності та підвищення довіри клієнтів.

Джерело: розроблено автором на основі [35,40,41]

Людський фактор є одним із найслабших місць у системі безпеки, тому навчання та підвищення обізнаності персоналу має велике значення. Працівники повинні регулярно проходити тренінги з виявлення фішингових атак, безпечного використання паролів, уникнення витоків інформації та реагування на підозрілі активності. Важливою є ідентифікація внутрішніх загроз, що можуть виникнути через ненавмисні помилки або зловмисні дії співробітників [13].

Оперативне реагування на інциденти відіграє ключову роль у забезпеченні кіберстійкості бізнесу. Необхідно впроваджувати систему моніторингу інформаційної безпеки, яка дозволяє виявляти та аналізувати загрози в режимі реального часу. Також важливим є розробка планів дій у разі кіберінцидентів, які

включають процедури локалізації загрози, відновлення систем та комунікації із зацікавленими сторонами.

Дотримання міжнародних та національних стандартів кібербезпеки, таких як ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, є важливим елементом управління інформаційною безпекою. Відповідність цим стандартам забезпечує не лише правову захищеність компанії, але й підвищує довіру з боку клієнтів, партнерів та інвесторів [40,41].

Ефективне управління кібербезпекою є ключовим для забезпечення захисту інформаційних активів організацій у сучасному бізнес–середовищі, де кіберзагрози стають дедалі складнішими. Підходи до управління кібербезпекою дозволяють організаціям системно протистояти зовнішнім і внутрішнім загрозам, таким як фішинг, DDoS–атаки чи витоки даних через людський фактор, шляхом використання проактивних, реактивних і адаптивних стратегій [33]. Ці підходи ґрунтуються на принципах конфіденційності, цілісності та доступності і відповідають міжнародним стандартам, таким як ISO/IEC 27001 і NIST Cybersecurity Framework.

Для протидії кіберзагрозам, описаним у пункті 1.1, організації застосовують різноманітні підходи до управління кібербезпекою, які охоплюють превентивні, оперативні та адаптивні стратегії. Ці підходи ґрунтуються на принципах конфіденційності, цілісності та доступності (CIA–тріада) і відповідають міжнародним стандартам, таким як ISO/IEC 27001 і NIST Cybersecurity Framework. Вони дозволяють не лише мінімізувати ризики, пов'язані з фінансовими втратами, репутаційними збитками чи юридичними санкціями, а й забезпечити безперервність бізнес–процесів і підвищити довіру стейкхолдерів, що є основою конкурентоспроможності в цифрову епоху.

Для систематизації та кращого розуміння цих стратегій нижче у таблиці 1.2 наведено основні підходи до управління кібербезпекою, їх опис та приклади практичного застосування.

Таблиця 1.2

Підходи до управління кібербезпекою

Підхід	Опис	Приклади застосування
Проактивний	Запобігання загрозам шляхом аналізу вразливостей, оновлення ПЗ, етичного хакерства, навчання персоналу та використання стандартів (ISO/IEC 27001, NIST CSF).	Регулярне сканування вразливостей, тренінги з кібергігієни.
Реактивний	Оперативне реагування на інциденти з використанням SIEM–систем (Splunk, QRadar), швидке відновлення після атак.	Аналіз логів після фішингової атаки, відновлення даних.
Ризик–орієнтований	Аналіз, оцінка та мінімізація кіберризиків із застосуванням методів оцінки ризиків і пріоритезації загроз.	Пріоритизація захисту критичних активів організації.
Комплексний	Поєднання технічних (шифрування, брандмауери), організаційних (політики безпеки) і людських факторів, інтеграція з COBIT.	Впровадження багаторівневих систем захисту в організації.
Адаптивний	Динамічне налаштування захисту з використанням ШІ та автоматизованих систем аналізу поведінки (UEBA).	Виявлення аномалій у поведінці користувачів за допомогою ШІ.

Джерело: розроблено автором на основі [10, 26, 31]

Проактивний підхід базується на запобіганні кіберзагрозам до їхнього виникнення. Його застосування включає регулярний аналіз вразливостей, своєчасне оновлення програмного забезпечення та розробку чітких політик безпеки. Особливу увагу приділяють навчанню персоналу, оскільки людський фактор часто є найслабшою ланкою кіберзахисту. Одним із найефективніших інструментів у межах цього підходу є етичне хакерство (penetration testing), яке дозволяє виявити слабкі місця в системах безпеки до того, як їх використають зловмисники. Також застосовуються системи моніторингу трафіку та поведінковий аналіз, що дає змогу заздалегідь виявити підозрілі дії [28].

На відміну від проактивного, реактивний підхід орієнтований на швидке виявлення та нейтралізацію атак, що вже відбулися. Важливими складовими

цього методу є використання систем виявлення та реагування (SIEM, SOC), які в режимі реального часу аналізують мережеву активність і сигналізують про загрози. Компанії, що дотримуються цього підходу, зосереджуються на мінімізації шкоди, швидкому відновленні даних та забезпеченні безперервності бізнес–процесів. До ключових заходів входять резервне копіювання даних, швидке оновлення систем безпеки після інцидентів та оперативне інформування співробітників про потенційні загрози.

Ризик–орієнтований підхід спрямований на оцінку та управління ризиками відповідно до потенційних загроз. Використання стандартів, таких як ISO 27005, дозволяє компаніям ідентифікувати найбільш критичні загрози, розставити пріоритети у захисті та ефективно розподілити ресурси. Наприклад, якщо компанія обробляє значні обсяги фінансових транзакцій, її основні ризики можуть бути пов'язані з шахрайством або витоком платіжних даних, що потребує підвищеного рівня безпеки саме в цій сфері. Завдяки такому підходу організація уникає зайвих витрат на неактуальні загрози, спрямовуючи зусилля на найбільш критичні аспекти [22].

Комплексний підхід поєднує елементи проактивного та реактивного підходів, охоплюючи технічні, організаційні та людські аспекти кібербезпеки. Основна ідея – створення багаторівневої системи захисту, що включає:

- Контроль доступу та багатофакторну аутентифікацію;
- Регулярне резервне копіювання даних;
- Використання міжмережевих екранів та антивірусного програмного забезпечення;
- Розробку планів швидкого реагування у разі кіберінцидентів. Такий підхід дає змогу не лише зменшити ймовірність атак, а й швидко відновити роботу компанії у випадку порушення безпеки [42].

Адаптивний підхід є найбільш динамічним, оскільки передбачає постійне оновлення стратегій кібербезпеки відповідно до змінюваного ландшафту загроз. Він ґрунтується на використанні технологій штучного інтелекту та машинного навчання для автоматичного аналізу поведінки користувачів і виявлення

аномалій. Адаптивні системи безпеки можуть самостійно змінювати свої механізми захисту залежно від виявлених ризиків, що робить їх ефективними навіть проти нових, невідомих атак. Наприклад, якщо алгоритми виявляють підозрілу активність у внутрішній мережі компанії, вони можуть автоматично обмежити доступ користувачів до критично важливих ресурсів, мінімізуючи можливі втрати.

Ефективне управління кібербезпекою передбачає вибір оптимального підходу залежно від специфіки бізнесу, рівня ризиків та ресурсних можливостей. У реальній практиці компанії часто комбінують різні методи, поєднуючи елементи проактивного, реактивного, ризик–орієнтованого, комплексного та адаптивного підходів. Такий гнучкий підхід дозволяє не лише запобігати кіберзагрозам, а й швидко реагувати на них, забезпечуючи безперервність бізнесу та надійний захист даних.

Отже, ефективне управління кібербезпекою потребує комплексного підходу, що враховує різні методи та концепції захисту. Вибір стратегії залежить від специфіки діяльності організації, рівня кіберризиків та доступних ресурсів. Впровадження багаторівневого захисту, політик безпеки, навчання персоналу та дотримання міжнародних стандартів сприяє підвищенню кіберстійкості бізнесу та забезпеченню його безперервної роботи в умовах сучасних загроз.

1.3. Інструменти, методи та технології забезпечення кібербезпеки в організаціях

Кібербезпека є важливим аспектом функціонування сучасних організацій, оскільки цифровізація бізнес–процесів значно розширює можливості для кібератак. У світі, де інформація є одним із найцінніших активів, захист даних набуває критичного значення. Кіберзагрози стають усе складнішими та

різноманітнішими, що змушує компанії активно впроваджувати новітні технології та методи забезпечення безпеки. Кожна організація, незалежно від її розміру та сфери діяльності, стикається з ризиками втрати конфіденційної інформації, несанкціонованого доступу та фінансових збитків через діяльність кіберзлочинців. Саме тому впровадження ефективних заходів кібербезпеки є не просто рекомендацією, а необхідністю для сталого розвитку організацій.

Для забезпечення захисту інформаційних систем використовуються різні інструменти, методи та технології, які сприяють зменшенню ризиків несанкціонованого доступу, витоку даних та кібератак. У таблиці 1.3 систематизовано ключові методи кіберзахисту.

Таблиця 1.3

Методи кіберзахисту

Метод	Опис
Запобігання кібератакам	Включає в себе заходи для запобігання атакам через впровадження політики безпеки, використання антивірусів, оновлення програмного забезпечення, обмеження доступу до чутливих даних та навчання співробітників.
Своєчасне виявлення кібератаки	Використання систем виявлення вторгнень (IDS), аналітики великих даних і штучного інтелекту для виявлення аномалій та підозрілих патернів у реальному часі. Це дозволяє швидко реагувати на загрози.
Нейтралізація кібератаки та відновлення систем	Включає ізоляцію заражених систем, аналіз наслідків атаки, відновлення з резервних копій і тестування на шкідливі програми. Після відновлення проводиться аналіз інциденту для покращення політик безпеки.

Джерело: розроблено автором на основі [22, 38].

Запобігання є найефективнішим методом боротьби з кіберзагрозами, оскільки він дозволяє зменшити ризик атаки до мінімуму. Одним з основних засобів запобігання є впровадження політики безпеки в організаціях. Включає

використання складних паролів, регулярну зміну паролів, а також обмеження доступу до чутливої інформації. Крім того, важливим елементом є встановлення антивірусного програмного забезпечення та брандмауерів, які фільтрують небажаний трафік і блокують доступ до шкідливих ресурсів [9].

Іншим важливим аспектом є впровадження системи оновлень програмного забезпечення. Багато кіберзагроз використовують вразливості в застарілих програмах. Тому регулярне оновлення операційних систем та програм є необхідним заходом для зменшення можливості кібератаки.

Також великою мірою забезпечити захист допомагає навчання співробітників. Людський фактор залишається одним із найбільших ризиків для безпеки, тому регулярні тренінги і підвищення обізнаності про потенційні загрози, такі як фішинг або соціальна інженерія, є важливими заходами.

Своєчасне виявлення кіберзагроз – важливо для мінімізації шкоди. Розвиток технологій дозволяє використовувати передові інструменти для моніторингу та виявлення атак. Одним із таких інструментів є системи виявлення вторгнень (IDS), які здатні відстежувати аномальні дії в мережі та системах. Вони виявляють підозрілі патерни, такі як незвичайний трафік або спроби доступу до захищених частин мережі, що можуть свідчити про наявність атаки [23].

Іншим важливим аспектом є використання методів аналітики великих даних (Big Data) для виявлення загроз. Ці системи здатні обробляти великі обсяги даних в реальному часі, виявляючи аномалії та дозволяючи швидко реагувати на потенційні загрози [47].

Виявлення кібератак також може включати використання систем штучного інтелекту (ШІ), які здатні навчатися та адаптуватися до нових типів загроз. ШІ може виявляти нові методи атак ще до того, як вони стануть широко відомими, що забезпечує швидшу реакцію на інциденти [33].

Коли кібератака все ж таки сталася, важливо швидко нейтралізувати загрозу та відновити роботу систем. Це може включати в себе кілька етапів.

Перший етап – це ізоляція зараженої системи від інших частин мережі. Якщо зловмисники мають доступ до важливих даних або систем, швидка ізоляція дозволяє запобігти поширенню атаки.

Наступний крок – це визначення виду атаки та її наслідків. Важливо точно зрозуміти, які системи та дані були пошкоджені або викрадені. Це дозволяє визначити правильний спосіб відновлення та захисту даних [7].

Процес відновлення системи зазвичай включає в себе відновлення з резервних копій. Регулярне створення резервних копій є важливою частиною стратегії кіберзахисту, оскільки це дозволяє відновити роботу після атаки з мінімальними втратами.

Після відновлення системи необхідно провести ретельне тестування, щоб переконатися, що атака не залишила шкідливого коду в системі. Це включає в себе перевірку на наявність вірусів або інших шкідливих програм, які можуть бути вбудовані в систему під час атаки.

Також важливо провести аналіз події для того, щоб зрозуміти, як атака відбулася, і яких заходів можна вжити, щоб уникнути подібних інцидентів у майбутньому. Зазвичай після таких інцидентів переглядаються політики безпеки, щоб посилити захист і знизити ймовірність повторення атаки.

Кіберзахист є невід'ємною частиною забезпечення безпеки сучасних комп'ютерних систем та мереж. З кожним роком кількість і складність кіберзагроз зростає, тому впровадження ефективних інструментів захисту стає надзвичайно важливим для користувачів, організацій та державних установ. Одними з основних інструментів кіберзахисту є антивірусне програмне забезпечення та брандмауер, які забезпечують захист від різноманітних кіберзагроз, таких як віруси, шпигунські програми, трояни, руткіти та інші шкідливі програми [16]. Розглянемо ці інструменти детальніше, а також їх роль у системі кібербезпеки.

Антивірусне програмне забезпечення є одним із найпоширеніших та найважливіших інструментів у боротьбі з кіберзагрозами. Основна функція антивірусів полягає у виявленні, запобіганні та усуненні шкідливих програм, які

можуть потрапити в комп'ютер через інтернет, переносні носії інформації або за допомогою сторонніх пристроїв. Віруси – це програми, що здатні самовідтворюватися і поширюватися, заражаючи інші файли та системи. Вони можуть викликати серйозні проблеми: від повного збою системи до втрати важливих даних або крадіжки особистої інформації. Антивірусні програми використовують кілька методів для захисту.

Сканування файлів – основний метод, який дозволяє виявляти шкідливе програмне забезпечення, аналізуючи файли та програми на наявність відомих вірусів і загроз. Сканування може проводитись за запитом користувача або автоматично у фоновому режимі.

Підписні бази даних – антивірусні програми регулярно оновлюють свої бази даних, які містять підписи (відбитки) відомих вірусів. Це дозволяє програмі швидко виявляти загрози, що вже були зафіксовані раніше [22].

Аналіз поведінки – сучасні антивірусні програми можуть також застосовувати методи аналізу поведінки програм. Це дозволяє виявляти нові невідомі загрози шляхом спостереження за підозрілою активністю в системі, навіть якщо сам вірус ще не зафіксований у базах даних [13].

Нейтралізація загроз – коли антивірус виявляє шкідливу програму, він може заблокувати її, видалити або помістити в карантин для подальшого аналізу [23].

Іншим важливим інструментом кіберзахисту є брандмауер (firewall). Брандмауер – це система безпеки, яка контролює трафік між комп'ютером або мережею та зовнішнім середовищем, зокрема Інтернетом. Він фільтрує вхідний і вихідний трафік, дозволяючи або блокуючи з'єднання на основі встановлених політик безпеки. Брандмауер допомагає захищати комп'ютери та мережі від несанкціонованого доступу, блокуючи спроби зловмисників отримати контроль над системою або викрасти дані.

Існують два основних типи брандмауерів: програмні та апаратні. Програмні брандмауери працюють на операційній системі і контролюють трафік, що проходить через комп'ютер. Апаратні брандмауери зазвичай

використовуються для захисту цілих мереж і забезпечують більш високий рівень безпеки. Вони встановлюються на спеціальних пристроях і контролюють трафік, що проходить через мережу.

Брандмауери виконують кілька важливих функцій:

1) Контроль доступу – брандмауери дозволяють блокувати або дозволяти з'єднання з певними адресами чи портами. Наприклад, якщо система не повинна отримувати з'єднання з певним сервером, брандмауер заблокує доступ до нього.

2) Фільтрація трафіку – брандмауер фільтрує пакети даних, що передаються через мережу, перевіряючи їх на наявність шкідливих елементів або загроз.

3) Моніторинг і виявлення атак – сучасні брандмауери можуть виявляти спроби несанкціонованого доступу до системи або атаки на мережу (наприклад, DoS–атаки) і негайно реагувати на них, блокуючи загрозу.

4) Розширена безпека – брандмауери можуть бути частиною комплексних систем захисту, таких як системи виявлення та запобігання вторгнень (IDS/IPS), які забезпечують додатковий рівень безпеки [35].

Антивірусне програмне забезпечення та брандмауери є важливими складовими кіберзахисту, однак їх недостатньо для забезпечення повної безпеки. Система кіберзахисту повинна включати в себе також регулярне оновлення програмного забезпечення, шифрування даних, резервне копіювання, навчання користувачів та інші заходи. Усі ці інструменти працюють разом, створюючи багатошарову систему захисту, що знижує ризик успішної атаки зловмисників.

Технологічна складова кіберзахисту є одним із найважливіших елементів забезпечення інформаційної безпеки у будь–якій організації, зокрема в закладах охорони здоров'я (ЗОЗ). Вона включає широкий спектр комп'ютерних і програмних ресурсів, які призначені для спостереження за інформаційними системами та зменшенням ризиків, пов'язаних із загрозами інформаційної безпеки. Ключові компоненти цієї складової включають антивірусне програмне забезпечення, системи управління доступом, засоби шифрування, сканери

вразливостей, інструменти моніторингу та журнали подій, а також інші технічні засоби, які дозволяють підтримувати захищеність інформаційних систем.

Одним із основних елементів технологічного захисту є антивірусне програмне забезпечення, яке встановлюється на всі робочі пристрої та сервери ЗОЗ. Антивірусне ПЗ забезпечує безпеку комп'ютерних систем, виявляючи і блокуючи зловмисні програми, які можуть призвести до витоку або пошкодження даних. Підтримка з боку розробників, регулярне оновлення баз даних та наявність можливості евристичного аналізу роблять антивірусні програми ефективними у виявленні нових, ще невідомих загроз [34].

Системи управління доступом є невід'ємною частиною кіберзахисту. Вони дозволяють контролювати, хто має право доступу до інформаційних ресурсів ЗОЗ і в якому обсязі. Завдяки цим системам можна забезпечити надійний захист від несанкціонованого доступу. Системи управління доступом базуються на ідентифікації користувачів за допомогою паролів, шифрування даних і різноманітних таблиць контролю доступу. Вони також включають зовнішні засоби, такі як брандмауери і пристрої захисту портів, що дозволяють блокувати непотрібні або небезпечні з'єднання [14].

Ще одним важливим компонентом є система резервного копіювання та відновлення даних. Вона дозволяє оперативно відновити інформацію у разі її втрати або пошкодження. Система резервного копіювання має два основні типи: повне резервне копіювання, яке робить точну копію всіх даних, та диференційне резервне копіювання, яке зберігає тільки зміни, внесені після останнього повного бекапу. Для покращення надійності часто використовують також додаткові методи, такі як інкрементне резервне копіювання, що дозволяє зберігати лише нові або змінені дані з моменту останнього резервного копіювання.

Засоби шифрування є незамінними для забезпечення конфіденційності даних. Вони дозволяють перетворювати інформацію в такий вигляд, що її можна прочитати тільки за допомогою відповідного ключа шифрування. Цей процес дозволяє захистити дані від несанкціонованого доступу, особливо коли йдеться про передачу чутливої інформації через мережу.

Крім цього, у сучасних інформаційних системах важливу роль відіграють сканери вразливостей. Ці інструменти дозволяють автоматично знаходити слабкі місця в мережі або програмному забезпеченні, що можуть бути використані зловмисниками для проникнення в систему. Вони допомагають своєчасно виявляти загрози та мінімізувати ризики безпеки.

Моніторинг і аналіз поведінки користувачів є ще однією важливою складовою технологічного захисту. Спеціалізоване програмне забезпечення для моніторингу дозволяє стежити за діяльністю користувачів системи, виявляючи аномалії, які можуть свідчити про спроби зловмисного проникнення або витоку даних. Ці інструменти допомагають своєчасно реагувати на інциденти безпеки, попереджаючи про можливі загрози.

Не менш важливими є засоби виявлення вторгнень (IDS) та запобігання вторгнень (IPS). Системи IDS активно моніторять мережу та інші компоненти інформаційної інфраструктури на предмет спроб вторгнення або інших підозрілих дій. Вони сигналізують про порушення, що дає змогу швидко реагувати на загрози. Системи IPS, в свою чергу, не тільки виявляють вторгнення, а й активно блокують їх, захищаючи ресурси організації [34].

Окремо слід зазначити використання пісочниць – спеціальних середовищ, що дозволяють запускати потенційно небезпечні програми або файли в ізольованому середовищі. Це дає змогу виявити їх шкідливі властивості без ризику для основної системи.

Інші інструменти, як брандмауери, інструменти глибокої перевірки пакетів та системи запобігання витоку інформації (DLP), також є важливими для забезпечення безпеки. Брандмауери контролюють вхідний і вихідний трафік, дозволяючи лише авторизованим з'єднанням доступ до мережі, а DLP–системи блокують спроби передачі конфіденційної інформації без відповідного дозволу.

Технологічна складова кіберзахисту є комплексним набором інструментів і методів, що дозволяють забезпечити безпеку інформаційних систем, зменшити ризики втрати або пошкодження даних та протидіяти зовнішнім загрозам. Використання сучасних засобів кіберзахисту є важливою складовою в діяльності

медичних установ, де інформація про пацієнтів є надзвичайно чутливою та потребує надійного захисту від зловмисних атак.

Таким чином, забезпечення кібербезпеки потребує комплексного підходу, що включає не лише технологічні інструменти, але й постійне вдосконалення політик, навчання персоналу та вдосконалення стратегій захисту, що дозволяє успішно протидіяти сучасним кіберзагрозам.

Висновки до розділу 1

Виявлено, що кібербезпека є критично важливою складовою стійкого функціонування сучасного бізнесу, який активно інтегрується в цифрове середовище. В умовах стрімкої цифровізації та зростання кількості кіберзагроз, вона перетворилася з технічної необхідності на стратегічний пріоритет організацій. Її ефективне забезпечення вимагає комплексного підходу – поєднання технічних засобів захисту, регламентації внутрішніх процесів, навчання персоналу та дотримання законодавчих норм. Кібербезпека виконує не лише захисну функцію, а й забезпечує довіру до бізнесу з боку клієнтів, партнерів та інвесторів, сприяючи його конкурентоспроможності, стійкості та дотриманню міжнародних стандартів. Враховуючи динаміку розвитку кіберзлочинності, для сучасних компаній важливо не лише реагувати на інциденти, а й передбачати ризики, розробляти проактивні стратегії управління ними та інтегрувати кібербезпеку в загальну систему корпоративного управління.

Ефективне управління кібербезпекою у сучасному бізнес–середовищі передбачає поєднання кількох концепцій і підходів, орієнтованих на запобігання, виявлення, реагування та адаптацію до нових кіберзагроз. Впровадження ризик–орієнтованого мислення, багаторівневого захисту, внутрішніх політик безпеки, системного навчання персоналу та відповідність міжнародним стандартам є

ключовими чинниками забезпечення стійкості до кіберризиків. Комплексне поєднання проактивних, реактивних та адаптивних стратегій дозволяє організаціям зменшити потенційні втрати, захистити критичні активи та забезпечити безперервність діяльності в умовах зростаючої цифрової загрози.

Отже, ефективне забезпечення кібербезпеки в сучасних організаціях потребує комплексного підходу, який охоплює як технічні, так і організаційні аспекти захисту інформації. Ключовими елементами такого підходу є запобігання загрозам, своєчасне їх виявлення та оперативна нейтралізація наслідків. Використання антивірусного програмного забезпечення, брандмауерів, систем виявлення вторгнень, аналітики великих даних та штучного інтелекту дозволяє істотно підвищити рівень інформаційної безпеки. Водночас людський фактор залишається вразливим місцем, що зумовлює необхідність постійного навчання персоналу. Тільки скоординоване впровадження технологічних рішень і політик безпеки забезпечує організаціям стійкість до сучасних кіберзагроз.

РОЗДІЛ 2. АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ В БІЗНЕС–СЕРЕДОВИЩІ

2.1. Аналіз фінансово–економічного стану організації

ТОВ «Нова пошта» розпочала свою діяльність у 2001 році, зосередившись на оперативній доставці документів і вантажів для приватних осіб та бізнесу. Статутний капітал компанії, який становить 412 тисяч гривень, був сформований її засновниками – Інною Степанівною Попершнюк, Володимиром Анатолійовичем Попершнюком та В'ячеславом Валерійовичем Климовим.

На сьогодні мережа «Нової пошти» налічує понад 6000 відділень у більш ніж 318 містах і населених пунктах країни, а їхня кількість постійно збільшується. Окрім стаціонарних точок, компанія надає кур'єрські послуги, що дає змогу клієнтам отримувати посилки за індивідуальним графіком.

ТОВ «Нова пошта» охоплює як українські, так і закордонні організації. До її складу входять: «Нова пошта» (відповідає за перевезення відправлень до відділень і за адресами), «НП Логістик» (надає послуги складського зберігання та логістики), «ПОСТ ФІНАНС» (забезпечує фінансові перекази та електронні платежі) і «Нова Пошта Глобал» (спеціалізується на міжнародних перевезеннях).

Організація має понад 32 тисячі працівників різного віку, статі, кваліфікації та професійного досвіду. Постійно вдосконалюючи свої сервіси, «Нова пошта» орієнтується на міжнародні логістичні стандарти та дотримується вимог українського законодавства. Для зручності клієнтів застосовуються різні моделі доставки: «Склад–Склад», «Склад–Двері», «Двері–Склад» і «Двері–Двері» [24].

Спочатку компанія працювала переважно у сфері доставки між фізичними особами (C2C), однак завдяки модернізації процесів та технологій вона успішно вийшла на ринок електронної комерції. Ставши стратегічним партнером

численних інтернет–магазинів в Україні, компанія з 2009 року демонструє стабільний ріст, збільшуючи обсяг відправлень і розширюючи свою мережу відділень.

Як один із провідних операторів логістичного ринку України, «Нова пошта» приділяє велику увагу інноваціям у сфері управління проєктами, що сприяє її конкурентоспроможності. Впровадження сучасних технологій, таких як автоматизація процесів, штучний інтелект для оптимізації маршрутів і розробка мобільних застосунків, допомагає компанії не лише підвищити ефективність, а й оперативно реагувати на зміни ринку та потреби клієнтів.

Проведемо фінансово–економічний аналіз діяльності ТОВ «Нова Пошта» за 2022–2024 роки, який дозволяє оцінити фінансовий стан організації, її здатність інвестувати в захист інформаційних активів і протистояти кіберзагрозам, описаним вище у пункті 1.1, таким як зовнішні атаки та внутрішні загрози.

У таблиці 2.1 проведемо аналіз основних показників балансу ТОВ «Нова Пошта».

Таблиця 2.1

Динаміка основних показників балансу ТОВ «Нова Пошта»

Фінансові показники	Абсолютне відхилення, +,–. тис.грн		Відносне відхилення, +,–, %	
	2023/2022	2024/2023	2023/2022	2024/2023
Активи	7346786	8364877	146,63	136,20
Оборотні активи	–8345	–15687	98,02	96,21
Гроші та еквіваленти	405745	1580303	160,24	246,42
Поточні зобов'язання	2805180	2491417	151,46	130,18
Довгострокові зобов'язання	1549370	3793389	140,91	171,07

Джерело: створено автором на основі [30,31,32]

Динаміка балансових показників ТОВ «Нова Пошта» демонструє значне зростання активів: на 7,35 млн грн у 2023 році на 8,36 млн грн у 2024 році. Це зростання відображає розширення операційної діяльності, зокрема інвестиції в логістичну інфраструктуру, а саме в термінали та поштомати «Новобокс» та цифрові платформи, такі як NovaPay. Збільшення активів свідчить про фінансовий потенціал організації для впровадження систем кіберзахисту, таких як SIEM–системи (Splunk, QRadar) чи багатофакторної аутентифікація (MFA), що знижують ризики кіберзагроз, описаних вище у Розділі 1.

Оборотні активи незначно скоротилися на 1,98% у 2023 році та на 3,79% у 2024 році, що може вказувати на оптимізацію запасів або перерозподіл ресурсів на необоротні активи, як–от IT–інфраструктура. Водночас зростання грошових коштів та їх еквівалентів на 60,24% у 2023 році та на 146,42% у 2024 році є позитивним сигналом, оскільки забезпечує ліквідність для фінансування превентивних заходів кібербезпеки, наприклад, сканування вразливостей (Nessus) чи навчання персоналу через платформи, як KnowBe4, що знижують ризик соціальної інженерії.

Поточні зобов'язання зросли на 51,46% у 2023 році та на 30,18% у 2024 році, що відображає зростання операційних витрат, пов'язаних із розширенням логістичних і цифрових сервісів. Довгострокові зобов'язання також значно зросли на 40,91% у 2023 році та на 71,10% у 2024 році, що може бути пов'язано з інвестиційними кредитами на розвиток інфраструктури. Це зростання зобов'язань підвищує фінансові ризики, які необхідно враховувати при бюджетуванні кібербезпеки, оскільки обмежені ресурси можуть ускладнити реактивний підхід типу швидкого відновлення після атак.

Аналіз балансових показників ТОВ «Нова Пошта» демонструє фінансовий потенціал організації для забезпечення кіберстійкості. Значне зростання активів і грошових коштів створює можливості для реалізації проактивного підходу до кібербезпеки, зокрема впровадження стандартів ISO/IEC 27001, етичного хакерства чи резервного копіювання. Ці заходи знижують ризик зовнішніх загроз, таких як програми–вимагачі чи кібершпигунство, які можуть

скомпрометувати дані клієнтів у системі NovaPay. Зростання грошових коштів також підтримує адаптивний підхід, наприклад, використання ШІ та UEBA (Exabeam) для виявлення аномалій.

Однак незначне скорочення оборотних активів і зростання зобов'язань вказують на потенційні ризики ліквідності, які можуть обмежити бюджет на кібербезпеку. Це підкреслює важливість ризик–орієнтованого підходу, який передбачає пріоритизацію захисту критичних активів, а саме платіжних систем чи логістичних платформ. Зростання зобов'язань також може бути пов'язано з інвестиціями в IT–інфраструктуру, що підвищує потребу в комплексному підході для ахисту від DDoS–атак чи витоків даних.

У таблиці 2.2 наведено динаміку доходів і витрат ТОВ «Нова Пошта» у 2022–2024 роках.

Таблиця 2.2

Динаміка доходів і витрат ТОВ «Нова Пошта» у 2022–2024 роках

Фінансові показники	Абсолютне відхилення, +,– тис.грн		Відносне відхилення, +,– %	
	2023/2022	2024/2023	2023/2022	2024/2023
Чистий дохід від реалізації продукції	12781845	8310978	153,96	122,79
Собівартість реалізованої продукції	9348505	6659672	148,49	123,26
Валовий прибуток	3433340	1651306	177,84	121,05
Фінансовий результат від операційної діяльності: прибуток	1277926	599647	150,50	115,74
Адміністративні витрати	1312657	1223509	178,45	140,98
Витрати на збут	417152	51945	96,46	106,06
Фінансові витрати	360527	786227	140,61	162,99

Джерело: створено автором на основі [30,31,32]

Чистий дохід організації зріс на 53,96% у 2023 році і на 22,79% у 2024 році, що відображає розширення логістичних і цифрових сервісів, зокрема системи NovaPay. Це зростання доходу створює фінансові можливості для інвестицій у кібербезпеку, наприклад, у системи моніторингу чи кіберстрахування, що знижують ризики витоків даних.

Собівартість реалізованої продукції також зросла, що пов'язано зі збільшенням операційних витрат на логістику та цифрові платформи. Однак валовий прибуток значно збільшився на 77,84% у 2023 році, і на 21,05% у 2024 році відповідно, що свідчить про ефективне управління витратами. Цей прибуток підтримує фінансування адаптивних стратегій кібербезпеки, таких як ШІ для аналізу поведінки користувачів.

Прибуток від операційної діяльності зріс на 50,50% у 2023 році, але темпи зростання сповільнилися у 2024 році, а саме на 15,74%, що може бути пов'язано зі зростанням адміністративних витрат на 78,45% у 2023 році, та на 40,98% у 2024 році. Ці витрати включають, ймовірно, інвестиції в IT–інфраструктуру та навчання персоналу, що є частиною проактивного підходу до кібербезпеки. Витрати на збут зросли незначно лише на 6,06% у 2024 році, тоді як фінансові витрати значно збільшилися на 62,99% у 2024 році, що може відображати кредити на розвиток цифрових сервісів, які потребують посиленого захисту від кібершпигунства чи DDoS–атак.

Аналіз доходів і витрат ТОВ «Нова Пошта» підкреслює її фінансовий потенціал для забезпечення кіберстійкості. Значне зростання чистого доходу і валового прибутку створює ресурси для реалізації комплексного підходу до кібербезпеки, включаючи шифрування, брандмауери і системи IAM. Ці заходи знижують ризик зовнішніх загроз, таких як фішинг чи програми–вимагачі, які можуть порушити роботу платіжних систем NovaPay.

Зростання адміністративних витрат і фінансових витрат вказує на інвестиції в IT–інфраструктуру та розвиток сервісів, що підвищує потребу в ризик–орієнтованому підході для захисту критичних активів. Сповільнення зростання операційного прибутку може обмежити бюджет на реактивні заходи,

такі як швидке відновлення після атак, що підкреслює важливість превентивних стратегій типу сканування вразливостей, тренінги з кібергігієни. Аналіз цих показників надає можливість оцінити здатність організації фінансувати кіберзахист, забезпечуючи безперервність операцій і довіру клієнтів у цифрову епоху.

Надалі проведемо аналіз показнікі ліквідності, фінансової стійкості, рентабельності та ділової активності організації, представлені на рисунках 2.1–2.4., який демонструє, як фінансовий потенціал організації впливає на реалізацію підходів до управління кібербезпекою.

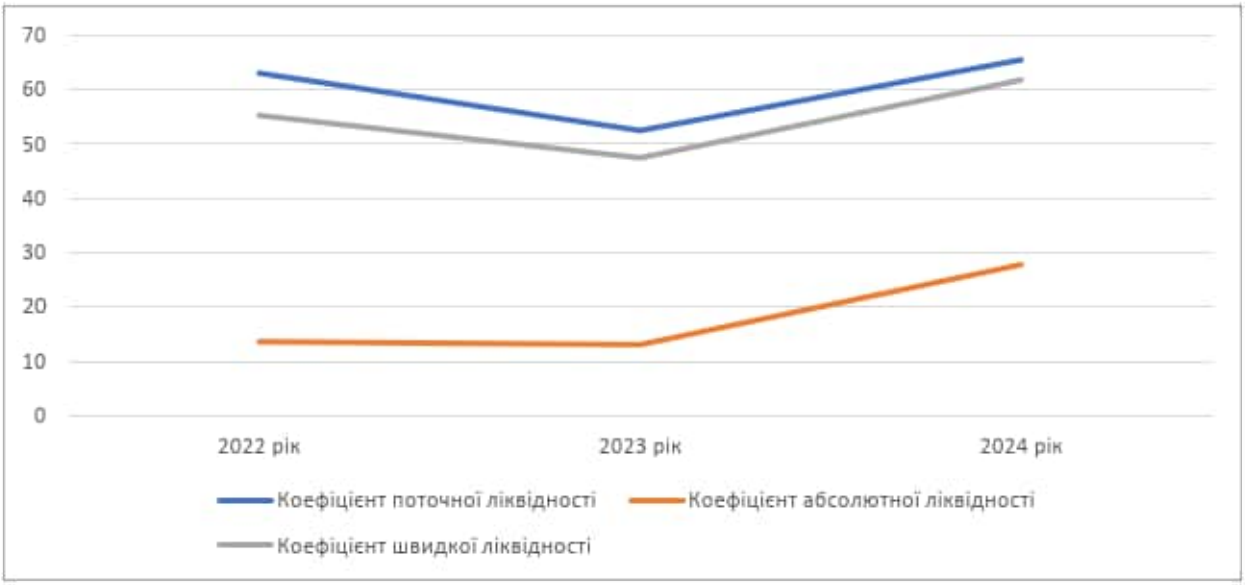

Рис.2.1. Динаміка коефіцієнтів ліквідності ТОВ «Нова Пошта» за 2022–2024 рр.

Джерело: створено автором на основі [30,31,32]

Коефіцієнт поточної ліквідності знизився з 63,03% у 2022 році до 52,47% у 2023 році через зростання поточних зобов'язань на 51,17%, але відновився до 65,48% у 2024 році завдяки збільшенню грошових коштів на 145,95%. Коефіцієнт абсолютної ліквідності зріс із 13,12% у 2023 році до 27,84% у 2024 році, що відображає значне накопичення грошових коштів. Коефіцієнт швидкої ліквідності також покращився з 47,46% у 2023 році до 61,77% у 2024 році. Ці

зміни свідчать про підвищення здатності організації покривати короткострокові зобов'язання, що в свою чергу може підтримати фінансування кібербезпеки.

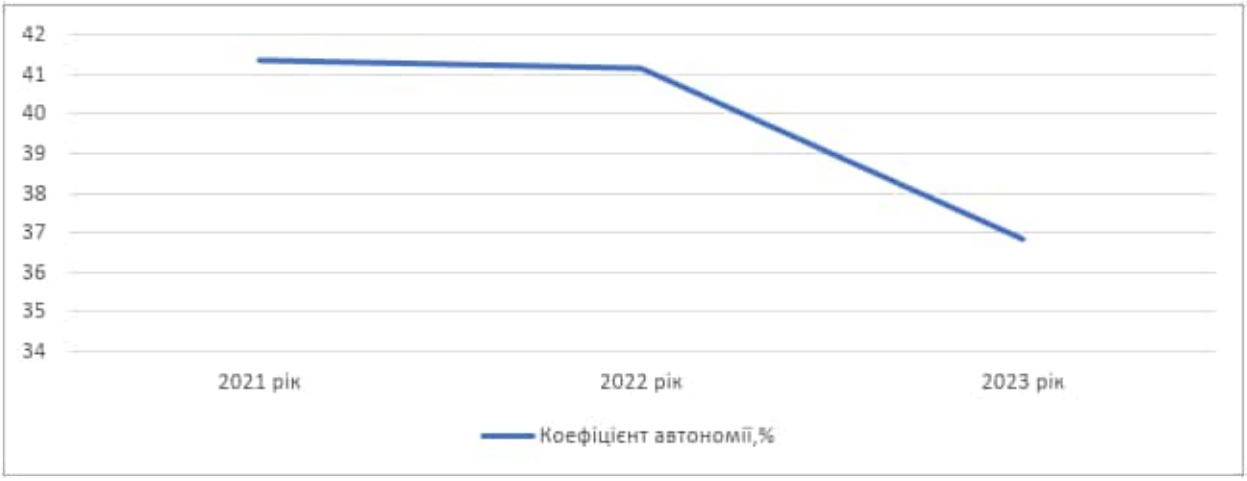

Рис.2.2. Динаміка коефіцієнта автономії ТОВ «Нова Пошта» за 2022–2024 рр.

Джерело: створено автором на [30,31,32]

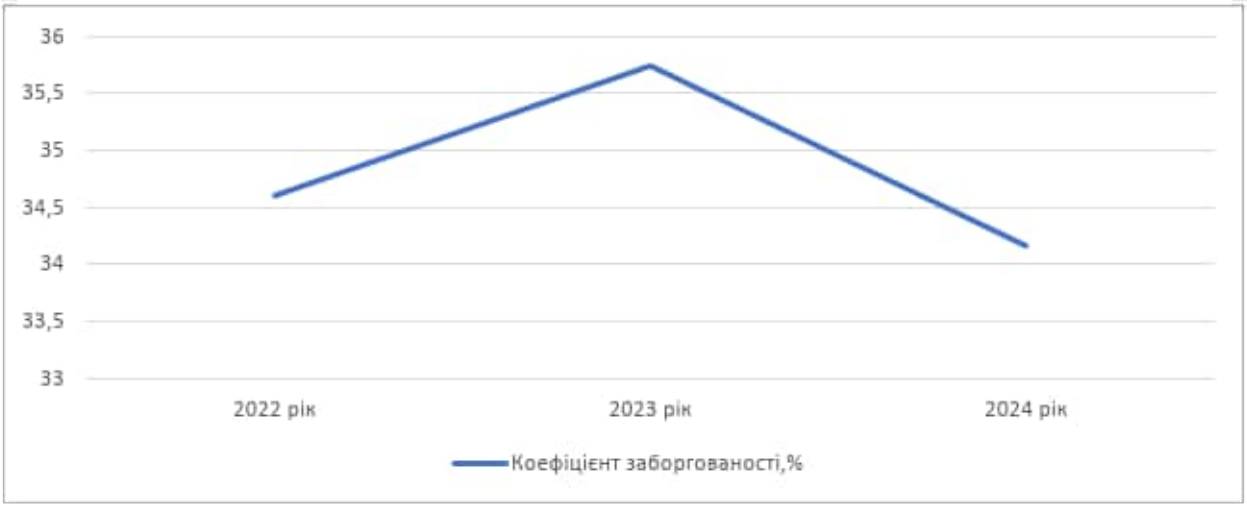

Рис.2.3. Динаміка коефіцієнта заборгованості ТОВ «Нова Пошта» за 2022–2024 рр.

Джерело: створено автором на основі [30,31,32]

Коефіцієнт автономії незначно знизився, що пов'язано зі зростанням довгострокових зобов'язань. Коефіцієнт заборгованості залишався відносно стабільним в розмірі 34,60–35,74%, що вказує на помірну залежність від

позичених коштів. Це дозволяє організації інвестувати в кіберзахист, але зниження автономії вимагає обережного планування.

Тепер на рис. 2.4. проаналізуємо показники рентабельності

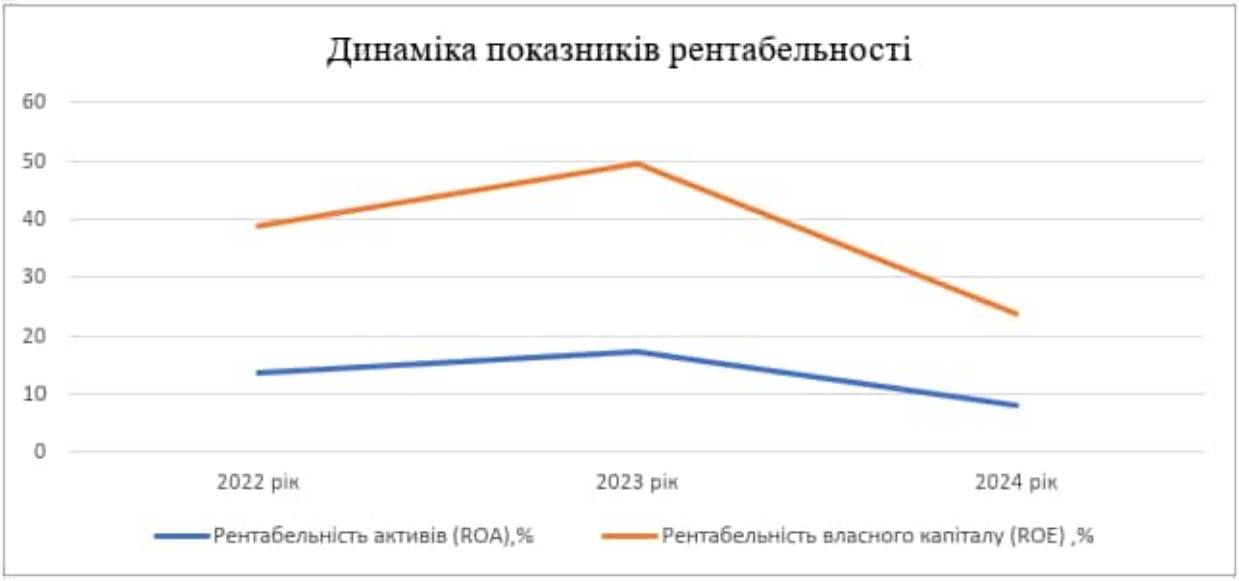

Рис.2.4. Динаміка показників рентабельності ТОВ «Нова Пошта» за 2022–2024 рр.

Джерело: створено автором на основі [30,31,32]

Рентабельність активів (ROA) зросла з 13,56% у 2022 році до 17,17% у 2023 році, але знизилася до 7,95% у 2024 році, що може бути пов'язано зі зростанням активів на 36,22% і витрат. В свою чергу, рентабельність власного капіталу (ROE) також знизилася з 49,51% у 2023 році до 23,70% у 2024 році, що відображає меншу ефективність використання власного капіталу. Ці зміни вказують на потребу в оптимізації витрат для підтримки інвестицій у кібербезпеку.

Зниження коефіцієнта автономії (–4,53% у 2024 році) і стабільна заборгованість (34,16%) вказують на зростання фінансових ризиків, що вимагає ризик–орієнтованого підходу для пріоритизації захисту критичних систем, таких як NovaPay. Падіння рентабельності може обмежити бюджет на адаптивні стратегії, такі як ШІ чи UEBA, що необхідні для протидії новим загрозам, як–от

атаки на ланцюги постачання. Аналіз цих показників є ключовим для оцінки фінансових можливостей організації інвестувати в кібербезпеку, забезпечуючи сталість операцій і довіру клієнтів у цифрову епоху.

Проведений аналіз ліквідності, фінансової стійкості та рентабельності ТОВ «Нова Пошта» демонструє її здатність протистояти кіберзагрозам, але також виявляє виклики, що впливають на кіберстійкість. Підвищення коефіцієнта абсолютної ліквідності і поточної ліквідності забезпечує ресурси для реалізації проактивного підходу, через впровадження MFA чи тренінгів із кібергігієни через KnowBe4, що знижують ризик фішингу та соціальної інженерії. Зростання ліквідності також підтримує реактивний підхід, наприклад, швидке відновлення після DDoS–атак за допомогою резервного копіювання (Veeam).

2.2. Оцінка рівня кіберзагроз і вразливостей організації

Оцінка рівня кіберзагроз і вразливостей інформаційних систем ТОВ «Нова Пошта» є ключовим етапом для забезпечення кіберстійкості організації в умовах цифрової економіки та геополітичних викликів. Як провідний оператор логістичних і фінансових послуг в Україні, ТОВ «Нова Пошта» оперує розвиненою цифровою інфраструктурою, що включає платіжну систему NovaPay, автоматизовані поштомати «Новобокс» і онлайн–платформи для обробки замовлень. Ця інфраструктура обробляє значні обсяги персональних даних клієнтів, фінансових транзакцій і логістичної інформації, що робить організацію привабливою мішенню для кіберзагроз, класифікованих у пункті 1.1 як зовнішні та внутрішні. Проведений у пункт 2.1 фінансовий аналіз підтвердив зростання активів і чистого доходу, що забезпечує ресурси для кібербезпеки, але також виявив зниження рентабельності активів і зростання довгострокових зобов'язань, які в свою чергу можуть обмежувати інвестиції в захист. У контексті

російської кіберагресії, що посилилася з 2014 року та досягла піку після повномасштабного вторгнення у 2022 році, оцінка загроз набуває стратегічного значення для захисту критичної інфраструктури.

ТОВ «Нова Пошта» функціонує в умовах високого ризику кіберзагроз через інтенсивне використання інформаційно–комунікаційних технологій у логістичних операціях, обробці даних і фінансових транзакціях. Для систематизації оцінки кіберзагроз, що загрожують ТОВ «Нова Пошта», нижче наведено таблицю 2.3, яка узагальнює зовнішні та внутрішні загрози, їхній потенційний вплив, ймовірність і специфіку для організації.

Таблиця 2.3

Оцінка кіберзагроз для ТОВ «Нова Пошта»

Тип загрози	Опис загрози	Потенційний вплив	Ймовірність	Специфіка для ТОВ «Нова Пошта»
Зовнішні загрози				
Фішингові атаки	Розсилка підроблених листів чи SMS для викрадення PII (логіни, паролі, дані карток)	Витік даних клієнтів, репутаційні втрати, фінансові збитки.	Висока	Фішинг 2024 року з повідомленнями про заборгованість для клієнтів NovaPay
DDoS–атаки	Перевантаження серверів онлайн–платформ чи поштоматів для зупинки сервісів	Перебої в логістиці, втрата доходу (середня вартість 1,2 млн дол. США	Середня	Атака на сайт чи API NovaPay, що зупиняє обробку замовлень
Програми–вимагачі	Шифрування даних у логістичних чи платіжних системах із вимогою викупу	Параліч операцій, збитки	Висока	Атака на логістичну систему, що блокує відстеження посилок
Кібершпигунство	Несанкціонований доступ до стратегічних даних (маршрути, клієнтські бази)	Втрата конкурентної переваги, репутаційні ризики	Середня	Викрадення даних про клієнтів NovaPay для конкурентів чи державних акторів

Продовження таблиці 2.3

Внутрішні загрози				
Людський фактор	Помилки працівників (перехід за підозрілими посиланнями, слабкі паролі)	Витік даних, компрометація систем	Висока	Співробітник відкриває фішинговий лист, надаючи доступ до системи NovaPay
Системні вразливості	Застаріле ПЗ чи незахищені API у поштоматах чи платіжних системах	Несанкціонований доступ, витік даних (17% витоків через API	Середня	Вразливість в API NovaPay, що дозволяє доступ до даних клієнтів

Джерело:створено автором на основі [22]

Серед зовнішніх кіберзагроз, з якими стикається ТОВ «Нова Пошта», особливу увагу привертають фішингові атаки, які є одними з найпоширеніших методів кіберзлочинців у фінансовому секторі. Ці атаки передбачають розсилку підроблених електронних листів, SMS або створення фальшивих вебсайтів, що імітують офіційні ресурси компанії, з метою викрадення конфіденційних даних, таких як логіни, паролі чи банківські реквізити. Клієнти NovaPay, які активно користуються платіжними сервісами, а також працівники компанії стають потенційними цілями таких кампаній. Згідно зі звітом Verizon DBIR 2024, 36% усіх кібератак у фінансовому секторі пов'язані саме з фішингом, що підкреслює їхню високу актуальність. Наприклад, у грудні 2024 року ТОВ «Нова Пошта» зіткнулася з масштабною фішинговою атакою, коли зловмисники розсилали повідомлення про нібито заборгованість, перенаправляючи користувачів на фальшиві сайти для введення особистих даних. Такі інциденти не лише загрожують безпеці клієнтів, але й можуть призвести до значних репутаційних втрат, адже довіра до бренду є ключовим активом компанії. Крім того, успішна фішингова атака може відкрити доступ до внутрішніх систем, що створює додаткові ризики для операційної діяльності.

Іншою серйозною зовнішньою загрозою є розподілені атаки на відмову в обслуговуванні, відомі як DDoS–атаки, які спрямовані на перевантаження

серверів онлайн–платформ або поштоматів, що призводить до зупинки логістичних операцій. Оскільки "Нова Пошта" значною мірою залежить від безперебійної роботи своїх цифрових сервісів, таких як вебсайт, мобільний додаток і API для обробки замовлень, DDoS–атаки можуть спричинити суттєві перебої в обслуговуванні клієнтів. Звіт IBM Security 2024 оцінює середню вартість однієї такої атаки в 1,2 мільйона доларів США, враховуючи втрати доходу, витрати на відновлення та репутаційні збитки. Для компанії, яка обробляє тисячі посилок щодня, навіть короткочасна зупинка може призвести до значних фінансових втрат і незадоволення клієнтів. Наприклад, атака на сервери NovaPay може тимчасово унеможливити проведення платежів, тоді як перевантаження системи поштоматів може порушити доступ до посилок, що особливо критично в пікові періоди, такі як святковий сезон.

Програми–вимагачі, або ransomware, представляють ще одну значну зовнішню загрозу, яка може паралізувати діяльність компанії. Це шкідливе програмне забезпечення шифрує критичні дані в логістичних або платіжних системах, вимагаючи викуп за їхнє розшифрування. Історичний приклад атаки NotPetya 2017 року, яка завдала логістичним і фінансовим організаціям збитків на суму 10 мільярдів доларів США, демонструє руйнівний потенціал таких загроз. Для ТОВ «Нова Пошта» подібна атака може заблокувати доступ до системи відстеження посилок, зупинити обробку замовлень або порушити роботу платіжної системи NovaPay, що призведе до тривалих перебоїв у роботі та значних фінансових втрат. Навіть якщо викуп буде сплачено, немає гарантії відновлення даних, а репутація компанії може серйозно постраждати через витік інформації про інцидент. У контексті російської кіберагресії, яка активно використовує подібні методи для дестабілізації української економіки, ризик таких атак для ТОВ «Нова Пошта» залишається надзвичайно високим.

Кібершпигунство є ще однією зовнішньою загрозою, яка загрожує комерційній таємниці та конкурентоспроможності компанії. Зловмисники, включаючи конкурентів або державних акторів, можуть прагнути отримати несанкціонований доступ до стратегічних даних, таких як логістичні маршрути,

клієнтські бази, фінансові звіти чи плани розширення. Для ТОВ «Нова Пошта», яка є лідером на українському ринку логістики, такі дані мають високу цінність, а їхній витік може послабити позиції компанії на ринку або бути використаним для шантажу. Наприклад, викрадення клієнтської бази NovaPay може дозволити конкурентам пропонувати цільові послуги, тоді як доступ до логістичних маршрутів може бути використаний для організації атак на ланцюги постачання.

Переходячи до внутрішніх кіберзагроз, слід зазначити, що людський фактор залишається однією з найслабших ланок у системі кібербезпеки ТОВ «Нова Пошта». Помилки працівників, такі як перехід за підозрілими посиланнями, введення облікових даних на фішингових сайтах або використання слабких паролів, є причиною 68% кіберінцидентів, як зазначає Verizon DBIR 2024. З урахуванням того, що в компанії працює понад 28 тисяч осіб, включаючи логістів, операторів поштоматів, працівників кол–центрів і офісний персонал, масштаб цього ризику є значним. Наприклад, якщо співробітник випадково відкриває фішинговий лист, це може надати зловмисникам доступ до внутрішніх систем, таких як платіжна платформа NovaPay, що поставить під загрозу дані клієнтів. Відсутність регулярних тренінгів із кібергігієни або недостатня обізнаність персоналу про сучасні методи атак, такі як соціальна інженерія, ще більше посилюють цю проблему. У контексті великої кількості працівників, навіть поодинокі помилки можуть мати катастрофічні наслідки, що вимагає системного підходу до навчання та підвищення кіберграмотності.

Системні вразливості, пов'язані з технічною інфраструктурою, є ще однією внутрішньою загрозою, яка створює точки входу для зловмисників. Застаріле програмне забезпечення, яке не отримує регулярних оновлень безпеки, або незахищені API в системах NovaPay чи поштоматах можуть бути використані для несанкціонованого доступу до даних. Вразливості в API є причиною 17% витоків даних у фінансових організаціях, що особливо актуально для ТОВ «Нова Пошта», враховуючи інтеграцію її платіжної системи з зовнішніми сервісами. Наприклад, недостатньо захищений API у платформі NovaPay може дозволити зловмисникам отримати доступ до фінансових транзакцій або персональних

даних клієнтів, що призведе до значних збитків. Аналогічно, поштомати «Новобокс», які підключені до мережі, можуть бути скомпрометовані через вразливості в їхньому програмному забезпеченні, що поставить під загрозу безпеку посилок і довіру клієнтів. Відсутність регулярного сканування вразливостей або несвоєчасне оновлення систем підвищує ймовірність таких інцидентів, що вимагає від компанії посилення технічних заходів захисту.

Фінансовий аналіз, проведений у попередніх розділах, підкреслює, що зростання активів і доходу ТОВ «Нова Пошта» робить її привабливою мішенню для кіберзлочинців, які прагнуть отримати фінансову вигоду або стратегічну інформацію. Водночас зростання довгострокових зобов'язань і зниження рентабельності активів створюють обмеження для фінансування кібербезпеки, що може ускладнити впровадження сучасних технологій захисту, таких як системи SIEM, багатофакторна аутентифікація чи інструменти на основі штучного інтелекту. У поєднанні з російською кіберагресією, яка активно спрямована на критичну інфраструктуру України, ці фактори створюють складне середовище, в якому ТОВ «Нова Пошта» мусить постійно адаптуватися до нових загроз. Зокрема, зростання кількості атак, таких як фішинг чи програми–вимагачі, з початком воєнного стану підкреслює необхідність комплексного підходу до кібербезпеки, який би охоплював як зовнішні, так і внутрішні ризики, щоб забезпечити стійкість бізнес–процесів і захист даних клієнтів.

Російська кіберагресія, що активізувалася після Революції Гідності 2014 року та досягла піку з початком повномасштабного вторгнення у 2022 році, становить системну загрозу для українських організацій, зокрема тих, що належать до критичної інфраструктури, як ТОВ «Нова Пошта».

У грудні 2024 року ТОВ «Нова Пошта» зазнала фішингової атаки з підробленими повідомленнями про заборгованість. Підрозділ кібербезпеки оперативно заблокував сервери та попередив клієнтів, демонструючи реактивний підхід. Виходячи з аналізу слід зазначити, що зростання атак вимагає проактивних (KnowBe4) і адаптивних (ШІ, UEBA) заходів.

Проведений вище у пункті 2.1 фінансовий аналіз вказує на обмеження бюджету через зобов'язання, що вимагає ризик–орієнтованого підходу.

У таблиці 2.4 проведемо SWOT–аналіз кібербезпеки ТОВ «Нова Пошта», що є інструментом стратегічного аналізу, який дозволяє систематизувати внутрішні та зовнішні фактори, які впливають на здатність організації протистояти кіберзагрозам і забезпечувати стійкість бізнес–процесів у цифровому середовищі. Цей аналіз охоплює сильні сторони, слабкі сторони, можливості та загрози, які відображають поточний стан кібербезпеки компанії, враховуючи її специфіку як лідера логістичного ринку України з розвиненою цифровою інфраструктурою, включаючи платіжну систему NovaPay, автоматизовані поштомати «Новобокс» і онлайн–платформи. Детальний розгляд кожної категорії SWOT–аналізу забезпечує глибоке розуміння сильних і слабких аспектів організації, а також зовнішніх перспектив і ризиків.

Таблиця 2.4

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)
• Фінансовий потенціал (дохід 44,78 млрд грн у 2024 році, +22,79%) • IT–інфраструктура (NovaPay, поштомати) для SIEM, MFA, UEBA • Клієнтська база, що мотивує захист даних • Досвід цифрової трансформації	• Зниження автономії та зростання зобов'язань • Людський фактор через 28 тис. працівників • Відсутність сертифікації ISO/IEC 27001. • Обмежена інформація про витрати на кіберзахист
Можливості (Opportunities)	**Загрози (Threats)**
• ШІ та UEBA (Exabeam) для адаптивного захисту • Сертифікація ISO/IEC 27001 • Кіберстрахування • Тренінги KnowBe4	• Російська кіберагресія (фішинг, DDoS, HermeticWiper) • Атаки на ланцюги постачання • Юридичні ризики GDPR • Репутаційні втрати через витоки даних

Джерело: створено автором на основі [22,30,31,32]

Сильні сторони кібербезпеки ТОВ «Нова Пошта» відображають внутрішні ресурси та конкурентні переваги, які сприяють захисту від кіберзагроз. Значний фінансовий потенціал організації, підтверджений зростанням чистого доходу, є

ключовим активом, що дозволяє інвестувати в сучасні технології кіберзахисту, такі як системи моніторингу безпеки (SIEM), багатофакторна аутентифікація (MFA) або інструменти на основі штучного інтелекту для виявлення аномалій (UEBA). Цей фінансовий ресурс дає змогу компанії реагувати на зростаючі кіберзагрози, зокрема фішингові атаки чи програми–вимагачі, які потребують значних витрат на протидію. Розвинена IT–інфраструктура, що включає платіжну систему NovaPay, поштомати та онлайн–сервіси, забезпечує технічну основу для інтеграції передових рішень безпеки. Наприклад, NovaPay може використовувати сучасні протоколи шифрування (TLS 1.3) для захисту фінансових транзакцій, а поштомати – системи сканування вразливостей (Nessus) для запобігання компрометації. Широка клієнтська база, яка охоплює мільйони користувачів по всій Україні, є додатковим стимулом для компанії підтримувати високий рівень захисту даних, оскільки втрата довіри клієнтів може призвести до значних репутаційних і фінансових збитків. Досвід цифрової трансформації, накопичений під час розширення мережі поштоматів і запуску NovaPay, дозволяє організації швидко адаптувати нові технології, такі як хмарні рішення для резервного копіювання (Veeam) або системи аналізу поведінки користувачів (Exabeam), що відповідає принципам CIA–тріади. Ці сильні сторони створюють міцну основу для проактивного підходу до кібербезпеки, дозволяючи компанії не лише реагувати на інциденти, але й запобігати їм.

Слабкі сторони кібербезпеки ТОВ «Нова Пошта» вказують на внутрішні обмеження, які знижують ефективність захисту від кіберзагроз. Зниження коефіцієнта автономії і зростання довгострокових зобов'язань створюють фінансові обмеження, що можуть скоротити бюджет на впровадження дорогих технологій, таких як SIEM–системи (Splunk) або інструменти адаптивного захисту (UEBA). Високий ризик людського фактора, пов'язаний із великою кількістю працівників, є ще однією слабкою стороною. Помилки персоналу, такі як перехід за фішинговими посиланнями чи використання слабких паролів, є причиною 68% кіберінцидентів, як вказує Verizon DBIR 2024 [35]. Відсутність підтверджених даних про регулярні тренінги з кібергігієни, наприклад, за

програмами KnowBe4, посилює цей ризик, оскільки працівники можуть бути недостатньо підготовленими до розпізнавання сучасних атак, таких як соціальна інженерія. Відсутність сертифікації за міжнародними стандартами, зокрема ISO/IEC 27001, знижує прозорість системи кібербезпеки та може викликати недовіру з боку клієнтів і партнерів, особливо в контексті обробки PII через NovaPay. Обмежена інформація про структуру та обсяг витрат на кіберзахист ускладнює оцінку рівня готовності організації до нових загроз, таких як атаки на ланцюги постачання, що є актуальними в умовах російської кіберагресії. Ці слабкі сторони вказують на необхідність посилення внутрішніх процесів і ресурсного забезпечення для підвищення кіберстійкості.

Можливості, визначені в SWOT–аналізі, відображають зовнішні перспективи, які ТОВ «Нова Пошта» може використати для вдосконалення кібербезпеки. Впровадження технологій штучного інтелекту та аналізу поведінки користувачів (UEBA), таких як платформа Exabeam, дозволяє виявляти аномалії в реальному часі, що є ефективним для протидії складним загрозам, таким як фішинг чи програми–вимагачі. Сертифікація за стандартом ISO/IEC 27001 може не лише підвищити довіру клієнтів і партнерів, але й забезпечити структурований підхід до управління ризиками, що відповідає принципам ISO/IEC 27005 [40]. Кіберстрахування є ще однією можливістю, яка дозволяє мінімізувати фінансові ризики від кіберінцидентів, таких як витоки даних чи зупинка операцій через DDoS–атаки. Впровадження програм тренінгів із кібергігієни, наприклад, KnowBe4, може значно знизити ризик людського фактора, який є причиною 68% інцидентів. Ці можливості у контексті зростання кіберагресії стають стратегічно важливими для забезпечення конкурентоспроможності та безпеки.

Загрози, виділені в SWOT–аналізі, відображають зовнішні ризики, які ускладнюють захист інформаційних систем ТОВ «Нова Пошта». Ескалація російської кіберагресії, що призвела до зростання кіберінцидентів є основною загрозою. Атаки, такі як фішинг, DDoS або шкідливе програмне забезпечення типу HermeticWiper, спрямовані на критичну інфраструктуру, можуть зупинити

логістичні операції або скомпрометувати дані NovaPay. Атаки на ланцюги постачання, які стають дедалі поширенішими, загрожують порушенням логістичних маршрутів, що є критично важливим для компанії, яка щодня обробляє тисячі посилок. Юридичні ризики, пов'язані з можливим порушенням Загального регламенту захисту даних (GDPR), передбачають штрафи до 20 млн євро, що становить значну загрозу для фінансової стабільності, особливо враховуючи зростання зобов'язань організації. Репутаційні втрати через витоки даних, особливо в системі NovaPay, можуть підірвати довіру клієнтів і партнерів, що є критичним для компанії з широкою клієнтською базою. Ці загрози посилюються в умовах гібридної війни, де кібератаки використовуються для економічної дестабілізації, що вимагає від організації посилення захисних заходів.

Виявлені проблеми кібербезпеки ТОВ «Нова Пошта» є результатом аналізу кіберзагроз, російської кіберагресії та SWOT–аналізу, і відображають ключові недоліки, які потребують негайного вирішення для забезпечення стійкості організації. Недостатній захист від внутрішніх загроз, спричинений людським фактором, є однією з основних проблем. Велика кількість працівників і брак підтверджених даних про регулярні тренінги з кібергігієни підвищують імовірність помилок, таких як перехід за фішинговими посиланнями, що є причиною 68% кіберінцидентів. Наприклад, працівник, який випадково відкриває підроблений лист, може надати зловмисникам доступ до системи NovaPay, що призведе до витоку даних клієнтів. Ця проблема суперечить проактивному підходу до кібербезпеки, описаному в пункті 1.2, який вимагає систематичного навчання персоналу для зниження ризиків.

Обмеження бюджету на кібербезпеку, спричинене зростанням довгострокових зобов'язань і зниженням рентабельності активів є ще однією значною проблемою. Ці фінансові обмеження, виявлені в пункті 2.1, ускладнюють інвестування в сучасні технології, такі як інструменти на основі штучного інтелекту (UEBA) або системи резервного копіювання (Veeam), які

необхідні для протидії новим загрозам, таким як атаки на ланцюги постачання чи програми–вимагачі типу HermeticWiper.

Відсутність сертифікації за міжнародними стандартами, зокрема ISO/IEC 27001, є ще однією проблемою, яка знижує прозорість і надійність системи кібербезпеки. Без такої сертифікації організація стикається з підвищеними юридичними ризиками, оскільки невідповідність вимогам GDPR може призвести до штрафів до 20 млн євро. Крім того, брак сертифікації може викликати недовіру з боку клієнтів і партнерів, особливо в контексті обробки PII через NovaPay, що є критичним для підтримки репутації. Ця проблема може бути зумовлена недостатньою увагою до стандартизації процесів або обмеженими ресурсами для підготовки до сертифікації, що вимагає стратегічного перегляду пріоритетів.

Вразливість цифрових платформ, таких як NovaPay і поштомати, до зовнішніх атак, зокрема DDoS і шкідливого ПЗ типу HermeticWiper, становить серйозну проблему. Ці платформи є ключовими для операційної діяльності, але їхня залежність від ІКТ робить їх уразливими до атак, які можуть зупинити логістичні операції або скомпрометувати дані клієнтів. Наприклад, DDoS–атака на сервери NovaPay може унеможливити обробку платежів, а компрометація поштоматів через вразливості в API може порушити доступ до посилок. Ця проблема порушує принципи CIA–тріади, оскільки загрожує доступності та конфіденційності даних. Причиною може бути недостатнє тестування вразливостей або застаріле програмне забезпечення, що вимагає регулярного оновлення та сканування систем.

Брак кіберстрахування є ще однією проблемою, яка підвищує фінансові ризики від кіберінцидентів. Без страхування організація може зіткнутися з повним обсягом збитків від атак, таких як програми–вимагачі чи витоки даних, що особливо критично в умовах зростання кіберагресії. Наприклад, атака типу NotPetya, яка завдала збитків на 10 млрд доларів США [42], могла б мати менший фінансовий вплив за наявності страхування. Ця проблема може бути зумовлена

недостатньою оцінкою ризиків або обмеженим бюджетом, що підкреслює необхідність перегляду фінансової стратегії.

Ці проблеми, виявлені на основі аналізу кіберзагроз, російської кіберагресії та SWOT–аналізу, є взаємопов'язаними та вимагають комплексного підходу до їхнього вирішення. Недостатній захист від людського фактора, бюджетні обмеження, брак сертифікації, вразливість платформ і відсутність кіберстрахування створюють значні ризики для операційної діяльності та репутації ТОВ «Нова Пошта». У контексті зростання кіберагресії, зокрема атак типу HermeticWiper чи фішингу, ці недоліки можуть призвести до зупинки логістичних операцій, витоку даних клієнтів, юридичних штрафів і втрати довіри. Для їхньої ліквідації необхідно впровадити проактивні заходи, такі як тренінги з кібергігієни, адаптивні технології (ШІ, UEBA), сертифікацію ISO/IEC 27001 і кіберстрахування.

Висновки до розділу 2

Фінансово–економічний аналіз ТОВ «Нова пошта» за 2022–2024 роки підтверджує її сильну фінансову позицію, яка підтримує реалізацію підходів до управління кібербезпекою. Зростання активів, чистого доходу і грошових коштів створює ресурси для впровадження комплексного підходу, включаючи шифрування, брандмауери та навчання персоналу. Однак зростання зобов'язань і зниження рентабельності вказують на виклики, що вимагають ризик–орієнтованого підходу для оптимізації витрат на кіберзахист. Ці показники є критичними для оцінки здатності організації протистояти кіберзагрозам, забезпечуючи безперервність бізнес–процесів і конкурентоспроможність.

Оцінка кіберзагроз ТОВ «Нова Пошта» виявила високий рівень ризиків, посилених російською кіберагресією з початком воєнних дій. Систематизовано загрози, що підкреслило вразливість NovaPay і поштоматів.

SWOT–аналіз виявив сильні сторони організації, такі як фінансовий потенціал і розвинена IT–інфраструктура, які дозволяють інвестувати в проактивні заходи, наприклад, SIEM–системи чи MFA, що відповідає принципам CIA–тріади. Проте слабкі сторони, зокрема зниження автономії, зростання зобов'язань і людський фактор, обмежують можливості для реалізації дорогих рішень, таких як UEBA. Можливості, включаючи сертифікацію ISO/IEC 27001, кіберстрахування та тренінги KnowBe4, пропонують перспективу підвищення кіберстійкості, тоді як загрози, такі як російська кіберагресія, юридичні ризики GDPR і репутаційні втрати, створюють значні виклики. Ці результати підкреслюють необхідність адаптивного підходу до кібербезпеки, який поєднує реактивні та проактивні заходи.

Виявлені проблеми, зокрема недостатній захист від людського фактора, бюджетні обмеження, відсутність сертифікації, вразливість платформ і брак кіберстрахування, є критичними бар'єрами для забезпечення безпеки. Людський фактор, що спричиняє 68% інцидентів, посилюється відсутністю підтверджених тренінгів, що суперечить проактивним підходам. Фінансові обмеження, зумовлені зниженням рентабельності, ускладнюють інвестиції в захист від атак на ланцюги постачання чи програм–вимагачів. Відсутність сертифікації ISO/IEC 27001 підвищує юридичні ризики, тоді як вразливість NovaPay і поштоматів до DDoS і HermeticWiper загрожує доступності та конфіденційності даних. Брак кіберстрахування залишає організацію відкритою до фінансових збитків.

РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ ЕФЕКТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В ОРГАНІЗАЦІЇ

3.1. Обгрунтування заходів з підвищення рівня кіберзахисту

Ефективне управління кібербезпекою в ТОВ «Нова Пошта» вимагає системного підходу до вирішення виявлених проблем, зокрема: недостатній захист від людського фактора, бюджетні обмеження, відсутність сертифікації ISO/IEC 27001, вразливість цифрових платформ до зовнішніх атак і брак кіберстрахування. Ці проблеми створюють значні ризики для операційної діяльності, репутації та фінансової стабільності організації, особливо в умовах ескалації російської кіберагресії і фінансових викликів. Для їхнього вирішення розглядається широкий спектр заходів, які оцінюються за критеріями ефективності, вартості, складності впровадження, часу реалізації та відповідності специфіці організації, яка є лідером логістичного ринку України з розвиненою ІКТ–інфраструктурою, великою кількістю працівників і значним фінансовим потенціалом. Аналіз ґрунтується на принципах CIA–тріади, адаптивного та ризик–орієнтованого підходів, а також розглянутих вище інструментах і технологіях кібербезпеки. Вибір оптимальних заходів спрямований на забезпечення кіберстійкості організації в умовах гібридної війни, мінімізацію юридичних ризиків, пов'язаних із GDPR, і підтримку конкурентоспроможності на ринку шляхом підвищення довіри клієнтів до цифрових сервісів, зокрема фінансових операцій через NovaPay, що обробляє значні обсяги транзакцій. Комплексний підхід передбачає поєднання проактивних (тренінги, стандартизація) і реактивних (страхування, захист від DDoS) заходів, які враховують як поточні загрози, так і стратегічні цілі організації, забезпечуючи баланс між безпекою, економічною доцільністю та операційною ефективністю.

Стратегічні переваги посилення кібербезпеки для ТОВ «Нова Пошта» виходять за межі захисту внутрішніх процесів, створюючи основу для міжнародної експансії та зміцнення глобальної репутації. Як організація, що активно розвиває цифрові сервіси, зокрема NovaPay, яка конкурує на ринку фінансових технологій, ТОВ «Нова Пошта» може використати кібербезпеку як конкурентну перевагу для залучення міжнародних партнерів і клієнтів. Відповідність стандартам безпеки і впровадження передових технологій сигналізують про надійність організації, що є критично важливим для укладання контрактів із європейськими логістичними операторами та фінансовими установами. У контексті зростання кіберагресії, демонстрація стійкості до атак, підвищує довіру інвесторів і підтримує амбіції організації щодо виходу на нові ринки, де кібербезпека є ключовим критерієм оцінки партнерів. Таким чином, інвестиції в кібербезпеку не лише захищають активи, але й трансформують організацію в глобального гравця, здатного відповідати вимогам цифрової економіки.

Довгострокова стійкість організації залежить від її здатності інтегрувати інноваційні рішення та адаптуватися до нових кіберзагроз, що постійно еволюціонують. У контексті гібридної війни та зростання складності атак, таких як HermeticWiper, ТОВ «Нова Пошта» потребує гнучкої архітектури безпеки, яка поєднує хмарні технології, ШІ–аналітику та стандартизовані процеси. Впровадження таких рішень забезпечує не лише захист від поточних ризиків, але й створює платформу для швидкого реагування на майбутні виклики. Для організації з 28 тисячами працівників і розвиненою мережею поштоматів це дає можливість масштабувати безпеку без значного зростання витрат, зберігаючи операційну ефективність. Такий підхід підтримує стратегічну мету сталого розвитку, забезпечуючи безперервність бізнес–процесів у динамічному середовищі.

Відповідність глобальним трендам кібербезпеки, зокрема принципам ESG – екологічне, соціальне та корпоративне управління, є додатковим фактором, що підвищує цінність запропонованих заходів для ТОВ «Нова Пошта».

Кібербезпека все частіше розглядається як складова соціальної відповідальності, оскільки захист даних клієнтів і працівників сприяє довірі суспільства та знижує ризики репутаційних втрат. Для організації, що оперує платформою NovaPay, яка обробляє чутливі фінансові дані, впровадження заходів, спрямованих на забезпечення конфіденційності, відповідає очікуванням регуляторів і клієнтів у контексті GDPR. Крім того, використання енергоефективних хмарних рішень і оптимізація ІКТ–інфраструктури сприяють екологічним аспектам ESG, що є важливим для залучення інвестицій і партнерства в Європі. Таким чином, кібербезпека стає не лише технічним, але й стратегічним інструментом, який гармонізує бізнес–цілі організації з глобальними стандартами відповідального управління.

Для реалізації стратегічного потенціалу кібербезпеки та забезпечення стійкості ТОВ «Нова Пошта» детально проаналізуємо ключові проблеми, що загрожують її ІКТ–інфраструктурі, і обиремо оптимальний комплекс заходів, які ефективно усунуть ці ризики, відповідаючи фінансовим можливостям і операційним потребам організації.

Першою проблемою є – недостатній захист від людського фактора, який є причиною 68% кіберінцидентів, зумовлена великою кількістю працівників і відсутністю підтверджених даних про регулярні тренінги з кібергігієни. Для її вирішення розглядаються чотири заходи: регулярні тренінги з кібергігієни (KnowBe4), багатофакторна аутентифікація (MFA, Duo Security), системи аналізу поведінки користувачів (UEBA, Exabeam) і розгортання внутрішньої кампанії з кіберобізнаності. Тренінги KnowBe4 – це хмарна платформа, яка пропонує модулі з розпізнавання фішингу, соціальної інженерії та інших атак, а також симуляції атак для практичного навчання. Для ТОВ «Нова Пошта» цей захід є ефективним, оскільки дозволяє навчити 28 тис. працівників розпізнавати фішингові листи, знижуючи ризик компрометації систем, таких як NovaPay. Переваги включають масштабованість, адаптивність контенту до нових загроз і відносно низьку вартість, приблизно 20 грн/користувач/місяць, або 6,72 млн грн/рік для 28 тис. осіб. Недоліками є потреба в регулярному оновленні контенту

та часі працівників, що може ускладнити навчання для логістів із щільним графіком.

В свою чергу MFA (Duo Security) додає додатковий рівень аутентифікації через SMS–коди чи біометрію, ускладнюючи доступ зловмисників навіть при викраденні паролів. Цей захід є швидким у впровадженні – 1–2 місяці і недорогим, близько 10 грн/користувач/місяць, або 3,36 млн грн/рік, але може викликати незручності для працівників і клієнтів NovaPay, знижуючи зручність сервісу.

UEBA (Exabeam) використовує ШІ для аналізу поведінки користувачів, виявляючи аномалії, такі як несанкціонований доступ до логістичних систем. Це високоефективне рішення для складних атак, але його висока вартість (понад 20 млн грн для початкового впровадження) і складність інтеграції роблять його менш доцільним у контексті бюджетних обмежень ТОВ «Нова Пошта», так як рентабельність активів у 2024 році знизилась до 7,95%. Внутрішня кампанія з кіберобізнаності шляхом плакатів та розсилок є найдешевшою, близько 0,5 млн грн/рік, але її ефективність обмежена через пасивний характер і низьку залученість працівників. Тому слід зазначити, що тренінги KnowBe4 є оптимальними, оскільки адресують першопричину, саме людський фактор, мають помірну вартість і масштабованість, ідеально відповідаючи великій кількості працівників і потребі протидії фішингу.

Другою проблемою є бюджетні обмеження, спричинені зростанням довгострокових зобов'язань і зниженням рентабельності активів, що обмежує інвестиції в дорогі технології, такі як SIEM чи UEBA. Розглядаються чотири заходи: хмарні рішення (Microsoft Azure), грантове фінансування (USAID), кіберстрахування (AIG) і аутсорсинг кібербезпеки. Хмарні рішення Microsoft Azure з вбудованими інструментами безпеки Microsoft Defender та Sentinel дозволяють оптимізувати витрати, замінюючи фізичні сервери хмарною інфраструктурою, що забезпечує захист NovaPay і поштоматів. До переваг можна віднести економію – близько 10 млн грн/рік порівняно з локальними серверами, гнучкість масштабування та інтеграцію з SIEM–функціоналом.

Недоліками є ризики міграції даних і залежність від постачальника. Відповідно для ТОВ «Нова Пошта» хмарні рішення Microsoft Azure є доцільними, оскільки знижують капітальні витрати, враховуючи зростання зобов'язань.

Щодо грантового фінансування від USAID Cybersecurity Activity, то воно може покрити витрати на SIEM (Splunk) чи сертифікацію ISO/IEC 27001, що є актуальним в умовах російської кіберагресії . Перевагою є відсутність прямих витрат, але доступ до грантів є конкурентним, а процес подання заявки тривалий від 6 до 12 місяців.

В свою чергу кіберстрахування AIG мінімізує фінансові ризики від інцидентів, таких як DDoS–атаки чи програм–вимагачів, із покриттям до 50 млн грн за річний внесок близько 5 млн грн. Недоліком є те, що страховка не запобігає атакам, лише компенсує збитки. Аутсорсинг кібербезпеки забезпечує доступ до експертизи, але коштує дорого – понад 15 млн грн/рік і знижує контроль над процесами. Тому для цієї проблеми – оптимальними є хмарні рішення Azure і кіберстрахування AIG, оскільки вони балансують економію та захист, враховуючи фінансовий стан організації.

Третою проблемою є відсутність сертифікації ISO/IEC 27001, що підвищує юридичні ризики GDPR і знижує довіру клієнтів. В цій ситуації можна розглянути три заходи, такі як – сертифікація ISO/IEC 27001, впровадження NIST CSF і часткова стандартизація процесів. Сертифікація ISO/IEC 27001 передбачає розробку системи управління інформаційною безпекою (СУІБ), аудит і сертифікацію, що забезпечує структурований підхід до ризиків. Її вартість становить 2–3 млн грн, а тривалість – 6–12 місяців, але вона підвищує довіру до NovaPay і знижує юридичні ризики. Недоліком є високі витрати та потреба в організаційних змінах. NIST CSF – є гнучким фреймворком, який фокусується на ідентифікації, захисті та відновленні, коштує дешевше – близько 1 млн грн і впроваджується за 3–6 місяців, але має меншу ринкову вагу. Часткова стандартизація, а саме оновлення політик безпеки є найдешевшою – 0,3 млн грн, але не усуває ризиків GDPR. Тому для вирішення цієї проблеми оптимальним є

ISO/IEC 27001 оскільки фінансовий потенціал організації дозволяє покрити витрати, а сертифікація зміцнить репутацію.

Четвертою проблемою є вразливість цифрових платформ до DDoS–атак і шкідливого програмного забезпечення типу HermeticWiper, що загрожує доступності та конфіденційності даних. Для її вирішення розглядаються чотири заходи: SIEM–системи (Splunk), захист від DDoS (Cloudflare), сканування вразливостей (Nessus) і оновлення програмного забезпечення. SIEM (Splunk) забезпечує моніторинг у реальному часі, виявляючи атаки на NovaPay, але коштує дорого – понад 25 млн грн для впровадження і потребує кваліфікованого персоналу. Cloudflare захищає від DDoS–атак шляхом фільтрації трафіку, є доступним – близько 2 млн грн/рік і швидким у впровадженні –1 місяць, але не вирішує внутрішніх вразливостей. Nessus сканує API та ПЗ поштоматів, виявляючи слабкі місця, коштує помірно – 1,5 млн грн/рік і є простим у використанні, але потребує регулярності. Оновлення рограмного забезпечення є базовим заходом коштує коштує – 0,5 млн грн/рік, але не захищає від нових загроз. Серед наведених заходів, оптимальними є Cloudflare і Nessus, оскільки вони адресують зовнішні (DDoS) та внутрішні (API) загрози за помірною вартістю.

Останньою п'ятою проблемою є брак кіберстрахування, що підвищує фінансові ризики від інцидентів. Для вирішення цієї проблеми можна розглянути два заходи: кіберстрахування AIG і створення резервного фонду. AIG пропонує покриття до 50 млн грн за внесок – 5 млн грн/рік, що захищає від збитків типу NotPetya. Перевагою є швидке відшкодування, недоліком – регулярні внески. Резервний фонд забезпечує гнучкість, але заморожує капітал. Тому кіберстрахування AIG є оптимальним, оскільки ефективніше розподіляє ризики.

Відповідно оптимальний набір заходів включає: тренінги KnowBe4, хмарні рішення Microsoft Azure, кіберстрахування AIG, сертифікацію ISO/IEC 27001, Cloudflare і Nessus. Цей вибір обґрунтований їхньою ефективністю в адресуванні всіх проблем, помірною вартістю з загальною оцінкою 20–25 млн грн/рік, швидкістю впровадження – від 3 до 12 місяців і відповідністю фінансовому стану

ТОВ «Нова Пошта». KnowBe4 знижує ризик людського фактора, Azure і AIG оптимізують бюджет, ISO/IEC 27001 усуває юридичні ризики, а Cloudflare і Nessus захищають платформи.

Стратегічна цінність запропонованого набору заходів для ТОВ «Нова Пошта» полягає в його здатності забезпечити довгострокову кіберстійкість і підтримати амбітні цілі організації як лідера логістичного ринку України в умовах глобалізації та цифровізації. Інтеграція тренінгів KnowBe4, хмарних рішень Azure, страхування AIG, сертифікації ISO/IEC 27001, Cloudflare і Nessus формує синергетичний ефект, що виходить за межі негайного усунення виявлених вразливостей. Цей підхід відповідає глобальним трендам кібербезпеки, зокрема акценту на гібридних моделях захисту, які поєднують технологічні, організаційні та фінансові інструменти. Для ТОВ «Нова Пошта» це означає не лише захист критичних активів, таких як NovaPay, але й зміцнення позицій на міжнародному ринку шляхом демонстрації відповідності високим стандартам безпеки, що є конкурентною перевагою в логістичному секторі. Крім того, інвестиції в кібербезпеку у розмірі 27,52 млн грн/рік становить лише 0,06% доходу, що є економічно обґрунтованим вкладенням для запобігання потенційних збитків. У контексті гібридної війни та зростання кіберагресії, цей набір заходів забезпечує адаптивність до нових загроз, сприяючи сталому розвитку організації та довірі стейкхолдерів, що є основою для її стратегічного успіху в цифровій економіці.

3.2. Оцінка економічної ефективності запропонованих заходів

На основі проведено аналізу проблем та варіантів заходів щодо їх вирішення для забезпечення кібербезпеки ТОВ «Нова Пошта» обрано два заходи: тренінги KnowBe4 (проти фішингу) і захист від DDoS–атак Cloudflare. Вибір обґрунтовано їхньою економічною ефективністю, швидким

впровадженням і адресуванням ключових загроз. Як було зазначено вище фішинг становить 68% інцидентів у логістиці, а шахрайські листи від імені компанії у 2024 році підкреслюють потребу в KnowBe4. DDoS–атаки становлять 30% інцидентів, що загрожує стабільності NovaPay, що в свою чергу робить Cloudflare актуальним. Заходи мають низькі витрати (5,81 млн грн/рік, 0,013% доходу), швидке впровадження (1–3 місяці) і значні ефекти (20,09 млн грн/рік у базовому сценарії), що відповідає фінансовим можливостям організації та її масштабу: 28 тис. працівників, 37,210 точок, платформа NovaPay. Альтернативи, такі як Azure (10,50 млн грн/рік) чи AIG (5,10 млн грн/рік) є ще більш дорожчими.

Для забезпечення фінансової доцільності KnowBe4 впроваджується частково– для 14 тис. працівників, найбільш вразливих до фішингу, що знижує витрати до 3,71 млн грн/рік. Cloudflare застосовується для захисту всієї інфраструктури NovaPay (витрати 2,10 млн грн/рік). Сумарні витрати становлять 5,81 млн грн/рік, що є мінімальним навантаженням на бюджет організації.

У таблиці 3.1. наведено витрати на впровадження KnowBe4.

Таблиця 3.1.

Витрати на на впровадження KnowBe4

Стаття витрат	Сума, млн.грн
Ліцензії (14,000 працівників)	3,36
Технічна підтримка	0,25
Адаптація контенту	0,10
Загальні витрати	3,71

Джерело: складено автором

Таблиця 3.2.

Витрати на на впровадження Cloudflare

Стаття витрат	Сума, млн.грн
Ліцензії	2,00
Налаштування DNS	0,10
Загальні витрати	2,10

Джерело: складено автором

У таблиці 3.2. наведено витрати на впровадження Cloudflare.

Для забезпечення прозорості та фінансової доцільності витрати на KnowBe4 і Cloudflare розбито за статтями, враховуючи одноразові (налаштування та адаптацію) та регулярні (ліцензії та підтримка) витрати. Часткове впровадження KnowBe4 лише для 14 тис. працівників знижує витрати вдвічі порівняно з повним охопленням, зберігаючи значну ефективність. Cloudflare застосовується до всієї інфраструктури NovaPay, що виправдано через залежність від API. Разом загальні витрати за рік на впровадження цих заходів склали: 5,81 млн грн, що є посильним для ТОВ «Нова Пошта».

Для оцінки ефектів використано дані розділу 2, збитки від кіберінцидентів становлять в середньому 50 млн грн/рік, з яких фішинг відповідає за 68%, а DDoS–атаки – за 30%. Додатково враховано зниження продуктивності через інциденти на 10%.

Часткове впровадження для 14 тис. працівників, 50% персоналу, фокусується на операторах і менеджерах, найбільш вразливих до соціальної інженерії. Планується зниження фішингових інцидентів на 6% (50% від 12% для повного впровадження). Для ТОВ «Нова Пошта» ефект обмежено через часткове впровадження і високу інтенсивність атак. Крім того, 30% працівників відзначають низьку обізнаність із кібербезпекою, що знижує початкову ефективність тренінгів. Тому обрано консервативну оцінку – 6% зниження інцидентів, що відповідає нижній межі аналогів. Зменшення людських помилок через фішинг покращує ефективність обробки транзакцій NovaPay, але ефект обмежено через часткове охоплення та необхідність адаптації працівників до тренінгів.

Cloudflare усуває ризики DDoS–атак, які становлять 30% інцидентів. Планується зниження таких атак на 10%. Для ТОВ «Нова Пошта» ефект обмежено через складність інтеграції з мережею поштоматів і залежність від зовнішніх провайдерів. Проте висока автоматизація NovaPay сприяє швидкому розгортанню (1–2 місяці), тому обрано 10% зниження інцидентів, що відповідає нижній межі аналогів.

Сумарна економія за оптимістичним і песимістичним сценаріями наведена в таблиці 3.3.

Таблиця 3.3.

Економія від впровадження заходів за сценаріями

Заходи	Сценарій	Економія від інцидентів, млн. грн	Економія від продуктивності, млн. грн	Загальна економія, млн. грн
KnowBe4	Оптимістичний	4,20	5,64	9,84
	Песимістичний	1,80	2,42	4,22
Cloudflare	Оптимістичний	7,00	11,28	18,28
	Песимістичний	5,00	8,06	13,06
Загальна сума	Оптимістичний	11,20	16,92	28,12
	Песимістичний	4,80	7,26	12,06

Джерело: складено автором

Оцінка економічних ефектів від впровадження тренінгів проти фішингу та захисту від DDoS–атак підтверджує доцільність обраних заходів для забезпечення кібербезпеки організації. Прогнозована економія відображає обережний підхід, враховуючи зменшення фішингових атак і DDoS–інцидентів, а також підвищення продуктивності завдяки стабільності цифрових сервісів і зниженню людських помилок. Часткове застосування тренінгів дозволяє оптимізувати витрати, зосередившись на найбільш вразливих групах працівників, тоді як захист від DDoS охоплює всю інфраструктуру, що є критично важливим для безперебійної роботи фінансових сервісів. Фінансова ефективність заходів забезпечується завдяки поступовому зростанню ефектів та швидкому поверненню інвестицій навіть у найгірших умовах. Заходи демонструють високий потенціал для зниження ключових кіберзагроз, які домінують у структурі інцидентів, а їхня швидка реалізація відповідає потребам організації в оперативному захисті. Порівняно з альтернативними рішеннями, такими як хмарні платформи чи страхування, обрані заходи є більш

економічними, швидкими у впровадженні та спрямованими на запобігання загроз, а не лише компенсацію збитків. Впровадження заходів супроводжується ризиками, зокрема низькою залученістю персоналу до тренінгів і складністю інтеграції захисту в розгалужену мережу, однак ці виклики можна подолати через гейміфікацію навчання та залучення кваліфікованих фахівців. У перспективі доцільно розглядати додаткові заходи для комплексного захисту цифрових сервісів, що посилить стійкість організації до нових загроз.

При розрахунках грошових потоків для заходів KnowBe4 і Cloudflare ,чисті потоки в усіх сценаріях залишаються позитивними, що забезпечує фінансову доцільність заходів, особливо в умовах швидкого впровадження та високої актуальності захисту від фішингу й DDoS–атак для організації.

У таблиці 3.4. наведено економічну оцінку ефективності заходів.

Таблиця 3.4.

Економічна оцінка ефективності заходів

Показник	Оптимістичний сценарій	Базовий сценарій	Песимістичний сценарій
NPV, млн. грн	31,05	16,96	2,87
IRR, %	70	50	25
Простий термін окупності, місяців	6,3	11,2	24,2
Дисконтований термін окупності, місяців	7,3	12,6	28,0

Джерело: складено автором

Економічна оцінка підтверджує високу ефективність: NPV позитивне у всіх сценаріях, відповідно – 31,05/16,96/2,87 млн грн. Простий термін окупності в оптимістичному сценарії склав 6,3 місяці, у базовому – 11,2 місяці, у песимістичному – 24,2 місяці. В свою чергу дисконтовані терміни 7,3/12,6/28,0 місяців підтверджують надійність результатів.

Аналіз економічної ефективності заходів із забезпечення кібербезпеки організації демонструє їхню високу фінансову доцільність і стратегічну цінність. Позитивна чиста приведена вартість у всіх сценаріях підтверджує, що вкладення в тренінги проти фішингу та захист від DDoS–атак окупаються навіть за найменш сприятливих умов, створюючи запас фінансової стійкості. Високі показники внутрішньої норми дохідності свідчать про значний потенціал заходів для генерації економічної вигоди, перевищуючи ринкові вимоги до прибутковості. Короткі терміни окупності, особливо в оптимістичному сценарії, підкреслюють швидке повернення інвестицій, що є критичним для організації з високою залежністю від цифрових сервісів. У песимістичному сценарії окупність залишається досяжною в межах планового періоду, що підтверджує надійність заходів у протидії ключовим кіберзагрозам, які домінують у структурі інцидентів. Порівняно з альтернативними рішеннями, такими як хмарні платформи чи страхування, обрані заходи вирізняються нижчими витратами, швидшим впровадженням і превентивним характером, що забезпечує захист репутації та стабільності фінансових операцій. Незважаючи на ризики, пов'язані з низькою залученістю персоналу до тренінгів і складністю інтеграції захисту, ці виклики можна подолати через адаптацію навчального процесу та залучення фахівців. У довгостроковій перспективі заходи створюють основу для впровадження додаткових рішень, що підвищить стійкість організації до нових викликів кібербезпеки.

Висновки до розділу 3

У ході проведеного порівняльного аналізу інструментів забезпечення інформаційної безпеки було визначено, що ефективний захист підприємства в умовах цифровізації потребує як технічних рішень, так і роботи з людським фактором. Серед розглянутих альтернатив оптимальними виявилися KnowBe4 –

платформа для підвищення обізнаності співробітників щодо кіберзагроз, яка дозволяє знизити ризики фішингових атак, соціальної інженерії та ненавмисних помилок користувачів, а також Cloudflare – хмарний сервіс, що забезпечує надійний захист від DDoS–атак, фільтрацію шкідливого трафіку та безперебійну роботу вебресурсів. Таким чином, комбінація KnowBe4 і Cloudflare створює комплексний багаторівневий захист, що охоплює як вразливості, пов'язані з поведінкою персоналу, так і інфраструктурні загрози з боку зовнішніх атак. Це дозволяє підприємству підвищити стійкість до кіберзагроз та забезпечити безпеку бізнес–процесів в умовах зростаючої цифрової взаємодії.

Оцінка економічної ефективності впровадження заходів із кібербезпеки в ТОВ «Нова Пошта» підтверджує їхню фінансову доцільність, оперативність реалізації та відповідність масштабам і потребам компанії. Запропоноване часткове впровадження тренінгів проти фішингу KnowBe4 для найбільш вразливих 14 тисяч працівників дозволило суттєво зменшити витрати, зберігаючи при цьому значну частину запланованого ефекту. Повне застосування Cloudflare до інфраструктури NovaPay забезпечує захист від DDoS–атак, що є критично важливим для безперервності фінансових операцій. Сукупні витрати на заходи в розмірі 5,81 млн грн/рік є незначними порівняно з масштабом діяльності організації та дозволяють досягти суттєвої економії (від 12,06 до 28,12 млн грн/рік залежно від сценарію), що свідчить про високу віддачу на вкладені інвестиції. Чиста приведена вартість залишається позитивною в усіх сценаріях, внутрішня норма дохідності перевищує порогові значення, а строки окупності становлять від 6 до 28 місяців, що є прийнятним навіть у песимістичних умовах. Усі ці фактори підтверджують стратегічну доцільність обраних рішень як інструментів зниження ключових кіберризиків, збереження операційної стійкості та запобігання фінансовим втратам. Отже, впровадження тренінгів KnowBe4 та платформи Cloudflare не лише економічно обґрунтоване, а й сприяє формуванню довгострокової кіберстійкості організації в умовах зростаючих цифрових загроз.

ВИСНОВКИ

Кібербезпека є критично важливим елементом сучасного бізнес–середовища, де інформація виступає ключовим ресурсом, а кіберзагрози постійно зростають за своєю складністю та масштабами. Захист даних, комп'ютерних систем і мереж від зовнішніх і внутрішніх загроз, таких як фішинг, DDoS–атаки, шкідливе програмне забезпечення та витоки інформації, вимагає комплексного підходу, що поєднує технічні, організаційні та людські аспекти. Основні принципи кібербезпеки, такі як конфіденційність, цілісність і доступність, забезпечують надійний захист інформаційних активів, сприяючи стабільності бізнес–процесів, збереженню репутації та довіри клієнтів. Впровадження політик безпеки, дотримання міжнародних стандартів, таких як ISO/IEC 27001 і GDPR, а також підвищення обізнаності персоналу відіграють ключову роль у формуванні кіберстійкості організацій.

Ефективне управління кібербезпекою базується на різноманітних підходах, включаючи проактивний, реактивний, ризик–орієнтований, комплексний та адаптивний методи. Ці стратегії дозволяють організаціям не лише запобігати кібератакам, але й оперативно реагувати на інциденти, мінімізуючи їх наслідки. Використання сучасних технологій, таких як штучний інтелект, аналітика великих даних, системи виявлення вторгнень та шифрування, значно підвищує ефективність захисту. Водночас людський фактор залишається одним із найуразливіших елементів, що підкреслює необхідність регулярного навчання працівників і створення культури кібергігієни. Дотримання законодавчих вимог і стандартів безпеки сприяє не лише правовій відповідності, але й зміцненню конкурентоспроможності компаній у цифровій економіці.

Технологічна складова кібербезпеки відіграє центральну роль у забезпеченні захисту інформаційних систем. Інструменти, такі як антивірусне програмне забезпечення, брандмауери, системи управління доступом, резервне копіювання та сканери вразливостей, створюють багаторівневу систему захисту,

що дозволяє своєчасно виявляти, нейтралізувати та відновлювати системи після кібератак. Постійне оновлення програмного забезпечення, впровадження шифрування та використання адаптивних систем на основі ШІ забезпечують гнучкість і стійкість до нових загроз. У поєднанні з організаційними заходами, такими як розробка чітких політик безпеки та навчання персоналу, ці інструменти формують надійний фундамент для захисту даних, що є запорукою успішного функціонування організацій у сучасному цифровому світі.

Проведений фінансовий аналіз ТОВ «Нова Пошта» підтверджує її міцне економічне становище, яке створює основу для інвестицій у кібербезпеку, але також виявляє виклики, що впливають на кіберстійкість. Значне зростання доходів і активів відображає розширення логістичних і цифрових сервісів, зокрема платіжної системи NovaPay, що забезпечує ресурси для впровадження сучасних захисних технологій. Водночас зростання зобов'язань і зниження рентабельності вказують на обмеження бюджету, які вимагають ретельного планування витрат на захист від кіберзагроз. Збільшення ліквідності, зокрема грошових коштів, підтримує можливість реалізації як проактивних, так і реактивних заходів, спрямованих на протидію зовнішнім атакам і внутрішнім вразливостям. Однак фінансова залежність від позик і сповільнення зростання прибутковості підкреслюють необхідність ризик–орієнтованого підходу, що фокусується на захисті критичних активів, таких як платіжні платформи та логістична інфраструктура.

Оцінка кіберзагроз виявила високу вразливість організації до зовнішніх атак, таких як фішинг, DDoS і програми–вимагачі, які становлять серйозну небезпеку для операційної діяльності та репутації. Фішингові кампанії, що імітують офіційні повідомлення компанії, загрожують безпеці клієнтських даних, тоді як DDoS–атаки можуть зупинити цифрові сервіси, що є критично важливим для обробки тисяч щоденних транзакцій. Програми–вимагачі та кібершпигунство посилюють ризики, особливо в умовах російської кіберагресії, яка спрямована на дестабілізацію критичної інфраструктури. Ці загрози ускладнюються геополітичним контекстом, де зростання атак після 2022 року

вимагає від організації посилення захисту для забезпечення безперервності бізнес–процесів і збереження довіри клієнтів.

Внутрішні вразливості, зокрема людський фактор і технічні недоліки, є значними перешкодами для кібербезпеки. Помилки працівників, спричинені недостатньою кіберграмотністю, створюють точки входу для зловмисників, що особливо небезпечно для компанії з великою кількістю персоналу. Незахищені цифрові інтерфейси, такі як API платіжних систем, підвищують ризик несанкціонованого доступу до даних. Відсутність систематичних тренінгів і регулярного оновлення систем підкреслює потребу в комплексному підході до управління внутрішніми ризиками. Ці слабкі сторони вимагають негайних заходів, спрямованих на підвищення обізнаності персоналу та модернізацію технічної інфраструктури.

SWOT–аналіз кібербезпеки організації виявив сильні сторони, які можуть бути використані для протидії загрозам, а також можливості для вдосконалення захисту. Фінансовий потенціал і розвинена цифрова інфраструктура дозволяють інвестувати в передові технології, такі як системи моніторингу та аналізу поведінки користувачів, що підвищують здатність виявляти аномалії. Можливості сертифікації за міжнародними стандартами та впровадження кіберстрахування відкривають перспективи для підвищення довіри клієнтів і мінімізації ризиків. Проте зовнішні загрози, зокрема російська кіберагресія та юридичні вимоги щодо захисту даних, створюють складне середовище, яке вимагає адаптивних і превентивних стратегій для забезпечення безпеки.

Виявлені проблеми кібербезпеки, такі як недостатній захист від людського фактора, обмежений бюджет, брак сертифікації, вразливість платформ і відсутність страхування, є взаємопов'язаними та потребують комплексного вирішення. Ці недоліки посилюють ризики зупинки операцій, витоку даних і репутаційних втрат, що є неприпустимим для компанії, яка оперує великими обсягами транзакцій і даних. Для їх подолання необхідно впровадити тренінги з кібергігієни, модернізувати технічні системи, отримати міжнародну сертифікацію та розглянути страхування ризиків. Такий підхід не лише зміцнить

кіберстійкість організації, але й забезпечить її конкурентоспроможність і довіру клієнтів у цифровій економіці.

Запропоновані заходи, а саме тренінги KnowBe4 для 14 тисяч працівників і захист від DDoS–атак Cloudflare для всієї інфраструктури, є стратегічно обґрунтованими для підвищення кібербезпеки ТОВ «Нова Пошта», демонструючи високу ефективність у протидії фішингу, що становить 68% інцидентів, і DDoS–атакам, які охоплюють 30% загроз. Оцінка ефективності підтверджує, що при витратах 5,81 мільйона гривень на рік, що становить лише 0,013% доходу організації, заходи забезпечують економію 28,12 мільйона гривень в оптимістичному сценарії та 12,06 мільйона гривень у песимістичному, знижуючи збитки від кіберінцидентів і підвищуючи продуктивність. Чиста приведена вартість досягає 31,05 мільйона гривень в оптимістичному, 16,96 мільйона в базовому та 2,87 мільйона гривень у песимістичному сценаріях, а внутрішня норма дохідності варіюється від 25% до 70%, перевищуючи ринкові стандарти. Прості терміни окупності становлять від 6,3 до 24,2 місяця, що підкреслює швидке повернення інвестицій. Порівняно з альтернативами, такими як хмарні рішення за 10,50 мільйона гривень на рік чи страхування за 5,10 мільйона, ці заходи є економічнішими, швидшими у впровадженні за 1–3 місяці та превентивними, забезпечуючи захист критичних платформ, таких як NovaPay, і підтримуючи довіру клієнтів в умовах гібридної війни.

Комплексний підхід, реалізований через ці заходи, створює основу для довгострокової кіберстійкості, усуваючи вразливості та підвищуючи адаптивність до нових загроз. Економічна ефективність, підтверджена позитивними фінансовими показниками, дозволяє організації підтримувати безперервність операцій за витрат, що не перевищують 5,81 мільйона гривень щорічно. Швидке розгортання заходів мінімізує ризики, тоді як їхня здатність протидіяти домінуючим загрозам зміцнює конкурентні позиції. У перспективі ці заходи відкривають можливості для стандартизації процесів і додаткових рішень, сприяючи міжнародній експансії організації та її репутації надійного партнера в цифровій економіці.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.

2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. Навчальний посібник. Київ. 2019. 320 с.

3. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. Цифрова трансформація кібербезпеки: науково–практична інтернет–конференція, 20 квітня 2022, Державний університет телекомунікацій Навчально–наукового інститут захисту інформації. Київ, 2022. С. 31 33.

4. Волосович С. Детермінанти виникнення та реалізації кібер–ризиків. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 3. С. 101–115.

5. Герасимович І. А. Організація облікової політики сучасного підприємства. *Інвестиції: практика та досвід*. 2021. № 7. С. 49–53.

6. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security*. 2023. №19. С. 118–129.

7. Горбаченко С. А. IT-маркетинг: навчальний посібник. Одеса, 2024. 218 с. URL: https://hdl.handle.net/11300/27929

8. Грабчук І.Л. Організація захисту облікової інформації в умовах гібридної війни. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу*. 2018. №3 (41). С. 20–24.

9. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Одеса, 2019. 320 с.

10. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. *Адміністративне право і процес*. 2017. № 4. С. 99–107.

11. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*.2017. № 7. С.109-116.

12. Жила Г. Вища освіта в умовах війни: виклики, проблеми, перспективи для студентів та науковців. *Молодь і ринок*. 2023. № 2 (210). С. 141–145.

13. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук. -практ конф. молодих 8 учених, студентів і курсантів "Інформаційна безпека та інформаційні технології" (м. Львів, 26 листопада 2020 р.). Львів: ЛДУБЖД, 2020. С. 21–22.

14. Кібік О.М., Котлубай В.О., Хаймінова Ю.В., Рединa Є.В., Примаченко І.Ф. Економічна безпека. Одеса: Фенікс, 2018. 126 с.

15. Кібік О.М., Котлубай В.О., Хаймінова Ю.В., Рединa Є.В., Белоус К.В. Стратегічне управління. Антикризове управління: навч. посібник. Одеса. 2019. 208 с.

16. Кібік О.М., Котлубай В.О., Рединa Є.В., Хаймінова Ю.В., Белоус К.В., Скрипник М.О. Менеджмент організацій. Проектний менеджмент: навч.-метод, посібник. Одеса. 2020. 143 с.

17. Клименко В. Внутрішні загрози інформаційній безпеці організації. *Вісник НБУ*. 2020. № 5. С. 62–63.

18. Краус К. М., Краус Н. М., Штепа О. В. Цифрова трансформація кібербезпеки на мікрорівні в умовах воєнного стану. *Innovation and Sustainability*. 2022. No 3: c. 26-37.

19. Лісовська Ю. Кібербезпека: ризики та заходи: навч. посіб. Київ: Кондор, 2019. 272 с.

20. Маковець О., Дрозд І. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право*. 2020. № 5/3. С. 31–35.

21. Мельник Л. Г., Карінцева О. І. Економіка і бізнес. Суми: *Університетська книга*, 2021. 316 с.

22. Муравський В. Облік та кібербезпека: монографія. Тернопіль: *ЗУНУ*. 2023. 200 с.

23. Нехай В. А., Нехай В. В. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету*. 2017. Вип. 24(2). С. 137–140.

24. Офіційний сайт «Нова пошта». URL: https://novaposhta.ua/.

25. Половенко Л., Мерінова С. Виявлення ознак соціальної інженерії та технологія протидії соціальним хакерам на підприємстві. *Підприємництво та інновації*. 2019. № 10. С. 183–187.

26. Потапюк І., Годловський А. Теоретичні аспекти управління економічною безпекою підприємства. *Проблеми і перспективи розвитку підприємництва*. Харків : ХНАДУ, 2016. № 2 (13), т. 1. С. 25–30.

27. Положення про кваліфікаційну роботу здобувачів, що отримують освіту на бакалаврському та магістерському рівнях зі спеціальності 073 «Менеджмент». За заг. редакцією д.ю.н., проф. Ульянової Г.О. Укладачі: д.е.н., проф. Кібік О.М., к.е.н., доц. Котлубай В.О. Національний університет «Одеська юридична академія». Одеса, 2024. 30 с.

28. Ревак І. О., Грень Р. Т. Особливості формування безпечного кіберпростору в умовах розвитку цифрової економіки. *Інноваційна економіка*. 2021. № 3–4. С. 164–169.

29. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціо–культурній сфері*. 2018. Вип. 1. С. 75–86.

30. Товариство з обмеженою відповідальністю «НОВА ПОШТА». Фінансова звітність за 2022 рік URL: https://clarity–project.info/edr/31316718/finances?current_year=2022#google_vignette

31. Товариство з обмеженою відповідальністю «НОВА ПОШТА». Фінансова звітність за 2023 рік URL: https://clarity–project.info/edr/31316718/finances?current_year=2023

32. Товариство з обмеженою відповідальністю «НОВА ПОШТА». Фінансова звітність за 2024 рік URL: https://clarity–project.info/edr/31316718/yearly–finances?current_year=2024

33. Шостак Л., Більо І., Микитюк Є. Потенціал цифровізації вітчизняного бізнес–середовища. *Економічний аналіз*. 2021. Том 31. No 1. С. 245–251

34. Albahar M. Cyber attacks and terrorism: A twenty–first century conundrum. *Science and engineering ethics*. 2019. № 25(4). P. 993–1006.

35. Cybersecurity Awareness Report 2024. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/publications/cybersecurity-awareness-report-2024

36. Geer D., Jardine E., Leverett E. On market concentration and cybersecurity risk. *Journal of Cyber Policy*. URL: https://www.researchgate.net/publication/339459416_On_market_concentration_and_cybersecurity_risk

37. Kibik O., Slobodianiuk O., Belous K., Redina Y., Kornilova O., Prymachenko I. Strategy for developing competitive advantages of market entities in the era of digitalization , *Economic Affairs*. Vol. 69 (special issue) 2024. Pp. 139-147. URL: https://ndpublisher.in/admin/issues/EAv69n1p.pdf

38. Leevy J.L., Hancock J. Detecting cybersecurity attacks across different network feaures and learners. *Journal of Big Data*. 2021. P. 190–197.

39. IBM Security Report 2024.https://www.ibm.com/reports/data-breach

40. ISO /IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management systems requirements. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_iso_iec_27001_2023.pdf

41. NIST Cybersecurity Framework. URL:https://www.nist.gov/cyberframework

42. Rass S., Schauer S., König S., Zhu Q. Cyber–Security in Critical Infrastructures. *Springer International Publishing*, 2020. 297 p.