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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління ризиками кібербезпеки в банківській сфері»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Яна МАРТИНЕНКО
(підпис)

Виконала: здобувач вищої освіти групи БСДМ-62
МАРТИНЕНКО Яна
(прізвище, ім'я)

Керівник д.т.н., професор ЗИБІН Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

КИЇВ-2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ — автоматизоване робоче місце

АБС — Автоматізована банківська система

АМКУ — Антимонопольний комітет України

БД — База даних

ДІС — Департамент інформаційних систем

ЗУ — Закон України

ІБ — Інформаційна безпека

ІС — Інформаційна система

ІТ — Інформаційна технологія

НБУ — Національний банк України

ОР — операційний ризик (кіберризик)

ПЗ — Програмне забезпечення

СУБД — Система управління базами даних

ЮУ — Юридичне управління

ACL — Access Control List

Anti-DDoS — Anti-Distributed Denial of Service

APT-атаки — Advanced Persistent Threat

APM — Application Performance Monitoring

CEH — Certified Ethical Hacker

CVSS — Common Vulnerability Scoring System

DAC — Discretionary Access Control, вибіркове керування доступом

DDoS — Distributed Denial of Service

DMZ — Demilitarized Zone

DLP — Data Loss Prevention

HACCP — Hazard Analysis and Critical Control Points

HAZOP — Hazard and Operability Study

HTTP — HyperText Transfer Protocol

IDS — Intrusion Detection System

IoC — Indicators of Compromise

IPS — Intrusion Prevention System

MFA — Multifactor Authentication, багатофакторна аутентифікація

NGFW — Next Generation Firewall, фаєрвол наступного покоління

OTP — One Time Password, одноразовий пароль

PCI DSS — Payment Card Industry Data Security Standard

RBAC — Role Based Access Control, ролева модель доступу

SIEM — Security Information and Event Management

SOC — Security Operations Center

SWIFT — Structured What-If Technique

UEBA — User and Entity Behavior Analytics

URL — Uniform Resource Locator

VLAN — Virtual Local Area Network

VPN — Virtual Private Network

WAF — Web Application Firewall

WAAP — Web Application and API Protection

XSS — Cross-Site Scripting

ВСТУП

Актуальність дослідження. У сучасному світі, де цифровізація банківських послуг стає все більш поширеною, питання захисту від кіберзагроз набувають критичного значення. Банки обробляють величезні обсяги чутливої інформації, здійснюють фінансові операції та забезпечують доступ до онлайн-сервісів, що робить їх привабливою мішенню для кіберзлочинців. У зв'язку з постійно зростаючими кіберризиками, ефективне управління цими загрозами є ключовим фактором забезпечення безпеки фінансових операцій і довіри клієнтів. Технології, що допомагають банкам своєчасно виявляти та нейтралізувати кіберзагрози, стають необхідними для підтримки стабільності та безперервності банківських послуг.

Актуальність дослідження ще більше підкреслюється зростанням складності та кількості кіберзагроз. Сьогодні банківські установи часто стикаються з новими типами атак, такими як фішинг, зловмисні програми, DDoS-атаки та інші форми кібер-шахрайства. Ці загрози не лише ставлять під загрозу безпеку фінансових транзакцій, але й можуть призвести до значних фінансових втрат, порушень репутації та довіри з боку клієнтів. З огляду на це, питання ефективного управління кіберризиками стає пріоритетом для всіх банківських установ, незалежно від їх розміру чи спеціалізації.

Управління кіберризиками в банківській сфері передбачає впровадження комплексних технологій для виявлення, аналізу та реагування на кіберзагрози. Однією з найважливіших складових є використання систем моніторингу та виявлення інцидентів безпеки (SIEM), які дозволяють здійснювати реальний моніторинг усіх операцій та подій в банківській інфраструктурі. Крім того, сучасні платформи для управління ідентифікацією та доступом (IAM) забезпечують захист від несанкціонованого доступу до банківських ресурсів, що є ключовим аспектом для безпеки клієнтських даних і самих фінансових операцій. Впровадження таких технологій дозволяє банкам знижувати ризики, пов'язані з кіберзагрозами, і швидко реагувати на інциденти безпеки.

Таким чином, дослідження технологій управління кіберризиками є надзвичайно актуальним, оскільки надає можливість банківським установам адаптувати свої стратегії безпеки до новітніх викликів та підвищувати рівень захисту. Враховуючи постійно змінювану природу кіберзагроз і розвиток нових методів атаки, важливо, щоб банки регулярно оновлювали свої підходи до управління кіберризиками та застосовували інноваційні технології для

ефективного захисту від кіберзлочинців. Вивчення та впровадження таких технологій дозволить забезпечити стабільність, безпеку та довіру до банківської сфери, що є критичним для розвитку економіки в умовах сучасних цифрових трансформацій.

Об'єкт дослідження: процес управління кіберризиками в банківських установах України.

Предмет дослідження: національні та міжнародні стандарти з інформаційної безпеки, нормативно-правова, законодавча база України для побудови системи управління інформаційною безпекою, а також існуючі програмно-технічні засоби кіберзахисту критичної інформаційної інфраструктури банківської системи України.

Мета роботи: проаналізувати існуючу нормативно-правову і законодавчу базу з питань управління кіберризиками у банківському секторі, дослідити сучасні програмно-технічні засоби захисту інформації, розробити рекомендації щодо підвищення рівня захищеності кіберстійкості елементів критичної інфраструктури банківських установ, спрямованих на зниження рівня кіберризиків.

Наукові завдання:

- проаналізувати основні кіберзагрози, що впливають на безпеку банківських систем та фінансових операцій;

- дослідити існуючі технології та інструменти управління кіберризиками, що застосовуються в банківській сфері;

- проаналізувати форми та методи кіберзахисту з точки зору їх ефективності в напрямку уникнення потенційних ризиків та зниження виявлених кіберризиків;

- розробити рекомендації щодо покращення систем управління кібербезпекою в банках на основі аналізу існуючих технологій.

Методи дослідження: опрацювання літератури за даною темою, порівняльний аналіз нормативно-правових актів, міжнародних та вітчизняних стандартів, аналіз використовуваних програмно-технічних засобів забезпечення інформаційної безпеки банківських установ.

Практичне значення одержаних результатів: впровадження розроблених рекомендацій допоможе банківським установам значно підвищити рівень технологій управління ризиками та зменшити ризики кіберзагроз. Це, у свою чергу, сприятиме зміцненню довіри клієнтів до банківських послуг та підвищенню загальної стійкості фінансової системи до кібератак.

1. ДОСЛІДЖЕННЯ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

1.1 Стандарти і нормативно-правове забезпечення управління ризиками інформаційної безпеки у банківській сфері.

Банківська сфера є однією з найбільш залежних від інформаційних технологій галузей економіки. Сучасні банки здійснюють більшість операцій у цифровому середовищі, використовуючи автоматизовані банківські системи, електронні платіжні інструменти, дистанційні канали обслуговування клієнтів, хмарні сервіси та інтегровані інформаційні платформи. За таких умов інформаційна безпека набуває стратегічного значення, а управління ризиками кібербезпеки стає ключовим фактором забезпечення стабільності та надійності банківської діяльності.

Управління ризиками інформаційної безпеки є невід'ємною складовою загальної системи управління ризиками банку та тісно пов'язане з управлінням операційними, фінансовими, правовими та репутаційними ризиками. Кіберінциденти можуть призводити не лише до прямих фінансових втрат, а й до втрати довіри клієнтів, порушення регуляторних вимог і негативного впливу на фінансову систему держави в цілому.

З огляду на високу концентрацію фінансових ресурсів, персональних даних та критично важливої інформації, банки є пріоритетними цілями кіберзлочинців. Саме тому регулювання інформаційної безпеки в банківській сфері здійснюється на основі комплексної системи міжнародних стандартів, рекомендацій фінансових регуляторів та національного законодавства.

Враховуючи негативні чинники загроз безпеки банківського сектору економіки, управління ризиками інформаційної безпеки в банках повинно бути системним, безперервним і орієнтованим не лише на реагування на вже реалізовані інциденти, на упередження загроз.

У сучасному фінансовому середовищі стандарти та нормативно-правове забезпечення відіграють важливу роль у забезпеченні стабільності, надійності та

безпеки банківських установ. Правова база, що регулює діяльність банків, має значний вплив на ефективність управління як фінансовими ризиками, так і кібербезпекою. Враховуючи важливість банківських операцій для економіки в цілому, нормативно-правове забезпечення забезпечує контроль за виконанням зобов'язань та створює умови для захисту інтересів клієнтів і забезпечення стабільності фінансової системи.

Нормативно-правова база банківської діяльності складається з широкого спектру документів, які включають закони, постанови, директиви та рекомендації. Міжнародні стандарти, такі як ISO/IEC 27001, ISO/IEC 27002 та інші, визначають найкращі практики в управлінні інформаційною безпекою та ризиками. Вони встановлюють вимоги до розробки, впровадження та підтримки систем безпеки інформації, що допомагає банкам забезпечити захист від кіберзагроз і невідповідностей у сфері безпеки даних.

Стандартизація у сфері інформаційної безпеки спрямована на формування уніфікованих підходів до ідентифікації, аналізу, оцінки та обробки ризиків. В основі сучасних стандартів лежить ризик-орієнтований підхід, який передбачає концентрацію ресурсів банку на найбільш критичних загрозах та вразливостях.

Управління ризиками інформаційної безпеки охоплює:

- визначення контексту напрямків діяльності банку;
- ідентифікацію загроз, вразливостей та інформаційних активів;
- оцінювання ймовірності реалізації кіберзагроз та потенційних збитків;
- вибір і впровадження заходів захисту;
- постійний моніторинг та вдосконалення системи безпеки і системи управління кіберризиками.

Такі принципи закладені в провідних міжнародних стандартах, що застосовуються в банківській практиці.

Одним із провідних стандартів у сфері управління інформаційною безпекою є міжнародний ISO/IEC 27002, розроблений для надання рекомендацій щодо найкращих практик з кібербезпеки і кіберзахисту. Стандарт є частиною сімейства стандартів ISO/IEC 27000, які спрямовані на забезпечення захисту інформаційних активів організацій. ISO/IEC 27002 детально описує заходи безпеки, які можуть бути використані для впровадження, моніторингу, підтримки та покращення СУІБ банківських установ.

На основі цього стандарту розроблено державний стандарт України «ДСТУ ISO/IEC 27002:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки (ISO/IEC 27002:2022, IDT)». Впровадження стандарту дозволяє банкам та іншим фінансовим установам ефективно управляти ризиками та забезпечувати безпеку даних. Регулярний моніторинг, оцінка ефективності та вдосконалення заходів безпеки, що базуються на ДСТУ ISO/IEC 27002, сприяють підтримці високого рівня інформаційної безпеки та готовності до сучасних викликів у сфері кібербезпеки.

ISO/IEC 27002 створений для допомоги організаціям у захисті їхніх інформаційних активів від потенційних загроз, а також для забезпечення конфіденційності, цілісності та доступності даних.

Галузевий Регулятор (НБУ) розробляє та впроваджує на основі цього стандарту нормативи, які охоплюють питання якості управління безпеки інформаційних систем. Вони служать основою для формування практик, які забезпечують відповідність міжнародним вимогам, зокрема у сфері захисту персональних даних клієнтів.

Норми та вимоги, що встановлюються нормативними актами Національного банку України, є обов’язковими для всіх учасників банківської системи.

Систематизовані вимоги щодо забезпечення відповідного рівня інформаційної безпеки у банківській системі України розроблені і рекомендовані для впровадження постановою НБУ №95 від 14 грудня 2016 року "Про затвердження Положення про інформаційну безпеку в банківській системі України. Положення визначає обов'язкові мінімальні вимоги щодо організації заходів з інформаційної безпеки та кіберзахисту у банківській інфраструктурі. Особливо важливими є вимоги, які стосуються принципів управління інформаційною безпекою та вимог до інформаційних систем банку, що взаємодіють з інформаційними ресурсами НБУ.

Головними вимогами для банківських установ є заборона на використання незахищених каналів зв'язку, що означає, заборону банкам передавати конфіденційну інформацію незахищеними каналами і у відкритому (без шифрування) вигляді, особливо такими як електронна пошта або неконтрольовані месенджери. Також заборонено зберігати конфіденційну інформацію на незахищених носіях, таких як незашифровані жорсткі диски чи флеш-накопичувачі. Крім того, не дозволяється надавати доступ до

інформаційних систем і даних банку особам, які не мають відповідних повноважень або необхідності в такому доступі.

Згідно з цією постановою, банки зобов'язані використовувати лише те програмне забезпечення, яке пройшло перевірку на відповідність вимогам безпеки та стандартам інформаційної безпеки. Банки повинні також регулярно оновлювати програмне забезпечення та системи безпеки, особливо якщо ці оновлення мають на меті усунення вразливостей.

Дана постанова є одним з інструментів забезпечення високого рівня інформаційної безпеки в банківській системі, дотримання вимог якої банківськими установами допомагає мінімізувати ризики, пов'язані з несанкціонованим доступом до конфіденційної інформації.

Постанова НБУ №95 регламентує також процес ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою.

З точки зору цільового напрямку нормативно-правове забезпечення управління ризиками інформаційної безпеки в банківській сфері спрямоване на:

- визначення обов’язкових вимог до захисту інформаційних активів банківських установ;
- формування єдиних підходів до оцінювання кіберризиків;
- забезпечення відповідальності банків за порушення вимог безпеки;
- підвищення рівня кіберстійкості інформаційної інфраструктури.

Головна мета державних нормативно-правових документів у області інформаційної безпеки є забезпечення впровадження єдиної політики банків в галузі захисту інформації, що гарантує безперервність бізнес-процесів, збереження конфіденційності, цілісності, доступності інформаційних ресурсів і технологічних процесів шляхом мінімізації ризиків до прийнятного рівня, який не загрожує фінансовій стабільності банку та інтересам його клієнтів.

Основними цілями нормативно-методологічної бази є досягнення банківськими установами належного рівня кібербезпеки, здатного протистояти кіберзагрозам і забезпечити загальний кіберзахист банківської інформаційної інфраструктури.

Дотримання норм і положень, визначених законами України та нормативно-правовими актами Національного банку України, є обов’язковими для виконання. Системи управління інформаційною безпекою і кіберризиками банків мають будуватися, підтримуватися і удосконалюватися у відповідності до вимог

чинного законодавства України, нормативно-правових актів НБУ, в тому числі Положенню про організацію заходів із забезпечення інформаційної безпеки в банківській системі України,(затвердженого постановою Правління Національного Банку України від 28 вересня 2017 року № 95), стандартам ДСТУ ISO/IEC 27001:2015 “Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 “Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки”, стандарту PCI DSS.

Базовим законом щодо кібербезпеки є Закон України від 05 жовт. 2017 р. №2163-VIII «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення захисту національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

В області питань з управління ризиками Національним банком України розроблено ряд нормативних документів, дотримання положень і засад, визначених в них, є обов’язковим для банківських установ.

Загальні принципи і вимоги, якими банківські установи мають керуватися у напрямку організації комплексної, ефективної системи управління ризиками, визначені Постановою НБУ № 64 «Про затвердження Положення про організацію системи управління ризиками в банках України і банківських групах» від 11 червня 2018 р.

В області управління кіберризиками одним з визначальних нормативних документів є «Методичні рекомендації щодо управління операційним ризиком (у тому числі кіберризиком та безперервністю діяльності) та забезпечення зберігання інформації про клієнтів об’єктами платіжної інфраструктури» (далі-Рекомендації), який відповідно до п.1 розділу І створено з метою оперативного виявлення кіберзагроз, кібератак, кіберінцидентів, визначення їх наслідків, мінімізації їх впливу та встановлення часу відновлення здійснення/надання критичних послуг/операцій, забезпечення планового рівня функціонування платіжної інфраструктури, підвищення надійності платіжних систем та захисту інтересів їх користувачів.

Методичні Рекомендації розроблено відповідно до Законів України “Про Національний банк України”, “Про платіжні системи та переказ коштів в Україні”, Положення про нагляд (оверсайт) платіжних систем та систем

розрахунків в Україні, затвердженого постановою Правління Національного банку України від 28 листопада 2014 року №755 (зі змінами), а також з урахуванням кращих міжнародних практик, принципів та провідних міжнародних документів щодо забезпечення кіберстійкості інфраструктури фінансового ринку (розд. I, п.2 Рекомендацій).

Відповідно до п.5 другої частини статті 2 ЗУ «Про основні засади забезпечення кібербезпеки України», НБУ визначений суб'єктом, який безпосередньо здійснює у межах своєї компетенції заходи із забезпечення кібербезпеки, і відповідно до п.5 статті 5 повинен здійснювати виявлення і реагування на кіберінциденти та кібератаки, і усунення їх наслідків.

Таким чином ця норма має бути запроваджена в практику відповідних профільних служб банківських установ для проєктування організаційних заходів та технічних засобів забезпечення ідентифікації і оперативного вирішення інцидентів інформаційної безпеки шляхом мінімізації ризиків, пов'язаних з інформаційною безпекою, до того, як ці інциденти вплинуть на бізнес-процеси.

У сфері управління кіберризиками банківські установи керуються в першу чергу нормативно-правовою базою НБУ. Відповідно до пункту 6 частини другої статті 8 ЗУ «Про основні засади забезпечення кібербезпеки України» Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України і для суб'єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України.

Стандарти та нормативно-правове забезпечення створюють основу для формування єдиної системи управління ризиками кібербезпеки в банківській сфері. У відповідності до вимог чинного законодавства України банки відбудовують власну систему управління ризиками, використовуючи норми Законодавства і галузевого Регулятора (НБУ).

Їх дотримання дозволяє:

- зменшити ймовірність виникнення кіберінцидентів;
- мінімізувати фінансові та репутаційні втрати;
- підвищити довіру клієнтів і партнерів;

- забезпечити стабільність і безперервність банківських операцій.

Таким чином, національні, міжнародні стандарти, нормативно-правові акти Регулятора є ключовими інструментами ефективного управління ризиками інформаційної безпеки у банківській сфері та формують підґрунття для подальшого розвитку технологій кіберзахисту.

1.2 Загрози та вразливості кібербезпеки в банківській сфері

Банківська сфера є однією з найбільш привабливих цілей для кібератак унаслідок концентрації фінансових ресурсів, конфіденційної інформації та критично важливих платіжних сервісів. Інтенсивна цифровізація банківських процесів, впровадження дистанційного обслуговування клієнтів, мобільного та інтернет-банкінгу, а також інтеграція банківських систем з фінтех-платформами значно розширюють поверхню атаки та створюють нові вектори загроз.

Кіберзагрози в банківській сфері мають не лише локальний характер, але й можуть набувати системного масштабу, впливаючи на стабільність фінансової системи держави. Саме тому аналіз, класифікація та оцінювання загроз кібербезпеки є важливою складовою управління ризиками інформаційної безпеки банківських установ.

Банківська система має критичну інформаційну інфраструктуру, яка постійно підпадає під значну кількість атак як зовнішніми, так і внутрішніми каналами, тому класифікація існуючих (відомих) і потенційних загроз, які можуть спричинити не тільки порушення роботі систем, конфіденційності та цілісності фінансових даних, а і до руйнувань в загальній системі інформаційної безпеки та інформаційної інфраструктури в цілому, є необхідним компонентом в загальній системі кіберзахисту.

До основних категорій загроз належать:

1. Кіберзлочинність. Зловмисники, хакери можуть зламувати системи безпеки банків, красти конфіденційні дані, модифікувати і красти фінансові записи,
2. Внутрішні загрози. Співробітники банків можуть мати несанкціонований доступ до конфіденційних даних або навмисно змінювати дані з метою шахрайства.
3. Шкідливе програмне забезпечення. Віруси, троянські програми та інші види шкідливого програмного забезпечення можуть порушувати

конфіденційність, цілісність даних, функціонування телекомунікаційних, інформаційних систем, будь-яких компонентів внутрішньої мережі банківської установи, зупинку сервісів і бізнес процесів в кінцевому рахунку.

Задля забезпечення безпеки фінансових даних відповідними службами банківських установ проводяться заходи з виявлення подій, що можуть загрожувати цілісності банківської інформації і призвести до понесення Банком збитків або додаткових втрат. Такі події виникають внаслідок реалізації кіберризику. З цією метою на регулярній основі проводиться класифікація кіберзагроз, яка відбувається за критеріями: порушення вимог конфіденційності, цілісності та доступності.

Таблиця 1.1 Класифікація загроз

Ціль кіберзагрози	**Вид загрози**
порушення вимог конфіденційності	кіберінциденти, через які отримано несанкціонований доступ до інформації та або інформаційних систем
	втрата носіїв інформації за межами периметру Банку
	втрата або крадіжна ноутбука, планшета або смартфона, який містить інформацію з обмеженим доступом
	несанкціоновані спроби працівників отримати доступ вище наявного у них рівня в системі;
	спроби зсередини або ззовні отримати доступ до інформаційних систем
порушення вимог цілісності	втрата даних або незавершені транзакції
	віруси, «троянські коні» (шкідливе ПЗ, пошкодження інформації на жорстких дисках, помилки систем; невірні контрольні суми або значення хеш-функцій)
порушення вимог доступності	простої в роботі інформаційних систем протягом неприйнятного періоду часу. Якщо простій триває довше, ніж обумовлено в угодах підрядчих (аутсорсингових) організацій з Банком, і не може бути усунутий протягом певного часу, виконуються дії, які визначені в Плані забезпечення безперервної діяльності банківської установи
	крадіжка ноутбуків, комплектуючих або носіїв інформації.

Також відповідно до встановлених Політик безпеки банківськими працівниками відповідних служб (інформаційної безпеки, ІТ-департаменту)

мають бути визначені і систематизовані події несприятливого характеру, які мають негативний вплив на роботу елементів інформаційної структури і несуть загрозу раптового порушення штатного режиму їх роботи. При цьому враховується, що спроба реалізації інформаційної загрози є по суті кібератакою – інструментом реалізації кіберризику.

Основні типи подій, які виникають внаслідок реалізації кіберризику та призводять до понесення банком збитків або додаткових втрат, і можуть бути результатом навмисних дій зловмисників (кібератак) наведено в таблиці 1.2.

Таблиця 1.2. Перелік потенційних подій кіберризику

№ з/п	Зміст події
1	компрометація облікових записів привілейованих користувачів;
2	компрометація облікових записів зовнішніх сервісів;
3	атаки на веб-додатки;
4	мережеві атаки;
5	зараження зловмисним кодом (віруси);
6	виявлення збору інформації про інформаційну системи;
7	нелегітимне використання привілейованих облікових записів;
8	витік інформації з обмеженим доступом;
9	порушення правил віддаленого доступу;
10	порушення правил доступу (використання) до Інтернет;
11	несанкціоновані зміни в інфраструктурі інформаційних технологій (наприклад внаслідок діяльності підрядників);
12	незаконний (несанкціонований) моніторинг інформаційних систем (сканування, сніффінг тощо);
13	фіксування системами виявлення/запобігання вторгнень IDS/IPS подій, що можуть становити загрозу інформаційним активам Банку та мережі Банку в цілому
14	використання користувачем чужого ідентифікатора (логін, пароль);
15	несанкціонований доступ до активів, а також їх викрадення, модифікація та видалення як працівниками банківської установи, так і сторонніми особами;
16	несанкціонований доступ до мережі та сервісів;
17	компрометація інформаційних активів та репутації Банку
18	фіксування великої кількості невдалих спроб аутентифікації, а також зламу пароля до інформаційних систем Банку та мережі Інтернет
19	несанкціоновані зміни налаштувань мережевого обладнання
20	аномальні події в системах моніторингу серверного, мережевого обладнання

№ з/п	Зміст події
21	витік конфіденційної інформації;
22	фіксування швидкого розповсюдження вірусів, «троянських коней», «хробаків»
23	відмова в обслуговуванні та фіксування спроб порушення роботи сервісу чи системи
24	фіксування різкого збільшення мережевого трафіка
25	фіксування працівниками установи або повідомлення користувачів про наявність в поштових скриньках великої кількості повідомлень, що повторюються та мають неслужбовий характер

Сукупність несприятливих подій, або подія, що ставить під загрозу конфіденційність, цілісність, доступність інформації в платіжній інфраструктурі та/або захищеність її інформаційних систем у кіберпросторі, та/або порушує передбачену політику і процедури, які спрямовані на забезпечення кібербезпеки, шляхом навмисних, злочинних або ненавмисних дій визначається за нормами НБУ кіберінцидентом (п. 4, ст.5 розд.I Методичних рекомендацій).

Кіберінцидент несе потенційну або реальну небезпеку для даних, інформаційних систем, інформаційно-комунікаційних технологій, програмних, апаратно-технічних та технологічних засобів і обладнання обробки інформації банківської системи. Причинами кіберінцидентів є кібератаки (поширений інструмент реалізації кіберризику), які здійснюються із застосуванням шкідливого програмного коду/вірусних програм), а також технічні збої і людські помилки.

Таблиця 1.3.Перелік категорій кіберінцидентів

№	Категорія	Тип інциденту	Цільовий напрямок інциденту
1	Шкідливий вміст	Спам	Надсилання небажаних повідомлень або великої кількості повідомлень
2	Шкідливий програмний код	Зараження зловмисним кодом (Malware)	У системі виявлено шкідливе програмне забезпечення
		Розповсюдження шкідливого ПЗ	Розповсюдження шкідливого ПЗ, наприклад шляхом розсилки повідомлень електронної пошти, що містять вкладення з зловмисний кодом або посилання на його завантаження

№	Категорія	Тип інциденту	Цільовий напрямок інциденту
3	Збір інформації зловмисником	Сканування	Збір інформації про системи або мережі
		Фішинг (Phishing)	Спроба збору інформації про користувача чи систему за допомогою масової розсилки електронною поштою спрямованою на збір даних, що може містити посилання на фішингові сайти
4	Спроби втручання	Спроба авторизації в систему(Login attempts)	Спроба входу до служб доступу. Невдала спроба підбору автентифікаційних даних чи використання вже не актуальних даних
5	Втручання	Компрометація облікового запису (Account compromise)	Фактичне вторгнення в систему або мережу шляхом компрометації облікового систему шляхом запису користувача
		Компроментація системи (System compromise)	Фактичне вторгнення в систему чи її сервіс або застосунок через використання вразливості в мережі. Несанкціонований доступ до системи в обхід системи контролю доступу
6	Порушення доступності (Availability)	DoS/DDoS	Вплив на нормальне функціонування системи, що досягається направленням з одного чи багатьох джерел до цільового ресурсу запитів для перенасичення пропускної здатності чи системних ресурсів
		Шкідливі дії	Дії, спрямовані на пошкодження системи, переривання процесів, зміну або видалення інформації тощо
		Збій	Збій в роботі системи без зловмисного втручання
7	Порушення властивостей інформації	Несанкціонований доступ до інформації	Несанкціонований доступ до інформації. Несанкціонований обмін конкретним набором інформації

№	Категорія	Тип інциденту	Цільовий напрямок інциденту
8	Шахрайство	Шахрайський сайт	Створення фішингових сайтів для збору автентифікаційних чи інших даних користувачів

За результатами дослідження питання категоризації кіберзагроз за частотою здійснення найчастіше спрацьовують атаки, що наведені нижче.

1.Фішингові атаки та соціальна інженерія

Фішинг є однією з найпоширеніших кіберзагроз у банківській сфері. Він полягає у використанні підроблених електронних повідомлень, вебсайтів або мобільних застосунків з метою отримання конфіденційної інформації клієнтів або працівників банку для здійснення в подальшому незаконних фінансових операцій. Соціальна інженерія використовує психологічні методи впливу, зловживаючи довірою користувачів та їх недостатньою обізнаністю у сфері кібербезпеки.

Наслідками фішингових атак можуть бути:

- несанкціонований доступ до рахунків клієнтів;
- викрадення облікових даних;
- фінансові шахрайства;
- компрометація внутрішніх систем банку.

2.Шкідливе програмне забезпечення

Шкідливе програмне забезпечення є серйозною загрозою для банківських інформаційних систем. До нього належать банківські трояни, програми-вимагачі (ransomware), шпигунські програми та бекдори. Такі програми використовуються для викрадення фінансових даних, блокування роботи систем або здійснення несанкціонованих транзакцій.

Особливо небезпечними є програми-вимагачі, які можуть паралізувати роботу банку та спричинити значні фінансові втрати у разі відсутності ефективних механізмів резервного копіювання.

3.Атаки типу DDoS

Атаки DDoS («відмова в обслуговуванні», англ. Distributed Denial of Service) спрямовані на перевантаження банківських вебресурсів, телекомунікаційного обладнання, або платіжних, систем великою кількістю запитів. Метою таких атак є порушення доступності сервісів, що негативно впливає на обслуговування клієнтів та репутацію банку.

DDoS-атаки часто використовуються як інструмент тиску або відволікання уваги від інших кібератак.

DDoS-атака має багатопотоковий характер, який забезпечує спроби блокування сайту і виконується з використанням значної кількості пристроїв, комп'ютерів, які керуються дистанційно.

4.Внутрішні загрози кібербезпеки

Внутрішні загрози пов'язані з діяльністю працівників банку та є не менш небезпечними, ніж зовнішні атаки. Вони можуть бути як навмисними, так і ненавмисними.

До внутрішніх загроз належать:

- порушення політик інформаційної безпеки;
- зловживання службовим доступом;
- помилки персоналу;
- використання незахищених носіїв інформації;
- недостатній рівень кіберграмотності співробітників.

Внутрішні загрози часто є наслідком слабкого контролю, недостатнього навчання персоналу та відсутності ефективної системи управління доступом.

5.APT-атаки (Advanced Persistent Threat)

APT-атаки — складні цілеспрямовані кіберзагрози, що характеризуються тривалим прихованим перебуванням зловмисників в інформаційних системах банку з метою отримання стратегічно важливої інформації або фінансової вигоди.

Основні характеристики APT-атак:

Advanced (складні) — використовують сучасні та комбіновані методи атак, у тому числі шкідливе ПЗ, експлойти нульового дня, соціальну інженерію;

Persistent (стійкі) — зловмисники тривалий час залишаються в системі, уникаючи виявлення;

Threat (загроза) — атаки мають серйозні наслідки для фінансової, інформаційної та репутаційної безпеки.

APT-атака реалізується в декілька етапів:

1. Розвідка — збір інформації про банк, його персонал та IT-інфраструктуру;
2. Початкове проникнення — фішинг, експлуатація вразливостей або компрометація облікових даних;
3. Закріплення в системі — встановлення бекдорів і механізмів постійного доступу;
4. Розширення привілеїв — отримання доступу до критичних ресурсів;
5. Приховане виконання дій — викрадення даних або маніпуляції фінансовими операціями;
6. Вихід або маскування — збереження доступу для майбутніх атак.

Для банківських установ загрози типу APT націлені на:

- викрадення великих обсягів фінансових і персональних даних;
- маніпуляції платіжними системами;
- порушення безперервності бізнесу;
- значні фінансові та репутаційні втрати банку.

7. Загрози з боку третіх сторін (постачальники, підрядники, зовнішні партнери)

Сучасні банки активно співпрацюють з аутсорсинговими компаніями, фінтех-стартапами та постачальниками IT-послуг. Це створює додаткові ризики, пов’язані з кібербезпекою.

Загрози з боку третіх сторін включають:

- недостатній/ нижчій рівень захисту у партнерів за рахунок чого вони можуть стати точкою входу для кібератак на банківську установу;
- витоки даних через підрядників;
- компрометацію API та інтеграційних інтерфейсів;
- відсутність контролю за дотриманням вимог безпеки.

Реалізація кіберзагроз в банківській системі має потенційні негативні наслідки наступного характеру:

- прямі фінансові втрати;

- порушення безперервності бізнесу;
- зниження довіри клієнтів;
- витік конфіденційної інформації
- погіршення репутації.

В окремих випадках наслідки кіберінцидентів можуть мати довгостроковий характер та впливати на конкурентоспроможність банку. Всі кіберінциденти по суті є формою реалізації кіберризиків і є відправними точками при застосуванні методів аналізу, класифікації і оцінювання ризиків, розробки заходів їх усунення, а також розробки превентивних засобів безпеки.

Своєчасна ідентифікація та аналіз загроз кібербезпеки є ключовою передумовою ефективного управління ризиками інформаційної безпеки.

Регулярний моніторинг загроз, аналіз інцидентів та підвищення рівня кіберобізнаності персоналу дозволяють банкам мінімізувати ймовірність реалізації кіберзагроз і зменшити їх негативні наслідки.

Нижче представлена таблиця, яка систематизує основні загрози кібербезпеки в банківській сфері, їх джерела, можливі наслідки та ключові заходи протидії. Такий підхід дозволяє комплексно оцінити вплив кожної загрози на діяльність банківської установи та визначити пріоритетні напрями впровадження заходів кіберзахисту.

Таблиця 1.4. Систематизація загроз

Загроза	**Джерело загрози**	**Потенційні наслідки для банку**	**Основні заходи протидії**
Фішингові атаки	Кіберзлочинні угруповання, шахраї	Викрадення облікових даних клієнтів, фінансові втрати, зниження довіри	Навчання персоналу та клієнтів, багатофакторна автентифікація, антифішингові фільтри
Соціальна інженерія	Зовнішні зловмисники	Несанкціонований доступ до систем, витік конфіденційної інформації	Політики безпеки, регулярні тренінги, контроль доступу
Шкідливе ПЗ (трояни, ransomware)	Кіберзлочинні групи	Блокування систем, викрадення даних, вимагання коштів	Антивірусні системи, резервне копіювання, оновлення ПЗ
DDoS-атаки	Хакерські угруповання, бот-мережі	Відмова в обслуговуванні, порушення доступності	Системи захисту від DDoS, резервування каналів зв’язку

Загроза	Джерело загрози	Потенційні наслідки для банку	Основні заходи протидії
		сервісів	
APT-атаки	Організовані групи, кіберрозвідка	Тривалий прихований доступ, значні фінансові втрати	Моніторинг подій безпеки (SIEM), сегментація мережі
Внутрішні зловживання	Співробітники банку	Витік інформації, шахрайство	Розмежування доступу, аудит дій користувачів
Помилки персоналу	Людський фактор	Порушення цілісності та доступності даних	Навчання, стандарти операційної діяльності
Атаки через API	Треті сторони, зловмисники	Несанкціонований доступ до систем	Аутентифікація API, обмеження доступу
Компрометація платіжних систем	Зовнішні та внутрішні загрози	Фінансові втрати, порушення регуляторних вимог	Моніторинг транзакцій, криптографічний захист
Витік даних через підрядників	Аутсорсингові компанії	Репутаційні втрати, штрафні санкції	Контроль третіх сторін, договори з вимогами безпеки

Державною службою спецзв'зку України розроблений Перелік категорій кіберінцидентів, який призначений для впровадження в Україні єдиної таксономії як інструменту для обміну між профільними службами організацій інформацією щодо кіберінцидентів. Перелік може застосовуватись суб'єктами забезпечення кібербезпеки для формування за необхідності власних переліків кіберінцидентів відповідно до специфіки роботи з дотриманням кодування категорій кіберінцидентів, встановлених в системі MISP (Malware Information Sharing Platform), яка є системою (програмним рішенням з відкритим кодом) миттєвої передачі «координат» у кіберпросторі, для збору, зберігання, розповсюдження та обміну показниками і загрозами кібербезпеки. Ця платформа дозволяє службам інформаційної безпеки в автоматичному режимі обмінюватися технічними даними про кіберзагрози - індикаторами компрометації (IoC).

Засобами MISP в режимі онлайн поширюється інформація, за якою можна ідентифікувати зловмисників та їхній інструментарій, а саме:

- IP-адреси та доменні імена серверів, з яких ведуться атаки;
- URL-адреси шкідливих сайтів;

- e-mail зловмисників;
- хеш-суми вірусів та інших шкідливих файлів (MD5, SHA1, SHA256);
- назви файлів, що використовуються в атаках.

На основі цієї платформи заснована національна платформа MISP, до якої можуть отримати доступ зацікавлені у зміцненні власної системи кібербезпеки організації.

Державні банки України, що мають велику розгалужену мережу відділень, є потенційними користувачами цієї платформи і розробляють власні переліки категорій кіберінцидентів, які за рекомендацією Держспецзв'язку повинні регулярно переглядатися службами безпеки з урахуванням практики його застосування, появи нових категорій і типів кіберінцидентів, а також інформації, отриманої від працівників профільного підрозділу з кібербезпеки.

Перелік кіберінцидентів за класифікацією MISP, наведено в таблиці 1.5 (див. Додаток 1).

Для успішної реалізації кібератак кіберзлочинцями використовуються вразливості інформаційних і комунікаційних систем. В результаті дослідження цього питання визначено вразливості, які найчастіше використовуються хакерами:

1). Використання застарілих (вразливих) операційних систем та програмного забезпечення.

Зменшення рівня кіберризику і усунення вразливості залежить від регулярного і своєчасного оновлювання операційних систем та програмного забезпечення до останніх версій, оскільки це значно покращує швидкість, ефективність роботи. Також встановлені оновлення (патчі-patches) зміцнюють систему безпеки. Для усунення ризику програмне забезпечення, яке не підтримується виробником, замінюється альтернативним або встановлюються додаткові засоби контролю показників та/або режиму його функціонування і впливу на роботу пов'язаних з ним систем. В комп'ютерних мережах в якості заходу безпеки застосовується техніка мікросегментації, що забезпечує детальний контроль над мережевим трафіком, розділяючи його на менші, ізольовані сегменти. Додатковим засобом безпеки є обмеження доступу до систем, регулярне оновлення яких є неможливим або проблематичним.

2). Надмірна кількість відкритих сервісів на APM (Application Performance Monitoring – Моніторинг продуктивності додатків) та серверах, використання яких не обумовлено виробничою необхідністю.

Усунення цієї вразливості можливо за рахунок проведення на регулярній основі перевірки/аудиту відкритих портів для виявлення незахищених сервісів і закриття всіх портів і служб, які не використовуються в технологічних процесах.

Необхідно також використовувати брандмауер (Firewall) для обмеження доступу лише для дозволених IP-адрес, впровадити список дозволених сервісів (whitelist) та заблокувати всі інші.

3). Недоліки у налаштуваннях мережевого обладнання, в тому числі відсутність належно налаштованих списків контролю доступу.

Порушення контролю доступу – ситуації, коли користувачі отримують доступ до ресурсів або функцій, не маючи на це відповідних прав.

Для зниження кіберризику, залежного від цієї вразливості необхідно використовувати список контролю доступу (ACL-Access Control List) для обмеження міжмережевої взаємодії, відокремити критичні сервіси в окремі віртуальні локальні комп'ютерні мережі (VLAN- Virtual Local Area Network) або захищені зони; впровадити DMZ (Demilitarized Zones) для сервісів, які доступні з мережі Інтернет, використовувати програмні засоби моніторингу трафіка для виявлення підозрілої активності; застосувати фільтрацію MAC-адрес (адрес керування доступом до середовища) або 802.1X - аутентифікацію (протокол контролю доступу клієнт-сервер, що дозволяє встановлювати автентичність та забороняє підключатись до локальної мережі через загальнодоступні порти комутатора).

4). Недотримання вимог кібергігієни.

Дотримання базових правил кібергігієни допомагає захистити робочі станції працівників від ураження шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації, що в першу чергу пов'язано з необхідністю впровадження політики складних паролів, які мають складатися з мінімум 12 символів та змінюватися кожні 90 днів.

З метою зниження відповідних кіберризиків необхідно використовувати спеціалізовані менеджери паролів, заборонити зберігання паролів у відкритому вигляді, регулярно проводити тренінги з кібербезпеки, не допускати зберігання файлів уніфікованого електронного підпису на незахищених носіях інформації.

5). Ризики віддаленого доступу.

Віддалений доступ дозволяє користувачу отримувати доступ до систем і даних та керувати ними завдяки підключенню до комп’ютера або мережі з віддаленого місця.

Щоб не стати жертвою зловмисників під час використання віддаленого доступу необхідно використовувати VPN виключно зі стійкими алгоритмами шифрування; впровадити двофакторну автентифікацію для доступу до критичних ресурсів та встановити обмеження доступу за IP-адресами; дезактивувати віддалений доступ для облікових записів з правами адміністратора.

З урахуванням категоризації інцидентів інформаційної безпеки і визначених вразливостей службами інформаційної безпеки банківських установ відповідно до вимог Регулятора та державного законодавства розроблюються превентивні засоби контролю і протидії потенційним загрозам.

2. АНАЛІЗ ТЕХНОЛОГІЙ УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

2.1 Аналіз існуючих технологічних рішень забезпечення кібербезпеки в банках.

Для захисту своїх інформаційних ресурсів більшість банківських установ використовують найновітніші технічні засоби програмного і апаратного захисту, технології безпеки мережевого комп'ютерного простору, робочих станцій працівників.

За нормами НБУ банківськими установами із можливим залученням сертифікованих компаній на регулярній основі здійснюються перевірки стану інформаційної безпеки шляхом виконання:

- зовнішнього ASV-сканування мережі (сканування мережевої інфраструктури на наявність вразливостей у відповідності до стандарту PCI DSS) з метою виявлення критичних вразливостей, помилок в конфігурації, небезпечних служб (аналіз захищеності інформаційних ресурсів проводиться з зовнішніх мереж, зокрема з мережі Інтернет);
-внутрішнього сканування мережі (аналіз захищеності інформаційних ресурсів проводиться з внутрішньої мережі банку);
- сканування бездротових мереж (сканування ефіру на предмет виявлення несанкціонованих бездротових пристроїв) з метою аналізу захищеності бездротових мереж банку і перевірки наявності бездротового обладнання, несанкціоновано підключеного до мережі банку;
- тесту на проникнення (Penetration Test), за яким здійснюється оцінювання захищеності інформаційних ресурсів або мережі шляхом часткового моделювання дій зовнішніх зловмисників з проникнення у неї (які не мають авторизованих засобів доступу до системи) і внутрішніх зловмисників (які мають певний рівень санкціонованого доступу);
- виконання заходів з мінімізації кіберризиків.

Одним із дієвих і ефективних засобів виявлення вразливостей, недоліків у системах, неправильних конфігурацій, дефектів апаратних засобів та програмного забезпечення є тестування мереж і систем на проникнення.

Тестування мережевого, серверного обладнання, інформаційних систем на проникнення здійснюється етичними хакери шляхом імітації кібератак на комп'ютерну систему, мережу або програму, для пошуку та використання вразливостей безпеки, перш ніж це зроблять зловмисники. В результаті відпрацювання технічних тестових процедур і виявлення вразливостей банк отримує можливість завчасно виправити слабкі місця в інформаційній інфраструктурі і впровадити необхідні засоби програмного/апаратного захисту, що мінімізує рівень потенційних ризиків і є запобіжником дороговартісних заходів з відновлення даних.

Тест на проникнення виконується сертифікованими фахівцями. Існують чіткі вимоги до осіб, що залучаються банками для проведення тесту на проникнення:

- наявність досвіду проведення тестування на проникнення (не менший одного року);
- забезпечення особами незалежності експертизи (діє умова не прийняття особою участі у проектуванні, розробці, впровадженні та підтримці інформаційних систем та технічних засобів захисту Банку);
- наявність підтвердження кваліфікації в цій області (сертифікат CEH (Certified Ethical Hacker) або інший);
- знання та керування під час проведення тесту на проникнення вимогами відповідних міжнародних методик:
    - ISECOM OSSTMM3;
    - NIST SP800-115;
    - Penetration Testing Execution Standard;
    - Payment Card Industry Data Security Standard (PCI DSS), v.2.0;
    - ASV Security Scanning Procedures, PCI SSC;
    - Information Supplement: Requirement 11.3 Penetration Testing, PCI SSC;
    - Social Engineering Framework;
    - Open Web Application Security Project (OWASP) Testing Project;
    - Penetration Testing Model (BSI);
    - ISACA IS auditing procedure «Security assessment–penetration testing and vulnerability analysis».

Безпека інформаційних ресурсів банку має забезпечуватись на рівні робочих станцій користувачів систем, на рівні сегментів внутрішньої інформаційної мережі, на рівні межі внутрішньої мережі із зовнішньою.

Захист зовнішнього периметру мережі банків здійснюється за рахунок впровадження і застосування комплексу апаратних та програмних рішень, які контролюють вхідний/вихідний трафік, блокуючи зовнішні загрози і несанкціонований доступ до інформаційних ресурсів. При цьому профільні служби банків, що забезпечують систему управління інформаційною безпекою, при виборі технологій захисту повинні враховувати сучасний фактор кіберзагроз, який складається з нових технік та можливостей хакерів, які охоплюють потужності штучного інтелекту для розробки вірусних програм, що значно ускладнює процес побудови ефективної системи ІБ.

Основними програмно-технічними інструментами, які забезпечують безпеку інформаційної інфраструктури банків шляхом перевірки вхідного трафіку на межі корпоративної мережі та Інтернет, становлять міжмережеві екрани (NGFW/UTM), системи запобігання вторгненням (IPS), захист від DDoS-атак і WAF(Web Application Firewall) для веб-додатків.

1. Міжмережеві екрани.

Одним із сучасних технічних рішень в розпізнаванні хакерських загроз на етапі вторгнення в комп'ютерну мережу є NGFW- Next Generation Firewall (фаєрвол наступного покоління), який забезпечує комплексний захист мережі від різнорівневих атак та складних кіберзагроз і ефективну технологію для розпізнавання нових атак.

NGFW розроблений з новим набором можливостей і містить додаткові розширені функції безпеки, щоб виявляти відомі та невідомі кібератаки:

- контроль додатків та користувачів за допомогою інтелектуальних алгоритмів (ідентифікація та керування додатками незалежно від портів; ідентифікація користувачів за IP-адресами, даними Active Directory),
- перевірка зашифрованого трафіку шляхом аналізу ідентифікованих конкретних додатків і користувачів для блокування складних загроз,
- глибока інспекція пакетів (DPI) шляхом аналізу заголовків і вмісту пакетів,
- інтеграція з іншими технологіями кіберзахисту IPS/IDS (запобигання вторжень),
- інтеграція з Active Directory,
- можливість керування налаштуваннями доступу до мережі шляхом встановлення правил в політиках безпеки для конкретних груп користувачів, різних видів трафіку та різних мереж,

- прогнозування нових кібератак,
- потоковий антивірус,
- захист від шкідливих програм.

Такі функції забезпечують блокування кібератак в реальному часі.

2. Системи запобігання вторгненням.

До основних компонентів та технологій захисту периметру мережі банку відносяться системи запобігання вторгненням, які виявляють і блокують підозрілу активність в реальному часі , відносяться системи IPS/ IDS.

IDS (Intrusion Detection System) та IPS (Intrusion Prevention System) –програмно-апаратні засоби мережевої безпеки, які аналізують трафік для виявлення (IDS) або автоматичного запобігання (IPS) спроб несанкціонованого доступу, шкідливої активності та атак у режимі реального часу, захищаючи інфраструктуру від злому.

3.Захист від DDoS-атак.

Для захисту мережевої інфраструктури від DDos-атак розроблено і широко використовується в банках Anti-DDoS (Anti-Distributed Denial of Service) — комплекс програмних та апаратних інструментів, призначених для захисту мережі, серверів та вебсайтів від розподілених атак на відмову в обслуговуванні.

Anti-DDos забезпечує багаторівневий захист IT-інфраструктури банківських установ від відомих і невідомих атак і запобігає перевантаженню мережі зловмисним трафіком шляхом аналізу трафіку в реальному часі, виявлення шкідливих запитів та їх фільтрації (очищення), дозволяючи лише легітимним користувачам отримати доступ до ресурсу. Це рішення містить також комплексні інструменти для аналізу та автоматичного складання звітності. Форми реалізації цих рішень - хмарні сервіси, програмні продукти або апаратні комплекси.

4.Захист зовнішнього периметру мережі.

Для захисту зовнішнього периметру мережі банків застосовується міжмережевий екран для веб-додатків WAF(Web Application Firewall).

Існують апаратні, програмні та хмарні рішення WAF, а також сучасні WAAP (Web Application and API Protection) рішення, які розширюють функціонал WAF для захисту API (додатків) та бот-трафіку.

WAF аналізує вміст HTTP-запитів (URL, заголовки, тіло запиту) і, якщо запит не відповідає політикам безпеки або виглядає шкідливим, він блокується до того, як досягне веб-програми.

Головне призначення WAF – відслідкування та фільтрація HTTP-трафіку між інтернетом та банківським сайтом/додатком, захищаючи його від широкого

спектру кібератак, таких як SQL-ін'єкції, XSS, брутфорс та DDoS; аналізування запитів і блокування шкідливих.

До його функцій входить:

- фільтрування трафіку на основі заданих правил та сигнатур атак,
- захист від відомих та нових атак (уразливостей нульового дня), таких як SQL-ін'єкції, міжсайтовий скриптинг (XSS), віддалене виконання коду (RCE),
- запобігання несанкціонованому доступу та витоку даних,
- блокування шкідливих запитів (спроби підбору паролей, інші)

Сучасні файєрволи WAF є невід'ємною частиною захисту веб-ресурсів, який захищає від атак, націлених на бізнес-логіку веб-додатків.

Засоби захисту периметра мережі установи забезпечують:

- Зменшення ризиків зараження кінцевих пристроїв.
- Цілодобовий моніторинг інцидентів та контроль за доступом.
- Захист конфіденційних даних банків від витоків інформації.
- Безперервність банківських технологічних і бізнес-процесів.

Рівень захисту робочих станцій працівників.

Ефективна система управління інформаційною безпекою передбачає також обов’язковий кіберзахист робочих станцій користувачів. На цьому рівні використовуються інструменти, що гарантують зашифрований, захищений віддалений доступ для працівників, які працюють дистанційно.

Для робочих станцій працівників використовується відповідна група програмних додатків/систем, що контролюють вхідні запити із зовнішніх джерел (сервісів, веб-додатків), санкціонованість/легітимність встановленого на станцію програмного забезпечення (ПЗ). Це виконують:

- агенти системи антивірусного та антиспамівського захисту,
- агенти контролю ПЗ, такі, наприклад, як CheckPoint SandBlast Agent.

Агент Check Point SandBlast забезпечує комплексний захист кінцевих точок у режимі реального часу від загроз нульового дня та програм-вимагачів, використовуючи емуляцію загроз на основі штучного інтелекту, аналіз поведінки файлів та активності системи, і криміналістику. Він захищає робочі станції, браузери та дані за допомогою таких функцій, як автоматизований аналіз інцидентів, повне шифрування диску та захист від фішингу.

SandBlast має розширення для захисту браузера, яке запобігає крадіжці облікових даних та фішинговим атакам. Постійно фіксує дані про оновлення файлів,

процеси та зміни реєстру для автоматичного створення звітів про інциденти та усунення загроз.

Розширення Endpoint Security Suite здійснює повне шифрування диску, що важливо для захисту даних та систем, які встановлені і зберігаються на мобільних пристроях (ноутбуках) працівників.

Також в процесі управління кібербезпекою банками застосовуються технологія веб-фільтрації (блокування доступу до небезпечних сайтів), VPN-шлюзи і модель побудови інформаційних систем Zero Trust (інтерактивна перевірка користувачів та пристроїв. Модель з нульовою довірою (англ. zero trust model), яка виходить з того, що систему вже зламано, і тому довіряти не можна нікому, навіть легітимним користувачам, що знаходяться усередині периметра мережі. Тому кожен доступ до даних і програм потребує підтвердження.

Сучасним рішенням для мінімізації кіберризиків є програмні засоби SIEM.

Сьогодні SIEM є одним з провідних інструментів виявлення загроз та реагування на інциденти, що реалізується шляхом агрегації та аналізу даних журналів з усієї IT-інфраструктури.

Поєднуючи управління подіями безпеки (аналіз у режимі реального часу) та управління інформацією безпеки (довгострокове зберігання), SIEM допомагають командам/ центрам операцій безпеки (SOC) виявляти аномалії, автоматизувати реагування. Використання інструментів SIEM забезпечує проактивне управління загрозами та скорочує час між їх виявленням і усуненням.

Ключовою функцією рішення SIEM є агрегація даних та управління журналами: збір, нормалізація і зберігання даних журналів з різних джерел, включаючи сервери, мережі, програми та кінцеві пристрої, об'єднуючи їх в єдину платформу з можливістю пошуку.

Також реалізовано функцію кореляції та аналітики подій: система пов'язує пов'язані події в різних системах для виявлення закономірностей та потенційних загроз безпеці (наприклад, зіставлення невдалого входу з попередженням брандмауера).

Великою перевагою є реалізація негайних сповіщень аналітикам про потенційні інциденти безпеки через панелі інструментів, що дозволяє швидше ідентифікувати загрози.

Реалізовані також експертна система штучного інтелекту та машинне навчання (UEBA). Сучасні SIEM-системи включають аналітику поведінки користувачів та сутностей (UEBA) для виявлення аномальної поведінки та автоматизації ручних процесів.

2.2 Оцінка ефективності використовуваних підходів управління ризиками.

Відповідно до Постанови НБУ №95 банки повинні забезпечити:

- управління ризиками інформаційної безпеки, а саме регламентувати процес ідентифікації, оцінки та управління ризиками, пов'язаними з інформаційною безпекою;
- безперебійність банківської діяльності шляхом встановлення вимог до резервного копіювання даних та відновлення банківської діяльності в разі виникнення непередбачених ситуацій. Банківська установа має забезпечити спроможність своєчасно та ефективно виконувати критичні операції та послуги в штатному режимі функціонування інфраструктури в надзвичайних ситуаціях.

З цією метою банки розроблюють Плани безперервності діяльності (Business Continuity Plan) і Плани відновлення штатного режиму роботи інформаційних систем після катастроф (Disaster Recovery Plan).

Ключовими елементами управління безперервністю діяльності банку є:

1)розробка і затвердження стратегії безперервності діяльності;
2)визначення кіберінцидентів (природні катастрофи, припинення подання електроенергії, терористичні акти тощо), настання яких впливає на безперервність діяльності платіжної інфраструктури;
3) створення робочих груп з управління процесами у разі настання кіберзагроз, кіберінцидентів та кібератак, що можуть мати вплив на безперервність діяльності платіжної інфраструктури;
4) можливість швидко забезпечити відновлення діяльності на базі резервного обладнання, локалізованого в територіально віддаленому місці.

Заходи по забезпеченню безперервності банківської установи, які мають виконуватись відповідними службами банку:

1) створення детальної схеми комплексу програмно-апаратних засобів із описом функціонального призначення і взаємозв’язків його компонентів;
2) визначення переліку критично важливих компонентів комплексу програмно-апаратних засобів та особливо важливих даних, необхідних для надання послуг, та запровадження політики їх резервування й відновлення;
3) забезпечення роботи критично важливих компонентів комплексу програмно-апаратних засобів джерелами безперебійного електроживлення;
4) здійснення резервного копіювання баз даних та інших особливо важливих даних;

5) забезпечення моніторингу всіх компонентів комплексу програмно-апаратних засобів, реєстрації та аналізу інцидентів, пов’язаних із порушенням безперервності діяльності;

6) визначення порядку внесення змін до програмного забезпечення та конфігурації всіх компонентів комплексу програмно-апаратних засобів;

7) здійснення аналізу можливих загроз безперервному функціонуванню комплексу програмно-апаратних засобів,з абезпечення мінімізації їх можливого впливу та планування дій для випадків їх можливої реалізації;

8) зберігання електронних архівів, архівів особливо важливих даних, за місцем знаходженням та додаткового примірника в приміщенні, територіально віддаленому від основного;

9) забезпечення актуалізації Планів безперервності і Плану реагування на кіберзагрози у відповідності до змін в архітектурі інформаційної інфраструктури.

В банківських установах під час планових перевірок ефективності заходів щодо захисту периметру мережі має проводитись тренування щодо відпрацювання заходів Плану реагування на кіберзагрози шляхом виконання періодичних тестів на проникнення та захищеності мереж та систем; перегляд і оцінювання ефективності налаштувань параметрів безпеки.

З метою упередження кіберінцидентів підрозділи ІБ на постійній основі здійснюють наступні превентивні заходи:

- оновлення баз системи захисту від зловмисного коду:
- оновлення спеціалізованого програмного забезпечення:
- налаштування політики доступу до мережі Інтернет і до інформаційних систем банку:
- моніторинг подій ІБ:
- навчання персоналу.

Всі працівники банку мають бути відповідальними за своєчасне повідомлення про інциденти безпеки інформації та кіберінциденти до служби управління інформаційної безпеки, а також, у разі потреби, за допомогу у визначенні та впровадженні рішення щодо обробки таких подій. Внутрішніми політиками з інформаційної безпеки має бути передбачено, щоб усі працівники Банку мали доступ до відповідних програмних інструментів з метою забезпечення:

- фіксування подробиць подій, всієї необхідної інформації, в тому числі про носії інформації, які можуть вказувати на кіберінцидент;

- повідомляти про всі виявлені кіберінциденти безпосередньому керівнику і відповідним службам (управління інформаційної безпеки, управління ризик-менеджменту);
- вживати всіх можливих заходів безпеки з метою запобігання кіберінцидентам.

Управління операційними ризиками (в тому числі кіберризиками) за методикою НБУ базується на створенні комплексної системи, що включає організаційну структуру, внутрішні політики, культуру ризиків, інформаційні системи та методи контролю (мінімізації збитків). Це передбачає ідентифікацію, оцінку, моніторинг та заходи зменшення ризиків, пов'язаних з персоналом, процесами, системами або зовнішніми подіями, включаючи кіберризики та комплаєнс-ризик (відповідність нормам законодавства і галузевого Регулятора).

Загальний алгоритм побудови організаційної платформи системи (технології) управління кіберризиками.

Відповідно до п.130 постанови НБУ №95 банківська установа перш за все зобов'язана упровадити процес управління інцидентами безпеки інформації та розробити і затвердити внутрішні документи, які містять описи дій стосовно:

1) виявлення інцидентів;

2) інформування про інциденти, у тому числі відповідальної особи за інформаційну безпеку, підрозділу з безпеки інформації та працівників банку;

3) класифікації інцидентів та оцінки негативного впливу (збитку), нанесеного банку інцидентом;

4) реагування на інциденти.

Внутрішні бази, в яких зберігається інформація по зареєстрованих зверненнях користувачів про зупинку сервісів, помилки або збої в роботі інформаційних систем, зафіксованих фахівцями з ІБ або ІТ, та зафіксованих кіберінцідентах, є джерелами даних для визначення потенційного рівня кіберризиків, класифікованих за критеріями, визначеними внутрішніми політиками (документами) банку. Такими системами є програмні додатки реалізації Сервіс-Деску, ряд аналітичних систем, таких як QlikSense та інші, що впроваджуються банками в якості інструментів бізнес-аналітики та інтерактивної візуалізації даних.

Відповідно до Постанови НБУ № 64 загальна система управління ризиками повинна мати трьохрівневу структуру управління, що з точки зору регуляторного

органу - НБУ, є найбільш ефективною для забезпечення контрольованого і ефективного процесу управління ризиками.

За моделлю трьох ліній захисту система управління ризиками в банках України є розподіленої за функціоналом та зонам відповідальності:

- бізнес-підрозділи банку, які зобов'язані виявляти і оцінювати ризик, впроваджувати управлінські заходи з мінімізації ризику, своєчасно звітувати щодо обробки виявлених ризиків;
- профільний підрозділ з управління ризиками;
- служба внутрішнього аудиту, яка виконує оцінку ефективності системи управління ризиками.

Технологію управління кіберризиками можливо реалізувати окремими сервісами прикладної системи, в якій забезпечується життєвий цикл поетапного процесу управління кіберризиками (Рисунок 1):

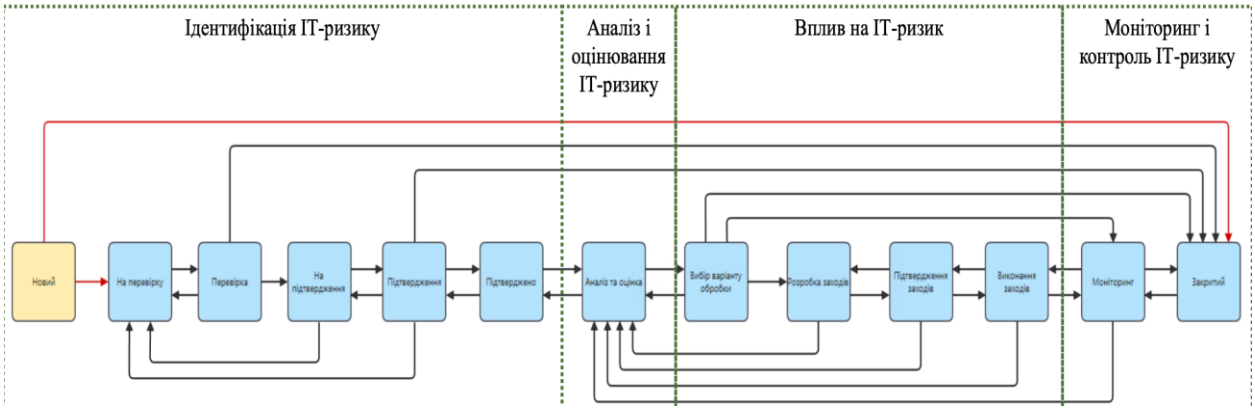

Рисунок 1. Життєвий цикл процесу управління кіберризиками в інформаційний системи прикладного рівня.

Загальна схема автоматизованого процесу управління кіберризиками має включати складові, що наведені нижче:

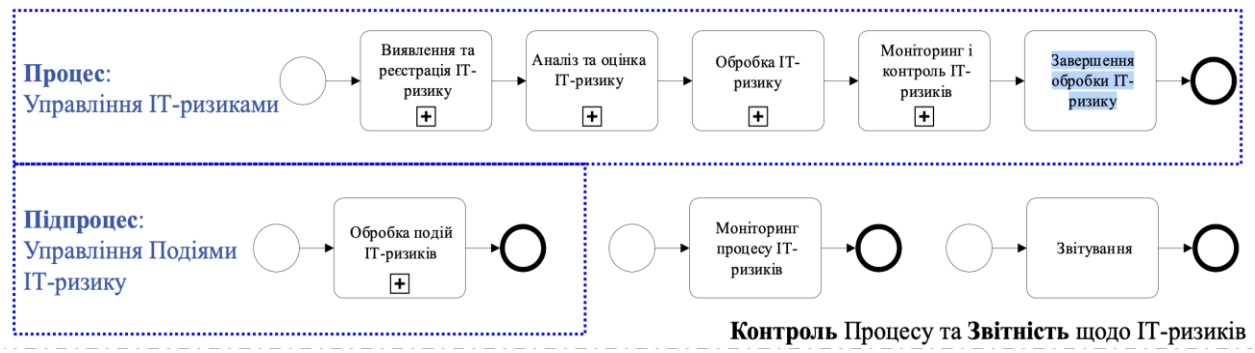

Рисунок 2. Етапи процесу управління ризиками

Відповідно до нормативних актів НБУ банківські установи в системі управління ризиками мають забезпечити функціональний розподіл і зони відповідальності учасників процесу.

Реалізація в прикладній інформаційній системі.

В системі ведення бази даних по кіберризиках впроваджується рольова модель розподілу повноважень учасників процесу управління ризиками, приклад якої в таблиці 2.1:

Таблиця 2.1.Ролі процесу

№ з/п	**Назва ролі**	**Короткий зміст**
1	Власник процесу	Визначає стратегію, призначає відповідальних за пидпорядкованими ролями (2-13), здійснює контроль за своєчасністю і якістю робіт
2	Менеджер процесу	Керівник ІТ-підрозділу, який визначає шляхи и методи управління ІТ-ризиками
3	Власник ІТ-ризику	Підрозділ або особа, яка організовує процес обробки і виконує контроль і якість виконання
4	Менеджер ІТ-ризику	Здійснює загальне керування процесом усунення інциденту/проблеми
5	Координатор ІТ-ризику	Відповідальний за процес управління ризиками окремого підрозділу *служби* ІТ
6	Реєстратор ІТ-ризику	Спеціаліст підрозділу ІТ, відповідальний за внесення показників за виявленим ризиком в БД
7	Відповідальний за контроль	Спеціаліст підрозділу ІТ
8	Експерт за напрямком (ІТ)	ведучий спеціаліст/менеджер у відповідній області ІТ-галузі (телекомунікаційні, прикладні, операційні системи, архітектура інші)
9	Експерт операційних ризиків	Фахівець підрозділу управління ризиків
10	Відповідальний за захід	Фахівець підрозділу ІТ, що здійснює контроль якості виконання заходів по усуненню інциденту
11	Виконавець заходу	Фахівець підрозділу, який виконує дії по вирішенню проблеми/інциденту
12	Відповідальний за надання значень KRI	На періодичній основі розраховує індикатор ризику на певну звітну дату і надає ці дані до підрозділу управління ризиками

№ з/п	Назва ролі	Короткий зміст
13	Реєстратор події ІТ-ризику	Працівник ІТ-підрозділу, призначений відповідним внутрішнім розпорядженням

База даних по кіберризикам є компонентом загальної бази ризиків банку. Наступним етапом процесу є розрахунок профільним підрозділом банку з управління ризиками індикаторів ризику, ризик-апетиту в цілому по банківській установі.

Представлена програмна реалізація технологічного процесу обробки кіберризиків є ефективною з точки зору повноти інформації по виявленим ризикам, оперативного прийняття заходів по усуненню і мінімізації ризиків, розробки управлінських рішень щодо впровадження додаткових або модифікації існуючих технічних рішень з інформаційної безпеки.

Для збільшення ефективності процесу управління кіберризиками банківськими фахівцями залучаються сучасні міжнародні практики і стандарти, що орієнтовані на мінімізацію потенційних фінансових і репутаційних втрат.

Аналіз міжнародних практик і моделей.

За результатами дослідження сучасних методів та моделей оцінювання кіберзахисту критичної інформаційної структури було виявлено, що в банках в практиці найчастіше використовуються метод мозкового штурму (Brainstorming), методики FMEA, HAZOP, Checklist, SWIFT. Ці інструменти є допомогою в процесах оцінки ризиків кібербезпеки, ідентифікації і категоризації ризиків, ідентифікації потенційних загроз, реагування на кіберінциденти, відновлення стану кібербезпеки, кіберахисту та кіберстійкості інформаційної інфраструктури.

Результативність дослідження доводіть, що такі методи, як аналіз вразливостей, оцінка кіберризиків та розробка стратегій відновлення функціонування елементів інформаційної інфраструктури, допомагають знижувати потенційні наслідки кіберінцидентів.

Проведено аналіз наступних методів:

1) Метод мозкового штурму (Brainstorming). Використовується в кібербезпеці в процесах ідентифікації ризиків та розробки стратегій відновлення після інцидентів. Під час ідентифікації ризиків кібербезпеки, Brainstorming дозволяє учасникам ефективно генерувати ідеї, що виявляють нові та недооцінені загрози, що є критично важливим у динамічному полі кіберзагроз. Для розробки

механізмів кіберзахисту, цей метод сприяє обговоренню та випробуванню стратегій захисту, що підвищує стійкість систем. Мозковий штурм необхідний для планування систем виявлення та моніторингу, дозволяючи визначити ключові показники для контролю аномалій. В контексті реагування на кіберінциденти, метод сприяє швидкій розробці стратегій реагування, обговоренню негайних дій для мінімізації наслідків кібератак, а також плануванню довгострокових заходів для запобігання подальшим інцидентам. Мозковий штурм використовується також для визначення стратегій відновлення та посилення кібербезпеки після атаки, зокрема через відновлення критичних служб та впровадження змін для підвищення загальної стійкості системи.

2) Метод HAZOP (Hazard and Operability Study) є технікою, суть якої полягає в систематичному підході до ідентифікації ризиків. Метод забезпечує аналіз можливих відхилень в роботі системи від норми, що дозволяє виявляти потенційні ризики або недоліки в безпеці.

Використання HAZOP ефективно при оцінці складних інформаційних систем та мереж, де потрібно розглянути широкий спектр потенційних загроз та вразливостей. Застосування HAZOP для ідентифікації ризиків кібербезпеки дозволяє проводити глибокий аналіз можливих небезпек, які можуть виникнути через неправильне конфігурування системи або через зовнішні атаки. Задля вдосконалення кіберзахисту, HAZOP може використовуватися для планування заходів з підвищення безпеки, виявлення слабких місць у безпеці, та розробки відповідних заходів реагування. Такий підхід допомагає забезпечити максимальну захищеність систем від можливих атак та відмов.

За цим методом розроблюються детальні процедури для виявлення і реагування на аномалії в системі, а також ефективні стратегії швидкого відновлення штатного режиму функціонування інформаційних систем, мінімізуючи час їх простою та фінансові втрати банку.

3).Метод HACCP (Hazard Analysis and Critical Control Points). Ефективність методу полягає в можливості розробки схем ідентифікації критичних точок у IT-інфраструктурі, де потенційні ризики або вразливості можуть негативно вплинути на операційну діяльність організації, що дозволяє розробити заходи для її захистуЗастосування методу HACCP допомогає встановити систему постійного оцінювання та вдосконалення заходів безпеки, що є фундаментом для забезпечення довгострокової кіберстійкості інформаційних систем.

4).Метод SWIFT (Structured What-If Technique) - це ефективний аналітичний інструмент, призначений для ідентифікації потенційних ризиків в системах або

технологічних процесах шляхом структурованого обговорення сценаріїв “що, якщо”. Ця техніка в кібербезпеці дозволяє оцінити можливі наслідки різних відхилень у роботі інформаційної системи, виявляючи таким чином потенційні уразливості і вектори атак, яки ще не були розглянуті. SWIFT дозволяє ідентифікувати та розробляти стратегії мінімізації ризиків для критичних точок системи. Це, в свою чергу, допомагає підвищити загальну безпеку інформаційних систем та забезпечити більш ефективний захист від можливих кібератак.

Засоби кіберзахисту, регламентовані галузевим Регулятором.

Загальні інструменти захисту інформаційної інфраструктури, заходи і засоби безпеки визначено статтями Постанови НБУ №95. Банківські установи зобов'язані впровадити і підтримувати в актуальному, робочому стані наступне:

- в бездротових мережах згідно статті 102 необхідно забезпечити використання в бездротових мережах банку режиму безпеки WPA2-Enterprise (корпоративний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) та використання режиму безпеки WPA2-Personal (персональний режим у наборі алгоритмів і протоколів Wireless protected access версії 2) для реалізації гостьових підключень.

- для організації віддаленого доступу до інформаційних систем банку згідно ст.103 необхідним є застосовування таких заходів безпеки інформації:

1) розміщення серверу (серверів) віддаленого доступу до інформаційних систем банку в демілітаризованій зоні (DMZ) мережі банку, з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

2) шифрування каналів зв'язку для доступу до сервера віддаленого доступу до інформаційних систем банку;

3) багатофакторна автентифікація користувачів.

- для захисту внутрішньої мережі банку згідно ст.104 необхідно забезпечити розмежування доступу між мережею банку і публічною мережею з використанням міжмережевих екранів та/або пристроїв уніфікованого управління загрозами; а також відповідно до ст.106 банк зобов'язаний забезпечити доступ з публічної мережі до мережі банку виключно із застосуванням захищених з'єднань.

- забезпечити відповідно до ст.144 шифрування каналів передавання даних між серверами СУБД і серверами застосувань або шифрування даних, що передаються між серверами СУБД і серверами застосувань банку.

Відповідно до ст.133 Банку забороняється використовувати радіотелефони та/або радіоподовжувачі телефонної лінії без активованих у них алгоритмів шифрування сигналу, який передається радіоканалом.

Засоби захисту поштового трафіку.

Відповідно до статей 120-123 Постанови НБУ №95 банки зобов’язані встановити засоби перевірки і захисту всіх повідомлень, що обробляються сервером застосувань електронної пошти, на наявність зловмисного коду.

Необхідно впровадити періодичне тестування захищеності та перегляд налаштувань параметрів безпеки операційної системи сервера застосувань електронної пошти та безпосередньо сервера застосувань електронної пошти. До цього ж сервер застосувань електронної пошти Банк зобов'язаний розміщувати на окремому фізичному або віртуальному сервері.

У разі використання віддаленого доступу до сервера застосувань електронної пошти банк зобов'язаний запровадити наступні заходи безпеки інформації:

1) сервер має бути розміщений в демілітаризованій зоні мережі банку з обмеженням доступу до нього з публічної мережі за допомогою міжмережевого екрана або пристрою уніфікованого управління загрозами;

2) доступ до сервера електронної пошти має надаватись лише шифрованими каналами зв'язку.

Для сервера електронної пошти банк зобов'язаний запровадити наступні заходи безпеки інформації:

1) використовувати міжмережевий екран операційної системи сервера електронної пошти для обмеження доступу до сервера;

2) заблокувати отримання вхідних повідомлень від серверів мережі Інтернет, що розсилають спам;

3) упровадити процес постійного моніторингу вразливостей сервера застосувань електронної пошти та клієнтського програмного забезпечення доступу до сервера застосувань електронної пошти, забезпечити встановлення відповідних оновлень, що усувають виявлені вразливості.

Засоби безпеки інформаційних систем.

Для всіх інформаційних систем банк зобов'язаний визначити та задокументувати вимоги безпеки інформації під час розроблення, модернізації (у тому числі їх компонентів) або в разі придбання систем (ст.124).

Відповідно до статті 125 на стадії розроблення і тестування інформаційних систем та/або їх компонентів банк зобов'язаний використовувати тестову програмно-апаратну платформу, яка підключена до окремого (тестового) виділеного сегмента мережі банку. В тестовому середовищі мають оброблюватись виключно знеособлені дані.

На стадії експлуатації інформаційних систем банк зобов'язаний задокументувати положення щодо:

1) контролю функціонування реалізованих в інформаційних системах банку заходів безпеки інформації, уключаючи контроль реалізації організаційних заходів та контроль складу і параметрів налагодження технічних засобів безпеки інформації;

2) контролю вразливостей в обладнанні та програмному забезпеченні інформаційних систем банку;

3) контролю конфігурації програмного забезпечення інформаційних систем банку;

4) відновлення всіх реалізованих заходів щодо забезпечення безпеки інформації в інформаційних системах банку після збоїв у роботі внаслідок інцидентів безпеки інформації (ст.127).

Відповідно до статті 128 внесення змін до параметрів налаштування ІБ в інформаційних системах повинно бути закріплено в якості функціонального обов'язка працівників банку, які здійснюють адміністрування цих систем.

Банк також зобов'язаний задокументувати та впровадити порядок виведення з експлуатації обладнання інформаційних систем банку, який має містити опис процесу видалення інформації з таких систем, використовуючи алгоритми та/або методи, що забезпечать неможливість її відновлення, що є по суті превентивним заходом ІБ.

Відповідно до статті 105 в рамках процесу управління інцидентами безпеки інформації банки зобов'язані обробляти виявлені атаки або вторгнення до мережі банку.

Для забезпечення вимог Регулятора банківськими установами розроблюються відповідні методології, які будуються комплексної оцінки кіберризиків з врахуванням всіх наявних даних та метрик безпеки, а також кореляції з існуючими факторами ризику, профілем потенційних загроз, та орієнтацією на аспекти практичної імплементації та застосування в корпоративному середовищі розподіленої інформаційної інфраструктури.

Методологія може мати метрико-орієнтовний характер з використанням метрики безпеки, яка є універсальним формалізованим критерієм для оцінки стану безпеки інформаційної системи та ефективним механізмом управління та контролю. Поняття «метрики безпеки» передбачає застосування кількісного, статистичного та математичного аналізу для вимірювання ключових показників безпеки, в тому числі, які виражені у фінансовому еквіваленті потенціних втрат чи вартості відновлення компонентів інформаційної системи. За методологією виділяється набір універсальних атрибутів, актуальних для розподіленої системи і в сукупності які можуть характеризувати рівень захищеності ІТ-активу. Метрика безпеки (або комбінація метрик) являє собою кількісну міру відповідного атрибуту, яким дана система, інший ІТ-актив володіє.

Стандартизовані метрики безпеки та інтегровані показники забезпечують можливість моніторингу, контролю та подальшого аналізу стану інформаційної інфраструктури.

Показниками окремого інформаційного / мережевого активу можуть бути:

– тип та категорія пристрою;

– тип розгортання пристрою (фізичний / віртуалізація);

– кількість виявлених вразливостей;

– тип середовища функціонування активу (продуктивне, тестове);

– наявність зареєстрованих інцидентів ІБ в минулому (врахування ретроспективних
даних);

– дата-час останньої активності об’єкту;

– наявність та тип антивірусного ПЗ;

– дата-час останнього оновлення сигнатур / агента;

– статус застосування політик ІБ;

– статус підключення об’єкту до SIEM / DLP тощо;

– дата-час останнього сканування вразливостей.

Відбір метрик безпеки при цьому враховує аспекти комплексної оцінки, уніфікації процедури аналізу та врахування актуальних факторів ризику, які притаманні розподіленій інфраструктурі. Для цього застосовується профіль ключових факторів кіберризику сучасних розподілених комп’ютерних мереж і систем, які можуть спричинити потенційні кіберінциденти. Це забезпечує системний підхід до аналізу факторів ризику, ідентифікації впливу загроз і визначення заходів підвищення стійкості систем и мереж до можливих кібератак.

Окрім цього, метод розробки і застосування профілю ключових факторів кіберризику враховує кореляційний аналіз та моделювання взаємозв'язків факторів ризику, а також визначає та структурує основні заходи та контролі інформаційної безпеки.

За цією методикою оцінювання ризику за кількісними показниками враховує критичність та число ідентифікованих вразливостей для кожного ІТ-активу відповідно до їх класу у CVSS score відкритої системи класифікації та ранжування вразливостей Common Vulnerability Scoring System (CVSS).

За методикою також визначається ваговий коефіцієнт рівня критичності ІТ-активу, який визначається на основі профілювання активів за типами та ранжування їх за важливістю для бізнес-процесів відносно шкали W. Відповідно до запропонованого підходу він може набувати значень наведених в Таблиці 2.2.

Таблиця 2.2.Профілювання ІТ-активів за типами

Профілювання ІТ-активів за типами

Рівень критичності	W_i	*Приклад*
Низький	1	Пристрої системи корпоративного відеонагляду та IP-телефонії, принтери / сканери / багатофункціональні пристрої / IOT тощо
Середній	2	Мережеве обладнання, робочі станції / персональні комп'ютери, ноутбуки, планшети, тонкі клієнти тощо
Високий	3	Сервери
Критичний	4	Касові апарати, платіжні термінали, реєстратори розрахункових операцій тощо

Такий підхід дозволяє врахувати потенційні наслідки та критичність настання інцидентів ІБ відносно категорії активу та ступеню його пріоритетності для інфраструктури.

Розроблений метод, інтегруючи метрико-орієнтовний підхід, може бути рекомендований для використання в сучасних розподілених ІТ-системах для комплексного аналізу ризиків ІБ, а також для оцінки ефективності системи захисту інформації. Методологія метрико-орієнтованого типу ефективна при побудові прикладних програмних модулів або сервісів підтримки прийняття рішень, що автоматично формують інтегральні показники ризику, виявляють закономірності та аномалії в даних і пропонують рекомендації з оптимального впровадження захисних заходів, що сприяє покращенню якості, швидкості та прозорості процесів управління безпекою.

Запропонований підхід надає можливість створити масштабовану, адаптивну та динамічну систему управління кіберризиками, яка ефективно реагує на сучасні кіберзагрози.

3. РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ РИЗИКАМИ В БАНКІВСЬКІЙ СФЕРІ

3.1. Рекомендації щодо методів управління ризиками в банківській структурі

Загальною умовою для побудови та функціонування ефективної і адекватної системи управління кіберризиками є дотримання норм законодавства, положень НБУ у сфері інформаційної безпеки і управління ризиками.

Розробка внутрішніх систем управління кіберризиками і управління кібербезпекою повинна будуватись на основі нормативно-правової бази НБУ, в якій вже закладено ефективні механізми керування процесами виявлення, обробки і оцінки кіберризиків, побудови превентивних заходів кібербезпеки, методів і засобів контролю безпеки критичних компонентів інформаційної інфраструктури .

Одним з ефективних методів управління кіберизиками є розробка, впровадження і підтримка в актуальному стані системи превентивних заходів безпеки в інформаційній банківській інфраструктурі, що мінімізує рівень кіберризику і збільшує рівень кіберстійкості інформаційних систем.

За результатами дослідження технологій управління ризиками, програмно-технічних засобів інформаційної безпеки, головними заходами по забезпеченню захисту інформаційних активів критичної інфраструктури банків повинні бути наступні:

- безпечна побудова серверної частини;
- здійснювання регулярного оновлення програмного і апаратного забезпечення всіх елементів інфраструктури;
- тестування навантаження комп’ютерної мережі, серверного обладнання, інших компонентів інфраструктури;
- проведення аналізу коду використовуваних бібліотек;
- проведення аналізу коду прикладних програм;
- ідентифікація вразливостей шляхом сканування;
- проведення регулярного аудиту системи інформаційної безпеки.

Для ефективної системи управління кіберризиками рекомендується розробити відповідну методику оцінки ризику інформаційної безпеки, основними складовими якої мають бути:

- регламентація послідовності кроків зі збору вхідних даних, їх обробки та інтерпретації, розрахунку рівнів ризиків інформаційної безпеки,
- процедури пріоритизації і ранжування ризиків;
- визначення основних етапів і принципів виконання процедури самостійної оцінки ризиків інформаційної безпеки, механізмів та засобів їх контролю профільними підрозділами банку.

Методику необхідно розроблювати з урахуванням міжнародних стандартів та світових практик в області управління інформаційною безпекою та управління ризиками, керуючись основними положеннями НБУ та відповідати вимогам чинного законодавства України.

На етапі оцінки та обробки ризиків необхідно виходити з розуміння того, що ризик реалізується коли:

1) активи банку не захищені від фінансових втрат,
2) існує недотримання політик та процедур банку, законодавства, нормативних актів та стандартів в сфері ІБ,
3) конфіденційність, цілісність і доступність інформації не є надійними.

Загальною метою практичного застосування методики з оцінки ризиків є формування інформації про кіберризики, сценарії прояву цих ризиків, кіберзагрози та їх джерела, визначені вразливості щодо цих загроз, рівень потенційного впливу цих загроз та рівень ймовірності прояву даного впливу на діяльність банку з врахуванням діючих засобів та механізмів контролю.

Вхідними даними для здійснення оцінки кіберризиків мають бути:

1) перелік технологічних і бізнес-процесів банку,
2) актуальний перелік інформаційних активів,
3) результати аналізу впливу негативних факторів на такі процеси,
4) перелік процесів, автоматизацію яких забезпечують програмно-технічні засоби обробки інформації,
5) результати попередніх оцінок кіберризиків,
6) аудиторські звіти перевірки СУІБ, системи управління ризиками,
7) інформація щодо подій кіберризику,
8) інформація щодо кіберінцидентів,
9) переліки виявлених та типових вразливостей ІБ,
10) результати здійснених тестувань безпеки інформаційних систем,
11) переліки вимог до контролів ІБ,
12) міжнародні практики щодо ІБ,

13) консультації та/або рекомендації постачальників ІТ послуг та/або послуг ІБ,
14) інформація про реалізовані засоби контролю ІБ та ті, що знаходяться на етапі впровадження/розгортання.

Для оцінки кіберризиків можливо застосувати один, або одночасно два наступних підходи щодо ідентифікації, подальшого аналізу та оцінки ризиків, які ґрунтуються на аналізі потенційних, або вже реалізованих сценаріїв прояву ризику:

- підхід на основі активів, який заснований на визначенні операційних сценаріїв, деталізованих з точки зору наявних інформаційних активів, загроз і вразливостей, їм притаманних. Такий підхід до оцінки ризиків ІБ використовується у разі необхідності оцінити ризики ІБ, під вплив яких підпадають конкретні інформаційні активи у визначеній області оцінки ризиків (наприклад, інформаційні системи, сервіси, ресурси, що підтримують певний процес, компоненти інформаційних систем, інформаційні технології);
- підхід на основі сценарію, за яким визначаються стратегічні сценарії прояву ризику ІБ та його негативний вплив, в цілому, на критичні з точки зору ІБ процеси банку, шляхом розгляду джерел ризику ІБ. Такий підхід до оцінки ризиків ІБ використовується у разі оцінки певної можливої події прояву ризику, що має відбуватись за визначеним сценарієм (наприклад, DDOS, хакерський злам або вірусна атака, збій у центрі обробки даних, комплексний збій ряду критичних компонентів ІТ інфраструктури, зміна ІТ технологій інше).

Оцінювання кіберризиків має виконуватись робочою групою фахівців профільного підрозділу банківської установи з питань ІБ, за необхідності із залученням експертів з підрозділу управління ризиками. Завданнями такої групи є визначення причин і потенційних наслідків виявленого кіберризику, розроблення діючих механізмів та засобів контролю, що мінімізують появу цього ризику ІБ (подію ризику).

Оцінка кіберризиків здійснюється бально-ваговим методом, який являє собою визначення експертним шляхом та/або на основі статистичної інформації окремих характеристик ризику, вираженого в балах, а саме:

1) оцінюється ймовірність реалізації ризику;
2) оцінюється суттєвість наслідків від реалізації ризику;

3) за результатами оцінки ймовірності та суттєвості реалізації ризику ІБ визначається результат оцінки рівня кіберризику.

1).Оцінка ймовірності кіберризику.

Зваженим фактором ризику є визначення величини ймовірності, що є результатом аналізу ймовірності того, що визначена загроза здатна використовувати визначену вразливість (або набір вразливостей). Фактор ризику ймовірності поєднує оцінку ймовірності того, що загроза буде ініційована, з оцінкою ймовірності її впливу. Оцінка ймовірності представляє собою якісну характеристику частоти виникнення загрозливої події, виражену в балах від 1 до 5, кожному з яких відповідає орієнтовний діапазон якісних та кількісних характеристик таблиці 3.1:

Таблиця 3.1. Оцінка ймовірності реалізації ризику ІБ

Значення балу	**Опис**	**Очікувана частота**
1	Дуже низька	Подія ризику ІБ може траплятися вкрай рідко, менше одного разу на рік. Вважається малоймовірною. Приблизна частота: менше одного разу на рік.
2	Низька	Подія ризику ІБ може траплятися рідко, але очікувано протягом року. Приблизна частота: кілька разів на рік або щоквартально.
3	Середня	Подія ризику ІБ може траплятися з помірною частотою, кілька разів на місяць, або щомісяця. Приблизна частота: кілька разів на місяць або щомісяця
4	Висока	Подія ризику ІБ може траплятися часто, регулярно, зазвичай не рідше одного разу на тиждень. Приблизна частота: кілька разів на тиждень або щотижня
5	Дуже висока	Ймовірність виникнення Подія ризику ІБ є практично неминучою, може траплятися регулярно, можливо щодня. Приблизна частота: кілька разів на день або щодня

2) Оцінка суттєвості.

Результатом оцінки суттєвості є отримання комплексної якісної агрегованої характеристики рівня можливих збитків від впливу на конфіденційність (К), цілісність (Ц), доступність (Д), що може понести банк при настанні події несанкціонованого розкриття, несанкціонованої модифікації, знищення інформації або втрати інформації чи доступності інформаційної системи, без урахування діючих механізмів та засобів контролю кіберризику. Кожному такому рівню відповідає орієнтовний діапазон якісних та кількісних характеристик.

3)Оцінка рівня кіберризику.

На підставі здійсненних оцінок ймовірності реалізації події ризику ІБ та суттєвості наслідків ризику ІБ здійснюється розрахунок оцінки рівня кіберризику – таблиця 3.2.

Таблиця 3.2. Матриця оцінки рівня кіберризику

Ймовірність реалізації ризику						
Дуже висока	*5*	5 С	10 В	15 В	20 ОВ	25 ОВ
Висока	*4*	4 С	8 С	12 В	16 ОВ	20 ОВ
Середня	*3*	3 Н	6 С	9 В	12 В	15 В
Низька	*2*	2 Н	4 С	6 С	8 С	10 В
Дуже низька	*1*	1 Н	2 Н	3 Н	4 С	5 С
		1	*2*	*3*	*4*	*5*
		Низький	*Нижче середнього*	*Середній*	*Високий*	*Значний*
		Суттєвість наслідків ризику (вплив)				

Кольорові зони таблиці визначають рівень кіберризику. Кожна з таких зон складається з групи частин однакового кольору за діапазоном значень ризику:

- зона низького ризику («Н») – включає сегменти зеленого кольору, де всі ризики, що потрапили до їх складу, оцінюються як ризик низького рівня (числове значення від 1 до 3);
- зона середнього ризику («С») – включає сегменти жовтого кольору, де всі ризики ІБ, що потрапили до їх складу, оцінюються як ризики середнього рівня (числове значення від 4 до 8);
- зона високого ризику («В») – включає сегменти помаранчевого кольору, де всі ризики, що потрапили до їх складу, оцінюються як кіберризики високого рівня (числове значення від 9 до 15);
- зона особливо високого ризику («ОВ») – включає сегменти червоного кольору, де всі ризики, що потрапили до їх складу, оцінюються як кіберризики дуже високого рівня (числове значення від 16 до 25).

Завершуючим етапом методики є оцінка доцільності, вибір методу управління кіберризиком та формування плану заходів по зменшенню (мінімізації) ризику.

На цьому етапі, в залежності від обраного Методу управління ризиком, відповідальним підрозділом розробляється План заходів щодо мінімізації кіберризику. Вимоги щодо визначення Методу управління ризиком ІБ та необхідності розробки Плану заходів визначені у таблиці 3.3.

Таблиця 3.3. Визначення Методу управління ризиком ІБ та розробка Плану заходів

Оцінка рівня Залишкового ризику ІБ	**Метод управління ризиком ІБ**	**Необхідність розробки Плану заходів**	**Примітка**
Низький Середній	Прийняти	Ні/Так (за необхідності)	План заходів може бути розроблений за необхідності, що визначається самостійно Власником ОР або за обґрунтованою вимогою ДРМ
Високий Особливо високий	Мінімізувати	Так	План заходів розробляється Власником ОР в обов'язковому порядку
	Передати	Так	
	Уникнути		

Метод «прийняти» означає, що ризик утримується на рівні, що перебуває в межах визначеної Банком схильності до ризиків (ризик-апетиту) і не створює загрози для інтересів вкладників, інших кредиторів, власників Банку та фінансової стійкості Банку.

Метод «мінімізувати» означає необхідність впровадження комплексу заходів (коригування певних процесів та впровадження додаткових контролів тощо), спрямованих на зменшення ймовірності виникнення кіберризику та/або зменшення впливу ризику на результати діяльності Банку.

Метод «передати» означає передавання Банком своєї відповідальності за кіберризик іншим особам за винагороду зі збереженням наявного рівня ризику. Передбачає страхування, переважно, ризиків з потенційно значними втратами з низькою імовірністю настання, або ризиків, які перебувають під обмеженим контролем Банку.

Метод «уникнути» означає відмову від здійснення певних операцій або припинення ділових відносин, які наражають Банк на кіберризик і можуть призвести до значних втрат з високою ймовірністю настання.

На основі виявлених ризиків, із визначеним методом управління ризику «мінімізувати», Робоча група або експерти Підрозділу здійснюють опис заходів щодо зменшення виявленого потенційного кіберризику та розроблюють «План заходів для мінімізації ризиків».

Результати процесу обробки і оцінки кіберризиків враховуються в подальших процесах по укріпленню і зміцненню системи кіберзахисту інформаційної інфраструктури банку, а саме:

- в плануванні безперервності бізнесу (Business Continuity Plan) для визначення цілей і пріоритетів, забезпечення рівня залишкових ризиків переривання діяльності в межах затвердженого Банком рівня (показника) ризик-апетиту щодо кожного з видів суттєвих ризиків, встановлених Декларацією схильності до ризиків;
- в плануванні реагування на кіберзагрози, кіберінциденти для адаптації процедур реагування (виявлення, аналіз, стримування, ліквідація, відновлення) залежно від критичності процесів, які постраждали, або можуть постраждати;
- в плануванні відновлення після катастроф (Disaster Recovery Plan) для визначення пріоритетів по відновленню інформаційних систем, що підтримують критичні процеси;
-управління ризиками третіх сторін для фокусування зусиль з належної перевірки (due diligence) та моніторингу постачальників, які забезпечують функціонування критичних процесів.

3.2 Побудова стратегії та опис практичних кроків з впровадження розроблених рекомендацій.

Надані рекомендації реалізуються за Стратегією, яка має бути розроблена банківською установою, і повинна включати цілі, організаційні заходи з питання розбудови ефективної системи управління кіберризиками, які наведені нижче:

1. Визначити організаційну структуру, функціональність і зони відповідальності працівників, які будуть залучені для виконання конкретних задач з управління кіберризиками.

2. Провести організаційні заходи по формуванню робочих груп для виконання процедур, націлених на мінімізацію (зниження рівня) ризиків.
3. Забезпечити придбання автоматизованих засобів (програмних інструментів) обробки інформації по ризиках, зокрема аналітичних систем для систематизації і аналізу даних по кіберінцідентах, аналізу і оцінки рівня кіберзагроз і кіберризиків.
4. Розробити План створення резервного центру обробки інформації, включаючи плани придбання резервного обладнання, програмного забезпечення.
5. Формалізувати процес створення резервних копій інформації і правил, відповідно до яких бази даних відновлюються з резервних копій.
6. Розробити сценарії усунення кіберзагроз. Здійснювати послідуючий контроль їх ефективності, забезпечити внесення коригуючих змін у разі негативного результату їх застосування.
7. Здійснювати щоквартальний розрахунок ключових індикаторів ризику,
8. Організувати процес розробки внутрішніх нормативно-методологічних документів – політик ІБ, методик оцінювання кіберризиків, технологічних інструкцій відповідно до норм законодавства і Регулятора.
9. Встановити внутрішні політики, процедур та заходів контролю за наданням, зміною та скасуванням прав фізичного та логічного доступу працівників до інформаційних систем платіжної інфраструктури; моніторингу та контролю активності привілейованих користувачів і користувачів, що мають доступ до критично важливих інформаційних ресурсів платіжної інфраструктури, з метою виявлення нетипової активності та протиправних дій з їх боку.
10. Розробити та запровадити заходи захисту для виявлення та запобігання несанкціонованим вторгненням до мережі платіжної системи.
11. Забезпечити регулярну перевірку кіберстійкості ІТ-активів інфраструктури шляхом зовнішнього аудиту (за міжнародним стандартом ISAE 3402),
12. Впровадити концепцію керування і контролю якості шляхом укладення угод про рівень обслуговування (Service Level Agreements, SLAs) .
13. З метою прийняття управлінських рішень забезпечити розробку програмно-апаратної бази для ведення бази даних щодо інформації про кіберзагрози шляхом придбання відповідного обладнання і програмного забезпечення.
14. Розробити та на регулярній основі виконувати процедуру оцінки вразливостей кіберстійкості інформаційної інфраструктури за методом систематичної експертизи інформаційної системи та засобів її контролю і процесів з метою визначення адекватності заходів безпеки, виявлення недоліків, надання даних для прогнозування ефективності запропонованих

заходів безпеки та підтвердження їх адекватності після реалізації (ст.9 Методичних рекомендацій).

15. Розробити технологію управління кіберризиками, що складається з трьох основних етапів:

    -аналіз кіберзагроз (встановлення контексту; аудит безпеки; формування концептів сценарію);

    -моделювання сценаріїв (декомпозиція загроз; установка критеріїв; установка оцінок імовірностей значень концептів (змінних); побудова архітектури мережі; формування приватної моделі загроз; аналіз сценаріїв);

    -оцінювання ризиків.

16. Розробити і впровадити програму навчання персоналу за напрямками кібербезпеки, управління ризиками.

Запропонований підхід до управління ризиками кібербезпеки забезпечує виявлення вразливостей та оцінку ризиків і спрощує розробку управлінських рішень.

ВИСНОВКИ

У ході виконання дипломної роботи було досліджено та проаналізовано сучасні підходи до управління кіберризиками в банківських установах України в умовах зростання кількості та складності кіберзагроз. Основну увагу приділено нормативно-правовому, організаційному та технологічному забезпеченню систем кібербезпеки банків.

У роботі здійснено аналіз чинної нормативно-правової бази Національного банку України, що регламентує питання інформаційної безпеки та управління кіберризиками в банківських установах. Встановлено, що дотримання вимог і методик, визначених нормативними актами НБУ, є ключовою передумовою побудови ефективної та стійкої системи управління кіберризиками і кіберзахисту інформаційної інфраструктури банків.

Досліджено сучасні тенденції розвитку інформаційних технологій та програмно-апаратних засобів кіберзахисту, які використовуються для захисту критичної інформаційної інфраструктури банківських установ. Визначено, що при формуванні довгострокових стратегій розвитку систем кібербезпеки банки повинні враховувати динаміку розвитку цифрових технологій, ускладнення архітектури інформаційних систем та появу нових класів кіберзагроз.

У межах роботи розглянуто сучасні методи та моделі виявлення, оцінювання та обробки кіберризиків, а також підходи до аналізу і класифікації вразливостей. Обґрунтовано доцільність використання комплексного підходу до управління кіберризиками, що поєднує технічні, організаційні та аналітичні заходи з метою мінімізації можливих негативних наслідків кіберінцидентів.

Проаналізовано можливості впровадження сучасних програмно-технічних засобів кіберзахисту, зокрема систем управління вразливостями (Vulnerability Scanner), систем моніторингу та аналізу подій безпеки (SIEM). Показано, що застосування таких рішень дозволяє підвищити рівень виявлення кіберзагроз, своєчасно реагувати на інциденти та здійснювати пріоритизацію ризиків.

Окрему увагу приділено питанням тестування на проникнення як ефективного інструменту оцінки стану захищеності інформаційної інфраструктури банків. Встановлено, що регулярне проведення таких тестів дає змогу своєчасно виявляти слабкі місця в архітектурі мереж, конфігураціях систем, веб- та мобільних застосунках і вживати коригувальних заходів для підвищення загального рівня кібербезпеки.

У роботі обґрунтовано доцільність інтеграції систем управління кіберризиками з рішеннями класу SIEM та SOAR, що забезпечує автоматизацію процесів аналізу подій безпеки, управління інцидентами та реагування на кіберзагрози в режимі реального часу.

Також розглянуто організаційні заходи з планування та забезпечення безперервності діяльності банків, зокрема розробку, впровадження та регулярне тестування планів відновлення критичних систем. Доведено, що дотримання вимог нормативних документів НБУ у цій сфері дозволяє банкам ефективно визначати пріоритети та забезпечувати стійкість бізнес-процесів у разі виникнення кіберінцидентів.

Отримані в роботі результати можуть бути використані банківськими установами для вдосконалення систем управління кіберризиками, підвищення рівня інформаційної безпеки та захисту критичної інформаційної інфраструктури в умовах сучасних кіберзагроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" (№ 80/94-ВР від 5 липня 1994 року)/
2. Закон України «Про банки та банківську діяльність» від 07 лютого 2000 року № 2121-III.
3. Закон України «Про інформацію» від 02 жовтня 1992 року №2657-XII.
4. Закон України «Про захист персональних даних» від …
5. Наказ Адміністрації Держспецзв'язку від 06.10.2021 No 601 "Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури"
6. Постанова НБУ № 95 "Про затвердження Положення про захист інформації та кібербезпеку в банківській системі України" (від 28 серпня 2018 року) https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
7. Постанова НБУ № 473 "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банках України" (від 16 листопада 2015 року)
8. Постанова НБУ № 243 "Про затвердження Правил організації захисту електронних банківських документів» (від 14 червня 2004 року)
9. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910
10. Гончар, С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія / С.Ф. Гончар. – К.: Альфа Реклама, 2019. – 176 с. ISBN 978-966-288-263-6
11. Іванченко, Є. В., Корченко, О. Г., Бакалинський, О. О., Мялковський, Д. В., Верба, Д. В., Зубков, Д. А., Юдіна, Д. О. Модель системи характеристик даних для оцінювання заходів кіберзахисту в Україні. Український науковий журнал інформаційної безпеки: том. 30 No 1, (2024).
12. ISO/IEC 27001:2022 URL https://www.iso.org/standard/27001
13. ISO/IEC 27005:2022 URL https://www.iso.org/standard/80585.html
14. Закон України «Про банки та банківську діяльність» URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text
15. Інформаційна безпека банків: шляхи розв'язання проблеми. URL: https://journal.bank.gov.ua/archive/2010/5.pdf#page=3

ДОДАТКИ

Додаток А: Таблиця 1.5. Перелік кіберінцидентів за класифікацією MISP

Код	Категорія інциденту	Назва інциденту	Назва інциденту в MISP
01.	Шкідливий (образливий) вміст (Abusive content)	Спам	Spam
		Образливий контент	Harmful Speech
		Шкідливий контент	Child/Sexual/Violence/…
02.	Шкідливий програмний код (Malicious Code)	Вірус	Virus
		Хробак	Worm
		Троян	Trojan
		Шпигунське програмне забезпечення	Spyware
		Діалер	Dialer
		Руткіт	Rootkit
		Шкідливе програмне забезпечення	Malware
		Управління ботами	Botnet drone
		Програма-здирник	Ransomware
		Конфігурація шкідливого програмного забезпечення	Malware configuration
		Командно-контрольний центр	C&C
03.	Збір інформації зловмисником (Information Gathering)	Сканування	Scanning
		Перехоплення і аналіз мережевого трафіку	Sniffing
		Соціальна інженерія	Social Engineering
04.	Спроби втручання (Intrusion Attempts)	Експлуатація відомих вразливостей	Exploiting of known Vulnerabilities
		Спроби авторизації	Login attempts
		Експлуатація раніше невідомих вразливостей	New attack signature (exploit)
05.	Втручання (Intrusion)	Компрометація привілейованого облікового запису	Privileged Account Compromise
		Компрометація непривілейованого облікового запису	Unprivileged account compromise
		Компрометація застосунку	Application compromise
		Бот	Bot
		Дефейс	Defacement
		Компрометація системи	Compromised
		Бекдор	Backdoor
06.	Порушення доступності (Availability)	Атака на відмову в обслуговуванні	DoS
		Розподілена атака на відмову в обслуговуванні	DDoS
		Саботаж, диверсія	Sabotage
		Збій без участі зловмисника	Outage, no malice

07.	Порушення властивостей інформації (Information Content Security)	Несанкціонований доступ до інформації	Unauthorised access to information
		Несанкціоноване внесення змін до інформації	Unauthorised modification of information
		Сервер з публічними правами на запис	Dropzone
08.	Шахрайство (Fraud)	Несанкціоноване використання ресурсів	Unauthorized use of resources
		Порушення авторських прав	Copyright
		Маскарадинг	Masquerade
		Фішинг	Phishing
09.	Відома вразливість (Vulnerable)	Вразливості, відкриті для експлуатації	Open for abuse
10.	Інше (Other)	Чорний список	Blacklist
		Недостатньо даних	Unknown
		Інше	Other

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)