Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут фінансів, економіки, управління та права
Кафедра менеджменту і логістики

Кваліфікаційна робота

на здобуття ступеня вищої освіти «бакалавр»
зі спеціальності 073 «Менеджмент»
на тему: «Управління інформаційною безпекою організації у цифровому середовищі»

Виконав:
студент групи 401-ЕМ
Кучин Сергій Сергійович

Керівник:
завідувач кафедри менеджменту і логістики,
д.е.н., професор Гришко В.В.

Полтава – 2026

ЗМІСТ

ВСТУП

Актуальність теми дослідження зумовлена необхідністю підвищення ефективності управління інформаційною безпекою бізнес-процесів у цифровому середовищі в умовах постійного зростання кіберзагроз, збільшення кількості кібератак та розвитку цифрових фінансових сервісів. Сучасні підприємства, зокрема цифрові банки, функціонують у середовищі, де інформація є стратегічним ресурсом, а належний рівень її захисту виступає важливою умовою забезпечення стабільності та конкурентоспроможності організації. Особливо це стосується діяльності АТ «УНІВЕРСАЛ БАНК», яке здійснює активний розвиток цифрових банківських послуг через платформу monobank та використовує значну кількість цифрових каналів взаємодії з клієнтами.

Проблематика управління інформаційною безпекою бізнес-процесів досліджується багатьма вітчизняними та зарубіжними науковцями. У науковій літературі значна увага приділяється питанням кібербезпеки, управління інформаційними ризиками, захисту цифрової інфраструктури, впровадження міжнародних стандартів інформаційної безпеки та розвитку систем управління безпекою інформації. Водночас недостатньо дослідженими залишаються питання комплексного поєднання організаційних, економічних та технологічних механізмів забезпечення інформаційної безпеки бізнес-процесів у діяльності цифрових банків в умовах швидких змін цифрового середовища та постійної еволюції кіберзагроз. Саме це визначає необхідність подальших наукових досліджень у даному напрямі.

Метою кваліфікаційної роботи є розробка теоретичних положень та практичних рекомендацій щодо підвищення ефективності управління інформаційною безпекою бізнес-процесів у цифровому середовищі з метою забезпечення стабільності та надійності функціонування підприємства в умовах сучасних кіберзагроз.

Для досягнення поставленої мети у роботі визначено такі завдання дослідження:

1) дослідити сутність інформаційної безпеки бізнес-процесів та її роль у діяльності цифрових підприємств;
2) розглянути класифікацію, види та основні характеристики систем управління інформаційною безпекою;
3) проаналізувати вітчизняний і світовий досвід розвитку систем управління інформаційною безпекою;
4) надати організаційно-економічну характеристику діяльності АТ «УНІВЕРСАЛ БАНК»;
5) провести діагностику показників фінансово-господарської діяльності АТ «УНІВЕРСАЛ БАНК»;
6) оцінити сучасний стан системи управління інформаційною безпекою в АТ «УНІВЕРСАЛ БАНК»;
7) визначити концептуальні напрями подальшого розвитку системи інформаційної безпеки бізнес-процесів у цифровому середовищі;
8) розробити комплексні рекомендації щодо вдосконалення системи управління інформаційною безпекою бізнес-процесів підприємства;

Об’єктом дослідження є система управління інформаційною безпекою організації.

Предметом дослідження є організаційно-економічні механізми та інструменти забезпечення інформаційної безпеки в цифровому середовищі.

У процесі виконання кваліфікаційної роботи використано сукупність загальнонаукових та спеціальних методів дослідження. Теоретичну основу становлять методи аналізу та синтезу, узагальнення, порівняння, системного підходу та логічного аналізу. Для оцінювання зовнішнього та внутрішнього середовища функціонування підприємства використано методи SWOT-аналізу, PESTLE-аналізу та бенчмаркінгу. Під час дослідження фінансово-господарської діяльності підприємства застосовано економіко-статистичні методи, методи графічного та табличного аналізу. Для оцінювання системи управління

інформаційною безпекою використано методи експертного оцінювання, порівняльного аналізу та узагальнення практичного досвіду цифрових підприємств.

Практична значущість одержаних результатів полягає у можливості використання запропонованих рекомендацій та підходів для вдосконалення системи управління інформаційною безпекою бізнес-процесів у діяльності цифрових підприємств, зокрема банківських установ. Запропоновані у роботі заходи можуть бути використані для підвищення рівня захисту інформаційних ресурсів, мінімізації кіберризиків, удосконалення механізмів управління інформаційною безпекою та забезпечення стабільності функціонування підприємства у цифровому середовищі.

Наукова новизна одержаних результатів полягає в удосконаленні підходів до управління інформаційною безпекою бізнес-процесів у цифровому середовищі шляхом комплексного поєднання організаційних, економічних та цифрових інструментів забезпечення кіберзахисту. У роботі розвинуто підходи до оцінювання ефективності системи управління інформаційною безпекою цифрових банків з урахуванням сучасних кіберзагроз та особливостей функціонування цифрових фінансових сервісів.

Гришко В.В., Кучин С. С. Удосконалення системи управління інформаційною безпекою бізнес-процесів. IV Міжнародна науково-практична Інтернет-конференція «Сталий розвиток: виклики та загрози в умовах сучасних реалій». Полтава, 2026.

Робота складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Загальний обсяг роботи становить 86 сторінок. Ілюстративний матеріал представлений 17 рисунками та 10 таблицями.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ У ЦИФРОВОМУ СЕРЕДОВИЩІ

1.1. Сутність інформаційної безпеки бізнес-процесів та її роль у діяльності цифрових підприємств

У сучасних умовах розвитку цифрової економіки інформаційні технології стали невід’ємною складовою функціонування більшості підприємств. Активне впровадження цифрових платформ, автоматизованих систем управління, хмарних сервісів та електронних каналів комунікації суттєво змінило підходи до організації бізнес-процесів. Особливо стрімко цифровізація відбувається у фінансовому секторі, де розвиток онлайн-банкінгу, мобільних застосунків та дистанційного обслуговування клієнтів формує нові вимоги до забезпечення стабільності та безпеки функціонування підприємств.

Використання цифрових технологій дозволяє підприємствам підвищувати ефективність управління, оптимізувати бізнес-процеси та покращувати взаємодію з клієнтами. Водночас цифрове середовище створює нові ризики, пов’язані з кіберзагрозами, витоком інформації, несанкціонованим доступом до даних та порушенням роботи інформаційних систем. Особливої актуальності проблема інформаційної безпеки набуває для цифрових підприємств та банківських установ, діяльність яких безпосередньо залежить від безперервності функціонування інформаційної інфраструктури та рівня захисту конфіденційної інформації.

Протягом останніх років у світі спостерігається стрімке зростання кількості кібератак на підприємства, державні установи та фінансові організації. За даними міжнародних аналітичних компаній, значна частина інцидентів пов’язана із фішинговими атаками, програмами-вимагачами, витоками персональних даних та атаками на хмарні сервіси. Крім фінансових збитків, кібератаки призводять до втрати ділової репутації підприємств, зниження рівня

довіри клієнтів та порушення стабільності бізнес-процесів. У сучасних умовах ефективна система управління інформаційною безпекою стає одним із ключових факторів забезпечення конкурентоспроможності цифрових підприємств.

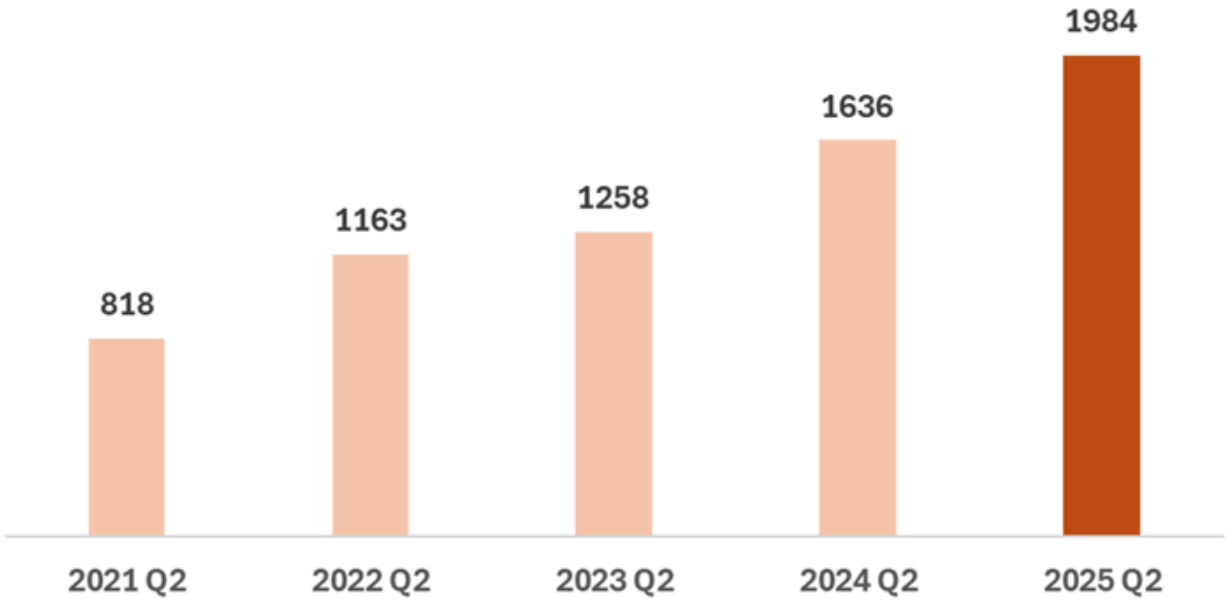

Рисунок 1.1 – Середня кількість щотижневих кібератак на організації у розрізі II кварталів 2021–2025 рр.

Примітка. Розроблено за джерелом [1].

Особливого значення питання інформаційної безпеки набуло в умовах активного розвитку онлайн-банкінгу та цифрових фінансових сервісів. Використання мобільних додатків, хмарних технологій, API-інтеграцій та дистанційної ідентифікації клієнтів значно розширює можливості фінансових установ, однак одночасно збільшує кількість потенційних вразливостей. Це зумовлює необхідність формування комплексної системи управління інформаційною безпекою, яка повинна поєднувати організаційні, технічні та управлінські механізми захисту інформації.

Підтвердженням актуальності зазначених вище загроз є статистичні дані (див. рис. 1.2), які свідчать, що фінансовий сектор залишається однією з ключових мішеней для кіберзлочинців. Зокрема, у другому кварталі 2025 року в

галузі фінансових послуг зафіксовано в середньому 1791 атаку на одну організацію щотижня. Попри те, що інтенсивність нападів на банки та фінтех-компанії є нижчою, ніж у сфері освіти чи державного управління, цей сектор продемонстрував стійку тенденцію до зростання кіберзагроз на рівні +18% порівняно з аналогічним періодом минулого року. Така динаміка вказує на те, що навіть попри високий рівень початкової захищеності, фінансові інституції змушені постійно адаптувати свої стратегії безпеки до дедалі складніших методів цифрового шахрайства та хакерських втручань.

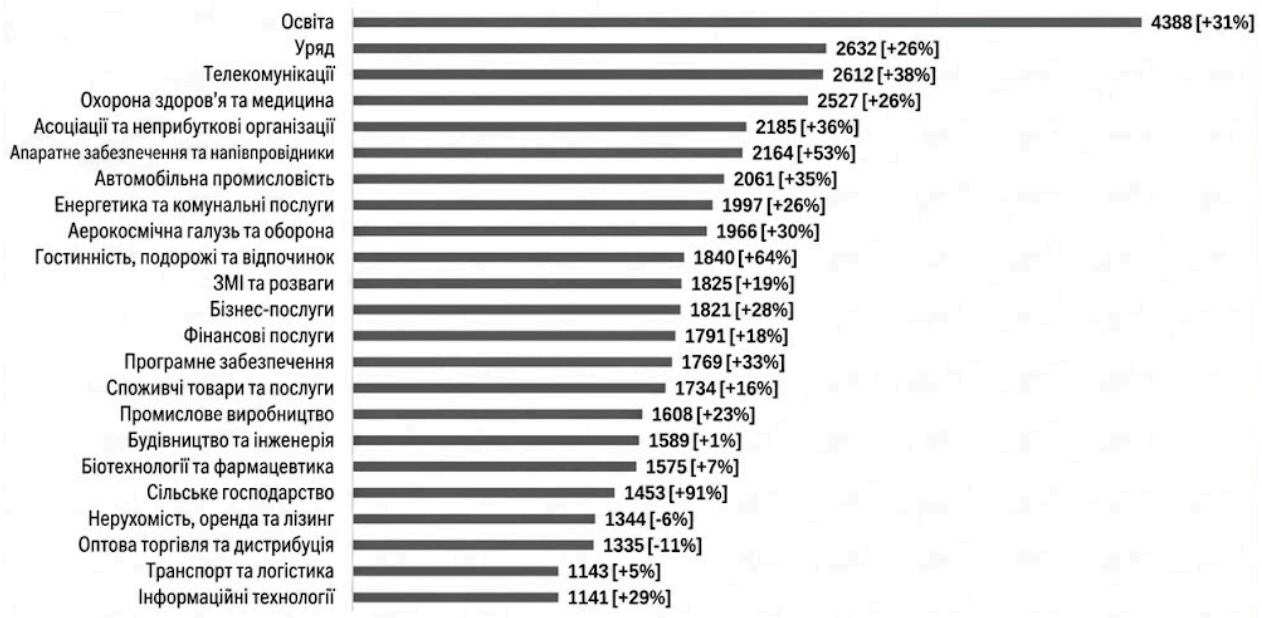

Рисунок 1.2 – Глобальна статистика щотижневих кібератак у розрізі сфер діяльності (порівняння Q2 2024 та Q2 2025 рр.)

Примітка. Розроблено за джерелом [1].

Наступним важливим етапом дослідження сутності інформаційної безпеки є аналіз наукових підходів до трактування цього поняття. У сучасній науковій літературі відсутній єдиний підхід до визначення інформаційної безпеки, оскільки різні автори акцентують увагу на окремих аспектах цього явища: технічному захисті інформації, управлінні ризиками, забезпеченні стабільності функціонування інформаційних систем або організаційних механізмах управління безпекою. Це пояснюється складністю та

багатогранністю інформаційної безпеки в умовах цифровізації економіки та розвитку сучасних інформаційних технологій.

У наукових працях інформаційна безпека часто розглядається як стан захищеності інформації та інформаційних ресурсів від внутрішніх і зовнішніх загроз. Водночас сучасні дослідники все частіше трактують її як комплексну систему управління ризиками, що включає технічні, організаційні, правові та управлінські механізми захисту інформації. Особливої актуальності це набуває для цифрових підприємств, діяльність яких безпосередньо залежить від безперервного функціонування цифрової інфраструктури та захисту даних клієнтів [2, с. 17].

Таблиця 1.1. Визначення кібербезпеки та їх критичний аналіз

№	Робочі визначення	Критичні зауваження
1	«Кібербезпека — це захист інформації/даних, активів, послуг і систем, що мають цінність, для зниження ймовірності втрати, пошкодження/псування, компрометації або нецільового використання до рівня, що відповідає призначеній вартості».	Відгуки свідчать, що включення поняття «цінності» вводить людський фактор у безпеку, проте визначення є занадто нормативним і страждає від обмеженого переліку об'єктів захисту.
2	«Кібербезпека — це сукупність взаємодіючих процесів, призначених для захисту кіберпростору та систем, що функціонують у ньому (спільно — ресурсів), від навмисних дій, спрямованих на порушення прав власності власника ресурсу».	Це визначення вводить поняття кіберфізичного середовища та важливу концепцію контролю над правами власності. Однак акцент лише на «навмисних діях людини» вважається занадто обмежувальним.
3	«Кібербезпека — це сукупність взаємодіючих процесів, призначених для того, щоб зробити кіберпростір безпечним і захищеним».	Спроба зробити визначення ширшим за попередні створила більше проблем, ніж розв'язала, оскільки воно є надмірно загальним і вводить суперечливе поєднання понять «safety» та «security».
4	«Кібербезпека — це галузь, присвячена вивченню та практиці захисту систем або цифрових активів від будь-яких дій, що спрямовані на авторизацію в цих системах, які не відповідають правам власності на ресурсний об'єкт».	Введено концепції прав власності та контролю. Проте виникли зауваження щодо термінів «вивчення» та «практика», які замикають питання переважно в академічній площині, а не в операційній.
5	«Кібербезпека — це стан, за якого влада над роботою комп'ютерів (у широкому сенсі) та над інформацією, що знаходиться під контролем комп'ютерів, здійснюється належним чином».	Це визначення підкріплює поняття контролю над інформацією та системами. Основна критика стосується визначення кібербезпеки саме як «стану».

Примітка. Розроблено за джерелами [2, с. 16].

Аналіз наведених у таблиці підходів свідчить про відсутність єдиного консенсусу серед дослідників: частину визначень критикують за надмірну нормативність, інші — за вузьке фокусування лише на навмисних діях людини або суто академічний характер. Водночас еволюція цих поглядів демонструє

поступовий перехід від розуміння кібербезпеки як статичного стану захищеності до її сприйняття як динамічної сукупності процесів управління правами власності та контролю в цифровому середовищі. Таке різноманіття наукових трактувань зумовлює необхідність звернення до міжнародних стандартів та установчих документів провідних інституцій, які пропонують більш уніфіковані та прикладні формулювання.

Згідно з нормативами CNSSI 4009-2015 та низкою стандартів NIST зокрема SP 800-37 та SP 800-53, кібербезпека розглядається як запобігання пошкодженню, захист і відновлення комп’ютерів, систем та служб електронного зв’язку, включаючи інформацію, що в них міститься, для гарантування її доступності, цілісності, автентичності, конфіденційності та незаперечності [3].

У Рамковій програмі кібербезпеки NIST Cybersecurity Framework Version 1.1 акцент зміщується на динаміку процесів, де кібербезпека визначається як безперервний цикл захисту інформації шляхом превентивних заходів, своєчасного виявлення загроз та оперативного реагування на проведені атаки [3].

Відповідно до положень CNSSI 4009-2015, термін «комп’ютерна безпека», що традиційно охоплював заходи контролю для забезпечення конфіденційності та цілісності даних безпосередньо в обчислювальних системах, на сьогодні вважається застарілим і офіційно замінюється ширшим поняттям «кібербезпека» [3].

Стандарт NIST SP 800-50r1 трактує кібербезпеку як комплекс дій із захисту та відновлення електронних комунікаційних систем і дротового зв'язку, що дозволяє підтримувати працездатність інфраструктури та цілісність даних навіть після виникнення інцидентів [3].

У документі NISTIR 8170 кібербезпека інтерпретується через призму оборонних спроможностей, визначаючи її як безпосередню здатність організації або системи захищати та відстоювати стабільне функціонування кіберпростору в умовах цілеспрямованих кібератак [3].

Згідно з NISTIR 8074 Vol. 2. Сутність кібербезпеки полягає у запобіганні

несанкціонованому використанню та експлуатації електронних інформаційних систем, а також, за потреби, у їхньому повному відновленні задля зміцнення базових характеристик безпеки: конфіденційності, цілісності та доступності [3].

У контексті звіту NIST IR 8323r1 зазначається, що до сфери кібербезпеки належить не лише захист загальних інформаційних мереж, а й специфічних пристроїв, що генерують критичні дані, наприклад, дані позиціонування та навігації PNT, оскільки безпека таких пристроїв є невід'ємною частиною захисту цифрової екосистеми в цілому [3].

Проведений аналіз наукових підходів та міжнародних стандартів дозволяє зробити висновок, що розуміння кібербезпеки еволюціонувало від вузькотехнічного захисту комп'ютерних систем до всеохопної стратегії управління цифровими ризиками. Сучасні трактування NIST та CNSSI підкреслюють, що кібербезпека є безперервним динамічним процесом, який охоплює не лише запобігання атакам, а й здатність до швидкого відновлення інфраструктури, захист прав власності на цифрові активи та гарантування цілісності специфічних даних у глобальній цифровій екосистемі.

Наступним варто дослідити бізнес-процеси, їх доцільно розглядати як сукупність взаємопов'язаних дій та операцій, спрямованих на досягнення стратегічних і поточних цілей підприємства. У цифровому середовищі такі процеси базуються на використанні інформаційних систем, автоматизованих платформ, електронного документообігу та мережевих технологій.

Цифровізація суттєво змінила підходи до організації бізнес-процесів, забезпечивши підприємствам можливість швидкого обміну інформацією, автоматизації управління та дистанційної взаємодії з клієнтами. Особливо це стосується фінансового сектору, де активно використовуються онлайн-банкінг, мобільні застосунки, API-інтеграції та хмарні сервіси. Використання цифрових платформ дозволяє підприємствам підвищити швидкість обробки даних, оптимізувати витрати та покращити якість обслуговування клієнтів. Водночас розширення цифрової інфраструктури створює нові виклики у сфері інформаційної безпеки, оскільки збільшується кількість потенційних точок

доступу до інформаційних ресурсів підприємства [4].

Доцільно зазначити, що розвиток онлайн-банкінгу та мобільних застосунків сприяв значному підвищенню рівня цифровізації фінансових послуг. Сучасні банки забезпечують можливість дистанційного відкриття рахунків, проведення платежів, управління фінансовими операціями та отримання консультацій у режимі реального часу. Однак використання мобільних платформ та віддалених каналів обслуговування підвищує ризики несанкціонованого доступу до персональних даних клієнтів, фінансового шахрайства та кібератак.

Важливу роль у цифровому середовищі також відіграють API-технології, які забезпечують інтеграцію між різними інформаційними системами та цифровими сервісами. Використання API дозволяє підприємствам автоматизувати бізнес-процеси та розширювати функціональні можливості цифрових платформ. Разом із тим, недостатній рівень захисту API-інтерфейсів може призводити до витоку інформації, компрометації облікових даних та порушення стабільності функціонування системи.

Окремої уваги потребують використання хмарних сервісів та організація віддаленої роботи персоналу. Хмарні технології забезпечують гнучкість управління даними та доступ до інформаційних ресурсів незалежно від місця перебування користувача. Водночас передача даних через мережу Інтернет та використання віддалених каналів доступу створюють додаткові ризики для інформаційної безпеки підприємства. Значна частина кіберінцидентів пов’язана саме з недостатнім рівнем захисту облікових записів працівників, використанням незахищених мереж або людським фактором.

У сучасному цифровому середовищі ландшафт загроз інформаційній безпеці підприємств трансформується під впливом технологічного прогресу, що підтверджується актуальними даними фахівців на 2025 рік (див. рис. 1.3). Найбільш критичними викликами експерти вважають використання штучного інтелекту зловмисниками, зокрема для створення складного шкідливого програмного забезпечення 43,4% та вдосконалення методів зламу паролів

39,2%. Значну небезпеку становлять моделі «вимагач як послуга» Ransomware as a service, 38,4%, атаки на ланцюги постачання, 33,6%, а також ризики, пов'язані з використанням тіньових IT-ресурсів Shadow IT, 32,6% та вразливостями пристроїв Інтернету речей IoT, 30,2%.

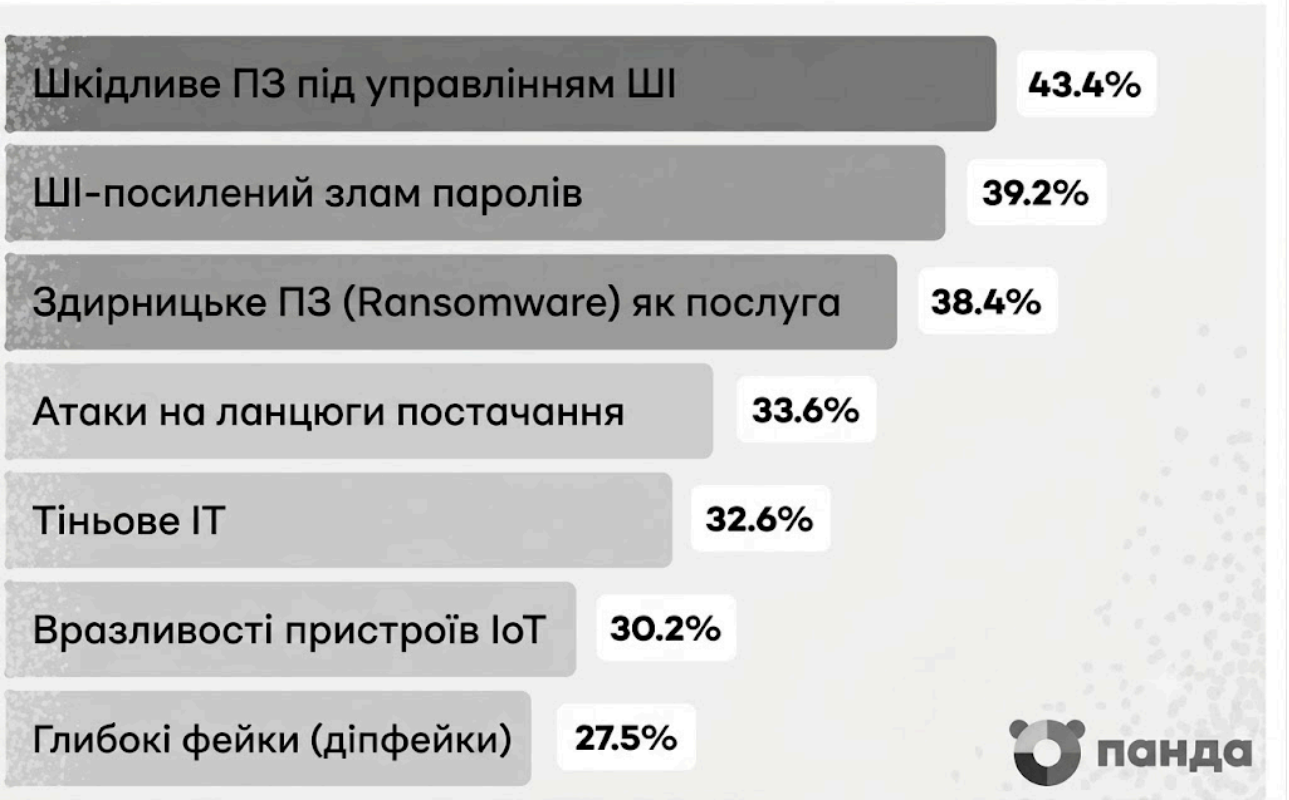

Рисунок 1.3 — Основні загрози інформаційній безпеці цифрових підприємств.

Примітка. Розроблено за джерелом [5].

Окрім візуалізованих даних, фахівці виділяють зростання загрози від використання дипфейків 27,5%, безфайлових атак 24,8% та потенційні ризики квантових обчислень для криптографічного захисту 20,9%. Менш пріоритетними, проте наявними, залишаються питання безпеки сторонніх постачальників та впровадження мереж 5G. Такі загрози можуть призводити до катастрофічних фінансових втрат, порушення безперервності бізнес-процесів, втрати репутації та зниження довіри клієнтів. Водночас важливо зауважити, що цифрові підприємства починають активно застосовувати штучний інтелект не

лише як вектор атаки, а й як інструмент для побудови високоефективних систем випереджального захисту.

Класифікація ключових загроз кібербезпеці у 2025 році, оформлена у вигляді таблиці, наведена для зручності у таблиці 1.2.

Таблиця 1.2. Характеристика актуальних загроз інформаційній безпеці у 2025 році

Категорія загрози	Визначення та сутність
Шкідливе ПЗ на основі ШІ	Віруси та програми, що використовують алгоритми штучного інтелекту для адаптації до систем захисту, самостійного пошуку вразливостей та обходу антивірусних фільтрів.
Злам паролів за допомогою ШІ	Застосування нейромереж для прогнозування комбінацій паролів на основі великих масивів даних значно пришвидшує процес несанкціонованого доступу.
Вимагач як послуга	Бізнес-модель, за якої розробники програм-вимагачів надають свій софт іншим зловмисникам («партнерам») за частку від отриманого викупу.
Атаки на ланцюги постачання	Проникнення в IT-інфраструктуру підприємства через виявлені вразливості у програмному забезпеченні або сервісах сторонніх постачальників і партнерів.
Тіньові IT	Використання персоналом програмних продуктів, хмарних сервісів або пристроїв без офіційного погодження з IT-відділом, що створює неконтрольовані зони ризику.
Вразливості пристроїв IoT	Слабкі місця в системі захисту «розумних» гаджетів та датчиків, які через відсутність складних механізмів безпеки стають точками входу в корпоративну мережу.
Дипфейки	Технологія створення реалістичних підробок аудіо- та відеоматеріалів за допомогою ШІ для проведення атак соціальної інженерії (наприклад, фейкові розпорядження керівництва).
Безфайлові атаки	Шкідливі дії, що реалізуються безпосередньо в оперативній пам'яті за допомогою легітимних системних інструментів, що робить їх складними для виявлення традиційними антивірусами.
Квантові обчислення	Потенційна загроза з боку квантових комп’ютерів, здатних швидко зламувати сучасні асиметричні алгоритми шифрування та криптографічні протоколи.
Ризики сторонніх вендорів	Загрози, що виникають через недостатній рівень інформаційного захисту у підрядників, які мають прямий або віддалений доступ до конфіденційних ресурсів компанії.
Загрози мереж 5G	Специфічні вразливості архітектури мереж п'ятого покоління, що через високу щільність підключень та швидкість передачі даних суттєво розширюють площу атаки.

Примітка. Авторська розробка.

На цьому етапі варто підсумувати результати першого підрозділу. Зазначаю, що в умовах глобальної цифровізації поняття інформаційної безпеки трансформувалося з суто технічного завдання IT-спеціалістів у стратегічний пріоритет для керівництва будь-якого сучасного підприємства. Якщо раніше ми говорили переважно про захист серверів від збоїв, то сьогодні мова йде про

складне управління цифровими ризиками, де на перший план виходить не тільки запобігання атакам, а й здатність бізнесу швидко відновити роботу після серйозних інцидентів.

Фундаментом безпеки залишається класичне поєднання конфіденційності, цілісності та доступності даних. Проте реалії 2025 року змушують нас дивитися ширше: хакери почали використовувати штучний інтелект для створення вірусів та дипфейків, що робить традиційні методи захисту недостатніми. Для цифрових підприємств це означає, що будь-який бізнес-процес — від внутрішнього документообігу до обслуговування клієнтів у додатках — має бути захищеним на кожному етапі.

Отже, ефективна система управління інформаційною безпекою сьогодні є головною умовою виживання на ринку. Вона дозволяє не лише вберегти гроші компанії, а й зберегти найцінніший актив у цифрову епоху — довіру клієнтів та партнерів.

1.2. Класифікація, види та основні характеристики системи управління інформаційною безпекою

Ефективне функціонування цифрових підприємств значною мірою залежить від рівня організації системи управління інформаційною безпекою. У сучасних умовах такі системи повинні забезпечувати комплексний захист інформаційних ресурсів, цифрової інфраструктури та бізнес-процесів від внутрішніх і зовнішніх загроз. Залежно від підходів до забезпечення захисту інформації системи управління інформаційною безпекою можуть класифікуватися за наступними видами.

Управління інформаційною безпекою зосереджене на стратегічному захисті корпоративних даних шляхом ідентифікації ризиків та розробки методів їх усунення. В основі цього виду управління лежить класична тріада CIA: забезпечення конфіденційності для запобігання витокам, підтримка цілісності для захисту даних від несанкціонованого спотворення та гарантування

доступності ресурсів для авторизованих користувачів. Окрім технічних аспектів, цей напрям значною мірою базується на дотриманні галузевих регуляцій та стандартів, що дозволяє бізнесу мінімізувати ймовірність успішних кібератак та зменшити їхній потенційний вплив на операційну діяльність [6].

Рисунок 1.4 – Види управління кібербезпекою

Примітка. Авторська розробка.

Управління мережевою безпекою виступає першою лінією оборони, консолідуючи різноманітні рішення для захисту корпоративних мереж, які є основними точками входу для зловмисників. Ця система об'єднує роботу міжмережевих екранів, механізмів сегментації мережі, систем резервного копіювання та захисту електронної пошти під єдиним контролем. Централізація управління мережевими засобами дозволяє суттєво підвищити видимість загроз, зменшити кількість помилок у конфігураціях та пришвидшити реагування на інциденти, забезпечуючи стабільність мережевої інфраструктури підприємства.

Управління безпекою кінцевих точок стає критично важливим у сучасних умовах, коли доступ до цифрових активів здійснюється з різноманітних пристроїв, таких як ноутбуки та смартфони, що часто знаходяться поза межами прямого контролю IT-відділів. Основне завдання цього напряму полягає в тому, щоб надавати доступ до корпоративних ресурсів лише тим пристроям, які повністю відповідають внутрішнім політикам безпеки та не мають ознак інфікування шкідливим програмним забезпеченням. Це дозволяє компаніям

ефективно впроваджувати моделі дистанційної роботи, мінімізуючи ризики, пов'язані з використанням неперевіреного обладнання.

Управління безпекою у хмарі визначає методи обмеження загроз і вразливостей під час використання хмарних мереж та додатків. Цей процес охоплює постійний аналіз хмарних сервісів, шифрування даних для збереження їхньої приватності, а також ретельний моніторинг поведінки користувачів для виявлення аномальної активності. Оскільки хмарні середовища зазвичай є дуже складними та динамічними, використання спеціалізованих платформ для централізації цих процесів дозволяє отримати повну видимість робочих навантажень і забезпечити високу ефективність захисту даних у віртуалізованому просторі.

Основою сучасної системи управління інформаційною безпекою є забезпечення трьох ключових характеристик інформації: конфіденційності, цілісності та доступності, які формують зазначену раніше класичну модель CIA (Confidentiality, Integrity, Availability). Саме ці складові визначають ефективність функціонування системи захисту інформації на підприємстві [7].

Рисунок 1.5 – Тріада CIA: Конфіденційність, Цілісність та Доступність

Примітка. Авторська розробка.

Конфіденційність передбачає обмеження доступу до інформації лише для авторизованих користувачів. Основною метою забезпечення конфіденційності є

захист інформації від несанкціонованого розголошення або витоку даних. Для цього використовуються механізми автентифікації користувачів, шифрування інформації, контроль доступу та системи ідентифікації.

Цілісність інформації означає збереження її точності, повноти та незмінності під час обробки, зберігання або передачі. Порушення цілісності даних може призвести до спотворення інформації, фінансових втрат та порушення роботи бізнес-процесів. Забезпечення цілісності досягається шляхом використання резервного копіювання, систем журналювання змін, електронного підпису та контролю змін у базах даних.

Доступність передбачає забезпечення безперервного та своєчасного доступу користувачів до інформаційних ресурсів і цифрових сервісів. Особливого значення ця складова набуває для банківських установ та цифрових платформ, де навіть короткочасне припинення роботи системи може призвести до значних фінансових і репутаційних втрат. Для підтримання доступності використовуються системи резервування, хмарні технології, балансування навантаження та механізми захисту від DDoS-атак.

Доцільно зазначити, що ефективність системи управління інформаційною безпекою залежить не лише від використання сучасних технологічних рішень, а й від комплексної взаємодії персоналу, внутрішніх політик безпеки, процедур ризик-менеджменту та постійного моніторингу цифрового середовища.

Наступним важливим елементом сучасної системи управління інформаційною безпекою є використання міжнародних стандартів та підходів, які визначають основні принципи організації захисту інформації у цифровому середовищі. У сучасних умовах глобалізації та цифровізації діяльності підприємств міжнародні стандарти виступають основою формування ефективної політики кібербезпеки, управління ризиками та забезпечення безперервності бізнес-процесів. Їх застосування дозволяє підприємствам адаптувати систему інформаційної безпеки до сучасних вимог цифрового середовища та міжнародних практик управління.

Одним із найбільш поширених міжнародних стандартів є ISO/IEC 27001,

який визначає вимоги до створення, функціонування та вдосконалення системи управління інформаційною безпекою. Основною особливістю даного стандарту є комплексний підхід до управління ризиками інформаційної безпеки та впровадження постійного контролю захисту інформаційних ресурсів підприємства. Доцільно зазначити, що стандарт ISO/IEC 27001 широко використовується банківськими установами, IT-компаніями та міжнародними корпораціями, оскільки дозволяє забезпечити системність управління інформаційною безпекою [8].

Важливе значення у сфері кібербезпеки має також NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США. Даний підхід орієнтований на управління кіберризиками та базується на п’яти ключових функціях: ідентифікація загроз, захист, виявлення інцидентів, реагування та відновлення. Перевагою NIST є його гнучкість та можливість адаптації до діяльності підприємств різного масштабу [9].

У сучасних умовах активного розвитку цифрових платформ значного поширення набуває концепція Zero Trust, відповідно до якої жоден користувач або пристрій не вважається автоматично безпечним навіть усередині корпоративної мережі. Основним принципом даної моделі є постійна перевірка автентичності користувачів, контроль доступу та мінімізація довіри до внутрішніх цифрових ресурсів. На нашу думку, впровадження концепції Zero Trust є особливо актуальним для банківського сектору та підприємств, які використовують хмарні сервіси й віддалений доступ до інформаційних систем [10].

Важливу роль у забезпеченні інформаційної безпеки відіграють SOC-центри (Security Operations Center), які забезпечують цілодобовий моніторинг інформаційної інфраструктури, виявлення кіберзагроз та оперативне реагування на інциденти безпеки. Використання SOC-центрів дозволяє підприємствам своєчасно виявляти підозрілу активність, аналізувати кіберризики та мінімізувати наслідки можливих атак [11].

Окремої уваги заслуговує GDPR (General Data Protection Regulation) —

регламент Європейського Союзу щодо захисту персональних даних. Даний нормативний документ встановлює вимоги до збору, обробки та зберігання персональної інформації користувачів. Основною метою GDPR є посилення контролю за використанням персональних даних та забезпечення прозорості діяльності компаній у сфері обробки інформації. Недоліком окремих підприємств є недостатнє врахування вимог GDPR, що може призводити до фінансових санкцій та репутаційних втрат [12].

Таблиця 1.2. Порівняльна характеристика міжнародних стандартів інформаційної безпеки

Назва підходу / стандарту	Основна характеристика та мета	Ключові функції / Принципи	Сфера застосування / Переваги
ISO/IEC 27001	Міжнародний стандарт вимог до створення та вдосконалення системи управління інформаційною безпекою	Комплексний підхід до управління ризиками та постійний контроль ресурсів.	Банківські установи, ІТ-компанії, міжнародні корпорації забезпечують системність.
NIST Cybersecurity Framework	Орієнтований на управління кіберризиками, розроблений у США.	5 функцій: ідентифікація, захист, виявлення, реагування та відновлення.	Підприємства різного масштабу завдяки високій гнучкості та адаптивності.
Zero Trust	Концепція, за якою жоден користувач чи пристрій не є безпечним за замовчуванням.	Постійна перевірка автентичності, контроль доступу та мінімізація довіри.	Банківський сектор, хмарні сервіси та компанії з віддаленим доступом.
SOC-центри	Центри цілодобового моніторингу та оперативного реагування.	Моніторинг інфраструктури, аналіз ризиків та мінімізація наслідків атак.	Будь-які підприємства, що потребують своєчасного виявлення підозрілої активності.
GDPR	Регламент ЄС щодо захисту персональних даних.	Суворі вимоги до збору, обробки та зберігання особистої інформації.	Забезпечення прозорості; ігнорування загрожує великими штрафами та втратою репутації.

Примітка. Авторська розробка.

У сучасному цифровому середовищі 2026 року ефективність системи управління інформаційною безпекою базується на впровадженні комплексної стратегії, що починається з розробки та встановлення надійної політики кібербезпеки. Важливим аспектом є захист не лише традиційних мереж, а й периметра та підключень Інтернету речей, що вимагає постійного

вдосконалення методів управління даними та їхнього захисту. Використання людиноцентричного підходу стає критично важливим, оскільки безпека системи залежить від обізнаності персоналу та розумного управління паролями на всіх рівнях організації.

Особлива увага приділяється контролю доступу до конфіденційних даних та обов'язковому впровадженню багатофакторної автентифікації, що мінімізує ризики несанкціонованого проникнення. Сучасні методи захисту передбачають моніторинг активності не лише штатних працівників, а й привілейованих та сторонніх користувачів у режимі реального часу. Це доповнюється системами виявлення загроз, ідентифікації та швидкого реагування на них, що дозволяють нейтралізувати атаки на етапі їх виникнення.

Рисунок 1.6 – Ключові методи забезпечення кібербезпеки у 2026 році

Примітка. Розроблено за джерелом [13].

Важливою складовою стійкості бізнесу є управління ризиками в ланцюгах постачання та регулярне проведення аудитів кібербезпеки для перевірки відповідності систем встановленим стандартам. Оптимізація та спрощення технологічної інфраструктури дозволяють зменшити кількість потенційних вразливостей, забезпечуючи стабільність бізнес-процесів. Тільки поєднання цих методів у єдину систему дозволяє підприємствам створити

захищене цифрове середовище, готове до викликів майбутнього.

Отже, узагальнення теоретичних засад дозволило встановити, що система управління інформаційною безпекою є комплексним механізмом, який інтегрує технічні, програмні та організаційні методи для захисту тріади «конфіденційність – цілісність – доступність». Визначено, що ефективність СУІБ базується на дотриманні міжнародних стандартів та впровадженні сучасних концепцій, зокрема Zero Trust та AI-моніторингу. Встановлено, що інтеграція міжнародних стандартів та сучасних методів кіберзахисту дозволяє створити гнучку архітектуру безпеки, яка мінімізує вразливості бізнес-процесів і гарантує стабільне функціонування підприємства в умовах динамічних цифрових загроз.

1.3. Вітчизняний та світовий досвід розвитку системи управління інформаційною безпекою

У сучасних умовах цифровізації економіки та зростання кількості кіберзагроз питання управління інформаційною безпекою набуває стратегічного значення для підприємств у всьому світі. Провідні міжнародні компанії активно впроваджують комплексні системи кіберзахисту, які поєднують сучасні технології, інструменти штучного інтелекту, автоматизований моніторинг та багаторівневий контроль доступу до інформаційних ресурсів. Світовий досвід свідчить про те, що ефективна система управління інформаційною безпекою є не лише засобом захисту інформації, а й важливою складовою забезпечення стабільності бізнес-процесів та конкурентоспроможності підприємства.

Одним із провідних світових прикладів ефективного управління інформаційною безпекою є Cisco, яка активно впроваджує концепцію Zero Trust, системи мережевого моніторингу та автоматизовані рішення з кіберзахисту. Компанія використовує сучасні SOC-центри для цілодобового аналізу кіберзагроз та оперативного реагування на інциденти безпеки. Важливою складовою системи захисту є багатофакторна автентифікація, контроль доступу

до корпоративних ресурсів та використання AI-аналітики для виявлення аномальної активності у мережі. Особливу увагу Cisco приділяє захисту хмарної інфраструктури та безпеці передачі даних у корпоративних мережах [14].

Значний досвід у сфері інформаційної безпеки має IBM, яка розробляє комплексні рішення для управління кіберризиками та цифрового захисту підприємств. Компанія активно використовує штучний інтелект у системах моніторингу кіберзагроз, а також впроваджує автоматизовані платформи аналізу безпеки на базі IBM QRadar. Особливістю підходу IBM є інтеграція AI-моніторингу, хмарного захисту та технологій прогнозування кіберінцидентів. Крім того, компанія активно розвиває рішення для захисту фінансових установ та критичної цифрової інфраструктури [15].

Важливе місце серед міжнародних компаній у сфері кібербезпеки займає Oracle, яка забезпечує захист корпоративних баз даних, хмарних сервісів та цифрових платформ за допомогою комплексних систем контролю доступу та шифрування інформації. Компанія використовує багаторівневі системи автентифікації користувачів, механізми резервного копіювання даних та автоматизовані інструменти управління ризиками. Важливою особливістю підходу Oracle є забезпечення безпеки хмарних середовищ та захист великих масивів корпоративної інформації від несанкціонованого доступу й витоку даних [16].

Суттєвий досвід у сфері кібербезпеки має JPMorgan Chase, яка після масштабної кібератаки 2014 року значно посилила систему управління інформаційною безпекою. Банк інвестував значні ресурси у створення сучасних SOC-центрів, розвиток AI-систем моніторингу та вдосконалення систем управління ризиками. Особливу увагу компанія приділяє захисту фінансових транзакцій та персональних даних клієнтів [17].

Світовий досвід свідчить про те, що сучасні підприємства дедалі більше переходять до комплексних моделей управління інформаційною безпекою, які поєднують технологічні, організаційні та аналітичні інструменти. На мою

думку, ключовими тенденціями розвитку систем кібербезпеки є використання штучного інтелекту, автоматизація моніторингу кіберзагроз, розвиток хмарних технологій та впровадження концепції Zero Trust.

Одним із найбільш відомих прикладів цифровізації банківського сектору є monobank, який функціонує на базі АТ «УНІВЕРСАЛ БАНК». Система інформаційної безпеки банку базується на використанні PCI-DSS-сумісних рішень, посиленого 3D Secure та захищених каналів взаємодії через мобільний застосунок. Для безпечної автентифікації користувачів використовуються технології Fingerprint, Touch ID та Face ID, а захист передачі даних забезпечується протоколом TLS 1.2.

Крім того, банк застосовує системи anti-fraud та anti-hacker-моніторингу для автоматичного виявлення підозрілих транзакцій, контролю аномальної активності та блокування потенційних кібератак. Особливістю monobank є високий рівень автоматизації бізнес-процесів та комплексний підхід до забезпечення інформаційної безпеки у цифровому середовищі [18].

Важливу роль у розвитку систем інформаційної безпеки в Україні відіграє ПриватБанк, який активно впроваджує сучасні системи кіберзахисту, AI-моніторинг транзакцій та принцип Zero Trust. З початку повномасштабної війни банк нейтралізував понад 1,5 мільйона кібератак, що свідчить про високий рівень захисту цифрової інфраструктури. Крім того, банк регулярно проводить тестування систем безпеки за участю міжнародних експертів та використовує комплексні механізми захисту клієнтських даних і онлайн-банкінгу [19].

Суттєве значення для розвитку цифрової безпеки має Дія, яка забезпечує доступ громадян до електронних державних послуг. Особливістю системи є те, що застосунок не зберігає персональні дані користувачів, а лише відображає інформацію з державних реєстрів за запитом користувача. Для захисту інформації використовуються механізми шифрування даних, цифрової ідентифікації через BankID, підхід «глибокого захисту» та хмарна інфраструктура із сертифікатами безпеки. Крім того, система проходила

державні та незалежні аудити безпеки, а також тестування за участю фахівців EPAM і білих хакерів для виявлення потенційних вразливостей [20].

Важливу координаційну роль у сфері кібербезпеки виконує Національний банк України, який здійснює оновлення нормативно-правових вимог щодо інформаційної безпеки, кіберзахисту та цифрової операційної стійкості фінансового сектору відповідно до європейських стандартів DORA. НБУ також контролює порядок використання хмарних сервісів банками та формує вимоги до взаємодії фінансових установ із міжнародними cloud- та SaaS-провайдерами, зокрема AWS, Google Cloud і Microsoft Azure. Крім того, важливу роль у реагуванні на кіберінциденти виконує CERT-UA — урядова команда реагування на комп'ютерні надзвичайні події України [21].

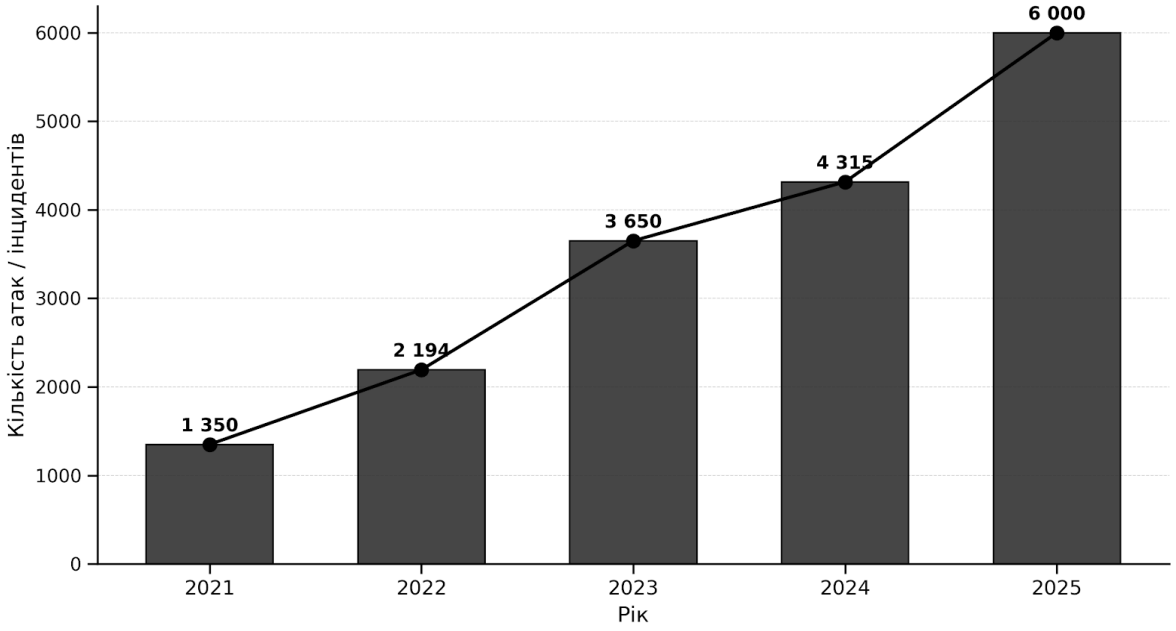

Рисунок 1.7 — Динаміка кібератак в Україні у 2021–2025 рр.

Примітка. Авторська розробка.

Особливої актуальності питання інформаційної безпеки набули в умовах повномасштабної війни та зростання кількості кібератак на українські підприємства та державні установи. Упродовж останніх років значно збільшилася кількість DDoS-атак на банківський сектор, державні сервіси та телекомунікаційну інфраструктуру України. Одними з основних загроз

залишаються фішингові кампанії, атаки на фінансові системи, шкідливе програмне забезпечення та спроби дестабілізації цифрової інфраструктури держави [22].

Доцільно зазначити, що українські підприємства активно адаптують міжнародний досвід управління інформаційною безпекою до умов воєнного стану та підвищених кіберризиків. Водночас, на мою думку, недоліком окремих систем захисту залишається недостатній рівень фінансування, дефіцит кваліфікованих фахівців та залежність від іноземних технологічних рішень. Подальший розвиток систем управління інформаційною безпекою в Україні повинен базуватися на поєднанні міжнародних стандартів, сучасних технологій кіберзахисту та національного досвіду протидії кіберзагрозам.

Висновки до розділу 1

1. У першому підрозділі досліджено сутність інформаційної безпеки бізнес-процесів та визначено її роль у діяльності цифрових підприємств. Встановлено, що розвиток цифрових технологій, онлайн-сервісів і хмарних платформ спричиняє зростання кіберризиків та потребує комплексного підходу до захисту інформації.
2. У другому підрозділі розглянуто основні види та характеристики систем управління інформаційною безпекою. Досліджено міжнародні стандарти та сучасні методи кіберзахисту, зокрема ризик-менеджмент, моніторинг, багатофакторну автентифікацію та концепцію Zero Trust.
3. У третьому підрозділі проаналізовано світовий та український досвід управління інформаційною безпекою. Встановлено, що сучасні підприємства активно впроваджують AI-моніторинг, SOC-центри, хмарний захист та багаторівневі системи безпеки для протидії кіберзагрозам. Загалом надійний захист даних неможливий без поєднання технологій, дисципліни та менеджменту.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ АТ «УНІВЕРСАЛ БАНК»

2.1. Організаційно-економічна характеристика діяльності АТ «УНІВЕРСАЛ БАНК»

АТ «УНІВЕРСАЛ БАНК» є одним із провідних комерційних банків України, який здійснює діяльність на фінансовому ринку відповідно до банківської ліцензії Національного банку України. Банк працює з 1994 року та за період свого існування пройшов декілька етапів розвитку і реорганізації, поступово трансформувавшись у сучасну цифрову фінансову установу. Історія банку розпочалася 20 січня 1994 року, коли була зареєстрована банківська установа під назвою КБ «Оазис». У подальшому банк неодноразово змінював назву та організаційну структуру, а з 2018 року функціонує як Акціонерне товариство «УНІВЕРСАЛ БАНК» [23].

На сьогодні АТ «УНІВЕРСАЛ БАНК» входить до банківської групи ТАС та здійснює повний спектр банківських операцій для фізичних і юридичних осіб. Кінцевим власником істотної участі банку є Сергій Тігіпко. Банк працює на підставі банківської ліцензії № 92 та є учасником Фонду гарантування вкладів фізичних осіб. Організаційно-правова форма банку – акціонерне товариство. Така форма господарювання забезпечує ефективне корпоративне управління, можливість залучення інвестицій та дотримання вимог банківського законодавства України. Діяльність банку регулюється Законом України «Про банки і банківську діяльність», нормативно-правовими актами Національного банку України та внутрішніми положеннями установи.

Основними напрямами діяльності АТ «УНІВЕРСАЛ БАНК» є обслуговування фізичних осіб, кредитування, депозитні операції, розрахунково-касове обслуговування, випуск та обслуговування платіжних карток, проведення валютних операцій, дистанційне банківське обслуговування

та надання сучасних цифрових фінансових послуг. Значну частину операцій банк здійснює через електронні канали взаємодії з клієнтами, що відповідає сучасним тенденціям цифровізації фінансового сектору.

Особливе місце в діяльності АТ «УНІВЕРСАЛ БАНК» займає проєкт monobank, який є роздрібним банківським продуктом банку та функціонує на його банківській ліцензії. Проєкт був запущений у 2017 році у співпраці з командою Fintech Band і став першим в Україні банком без традиційної мережі відділень. Усі основні банківські послуги клієнти отримують через мобільний застосунок, що дозволило значно скоротити операційні витрати та підвищити швидкість обслуговування клієнтів.

Важливо зазначити, що саме запуск monobank став одним із ключових факторів зростання АТ «УНІВЕРСАЛ БАНК» на банківському ринку України. Завдяки цифровій моделі обслуговування банк зміг залучити мільйони клієнтів та сформувати репутацію одного з найбільш інноваційних банків країни. Станом на 2025 рік кількість клієнтів monobank перевищила 10 млн осіб, що свідчить про високу популярність цифрових банківських послуг серед населення.

Серед конкурентних переваг банку доцільно виділити високий рівень цифровізації бізнес-процесів, зручність мобільного застосунку, широкий спектр дистанційних сервісів, швидкість проведення фінансових операцій та активне впровадження інноваційних технологій. Разом із тим така модель діяльності передбачає значну залежність від інформаційних систем, телекомунікаційної інфраструктури та цифрових каналів обслуговування клієнтів.

Важливо зазначити, що АТ «УНІВЕРСАЛ БАНК» займає вагоме місце на банківському ринку України не лише завдяки активному розвитку цифрових технологій, а й завдяки високому рівню фінансової стійкості та довіри клієнтів. Банк понад 30 років здійснює діяльність на українському фінансовому ринку та є учасником Фонду гарантування вкладів фізичних осіб. Надійність діяльності установи підтверджується довгостроковим кредитним рейтингом на рівні uaAA, а також найвищим рейтингом надійності банківських вкладів «5», що свідчить

про стабільне фінансове становище банку та його здатність виконувати зобов’язання перед клієнтами [24].

Станом на 2025 рік статутний капітал АТ «УНІВЕРСАЛ БАНК» становив понад 4,2 млрд грн, а обсяг активів перевищував 163 млрд грн. Такі показники характеризують банк як одну з найбільших фінансових установ України та свідчать про значний масштаб його операційної діяльності. Водночас важливим фактором розвитку банку є його орієнтація на довгострокове зростання, яке базується на принципах фінансової стабільності, бездоганної ділової репутації та впровадження сучасних технологічних рішень.

Діяльність АТ «УНІВЕРСАЛ БАНК» ґрунтується на системі корпоративних цінностей, серед яких особливе значення мають довіра та повага до клієнтів, прозорість діяльності, інноваційність, командна робота та постійне вдосконалення якості послуг. Банк активно впроваджує принципи сталого розвитку та корпоративної соціальної відповідальності, приділяючи увагу екологічним, соціальним та управлінським аспектам своєї діяльності. Крім того, важливим елементом розвитку персоналу є функціонування системи дистанційного навчання, що дозволяє підвищувати професійний рівень працівників та забезпечувати відповідність сучасним вимогам банківського сектору [25].

Про високий рівень конкурентоспроможності банку свідчать численні професійні нагороди та відзнаки. Зокрема, у 2025 році АТ «УНІВЕРСАЛ БАНК» було визнано переможцем у номінаціях «Роздрібний банк» та «Ощадний банк для населення» за результатами рейтингу «Банки року». Також банк отримав нагороду «Лідер банківського ринку» та переміг у номінації «Банк, якому довіряють українці». Водночас проєкт monobank неодноразово отримував міжнародне визнання як один із найкращих цифрових фінансових сервісів. Зокрема, у 2024 році він увійшов до рейтингу «250 найкращих фінтех-компаній світу» за версією CNBC, а у 2025 році його мобільний застосунок був визнаний найкращим фінансовим мобільним сервісом за результатами Mobile App Vision Awards [26].

Наявність значної клієнтської бази, високий рівень цифровізації бізнес-процесів та широке використання дистанційних каналів обслуговування створюють додаткові вимоги до забезпечення інформаційної безпеки банку. У сучасних умовах функціонування фінансових установ захист персональних даних клієнтів, безпека платіжних операцій, стійкість інформаційних систем та безперервність надання цифрових послуг стають одними з ключових факторів успішної діяльності банку.

Ефективність функціонування будь-якої банківської установи значною мірою залежить від побудови раціональної організаційної структури управління, яка забезпечує координацію діяльності структурних підрозділів, розподіл відповідальності між посадовими особами та контроль за виконанням стратегічних і операційних завдань. Для АТ «УНІВЕРСАЛ БАНК», діяльність якого базується на активному використанні цифрових технологій та дистанційних каналів обслуговування клієнтів, особливого значення набуває ефективна взаємодія між підрозділами, що відповідають за фінансову діяльність, інформаційні технології, управління ризиками та інформаційну безпеку.

Організаційна структура управління АТ «УНІВЕРСАЛ БАНК» побудована відповідно до вимог Національного банку України та принципів корпоративного управління, що застосовуються у провідних фінансових установах. Система управління банком передбачає чітке розмежування функцій стратегічного контролю та оперативного управління. Вищим органом корпоративного контролю виступає Наглядова рада, а безпосереднє керівництво поточною діяльністю здійснює Правління банку.

Наглядова рада виконує функції стратегічного управління та контролю за діяльністю банку. До її компетенції належать визначення стратегічних напрямів розвитку, затвердження внутрішніх політик, контроль за діяльністю Правління, оцінка системи внутрішнього контролю та управління ризиками. Головою Наглядової ради є Сергій Попенко, який має значний досвід роботи у фінансовому секторі та структурах Групи ТАС. До складу ради також входять

незалежні члени, які мають багаторічний досвід роботи у сфері банківської діяльності, фінансів, міжнародного бізнесу та фінансових технологій. Наявність незалежних членів забезпечує об’єктивність прийняття рішень та сприяє підвищенню ефективності корпоративного управління [27].

Операційне управління діяльністю банку здійснює Правління на чолі з Іриною Старомінською. Правління відповідає за реалізацію стратегії розвитку банку, організацію бізнес-процесів, забезпечення прибутковості діяльності, управління персоналом та впровадження інноваційних рішень. До складу Правління входять керівники ключових функціональних напрямів, що дозволяє оперативно координувати діяльність усіх структурних підрозділів банку [28].

Особливу роль у сучасній моделі управління АТ «УНІВЕРСАЛ БАНК» відіграють інформаційно-технологічні підрозділи. Враховуючи, що значна частина банківських операцій здійснюється через цифрові сервіси та мобільний застосунок monobank, безперебійне функціонування інформаційної інфраструктури є одним із головних факторів успішної діяльності банку. За розвиток IT-інфраструктури, цифрових платформ, програмного забезпечення та технологічних сервісів відповідає член Правління Валерій Задорожний. Під його керівництвом функціонують підрозділи, які забезпечують підтримку інформаційних систем, розвиток цифрових продуктів, адміністрування мережевої інфраструктури та супровід програмних комплексів банку.

Важливим елементом організаційної структури банку є система управління ризиками. Банківська діяльність пов’язана з великою кількістю фінансових, операційних, кредитних, ринкових та кібернетичних ризиків, що потребує постійного моніторингу та контролю. Система ризик-менеджменту забезпечує виявлення, оцінювання та мінімізацію потенційних загроз, які можуть негативно впливати на фінансову стійкість банку та його репутацію. Особливого значення в умовах цифровізації набуває управління кіберризиками та ризиками, пов’язаними із захистом інформаційних ресурсів.

Окреме місце в системі управління займає служба інформаційної безпеки та кіберзахисту. Її діяльність спрямована на забезпечення конфіденційності,

цілісності та доступності інформаційних ресурсів банку. За даний напрям діяльності на рівні Правління відповідає Тарас Лобода, до функціональних обов'язків якого належать організація системи інформаційної безпеки, контроль за дотриманням внутрішніх політик безпеки, управління кіберризиками та координація заходів щодо протидії кіберзагрозам. Підрозділи інформаційної безпеки здійснюють моніторинг подій безпеки, контроль доступу до інформаційних систем, захист персональних даних клієнтів, організацію реагування на кіберінциденти та забезпечення відповідності вимогам Національного банку України.

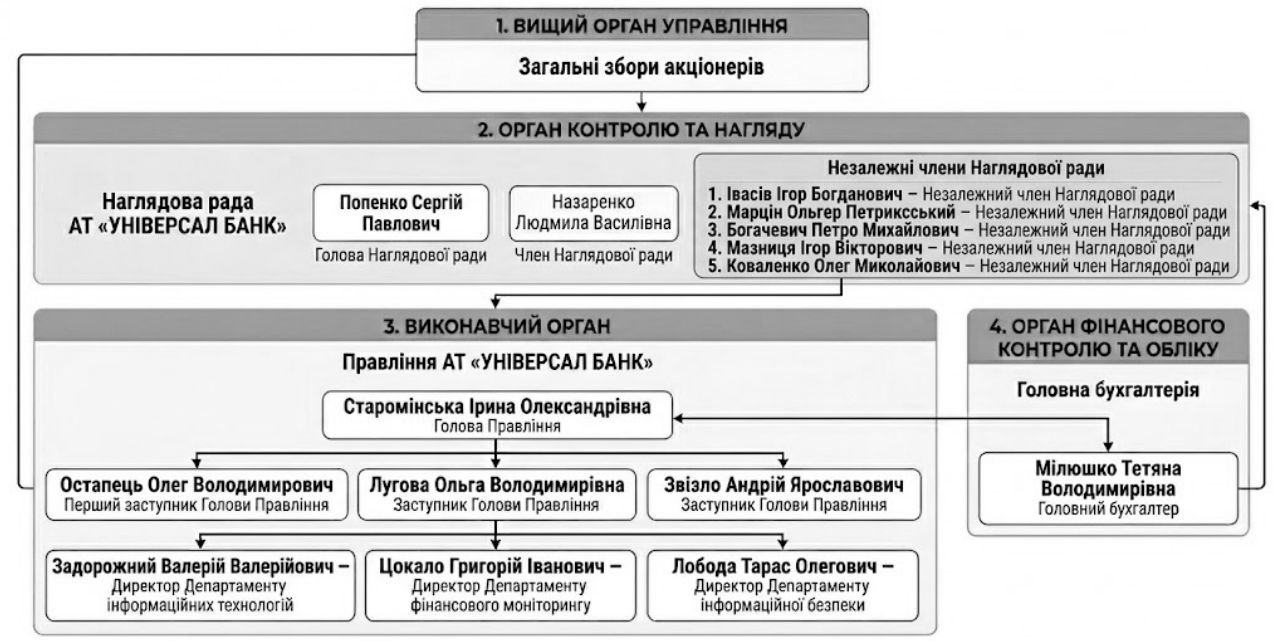

Рисунок 2.1 – Організаційна структура управління АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

З позиції теорії менеджменту суб'єктом управління в АТ «УНІВЕРСАЛ БАНК» виступає система органів управління, до складу якої входять Наглядова рада, Правління та керівники структурних підрозділів. Саме вони приймають управлінські рішення, визначають напрями розвитку банку та здійснюють контроль за виконанням поставлених завдань. Об'єктом управління є сукупність

бізнес-процесів, ресурсів та структурних підрозділів банку, які забезпечують надання банківських послуг та реалізацію стратегічних цілей установи.

У структурі управління банком інформаційна безпека займає міжфункціональне положення та взаємодіє практично з усіма напрямами діяльності. Вона пов’язана з ІТ-підрозділами, ризик-менеджментом, фінансовим моніторингом, внутрішнім контролем та операційною діяльністю. Такий підхід дозволяє інтегрувати процеси захисту інформації в усі бізнес-процеси банку та забезпечувати належний рівень захисту інформаційних активів, цифрових сервісів і персональних даних клієнтів.

Наступним варто розглянути ключові бізнес-процеси АТ «УНІВЕРСАЛ БАНК», до них належать відкриття та обслуговування рахунків клієнтів, здійснення платіжних операцій, кредитування, залучення депозитів, дистанційне банківське обслуговування та підтримка мобільного банкінгу. Особливістю діяльності банку є високий рівень цифровізації цих процесів, оскільки значна частина клієнтів користується послугами через мобільний застосунок monobank та інші онлайн-сервіси.

Одним із найважливіших бізнес-процесів є дистанційна ідентифікація клієнтів та відкриття рахунків. Використання цифрових технологій дозволяє проводити значну частину процедур без відвідування банківських відділень, що значно спрощує взаємодію клієнта з банком. Водночас це потребує використання сучасних механізмів перевірки особи, захисту персональних даних та контролю доступу до інформаційних систем.

Важливе місце в діяльності банку займають процеси кредитування та здійснення платежів. Для прийняття рішень щодо видачі кредитів використовуються автоматизовані системи аналізу клієнтських даних та оцінки ризиків. Платіжні операції обробляються в режимі реального часу, що вимагає безперебійної роботи інформаційної інфраструктури та високого рівня захисту від зовнішніх і внутрішніх загроз.

Окрему увагу банк приділяє роботі з персональними даними клієнтів. У процесі надання фінансових послуг здійснюється збір, обробка, зберігання та

передача значних обсягів конфіденційної інформації, включаючи персональні дані, фінансові показники, історію операцій та іншу інформацію з обмеженим доступом. Саме тому питання захисту інформаційних ресурсів є невід'ємною складовою всіх бізнес-процесіва банку.

Оскільки переважна більшість бізнес-процесів АТ «УНІВЕРСАЛ БАНК» реалізується через цифрові канали обслуговування клієнтів, особливого значення набуває забезпечення належного рівня інформаційної безпеки та захисту персональних даних. Ефективність функціонування банку значною мірою залежить від стійкості його інформаційних систем до кіберзагроз, безпеки цифрових сервісів та здатності забезпечувати безперервність надання фінансових послуг навіть в умовах підвищених ризиків. Разом з тим на діяльність банку впливають численні зовнішні фактори економічного, політичного, технологічного та правового характеру, що обумовлює необхідність аналізу соціально-економічних умов його функціонування.

Для всебічного оцінювання середовища, в якому функціонує фінансова установа, та визначення ступеня впливу глобальних макроекономічних і суспільних трендів на її стабільність, доцільно застосувати метод PESTLE-аналізу. Цей інструмент стратегічного менеджменту дозволяє структурувати зовнішні чинники за шістьма ключовими напрямами: політичними, економічними, соціальними, технологічними, екологічними та правовими. Його використання є критично важливим для банку, оскільки цифровізація послуг та робота з великими масивами даних вимагають постійної адаптації до динамічних змін у законодавстві, технологіях та споживчій поведінці.

Проведення PESTLE-аналізу для АТ «УНІВЕРСАЛ БАНК» дасть змогу не лише ідентифікувати потенційні загрози, такі як посилення кібератак чи регуляторні обмеження, але й виявити нові ринкові можливості для масштабування бізнесу. Розуміння макроконтексту допоможе керівництву банку оптимізувати стратегію управління ризиками, забезпечити високу стійкість цифрової інфраструктури та підвищити конкурентоспроможність.

Таблиця 2.4. PESTLE-аналіз АТ «УНІВЕРСАЛ БАНК»

Політичні фактори	Вага , V	Бал , B	Добуток, P	Економічні фактори	Вага , V	Бал , B	Добуток, P	Юридичні фактори	Вага , V	Бал , B	Добуток, P
Вплив воєнних дій	0,4	5	2	Процентні ставки (облікова ставка НБУ)	0,3	4	1,2	Фінансове регулювання та вимоги НБУ	0,35	5	1,75
Фіскальна політика та державні програми	0,25	4	1	Інфляція та купівельна спроможність	0,25	4	1	Закони про захист персональних даних	0,25	4	1
Зміни в законодавстві щодо лімітів переказів	0,2	4	0,8	Рівень безробіття та якість кредитів	0,25	3	0,75	Закони про захист прав споживачів	0,2	4	0,8
Політична стабільність та євроінтеграція	0,15	3	0,45	Валютні курси та обмінні операції	0,2	4	0,8	Законодавство та нормативи безпеки	0,2	4	0,8
Середня оцінка впливу політичних факторів			4,25	Середня оцінка впливу економічних факторів факторів			3,75	Середня оцінка впливу юридичних факторів			4,35
Сила впливу політичних факторів			Сильний вплив	Сила впливу економічних факторів			Помірний вплив	Сила впливу юридичних факторів			Сильний вплив
Соціальні фактори	Вага , V	Бал , B	Добуток, P	Технологічні фактори	Вага , V	Бал , B	Добуток, P	Екологічні фактори	Вага , V	Бал , B	Добуток, P
Демографічні зміни та міграція населення	0,3	4	1,2	Кібербезпека та захист від DDoS-атак	0,35	5	1,75	Цифровий формат сприяє скороченню використання паперових документів.	0,35	4	1,4
Зростання довіри до безготівкових розрахунків	0,3	5	1,5	Штучний інтелект	0,25	4	1	Відсутність фізичних відділень зменшує споживання ресурсів та викиди CO_2.	0,25	4	1
Популяризація банку через соцмережі та ігрові елементи	0,25	5	1,25	Хмарні обчислення	0,25	5	1,25	Енергоспоживання IT-інфраструктури.	0,2	4	0,8
Вміння користуватися інтернет-банкінгом	0,15	4	0,6	Технології розпізнавання (Дія, FaceID)	0,15	5	0,75	Впровадження ESG-підходів.	0,2	3	0,6
Середня оцінка впливу соціальних факторів			4,55	Середня оцінка впливу технологічних факторів			4,75	Середня оцінка впливу екологічних факторів			3,8
Сила впливу соціальних факторів			Сильний вплив	Сила впливу технологічних факторів			Критичний вплив	Сила впливу екологічних факторів			Помірний вплив

Примітка. Авторська розробка

Проведений PESTEL-аналіз демонструє, що АТ «УНІВЕРСАЛ БАНК» функціонує в надзвичайно динамічному та високоризиковому середовищі, де ключовими драйверами розвитку є технологічні та соціальні фактори. Максимальна середня оцінка технологічного блоку (4,75) підтверджує, що для АТ «УНІВЕРСАЛ БАНК» критично важливо інвестувати в кібербезпеку, захист від DDoS-атак та інтеграцію штучного інтелекту й хмарних обчислень. Це підкріплюється потужним соціальним капіталом (4,55), адже міграція населення, висока довіра до безготівкових розрахунків та цифрова грамотність українців формують стабільний попит на продукт компанії.

З іншого боку, найважчими викликами для банку залишаються зовнішні загрози, зафіксовані в юридичному (4,35) та політичному (4,25) секторах. Вплив воєнних дій, коливання фіскальної політики та жорсткі вимоги НБУ щодо фінансового регулювання і лімітів переказів створюють постійний тиск на операційну діяльність. Водночас рух у бік євроінтеграції виступає потужним стимулом для підтягування внутрішніх стандартів безпеки та захисту прав споживачів до міжнародного рівня. Економічні фактори (3,75), хоч і мають помірний характер, змушують банк гнучко реагувати на інфляцію та зміну облікової ставки.

Щодо екологічного блоку, то із середньою оцінкою 3,8 він має помірний, але стратегічно важливий вплив. Цифровий формат банку без фізичних відділень та паперової тяганини є його суттєвою конкурентною перевагою, що знижує операційні витрати та покращує репутацію. Проте високе енергоспоживання IT-інфраструктури в поєднанні з ризиками для стабільності енергосистеми вимагає від АТ «УНІВЕРСАЛ БАНК» фокусу на автономності. Загалом, для збереження лідерства банк повинен використовувати свою технологічну гнучкість для нівелювання регуляторних і воєнних ризиків, паралельно впроваджуючи ESG-підходи для майбутнього масштабування на європейському ринку.

2.2. Діагностика показників фінансово-господарської діяльності підприємства АТ «УНІВЕРСАЛ БАНК»

Для оцінки результативності діяльності АТ «УНІВЕРСАЛ БАНК» було проведено аналіз основних фінансово-господарських показників за 2022–2025 роки. Дослідження дозволяє оцінити масштаби діяльності банку, рівень його фінансової стійкості та ефективність використання ресурсів [29].

Таблиця 2.5. Основні показники фінансово-господарської діяльності АТ «УНІВЕРСАЛ БАНК» у 2022–2025 рр.

Найменування показника	2022 рік	2023 рік	2024 рік	2025 рік
Усього активів, тис.грн	86 559 232	119 822 713	146 678 600	213 356 583
Усього зобов'язань, тис.грн	77 355 432	108 251 273	131 327 542	187 718 803
Усього власного капіталу, тис.грн	9 203 800	11 571 440	15 351 058	25 637 780
Прибуток за рік, тис.грн	2 158 814	1 797 238	3 686 567	10 375 964
Чистий процентний дохід, тис.грн	8 486 073	12 003 001	16 000 499	21 000 231
Усього сукупного доходу за рік, тис.грн	2 479 493	2 367 640	3 779 618	10 286 722
Середня кількість працівників	2 065	2 183	2 435	2 834

Примітка. Розроблено за джерелом [29].

Аналіз динаміки фінансових показників свідчить про те, що протягом досліджуваного періоду банк демонстрував стабільне та високодинамічне зростання обсягів своєї діяльності. Про це яскраво свідчить траєкторія зміни балансової вартості ресурсів: загальний обсяг активів фінансової установи суттєво збільшився — з 86 559 232 тис. грн у 2022 році до 213 356 583 тис. грн на кінець 2025 року, що становить приріст майже у 2,5 раза (або на 146,5%).

Така стійка позитивна тенденція, навіть за умов макроекономічної нестабільності, підтверджує ефективність обраної стратегії розвитку, активне нарощування ресурсної бази, а також капіталізацію отриманих прибутків.

Подібне масштабування діяльності вказує на зміцнення ринкових позицій банку, підвищення рівня довіри з боку клієнтів та інвесторів, а також на послідовне розширення спектра й обсягів проведення активних банківських операцій.

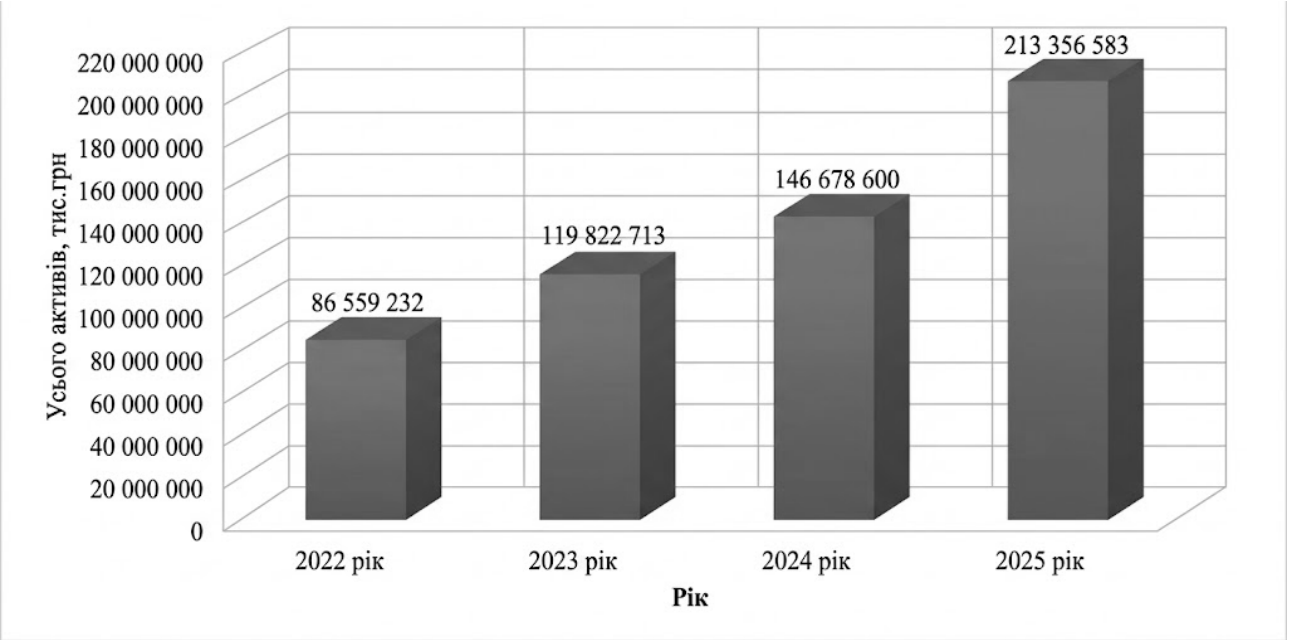

Рисунок 2.2 – Результати аналізу динаміки активів АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Аналогічна стійка тенденція до зростання спостерігається і при дослідженні структури та обсягів зобов'язань фінансової установи. Протягом аналізованого чотирирічного періоду загальний обсяг зобов'язань банку продемонстрував стрімке збільшення — з 77 355 432 тис. грн у 2022 році до 187 718 803 тис. грн на кінець 2025 року, що свідчить про зростання показника у понад 2,4 раза.

Головним детермінуючим фактором такої вираженої висхідної динаміки стало послідовне збільшення обсягів залучених коштів клієнтів, як фізичних, так і юридичних осіб, а також системне розширення й диверсифікація депозитної бази банку. Отримані результати підтверджують високий рівень фінансової надійності установи та зростання довіри з боку вкладників, що дозволило банку сформувати стабільний пул строкових ресурсів для

подальшого фінансування активних операцій і забезпечення належної ліквідності в довгостроковій перспективі.

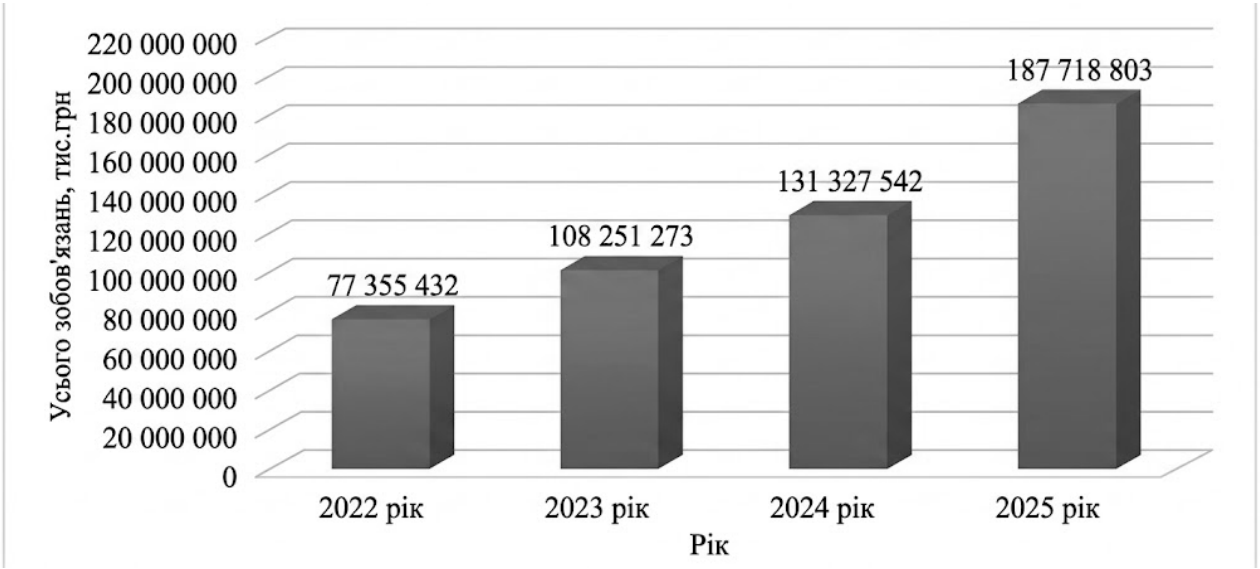

Рисунок 2.3 – Результати аналізу динаміки зобов'язань АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Вкрай позитивно є суттєве й планомірне зростання власного капіталу фінансової установи протягом усього досліджуваного періоду. Якщо наприкінці 2022 року обсяг забезпечення банку власними коштами становив 9 203 800 тис. грн, то до 2025 року його величина досягла значного показника у 25 637 780 тис. грн, що майже у 2,8 раза перевищує базовий рівень. Процес нарощування капіталу відбувався безперервно, фіксуючи проміжні значення на рівні 11 571 440 тис. грн у 2023 році та 15 351 058 тис. грн у 2024 році.

Така чітко виражена позитивна динаміка капіталізації є ключовим індикатором системного зміцнення фінансової стійкості та автономності банку. Стрімке розширення капітальної бази, що відбулося переважно внаслідок реінвестування чистого прибутку, значно підвищує рівень платоспроможності установи та її здатність ефективно протистояти агресивним зовнішнім ризикам і макроекономічним шокам. Збільшення власного капіталу створює міцний фундамент для захисту інтересів вкладників, розширює потенціал для

подальшого нарощування масштабів активних операцій та виступає надійним гарантом довгострокової фінансової стабільності і конкурентоспроможності банку на вітчизняному ринку фінансових послуг..

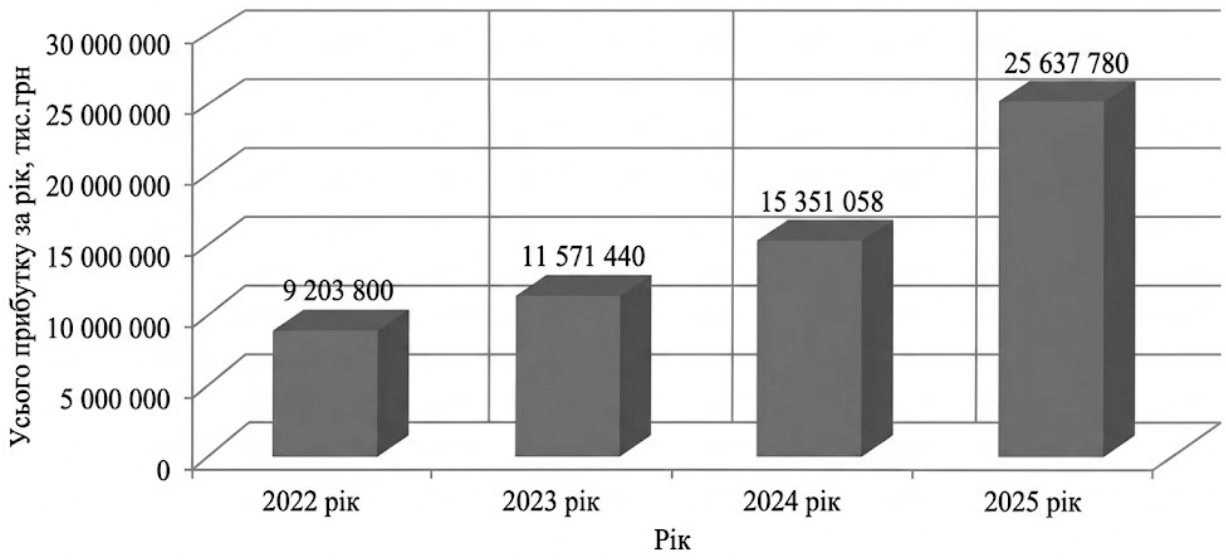

Рисунок 2.4 – Результати аналізу динаміки прибутку АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Особливої уваги в межах дослідження фінансових результатів діяльності установи заслуговує аналіз динаміки її чистого прибутку. Протягом 2022–2025 років фінансова установа демонструвала вражаючі темпи зростання рентабельності, попри незначне коливання на початку аналізованого періоду, коли у 2023 році прибуток склав 1 797 238 тис. грн проти 2 158 814 тис. грн у 2022 році. Починаючи з 2024 року, відбулося стрімке відновлення та інтенсифікація фінансових результатів: показник зріс до 3 686 567 тис. грн, а на кінець 2025 року досяг рекордного значення у 10 375 964 тис. грн, що перевищує рівень 2022 року майже у 4,8 раза.

Такий вагомий кумулятивний ефект та експоненціальний приріст кінцевого фінансового результату свідчать про високу ефективність менеджменту, оптимізацію структури доходів і витрат, а також про високу маржинальність проведених банківських операцій. Стрімке генерування

прибутку не лише підтверджує ринкову конкурентоспроможність банку, але й створює надійне підґрунтя для подальшого саморозвитку, капіталізації установи, підвищення її фінансової стійкості та формування додаткових резервних фондів для мінімізації можливих банківських ризиків.

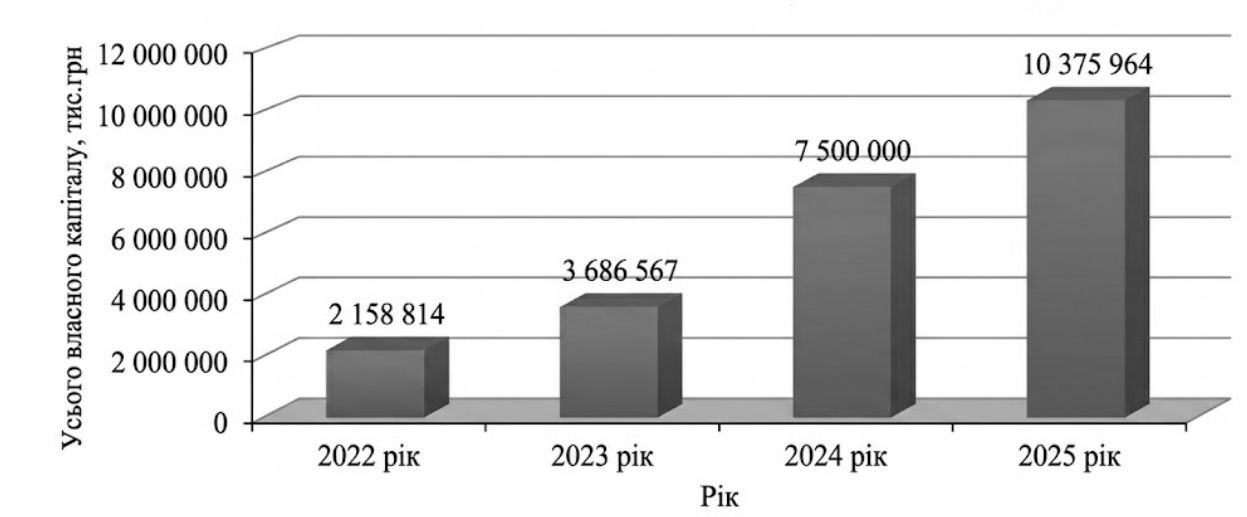

Рисунок 2.5 – Результати аналізу динаміки чистого прибутку АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Важливим індикатором фінансової стабільності та ключовим показником ефективності діяльності фінансової установи є чистий процентний дохід. За досліджуваний період цей показник продемонстрував стрімку позитивну динаміку, збільшившись майже у 2,5 раза — з 8 486 073 тис. грн до 21 000 231 тис. грн

Така стійка висхідна тенденція свідчить передусім про високу якість та ефективність управління активними й пасивними операціями банку. Зокрема, це є результатом оптимізації структури балансу, зваженої політики формування процентної маржі та здатності інституції адаптуватися до мінливих макроекономічних умов. Зростання чистого процентного доходу підтверджує значне розширення масштабів та прибутковості основної банківської діяльності, посилення ринкових позицій.

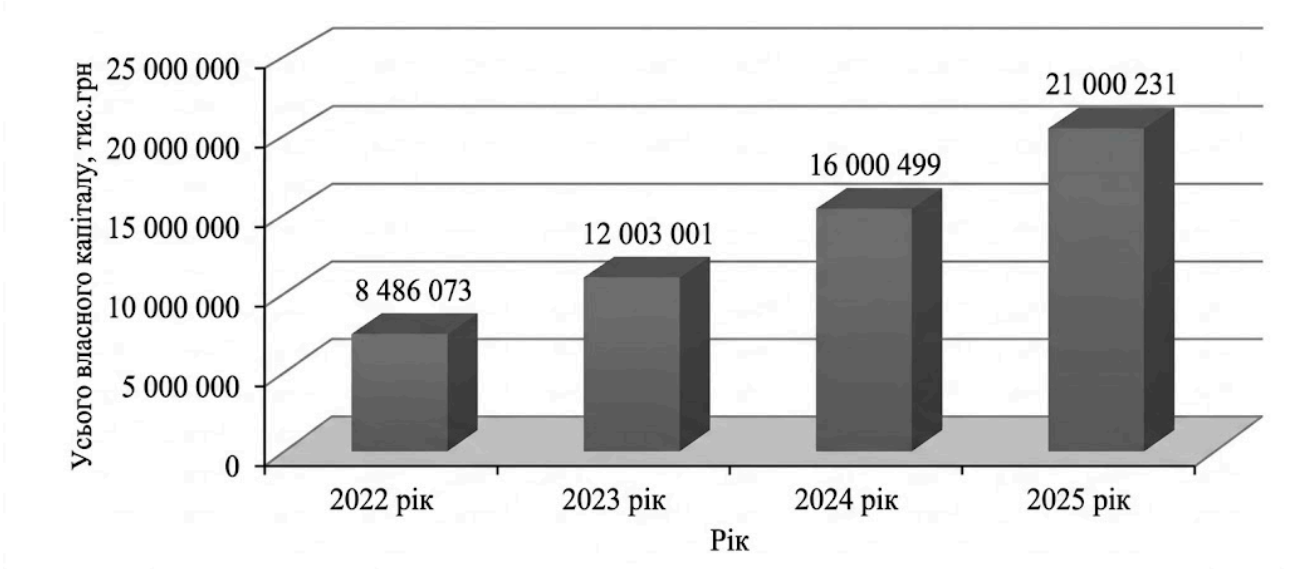

Рисунок 2.6 – Результати аналізу динаміки власного капіталу АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Суттєве та динамічне зростання протягом аналізованого періоду спостерігається за показником усього сукупного доходу банку. У 2025 році цей індикатор досяг рекордної позначки, склавши 10 286 722 тис. грн. Порівнюючи з базовим 2022 роком, коли сукупний дохід становив 2 479 493 тис. грн, обсяг надходжень збільшився більш ніж у чотири рази. При цьому траєкторія розвитку демонструє, що після незначного коливання у 2023 році, фінансова установа вийшла на стабільний тренд прискореного зростання, починаючи з 2024 року.

Така стрімка висхідна динаміка є чітким свідченням високої операційної ефективності діяльності банку, його фінансової стійкості та здатності генерувати стабільні потоки доходів навіть в умовах макроекономічної турбулентності. Це також підтверджує успішну реалізацію стратегічної бізнес-моделі установи, виважену диверсифікацію джерел прибутку, оптимізацію структури активів та високу конкурентоспроможність банку на фінансовому ринку.

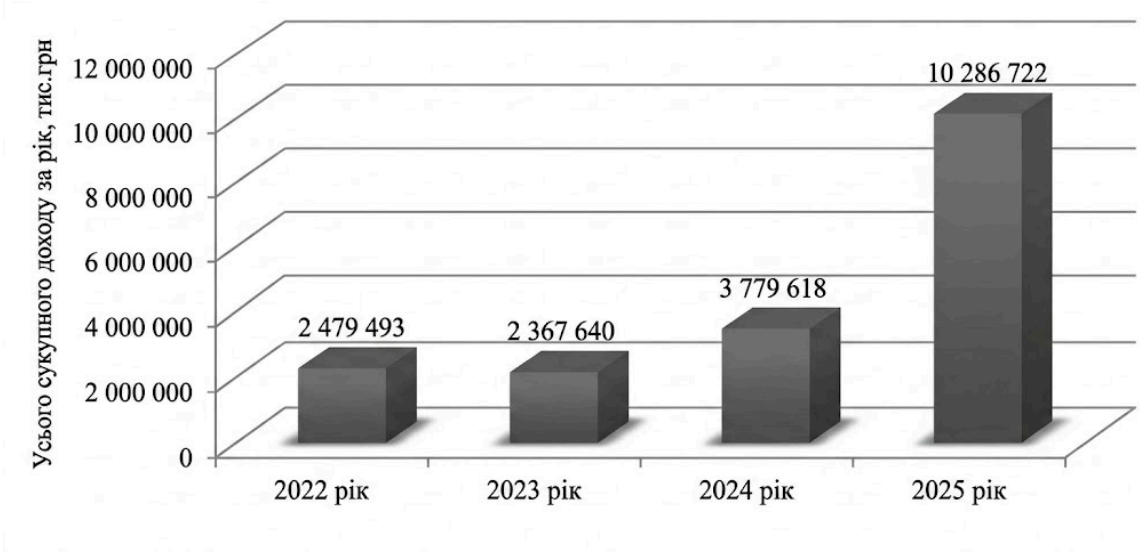

Рисунок 2.7 – Результати аналізу динаміки сукупного доходу АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Поряд зі зростанням фінансових результатів збільшувалася і чисельність персоналу. Якщо у 2022 році середня кількість працівників становила 2 065 осіб, то у 2025 році вона досягла 2 834 осіб. Це пов'язано з розвитком цифрових сервісів, розширенням клієнтської бази та необхідністю забезпечення безперебійної роботи банківських систем.

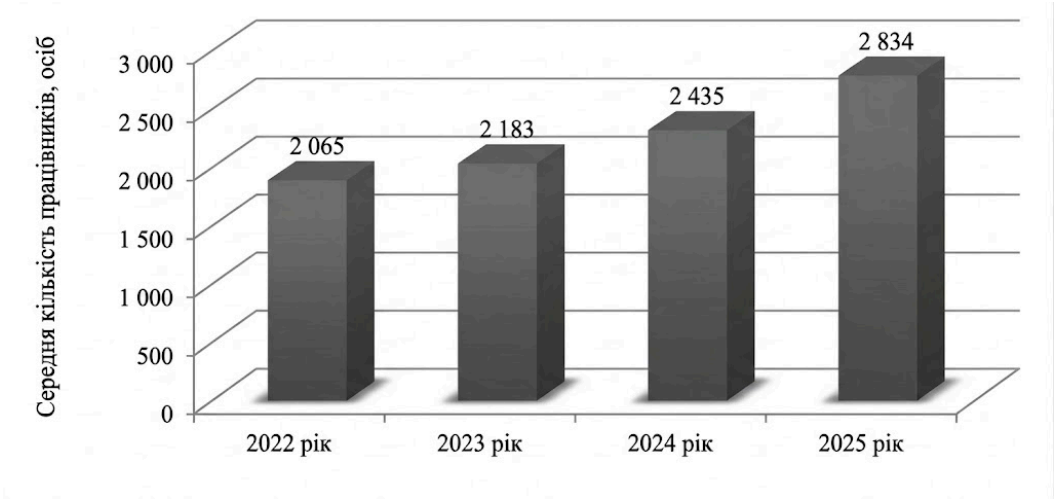

Рисунок 2.8 – Результати аналізу динаміки кількості працівників АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Для більш повної оцінки результативності діяльності АТ «УНІВЕРСАЛ БАНК» було розраховано показники рентабельності та фінансової стійкості.

Таблиця 2.6. Показники ефективності діяльності АТ «УНІВЕРСАЛ БАНК» у 2022–2025 рр.

Показник	2022	2023	2024	2025
Рентабельність активів (ROA), %	2,49	1,5	2,51	4,86
Рентабельність власного капіталу (ROE), %	23,46	15,53	24,02	40,47
Коефіцієнт фінансової стійкості	0,106	0,097	0,105	0,12
Коефіцієнт фінансової залежності	9,4	10,36	9,55	8,32

Примітка. Авторська розробка.

Формули розрахунку: ROA: Прибуток за рік / Активи × 100%; ROE: Прибуток за рік / Власний капітал × 100%; Коефіцієнт фінансової стійкості: Власний капітал / Активи; Коефіцієнт фінансової залежності: Активи / Власний капітал.

Аналіз показника рентабельності активів свідчить про позитивну тенденцію підвищення ефективності використання активів банку. У 2022 році значення показника становило 2,49 %, однак у 2023 році воно знизилося до 1,50 %, що було пов'язано зі складними економічними умовами функціонування банківської системи України в період воєнного стану. Водночас уже у 2024 році спостерігалося відновлення позитивної динаміки, а у 2025 році ROA досяг 4,86 %, що є найкращим результатом за досліджуваний період. Це свідчить про зростання прибутковості активних операцій та ефективніше використання ресурсної бази банку.

Рентабельність власного капіталу протягом 2022–2025 років також демонструвала загальну тенденцію до зростання. Після зниження до 15,53 % у 2023 році показник поступово зростав і в 2025 році досяг 40,47 %. Такий результат свідчить про високу ефективність використання власного капіталу та

значне підвищення прибутковості діяльності банку для його акціонерів.

Коефіцієнт фінансової стійкості протягом аналізованого періоду перебував у межах від 0,097 до 0,120. Найвище значення показника зафіксовано у 2025 році, що свідчить про зміцнення капітальної бази банку та підвищення рівня його фінансової незалежності. Зростання частки власного капіталу в структурі активів позитивно впливає на здатність банку протистояти фінансовим ризикам та забезпечувати стабільність своєї діяльності.

Водночас коефіцієнт фінансової залежності мав тенденцію до поступового зниження. Якщо у 2023 році його значення становило 10,36, то у 2025 році воно скоротилося до 8,32. Це свідчить про зменшення залежності банку від залучених ресурсів та покращення структури джерел фінансування його діяльності.

Отже, результати проведеного аналізу підтверджують високий рівень ефективності діяльності АТ «УНІВЕРСАЛ БАНК». Банк демонструє стабільне зростання прибутковості, зміцнення фінансової стійкості та покращення показників використання активів і капіталу. Позитивна динаміка фінансових результатів створює сприятливі умови для подальшого розвитку цифрових банківських сервісів та вдосконалення системи управління інформаційною безпекою, яка є одним із ключових факторів забезпечення надійності та конкурентоспроможності банку в сучасних умовах цифровізації фінансового сектору.

2.3. Оцінка системи управління інформаційною безпекою на підприємстві АТ «УНІВЕРСАЛ БАНК»

Після проведення аналізу фінансово-господарської діяльності АТ «УНІВЕРСАЛ БАНК» доцільно перейти до оцінки системи управління інформаційною безпекою підприємства. Для цифрового банку рівень захисту інформаційних ресурсів є одним із ключових факторів забезпечення стабільності діяльності, підтримання довіри клієнтів та дотримання вимог

регуляторів. Особливого значення це питання набуває в умовах зростання кількості кіберзагроз, активного розвитку цифрових банківських сервісів та високої залежності бізнес-процесів від функціонування інформаційних систем.

Варто зазначити, що окремі елементи системи інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» уже були розглянуті у підрозділі 1.3 під час дослідження вітчизняного та світового досвіду розвитку систем управління інформаційною безпекою. Зокрема, було проаналізовано використання банком стандарту PCI DSS, технологій Face ID та Touch ID, протоколу TLS, а також систем anti-fraud-моніторингу. У даному підрозділі зазначені інструменти будуть розглянуті більш детально з позиції оцінки їх практичного використання в діяльності АТ «УНІВЕРСАЛ БАНК» [18].

Система управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК» сформована відповідно до сучасних вимог цифрового банкінгу та спрямована на забезпечення конфіденційності, цілісності й доступності інформації. Враховуючи, що значна частина банківських послуг надається через мобільний застосунок monobank, особлива увага приділяється захисту персональних даних клієнтів, безпеці фінансових транзакцій та безперервності роботи цифрової інфраструктури.

Основою функціонування системи інформаційної безпеки виступає політика інформаційної безпеки банку, яка визначає порядок управління інформаційними активами, розподіл відповідальності між структурними підрозділами, правила доступу до інформаційних ресурсів та механізми реагування на кіберінциденти. Політика інформаційної безпеки спрямована на мінімізацію ризиків витоку даних, несанкціонованого доступу та порушення функціонування інформаційних систем.

Важливим елементом захисту платіжної інфраструктури є відповідність міжнародному стандарту PCI DSS (Payment Card Industry Data Security Standard). Дотримання вимог даного стандарту дозволяє забезпечити безпечне зберігання, обробку та передачу даних платіжних карток, а також мінімізувати ризики шахрайства під час здійснення фінансових операцій. Використання

стандарту PCI DSS є необхідною умовою функціонування сучасних цифрових банків та виступає одним із базових інструментів захисту платіжних систем.

Для забезпечення безпечної передачі інформації між клієнтськими пристроями та серверною інфраструктурою банк використовує криптографічний протокол TLS (Transport Layer Security). Завдяки застосуванню сучасних алгоритмів шифрування забезпечується захист даних від перехоплення, модифікації або несанкціонованого доступу під час їх передачі через мережу Інтернет. Використання TLS є важливим складником підтримання конфіденційності та цілісності інформації в цифровому середовищі.

Значна увага приділяється безпечній автентифікації клієнтів. Для підтвердження особи користувача мобільний застосунок підтримує використання біометричних технологій Face ID та Touch ID. Застосування біометричної ідентифікації дозволяє суттєво знизити ризики компрометації облікових записів та підвищує рівень захищеності клієнтських даних. Крім того, біометричні методи забезпечують зручність користування цифровими сервісами без зниження рівня безпеки.

Одним із ключових елементів системи захисту є використання багатофакторної автентифікації. Даний механізм передбачає підтвердження особи користувача за допомогою декількох незалежних факторів, зокрема пароля, одноразового коду підтвердження або біометричних даних. Використання багатофакторної автентифікації значно ускладнює можливість несанкціонованого доступу навіть у випадку компрометації одного із засобів автентифікації.

Для протидії фінансовому шахрайству в банку функціонують спеціалізовані anti-fraud системи. Їх призначення полягає у виявленні підозрілих операцій, аналізі поведінки користувачів та автоматичному блокуванні потенційно небезпечних транзакцій. Такі системи дозволяють оперативно реагувати на спроби шахрайських дій та мінімізувати можливі фінансові втрати як банку, так і його клієнтів.

Важливою складовою системи інформаційної безпеки є постійний моніторинг фінансових транзакцій. Аналіз операцій у режимі реального часу дозволяє своєчасно виявляти аномальну активність, нетипову поведінку користувачів та ознаки кіберзагроз. Використання автоматизованих засобів моніторингу забезпечує оперативне реагування на інциденти безпеки та сприяє підвищенню загального рівня захищеності банківської інфраструктури.

Система управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК» базується на комплексному поєднанні організаційних, програмних та технічних засобів захисту. Використання стандарту PCI DSS, протоколів шифрування TLS, біометричної автентифікації, багатофакторного захисту, anti-fraud систем та моніторингу транзакцій дозволяє забезпечити високий рівень захисту інформаційних ресурсів і підтримувати стабільне функціонування цифрових банківських сервісів.

Важливою складовою ефективного функціонування системи управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК» є належне організаційне забезпечення, яке визначає розподіл повноважень, відповідальності та взаємодії між структурними підрозділами банку у сфері кіберзахисту. На відміну від технічних засобів захисту, організаційне забезпечення спрямоване на формування системи управління, яка дозволяє координувати процеси інформаційної безпеки на всіх рівнях діяльності установи [28].

Як було встановлено під час аналізу організаційної структури банку в підрозділі 2.1, управління інформаційною безпекою здійснюється на рівні Правління та профільних структурних підрозділів. Загальне керівництво системою інформаційної безпеки забезпечується через взаємодію IT-підрозділів, служби інформаційної безпеки та ризик-менеджменту, що дозволяє інтегрувати заходи кіберзахисту в усі бізнес-процеси банку.

Особливу роль у забезпеченні інформаційної безпеки відіграють інформаційно-технологічні підрозділи банку. Враховуючи високий рівень цифровізації діяльності АТ «УНІВЕРСАЛ БАНК» та функціонування мобільного застосунку monobank, стабільність і захищеність інформаційної

інфраструктури безпосередньо впливають на якість банківського обслуговування та безперервність надання послуг клієнтам. За розвиток інформаційних технологій та цифрової інфраструктури відповідає член Правління Валерій Задорожний. Під його керівництвом функціонують підрозділи, які забезпечують адміністрування серверної та мережевої інфраструктури, підтримку програмного забезпечення, впровадження нових цифрових сервісів, резервування даних та підтримання безперервності роботи інформаційних систем.

Одним із ключових елементів організаційного забезпечення інформаційної безпеки є служба інформаційної безпеки та кіберзахисту. Її діяльність спрямована на реалізацію внутрішньої політики безпеки, контроль дотримання встановлених вимог, моніторинг подій безпеки та координацію заходів щодо протидії кіберзагрозам. Як було зазначено раніше, на рівні Правління за даний напрям відповідає Тарас Лобода. До його функціональних обов’язків належать організація системи захисту інформаційних ресурсів, управління кіберризиками, забезпечення відповідності вимогам Національного банку України та координація реагування на кіберінциденти.

Підрозділи інформаційної безпеки здійснюють постійний контроль доступу до інформаційних систем банку, забезпечують захист персональних даних клієнтів, контролюють використання облікових записів працівників та здійснюють моніторинг потенційно небезпечної активності. Крім того, вони беруть участь у проведенні внутрішніх аудитів безпеки, тестуванні вразливостей та впровадженні нових механізмів кіберзахисту відповідно до сучасних вимог цифрового банкінгу.

Важливе місце в системі організаційного забезпечення займає підрозділ ризик-менеджменту. Банківська діяльність характеризується наявністю значної кількості ризиків, серед яких особливого значення набувають кіберризики та ризики, пов’язані із захистом інформаційних ресурсів. Основним завданням ризик-менеджменту є виявлення потенційних загроз, оцінювання їх впливу на діяльність банку та розробка заходів щодо мінімізації можливих негативних

наслідків.

У сфері інформаційної безпеки підрозділи ризик-менеджменту здійснюють оцінювання ризиків витоку даних, несанкціонованого доступу до інформаційних систем, збоїв у роботі цифрової інфраструктури та можливих наслідків кібератак. Результати такого аналізу використовуються під час прийняття управлінських рішень щодо модернізації систем захисту, впровадження нових технологій безпеки та формування планів реагування на надзвичайні ситуації.

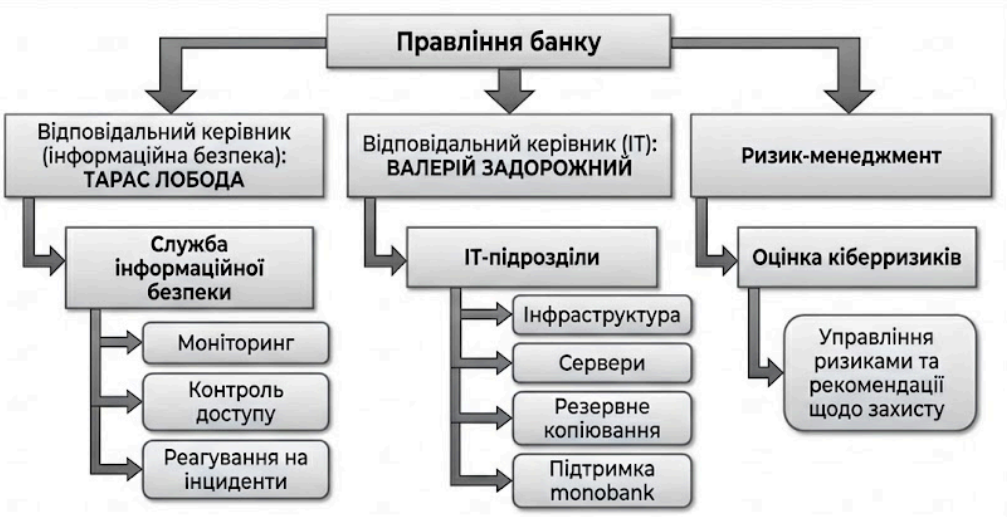

Рисунок 2.9 – Організаційне забезпечення системи інформаційної безпеки АТ «УНІВЕРСАЛ БАНК

Примітка. Авторська розробка.

Доцільно зазначити, що ефективність організаційного забезпечення інформаційної безпеки значною мірою залежить від рівня взаємодії між IT-підрозділами, службою інформаційної безпеки та системою ризик-менеджменту. Такий підхід дозволяє забезпечити комплексний захист інформаційних активів банку, своєчасно виявляти потенційні загрози та оперативно реагувати на інциденти безпеки.

Організаційне забезпечення інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» базується на чіткому розподілі функцій між структурними підрозділами

та інтеграції процесів кіберзахисту в систему корпоративного управління. Координація діяльності ІТ-підрозділів, служби інформаційної безпеки та ризик-менеджменту створює необхідні умови для підтримання високого рівня захисту інформаційних ресурсів і стабільного функціонування цифрових банківських сервісів.

Функціональне забезпечення системи інформаційної безпеки характеризує практичну реалізацію заходів захисту інформаційних ресурсів банку та охоплює сукупність процедур, технологій і механізмів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації. Для АТ «УНІВЕРСАЛ БАНК», діяльність якого значною мірою базується на використанні цифрових сервісів та мобільного застосунку monobank, ефективність функціонального забезпечення є одним із ключових факторів підтримання довіри клієнтів та забезпечення безперервності банківської діяльності.

Одним із базових напрямів функціонального забезпечення виступає контроль доступу до інформаційних ресурсів банку. Доступ до інформаційних систем надається відповідно до посадових обов’язків працівників та принципу мінімально необхідних привілеїв. Такий підхід дозволяє обмежити можливість несанкціонованого доступу до критично важливих даних та знизити ризики внутрішніх загроз. Для клієнтів банку застосовуються механізми багатофакторної автентифікації, а також біометричні засоби підтвердження особи у вигляді Face ID та Touch ID. Використання багаторівневого контролю доступу забезпечує додатковий рівень захисту облікових записів та фінансових операцій.

Важливим елементом функціонування системи інформаційної безпеки є моніторинг інцидентів та подій безпеки. Для своєчасного виявлення кіберзагроз банк використовує автоматизовані засоби контролю активності користувачів, мережевого трафіку та фінансових операцій. Постійний моніторинг дозволяє виявляти підозрілі дії, аномальну поведінку користувачів та ознаки можливих кібератак. Особливого значення набуває використання anti-fraud систем, які

забезпечують аналіз транзакцій у режимі реального часу та автоматичне реагування на потенційно шахрайські операції.

Необхідною складовою забезпечення безперервності діяльності банку є резервне копіювання інформації. Резервні копії критично важливих даних дозволяють оперативно відновити роботу інформаційних систем у випадку технічних збоїв, кібератак або пошкодження інформаційних ресурсів. Використання резервування даних мінімізує ризики втрати інформації та забезпечує стабільність функціонування банківських сервісів навіть у разі виникнення надзвичайних ситуацій.

Особливу увагу АТ «УНІВЕРСАЛ БАНК» приділяє захисту мобільного застосунку monobank, який є основним каналом взаємодії з клієнтами. Захист застосунку забезпечується за допомогою шифрування даних, використання захищених протоколів передачі інформації TLS, біометричної автентифікації та постійного оновлення програмного забезпечення. Крім того, реалізовані механізми контролю пристроїв користувачів, підтвердження фінансових операцій та виявлення підозрілої активності, що дозволяє знизити ризики несанкціонованого доступу до рахунків клієнтів.

Важливим функціональним напрямом є захист клієнтських даних. Банк обробляє значні обсяги персональної та фінансової інформації, що потребує впровадження ефективних механізмів захисту від витоку, модифікації або несанкціонованого доступу. Для цього використовуються технології шифрування, розмежування прав доступу, моніторинг інформаційних потоків та контроль операцій з конфіденційними даними. Додатково застосовуються процедури внутрішнього контролю та аудиту, які спрямовані на забезпечення відповідності вимогам регуляторів та внутрішніх політик безпеки.

Таким чином, функціональне забезпечення системи інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» охоплює комплекс взаємопов’язаних заходів, спрямованих на захист інформаційних ресурсів, фінансових операцій та персональних даних клієнтів. Використання сучасних механізмів контролю доступу, моніторингу інцидентів, резервного копіювання та захисту цифрових

сервісів дозволяє підтримувати високий рівень кіберстійкості банку в умовах зростання кількості цифрових загроз.

Наступним для комплексної оцінки системи управління інформаційною безпекою доцільно провести SWOT-аналіз, який дозволяє визначити сильні та слабкі сторони існуючої системи захисту, а також оцінити перспективи її розвитку та потенційні загрози зовнішнього середовища.

Таблиця 2.7. SWOT-аналіз системи інформаційної безпеки АТ «УНІВЕРСАЛ БАНК»

Сильні сторони	Слабкі сторони
1. Високий рівень цифровізації 2. Багатофакторна автентифікація та біометрія 3. Використання anti-fraud систем 4. Відповідність вимогам НБУ та міжнародним стандартам інформаційної безпеки	1. Залежність від цифрових каналів 2. Високі витрати на кіберзахист 3. Людський фактор
Можливості	**Загрози**
1. AI-моніторинг 2. Впровадження Zero Trust 3. Розвиток хмарних технологій 4. Розвиток SOC-центрів 5. Використання технологій машинного навчання для прогнозування кіберзагроз	1. Кібератаки 2. Фішингові атаки 3. Витік даних 4. DDoS-атаки

Примітка. Авторська розробка.

Проведений SWOT-аналіз свідчить про те, що система інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» характеризується значною кількістю сильних сторін. Насамперед це пов’язано з високим рівнем цифровізації бізнес-процесів, використанням багатофакторної автентифікації, біометричних технологій та сучасних anti-fraud систем, які забезпечують ефективний захист фінансових операцій і клієнтських даних.

Таблиця 2.8. Стратегія АТ «УНІВЕРСАЛ БАНК»

	Сильні сторони	Слабкі сторони
Можливості	9	7
Загрози	8	7

Примітка. Авторська розробка.

Проведений SWOT-аналіз свідчить, що для АТ «УНІВЕРСАЛ БАНК»

доцільною є стратегія використання комбінації «Сильні сторони – Можливості» (СМ-стратегія). Такий підхід передбачає максимальне використання наявного високого рівня цифровізації, багатофакторної автентифікації, біометричних технологій та anti-fraud систем у поєднанні з перспективами розвитку сучасних технологій кіберзахисту. Зокрема, впровадження AI-моніторингу, технологій машинного навчання для прогнозування кіберзагроз, розвиток SOC-центрів, а також перехід до архітектури Zero Trust і хмарних рішень дозволяє суттєво підвищити рівень кіберстійкості банку. Реалізація такої стратегії забезпечить не лише посилення захисту інформаційних систем, але й підвищення ефективності управління ризиками та відповідність сучасним міжнародним стандартам інформаційної безпеки.

Водночас функціонування цифрового банку супроводжується певними слабкими сторонами. Основною з них є висока залежність від цифрових каналів обслуговування, оскільки будь-які порушення роботи інформаційної інфраструктури можуть впливати на доступність банківських послуг. Крім того, підтримання сучасної системи кіберзахисту потребує значних фінансових витрат, а людський фактор залишається джерелом потенційних ризиків інформаційної безпеки.

Серед перспективних можливостей розвитку системи інформаційної безпеки доцільно виділити впровадження розширених інструментів AI-моніторингу, використання концепції Zero Trust, розвиток хмарних технологій та створення більш потужних центрів моніторингу безпеки (SOC). Реалізація зазначених напрямів дозволить підвищити рівень кіберстійкості банку та забезпечити більш ефективне реагування на сучасні кіберзагрози.

Разом із тим зовнішнє середовище характеризується значною кількістю загроз. Найбільш суттєвими серед них є кібератаки на фінансові установи, поширення фішингових схем, ризики витоку конфіденційної інформації та DDoS-атаки, які можуть негативно впливати на стабільність функціонування цифрових сервісів банку. В умовах постійного зростання кількості кіберзагроз АТ «УНІВЕРСАЛ БАНК» потребує безперервного вдосконалення системи

інформаційної безпеки та впровадження новітніх технологій кіберзахисту.

Результати SWOT-аналізу підтверджують, що АТ «УНІВЕРСАЛ БАНК» має достатньо ефективну систему управління інформаційною безпекою, яка відповідає сучасним вимогам цифрового банкінгу. Водночас виявлені слабкі сторони та зовнішні загрози свідчать про необхідність подальшого розвитку системи кіберзахисту, що стане предметом більш детального дослідження у наступних підрозділах роботи.

Важливим інструментом оцінки конкурентоспроможності та ефективності системи управління АТ «УНІВЕРСАЛ БАНК» є комплексний бенчмаркінг, який дозволяє порівняти ключові фінансово-економічні, структурні та кадрові показники установи з провідними учасниками вітчизняного банківського ринку. Для проведення порівняльного аналізу було обрано ключових конкурентів та лідерів сектору: ПриватБанк, Ощадбанк, Райффайзен Банк, ПУМБ, Sense Bank та UKRSIBBANK BNP Paribas Group.

Таблиця 2.9. Комплексний бенчмаркінг АТ «УНІВЕРСАЛ БАНК» та його основних конкурентів на ринку України

Критерій	Universal Bank	UKRSIBBANK BNP Paribas Group	Sense Bank	Ощадбанк	Райффайзен Банк	ПУМБ	ПриватБанк
Технічні спеціалісти	105	250	550	624	763	901	2 395
Працівники в IT-підрозділах	105	400	555	624	863	901	2 395
Співробітники в Україні	2 984	4 300	4 444	16 193	5 461	7 200	17 255
Список 10 надійних банків для фізичних осіб	Топ 9	Топ 5	-	Топ 2	-	-	Топ 1
Банки що діють в Україні	Так	Так/є дочірній банк в росії	Так	Так	Так/є дочірній банк в росії	Так	Так
Депозити фізичних осіб	44 659 365 тис.грн	-	46 258 820 тис.грн	128 798 695 тис.грн	53 717 596 тис.грн	-	290 030 221 тис.грн
Кредити фізособам	25 322 664 тис.грн	-	-	17 744 422 тис.грн	-	22 257 611 тис.грн	73 596 983 тис.грн
Величина активів	213 356 583 тис.грн	107 135 38 тис. грн	110 191 450 тис. грн	271 908 631 тис.грн	108 513 066 тис.грн	203 200 000 тис. грн	572 448 057 тис.грн
Кількість клієнтів	10 мільйонів	2 мільйони	3 мільйони	20 мільйонів	3 мільйони	2 мільйони	19 мільйонів

Примітка. Авторська розробка.

Такий вибір фінансових установ обумовлений необхідністю зіставлення показників банку як з потужними державними конгломератами, так і з провідними приватними та іноземними банківськими групами, що задають тренди в українському фінансовому просторі.

Результати зведеного аналізу свідчать про те, що АТ «УНІВЕРСАЛ БАНК» має яскраво виражену специфіку бізнес-моделі, орієнтовану на цифровий роздрібний банкінг. На відміну від класичних системних банків із розгалуженими мережами та величезним штатом, досліджувана установа демонструє високу концентрацію ресурсів у сегменті обслуговування фізичних осіб.

Особливої уваги заслуговує порівняння кадрового IT-потенціалу та масштабів інфраструктури. За чисельністю технічних спеціалістів та працівників в IT-підрозділах АТ «УНІВЕРСАЛ БАНК» наразі замикає вибірку із показником 105 осіб. Для порівняння: лідер ринку ПриватБанк акумулює 2 395 IT-фахівців, а найближчі конкуренти у приватному та іноземному сегментах, такі як Sense Bank та UKRSIBBANK, мають у штаті 550 та 250–400 профільних спеціалістів відповідно. За загальною чисельністю співробітників в Україні 2 984 особи АТ «УНІВЕРСАЛ БАНК» також є компактним за інші великі установи, наприклад, Ощадбанк має понад 16 тис. працівників, а ПриватБанк — понад 17 тис. Проте така лаконічність штату компенсується над високим рівнем цифровізації процесів [30].

Попри відносно невеликі загальні активи 213 356 583 тис. грн, що поступаються ПриватБанку 572 448 057 тис. грн та Ощадбанку 271 908 631 тис. грн, АТ «УНІВЕРСАЛ БАНК» посідає лідируючі позиції у ключових роздрібних напрямках завдяки успішній реалізації проєкту monobank. Зокрема, у сфері кредитування фізичних осіб банк міцно утримує 3-тє місце на ринку з обсягом 25 322 664 тис. грн, поступаючись лише ПриватБанку та Sense Bank. За обсягом залучених депозитів фізичних осіб банк входить до ТОП-5 в Україні 44 659 365 тис. грн, випереджаючи значну частину великих банківських груп. Крім того, банк офіційно зафіксовано на 9-му місці у списку 10 найнадійніших банків

для фізичних осіб, що є високим показником для фінустанови з приватним капіталом [31].

За критерієм кількості клієнтів АТ «УНІВЕРСАЛ БАНК» посідає впевнене третє місце на ринку з показником 10 мільйонів осіб, поступаючись лише традиційним державним гігантам — Ощадбанку 20 млн та ПриватБанку 19 млн. Водночас фінтех-модель банку дозволила йому суттєво випередити інших сильних конкурентів, таких як Sense Bank і Райффайзен Банк по 3 млн, а також UKRSIBBANK та ПУМБ по 2 млн, що підтверджує надвисоку ефективність та привабливість його цифрового продукту для українських користувачів.

Також бенчмаркінг виявив геополітичні переваги АТ «УНІВЕРСАЛ БАНК» перед деякими міжнародними групами. На відміну від Райффайзен Банку та UKRSIBBANK, які досі мають юридичні чи операційні зв'язки через дочірні структури в РФ, АТ «УНІВЕРСАЛ БАНК» діє виключно в правовому полі України та вільний від подібних репутаційних і санкційних ризиків третіх сторін.

Разом з тим, спроба провести поглиблений порівняльний аналіз зазначених установ безпосередньо у сфері кібербезпеки та детальних механізмів захисту інформації зіткнулася з об'єктивними обмеженнями. Пряме зіставлення банків за цим вектором виявилося неможливим через високу конфіденційність інформації, яка становить банківську та комерційну таємницю, а також через повну відсутність детальних технічних даних про архітектуру кіберзахисту у відкритих джерелах. Більше того, базові практичні інструменти захисту, такі як багатофакторна автентифікація, шифрування даних, моніторинг транзакцій та антивірусні комплекси, є стандартизованими й уніфікованими вимогами Національного банку України, які однаковою мірою впроваджені в усіх системно важливих фінустановах. Відповідно, через схожість нормативних практик безпеки та високий рівень закритості внутрішніх систем моніторингу, детальний бенчмаркінг технологічних систем кіберзахисту було замінено на аналіз кадрового IT-потенціалу та загальних масштабів

діяльності, що відображені у звітності банків.

Висновки до розділу 2

1. У підрозділі 2.1 проведено аналіз організаційно-економічної характеристики АТ «УНІВЕРСАЛ БАНК». Встановлено, що банк є однією з провідних фінансових установ України та активно розвиває цифрову модель обслуговування через проєкт monobank. Дослідження організаційної структури показало наявність чіткого розподілу управлінських функцій між Наглядовою радою, Правлінням, IT-підрозділами, службою інформаційної безпеки та ризик-менеджментом. Результати PESTLE-аналізу засвідчили, що найбільший вплив на діяльність банку мають технологічні, соціальні, юридичні та політичні фактори, що обумовлює необхідність постійного розвитку цифрової інфраструктури та системи захисту інформаційних ресурсів.

2. У підрозділі 2.2 здійснено діагностику фінансово-господарської діяльності АТ «УНІВЕРСАЛ БАНК» за 2022–2025 роки. Встановлено стійку тенденцію до зростання активів, зобов’язань, власного капіталу, чистого прибутку та сукупного доходу банку. Розраховані показники рентабельності активів і власного капіталу свідчать про підвищення ефективності використання фінансових ресурсів, а покращення коефіцієнтів фінансової стійкості та фінансової залежності підтверджує зміцнення фінансового стану установи. Отримані результати характеризують банк як фінансово стабільну та конкурентоспроможну установу, що має достатній ресурсний потенціал для подальшого розвитку цифрових сервісів і системи інформаційної безпеки.

3. У підрозділі 2.3 проведено оцінку системи управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК». Визначено, що система інформаційної безпеки базується на комплексному використанні організаційних, технічних та програмних засобів захисту, зокрема стандарту PCI DSS, протоколів TLS, багатофакторної та біометричної автентифікації, anti-fraud систем і механізмів моніторингу транзакцій. Аналіз організаційного та функціонального

забезпечення підтвердив ефективну взаємодію ІТ-підрозділів, служби інформаційної безпеки та ризик-менеджменту. За результатами SWOT-аналізу було обрано СМ-стратегію, додавання результатів бенчмаркінгу для аналізу дозволяє виявити окремі проблеми, пов’язані з високою залежністю від цифрових каналів обслуговування, значними витратами на кіберзахист, впливом людського фактора та необхідністю подальшого розвитку механізмів моніторингу й реагування на кіберзагрози. Виявлені недоліки формують основу для розробки заходів щодо вдосконалення системи управління інформаційною безпекою банку у третьому розділі роботи.

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БІЗНЕС-ПРОЦЕСІВ

3.1. Визначення загальної концепції подальшого розвитку інформаційної безпеки бізнес-процесів у цифровому середовищі

Проведене дослідження системи управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК» дозволило встановити, що банк забезпечує високий рівень захисту інформаційних ресурсів та активно впроваджує сучасні цифрові технології у процес обслуговування клієнтів. Результати аналізу організаційного, функціонального та інформаційного забезпечення системи інформаційної безпеки, а також проведений SWOT-аналіз і бенчмаркінг із провідними фінансовими установами підтвердили відповідність системи захисту актуальним вимогам банківського сектору. Водночас динамічний розвиток цифрового середовища та постійне зростання кількості кіберзагроз вимагають подальшого вдосконалення існуючої системи управління інформаційною безпекою.

Однією з ключових проблем сучасного цифрового середовища є постійне збільшення кількості та складності кіберзагроз. Якщо раніше основними ризиками були традиційні віруси та спроби несанкціонованого доступу, то сьогодні кіберзлочинці активно використовують штучний інтелект для автоматизації атак, створення адаптивного шкідливого програмного забезпечення та проведення складних атак соціальної інженерії. Особливу небезпеку становлять технології дипфейків, автоматизований підбір паролів, фішингові кампанії нового покоління та атаки на ланцюги постачання програмного забезпечення.

Не менш важливою проблемою залишається людський фактор. Незважаючи на високий рівень технічного захисту, значна частина кіберінцидентів виникає саме через помилки працівників, використання

слабких паролів, нехтування вимогами політики безпеки або недостатню обізнаність щодо сучасних кіберзагроз. У цифровому банкінгу людський фактор може стати причиною витоку конфіденційної інформації, компрометації облікових записів або несанкціонованого доступу до інформаційних ресурсів.

Проведений аналіз також показав необхідність подальшого розвитку концепції Zero Trust. В умовах активного використання мобільних додатків, хмарних сервісів та віддаленого доступу класичні моделі захисту периметра мережі поступово втрачають свою ефективність. Саме тому сучасна система інформаційної безпеки повинна базуватися на принципі постійної перевірки кожного користувача, пристрою та цифрового ресурсу незалежно від їхнього місцезнаходження.

Окремої уваги потребує розширення використання технологій штучного інтелекту для моніторингу кіберзагроз. Незважаючи на наявність сучасних систем виявлення інцидентів, швидкість розвитку нових видів атак вимагає переходу до проактивних методів захисту, які дозволяють прогнозувати ризики та виявляти аномальну активність ще до виникнення критичних наслідків.

Крім того, актуальним напрямом розвитку є посилення захисту хмарної інфраструктури. Банківський сектор дедалі активніше використовує хмарні сервіси для забезпечення гнучкості бізнес-процесів, резервного копіювання даних та підтримки цифрових сервісів. Разом із перевагами використання хмарних технологій виникають додаткові ризики, пов'язані з несанкціонованим доступом до даних, компрометацією облікових записів та залежністю від сторонніх провайдерів.

Суттєвим викликом залишається також необхідність удосконалення системи управління ризиками постачальників. Використання сторонніх програмних продуктів, хмарних платформ та сервісів створює додаткові точки потенційного проникнення в інформаційну інфраструктуру банку. Саме тому ефективна система кібербезпеки повинна охоплювати не лише внутрішні процеси організації, а й контролювати безпеку зовнішніх партнерів та постачальників цифрових послуг.

З урахуванням виявлених проблем доцільно запропонувати «Концепцію проактивного управління інформаційною безпекою бізнес-процесів АТ «УНІВЕРСАЛ БАНК»». Основною метою запропонованої концепції є забезпечення стійкості банку до сучасних кіберзагроз, підвищення рівня захисту клієнтських даних, мінімізація кіберризиків та забезпечення безперервності бізнес-процесів у цифровому середовищі.

На відміну від традиційного підходу, який орієнтується переважно на реагування після виникнення інцидентів, запропонована концепція передбачає реалізацію проактивної моделі захисту. Її сутність полягає у постійному моніторингу цифрового середовища, прогнозуванні потенційних ризиків, своєчасному виявленні аномалій та автоматизованому реагуванні на загрози ще до моменту їхнього негативного впливу на діяльність банку.

Визначено основні стратегічні напрями розвитку системи інформаційної безпеки АТ «УНІВЕРСАЛ БАНК», які наведено у таблиці 3.1.

Таблиця 3.1. Стратегічні напрями розвитку системи інформаційної безпеки

Напрям	Очікуваний результат
Розвиток архітектури Zero Trust • Впровадження суворої автентифікації (MFA/2FA) • Мікросегментація мережі для обмеження руху зловмисника всередині периметру • Постійна верифікація кожного пристрою та користувача (IAM/PAM).	Мінімізація ризику несанкціонованого доступу • Зниження ймовірності горизонтального переміщення (Lateral Movement) зловмисника на 90%. • Повний контроль та видимість усіх сесій у реальному часі. • Захист критичних даних навіть у разі компрометації одного з облікових записів.
AI-моніторинг та аналітика загроз • Інтеграція алгоритмів машинного навчання в системи безпеки. • Автоматичний аналіз аномалій у поведінці користувачів та систем (UEBA) • Використання прогнозної аналітики для виявлення загрози до моменту активної фази атаки.	Радикальне прискорення виявлення атак • Скорочення часу виявлення інцидентів (Mean Time to Detect — MTTD) з кількох днів/тижнів до кількох хвилин. • Автоматичне відсікання до 95% хибнопозитивних спрацьовувань, що розвантажує аналітиків.
Модернізація та розвиток SOC • Перехід на модель SOC 2.0 із залученням платформ автоматизації та реагування (SOAR). • Цілодобовий моніторинг (24/7/365) критичної інфраструктури. • Створення чітких сценаріїв реагування на типові інциденти.	Оптимізація та автоматизація реагування на інциденти • Зменшення часу ліквідації наслідків (Mean Time to Remediate — MTTR) у 4-5 разів. • Локалізація кібератак на ранніх стадіях, що мінімізує фінансові та репутаційні збитки для компанії.

Продовження Табл. 3.1.

Напрям	Очікуваний результат
Навчання персоналу • Проведення регулярних симуляцій фішингових атак. • Обов'язкові інтерактивні тренінги з кібергігієни для нових та діючих співробітників. • Тестування знань щодо поводження з конфіденційною інформацією.	Зниження впливу людського фактора • Зменшення кількості успішних фішингових атак на співробітників компанії на 70-80%. • Трансформація персоналу з "слабкої ланки" на перший рубіж оборони (створення культури безпеки).
Контроль безпеки підрядників та партнерів (Third-Party Risk Management) • Впровадження обов'язкового аудиту безпеки для всіх підрядників та SaaS-сервісів. • Включення жорстких вимог щодо кібербезпеки в договори (SLA/NDA). • Моніторинг захищеності партнерів через автоматизовані платформи оцінки ризиків.	Посилення безпеки ланцюга постачання (Supply Chain) • Унеможливлення загрози проникнення в корпоративну мережу через компрометацію сторонніх вендорів. • Чітке юридичне та технічне розмежування зон відповідальності за збереження даних.
Комплексний захист хмарної інфраструктури • Впровадження рішень класу CNAPP (Cloud-Native Application Protection Platform). • Шифрування даних як під час передачі, так і у стані спокою.. • Регулярний аудит конфігурацій хмарних середовищ.	Максимізація стійкості цифрових сервісів • Забезпечення безперервності бізнес-процесів (Uptime сервісів на рівні 99.99%). • Швидке відновлення систем із захищених резервних копій у разі масштабного збою чи атаки.

Примітка. Авторська розробка.

Першим стратегічним напрямом є впровадження та подальший розвиток архітектури Zero Trust. Запровадження даного підходу передбачає розгортання суворої багатофакторної автентифікації MFA/2FA, мікросегментації мережі для обмеження руху зловмисника всередині периметру, а також постійну верифікацію кожного пристрою та користувача IAM/PAM [32]. У результаті очікується радикальне зниження ризику несанкціонованого доступу, зокрема зменшення ймовірності горизонтального переміщення зловмисника на 90%, забезпечення повного контролю сесій у реальному часі та надійний захист критичних даних навіть у разі компрометації окремого облікового запису [33].

Другим напрямом є інтеграція AI-моніторингу та аналітики загроз. Використання алгоритмів машинного навчання, автоматичного аналізу аномалій у поведінці користувачів та систем UEBA, а також прогнозної аналітики дозволить виявляти загрози до моменту настання активної фази атаки [34]. Це забезпечить радикальне прискорення виявлення атак: скорочення часу виявлення інцидентів MTTD з кількох днів або тижнів до кількох хвилин, а

також автоматичне відсікання до 95% хибнопозитивних спрацьовувань, що суттєво розвантажить аналітиків [35].

Третім напрямом визначено модернізацію та розвиток SOC. Трансформація передбачає перехід на модель SOC 2.0 із залученням платформ автоматизації та реагування, забезпечення цілодобового моніторингу критичної інфраструктури та впровадження чітких сценаріїв реагування. Очікуваним результатом є оптимізація та автоматизація реагування на інциденти, що дозволить зменшити час ліквідації наслідків у 4–5 разів і забезпечить локалізацію кібератак на ранніх стадіях для мінімізації фінансових та репутаційних збитків [36].

Наступним стратегічним напрямом є систематичне навчання персоналу. Проведення регулярних симуляцій фішингових атак, обов'язкових інтерактивних тренінгів з кібергігієни та тестування знань щодо поводження з конфіденційною інформацією дозволить досягти суттєвого зниження ризику людського фактора. Зокрема, очікується зменшення кількості успішних фішингових атак на співробітників на 70–80% та формування стійкої внутрішньої культури кібербезпеки в організації [37].

Важливим напрямом виступає управління ризиками постачальників. Для реалізації цього вектора впроваджується обов'язковий аудит безпеки для всіх підрядників та SaaS-сервісів, включення жорстких вимог щодо кібербезпеки в договори, а також безперервний моніторинг захищеності партнерів через автоматизовані платформи оцінки ризиків [38]. Це гарантує посилення безпеки ланцюга постачання та унеможливлює проникнення в корпоративну мережу банку через компрометацію сторонніх вендорів [39].

Останнім стратегічним напрямом є комплексний захист хмарної інфраструктури. Він передбачає використання спеціалізованих рішень класу CNAPP та CSPM, тотального шифрування даних як під час передачі, так і у стані спокою, а також регулярний аудит конфігурацій хмарних середовищ [40]. Результатом стане максимальне підвищення стійкості цифрових сервісів, забезпечення безперервності бізнес-процесів та можливість миттєвого

відновлення систем із захищених резервних копій у разі збою чи атаки.

Для візуалізації запропонованого підходу доцільно представити модель концепції проактивного управління інформаційною безпекою бізнес-процесів АТ «УНІВЕРСАЛ БАНК» (рис. 3.1).

Рисунок 3.1 – Модель концепції проактивного управління інформаційною безпекою бізнес-процесів АТ «УНІВЕРСАЛ БАНК»

Примітка. Авторська розробка.

Наукова новизна запропонованого підходу полягає у формуванні комплексної концепції управління інформаційною безпекою бізнес-процесів банку, яка технологічно та процесно поєднує принципи Zero Trust, технології штучного інтелекту, модернізований інструментарій SOC, ризик-орієнтований підхід NIST Cybersecurity Framework та безперервний моніторинг хмарного середовища. На відміну від традиційних моделей захисту, запропонована концепція орієнтована на випереджальне виявлення загроз, автоматизацію реагування та адаптацію системи безпеки до нових викликів цифрового середовища з чітко вимірюваними KPI.

Таким чином, запропонована концепція проактивного управління інформаційною безпекою створює основу для подальшого вдосконалення системи кіберзахисту АТ «УНІВЕРСАЛ БАНК». Її реалізація дозволить підвищити рівень захисту інформаційних ресурсів, забезпечити стійкість до сучасних кіберзагроз та створити умови для безпечного розвитку цифрових банківських сервісів у довгостроковій перспективі.

3.2. Розробка комплексного забезпечення системи управління інформаційною безпекою бізнес-процесів у цифровому середовищі

Ефективність системи інформаційної безпеки значною мірою залежить не лише від рівня технологічного оснащення підприємства, а й від належної організації процесів управління кібербезпекою. В умовах цифровізації банківської діяльності та постійного зростання кількості кіберзагроз особливого значення набуває побудова чіткої організаційної структури, яка забезпечує розподіл відповідальності між усіма учасниками процесу управління інформаційною безпекою.

З урахуванням сучасних вимог до кіберстійкості банківських установ та високого рівня цифровізації АТ «УНІВЕРСАЛ БАНК» доцільним є вдосконалення організаційної структури управління інформаційною безпекою на основі підходу трьох ліній захисту. Така модель дозволяє чітко розмежувати відповідальність між рівнями управління, підвищити прозорість процесів контролю та забезпечити більш ефективне управління кіберризиками в межах цифрових бізнес-процесів, включаючи дистанційні канали обслуговування та мобільний застосунок monobank.

На першому рівні захисту доцільно визначити бізнес-підрозділи та IT-служби банку, які безпосередньо здійснюють експлуатацію інформаційних систем, впровадження цифрових сервісів і забезпечення безперервності їх функціонування. У межах цієї лінії відповідальність полягає у дотриманні базових вимог інформаційної безпеки під час розробки, впровадження та використання систем, а також у своєчасному виявленні та первинному реагуванні на потенційні загрози. Важливо підкреслити, що саме цей рівень є найбільш наближеним до операційних процесів, однак водночас і найбільш вразливим до впливу людського фактора та помилок конфігурації.

Другий рівень захисту формується службою інформаційної безпеки та підрозділами управління ризиками, які здійснюють функції контролю, моніторингу та методологічного супроводу. У контексті АТ «УНІВЕРСАЛ

БАНК» ця лінія вже представлена відповідними функціональними структурами, однак потребує посилення координаційної ролі. Основними завданнями цього рівня є формування політик інформаційної безпеки, управління кіберризиками, контроль дотримання нормативних вимог Національного банку України, а також організація заходів із запобігання кіберінцидентам. Саме на цьому рівні відбувається узгодження вимог безпеки з бізнес-цілями банку, що є критично важливим для стабільного функціонування цифрової екосистеми.

Третій рівень захисту представлений внутрішнім аудитом, який виконує незалежну оцінку ефективності системи управління інформаційною безпекою. Його функція полягає у перевірці дотримання внутрішніх політик, оцінці адекватності впроваджених контрольних механізмів, а також у виявленні системних недоліків, які можуть бути неочевидними для операційних або контрольних підрозділів. Такий підхід забезпечує об’єктивність оцінки та дозволяє формувати стратегічні рекомендації щодо вдосконалення системи захисту.

Важливою проблемою чинної моделі управління інформаційною безпекою є певна розрізненість взаємодії між IT-підрозділами, службою інформаційної безпеки та ризик-менеджментом. Це може проявлятися у дублюванні контрольних функцій, недостатньо швидкому обміні інформацією про кіберзагрози та ускладненій координації дій під час реагування на інциденти. У результаті знижується загальна оперативність прийняття управлінських рішень у сфері кіберзахисту, що є критичним для банківської установи з високим рівнем цифрової інтеграції.

Для усунення зазначених недоліків пропонується посилити координаційну складову організаційної структури шляхом створення єдиного органу управління кіберризиками. Такий орган може функціонувати як міжфункціональна платформа взаємодії між IT, службою інформаційної безпеки, ризик-менеджментом та представниками бізнес-напрямів. Його основними завданнями мають стати узгодження стратегічних рішень у сфері кібербезпеки, пріоритизація ризиків, контроль реалізації захисних заходів та

підвищення швидкості реагування на інциденти.

Запропонована модель дозволяє трансформувати систему управління інформаційною безпекою з фрагментованої структури в інтегровану систему управління ризиками, в якій кожен рівень має чітко визначені функції та зони відповідальності. Це забезпечує не лише підвищення ефективності контролю, а й більш глибоку інтеграцію інформаційної безпеки в загальну систему корпоративного управління банку.

Ефективність системи управління інформаційною безпекою в сучасному цифровому банку визначається не лише її організаційною структурою, але й рівнем розвитку функціонального, методичного та інформаційного забезпечення. У цьому контексті для АТ «УНІВЕРСАЛ БАНК» доцільно запропонувати комплекс заходів, спрямованих на підвищення автоматизації процесів кіберзахисту, формалізацію внутрішніх процедур та створення єдиного інформаційного середовища для управління ризиками та інцидентами.

Ключовим напрямом удосконалення функціонального забезпечення є посилення можливостей оперативного моніторингу та реагування на кіберзагрози шляхом розвитку SOC. Впровадження або розширення SOC дозволить забезпечити централізоване спостереження за подіями інформаційної безпеки в режимі реального часу, а також координацію дій під час інцидентів. Це особливо важливо для банківських установ із високим рівнем цифровізації, де навіть короткочасні збої можуть мати суттєвий вплив на клієнтський сервіс.

Додатково доцільним є активне використання SIEM- та SOAR-систем, які забезпечують автоматизований збір, кореляцію та аналіз подій безпеки, а також автоматизацію реагування на типові інциденти. Це дозволяє суттєво скоротити час виявлення загроз і мінімізувати вплив людського фактора. Важливим елементом також є автоматизація процесів управління інцидентами, що включає їх реєстрацію, класифікацію, розподіл відповідальності та контроль виконання заходів реагування.

Окрему увагу слід приділити регулярному аудиту прав доступу та контролю привілеїв користувачів інформаційних систем. Такий підхід дозволяє

зменшити ризики несанкціонованого доступу та забезпечити принцип мінімально необхідних прав. Крім того, управління кіберризиками має розглядатися як безперервний процес, інтегрований у всі етапи життєвого циклу інформаційних систем — від їх розробки до експлуатації та модернізації.

Важливою складовою розвитку системи інформаційної безпеки є оновлення та гармонізація внутрішньої нормативної бази банку. У першу чергу це стосується актуалізації політики інформаційної безпеки з урахуванням сучасних кіберзагроз, вимог Національного банку України та міжнародного стандарту ISO/IEC 27001. Такий підхід дозволяє забезпечити відповідність системи управління безпекою міжнародним практикам та регуляторним вимогам.

До переліку ключових методичних документів доцільно включити політику управління кіберризиками, інструкції з реагування на інциденти інформаційної безпеки, регламенти управління доступом до інформаційних систем, а також методики оцінювання та класифікації вразливостей. Наявність таких документів забезпечує формалізацію процесів та зменшує залежність від індивідуальних рішень співробітників.

Окремим напрямом є стандартизація процесів інформаційної безпеки, що передбачає уніфікацію процедур виявлення, аналізу та усунення загроз. Це дозволяє забезпечити повторюваність та контрольованість усіх ключових процесів у сфері кіберзахисту, а також підвищити рівень їх прозорості для управлінських рівнів банку.

Інформаційне забезпечення системи управління інформаційною безпекою відіграє ключову роль у забезпеченні її керованості та прозорості. У цьому контексті доцільним є впровадження єдиної системи моніторингу ключових показників ефективності та ризику, яка дозволить у режимі реального часу оцінювати стан кібербезпеки та ефективність впроваджених заходів захисту.

Важливим елементом є створення централізованого реєстру IT-активів, який забезпечує повну інвентаризацію інформаційних ресурсів банку та дозволить встановити зв’язок між активами, загрозами та заходами контролю.

Паралельно доцільно впровадити реєстр кіберризиків, який забезпечить систематизацію інформації про потенційні загрози, їх ймовірність та рівень впливу.

Додатково необхідним є формування централізованої аналітичної системи інцидентів, яка забезпечуватиме накопичення, аналіз та візуалізацію даних про кіберінциденти. На основі таких даних доцільно створити управлінські дашборди для керівництва банку, що дозволить оперативно приймати обґрунтовані рішення у сфері інформаційної безпеки.

Таким чином, розвиток функціонального, методичного та інформаційного забезпечення дозволяє перейти від формальної наявності системи інформаційної безпеки до її повноцінного практичного функціонування як автоматизованої, стандартизованої та вимірюваної системи управління кіберризиками.

Висновки до розділу 3

1. У підрозділі 3.1 розроблено концепцію проактивного управління інформаційною безпекою бізнес-процесів АТ «УНІВЕРСАЛ БАНК» з урахуванням результатів проведеного аналізу та сучасних тенденцій розвитку цифрового банкінгу. Визначено ключові проблеми функціонування системи інформаційної безпеки, серед яких зростання складності кіберзагроз, вплив людського фактора, необхідність розвитку архітектури Zero Trust, посилення захисту хмарної інфраструктури та управління ризиками постачальників. Запропонована концепція базується на принципах проактивного кіберзахисту та передбачає реалізацію стратегічних напрямів розвитку, зокрема впровадження Zero Trust, AI-моніторингу, модернізації SOC, навчання персоналу, контролю безпеки партнерів і комплексного захисту хмарних середовищ. Реалізація концепції сприятиме підвищенню кіберстійкості банку, зменшенню кіберризиків та забезпеченню безперервності цифрових бізнес-процесів.

2. У підрозділі 3.2 розроблено комплексне організаційне, функціональне, методичне та інформаційне забезпечення системи управління інформаційною безпекою АТ «УНІВЕРСАЛ БАНК». Запропоновано вдосконалення організаційної структури на основі моделі трьох ліній захисту та створення єдиного органу координації управління кіберризиками. Обґрунтовано доцільність розвитку SOC, впровадження SIEM- та SOAR-систем, автоматизації управління інцидентами, регулярного аудиту доступу та посилення управління кіберризиками. Також запропоновано актуалізацію внутрішньої нормативної бази відповідно до вимог ISO/IEC 27001 та НБУ, впровадження реєстру IT-активів, реєстру кіберризиків, централізованої аналітичної системи інцидентів і управлінських дашбордів. Запропоновані заходи дозволять підвищити ефективність управління інформаційною безпекою, забезпечити прозорість процесів кіберзахисту, скоротити час реагування на інциденти та зміцнити загальний рівень кіберстійкості банку.

ВИСНОВКИ

У результаті проведеного дослідження досягнуто поставленої мети кваліфікаційної роботи, яка полягала в обґрунтуванні теоретичних положень та розробці практичних рекомендацій щодо вдосконалення системи управління інформаційною безпекою бізнес-процесів у цифровому середовищі на прикладі АТ «УНІВЕРСАЛ БАНК». Отримані результати дозволяють сформулювати такі висновки:

1. Досліджено сутність інформаційної безпеки бізнес-процесів та її роль у діяльності цифрових підприємств. Встановлено, що в умовах цифрової трансформації інформація є одним із ключових стратегічних ресурсів організації, а ефективне управління її захистом виступає необхідною умовою забезпечення стабільності бізнес-процесів, підтримання довіри клієнтів та конкурентоспроможності підприємства. Для цифрових банків інформаційна безпека є основою безперервності діяльності, оскільки порушення конфіденційності, цілісності або доступності інформації здатні спричинити значні фінансові та репутаційні втрати.
2. Розглянуто класифікацію, види та основні характеристики систем управління інформаційною безпекою. Визначено, що сучасна система управління інформаційною безпекою являє собою комплекс взаємопов’язаних організаційних, технічних, програмних, економічних та правових заходів, спрямованих на забезпечення захисту інформаційних ресурсів. Узагальнення наукових підходів дозволило класифікувати системи захисту за напрямами забезпечення мережевої безпеки, захисту кінцевих пристроїв, хмарної інфраструктури та цифрових сервісів, що забезпечує реалізацію принципів конфіденційності, цілісності та доступності інформації.
3. Проаналізовано вітчизняний і світовий досвід розвитку систем управління інформаційною безпекою. Встановлено, що сучасні тенденції

розвитку кібербезпеки характеризуються переходом від реактивних моделей захисту до проактивних концепцій кіберстійкості. Визначено, що провідні міжнародні практики базуються на використанні стандартів ISO/IEC 27001, NIST Cybersecurity Framework, концепції Zero Trust, центрів моніторингу безпеки (SOC), технологій штучного інтелекту та автоматизації процесів реагування на кіберінциденти. Це підтверджує необхідність постійного вдосконалення систем захисту в умовах зростання кількості та складності кіберзагроз.

4. Надано організаційно-економічну характеристику діяльності АТ «УНІВЕРСАЛ БАНК». Встановлено, що банк є однією з провідних фінансових установ України та успішно реалізує цифрову бізнес-модель через проєкт monobank. Проведений PESTLE-аналіз показав значний вплив технологічних, соціальних, політичних і правових факторів на діяльність банку. Високий рівень цифровізації бізнес-процесів та значна клієнтська база обумовлюють підвищені вимоги до забезпечення інформаційної безпеки та кіберстійкості установи.
5. Проведено діагностику показників фінансово-господарської діяльності АТ «УНІВЕРСАЛ БАНК». Результати аналізу за 2022–2025 роки свідчать про стійке зростання активів, власного капіталу, доходів та чистого прибутку банку. Показники рентабельності активів і власного капіталу демонструють високу ефективність використання ресурсів, а позитивна динаміка фінансової стійкості підтверджує здатність банку забезпечувати подальший розвиток цифрових сервісів та фінансувати впровадження сучасних технологій інформаційної безпеки.
6. Оцінено сучасний стан системи управління інформаційною безпекою в АТ «УНІВЕРСАЛ БАНК». Встановлено, що система інформаційної безпеки банку відповідає сучасним вимогам цифрового банкінгу та включає використання стандарту PCI DSS, протоколів TLS, багатофакторної та біометричної автентифікації, anti-fraud систем і механізмів моніторингу транзакцій. Проведені SWOT-аналіз і

бенчмаркінг дозволили виявити низку проблемних аспектів, зокрема вплив людського фактора, високу залежність від цифрових каналів обслуговування, необхідність посилення координації між IT-підрозділами, службою інформаційної безпеки та ризик-менеджментом, а також потребу у подальшому розвитку інструментів моніторингу кіберзагроз.

7. Визначено концептуальні напрями подальшого розвитку системи інформаційної безпеки бізнес-процесів у цифровому середовищі. Запропоновано концепцію проактивного управління інформаційною безпекою, яка передбачає впровадження архітектури Zero Trust, використання AI-моніторингу та прогнозної аналітики загроз, модернізацію SOC, посилення захисту хмарної інфраструктури, управління ризиками постачальників та розвиток культури кібербезпеки серед персоналу. Реалізація зазначених напрямів забезпечить підвищення кіберстійкості банку та зниження рівня інформаційних ризиків.
8. Розроблено комплексні рекомендації щодо вдосконалення системи управління інформаційною безпекою бізнес-процесів АТ «УНІВЕРСАЛ БАНК». Запропоновано удосконалення організаційного забезпечення на основі моделі трьох ліній захисту та створення міжфункціонального органу управління кіберризиками. Обґрунтовано доцільність розвитку SOC, впровадження SIEM- та SOAR-систем, автоматизації процесів реагування на інциденти, актуалізації внутрішньої нормативної бази відповідно до ISO/IEC 27001, формування реєстрів IT-активів і кіберризиків, а також створення централізованої аналітичної системи моніторингу кіберінцидентів. Реалізація запропонованих заходів дозволить підвищити ефективність управління інформаційною безпекою, скоротити час реагування на кіберзагрози, мінімізувати потенційні збитки від кібератак та забезпечити безпечний розвиток цифрових банківських сервісів у довгостроковій перспективі.

СПИСКИ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Global Cyber Attacks Surge 21% in Q2 2025 — Europe Experiences the Highest Increase of All Regions. URL: https://blog.checkpoint.com/research/global-cyber-attacks-surge-21-in-q2-2025-europe-experiences-the-highest-increase-of-all-regions/ (дата звернення 09.05.2026)
2. *Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21.*
3. cybersecurity. URL: https://csrc.nist.gov/glossary/term/cybersecurity?ref=securityscientist.net#:~:text=The%20process%20of%20protecting%20information,NIST%20Cybersecurity%20Framework%20Version%201.1 (дата звернення 09.05.2026)
4. Інтеграція хмарних серверів із технологією API. URL: https://cases.media/en/article/integraciya-khmarnikh-serveriv-iz-tekhnologiyeyu-api?srsltid=AfmBOop8BB2RtpU6-FTt93Kd2dIIANuJpsdhiuHk324dPJTbZI_JZONt (дата звернення 09.05.2026)
5. 9 Key Cybersecurity Trends to Know in 2025 [New Data]. URL: https://www.pandasecurity.com/en/mediacenter/cybersecurity-trends/ (дата звернення 09.05.2026)
6. Cyber Security Management - The different types. URL: https://www.checkpoint.com/cyber-hub/cyber-security/cyber-security-management-the-different-types/ (дата звернення 10.05.2026)
7. What Is the CIA Triad? URL: https://www.fortinet.com/resources/cyberglossary/cia-triad (дата звернення 10.05.2026)
8. What is ISO 27001? URL: https://www.ibm.com/products/cloud/compliance/iso-27001 (дата звернення 10.05.2026)
9. What is the NIST Cybersecurity Framework? The Ultimate Guide. URL: https://bitwarden.com/resources/nist-cybersecurity-framework/ (дата

звернення 10.05.2026)
10. Zero trust architecture. URL: https://w.wiki/MzmZ (дата звернення 10.05.2026)
11. Security operations center. URL: https://w.wiki/FcAh (дата звернення 10.05.2026)
12. What is GDPR, the EU’s new data protection law? URL: https://gdpr.eu/what-is-gdpr/ (дата звернення 10.05.2026)
13. 12 Cybersecurity Best Practices & Measures to Prevent Cyber Attacks in 2026. URL: https://www.syteca.com/en/blog/best-cyber-security-practices (дата звернення 10.05.2026)
14. Cisco Zero Trust Architecture Guide. URL: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/zt-ag.html (дата звернення 10.05.2026)
15. IBM QRadar. URL: https://www.ibm.com/products/qradar (дата звернення 10.05.2026)
16. What is Oracle Cloud Security? URL: https://orca.security/resources/blog/what-is-oracle-cloud-security/ (дата звернення 10.05.2026)
17. How JPMorgan Chase Strengthened Security After Facing Cyber Threats. URL: https://www.sprintzeal.com/blog/jpmorgan-cybersecurity (дата звернення 10.05.2026)
18. Безпека. URL: https://monobank.ua/security (дата звернення 10.05.2026)
19. "ПриватБанк" нейтралізував 1,5 мільйона кібератак з початку війни, – голова правління Мікаель Бьоркнерт. URL: https://censor.net/biz/news/3602745/pryvatbank-neyitralizuvav-1-5-milyiona-kiberatak-z-pochatku-viyiny (дата звернення 10.05.2026)
20. Безпека мобільного застосунку Дія. URL: https://thedigital.gov.ua/news/technologies/bezpeka-mobilnogo-zastosunku-diya (дата звернення 10.05.2026)
21. НБУ системно працює над імплементацією DORA в фінансовому секторі та оновленням нормативно-правових актів щодо забезпечення інформаційної безпеки, кіберзахисту та цифрової операційної стійкості —

Антон Кудін. URL: https://aub.org.ua/nbu-systemno-praczyuye-nad-implementacziyeyu-dora-v-finansovomu-sektori-ta-onovlennyam-normatyvno-pravovyh-aktiv-shhodo-zabezpechennya-informaczijnoyi-bezpeky-kiberzahystu-ta-czyfrovoyi-operaczijnoyi/ (дата звернення 10.05.2026)

22. 6 тисяч кібератак проти України здійснили у 2025 році, на 37% більше ніж у попередньому. URL: https://ain.ua/2026/02/20/za-2025-rik-proti-ukrayini-zdiisnili-priblizno-6000-kiberatak/ (дата звернення 10.05.2026)
23. Універсал Банк. URL: https://w.wiki/QZpC (дата звернення 27.05.2026)
24. АТ «УНІВЕРСАЛ БАНК» підтвердило рейтинг uaAAA та найвищу надійність вкладів. URL: https://www.universalbank.com.ua/news/universal-bank-pidtverdylo-rejtynh-uaaaa-ta-najvyshchu-nadijnist-vkladiv (дата звернення 27.05.2026)
25. Про нас. URL: https://www.universalbank.com.ua/our-bank (дата звернення 27.05.2026)
26. monobank потрапив до рейтингу 250 найкращих фінтех-компаній світу від CNBC. URL: https://forbes.ua/news/monobank-potrapiv-do-reytingu-250-naykrashchikh-fintekh-kompaniy-svitu-vid-cnbc-12072024-22360 (дата звернення 27.05.2026)
27. Наглядова Рада. URL: https://www.universalbank.com.ua/supervisory-board (дата звернення 27.05.2026)
28. Правління та Головний бухгалтер. URL: https://www.universalbank.com.ua/top-management (дата звернення 27.05.2026)
29. Фінансова звітність. URL: https://www.universalbank.com.ua/financial-reports (дата звернення 28.05.2026)
30. Найбільші банки України за кількістю IT-спеціалістів 2025. Рейтинг DOU. URL: https://dou.ua/lenta/articles/bank-rating-2025/ (дата звернення 29.05.2026)
31. Рейтинг надійних банків України 2026 (квітень). URL:

https://forinsurer.com/rating-banks (даат звернення 29.05.2026)

32. Що таке багатофакторна автентифікація (MFA)? URL: https://www.protectimus.com/uk/what-is-multi-factor-authentication-mfa/ (дата звернення 05.06.2026)
33. Lateral Movement Explained. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/ (дата звернення 05.06.2026)
34. Що таке MTTR та як він відрізняється від інших показників управління інцидентами? URL: https://dynatrace.bakotech.com/ua/what-is-mttr (дата звернення 05.06.2026)
35. What is false positive in cybersecurity? What is false positive in cybersecurity? URL: https://www.contrastsecurity.com/glossary/false-positive (дата звернення 05.06.2026)
36. SOC vs SIEM vs SOAR — What Are the Differences and How Do They Work Together? URL: https://nflo.tech/knowledge-base/soc-vs-siem-vs-soar-differences/ (дата звернення 05.06.2026)
37. Security Awareness Training: What It Is and What It Should Include. URL: https://abnormal.ai/glossary/security-awareness-training (дата звернення 05.06.2026)
38. What is third-party risk management (TPRM)? URL: https://www.ibm.com/think/topics/third-party-risk-management (дата звернення 05.06.2026)
39. What Is Supply Chain in Cybersecurity? https://pointsolutions-security.com/what-is-supply-chain-in-cyber-security/ (дата звернення 05.06.2026)
40. CNAPP vs CSPM: What Role Does Each Play? URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cnapp-vs-cspm/ (дата звернення 05.06.2026)

ДОДАТКИ