МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ПОБУДОВА ТИПОВОЇ МОДЕЛІ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ”

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

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

_____ Максим КОВРИГА
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД-41
Максим КОВРИГА
Ім’я, ПРІЗВИЩЕ

Керівник: Світлана ЛЕГОМІНОВА
Д.е.н., проф. Ім’я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Коризі Максиму Віталійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “ Побудова типової моделі загроз інформаційній безпеці банку”, керівник кваліфікаційної роботи ЛЕГОМІНОВА Світлана, д.е.н., проф.,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій "Про закріплення тем випускних кваліфікаційних робіт та призначення наукових керівників на 2023-2024 н.р. за студентами першого (бакалаврського) рівня вищої освіти". № 36 від 27.02.24

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека банку, методи та засоби захисту ІБ банку, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати теоретичні аспекти загроз ІБ та значення моделі загроз.
   4.2. Дослідити внутрішні, зовнішні та системні загрози інформаційній безпеці банку.
   4.3. Вивчити інструменти та методи захисту ІБ від загроз, розробити практичні рекомендації.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “11“ березня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз теоретичних аспектів загроз ІБ та значення моделі загроз	08.04.2024	
4.	Дослідження внутрішніх, зовнішніх та системних загроз інформаційній безпеці банку.	22.04.2024	
5.	Вивчення інструментів та методів захисту ІБ банку від загроз.	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувач вищої освіти _____ Максим КОВРИГА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувачка Коврига В.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Побудова типової моделі загроз інформаційній безпеці банку"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач КОВРИГА Максим у кваліфікаційній роботі проаналізував теоретичні аспекти загроз ІБ та значення моделі загроз, дослідив внутрішні, зовнішні та системні загрози інформаційній безпеці банку, вивчив інструменти та методи захисту ІБ від загроз, розробив практичні рекомендації за темою дослідження.

КОВРИГА Максим показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача КОВРИГИ Максима на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Коврига М.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти КОВРИГИ Максима
на тему “ Побудова типової моделі загроз інформаційній безпеці банку”

Актуальність.

Швидкий розвиток технологій, зростання кількості цифрових платформ і обсягів оброблюваних даних створюють серйозні виклики для забезпечення інформаційної безпеки банків. Одна з ключових причин актуальності цієї теми - постійне збільшення кількості та складності кіберзагроз. Зловмисники прагнуть використовувати вразливості в системах безпеки для несанкціонованого доступу до конфіденційної інформації, крадіжки даних або впливу на нормальне функціонування банківської установи.

Оцінка ефективності засобів і методів захисту інформації в банках стає стратегічно важливою для забезпечення довіри зацікавлених сторін. Клієнти, партнери та регулятори вимагають від банків доказів того, що їхні дані та системи належним чином захищені від можливих загроз. Важливо, щоб банки постійно контролювали та оцінювали свої засоби і методи захисту інформації, щоб забезпечити їхню актуальність та ефективність у протидії новітнім загрозам.

Значення вимірювання показників управління ризиками та оцінки ефективності заходів безпеки постійно зростає. Комплексний аналіз і оцінка ефективності засобів захисту інформації є критичними аспектами для постійного вдосконалення систем управління ризиками та адаптації до змін у загрозах. Регулярне тестування і аудит систем захисту допомагають виявити слабкі місця та впровадити необхідні покращення для підвищення рівня безпеки інформації у банку.

Позитивні сторони.

Кваліфікаційна робота охоплює важливу та актуальну тему, пов'язану з ефективністю засобів і методів захисту інформації в банках, що відображає значущість цієї проблеми у сучасному цифровому світі. Кваліфікаційна робота вражає глибиною аналізу застосовуваних методик та підходів до оцінки ефективності засобів і методів захисту інформації. Чітко структуровані вступ та висновки роблять роботу добре організованою та логічно зв'язаною. Акцент на рекомендаціях щодо підвищення ефективності захисту інформації в банку є важливим аспектом роботи, що відображає сучасні тенденції у галузі інформаційної безпеки.

Недоліки.

Хоча робота добре структурована, варто розглянути можливість більш детального аналізу окремих методик та їхнього порівняння, щоб надати читачеві глибше розуміння вибору конкретних підходів. Це дозволить визначити найбільш

ефективні та відповідні методи захисту інформації для різних типів банків.

Рекомендацією для майбутнього дослідження може бути розгляд можливості застосування обраної методики управління ризиками на конкретних прикладах чи в реальних умовах банківської діяльності. Такий підхід дозволить оцінити практичну ефективність методів та адаптувати їх до специфічних потреб і умов різних банків, забе

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач КОВРИГА Максим заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
к.т.н., доцент _____ *підпис* _____ Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню побудови типової моделі загроз інформаційній безпеці банку. Робота складається зі вступу, трьох розділів, що містять 4 рисунка, висновків і списку використаних джерел із 46 найменувань. Загальний обсяг роботи становить 62 аркуші, з яких 6 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є побудови типової моделі загроз інформаційній безпеці банку.

Об'єктом дослідження є класифікація загроз інформаційній безпеці банку.

Предмет дослідження – особливості побудови загроз ІБ банку.

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

Як результат у роботі проаналізовано особливості управління інформаційною безпекою банку, досліджено основні загрози ІБ банку; вивчено інструменти та методи побудови типової моделі загроз, розроблено практичні рекомендації.

Галузь застосування. Розроблені підходи можуть бути використані при аналізі та класифікації загроз для побудови моделі загроз у контексті забезпечення захисту інформації.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА БАНКУ, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, МОДЕЛЬ ЗАГРОЗ, ПОБУДОВА МОДЕЛІ ЗАГРОЗ, ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ.

ABSTRACT

The qualification work is devoted to the study of building a typical model of threats to the information security of a bank. The work consists of an introduction, three chapters containing 4 figures, conclusions and the list of references containing 46 items. The total volume of the work is 62 pages, of which 6 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to build a typical model of threats to the information security of a bank.

The object the study is the classification of threats to the information security of a bank.

The subject of the study is the peculiarities of building threats to the bank's IS.

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

As a result, the work analyzed the peculiarities of bank information security management, investigates the main threats to the bank's IS, studies the tools and methods for building a typical threat model, and develops practical recommendations.

Field of application. The developed approaches can be used in the analysis and classification of threats to build a threat model in the context of information security.

Keywords: INFORMATION SECURITY OF THE BANK, INFORMATION SECURITY MANAGEMENT, THREAT MODEL, BUILDING A THREAT MODEL, THREATS TO INFORMATION SECURITY.

ЗМІСТ

ВСТУП

Актуальність теми. У світі, де банки є постійним об’єктом кібератак, забезпечення інформаційної безпеки банку є важливим, як ніколи. Банківська сфера постійно стикається з викликами кіберзлочинців, такими як крадіжка конфіденційної інформації клієнтів, фінансові шахрайства та різні види кібератак. Розробка моделі загроз дозволить банкам систематизувати і класифікувати потенційні загрози, визначати їхні можливі наслідки та розробляти ефективні стратегії захисту

З огляду на зазначене дослідження побудова моделі загроз інформаційної безпеки банку є актуальним науковим завданням.

Мета роботи полягає у дослідженні побудови типової моделі загроз інформаційній безпеці банку.

Об’єкт дослідження – класифікація загроз інформаційній безпеці банку.

Предмет дослідження – особливості побудови загроз ІБ банку.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати теоретичні аспекти загроз ІБ та значення моделі загроз.

2. Дослідити внутрішні, зовнішні та системні загрози інформаційній безпеці банку.

3. Вивчити інструменти та методи захисту ІБ від загроз, розробити практичні рекомендації.

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

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу банкам систематично і комплексно аналізувати потенційні загрози та визначати їх вплив на інформаційну безпеку банку. Натомість цей аналіз дасть можливість банкам побудувати модель загроз ІБ для мінімізації можливих наслідків загроз.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 28 лютого 2024 року.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ

Беручи до уваги стрімкий розвиток технологій та зростаючу комплексність інформаційних систем, проблема забезпечення інформаційної безпеки банків набуває особливого актуальності в контексті сучасного економічного середовища. З урахуванням розмаїтості загроз, що виникають у цій сфері, важливим є ретельний аналіз теоретичних аспектів цього питання. У цьому контексті необхідно вивчити фундаментальні принципи і підходи до забезпечення інформаційної безпеки банківських установ, розглянути основні загрози, які ставлять під загрозу цю безпеку, а також визначити стратегічні напрями її забезпечення. Враховуючи важливість зазначеної проблематики для стабільності банківської системи та довіру громадськості до фінансових установ, дослідження теоретичних аспектів загроз інформаційній безпеці банку є актуальним та перспективним напрямком наукових досліджень.

1.1 Сутність та класифікація загроз інформаційній безпеці банку

Банківська система відіграє ключову роль у фінансовій стабільності та економічному розвитку, забезпечення інформаційної безпеки є важливим завданням для забезпечення довіри клієнтів, захисту конфіденційної інформації та уникнення фінансових втрат. Однак інформаційна безпека банку постійно стикається з різноманітними загрозами, які можуть бути класифіковані залежно від їхнього джерела, характеру та наслідків. У цьому розділі розглянемо сутність загроз інформаційній безпеці банку та їх класифікацію з урахуванням сучасних тенденцій та підходів.

Сутність загроз інформаційній безпеці банку полягає у потенційних небезпеках, що можуть призвести до порушення цілісності, конфіденційності та доступності інформації в банківській системі. Ці загрози можуть виникати як внаслідок зовнішніх атак, так і через внутрішні порушення безпеки, такі як

недбале використання інформації або недостатня кібербезпека. Джерела загроз можуть бути різноманітними, включаючи кіберзлочинців, конкурентів, зловживання співробітників або природні катастрофи[1].

Загрози, які порушують конфіденційність, можуть призвести до несанкціонованого доступу до конфіденційної інформації, такої як особисті дані клієнтів, фінансові та комерційні відомості. Це може викликати серйозні наслідки, включаючи витрати на компенсацію клієнтів, втрату довіри та погіршення репутації банку.

Загрози, що стосуються цілісності даних, можуть призвести до випадкового або навмисного внесення змін у банківську інформацію, що може призвести до недостовірних фінансових звітів, втрати даних або збоїв у функціонуванні банківської системи.

Загрози для доступності інформації можуть призвести до тимчасового або постійного втрати доступу до важливої інформації, що може спричинити перерви в роботі банківської системи, втрату довіри клієнтів та фінансові збитки[2].

Загрози, які стосуються фінансової стійкості банку, можуть призвести до втрати фінансових ресурсів через кіберзлочинність, шахрайство або інші види фінансових злочинів.

Загрози, що можуть впливати на репутацію банку, можуть включати в себе витік конфіденційної інформації, виявлення недоліків у системах безпеки або невдалий відгук на кризову ситуацію.

Ці аспекти підкреслюють важливість розуміння та управління загрозами інформаційній безпеці банку для забезпечення його стабільності, надійності та довіри клієнтів. Аналіз сутності загроз дає змогу розробити ефективні стратегії захисту та мінімізувати ризики для банківської системи та її клієнтів.

Класифікація загроз інформаційній безпеці банку є важливим інструментом для розуміння та управління ризиками. Вона може бути здійснена за декількома критеріями, включаючи джерело, призначення та характер загроз.

Основні типи загроз інформаційній безпеці банку згідно з їхніми класифікаційними ознаками[3]:

- *За джерелом*:

- кібератаки, що включають в себе різноманітні типи зловмисних дій, такі як віруси, вторгнення у систему, фішинг тощо, спрямовані на отримання незаконного доступу до банківської інформації;
- соціальне інженерство, яке включає використання маніпуляційних технік для отримання конфіденційної інформації шляхом маніпулювання співробітниками банку або клієнтами;
- недбале використання інформації, що включає в себе неналежне поводження з конфіденційною інформацією співробітниками банку, таке як втрата або небезпечне зберігання даних;
- внутрішній шпигунство, а саме намагання співробітників банку отримати несанкціонований доступ до інформації з метою використання її в особистих цілях або для продажу третім сторонам.

- *За призначенням*:

- кіберзлочинність, яка спрямована на отримання несанкціонованого доступу до фінансової інформації банку з метою викрадення грошових коштів або вчинення інших фінансових злочинів;
- шпигунство, спрямоване на отримання конфіденційної інформації про діяльність банку з метою отримання конкурентної переваги або нанесення шкоди бізнесу.

- *За характером*:

- пасивні загрози, які можуть призвести до витоку інформації або порушення безпеки без активних дій з боку зловмисників;
- активні загрози, які включають активні дії зловмисників для отримання несанкціонованого доступу або виконання шкідливих операцій у банківській системі.

Зазначена класифікація загроз інформаційній безпеці банку відображає різноманітність та складність викликів, які виникають у сфері захисту інформації в банківській сфері. Враховуючи ці загрози, розробка ефективних стратегій та заходів забезпечення безпеки стає надзвичайно важливою для забезпечення стабільності та надійності банківської системи.

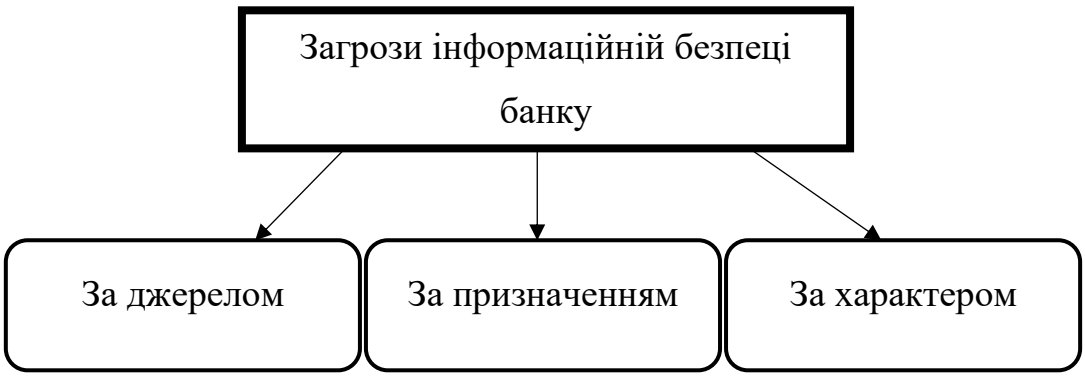

Рис.1.1. Класифікація типів загроз інформаційній безпеці банку

1.2 Аналіз сучасних методів та засобів захисту інформаційних ресурсів банківських установ

У світлі зростаючої кількості кіберзагроз та необхідності забезпечення безпеки фінансових даних, аналіз сучасних методів та засобів захисту інформаційних ресурсів банківських установ стає предметом великого інтересу для дослідників, практиків та регуляторів. Цей розділ спрямований на розширене дослідження цієї теми, зосереджуючись на технологічному прогресі, стратегічних аспектах та важливості інновацій у забезпеченні інформаційної безпеки в банківському секторі.

Сучасні методи захисту інформаційних ресурсів банківських установ нерозривно пов'язані з технологічним прогресом. Впровадження штучного інтелекту, машинного навчання та аналізу великих даних (Big Data) дозволяє виявляти та усувати загрози в реальному часі. Автоматизовані системи виявлення та запобігання інцидентам (IDPS), які базуються на алгоритмах машинного навчання, дозволяють виявляти відхилення від звичних патернів поведінки та реагувати на них негайно. Блокчейн-технологія використовується

для створення безпечних та незмінних журналів транзакцій, що забезпечує надійність та цілісність фінансових даних[4].

Штучний інтелект (ШІ) та машинне навчання (МН) відіграють ключову роль у сучасних системах кіберзахисту банків. Алгоритми ШІ та МН використовуються для аналізу великих обсягів даних та виявлення аномальних патернів, які можуть свідчити про потенційні загрози. Наприклад, системи, які використовують МН, можуть навчатися розпізнавати звичайні та незвичайні патерни мережевого трафіку, щоб виявити потенційно шкідливі дії або атаки.

Блокчейн-технологія відіграє важливу роль у забезпеченні безпеки фінансових даних у банківських установах. Блокчейн дозволяє створювати децентралізовані та незмінні журнали транзакцій, що забезпечує надійність та цілісність фінансових даних. Кожна транзакція, що вноситься до блокчейну, має високий рівень шифрування та підтверджується всіма учасниками мережі, що робить її майже неможливою до модифікації або видалення.

Системи виявлення та запобігання вторгнень (IDPS) використовуються для надання захисту від широкого спектру кіберзагроз, включаючи віруси, шкідливі програми, вторгнення у мережу та атаки з використанням вразливостей. Ці системи виявляють аномальну або підозрілу активність та приймають відповідні заходи для її блокування або усунення[5].

Аналітика та візуалізація даних стають все більш важливими у сфері кіберзахисту банків. Системи аналізу та візуалізації даних дозволяють ідентифікувати та аналізувати великі обсяги даних, виявляючи тенденції, патерни та аномалії, які можуть свідчити про потенційні загрози. Це дозволяє аналітикам швидше реагувати на загрози та вживати відповідних заходів захисту.

Сучасні системи кіберзахисту банківських установ стають все більш адаптивними та інтелектуальними. Вони використовують розумні алгоритми та моделі, що навчаються, щоб адаптуватися до змін у кіберзагрозах та навколишньому середовищі. Це дозволяє системам реагувати на нові та

невідомі загрози та швидко адаптуватися до них, забезпечуючи високий рівень захисту.

Ефективний захист інформаційних ресурсів банку передбачає розробку стратегій, які охоплюють не лише технічні аспекти, але й організаційні та людські ресурси. Управління ризиками та забезпеченням безпеки (ERM/ESM) визначає процеси та політики, спрямовані на ідентифікацію, оцінку та управління ризиками в сфері інформаційної безпеки. Цільове залучення інформаційної безпеки до стратегічного планування банку та залучення вищого керівництва може забезпечити необхідні ресурси та підтримку для ефективного впровадження заходів захисту[6].

Ефективне управління ризиками та забезпеченням безпеки (ERM/ESM) передбачає розробку і впровадження стратегій, спрямованих на ідентифікацію, оцінку та управління ризиками в сфері інформаційної безпеки. Це включає в себе аналіз потенційних загроз, оцінку вразливостей, розробку заходів з мінімізації ризиків та планування реагування на непередбачені події. Управління ризиками є невід'ємною частиною стратегічного планування банку і дозволяє йому зберігати інформаційну стійкість та надійність в умовах непередбачуваних кіберзагроз.

Інформаційна безпека повинна бути інтегрована у стратегічне планування банку з самого початку. Це включає в себе визначення цілей та приоритетів в галузі інформаційної безпеки, а також аналіз інвестиційних потреб і ресурсів, необхідних для досягнення цих цілей. Цільове залучення інформаційної безпеки до стратегічного планування дозволяє банку ефективно адаптуватися до змін у кіберзагрозах та забезпечити необхідні ресурси для забезпечення безпеки інформаційних ресурсів.

Розробка та впровадження політик безпеки є важливою частиною стратегії захисту інформаційних ресурсів банку. Ці політики визначають правила, процедури та стандарти, що регулюють використання та захист інформації, і включають в себе аспекти, такі як доступ до даних, шифрування, аутентифікація, моніторинг та забезпечення відповідності[7]. Розробка та

впровадження ефективних політик безпеки дозволяє банку створити культуру безпеки та забезпечити високий рівень захисту інформаційних ресурсів.

Успішне впровадження стратегій захисту інформаційних ресурсів вимагає активного залучення вищого керівництва банку. Керівництво повинно виявити підтримку ініціатив у сфері кіберзахисту та виділити необхідні ресурси для їх впровадження. Активна підтримка вищого керівництва допомагає створити атмосферу, в якій інформаційна безпека є пріоритетом, і забезпечує необхідну підтримку та ресурси для ефективного впровадження стратегій захисту.

Сучасна загроза кібератак вимагає постійної інновації та адаптації з боку банківських установ. Розвиток новітніх методів аутентифікації, таких як біометричні системи або мультифакторна аутентифікація, дозволяє забезпечити високий рівень безпеки доступу до фінансових даних. Використання аналітичних інструментів для прогнозування та виявлення потенційних загроз дозволяє банкам реагувати на них перед тим, як вони стануть критичними. Постійна співпраця з індустрією кібербезпеки та активна участь у вирішенні спільних проблем можуть сприяти розробці новітніх рішень та технологій, які відповідають сучасним викликам.

Важливою також є постійна адаптація до новітніх технологій та інновацій. Залучення до розробки та впровадження новітніх технологій у сфері кібербезпеки дозволяє банкам залишатися кроку вперед у боротьбі зі злочинними елементами, які постійно шукають нові шляхи проникнення[8].

Однією з ключових сучасних інновацій у сфері кібербезпеки є розвиток нових методів аутентифікації, таких як біометричні системи та мультифакторна аутентифікація. Використання біометричних даних, таких як відбитки пальців, розпізнавання обличчя чи голосу, дозволяє створити надійні механізми ідентифікації користувачів, що є значно важливим у запобіганні несанкціонованого доступу до фінансових даних. Мультифакторна аутентифікація, яка вимагає два або більше методів підтвердження особи (наприклад, пароль і біометричні дані), забезпечує ще вищий рівень безпеки.

Інноваційні методи аналізу даних та машинного навчання використовуються для прогнозування та виявлення потенційних кіберзагроз заздалегідь. Шляхом аналізу великого обсягу даних, які стосуються попередніх інцидентів та відхилень у поведінці, алгоритми можуть ідентифікувати можливі загрози та надавати рекомендації щодо вжиття заходів для їх запобігання.

Співпраця з індустрією кібербезпеки та активна участь у вирішенні спільних проблем можуть сприяти розробці та впровадженню новітніх рішень та технологій. Обмін досвідом та інформацією між учасниками галузі дозволяє ідентифікувати та реагувати на нові та еволюційні загрози швидше та ефективніше[9].

Забезпечення безпеки інформаційних ресурсів банківських установ є складним завданням, що вимагає інтеграції різноманітних підходів та стратегій. Технологічний прогрес в цій галузі визначається швидким розвитком новітніх технологій, таких як штучний інтелект, блокчейн та системи виявлення та запобігання вторгнень. Ці технології дозволяють банкам ефективно виявляти, відстежувати та захищати свої інформаційні ресурси від різноманітних кіберзагроз.

Однак, успішне забезпечення інформаційної безпеки також потребує розробки та впровадження стратегічних аспектів. Це включає управління ризиками та забезпеченням безпеки, визначення цілей та приоритетів у сфері кібербезпеки, розробку та впровадження політик безпеки, а також активне залучення вищого керівництва[10].

Крім того, важливість інновацій у сфері захисту інформаційних ресурсів банківських установ наголошується на постійному пошуку нових технологій та стратегій, що дозволяють банкам ефективно адаптуватися до зростаючих кіберзагроз. Розвиток нових методів аутентифікації, використання аналітики для прогнозування загроз та співпраця з індустрією кібербезпеки є лише деякими з інноваційних підходів, які допомагають банкам зберігати інформаційну безпеку та захищати фінансові дані своїх клієнтів.

У підсумку, лише комплексний підхід, який поєднує технологічний прогрес, стратегічні аспекти та інновації, може забезпечити надійний захист інформаційних ресурсів банківських установ у сучасному кібербезпечному середовищі.

1.3 Роль та значення побудови типової моделі загроз у забезпеченні інформаційної безпеки банку

Побудова типової моделі загроз є важливим етапом у забезпеченні інформаційної безпеки банку, оскільки вона сприяє систематизації та аналізу різноманітних потенційних загроз, які можуть виникнути в контексті банківської діяльності. Цей підхід ґрунтується на комплексному аналізі ідентифікованих загроз, їх характеристик, потенційних наслідків та методів протидії.

Першочергове завдання при побудові типової моделі загроз полягає у визначенні широкого спектру потенційних загроз, які можуть стати виходом з огляду на особливості функціонування банківської системи. Це можуть бути загрози зовнішнього та внутрішнього характеру, такі як кібератаки, внутрішні шахрайства, технічні вади, недбалість персоналу та інші.

Визначення широкого спектру потенційних загроз є важливою складовою побудови типової моделі загроз у забезпеченні інформаційної безпеки банку. Цей процес передбачає систематичний аналіз різноманітних загроз, які можуть виникнути в контексті банківської діяльності, та їхнього подальшого класифікування[11].

Важливо розуміти, що загрози можуть мати різноманітний характер та походити як зовнішніх, так і внутрішніх джерел. Зовнішні загрози можуть включати кібератаки від зловмисників, кібершпигунство, фішингові атаки, деніал-оф-сервіс атаки та інші форми кіберзлочинності, які спрямовані на викривлення роботи банку та шахрайство. Внутрішні загрози можуть виникати

з боку співробітників банку через недбалість, зловживання привілеями, невірну обробку даних чи інші форми внутрішньої саботажу.

Для ефективного виявлення та аналізу загроз необхідно ретельно проаналізувати різні аспекти банківської діяльності, такі як обробка фінансових транзакцій, управління клієнтськими даними, забезпечення доступу до онлайн-систем, інтеграція з партнерами та постачальниками послуг тощо. Наприклад, розгляд загроз пов'язаних з обробкою фінансових транзакцій може включати аналіз ризиків зв'язаних з підробкою документів, втратою грошей через несанкціоновані операції, вразливості систем передачі платежів тощо.

Важливо враховувати актуальні тренди та відомі методи атак, які можуть використовуватися зловмисниками. Регулярне оновлення знань про нові та еволюціонні загрози дозволяє забезпечити більш ефективний аналіз та протидію.

Звернення до експертів у сфері кібербезпеки та співпраця з ними може допомогти ідентифікувати потенційні загрози, які можуть бути незрозумілі або невидимі для внутрішнього персоналу банку.

Визначення широкого спектру потенційних загроз передбачає комплексний аналіз зовнішніх та внутрішніх загроз, врахування специфіки банківської діяльності, використання актуальних трендів та експертних знань у сфері кібербезпеки. Цей процес є важливим етапом у побудові ефективної стратегії захисту інформаційних ресурсів банку[12].

Наступним кроком у процесі побудови типової моделі є класифікація і ранжування загроз за ступенем ймовірності виникнення та потенційними наслідками для банківської діяльності. Цей аналіз дозволяє визначити найбільш критичні та серйозні загрози, які потребують негайного уваги та протидії.

Класифікація і ранжування загроз за ступенем ймовірності виникнення та потенційними наслідками для банківської діяльності є важливим етапом у процесі забезпечення інформаційної безпеки банку. Цей процес дозволяє ідентифікувати найбільш критичні та серйозні загрози, які можуть мати

негативний вплив на функціонування банку, та визначити пріоритети для вжиття заходів з їхнього протидії.

Класифікація загроз може проводитися з різних точок зору, враховуючи їхній джерело, способи виявлення та вплив на інформаційні ресурси банку[13].

- Джерело:

зовнішні загрози: наприклад, кібератаки, віруси, хакерські напади;

внутрішні загрози: наприклад, недбалість співробітників, зловживання привілеями, внутрішні шахрайства.

- Способи виявлення:

активні загрози: наприклад, кібератаки, які спрямовані на вразливості в системах банку;

пасивні загрози: наприклад, зловмисники, які здійснюють розвідку або намагаються зібрати конфіденційну інформацію без публічних атак.

- Потенційний вплив:

фінансовий вплив: наприклад, втрата коштів через шахрайство або віруси;

репутаційний вплив: наприклад, втрата довіри клієнтів через кібератаки або витік конфіденційної інформації.

Ранжування загроз зазвичай здійснюється на основі двох основних критеріїв: ймовірності виникнення та потенційних наслідків для банківської діяльності[14].

- Ймовірність виникнення:

висока: загроза, яка має велику ймовірність виникнення через широкий розповсюджений спосіб або відомі вразливості в системах банку;

середня: загроза, яка може виникнути при сприятливих умовах або внаслідок випадкових подій;

низька: загроза, яка має малу ймовірність виникнення через відсутність відомих вразливостей або малу активність з боку зловмисників.

- Потенційні наслідки:

високі: загроза, яка може призвести до серйозних фінансових втрат, порушення роботи банку або втрати довіри клієнтів;

середні: загроза, яка може призвести до обмежених фінансових втрат або незначного порушення роботи банку;

низькі: загроза, яка має малу потенційну шкоду для банківської діяльності та може бути легко контрольована.

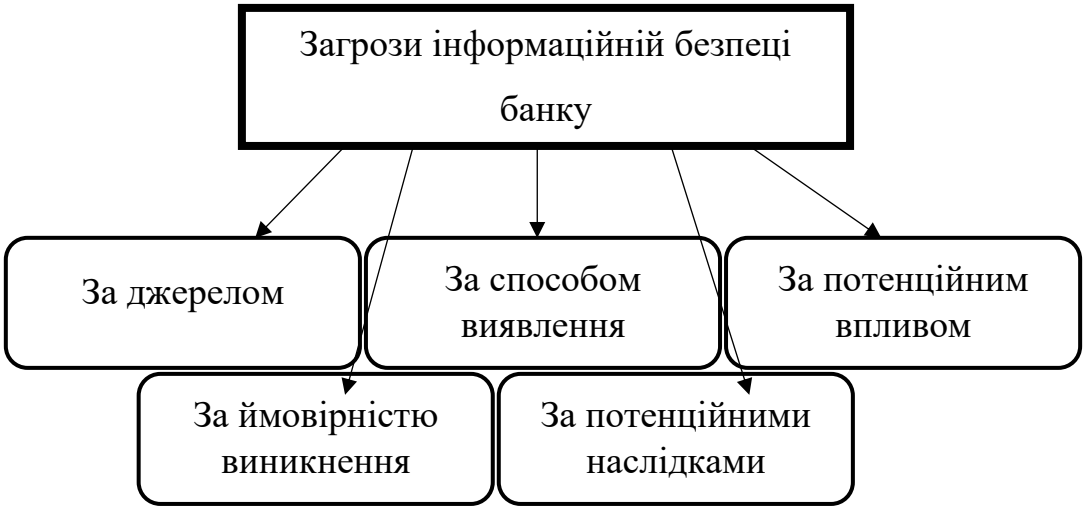

Рис. 1.2 Класифікація загроз за ступенем ймовірності виникнення та потенційними наслідками для банківської діяльності

Загрози ранжуються за ступенем їхньої серйозності та важливості для банківської діяльності, що дозволяє визначити пріоритети для розробки та впровадження заходів з протидії. Такий підхід допомагає банкам ефективно спрямовувати свої ресурси на захист від найбільш критичних загроз та мінімізацію потенційних ризиків[15].

Далі важливим етапом є визначення та розробка відповідних заходів з протидії кожній із ідентифікованих загроз. Ці заходи можуть включати в себе технічні заходи забезпечення кібербезпеки, вдосконалення процедур контролю та моніторингу, а також підвищення кваліфікації персоналу.

Ефективне забезпечення інформаційної безпеки банку передбачає не лише ідентифікацію потенційних загроз, але й розробку та впровадження відповідних заходів з протидії кожній із цих загроз. Цей процес є складним і багатоплановим, оскільки вимагає ретельного аналізу, планування та реалізації заходів з метою мінімізації ризиків та забезпечення надійності інформаційної інфраструктури банку[16].

Після ідентифікації загроз, перший крок у розробці заходів з протидії полягає у проведенні комплексного аналізу кожної із них з метою розуміння їхньої суті та потенційного впливу на банківську діяльність. Це включає в себе оцінку технічних, організаційних та людських аспектів загрози, визначення потенційних слабких місць та вразливостей у системах та процесах банку.

Після того, як загрози були аналізовані, необхідно розробити стратегії та плани дій для протидії кожній із них. Це включає в себе ряд заходів[17].

Технічні заходи забезпечення інформаційної безпеки:

впровадження сучасних систем захисту інформації, які забезпечують виявлення та блокування загроз на різних рівнях інформаційної інфраструктури банку. Наприклад, це може бути встановлення міцних файрволів, антивірусних програм, систем виявлення вторгнень та моніторингу безпеки.

Організаційні заходи забезпечення інформаційної безпеки:

вдосконалення процедур та політик безпеки банку, а також на підвищення освіченості персоналу щодо кібербезпеки. Наприклад, це може бути впровадження строгих правил паролів, регулярна підготовка персоналу з питань кібербезпеки та створення механізмів звітування про інциденти.

Людські ресурси:

залучення та підтримка кваліфікованого та досвідченого персоналу з кібербезпеки. Це може включати в себе найм спеціалістів з кібербезпеки, надання можливостей для професійного розвитку та створення ефективних команд з реагування на кіберінциденти.

Стратегічне управління ризиками:

постійне оцінювання та моніторинг ризиків і вжиття заходів для їхнього зменшення або уникнення.

Усі ці заходи повинні бути ретельно сплановані та реалізовані з урахуванням специфіки банківської діяльності, щоб забезпечити максимальний рівень захисту інформаційних ресурсів та даних клієнтів. Такий підхід до розробки заходів з протидії загрозам забезпечує банкам здатність ефективно відповідати на кіберзагрози та мінімізувати їхні наслідки для бізнесу[18].

Особлива увага при побудові типової моделі загроз повинна бути приділена урахуванню специфіки банківської галузі, так як вона має свої власні особливості та ризики, пов'язані з обробкою фінансової інформації та здійсненням фінансових операцій.

Урахування специфіки банківської галузі в процесі забезпечення інформаційної безпеки є важливим аспектом стратегії кібербезпеки банку. Банківська сфера відрізняється особливими характеристиками та вимогами, які потребують уважного аналізу та спеціалізованих підходів для забезпечення ефективного захисту інформаційних ресурсів та даних клієнтів[19].

По-перше, банківська галузь характеризується високим рівнем регулятивних вимог та відповідальності перед регуляторами. Банки мають дотримуватися строгих нормативно-правових вимог, які стосуються збереження та захисту конфіденційної інформації клієнтів, виявлення та запобігання випадкам відмивання грошей та інших фінансових злочинів. Такі вимоги вимагають від банків високого рівня контролю та захисту інформації, включаючи здійснення регулярних аудитів та перевірок з метою визначення вразливостей та розробки відповідних заходів для їх усунення.

По-друге, банківська галузь володіє великим обсягом конфіденційної та чутливої інформації, що робить її привабливою мішенню для кіберзлочинців. Банки зберігають велику кількість особистих даних клієнтів, фінансову інформацію та інші конфіденційні дані, які можуть бути використані для шахрайства, крадіжки особистості та інших злочинних дій. Тому захист цієї інформації від несанкціонованого доступу та витоків є пріоритетним завданням для банків, і вимагає вдосконалених технічних, організаційних та правових заходів[20].

По-третє, банківська галузь постійно зазнає впливу швидкого технологічного прогресу та інновацій. Впровадження новітніх технологій, таких як цифрові платежі, мобільні додатки та інші інновації, відкриває нові можливості для клієнтів, але одночасно створює нові кіберзагрози та вразливості для банківських систем. Тому банки повинні бути готові до

постійного моніторингу та адаптації до змін у технологічному середовищі, а також швидко реагувати на нові загрози та ризики.

Урахування специфіки банківської галузі вимагає комплексного підходу до забезпечення кібербезпеки, який охоплює технічні, організаційні, правові та кадрові аспекти. Лише такий підхід дозволить банкам ефективно захищати свою інформацію та забезпечувати надійність своїх послуг для клієнтів[21].

Загальна мета побудови типової моделі загроз полягає у створенні комплексної системи заходів захисту, яка дозволить банку ефективно протистояти потенційним загрозам та забезпечити безпеку своїх інформаційних ресурсів. Враховуючи постійне зростання кількості та складності кіберзагроз, побудова типової моделі є необхідною складовою для успішного забезпечення інформаційної безпеки банку.

Висновки до розділу 1

У розділі розглянуто різноманітні аспекти кіберзагроз, які становлять потенційну загрозу для банківської сфери. Починаючи з аналізу сутності та класифікації загроз, було виявлено, що вони можуть мати різноманітний характер та джерела, включаючи як зовнішні, так і внутрішні фактори. Крім того, було розглянуто важливість урахування специфіки банківської галузі при розробці стратегій захисту, оскільки вона характеризується великим обсягом конфіденційної інформації та підвищеним рівнем регулятивних вимог.

Детально проаналізовано класифікацію і ранжування загроз за ступенем ймовірності виникнення та потенційними наслідками для банківської діяльності, що дозволяє визначити найбільш критичні та серйозні загрози і встановити пріоритети для вжиття заходів з протидії. На основі цього аналізу розглянуто урахування специфіки банківської галузі при розробці відповідних заходів з протидії кожній із ідентифікованих загроз.

Зокрема, було виявлено, що для ефективного захисту інформаційної безпеки банку необхідно впроваджувати комплексні технічні, організаційні та

кадрові заходи, спрямовані на мінімізацію ризиків та забезпечення надійності інформаційних ресурсів. Урахування специфіки банківської галузі вимагає вдосконаленого контролю, надійних заходів з протидії кіберзагрозам та постійного моніторингу технологічного середовища.

Загалом розділ надає важливі відомості та аналіз для розуміння природи, класифікації та управління кіберзагрозами в банківській сфері, а також визначає ключові напрямки розвитку стратегій захисту інформаційної безпеки для забезпечення стабільності та надійності функціонування банківських установ.

Розділ 2 АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ

2.1 Внутрішні загрози: аналіз ризиків, пов'язаних з персоналом та внутрішніми процесами банку

У динамічному середовищі фінансових установ загрози постійно виникають за різних умов та негативно впливають на роботу установи. Для банківської установи необхідно розуміти які внутрішні фактори можуть постати великою проблемою для всієї роботи системи. Ці фактори включають в себе інсайдерське шахрайство, недбале виконання обов'язків працівниками, організаційні вразливості, недостатня ефективність механізмів контролю та ін.

Операційний ризик визначається [22] як ймовірність втрат або додаткових витрат, а також можливість невиконання запланованих доходів внаслідок недоліків або помилок у внутрішніх процесах організації. Ці ризики можуть виникнути внаслідок навмисних або ненавмисних дій працівників банку чи інших осіб, а також внаслідок порушень у роботі інформаційних систем банку або через вплив різноманітних факторів.

Внутрішні загрози можна розділити на дві категорії:ті, що пов’язані напряму з персоналом та ті, що пов'язані з внутрішніми процесами. [23]

Ризики, пов'язані з персоналом банківської установи, стосуються потенційних загроз, які створюють працівники, як через навмисні дії, так і через ненавмисні, і які можуть поставити під загрозу операційну діяльність та безпеку установи.

Одним із ризиків є шахрайство та зловживання, оскільки працівники, які мають доступ до фінансових систем і конфіденційної інформації, можуть використовувати ці можливості для особистої користі та незаконного збагачення. До цього ризику можна віднести такі маніпуляції, як крадіжка грошей, підробка документів та надання кредитів підставним особам або перевищення повноважень.

Помилки співробітників – ненавмисні дії, які можуть призвести до помилок в системі або втрат. Недостатня кваліфікація може бути причинами цих помилок. Часто це є наслідком неефективної системи навчання та розвитку кадрів. Якщо банк не надає достатньо уваги постійному підвищенню кваліфікації своїх працівників, а також проведенню різних тренінгів, це може призвести до неправильного виконання ними своїх обов'язків, що у свою чергу може збити процес обробки транзакцій, оформлення документів або проведення фінансових операцій.

Надодачу, нові співробітники, які не пройшли належного стажування та не пройшли оцінку знань по завершенню, можуть виявитися недостатньо компетентними для роботи. Досвідчені співробітники, які знають, як уникнути типових помилок, здатні ефективніше виконувати свої обов'язки та приймати зважені рішення.

Неуважність або недотримання встановлених політик банку є ще одним негативним ризиком. Він пов'язаний з рутинними завданнями, коли співробітники не звертають через різні причини належної уваги на деталі, що може призвести до допущення помилок у банківських операціях. Наприклад, помилки при введенні даних клієнтів або неправильне оформлення документів.

Рис. 2.1 Джерела загроз, пов'язаних з людським фактором [24]

Також, як зазначено було раніше, стабільності та ефективності функціонування банку залежить від правильності проведених внутрішніх процесів. Недосконалість або неефективність процедур та політик, що регулюють діяльність банку, є джерелами вразливостей та потенційних загроз. Якщо внутрішні процеси не є чітко визначеними та документованими, це може призвести до неправильного виконання операцій, помилок у звітності та недотримання регуляторних вимог.

Ще одна важлива деталь, що регулює внутрішні процеси, – управління змінами. Банки часто стикаються з необхідністю впроваджувати нові продукти, послуги та технології, щоб відповідати мінливим вимогам клієнтів та суспільному розвитку. Однак будь-які зміни в організаційній структурі або бізнес-процесах можуть створювати додаткові ризики, якщо ними не управляти ефективно. Наприклад, розгортання нової системи управління ризиками без належного навчання персоналу може призвести до неправильної оцінки ризиків та прийняття помилкових рішень.

Управління змінами передбачає структурований підхід до переходу окремих осіб, команд та організацій з поточного стану до бажаного майбутнього. У контексті банківської справи цей процес гарантує, що зміни впроваджуються плавно і стабільно, зводячи до мінімуму збої в роботі та зменшуючи потенційні ризики. Ефективне управління змінами вимагає ретельного планування, чіткої комунікації та комплексних навчальних програм для підготовки всіх зацікавлених сторін до майбутніх змін.

Впровадження нових технологій та систем є значною частиною управління змінами. Банки повинні забезпечити ретельне планування та виконання цих впроваджень. Це включає проведення оцінки впливу, щоб зрозуміти, як зміни вплинуть на існуючі процеси та системи, а також визначення потенційних ризиків, які можуть виникнути під час переходу. Крім того, залучення ключових зацікавлених сторін до процесу планування може надати цінну інформацію та сприяти підтримці, що забезпечить більш плавне прийняття нових ініціатив.

Навчання персоналу є важливим компонентом управління змінами. Коли впроваджується нова система або процес, працівники повинні бути належним чином підготовлені для ефективного використання. Це навчання має охоплювати не лише технічні аспекти нової системи, але й те, як вона інтегрується з існуючими процесами. Комплексні навчальні програми допомагають запобігти помилкам, які можуть виникнути через нерозуміння або незнання нової системи, тим самим знижуючи ризик неправильної оцінки ризиків і прийняття неякісних рішень.

Окрім навчання, для успішного управління змінами критично важливими є постійна підтримка та моніторинг. Надання постійної підтримки допомагає працівникам адаптуватися до нової системи, а моніторинг її впровадження дозволяє своєчасно виявляти та вирішувати будь-які проблеми, що можуть виникнути. Такий проактивний підхід гарантує, що нова система працюватиме так, як заплановано, а будь-які відхилення будуть оперативно усунені. [25].

Контроль за виконанням внутрішніх процесів є ще одним ключовим елементом управління ризиками у банківській сфері. Якщо банк не проводить регулярні аудити та перевірки, це може створити умови для шахрайських дій та більших можливостей для хакерів. Крім того, відсутність належного контролю може призвести до недотримання регуляторних вимог, що може мати серйозні юридичні наслідки та пошкодити репутацію банку.

Зрештою, внутрішні процеси банку повинні бути адаптивними та здатними швидко реагувати на зміни у зовнішньому середовищі. Відсутність гнучкості у внутрішніх процесах може призвести до того, що банк не зможе ефективно реагувати на нові виклики. Для забезпечення адаптивності внутрішніх процесів необхідно постійно аналізувати їх ефективність та впроваджувати зміни у разі виявлення недоліків або нових ризиків[26].

2.2 Зовнішні загрози: огляд загроз, які виникають в результаті дій зовнішніх агентів, таких як хакери, кіберзлочинці, конкуренти тощо

Банківська сфера є однією з найбільш уразливих до зовнішніх загроз. Банківський сектор, як і будь-яка інша галузь економіки, прямо залежить від змін у макроекономічному середовищі. Загальноекономічна ситуація в країні та світових регіонах, нормативно-правове забезпечення та урядові кризи — ключові фактори, які можуть мати вплив на діяльність фінансових інститутів.

Несприятливі макроекономічні умови включають у себе повільне економічне зростання, високу безробіття та зниження реальних доходів населення. Такі умови знижують попит на банківські продукти та послуги, наприклад, на кредити. В результаті погіршення економічного становища, банки можуть стикатися з підвищеним рівнем прострочених платежів, оскільки клієнти мають труднощі з виконанням своїх фінансових зобов'язань. Крім того, економічна нестабільність може спричинити відтік капіталу та зниження інвестиційної активності, що також негативно впливає на банківський сектор.

Нестійкість нормативно-правової бази та урядові кризи створюють додаткові ризики для банківської діяльності. Зміни у законодавстві, регуляторних вимогах чи податковій політиці можуть вимагати від банків негайного перегляду їхніх бізнес-моделей, стратегій управління ризиками та операційних процедур. Урядові кризи, що ведуть до політичної нестабільності, можуть спричинити зниження довіри до національної валюти, відтік капіталу та збільшення вартості залучення фінансування [27].

Варто також розглянути ризики, пов'язані з високим рівнем інфляції та інфляційними очікуваннями. Інфляція може знизити реальну вартість депозитів і кредитів, що негативно вплине на прибутковість як клієнтів, так і самих банків. Інфляційні очікування можуть спонукати домогосподарства та бізнес знімати кошти з рахунків, що призводить до зниження ліквідності банків. Крім того, в умовах високої інфляції центральний банк може підвищувати процентні ставки, щоб контролювати інфляцію, що згодом збільшує вартість залучення капіталу для банків.

Інфляція знижує купівельну спроможність грошей, тобто реальна вартість грошових активів, таких як банківські депозити, з часом зменшується. Для

вкладників це означає, що відсотки, отримані на їхні заощадження, можуть не встигати за інфляцією, що призведе до зниження реальних доходів. Для банків зниження реальної вартості депозитів може призвести до зменшення загальних заощаджень, що вплине на їхню здатність надавати кредити та інвестувати. З боку кредитування інфляція зменшує реальну вартість отриманих платежів за кредитами, що потенційно знижує прибутковість кредитної діяльності.

Висока інфляція також може впливати на поведінку споживачів. Коли інфляційні очікування зростають, споживачі та бізнес можуть очікувати подальшого зниження купівельної спроможності грошей. Такі очікування можуть спонукати їх зняти кошти з банківських рахунків, щоб інвестувати в активи, які, на їхню думку, краще зберігають вартість, такі як нерухомість, товари або іноземна валюта. Таке зняття коштів може суттєво знизити ліквідність банків, що ускладнює для них задоволення вимог про зняття коштів і підтримання достатнього рівня резервів.

У відповідь на високу інфляцію центральні банки часто вдаються до підвищення відсоткових ставок, щоб стримати інфляційний тиск. Хоча така політика може допомогти стабілізувати економіку, вона також збільшує вартість запозичень для банків. Вищі відсоткові ставки означають, що банки повинні платити більше за залучення депозитів і збільшення капіталу. Таке збільшення витрат може призвести до скорочення прибутку, особливо якщо банки не зможуть перекласти ці витрати на позичальників, не ризикуючи при цьому зменшити попит на кредити.

Крім того, вищі відсоткові ставки можуть призвести до зростання рівня неповернення кредитів, оскільки позичальники стикаються зі зростаючим тягарем виплат за кредитами. Цей ризик є особливо гострим для кредитів зі змінною процентною ставкою, яка коригується у відповідь на зміну облікової ставки центрального банку. Вищий рівень дефолтів може ще більше погіршити фінансовий стан банків, поглиблюючи проблеми, спричинені інфляцією та інфляційними очікуваннями [28].

Нестійкість податкової, кредитної та страхової політики є однією з ключових зовнішніх загроз для банківської системи. Непередбачуваність змін у законодавстві, що регулює ці сфери, може призвести до необхідності раптового перегляду бізнес-стратегій і моделей, збільшення витрат на їх адаптацію до нових реалій. Зміни в податковій політиці можуть вплинути на прибутковість банківських продуктів, кредитна політика може обмежити доступ до капіталу, а зміни в страховій політиці можуть збільшити вартість страхування ризиків [29].

Несприятлива криміногенна ситуація та зростання кримінальних і фінансових злочинів у кредитно-фінансовій сфері є ще однією серйозною загрозою. Фінансові інститути постійно стикаються з ризиком кібератак, шахрайства з кредитними картками, відмиванням грошей та іншими видами фінансових злочинів. Збільшення кількості таких злочинів не лише призводить до прямих фінансових втрат, але й підриває довіру клієнтів до банківської системи загалом.

Також, окрім макроекономічного стану, необхідно зазначити про зовнішні загрози, що виникають в результаті дій зовнішніх агентів, таких як хакери, кіберзлочинці, конкуренти тощо. Через негативні дії вищезазначених осіб, організацій та угруповань, перед банківськими установами постає серйозний виклик для безпеки та стабільності фінансових інститутів [30].

2.3 Системні загрози: аналіз ризиків, пов'язаних з інформаційною і технічною інфраструктурою банку та його програмним забезпеченням

Технічна інфраструктура банку є фундаментальною для його операцій та послуг. Вона включає в себе комп'ютерні системи, мережі, сервери, пристрої зберігання даних та програмне забезпечення. Розуміння рівня стійкості цих компонентів до потенційних загроз є критично важливим для забезпечення безперебійної роботи банку та захисту цінної інформації.

Несанкціонований доступ і витік даних становлять зростаючу проблему для банківського сектору. Кіберзлочинці використовують безліч витончених

методів для проникнення в банківські системи та отримання конфіденційної інформації. Ця інформація, як правило, включає персональні дані клієнтів, такі як імена, адреси, номери соціального страхування, реквізити рахунків і записи про транзакції. Мотиви таких атак варіюються від фінансової вигоди до маніпуляцій з даними та крадіжки особистих даних, що створює значні ризики як для клієнтів, так і для фінансових установ.

Для боротьби з цими загрозами банки повинні постійно вдосконалювати свої протоколи безпеки. Це передбачає впровадження багаторівневих заходів безпеки, які можуть ефективно запобігти спробам несанкціонованого доступу. Такі заходи включають використання сучасних методів шифрування, надійних процесів автентифікації та захищених каналів зв'язку. Шифрування гарантує, що дані не зможуть прочитати неавторизовані користувачі, а багатофакторна автентифікація додає додатковий рівень безпеки, вимагаючи декількох форм перевірки перед наданням доступу.

Крім того, активний і безперервний моніторинг банківських систем має першорядне значення. Спостереження в режимі реального часу допомагає на ранніх стадіях виявляти підозрілі дії, дозволяючи оперативно реагувати на потенційні порушення. Сюди входить використання систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS), які можуть виявити і пом'якшити загрози до того, як вони завдадуть значної шкоди. Крім того, використання штучного інтелекту та алгоритмів машинного навчання може покращити здатність виявляти аномалії та прогнозувати потенційні порушення безпеки.

Ще однією серйозною проблемою є вразливості програмного забезпечення. Кіберзлочинці часто обирають своїм об'єктом програмне забезпечення, що використовується банками, шукаючи слабкі місця в коді, які можна використати для отримання несанкціонованого доступу та контролю над банківськими системами. Ця постійна загроза вимагає багатогранного підходу до безпеки, при якому банки повинні не тільки застосовувати останні

оновлення та виправлення безпеки, але й розробляти комплексні стратегії для запобігання, виявлення та реагування на такі інциденти.

Вразливості програмного забезпечення можуть виникати з різних причин, включаючи помилки кодування, застарілі бібліотеки та недостатньо протестовані оновлення. Кіберзлочинці використовують ці вразливості за допомогою таких методів, як впровадження шкідливого коду, використання переповнень буферів та запуск атак "нульового дня". Наслідки таких порушень можуть бути серйозними, призводячи до несанкціонованих транзакцій, крадіжки даних та значної фінансової та репутаційної шкоди для постраждалої установи.

Щоб зменшити ці ризики, банки повинні займати проактивну позицію щодо безпеки програмного забезпечення. Це передбачає своєчасне застосування патчів безпеки та оновлень, що надаються постачальниками програмного забезпечення, які усувають відомі вразливості та підвищують загальний рівень безпеки. Однак покладатися на зовнішні оновлення недостатньо. Банки також повинні впроваджувати власні суворі протоколи безпеки для захисту своїх систем.

Розробка надійної стратегії безпеки включає проведення регулярних перевірок коду та аудитів безпеки для виявлення та усунення потенційних вразливостей до того, як вони можуть бути використані. Впровадження безпечних методів кодування, таких як перевірка вхідних даних та обробка помилок, може значно зменшити ймовірність вразливостей у новоствореному програмному забезпеченні. Крім того, використання автоматизованих інструментів для статичного та динамічного аналізу коду може допомогти у ранньому виявленні недоліків безпеки.

Враховуючи всі ці фактори, банки повинні віддавати велику увагу своїм системам безпеки і регулярно проводити оцінку ризиків, аналізувати потенційні загрози та тестувати свою здатність впоратися з ними. Такий комплексний підхід допоможе забезпечити надійну та стійку до загроз технічну

інфраструктуру, що є основою для ефективного та безпечного банківського обслуговування.

Ризики, пов'язані з внутрішніми процесами, можуть також виникати через недостатню автоматизацію та використання застарілих технологій. Банки повинні постійно оновлювати свої системи та процеси, щоб відповідати вимогам ринку та технологічному прогресу, що постійно змінюються. Використання застарілих технологій може призвести до затримок в обробці транзакцій та зниження якості обслуговування клієнтів. Крім того, недостатня автоматизація процесів може перешкоджати ефективному контролю та моніторингу транзакцій, підвищуючи ризик шахрайства та інших форм неправомірних дій.

Застарілим технологіям часто не вистачає ефективності та швидкості, необхідних для обробки сучасних банківських операцій. Це може призвести до виникнення вузьких місць в обробці транзакцій, спричиняючи затримки, які не тільки розчаровують клієнтів, але й впливають на операційну ефективність банку. Наприклад, застарілі системи можуть не підтримувати високошвидкісну обробку даних, необхідну для проведення транзакцій у режимі реального часу, що призводить до уповільнення обслуговування і зростання невдоволення клієнтів. Крім того, старі системи зазвичай більш вразливі до загроз безпеки, оскільки вони можуть бути несумісними з найновішими протоколами та оновленнями безпеки.

Недостатня автоматизація посилює ці проблеми, вимагаючи ручного втручання в процеси, які в іншому випадку можна було б оптимізувати. Ручні процеси за своєю суттю схильні до людських помилок, що може призвести до неточностей і невідповідностей у записах про транзакції. Відсутність автоматизації ускладнює здійснення всебічного нагляду та контролю за банківськими операціями. З іншого боку, автоматизовані системи можуть постійно відстежувати транзакції, виявляти аномалії та забезпечувати відповідність нормативним вимогам, тим самим зменшуючи ризик шахрайських дій.

Для вирішення цих завдань банки повинні інвестувати в модернізацію своєї технологічної інфраструктури. Це передбачає перехід на найсучасніші системи, здатні впоратися з вимогами сучасних банківських операцій і підтримувати безперебійні транзакції в режимі реального часу. Впровадження передових рішень з автоматизації може значно підвищити операційну ефективність, зменшивши потребу в ручній обробці та уможлививши безперервний моніторинг транзакцій. Такі системи можуть використовувати складні алгоритми та машинне навчання для виявлення нестандартних шаблонів і потенційного шахрайства в режимі реального часу.

Висновки до розділу 2

У розділі було проведено детальний аналіз загроз інформаційній безпеці банку, акцентуючи увагу на внутрішніх, зовнішніх та системних аспектах ризиків. Дослідження виявило, що кожен з цих аспектів має свої специфічні характеристики та вимагає особливого підходу до управління та мінімізації ризиків.

Внутрішні загрози були розглянуті з точки зору ризиків, пов'язаних з персоналом та внутрішніми процесами банку. Було визначено, що людський фактор є одним з найбільш значущих джерел загроз, оскільки недбалість або зловмисні дії співробітників можуть призвести до суттєвих втрат. Аналіз включав оцінку ризиків, пов'язаних з недотриманням політик безпеки та недостатньою підготовкою персоналу.

Зовнішні загрози були досліджені через призму дій зовнішніх агентів, таких як хакери, кіберзлочинці та конкуренти. Було виявлено, що зовнішні атаки можуть мати різноманітні форми, включаючи фішинг, DDoS-атаки, проникнення через вразливості в програмному забезпеченні та соціальну інженерію. Особливу увагу було приділено аналізу сучасних методів, що використовуються зловмисниками для проникнення у банківські системи та викрадення конфіденційної інформації.

Системні загрози охоплювали аналіз ризиків, пов'язаних з інформаційною та технічною інфраструктурою банку. Дослідження показало, що системні вразливості можуть виникати через недостатню захищеність програмного забезпечення, застарілі технології, а також неправильне налаштування систем безпеки. Також було виявлено, що постійний моніторинг та оновлення інфраструктури є критично важливими для підтримання високого рівня захищеності банківських систем.

Розділ 3 РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ВІД ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ БАНКУ

3.1 Оцінка потенційних ризиків та вразливостей банку

Оцінка ризиків у сфері інформаційної безпеки відіграє ключову роль у ефективному управлінні безпекою в межах банку. Цей процес допомагає ідентифікувати потенційні загрози, аналізувати можливі наслідки цих загроз та оцінювати їхню ймовірність. На основі цього визначаються стратегії зниження ризиків.

Управління ризиками в банку підтримується через впровадження відповідної політики, процедур та організаційних заходів, які сприяють інтеграції процесів керування ризиками на різних рівнях. В рамках цієї структури організація повинна розробити стратегію або політику, що дозволяє визначати час та методи проведення загальних оцінок ризику..

Оцінка ризиків інформаційної безпеки банку – це систематична оцінка, що проводиться банками з метою виявлення, аналізу та зменшення потенційних ризиків безпеки, пов'язаних з їхніми інформаційними системами та інформаційними активами. Ця оцінка є важливим компонентом загальної системи управління ризиками банку, спрямованої на захист конфіденційної інформації, дотримання нормативних вимог та захист від загроз кібербезпеки.

Основною метою оцінки ризиків є оцінка вразливостей і загроз конфіденційності, цілісності та доступності інформаційних активів банку. Сюди входять дані клієнтів, фінансові операції, а також внутрішні системи та мережі. Проводячи комплексну оцінку ризиків, банки можуть виявити потенційні слабкі місця в своїх засобах контролю безпеки та інфраструктурі, а також ймовірність і потенційний вплив різних інцидентів, пов'язаних з інформаційною безпекою.

Основні етапи проведення оцінки ризиків включають ідентифікацію активів, загроз, оцінку вразливостей, аналіз ризиків, розробку стратегій

реагування на ризики та заключним етапом моніторинг вжитих заходів. Цей процес зображено на Рис. 3.1.

Рис. 3.1 Процес оцінки ризиків

Ідентифікація активів передбачає комплексну ідентифікацію критично важливих інформаційних активів в банку, включаючи бази даних, програми, сервери та будь-яку відповідну інформацію, що потребує захисту. Цей процес передбачає ретельну інвентаризацію та категоризацію всіх активів, які є критично важливими для діяльності банку та потребують захисту.

На додаток до цього, ідентифікація активів може також включати оцінку залежностей та взаємозв'язків між активами в межах банківської внутрішньої системи. Такий цілісний підхід допомагає зрозуміти, як різні активи взаємодіють і залежать один від одного, що дає змогу провести більш комплексну оцінку потенційних вразливостей і ризиків.

Більше того, процес ідентифікації активів виходить за рамки простого переліку і враховує такі характеристики, як вразливість даних, критичність для бізнес-процесів та відповідність нормативним вимогам. Аналізуючи ці атрибути, банки можуть визначити пріоритети своїх активів на основі їхньої важливості та рівня захисту, якого вони потребують. Це полегшує розподіл ресурсів і впровадження цільових заходів безпеки, адаптованих до конкретних потреб кожного активу.

Ідентифікація загроз охоплює завчасне розпізнавання та аналіз потенційних ризиків, що загрожують кожному активу в банку. Сюди входить ідентифікація різних типів загроз, включаючи зовнішні та внутрішні типи загроз, які можуть поставити під загрозу конфіденційність, цілісність або

доступність активів. Ці загрози часто спрямовані на вразливості в системах і мережах банку з метою отримання несанкціонованого доступу до конфіденційної інформації або порушення роботи.

Окрім зовнішніх загроз, значні ризики для активів банку становлять внутрішні загрози. Ці загрози можуть виникати через ненавмисні дії співробітників, такі як ненавмисне розголошення даних або випадкове видалення критично важливої інформації. Крім того, внутрішні загрози можуть бути наслідком зловмисних дій інсайдерів, зокрема невдоволених працівників, недобросовісних підрядників або осіб з привілейованим доступом до систем банку. Такі загрози можуть включати навмисну крадіжку даних, саботаж або несанкціоновану модифікацію систем і даних.

Процес ідентифікації загроз передбачає ретельний аналіз потенційних учасників, причин і методів, пов'язаних з кожною з них, а також їхньої реалізації. Сюди входить розгляд можливостей і тактик, що застосовуються кіберзлочинцями, а також нових тенденцій і вразливостей у ландшафті кібербезпеки. Розуміючи природу і характеристики потенційних загроз, організації можуть краще оцінити їх ймовірність і потенційний вплив на безпеку своїх активів. Крім того, ідентифікація загроз передбачає врахування постійного розвитку загроз та відстеження нових ризиків і векторів атак.

Третім етапом йде оцінка вразливостей. Оцінка вразливостей – це систематичне вивчення інформаційної інфраструктури організації для виявлення потенційних слабких місць і вразливостей, якими можуть скористатися загрози. Цей процес включає аналіз систем, мереж, додатків та інших компонентів банківської організації для виявлення вразливостей, які можуть поставити під загрозу інформаційні активи.

Після визначення активів наступним кроком є виявлення потенційних вразливостей цих активів. Це може включати в себе проведення сканування вразливостей за допомогою автоматизованих інструментів, аналіз конфігурацій системи, перегляд коду програмних додатків, а також оцінку мережевої архітектури та конфігурації. До типових вразливостей, які можна виявити,

належать помилки в програмному забезпеченні, неправильні конфігурації, слабкі механізми автентифікації та неадекватні засоби контролю доступу.

Аналіз ризиків передбачає оцінку ймовірності та потенційного впливу кожної ідентифікованої загрози, використовуючи інформацію про вразливості та можливі способи їх використання. Цей процес має на меті кількісно оцінити рівень ризику для кожного активу в інформаційній інфраструктурі банку, що дає змогу приймати обґрунтовані рішення щодо стратегій зменшення ризиків та розподілу ресурсів.

Для ефективного проведення аналізу ризиків оцінюють ймовірність реалізації кожної загрози на основі різних факторів, включаючи наявність вразливостей, дані про аналогічні інциденти в минулому та галузеві тенденції. Ця оцінка передбачає розгляд ймовірності успішного використання загрози з урахуванням таких факторів, як досвідченість потенційних зловмисників, поширеність відомих вразливостей та ефективність існуючих засобів контролю безпеки.

Водночас банк оцінює потенційний вплив, який кожна загроза може мати на активи, операції та цілі організації. Ця оцінка впливу враховує ступінь, до якого конфіденційність, цілісність і доступність інформаційних активів можуть бути порушені, якщо загроза скористається існуючими вразливостями.

Поєднуючи оцінки ймовірності та впливу, банк може розрахувати рівень ризику, пов'язаний з кожною загрозою та активом. Це часто робиться за допомогою матриць ризиків або подібних інструментів, які присвоюють «рейтинг» ризику на основі оцінок ймовірності та впливу. Ризики, як правило, класифікуються за різними рівнями (наприклад, низький, середній, високий), щоб визначити пріоритети в управлінні ризиками та ефективно розподілити ресурси.

Ризики, які вважаються високими або середніми за ступенем серйозності, можуть вимагати негайних дій, таких як впровадження додаткових засобів контролю безпеки, виправлення відомих вразливостей або оновлення політик і процедур. І навпаки, ризики, які оцінюються як низькі за ступенем серйозності,

можуть бути прийняті або відстежуватися з меншою терміновістю, залежно від толерантності організації до ризиків і наявних ресурсів.

Розробка стратегії реагування на ризики передбачає визначення кроків, які будуть вжиті для зниження ризиків до прийнятного рівня та пом'якшення потенційного впливу виявлених загроз. Ця комплексна стратегія охоплює низку заходів, спрямованих на посилення безпеки, підвищення стійкості та формування культури проактивного управління ризиками:

1. Посилені заходи безпеки:

- Впровадження додаткових рівнів контролю безпеки, таких як шифрування, контроль доступу та системи виявлення вторгнень, для захисту чутливих інформаційних активів та критично важливих систем від несанкціонованого доступу та зловмисних дій.
- Розгортання передових технологій виявлення та запобігання загрозам, таких як платформи захисту кінцевих точок та системи управління інформацією та подіями безпеки (SIEM), для виявлення та реагування на інциденти безпеки в режимі реального часу.
- Регулярне оновлення та виправлення програмного забезпечення та систем для усунення відомих вразливостей та мінімізації ризику їх використання кіберзагрозами.

2. Нові політики та процедури безпеки:

- Розробка та впровадження надійних політик і процедур безпеки, що регулюють контроль доступу, захист даних, реагування на інциденти та поведінку співробітників, щоб встановити чіткі рекомендації щодо управління ризиками безпеки та забезпечення відповідності нормативним вимогам.
- Впровадження політики надійних паролів, багатофакторної автентифікації та принципу найменших привілеїв для обмеження доступу до конфіденційної інформації та зменшення ризику її несанкціонованого розголошення або зловживання.

- Створення протоколів реагування на інциденти та процедур ескалації для своєчасного виявлення, локалізації та усунення інцидентів безпеки, мінімізуючи їхній вплив на діяльність та репутацію організації.

3. Навчання працівників:

- Проведення комплексних тренінгів та освітніх програм з питань безпеки для працівників на всіх рівнях організації з метою покращення їхнього розуміння ризиків кібербезпеки, найкращих практик та їхньої ролі у підтримці безпечного робочого середовища.
- Проведення симульованих фішингових вправ та навчань з безпеки для перевірки реакції працівників на загрози безпеці та закріплення хороших навичок безпеки, таких як виявлення підозрілих електронних листів та негайне повідомлення про потенційні інциденти безпеки.
- Заохочення культури пильності та підзвітності шляхом сприяння відкритому спілкуванню, заохочення працівників повідомляти про проблеми безпеки та винагороди за проактивну поведінку, яка сприяє зміцненню загальної системи безпеки організації.

4. Постійний моніторинг та вдосконалення:

- Впровадження процесу постійного моніторингу, вимірювання та оцінки ефективності засобів контролю безпеки та стратегій управління ризиками для визначення сфер, що потребують вдосконалення, та забезпечення відповідності новим загрозам і бізнес-вимогам.
- Проведення регулярних оцінок ризиків, сканування вразливостей та аудитів безпеки для виявлення нових ризиків, оцінки стану безпеки організації та визначення пріоритетів щодо усунення недоліків на основі серйозності та ймовірності потенційних загроз.
- Постійно оновлювати та вдосконалювати стратегію реагування на ризики на основі уроків, отриманих з інцидентів безпеки, галузевих тенденцій, регуляторних змін та нових технологій, щоб підтримувати стійкість та адаптивність перед обличчям нових загроз.

Моніторинг та аналіз є заключним етапом оцінки ризиків. Цей безперервний процес включає моніторинг даних, пов'язаних з безпекою, аналіз інцидентів та оцінку показників ефективності для виявлення слабких місць для вдосконалення. Завдяки моніторингу банк може посилити свою безпеку та стійкість до нових кіберзагроз, мінімізуючи при цьому вплив інцидентів безпеки.

3.2 Розробка стратегій захисту

Розробка стратегій захисту важлива для банків з метою збереження фінансової стабільності, захисту клієнтів від кіберзагроз та шахрайства, а також дотримання регуляторних вимог. Ефективні заходи захисту допомагають уникнути фінансових втрат та зберегти довіру клієнтів, що є критично важливим для успішної діяльності банку.

Аналіз поточної системи безпеки передбачає всебічне вивчення існуючих заходів безпеки, впроваджених в банку. Ця оцінка охоплює різні аспекти, включаючи оцінку засобів контролю фізичної безпеки, протоколів кібербезпеки, систем управління доступом і процедур реагування на інциденти. Ретельно вивчаючи ці компоненти, банківські організації прагнуть отримати уявлення про ефективність своєї інфраструктури безпеки в захисті від потенційних загроз і вразливостей. Крім того, аналіз передбачає виявлення слабких місць і прогалин у механізмах захисту, які можуть включати застаріле програмне забезпечення, неадекватний контроль доступу, недостатню підготовку співробітників або недостатні можливості моніторингу. Завдяки цьому процесу організації можуть точно визначити зони вразливості та визначити пріоритетні заходи щодо їх усунення, щоб зміцнити свою систему безпеки та зменшити ризик порушень безпеки або витоку даних. Зрештою, аналіз поточної системи безпеки слугує важливою основою для розробки та впровадження цільових заходів з посилення безпеки, які відповідають толерантності до ризиків та бізнес-цілям організації.

Формулювання цілей захисту є найважливішим етапом у розробці стратегії безпеки банку, що включає в себе визначення та встановлення пріоритетів ключових завдань, на які мають бути спрямовані зусилля із захисту. Цей комплексний процес починається з всебічної оцінки активів банку, включаючи дані, системи, інфраструктуру та інтелектуальну власність, щоб визначити їх важливість для підтримки бізнес-операцій і досягнення стратегічних цілей. Розуміючи важливість цих активів, організації можуть встановити чіткі цілі захисту, які відповідають їхній загальній місії та цілям.

Ландшафт загроз відіграє важливу роль у визначенні пріоритетності цілей захисту. Банк повинен оцінювати мінливий ландшафт загроз, включаючи нові кіберзагрози, галузеві ризики та геополітичні фактори, які можуть вплинути на безпеку. Розуміючи характер і серйозність потенційних загроз, банківська установа може адаптувати свої цілі захисту для вирішення найбільш нагальних проблем безпеки та усунення вразливостей. Зрештою, формулювання цілей захисту дозволяє встановити стратегічні рамки для своїх зусиль у сфері безпеки, керуючи розробкою та впровадженням цільових заходів безпеки та контролю.

Розробка заходів безпеки охоплює комплексний підхід, спрямований на зміцнення захисту банку від потенційних загроз і вразливостей. Цей процес передбачає впровадження комбінації технічних, організаційних та фізичних заходів для створення надійної системи безпеки.

Технічні заходи передбачають розгортання передових технологій та інструментів для захисту цифрових активів та інфраструктури. Наприклад, шифрування для захисту даних під час передачі і в стані спокою, антивірусний захист для виявлення і зменшення загроз шкідливого програмного забезпечення, системи виявлення вторгнень (IDS) для моніторингу мережевого трафіку на предмет підозрілої активності, а також брандмауери для контролю доступу до мережевих ресурсів.

Організаційні заходи зосереджені на розробці політик, процедур і практик для управління доступом до інформації та систем, а також на

просуванні культури обізнаності та дотримання вимог безпеки серед співробітників.

Фізичні заходи передбачають захист фізичних приміщень та активів для запобігання несанкціонованому доступу та захисту від фізичних загроз, таких як крадіжки, вандалізм та шпигунство. Це може включати встановлення систем контролю доступу, камер спостереження та сигналізації для моніторингу та обмеження доступу до чутливих зон, а також впровадження протоколів безпеки, таких як реєстрація відвідувачів та процедури перевірки особи.

Інтегруючи технічні, організаційні та фізичні заходи, банки можуть створити комплексну систему безпеки, яка протидіє широкому спектру загроз і вразливостей. Такий комплексний підхід гарантує, що заходи безпеки відповідають профілю ризиків та бізнес-цілям організації, ефективно знижуючи ризики та підвищуючи стійкість до потенційних порушень та збоїв у системі безпеки.

План реагування на інциденти є важливим компонентом стратегії безпеки, покликаним сприяти швидкому та ефективному реагуванню на інциденти безпеки. Цей план передбачає розробку комплексних процедур і протоколів для швидкого виявлення, локалізації та усунення порушень або інцидентів безпеки.

По-перше, розробка процедур передбачає окреслення поетапного процесу виявлення та оцінки інцидентів безпеки, визначення їхньої серйозності та наслідків, а також ініціювання відповідних заходів реагування. Сюди входить визначення чітких ролей та обов'язків членів групи реагування на інциденти, визначення каналів зв'язку та шляхів ескалації, а також координація співпраці з відповідними зацікавленими сторонами, такими як IT-персонал, юрисконсульт та правоохоронні органи.

Крім того, план реагування на інциденти включає положення про навчання групи швидкого реагування, щоб забезпечити її необхідними навичками та знаннями для ефективного виконання своїх функцій та обов'язків під час інциденту безпеки. Таке навчання може включати проведення

регулярних тренувань і практичних занять для моделювання різних сценаріїв загроз безпеці, тестування процедур реагування та оцінки готовності команди до реагування на реальні інциденти. Це допомагає команді реагування бути в курсі нових загроз, нових методів атак та змін у нормативних вимогах, що дозволяє їм адаптуватися та ефективно реагувати на виклики безпеки, які постійно зростають.

Моніторинг та оцінка ефективності стратегій безпеки мають важливе значення для забезпечення надійності та адаптивності захисту банку до мінливих загроз. Це передбачає впровадження комплексної системи моніторингу для відстеження діяльності, пов'язаної з безпекою, в IT-інфраструктурі, мережах і системах організації. Використовуючи рішення для управління інформацією та подіями безпеки (SIEM), системи виявлення вторгнень (IDS) та інші інструменти моніторингу, організації можуть безперервно збирати та аналізувати дані про безпеку, щоб виявляти аномалії, ідентифікувати потенційні загрози та оперативно реагувати на інциденти безпеки.

Крім того, організації повинні встановити ключові показники ефективності і метрики для вимірювання ефективності стратегій безпеки і моніторингу прогресу в досягненні цілей безпеки. Визначивши чіткі орієнтири та цілі, банк може оцінювати вплив ініціатив з безпеки, відстежувати ефективність з плином часу та визначати можливості для оптимізації та вдосконалення. Такий підхід, заснований на даних, дозволяє організаціям приймати обґрунтовані рішення щодо розподілу ресурсів, інвестиційних пріоритетів і стратегій управління ризиками, забезпечуючи відповідність зусиль з безпеки бізнес-пріоритетам і цілям.

3.3 Впровадження та моніторинг заходів захисту

Важливість впровадження ефективних заходів захисту неможливо переоцінити в сучасному цифровому середовищі, де банківські установм

стикаються з безліччю кіберзагроз і викликів безпеці. Ефективні заходи захисту мають важливе значення для захисту конфіденційної інформації, збереження цілісності систем і мереж та підтримки безперервності. Впроваджуючи надійні засоби контролю безпеки, такі як шифрування, контроль доступу та системи виявлення вторгнень, банк може зменшити ризики, запобігти несанкціонованому доступу та мінімізувати наслідки інцидентів безпеки. Крім того, ефективні заходи захисту допомагають зміцнити довіру між зацікавленими сторонами, захистити від фінансових втрат і репутаційних збитків, а також забезпечити відповідність нормативним вимогам.

Процес моніторингу забезпечує банк критично важливим механізмом виявлення, аналізу та реагування на загрози та інциденти безпеки в режимі реального часу. Використовуючи передові інструменти та технології моніторингу, такі як системи управління інформацією та подіями безпеки (SIEM) і системи виявлення вторгнень (IDS), банк може отримати огляд свого IT-середовища, оперативно виявляти порушення безпеки та інциденти, а також ініціювати відповідні заходи реагування для зменшення ризиків і мінімізації впливу на операції та цілісність даних. Крім того, процес моніторингу дозволяє відстежувати продуктивність, вимірювати ефективність засобів контролю безпеки та виявляти можливості для оптимізації та вдосконалення своєї системи безпеки.

Планування впровадження заходів безпеки включає кілька ключових компонентів для забезпечення систематичного та успішного розгортання. По-перше, визначення етапів впровадження має вирішальне значення. Це передбачає розбиття процесу впровадження на керовані етапи, такі як оцінка, планування, тестування, розгортання та постійний моніторинг. Кожен етап має бути чітко визначений з конкретними цілями, завданнями і термінами, щоб ефективно керувати процесом імплементації.

По-друге, розподіл обов'язків між членами команди має важливе значення для забезпечення підзвітності та координації протягом усього процесу імплементації. Це передбачає розподіл ролей та обов'язків між членами

команди на основі їхнього досвіду, навичок та доступності. Ключові обов'язки можуть включати управління проектом, технічну реалізацію, комунікацію із зацікавленими сторонами, тестування та документування. Чітко визначивши ролі та очікування, банк може гарантувати, що кожен член команди розуміє свої обов'язки і робить ефективний внесок у процес впровадження.

Насамкінець, створення графіка впровадження заходів має вирішальне значення для збереження імпульсу і дотримання термінів проекту. Це передбачає розробку детального графіка, який окреслює послідовність завдань, етапів і результатів для кожного етапу процесу імплементації. Графік має враховувати такі фактори, як наявність ресурсів, взаємозв'язки між завданнями, а також потенційні ризики або перешкоди, які можуть вплинути на терміни. Регулярний моніторинг і відстеження прогресу відповідно до графіка дозволяють банківським організаціям виявляти будь-які відхилення або затримки на ранніх стадіях і вживати коригувальних заходів, щоб імплементація не відставала від графіка.

Загалом, ефективне планування впровадження заходів безпеки вимагає ретельного розгляду етапів реалізації, розподілу обов'язків між членами команди та створення реалістичного графіка. Дотримуючись структурованого підходу та залучаючи зацікавлені сторони, установи можуть забезпечити безперебійний та успішний процес впровадження, який посилить їхню позицію безпеки та ефективно зменшить ризики.

Впровадження технічних заходів передбачає розгортання передових технологій та інструментів для захисту цифрових активів та інфраструктури від потенційних загроз і вразливостей.

Організаційні заходи зосереджені на розробці політик, процедур і практик, що регулюють доступ до інформації та систем, а також сприяють формуванню культури обізнаності та дотримання вимог безпеки серед працівників.

Реалізація фізичних заходів передбачає захист фізичних приміщень та активів банку для запобігання несанкціонованому доступу та захисту від фізичних загроз, таких як крадіжки, вандалізм та шпигунство.

Оцінка ефективності заходів безпеки має першорядне значення для забезпечення постійного захисту активів та інформації організації. Цей процес включає кілька ключових компонентів, спрямованих на оцінку надійності та ефективності засобів контролю, політик і процедур безпеки.

Насамперед, проведення регулярних аудитів безпеки має важливе значення для виявлення вразливостей, слабких місць і сфер, які потребують вдосконалення в системі безпеки організації. Також, тестування заходів безпеки за допомогою таких методів, як тестування на проникнення ("пентест") і сканування вразливостей, має вирішальне значення для виявлення та усунення слабких місць у системах і додатках. Окрім цього, оцінка відповідності нормативним вимогам і стандартам має важливе значення для забезпечення відповідності заходів безпеки найкращим галузевим практикам і законодавчим вимогам. Це передбачає оцінку дотримання організацією відповідних нормативних актів, таких як Загальний регламент про захист даних (GDPR), Закон про переносимість і підзвітність у сфері медичного страхування (HIPAA), а також галузевих стандартів, таких як Стандарт безпеки даних індустрії платіжних карток (PCI DSS) і ISO/IEC 27001. Оцінюючи відповідність вимогам, організації можуть виявити прогалини та забезпечити впровадження заходів безпеки відповідно до чинних законів і нормативних актів.

Отже, ефективне впровадження заходів безпеки захищає банківські установи від кіберзагроз, посилюючи захист активів і безперервність операційної діяльності. Постійний моніторинг, навчання та співпраця забезпечують постійну стійкість. Рекомендації включають регулярне оцінювання, підвищення обізнаності працівників, галузеву співпрацю та дотримання нормативних вимог. Ці кроки в сукупності посилюють безпеку, зменшують ризики та сприяють розвитку культури стійкості.

Висновки до 3 розділу

У процесі оцінки потенційних ризиків та вразливостей банку слід проводити регулярний і комплексний аналіз інформаційних систем та інфраструктури. Цей аналіз повинен враховувати як внутрішні, так і зовнішні загрози, включаючи можливі сценарії атак, вразливості програмного забезпечення, а також поведінкові фактори співробітників. Виявлені ризики необхідно ранжувати за рівнем критичності, що дозволить визначити пріоритетні напрямки захисту та оптимально розподілити ресурси для їхньої мінімізації.

Розробка стратегій захисту повинна базуватися на результатах оцінки ризиків і включати комплексний підхід до захисту інформації. Це передбачає впровадження багаторівневих систем захисту, які поєднують технічні, організаційні та адміністративні заходи. Зокрема, важливо розробити політики безпеки, що регламентують доступ до інформації, використання мережевих ресурсів та обробку конфіденційних даних. Крім того, слід передбачити заходи щодо запобігання інцидентам, а також плани реагування та відновлення в разі їхнього виникнення.

Впровадження та моніторинг заходів захисту потребують постійного контролю за станом інформаційної безпеки банку. Це включає регулярне тестування систем захисту, проведення аудитів і перевірок відповідності встановленим стандартам безпеки. Моніторинг повинен здійснюватися у режимі реального часу з використанням сучасних засобів виявлення та реагування на інциденти. Важливо також забезпечити безперервне навчання персоналу щодо актуальних загроз та методів захисту, а також здійснювати оновлення програмного забезпечення і технологій відповідно до новітніх вимог інформаційної безпеки.

ВИСНОВКИ

Дослідження, присвячене побудові типової моделі загроз інформаційній безпеці банку, розкриває комплексний підхід до аналізу та забезпечення безпеки інформаційних ресурсів банківських установ. У рамках роботи було детально розглянуто теоретичні аспекти загроз, проведено ґрунтовний аналіз внутрішніх, зовнішніх та системних загроз, а також запропоновано рекомендації щодо захисту від них.

У першому розділі дослідження зосереджено на теоретичних основах загроз інформаційній безпеці банків. Було виявлено, що сутність загроз полягає у будь-яких діях або подіях, які можуть призвести до порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Класифікація загроз включає внутрішні та зовнішні загрози, фізичні та логічні загрози, а також загрози, що виникають з причин людських помилок, технічних несправностей або зловмисних дій.

Аналіз сучасних методів та засобів захисту інформаційних ресурсів банківських установ показав, що сучасні технології забезпечення інформаційної безпеки включають в себе криптографічні методи, системи виявлення вторгнень, фаєрволи, антивірусне програмне забезпечення та методи управління доступом. Проте, ефективність цих засобів значною мірою залежить від комплексного підходу до їхнього впровадження та постійного моніторингу.

Побудова типової моделі загроз відіграє ключову роль у забезпеченні інформаційної безпеки банку. Така модель дозволяє структуровано підходити до аналізу загроз, визначати потенційні ризики та розробляти адекватні заходи захисту. Типова модель загроз є фундаментом для розробки стратегій захисту, що враховують специфіку банківської діяльності та сучасні тенденції у сфері кібербезпеки.

У другому розділі було проведено детальний аналіз загроз інформаційній безпеці банків. Розгляд внутрішніх загроз показав, що основними ризиками є дії співробітників банку, які можуть бути як навмисними, так і випадковими.

До таких загроз відносяться витік інформації, зловживання доступом, та помилки при роботі з даними. Важливим аспектом є створення ефективної системи управління доступом та проведення регулярного навчання персоналу з питань інформаційної безпеки.

Зовнішні загрози, такі як атаки хакерів, дії кіберзлочинців та конкуренція, потребують постійного моніторингу та аналізу. Сучасні методи захисту від зовнішніх загроз включають використання багаторівневих систем захисту, застосування передових технологій шифрування та регулярні перевірки на вразливості. Особливу увагу слід приділити захисту від фішингових атак та атак типу "відмова в обслуговуванні" (DDoS).

Системні загрози, пов'язані з технічною інфраструктурою банку, включають ризики, пов'язані з апаратним та програмним забезпеченням. Аналіз показав, що важливо регулярно проводити аудит інформаційних систем, оновлювати програмне забезпечення та впроваджувати нові технології захисту. Окрім цього, необхідно забезпечити резервування критичних даних та безперервність бізнес-процесів у разі виникнення технічних збоїв.

У третьому розділі розглянуто рекомендації щодо захисту від загроз інформаційній безпеці банку. Розділ включає три основні підпункти: оцінка потенційних ризиків та вразливостей банку, розробка стратегій захисту, впровадження та моніторинг заходів захисту.

Оцінка потенційних ризиків та вразливостей банку повинна здійснюватися на постійній основі з використанням сучасних методів аналізу ризиків. Це дозволить виявити найбільш критичні вразливості та розробити адекватні заходи захисту. Рекомендується проводити регулярні оцінки безпеки інформаційних систем, залучаючи до цього процесу як внутрішніх, так і зовнішніх експертів.

Розробка стратегій захисту повинна включати комплексний підхід, що враховує всі аспекти інформаційної безпеки. Важливо розробити політики безпеки, які регламентують доступ до інформаційних ресурсів, а також впровадити технічні засоби захисту, такі як системи виявлення вторгнень,

фаєрволи та антивірусне програмне забезпечення. Окрім цього, необхідно передбачити заходи щодо швидкого реагування на інциденти та відновлення інформаційних систем у разі виникнення загроз.

Впровадження та моніторинг заходів захисту включають постійний контроль за станом інформаційної безпеки банку. Важливо забезпечити регулярне тестування систем захисту та проведення аудитів відповідності встановленим стандартам безпеки. Моніторинг повинен здійснюватися у режимі реального часу з використанням сучасних засобів виявлення та реагування на інциденти. Окрім цього, необхідно проводити регулярне навчання персоналу щодо актуальних загроз та методів захисту, а також забезпечувати оновлення програмного забезпечення відповідно до новітніх вимог інформаційної безпеки.

Загалом, побудова типової моделі загроз інформаційній безпеці банку дозволяє структурувати підходи до забезпечення безпеки, оптимально розподілити ресурси та розробити ефективні стратегії захисту. Це є критичним аспектом для забезпечення стійкості банківських установ у сучасному кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Lelyuk N., Rodchenko S. Identification of threats to the financial security of banks. *Technology audit and production reserves*. 2018. Vol. 2, no. 4(46). P. 28–33. URL: https://doi.org/10.15587/2312-8372.2019.168431

2. Плєхова Г., Суханова Н., Левтеров А. Кібербезпека: загрози, рішення. *Theoretical foundations in economics and management*. 2022. P. 681–692. URL: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6

3. Network and Information Security in the Finance Sector. Regulatory landscape and Industry priorities, 2014. ENISA. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj7gIqfiJmFAxX6bPEDHXErAIMQFnoECB0QAQ&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fnetwork-and-information-security-in-the-finance-sector%2F%40%40download%2FfullReport&usg=AOvVaw2_wTayFlnA2q7Rh9zO1r_8&opi=89978449

4. Інформаційна безпека / А. В. Булашенко та ін. 2010. URL: http://essuir.sumdu.edu.ua/handle/123456789/21090

5. Analysing Information Security in a Bank using Soft Systems Methodology. 2017, Edge Hill University. URL: https://research.edgehill.ac.uk/ws/files/20198397/Analysing%20IS%20using%20SSM%20V2.pdf

6. FSI Insights on policy implementation No 2. Regulatory approaches to enhance banks'cyber-security frameworks Bank for International Settlements 2017. URL: https://www.bis.org/fsi/publ/insights2.pdf

7. DOROSH I. Cyber security and its role in the financial sector: threats and protection measures. *Economics. Finances. Law.* 2023. Vol. 10, no. -. P. 48–51. URL: https://doi.org/10.37634/efp.2023.10.10

8. F. Mahardika. Information Security Risk Assessment For Banking. Global Journal of Computer Science and Technology. 2010, Vol. 10 Issue 10, P. 44-55. URL: https://www.academia.edu/5167208/Information_Security_Risk_Assessment_For_Banking

9. F. Curti, J. Gerlach, S. Kazinnik, M. Lee, A. Mihov. Cyber Risk Definition and Classification for Financial Risk Management. Federal Reserve Bank of Richmond. 2021. URL: https://www.richmondfed.org/-/media/RichmondFedOrg/banking/qsr-people/pdf/Cyber_Risk_Classification_White_Paper_2022.pdf

10. Banking Information Resource Cybersecurity System Modeling / O. Shulha et al. *Journal of Open Innovation: Technology, Market, and Complexity*. 2022. Vol. 8, no. 2. P. 80. URL: https://doi.org/10.3390/joitmc8020080

11. Information Security Policy. PrivatBank. URL: https://static.privatbank.ua/files/00000033010331111.1.0.pdf

12. Davydenko N., Lutsyk Y., Buriak A., Vovk L. Informational and Analytical Systems for Forecasting the Indicators of Financial Security of the Banking System of Ukraine. *Journal of Information Technology Management*. 2023, Vol. 15, Issue 2, P. 1-13. URL: https://www.academia.edu/108152675/Informational_and_Analytical_Systems_for_Forecasting_the_Indicators_of_Financial_Security_of_the_Banking_System_of_Ukraine

13. Gulyas O., Kiss G. Cybersecurity threats in the banking sector. *2022 8th international conference on control, decision and information technologies (codit)*, Istanbul, Turkey, 17–20 May 2022. 2022. URL: https://doi.org/10.1109/codit55151.2022.9804140

14. Iskuja I. Cybersecurity threats. *SSRN electronic journal*. 2024. URL: https://doi.org/10.2139/ssrn.4723335

15. Karthik Meduri. Cybersecurity threats in banking: unsupervised fraud detection analysis. *International journal of science and research archive*. 2024. Vol. 11, no. 2. P. 915–925. URL: https://doi.org/10.30574/ijsra.2024.11.2.0505

16. Sharma V. Securing payments and banking systems from cybersecurity threats. *Journal of economics & management research*. 2021. P. 1–4. URL: https://doi.org/10.47363/jesmr/2021(2)207

17. Hudaib A. Banking and Modern Payments System Security Analysis. International Journal of Computer Science and Security. 2014, Vol. 8, Issue 2. P. 38-62. URL: https://www.academia.edu/9252589/Banking_and_Modern_Payments_System_Security_Analysis

18. Hryshchuk R., Yevseiev S., Shmatko A. Construction methodology of information security system of banking information in automated banking systems : monograph. Vienna : Premier Publishing s.r.o., 2018. 284 p. URL: https://web.archive.org/web/20190429093000id_/http://ppublishing.org/upload/iblock/377/Mono_Shmatko_site.pdf

19. The Importance of Information Security for Financial Institutions and Proposed Countermeasures. With a Focus on Internet-Based Financial Service. *Bank of Japan*, 2000. URL: https://www.boj.or.jp/en/research/brp/ron_2000/data/fsk0004b.pdf

20. Information Security in the Banking Sector: A Systematic Literature Review on Current Trends, Issues, and Challenges / A. L. V. Ubaldo et al. *International Journal of Safety and Security Engineering*. 2023. Vol. 13, no. 1. P. 97–106. URL: https://doi.org/10.18280/ijsse.130111

21. A. Shostack Threat Modeling: Designing for Security. Indianapolis : John Wiley & Sons, Inc., 2014. 627 p. URL: https://terrorgum.com/tfox/books/threat_modeling_designing_for_security.pdf

22. C. Möckel1, A. Abdallah. Understanding the Value and Potential of Threat Modeling for Application Security Design – An E-Banking Case Study.

Journal of Information Assurance and Security. 2011, Vol. 6, P. 346-356. URL: https://mirlabs.org/jias/secured/Volume6-Issue5/Paper36.pdf

23. Kondratyeva M. N., Svirina D. D., Tsvetkov A. I. The role of information technologies in ensuring banking security. *IOP Conference Series: Materials Science and Engineering*. 2021. Vol. 1047, no. 1. P. 012069. URL: https://doi.org/10.1088/1757-899x/1047/1/012069

24. Грищук Р. В., Євсеєв С. П. Methodology of building a system for providing information security of bank information in automated banking systems. *Ukrainian Scientific Journal of Information Security*. 2018. Vol. 23, no. 3. URL: https://doi.org/10.18372/2225-5036.23.12095

25. Baur-Yazbeck S. Frickenstein J., Medine D. Cyber security in financial sector development. Challenges and potential solutions for financial inclusion. *Federal Ministry for Economic Cooperation and Development*. 2019. URL: https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf

26. Sharing of Threat and Vulnerability Information with Financial Institutions. *Office of Inspector General* : Evaluation Report. 2023. URL: https://www.fdicoig.gov/sites/default/files/reports/2023-08/EVAL-23-002%20REDACTED%20FINAL_0.pdf

27. Conklin L. Threat Modeling Process. *Owasp* : веб-сайт. URL: https://owasp.org/www-community/Threat_Modeling_Process#

28. Мінімальні вимоги до капіталу під операційний ризик. *Національний банк України*. URL: https://bank.gov.ua/admin_uploads/article/Operational_risk_2019-10_pr.pdf?v=4

29. Bucăţa G., Rizescu A.-M., Herman R.-E. The Risk of Personnel Management. *International conference KNOWLEDGE-BASED ORGANIZATION*. 2022. Vol. 28, no. 1. P. 169–179. URL: https://doi.org/10.2478/kbo-2022-0026

30. Гончарова К. Г. Кадрова безпека, як складова економічної безпеки банківської установи. *Ефективна економіка*, 2015. № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=4602

31. Risk Management Strategy. *JSC «Deutsche Bank DBU».* 2016. URL: https://country.db.com/ukraine/documents/Corporate-documents-/P-009-Risk-management-strategy-DBU-12-2023.pdf

32. Cerrone R. Banks' internal controls and risk management: Value-added functions in Italian credit cooperative banks. *Risk Governance and Control: Financial Markets and Institutions.* 2013. Vol. 3, no. 4. P. 16–27. URL: https://doi.org/10.22495/rgcv3i4art2

33. О. С. Дмитрова. Классифікація загроз та ризиків економічної безпеки банку. *Ефективна економіка*. 2015, № 11. URL: http://www.economy.nayka.com.ua/?op=1&z=4599

34. Prymostka L. O., Prymostka O. O. Risk-oriented management in the bank. *Financial and credit activity: problems of theory and practice*. 2019. Vol. 2, no. 29. P. 66–72. URL: https://doi.org/10.18371/fcaptp.v2i29.172224

35. The Bank's Integrity Risks Policy and Terms of Reference for the Office of the Chief Compliance Officer. European Bank for Reconstruction and Development. URL: https://www.ebrd.com/downloads/integrity/integrityriskpol.pdf

36. Grdošić L. Operational Risks in the Banking Industry. *IRENET – Society for Advancing Innovation and Research in Economy* : Conference Paper. URL: https://www.econstor.eu/bitstream/10419/183734/1/47-ENT61-Grdosic-330-337.pdf

37. Cyber security threats: A never-ending challenge for e-commerce / X. Liu et al. *Frontiers in Psychology*. 2022. Vol. 13. URL: https://doi.org/10.3389/fpsyg.2022.927398

38. Frauenstein E. A Framework to Mitigate Phishing Threats. Nelson Mandela Metropolitan University, 2013. URL: https://core.ac.uk/download/pdf/145052362.pdf

39. Overview of Threats in Cyberspace. Public security intelligence agency. URL: https://www.moj.go.jp/content/001381943.pdf

40. Cyber: The changing threat landscape. Risk trends, responses and the outlook for insurance. Allianz Global Corporate & Specialty. 2022. URL:

https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/agcs-cyber-risk-trends-2022.pdf

41. CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations. *Bank of England*, 2016. URL: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf

42. Stanikzai A. Q., Shah M. A. Evaluation of Cyber Security Threats in Banking Systems. *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, Orlando, FL, USA, 5–7 December 2021. 2021. URL: https://doi.org/10.1109/ssci50451.2021.9659862

43. Kaffenberger L., Kopp E. Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment. *Carnegie Endowment for International Peace*. 2019. URL: https://carnegieendowment.org/files/Kaffenberger_Cyber_Risk_Scenarios_final1.pdf

44. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *Journal of System and Management Sciences*. 2022. URL: https://doi.org/10.33168/jsms.2022.0310

45. Risk management. / ed. by M. G. M. Association. Englewood, CO : Medical Group Management Association, 2008.

46. A new look at global banking vulnerabilities. *International Monetary Fund.* 2023. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjL5K-_u5qFAxUYHxAIHfHwAjYQFnoECB0QAQ&url=https%3A%2F%2Fwww.imf.org%2F-%2Fmedia%2FFiles%2FPublications%2FGFSR%2F2023%2FOctober%2FEnglish%2Fch2.ashx&usg=AOvVaw0hMyFKVDydbDEpx3N2CbU9&opi=89978449