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: “ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ СПРОБІ РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

_____ Дмитро КАБЛУЧКО

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Дмитро КАБЛУЧКО

Керівник:
д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:
д.т.н., професор Олександр ТУРОВСЬКИЙ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____"_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Каблучку Дмитру Максимовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Технології захисту інформації при спробі рейдерського захоплення кредитно-фінансової установи"

керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА, д.е.н., професор
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *технології захисту інформації, методи та засоби захисту інформації, кредитно-фінансової установа, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література.*
4. Перелік питань, які потрібно розробити:
   1. Проаналізувати стан і можливості комплексних систем захисту інформації кредитно-фінансової установи;
   2. Провести аналіз комплексу моделей системи захисту інформації кредитно-фінансової установи;
   3. Розробити методику організації динамічного захисту інформації кредитно-фінансового установи при спробі рейдерського захоплення;
   4. Розробити організаційно-практичні рекомендації з реалізації захисту інформації структурним підрозділам кредитно-фінансової установи.
5. Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання "26" вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”26” вересня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2023	виконано
2.	Збір та аналіз літератури.	03.10.2023	виконано
3.	Аналіз стану і можливостей комплексних систем захисту інформації кредитно-фінансової установи	17.10.2023	виконано
4.	Аналіз практичного використання комплексу моделей системи захисту інформації кредитно-фінансової установи	31.10.2023	виконано
5.	Визначення методики організації динамічного захисту інформації кредитно-фінансової установи при спробі рейдерського захоплення	14.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження.	01.12.2023	виконано
7.	Оформлення роботи.	08.12.2023	виконано
8.	Оформлення презентації.	15.12.2023	виконано
9.	Отримання рецензії на роботу.	23.12.2023	виконано
10.	Захист в ДЕК.	16.01.2024	виконано

Здобувач вищої освіти _____ Дмитро КАБЛУЧКО
(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 магістра

Направляється здобувач Каблучко Д.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Технології захисту інформації при спробі рейдерського захоплення кредитно-фінансової установи"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **КАБЛУЧКО Дмитро** у кваліфікаційній роботі дослідив сучасний стан та можливості комплексних систем захисту інформації кредитно-фінансової установи, структурував та проаналізував моделі захисту інформації, виявив позитивні та недосконалі аспекти роботи системи захисту, приділив увагу методичним засадам динамічного захисту саме під час рейдерських атак на інформаційну систему, розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки кредитно-фінансової установи щодо підвищення ефективності захисту інформаційної системи установи. **КАБЛУЧКО Дмитро** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на трьох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **КАБЛУЧКУ Дмитру** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Каблучко Д.М. допускається до захисту роботи в екзаменаційної комісії**.**

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

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Каблучка Дмитра Максимовича
на тему **“ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ СПРОБІ РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВИ”**

Актуальність Зміна ландшафту загроз інформаційній безпеці організацій вимагає удосконалення систем захисту інформації, застосування новітніх технологій процедури реагування на інциденти та події, які мотивовані захопленням конфіденційної інформації з метою отримання економічної або іншої вигоди, тому обрана тема є актуальною та своєчасною.

Позитивні сторони

1. Автором детально проаналізована проблематика інформаційної безпеки кредитно-фінансової установи: особливості, основні загрози. Розглянута нормативно-правова база забезпечення захисту інформації у кредитно-фінансовій установі.
2. Окреслено модель динамічного середовища інформаційних загроз рейдерського захоплення установи, модель формування базового та маневреного комплекту сил та засобів захисту інформації кредитно-фінансової установи, модель захищеності інформаційного вузла інформаційної структури кредитно-фінансової установи.
3. Розроблено рекомендації керівництву установи для підвищення ефективності захисту інформаційної безпеки установи.

Недоліки

1. Робота суттєво виграла б, якщо б була досконало проаналізована сучасна технологія, яка дозволяє протистояти кібератакам високого ступеня ризику.

Відзначене зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує позитивну оцінку, а здобувач КАБЛУЧКО Дмитро - присвоєння кваліфікації магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент: завідувач кафедри Систем інформаційного та кібернетичного захисту
д.т.н, професор _____ Олександр ТУРОВСЬКИЙ
підпис *(Ім’я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 84 аркушів, 12 рис., 1 табл., 32 джерела.

Метою роботи є дослідження технології захисту інформації при спробі рейдерського захоплення банківської установи

Об'єктом дослідження є система захисту кредитно-фінансової установи.

Предметом дослідження є організація захисту інформації кредитно-фінансової установи.

Метою дослідження є підвищення рівня інформаційної безпеки кредитно-фінансової установи за рахунок розроблення методичного апарату динамічного захисту інформації кредитно-фінансової установи.

Наукова новизна дослідження полягає у розробці теоретичних та науково-практичних положень, що розвивають основні напрямки та вдосконалюють систему захисту інформації кредитно-фінансової установи шляхом динамічного розподілу сил та засобів захисту за елементами інформаційної структури об'єкта.

Галузь застосування. Результати цієї роботи можуть бути використані для управління інформаційною безпекою підприємств, що використовують інформаційні технології в своїй діяльності.

КЛЮЧОВІ СЛОВА : ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ, КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВА.

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 84 pages, 12 figures, 1 tables, 32 sources.

Object of research the study of Information Security Technology in the case of an attempted hostile takeover of a banking institution.

The object of the research is the security system of a credit and financial institution.

The subject of the research is the organization of information security in a credit and financial institution.

The aim of the research is to enhance the level of information security in the credit and financial institution by developing a methodological framework for dynamic information protection.

The scientific novelty of the research lies in the development of theoretical and scientific-practical provisions that advance the main directions and improve the information security system of a credit and financial institution through dynamic allocation of forces and means of protection based on the elements of the object's information structure.

Application field. The results of this work can be used for managing information security in enterprises that utilize information technologies in their operations.

KEYWORDS:. INFORMATION PROTECTION TECHNOLOGIES, METHODS AND MEANS OF INFORMATION PROTECTION, CREDIT AND FINANCIAL INSTITUTION

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЗУ – Закон України

РНКО – розрахункові небанківські кредитні організації;

НКДО – небанківські кредитно-депозитні організації

ПНКО – платіжні небанківські кредитні організації

ІХС – програмно-технічний комплекс

ІС – інформаційні системи

НБУ – Національний банк України

БД – Безпека доступу

Р – Ризик

З – Загроза

МБ – Мережева безпека

БД – Безпека даних

ФБ – Фізична безпека

БПЗ – Безпека програмного забезпечення

ВСТУП

*Актуальність теми***.** Однією з особливостей сучасного інформаційного суспільства є перетворення інформації на найважливіший ресурс, необхідний ефективного функціонування об'єктів будь-якої природи. У цьому частка інформаційного ресурсу у загальному обсязі ресурсомісткості об'єкта постійно зростає, й у наш час досягла величини 85 %. З іншого боку, ця ж особливість зумовила різке зростання уваги до інформаційного ресурсу об'єкта з боку кримінальних і подібних структур, зацікавлених у зміні статусу даного об'єкта.

Максимальну цінність з цієї точки зору має інсайдерська інформація про фінансові потоки і процеси, що протікають всередині об'єкта, що цікавиться. У зв'язку з тим, що кредитно-фінансова установа є основним елементом фінансової системи країни, необхідно звернути особливу увагу забезпечення захисту цього елемента. Метою порушення безпеки кредитно-фінансової установи можуть бути: розкрадання грошових коштів, фінансові махінації, шахрайство, незаконне переведення в готівку, “відмивання” грошових коштів, незаконне отримання коштів, неправомірне отримання контролю над активами кредитно-фінансової установи або безпосередньо над самою кредитно-фінансовою установою . У наведеному переліку найбільшу небезпеку становить остання зазначена загроза - загроза неправомірного отримання контролю за кредитно-фінансовою установою загалом, її активами або їхньою частиною. Іншими словами, рейдерське захоплення.

Рейдерське захоплення є комплексом узгоджених і взаємопов'язаних за цілями, завданнями, місцем і часом заходів, що проводяться за єдиним задумом і планом різними (у тому числі кримінальними) структурами, з метою поглинання суб'єкта господарювання проти волі його власників, які мають переважне становище в даному суб'єкті господарювання. , та/або його керівника.

На кожному етапі рейдерського захоплення потрібна інформація, що зберігається в різних елементах інформаційної структури кредитно-фінансової установи, до якої входять: інформація/дані на паперових та електронних носіях,

корпоративна інформаційна система, робочі станції тощо. Тому на кожному етапі рейдерського захоплення спектр інформаційних загроз та їх інтенсивність можуть бути різними. З іншого боку, існуючі підходи до захисту інформації орієнтовані на середньостатистичний потік загроз. Процедуру побудову інформаційного захисту кредитно-фінансових установ жорстко регламентовано. При різкому збільшенні інтенсивності потоку інформаційних загроз, що притаманно низки етапів рейдерського захоплення, забезпечення захисту стає проблематичним. У зв'язку з цим виникає важливе наукове завдання щодо розробки динамічної моделі захисту інформації при спробі рейдерського захоплення кредитно-фінансової установи. Ця обставина зумовлює актуальність теми цієї магістерської роботи, що дозволяє вдосконалити систему захисту кредитно-фінансової установи.

Важливою особливістю інформаційного забезпечення діяльності кредитно-фінансової установи є наявність значного обсягу програмного забезпечення, що працює з фінансовою інформацією, одержання якої сприяє прийняттю рішення щодо проведення щодо відповідної кредитно-фінансової установи неправомірних дій.

Ступінь розробленості теми дослідження. Питанням побудови інформаційної безпеки та захисту інформації присвячені роботи таких вчених, як Акімов Є.Є., Вишняков С.М., Гуляєв А.П., Алавердов А.Р., Вихорєв С.В., Жигулін Г.П., Заплатинський В.М. , Конєв І.Р., Бєляєв А.В., Левкін І.М., Ясенєв В.М.

Метою дослідження є підвищення рівня інформаційної безпеки кредитно-фінансової установи за рахунок розроблення методичного апарату динамічного захисту інформації кредитно-фінансової установи.

Для досягнення цієї мети необхідно вирішити такі *завдання*:

1) провести аналіз загроз інформаційній безпеці кредитно-фінансової установи;

2) провести аналіз стану та можливостей системи захисту інформації кредитно-фінансової установи;

3) розробити структуру динамічної моделі захисту інформації кредитно-фінансового закладу;

4) розробити елементи динамічної моделі захисту інформації кредитно-фінансової установи;

5) розробити методику застосування динамічної моделі захисту інформації кредитно-фінансової установи;

6) запропонувати практичні рекомендації відповідальним структурним підрозділам щодо забезпечення захисту інформації кредитно-фінансової установи.

Об'єктом дослідження є система захисту кредитно-фінансової установи.

Предметом дослідження є організація захисту інформації кредитно-фінансової установи.

Наукова новизна дослідження полягає у розробці теоретичних та науково-практичних положень, що розвивають основні напрямки та вдосконалюють систему захисту інформації кредитно-фінансової установи шляхом динамічного розподілу сил та засобів захисту за елементами інформаційної структури об'єкта.

Теоретична значущість дослідження характеризується розвитком основних положень теорії захисту інформації, присвяченим: удосконаленню наявних методів забезпечення інформаційної безпеки та захисту інформації, методів, моделей та засобів виявлення, ідентифікації загроз порушення інформаційної безпеки кредитно-фінансових установ; розроблення динамічної моделі захисту інформації кредитно-фінансової установи, що сприяє протидії загрозам розкрадання (руйнування, модифікації) інформації та порушення інформаційної безпеки кредитно-фінансової установи; розроблення організаційно-практичних рекомендацій щодо реалізації заходів формування забезпечення інформаційної безпеки для кредитно-фінансових установ при рейдерському захопленні.

Практична значущість дослідження полягає у створенні методичного апарату, що дозволяє:

1) своєчасно прогнозувати зростання інтенсивності загроз інформаційній безпеці кредитно-фінансової установи;

2) побудувати систему динамічного захисту інформації кредитно-фінансової установи.

Методи дослідження: системний аналіз, методи теорії ймовірностей, методи теорії інформаційної безпеки, методи математичного моделювання та математичної статистики, методи дослідження операцій, а також наукові роботи провідних фахівців та науковців у галузі інформаційної безпеки, загальнонаукові та спеціалізовані методи пізнання, нормативно-правові документи, фундаментальна довідкова та енциклопедична література.

РОЗДІЛ 1
АНАЛІЗ СТАНУ І МОЖЛИВОСТЕЙ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВИ

1.1. Особливості банківської системи України

Важливим та невід'ємним елементом сталого становища будь-якої країни є її фінансова система. Під фінансовою системою України мають на увазі [14]: сукупність різних сфер фінансових відносин у рамках цієї країни; сукупність фінансових установ країни, у широкому значенні охоплює і кредитні установи.

Фінансові відносини між суб'єктами обслуговують фінансові установи та кредитні організації. Під фінансовою установою розуміють юридичну особу, яка здійснює на підставі відповідної ліцензії банківські операції та угоди або надає послуги на ринку цінних паперів, послуги зі страхування або інші послуги фінансового характеру, а також недержавний пенсійний фонд, його керуюча компанія, керуюча компанія пайового інвестиційного фонду, лізингова компанія, кредитний споживчий союз та інша організація, яка здійснює операції та угоди на ринку фінансових послуг [2].

Кредитні організації також у свою чергу становлять банківську систему. В Україні банківська система має два рівні. Перший (верхній) рівень – Національний Банк України, другий (нижній) рівень – сукупність кредитних організацій. Кредитні організації, своєю чергою, поділяються на банки та небанківські кредитні організації. Схематично банківська система України представлена рис. 1.1.

Рис. 1.1. Структура банківської системи України

Згідно з Законом України “Про банки та банківську діяльність” [1], кредитна організація — це юридична особа, яка для отримання прибутку як основної мети своєї діяльності на підставі спеціального дозволу (ліцензії) Національного Банку України має право здійснювати банківські операції <...>. Кредитна організація утворюється з урахуванням будь-якої форми власності як господарське суспільство.

Відповідно до ст. 5 згаданого ЗУ [1], кредитні організації здійснюють такі банківські операції та угоди:

1) до банківських операцій належать:

залучення коштів фізичних та юридичних осіб у вклади (до запитання та на визначений термін);

розміщення залучених коштів від свого імені та за свій рахунок;

відкриття та ведення банківських рахунків фізичних та юридичних осіб;

здійснення переказів коштів за дорученням фізичних та юридичних осіб, у тому числі банків-кореспондентів, за їх банківськими рахунками;

інкасація коштів, векселів, платіжних та розрахункових документів та касове обслуговування фізичних та юридичних осіб;

купівля-продаж іноземної валюти у готівковій та безготівковій формах;

залучення у вклади та розміщення дорогоцінних металів;

видача банківських гарантій;

здійснення переказів коштів без відкриття банківських рахунків, у тому числі електронних коштів (за винятком поштових переказів).

2) до угод належить:

видача поруки за третіх осіб, які передбачають виконання зобов'язань у грошовій формі;

набуття права вимоги від третіх осіб виконання зобов'язань у грошовій формі;

довірче управління грошима та іншим майном за договором з фізичними та юридичними особами;

здійснення операцій з дорогоцінними металами та дорогоцінним камінням відповідно до законодавства України;

надання в оренду фізичним та юридичним особам спеціальних приміщень або сейфів для зберігання документів і цінностей;

лізингові операції;

надання консультаційних та інформаційних послуг.

Кредитна організація має право також здійснювати інші угоди відповідно до законодавства України [1].

Схематично наявну, відповідно до закону ЗУ “Про банки та банківську діяльність” [1], класифікацію кредитних організацій представимо на рис. 1.2.

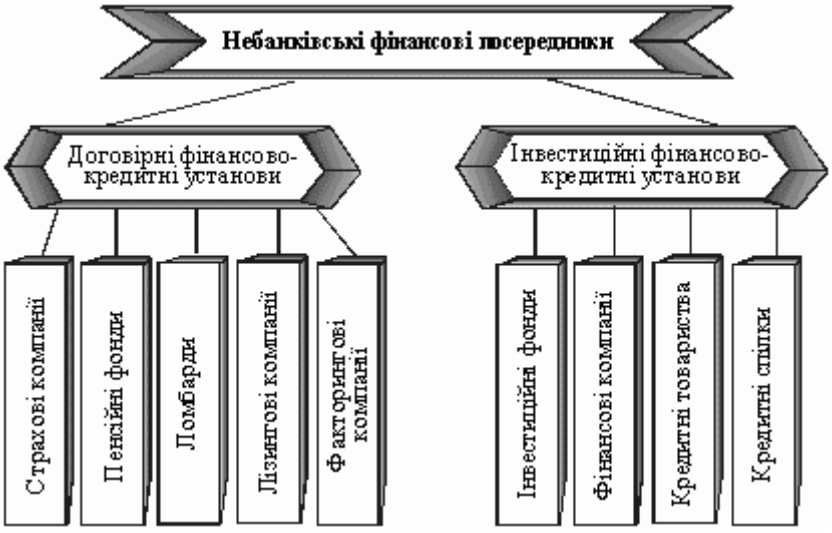

Рис. 1.2 Види кредитних організацій

де:

• РНКО – розрахункові небанківські кредитні організації;

• НКДО – небанківські кредитно-депозитні організації;

• ПНКО – платіжні небанківські кредитні організації.

Банк являє собою кредитну організацію, що має виключне та ліцензоване право здійснювати операції із залучення в якості вкладів грошових коштів фізичних та юридичних осіб, розміщення коштів від свого імені та за свій рахунок на умовах повернення, платності, терміновості, відкриття та ведення рахунків фізичних та юридичних осіб [1].

Небанківська кредитна організація - кредитна організація, має право здійснювати окремі банківські операції, передбачені Законом України [1]. Допустимі поєднання банківських операцій для небанківських кредитних організацій встановлюються НБУ.

Мікрофінансова організація - юридична особа, зареєстрована у формі фонду, автономної некомерційної організації, установи (за винятком бюджетної установи), некомерційного партнерства, господарського товариства або товариства, що дає макрофінансову діяльність та внесене до державного реєстру мікрофінансових організацій у порядку, передбаченому цим Законом України [3].

Суть діяльності мікрофінансової організації полягає у отриманні прибутку шляхом розміщення залучених коштів у вигляді мікропозик. Під мікропозикою розуміють позику, що надається позикодавцем (у даному випадку, мікрофінансовою організацією) позичальнику на умовах, передбачених договором позики, у сумі, що не перевищує мільйон гривень [3]. Кошти залучаються як позик і (чи) кредитів, добровільних (благодійних) внесків і пожертвувань, соціальній та інших не заборонених законами формах крім залучення коштів фізичних осіб у вклади [3]. Особливістю діяльності мікрофінансових організацій є клієнтоорієнтованість на фізичних осіб, швидке прийняття рішення щодо обігу та високий відсоток, під який розмішуються кошти, величина відсотка обумовлена закладеними ризиками неповернення, що виникають через обмежений час прийняття рішення про можливість кредитування.

Небанківські кредитні організації, своєю чергою, можна поділити на: розрахункові небанківські кредитні організації (РНКО), платіжні небанківські кредитні організації (ПНКО), небанківські депозитно-кредитні організації (НДКО).

Розрахункові небанківські кредитні організації - є найпоширенішим видом небанківських кредитних організацій, здійснюють розрахункові операції. Це організації, які здійснюють розрахункові операції, такі як відкриття та ведення банківських рахунків юридичних осіб, здійснення розрахунків за дорученням юридичних осіб за їх банківськими рахунками, інкасацію коштів, векселів, платіжних та розрахункових документів, касове обслуговування юридичних осіб, купівлю-продаж іноземної валюти безготівковій формі та ведення діяльності на ринку цінних паперів.

Платіжна небанківська кредитна організація здійснює грошові перекази без відкриття банківських рахунків та пов'язаних з ними інших банківських операцій. Порівняно з розрахунковою платіжною небанківською кредитною організацією

дозволено вужче коло операцій. Основна функція – забезпечення існування безризикової системи переказів у рамках організації платежів (миттєвих, електронних, мобільних).

Депозитно-кредитні небанківські організації мають право здійснювати діяльність тільки із залучення коштів юридичних осіб у вклади (на певний термін), розміщення залучених у вклади грошових коштів юридичних осіб від свого імені та за свій рахунок, купівлі-продажу іноземної валюти у безготівковій формі (дану операцію НДКО вправі здійснювати виключно від свого імені та власним коштом), видавати банківські гарантії, а також здійснювати діяльність на ринку цінних паперів.

Особливістю діяльності розрахункових небанківських кредитних організацій є обмежений спектр послуг, мікрофінансові організації вузько орієнтовані і так само обмежені за видами та обсягами діяльності, таким чином, найбільш привабливим об'єктом з точки зору організації різноманітних атак є саме банки через можливість широкого залучення, розміщення, акумулювання грошових коштів, інших активів, інформації, даних та їхньої універсальної спрямованості діяльності.

Банк, як юридична особа, входить в основу фінансової системи країни і є елементом кредитної системи країни, а так само є, виходячи з наведеного вище визначення фінансовою установою, у зв'язку з цим будемо позначати банк як кредитно-фінансове у установа.

У процесі здійснення своєї діяльності та мінімізації ризиків у кредитно-фінансових установах протікають певні інформаційні процеси, а саме:

одержання вхідних даних;

обробка вхідних даних та/або зміна власного внутрішнього стану (внутрішніх зв'язків/взаємодії);

уявлення результату чи зміна свого зовнішнього стану (зовнішніх зв'язків/взаємин);

надання мотивованого висновку щодо того чи іншого питання професійної діяльності кредитно-фінансової установи.

Здійснення зазначених процесів дозволяє говорити про кредитно-фінансові установи як про повноцінні інформаційні системи, що включають інформаційні вузли і обслуговують їх інформаційні потоки. Дані інформаційні системи та їх специфічної за діяльністю інформаційною структурою акумулюють у собі великий обсяг конфіденційної інформації про фізичних та юридичних осіб, фінансові потоки, грошові кошти, пропоновані продукти, активи самої кредитно-фінансової установи та її фінансове становище. З урахуванням викладеної специфіки діяльності кредитно-фінансових установ можна зробити висновок, що ці установи є найбільш привабливими об'єктами для здійснення різноманітних атак, у зв'язку з цим дані інформаційні системи гостро потребують забезпечення їх безпечного функціонування.

1.2 Аналіз інформаційної структури кредитно-фінансової установи

Інформаційна банківська система (ІХС) - програмно-технічний комплекс, який автоматизує обробку банківської інформації, що відбиває різні сторони діяльності банків, з урахуванням використання спеціалізованих банківських технологій.

Специфіка діяльності банку визначає архітектуру ІС, що інтегрується, а також тип інформаційного продукту, що використовується для забезпечення процесу прийняття рішень з управління його діяльністю. Характерною особливістю сучасних вітчизняних комерційних банків полягає в тому, що їхня виробнича діяльність, з урахуванням специфіки та спеціалізації, є в цілому універсальною. Багато в чому це визначає сферу палітри послуг і є підставою для аналізу структури ІС банку.

Слід зазначити, що специфіка організації виробничої діяльності в сучасному банківському бізнесі не передбачає необхідності в інтеграції та виконанні трудомістких та ресурсомістких обчислювальних розрахунків (наприклад, пошук оптимального плану у вантажних операціях). При цьому головними проблемами є обсяги облікової інформації та безпека доступу.

Тому в основі автоматизації банківської системи лежить середовище зберігання та доступу до даних. Середовище має забезпечувати рівень надійності зберігання та ефективність доступу. Відповідні сфери інформації повинні мати максимальну захищеність від несанкціонованого доступу. Також, структура інформаційної системи комерційного банку має базуватися та проектуватися у відповідність до його організаційної структури.

У загальному вигляді ця структура наведена на рис.3.

Рис.1.3 Організаційна структура банку

Головними складовими структури ІС банку є:

Інформаційне забезпечення. Являє собою сукупність всієї інформації, що зберігається в банку (системи різних фінансових показників, методи кодування інформації та документів, бази даних і бази знань).

Функціональне забезпечення. Необхідно на формування змістовної спрямованості ІВ КБ, реалізується у вигляді низки операцій та функцій.

Технологічне забезпечення виявляється у вигляді сукупності проектних рішень. Необхідно визначення технології створення технологічних умов задля забезпечення коректного виконання банківських операцій у автоматичному режимі. Даний тип забезпечення поєднує інформаційне та функціональне. Базовим елементом виступає зовнішня подія, у разі реакції ініціюється виконання низки технологічних операцій, певним чином взаємопов'язаних.

Програмне забезпечення. Полягає в інтеграції операційних систем із розгорнутими системами управління базами даних та модулями реалізації програмних інтерфейсів.

Апаратні засоби. Як правило, це засоби обчислювальної техніки, обладнання локальних та глобальних обчислювальних мереж, засоби зв'язку, платіжні термінали та банкомати.

Таким чином, структура ІС банку повинна бути максимально універсальним програмно-технологічним комплексом, що дозволяє задовольнити всі вимоги, що пред'являються до безпеки і ефективно використовується для забезпечення збалансованості всіх інформаційних і матеріальних ресурсів. Така ІС повинна дозволяти адекватно відображати специфіку взаємодії та взаємозв'язків всіх наявних бізнес-процесів, а також враховувати топологію ієрархічної організаційної структури компанії, різні функціональні цілі та операційні завдання, гнучкість у роботі із забезпечення завдань управління процесами, які найчастіше носять імовірнісний та малопередбачуваний.

1.3 Аналіз загроз інформаційній безпеці кредитно-фінансової установи

В даний час ролі банківської системи у розвитку економіки будь-якої країни та забезпечення різних аспектів її як економічної, так і в цілому національної безпеки приділяється підвищена увага. Банки, будучи структурним елементом фінансової системи будь-якої держави, дозволяють забезпечити її ефективне функціонування, виконуючи найрізноманітніші функції. При цьому банківська система надає величезний вплив на безпеку держави, оскільки в значній мірі саме вона дозволяє забезпечити ефективне функціонування як окремих суб'єктів господарювання, так і всієї національної економіки в цілому. Дані обставини зумовлюють необхідність реалізації комплексного підходу до виявлення ключових ризиків та загроз, що визначають найважливіші напрями забезпечення безпеки банківської системи України.

На етапі в спеціалізованої літературі відсутня загальновизнана класифікація загроз банківської системи. Аналіз існуючих підходів дозволяє сформувати таку узагальнену класифікацію основних видів загроз безпеці банківської системи:

1) зовнішні загрози:

несприятлива ринкова кон'юнктура;

криміналізація та шахрайство у банківському секторі;

політичні, економічні, соціальні та інші зміни;

зростання випадків легалізації доходів, одержаних злочинним шляхом;

посилення політики у сфері ліцензування кредитних організацій;

зростання частки іноземного капіталу в активах кредитних організацій країни;

ослаблення національної валюти.

2) внутрішні загрози:

зниження конкурентоспроможності банківських послуг та продуктів;

низька професійна кваліфікація кадрів;

втрата ліквідності банківського сектора;

зниження фінансової стійкості банківського сектора;

порушення законодавства у галузі банківської сфери;

нестабільність інформаційного забезпечення банківської системи.

Також велика кількість фахівців як одна з суттєвих загроз безпеці вітчизняної банківської системи виділяють досить високий рівень монополізації вітчизняного банківського сектора.

У своєму річному звіті за 2021 рік НБУ визначив такі основні ризики, яким схильна національна банківська система в даний час, водночас вказавши на їх певне зниження:

ризики ліквідності (у 2021 році залишалися на прийнятному рівні);

кредитний ризик (частка простроченої заборгованості за кредитами нефінансовим організаціям та фізичним особам знизилася на 0,7%);

ризики банків за кредитами нефінансовим організаціям (частка простроченої заборгованості зменшилась на 0,4%);

ризики за кредитами фізичним особам (обсяг простроченої заборгованості за подібними кредитами зменшився на 10%, а частка простроченої заборгованості – на 2,1%).

При цьому на стан банківської системи впливають такі негативні фактори:

1) зниження залучених коштів кредитних організацій через падіння ключової ставки. Незважаючи на те, що ставлення обсягу вкладів населення до ВВП на початок 2021 року становило 23,1%, депозити населення залишаються другою за величиною статтею пасивів кредитних організацій;

2) збільшення рівня простроченої позичкової заборгованості, що обумовлено проведенням банками ризикованої кредитної політики та суттєвим рівнем закредитованості населення. Ця тенденція нині послаблюється у зв'язку з тим, що ставки за банківськими кредитами поступово знижуються через зниження ключової ставки;

3) збільшення числа відкликаних ліцензій НБУ на ведення банківської діяльності у недобросовісних та нестійких банків: якщо за підсумками 2019 року

ліцензію було відкликано у 51 кредитної організації, то у 2021 році – вже у 77 кредитних організацій;

4) відтік капіталу до інших держав, внаслідок активної політики НБУ щодо відкликання ліцензій в кредитних організацій, і навіть розробки нових методів легалізації доходів, попри нагляд як із боку державні органи країни, і із боку міжнародних організацій;

5) участь кредитних організацій з іноземною участю в капіталі банківських організацій при тому, що конкурентоспроможність даних кредитних організацій значно вища за конкурентоспроможність національних банків, внаслідок чого може відбутися поступове витіснення національних банків із банківської системи держави;

6) збільшення кількості загроз інформаційній безпеці (атаки на сервери банків, крадіжка коштів з банківських рахунків, шахрайство через використання банківських карток, у тому числі карток із системою безконтактної оплати тощо).

1.4 Аналіз нормативно-правової бази забезпечення захисту інформації у кредитно-фінансовій установі

У кредитно-фінансових установах питання захисту даних є вкрай актуальними через те, що саме в них часто можна поставити знак тотожності між інформацією та грошима. Проблеми конфіденційності клієнтських даних, цілісності платіжних доручень, доступності банківських сервісів стоять як ніколи гостро саме в наш цифровий вік. З урахуванням великої конкуренції та різноманітності банківських продуктів лояльність клієнтів (як фізичних, так і юридичних осіб) цінується вкрай високо, а безпека платежів та конфіденційність наданих банку відомостей відносяться до найважливіших факторів вибору. Окрім очевидної та зрозумілої широкому колу людей мети проведення платежів банківська система служить фактично “кровоносною системою” економіки всієї

країни, і саме тому до суб'єктів критичної інформаційної інфраструктури України належать зокрема й організації банківської сфери (системно значущі кредитні організації, оператори платіжних систем, системно значні інфраструктурні організації ринку).

За даними, наданими Центром моніторингу та реагування на комп'ютерні атаки в кредитно-фінансовій сфері НБУ, у 2021 р. обсяг несанкціонованих операцій за картками склав 1,4 млрд. грн., а середня сума однієї несанкціонованої операції - 3 , 32 тис. грн. Для багатьох банків кіберриски стали одними з найважливіших факторів, що стримують розвиток, а шкода від кіберзлочинів, у тому числі репутаційна, вже давно перевищила таку від "класичних" пограбувань. Крім цього, НБУ у своєму Проекті "Положення про вимоги до системи управління операційним ризиком" включив ризики інформаційної безпеки та інформаційних систем до переліку операційних ризиків, які повинні бути враховані при управлінні капіталом фінансової організації.

Логічною відповіддю на кібер-виклики нашого часу послужила низка ініціатив керівництва країни, відповідно до яких було прийнято нормативно-правові акти для регулювання сфери інформаційної безпеки у фінансових організаціях України. Головним регулятором української фінансової галузі є Національний Банк України. Цілями НБУ у розрізі інформаційної безпеки є забезпечення кіберстійкості (за допомогою контролю показників ризику реалізації інформаційних загроз, забезпечення безперервності надання фінансових та банківських послуг, контролю рівня шахрайських операцій), захист споживачів фінансових послуг (шляхом моніторингу та контролю показників, що характеризують рівень фінансових втрат) , а також сприяння розвитку інноваційних фінансових технологій (за допомогою контролю ризику реалізації інформаційних загроз та реалізації необхідного рівня ІБ).

Національний банк України пропонує до обговорення проєкт змін до порядку розкриття фінансовими установами інформації, яка надається споживачу про умови та порядок надання споживчих кредитів, затвердженого постановою

Правління Національного банку України від 05 жовтня 2021 року № 100 (зі змінами).

Проєкт постанови Правління Національного банку України “Про внесення змін до деяких нормативно-правових актів Національного банку України” (далі – проєкт змін) актуалізує низку норм, що регламентують інформування споживачів небанківськими фінансовими установами України, які надають споживчі кредити, про свої послуги на власних вебсайтах, у рекламі на інших вебсайтах та в рекламних макетах при поширенні реклами.

Зокрема:

1) уточнюються місце та вигляд розміщення на власному вебсайті та в рекламі на інших вебсайтах попереджень про можливі наслідки для споживачів користування фінансовою послугою з надання споживчого кредиту, зокрема невиконання споживачами обов’язків згідно з договором про споживчий кредит;

2) додається попередження про наслідки для споживача у разі зазначення ним реквізитів своєї платіжної картки на вебсайті фінансової установи;

3) виокремлюється розмір витрат споживача на комісії та інші обов’язкові платежі за кредитом при розкритті Інформації про істотні характеристики послуги з надання споживчого кредиту/мікрокредиту;

4) уточнюються строки набрання чинності окремими вимогами Положення про інформаційне забезпечення фінансовими установами споживачів щодо надання послуг споживчого кредитування, затвердженого постановою Правління Національного банку від 05 жовтня 2021 року № 100 (зі змінами);

5) доповнюється порядок і спосіб розкриття істотних характеристик послуги з надання споживчого кредиту при поширенні реклами.

Крім того, проєкт змін містить такі нові терміни: “основний текст реклами”, “реквізити реклами” і “рекламний макет” та однозначно закріплює непоширення ознак, які свідчать, що спосіб викладення інформації про умови надання споживчого кредиту через поширення реклами ускладнює її візуальне сприйняття, на товарний знак фінансової установи (логотипа), що використовується в рекламі у сфері фінансових послуг.

Зазначені зміни запобігатимуть недоброчесній практиці небанківських кредитодавців приховувати або замовчувати попередження про можливі наслідки для споживача в разі користування послугами споживчого кредитування, розкривати інформацію про умови послуг неповно або перекручено, або у невідповідних місцях на вебсайтах, а також маніпулюванню увагою споживача в рекламі послуг з надання споживчого кредиту, викладаючи окремі істотні характеристики послуги та їхнє цифрове значення поза основним текстом реклами та неоднаковими гарнітурою, кольором і розміром шрифту.

1.5 Можливості існуючої системи захисту інформації у кредитно-фінансовій установі

На практиці забезпечення інформаційної безпеки відбувається за умов випадкового впливу чинників, які у повною мірою складно передбачити заздалегідь під час проектування системи захисту, але надалі вони здатні знизити ефективність передбачених проектом заходів інформаційної безпеки чи повністю скомпрометувати їх.

Однією із суттєвих проблем при проектуванні та експлуатації систем захисту є ігнорування методології системного аналізу щодо засобів та інструментів для їх захисту. Слід визнати складність, а іноді й неможливість об'єктивного підтвердження ефективності системи захисту інформації, що багато в чому визначається неповнотою нормативно-методичного забезпечення інформаційної безпеки, насамперед у сфері показників та критеріїв.

Так, наприклад, за статистичними даними Національного відділення ФБР США з комп'ютерних злочинів, реальний рівень ефективності систем захисту неприпустимо низький. Імовірність запобігання несанкціонованому проникненню в інформаційну систему становить у середньому близько 0,12. Імовірність виявлення нападу на корпоративні мережі становить 0,03-0,15. Для порівняння: у

багатьох прикладних сферах, де забезпеченню інформаційної безпеки процесів та об'єктів приділяється серйозна увага, норма безпеки, відображена у відповідних документах, становить 0,9.

Проектування та застосування систем захисту інформації об'єктивно пов'язані з невідомими подіями у майбутньому та завжди містять елементи невизначеності. Крім того, є інші причини неоднозначності властивостей систем захисту інформації. Тому етапу проектування природно супроводжує значна невизначеність. У міру реалізації проекту її рівень знижується. Тому об'єктивною характеристикою якості систем захисту може бути лише ймовірність, що характеризує ступінь об'єктивної можливості реалізації конкретної системи захисту при заданому комплексі умов.

Побудова моделей під час проектування чи модернізації системи захисту у банках представляється природним шляхом вирішення завдань аналізу та проектування з мінімальними витратами і високої ефективністю.

Так, на етапі аналізу модель системи захисту інформації використовується для дослідження кожної виконуваної функції (операції), щоб виявити, наприклад, якої інформації та яких ресурсів повинен мати доступ кожен співробітник при виконанні службових обов'язків.

З метою проведення повного аналізу ризиків для інформаційної системи можна використовувати модель, що включає:

види цінної інформації;

об'єкти її зберігання;

групи користувачів та види доступу до інформації;

засоби захисту (у т.ч. політику);

види небезпек.

Таке системне моделювання представляє суттєву алгоритмічну та математичну складність для розробників.

Після моделювання потрібно перейти до етапу аналізу захищеності побудованої моделі інформаційної системи. Саме тут виникає цілий комплекс теоретичних та практичних проблем, із якими стикаються розробники алгоритмів

аналізу ризиків. Практично неможливо автоматично, без участі експерта оцінити захищеність інформаційної системи. Таких систем аналізу ризиків сьогодні практично немає, а ті, що існують, мають узагальнений характер.

Наступна проблема – як алгоритмічно визначити всі класи вразливостей (достатність) у системі захисту аналізованої системи, як оцінити шкоду від усіх існуючих у системі загроз безпеці та як досягти адекватної оцінки сукупної шкоди за всіма класами загроз, уникнувши надмірного підсумовування збитків.

І найскладніша проблема: ризик – категорія суто ймовірнісна. Як оцінити ймовірність реалізації багатьох загроз інформаційної системи?

Не йдеться про сканування конкретних уразливостей у конкретному програмному забезпеченні.

Досить часто використовується модель порушника, яка визначає:

мотиви порушника, цілі, які він переслідує під час здійснення несанкціонованого доступу;

ступінь впливу на інформаційне середовище;

можливі місця проникнення порушника;

інформаційні ресурси, доступні порушнику;

Висновок до першого розділу

Результати аналізу особливостей банківської системи України вказують на визначення основних тенденцій та викликів, які можуть впливати на функціонування кредитно-фінансової установи.

Аналіз інформаційної структури кредитно-фінансової установи вказує на виявлення сильних та слабких сторін, що може служити основою для подальших рекомендацій.

Оцінка нормативно-правової бази захисту інформації вказує на визначення обов'язків та відповідальності, що є ключовим для ефективності системи захисту.

Аналіз можливостей існуючої системи захисту інформації кредитно-фінансової установи розкриває можливі шляхи оптимізації та підвищення рівня безпеки.

РОЗДІЛ 2
КОМПЛЕКС МОДЕЛЕЙ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВИ

2.1 Структура комплексу моделей захисту інформації кредитно-фінансової установи

Структура комплексу моделей захисту інформації кредитно-фінансової установи включає різні аспекти та етапи, охоплюючи технічні, організаційні та процесуальні заходи. Основні елементи структури можуть бути описані наступним чином:

1. Аналіз загроз:

- Ідентифікація загроз: Визначення потенційних небезпечних подій або дій, які можуть спричинити виток чи пошкодження інформації кредитно-фінансової установи.
- Оцінка ризиків: Аналіз ймовірності та важкості настання загроз, щоб визначити рівень ризику і прийняти рішення про заходи захисту.

2. Розробка політики інформаційної безпеки:

- Встановлення стандартів і правил: Розробка документів, що визначають правила та стандарти щодо обробки та захисту інформації.
- Планування заходів захисту: Розробка стратегії та тактики захисту інформації від конкретних загроз.

3. Фізичний захист:

- Захист приміщень: Контроль доступу, використання систем відеоспостереження, захист від стихійних лих.

4. Технічний захист:

- Системи інформаційної безпеки (ІБ): Використання антивірусних програм, брандмауерів, систем виявлення вторгнень та інших технічних засобів для захисту інформації.
- Шифрування інформації: Застосування методів шифрування для захисту конфіденційної інформації в електронних комунікаціях та зберіганні.

5. Адміністративний захист:

- Навчання та посилення обізнаності: Проведення навчань та тренінгів для персоналу з питань інформаційної безпеки.
- Управління доступом: Встановлення систем управління доступом та контролю прав доступу до інформації.

6. Аудит і моніторинг:

- Системи аудиту: Використання інструментів для реєстрації та аналізу подій в інформаційних системах.
- Моніторинг безпеки: Постійне відстеження та аналіз активності в мережі та системах для виявлення невідповідностей політиці інформаційної безпеки.

7. Реагування та відновлення:

- Планування реагування: Створення процедур та планів для відповіді на інциденти безпеки.
- Відновлення після інциденту: Відновлення роботи інформаційних систем після інциденту та відновлення інформації з резервних копій.

Ця структура відображає комплексний підхід до захисту інформації кредитно-фінансової установи, що враховує різні аспекти інформаційної безпеки та забезпечує високий рівень захисту від потенційних загроз.

2.2 Модель динамічного середовища інформаційних загроз рейдерського захоплення кредитно-фінансової установи

Серед багатьох інформаційних загроз безпеки кредитно-фінансового установи найбільш складні та небезпечні – це множинні узгоджені за цілями, завданнями, місцем та часом формування загрози типу дестабілізуючого концентрованого впливу. Це пов’язано, по-перше, з тим, що ці загрози мають комплексний характер (вимагають відповідних комплексних заходів для їх подолання); по-друге, інтенсивність загроз даного типу може суттєво змінюватися залежно від обраного сценарного підходу до досягнення кінцевої мети агресора (ініціатора загрози), що вимагає оперативного перерозподілу сил та засобів захисту на кожному етапі протидії комплексній загрозі; по-третє, загрози даного типу реалізуються на фоні традиційно існуючих загроз безпеки, для протидії яким повністю задіяні відповідні сили та засоби захисту. У кінцевому підсумку, множинна загроза представляє собою сукупність окремих загроз одного чи кількох видів, які можуть бути узгодженими або неузгодженими за цілями, завданнями, місцем та часом формування.

У даній роботі ми розглядатимемо дестабілізуючий концентрований вплив на кредитно-фінансову установу. Під дестабілізуючим концентрованим впливом на кредитно-фінансову установу ми будемо розуміти сукупність узгоджених та взаємопов’язаних за цілями, завданнями, місцем та часом загроз різних видів (внутрішніх та зовнішніх; технічних, інформаційних, економічних тощо), сконцентрованих в часі (одночасних) та формованих за єдиним планом і задумом, спрямованих на дискредитацію чи підпорядкування окремих структур кредитно-фінансової установи – рейдерському захопленню.

Також дестабілізуючою операцією ми розуміємо сукупність узгоджених та взаємопов’язаних за цілями, завданнями, місцем та часом, різнорідних окремих та масованих загроз і дестабілізуючих концентрованих впливів, які формуються одночасно і послідовно відповідно до єдиного плану і задуму для нанесення

значного збитку кредитно-фінансовій установі протягом встановленого періоду часу.

Однією з найважливіших особливостей процесу формування будь-якої загрози є необхідність її інформаційного забезпечення. Це передбачає отримання відповідної інформації про обраний для реалізації загрози (атаки) об’єкт, у нашому випадку – про кредитно-фінансову установу. Таким чином, загроза безпеки кредитно-фінансової установи під час реалізації дестабілізуючого концентрованого впливу, а саме рейдерського захоплення, супроводжується комплексом інформаційних загроз. Розглянемо рейдерське захоплення як дестабілізуючу операцію в частині загрози інформаційної безпеки кредитно-фінансової установи.

Система інформаційної безпеки кредитно-фінансової установи при загрозі рейдерського захоплення також повинна мати комплексний та динамічний характер. В основі побудови такої системи повинні лежати уявлення про: потужність поля (середовища) інформаційних загроз, номенклатуру інформаційних загроз, динаміку зміни інтенсивності загроз. Таке уявлення може бути отримане шляхом побудови моделі динамічного середовища загроз інформаційної безпеки кредитно-фінансової установи. Під динамічним середовищем загроз інформаційної безпеки кредитно-фінансової установи ми будемо розуміти складову частину зовнішньої та внутрішньої середовища функціонування кредитно-фінансової установи, що складається з різноманітних інформаційних загроз, постійно переходячи з потенційного стану в реальний і навпаки. Процес перетворення потенційних загроз в реальні, утворюючи в сукупності загрозу рейдерського захоплення кредитно-фінансової установи, буде визначатися їхнім життєвим циклом загрози, схематично зображеним на рис.2.1.

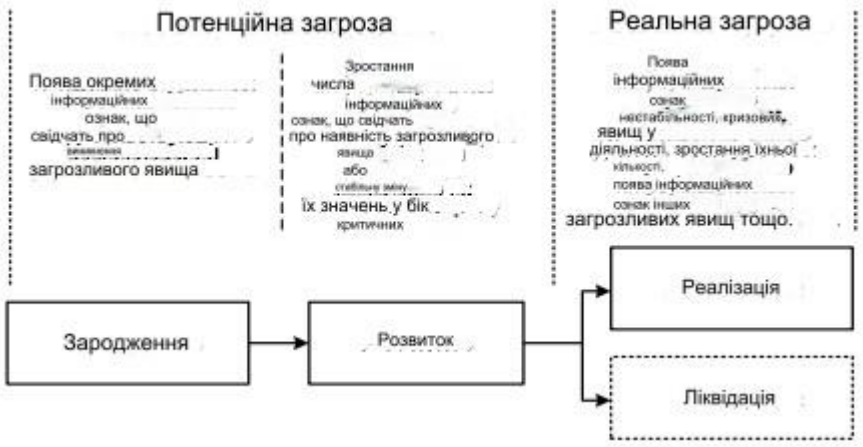

Рис. 2.1. Життєвий цикл загрози

Інтенсивність перетворення потенційних інформаційних загроз на реальні та їх реалізація залежатимуть від задуму та способу здійснення дестабілізуючих впливів, які можуть описуватись низкою параметрів, що утворюють модель динамічного середовища загроз інформаційній безпеці кредитно-фінансової установи.

Формалізоване опис динамічного середовища загроз інформаційної безпеки кредитно-фінансової установи (в канонічній формі) представимо у вигляді багатовимірного вектора $W_{<x>}$, що включає статичні $W^{c}_{<x'>}$ та динамічні $W^{\partial}_{<x''>}$ параметри:

$W_{<x>} = < W^{(1)}_{<\ell_1>}, ..., W^{(x)}_{<\ell_x>}, ..., W^{(X)}_{<\ell_X>} >$. $W^{(x)}_{<\ell_x>}$ - ℓ_x-вимірний вектор параметрів, що описує х -параметр ДСУ ІБ; $x = \overline{1, X}$. $W_{<x>} = W^{c}_{<x'>} + W^{\partial}_{<x''>}$, $x = x' + x''$.

Кожен параметр вектора $W_{<x>}$ має свій інформаційний аналог, що складається з

однієї або кількох інформаційних загроз, що описуються інформаційними ознаками (інформаційно-ознаковими моделями), що у сукупності утворюють загрозу рейдерського захоплення кредитно-фінансової установи.

До основних статичних параметрів відносяться:

$W^{c}_{<x'>} = W^{c}_{<6>} =< W^{c(1)}_{<\ell_1>}, W^{c(2)}_{<\ell_2>}, ..., W^{c(6)}_{<\ell_6>} >$, де:

$W^{c(1)}_{<\ell_1>} = W^{c(1)}_{<4>} < \omega_1^{c(1)}, \omega_2^{c(1)}, \omega_3^{c(1)}, \omega_4^{c(1)} >$ – характер дестабілізуючого впливу;

$W^{c(2)}_{<\ell_2>} = W^{c(2)}_{<10>} < \omega_1^{c(2)}, \omega_2^{c(2)}, ..., \omega_{10}^{c(2)} >$ - основні причини виникнення дестабілізуючого впливу (як усередині кредитно-фінансової установи, так і поза нею);

$W^{c(3)}_{<\ell_3>} = W^{c(3)}_{<7>} =< \omega_1^{c(3)}, \omega_2^{c(3)}, ..., \omega_7^{c(3)} >$ - характер об'єкта;

$W^{c(4)}_{<\ell_4>} = W^{c(4)}_{<3>} =< \omega_1^{c(4)}, \omega_2^{c(4)}, \omega_3^{c(4)} >$ – наявність на об'єкті сил та засобів захисту інформації;

Основною особливістю запропонованої моделі є те, що багато інформаційних ознак можуть належати різним за своєю загрозою. Це передбачає цілеспрямований пошук додаткових (супутніх, послідовних) інформаційних ознак для точнішої ідентифікації загрози.

На основі запропонованої моделі динамічного середовища інформаційних загроз можна побудувати прогноз інформаційної ситуації кредитно-фінансової установи. Якість цього прогнозу залежить від своєчасного визначення стану динамічного середовища загроз інформаційній безпеці кредитно-фінансової установи. Для цього виділимо N станів динамічного середовища загроз інформаційній безпеці кредитно-фінансової установи та позначимо їхній поточний стан $A_i, i = \overline{1, N.}$.

Як згадувалося вище, кожен стан динамічного середовища загроз інформаційної безпеки характеризується своїм набором інформаційних ознак. При цьому в кожному стані динамічного середовища загроз інформаційній безпеці можуть присутні інформаційні ознаки m , що характеризують одну з можливих несумісних варіантів (гіпотез) реалізації рейдерського захоплення кредитно-фінансового $S_j, \quad j = \overline{1, M}$ установи: відсутність заходів щодо

рейдерського захоплення; ($j=1$) здійснення “білого” рейдерського захоплення ($j=2$); здійснення “сірого” рейдерського захоплення ($j=3$); здійснення “чорного” рейдерського захоплення ($j=4$). Багато подій m можуть з'являтися за будь-якої з цих гіпотез, тому ймовірність події m обчислюється за формулою повної ймовірності:

$$P(m)=\sum_{j=1}^{N} P(m/S_j)P(S_j),$$ де: $P(S_j)$ - апріорна ймовірність того, що процес рейдерського захоплення кредитно-фінансової установи перебуває в стані (в якості вихідних даних може бути використане значення умовна ймовірність прояву ознаки (проведення заходу) m під час перебування процесу рейдерського захоплення кредитно-фінансової установи у стані S_j що характеризує силу відповідного причинно-наслідкового зв'язку.

При аналізі даних велике значення має апріорна інформація про стан процесу. Після отримання нових відомостей про ознаки (проведені заходи) апостеріорний розподіл ймовірностей різних можливих станів процесу рейдерського захоплення кредитно-фінансової установи може бути визначено за формулою Байєса:

$$P(S_j/m)=\frac{p(S_j)\cdot P(m/S_j)}{\sum_{i=1}^{N} P(S_j)\cdot P(m/S_j)}$$ де $P(S_j/m)$ - умовна ймовірність того, що процес рейдерського захоплення знаходиться в S_j - м (з N можливих) станів при прояві ознаки (Проведення заходу) m .

Таким чином, формула Байєса дозволяє переоцінити ймовірність гіпотез про стан процесу рейдерського захоплення кредитно-фінансової установи після того, як результати спостереження стають відомими.

Кориговані ймовірності самих гіпотез $P(S_j/m)$ можуть бути розраховані

прямим чином (за формулою Байєса). У цьому дана процедура є рекурсивної, тобто. якщо має бути оцінена більш ніж одна подія, то скориговані ймовірності гіпотез при першій ітерації стають початковими ймовірностями чергової ітерації.

Запропонована модель та методика її реалізації дозволяють: за сукупністю зафіксованих інформаційних ознак визначити наявність та стан загроз безпеці кредитно-фінансової установи в цілому, та інформаційних загроз, зокрема; побудувати інформаційно-ознакові моделі інформаційних загроз кредитно-фінансовій установі; визначити інтенсивність та динаміку інформаційних загроз; сформувати вихідні дані для побудови ефективної та оптимальної системи захисту інформації кредитно-фінансової установи.

2.3 Модель формування структури загроз інформаційній безпеці кредитно-фінансової установи під час рейдерського захоплення

Модель формування структури загроз інформаційній безпеці кредитно-фінансової установи під час рейдерського захоплення може бути розглянута в контексті кількох ключових аспектів. Давайте розглянемо таку модель:

1. Ідентифікація загроз:

- Зовнішні загрози: Розгляд різних можливих джерел загроз інформаційній безпеці, таких як конкуренти, злочинні організації, зловмисники, які можуть зацікавитися кредитно-фінансовою установою під час рейдерського захоплення.
- Внутрішні загрози: Врахування можливості участі внутрішнього персоналу або колишніх співробітників у рейдерському захопленні, а також можливості витоку конфіденційної інформації.

2. Оцінка рівня ризику:

- Аналіз ймовірності та наслідків можливих інцидентів інформаційного порушення під час рейдерського захоплення.

- Визначення потенційних втрат (фінансових, репутаційних тощо) внаслідок інформаційних загроз.

3. Категоризація загроз:

- Групування загроз за типами (технічні, соціальні, економічні), щоб легше аналізувати та вирішувати проблеми безпеки.

4. Сценарії атак:

Розробка різних сценаріїв можливих атак, які можуть бути використані при рейдерському захопленні, включаючи виток конфіденційної інформації, атаки на системи зв'язку, зміну фінансових операцій тощо.

5. Захистні заходи:

- Розробка заходів забезпечення безпеки для запобігання чи мінімізації наслідків рейдерського захоплення, таких як політики безпеки, шифрування, системи виявлення вторгнень, контроль доступу тощо.

6. Аудит і моніторинг:

- Встановлення систем аудиту та моніторингу для виявлення незвичайної або підозрілої активності в інформаційних системах.

7. Навчання та свідомість:

- Підвищення обізнаності персоналу щодо загроз рейдерського захоплення та інформаційної безпеки.

8. Кризове управління:

- Розробка плану кризового управління для відповіді на рейдерське захоплення, включаючи відновлення роботи інформаційних систем та відновлення послуг.

Ця модель слід розглядати як інтегровану систему заходів та процесів, яка призначена для попередження, виявлення та відповіді на загрози інформаційній безпеці під час рейдерського захоплення кредитно-фінансової установи.

2.4 Модель формування базового та маневреного комплекту сил та засобів захисту інформації кредитно-фінансової установи

Модель формування базового та маневреного комплекту сил та засобів захисту інформації кредитно-фінансової установи може включати наступні етапи та компоненти:

1. Аналіз загроз та ризиків:

- Оцінка сучасного стану існуючих і потенційних загроз для інформаційної безпеки кредитно-фінансової установи.
- Визначення ключових ризиків, які можуть виникнути при різних сценаріях атак чи рейдерських захопленнях.

2. Розробка базового комплекту сил і засобів:

- Системи безпеки:
  - Встановлення ефективних антивірусних програм, брандмауерів, систем виявлення вторгнень та систем криптографічного захисту.
- Системи моніторингу:
  - Розгортання систем виявлення аномалій і моніторингу подій для попередження та виявлення інцидентів.
- Контроль доступу:
  - Реалізація строгого контролю доступу до інформаційних ресурсів та конфіденційних даних.

3. Створення маневреного комплекту сил і засобів:

- Реагування на інциденти:
  - Створення ефективного механізму реагування на інциденти та впровадження швидких процедур відновлення після інцидентів.
- Оновлення та модернізація:
  - Постійне оновлення та модернізація систем і засобів захисту для врахування нових загроз та вдосконалення реагування.

4. Технологічна інтеграція:

- Інтеграція систем:
  - Забезпечення взаємодії між різними системами безпеки для створення єдиної та комплексної системи захисту.
- Автоматизація процесів:
  - Використання автоматизованих засобів для виявлення, аналізу та реагування на загрози.

5. Організаційні заходи:

- Політики безпеки:
  - Розробка та впровадження строгих політик та процедур інформаційної безпеки.
- Тренінг та освіта:
  - Навчання персоналу та створення свідомого підходу до захисту інформації.

6. Системи попередження та аналізу:

- Аналіз загроз:
  - Використання систем аналізу загроз для попередження можливих атак та формування відповідей.
- Моніторинг та інтелектуальний аналіз:
  - Впровадження систем моніторингу та аналізу, що використовують інтелектуальні технології для виявлення нових загроз.

7. Оцінка ефективності:

- Аудит інформаційної безпеки:
  - Проведення регулярних аудитів для перевірки ефективності систем захисту та виявлення можливих слабких місць.
- Впровадження змін:
  - Внесення змін у структуру та стратегії захисту на основі отриманих даних.

Ця модель має на меті створення інтегрованої системи захисту, яка охоплює як базові, так і маневрені засоби та сили для ефективного вирішення викликів інформаційної безпеки кредитно-фінансової установи.

2.5 Модель захищеності інформаційного вузла інформаційної структури кредитно-фінансової установи

Модель захищеності інформаційного вузла в інформаційній структурі кредитно-фінансової установи включає різні аспекти технічного, організаційного та процесуального характеру для забезпечення надійного захисту від потенційних загроз. Розглянемо основні компоненти такої моделі:

1. Фізичний захист:

- Центр обробки даних (ЦОД):

  - Забезпечення фізичної безпеки серверних приміщень, де зберігається та обробляється конфіденційна інформація.

  - Встановлення контролю доступу до ЦОД, використання систем відеоспостереження та систем захисту від несанкціонованого доступу.

2. Технічний захист:

- Захист мережі:

  - Використання брандмауерів, систем виявлення вторгнень та інших технічних засобів для захисту мережевого периметру.

  - Шифрування трафіку для захисту конфіденційної інформації під час передачі по мережі.

- Захист інформації:

  - Використання систем антивірусного захисту, антиспаму та інших засобів для захисту від загроз програмного забезпечення.

  - Регулярне виконання патчів та оновлень для усунення вразливостей систем.

3. Організаційний захист:

- Політики та процедури безпеки:

  - Розробка та впровадження строгих політик і процедур безпеки для персоналу.

- Забезпечення свідомості персоналу щодо важливості безпеки інформації та дотримання встановлених правил.

- Моніторинг та аудит безпеки:

- Впровадження систем моніторингу та аудиту для виявлення незвичайної або підозрілої активності.

- Проведення регулярних аудитів для перевірки відповідності політикам та стандартам безпеки.

4. Свідомість та навчання:

- Тренінг персоналу:

- Проведення регулярних навчань та тренінгів щодо безпеки інформації та процедур дії в разі інцидентів.

- Створення свідомого підходу до захисту інформації серед персоналу.

5. Адаптивність та реагування на інциденти:

- Планування відновлення після інциденту:

- Розробка та впровадження плану відновлення роботи після інциденту для мінімізації втрат та перерв в роботі.

- Аналіз інцидентів для вдосконалення заходів безпеки та підвищення рівня захищеності.

Ця модель спрямована на створення комплексного підходу до захисту інформаційного вузла в інформаційній структурі кредитно-фінансової установи, охоплюючи різні аспекти технічного, організаційного та поведінкового характеру.

Висновок до другого розділу

Висновки з аналізу структури комплексу моделей захисту інформації кредитно-фінансової установи вказують на можливості вдосконалення та розвитку існуючих підходів.

Результати аналізу моделі динамічного середовища інформаційних загроз рейдерського захоплення свідчать про необхідність впровадження ефективних заходів для запобігання та виявлення потенційних загроз.

Модель формування структури загроз інформаційній безпеці кредитно-фінансової установи під час рейдерського захоплення розкриває ключові аспекти ризиків та їхні можливі впливи.

Модель формування базового та маневреного комплекту сил та засобів захисту інформації кредитно-фінансової установи вказує на необхідність гнучкості та адаптабельності системи.

Висновки з аналізу моделі захищеності інформаційного вузла свідчать про важливість вдосконалення технічних засобів та методів захисту для забезпечення стійкості вузла.

РОЗДІЛ 3
МЕТОДИКА ОРГАНІЗАЦІЇ ДИНАМІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ КРЕДИТНО-ФІНАНСОВОГО УСТАНОВИ ПРИ СПРОБУ РЕЙДЕРСЬКОГО ЗАХОПЛЕННЯ

3.1 Методика прогнозування інформаційних загроз у процесі розвитку рейдерського захоплення кредитно-фінансової установи

У процесі розгляду сутності безпеки фінансово-кредитних установ з позиції захисного підходу основним, вихідним поняттям виступають загрози як певні процеси і явища, що відбуваються у зовнішньому і внутрішньому середовищах, а також дії інших суб'єктів, що за деяких умов можуть негативно вплинути на діяльність цих установ. Оскільки середовище функціонування організацій формується внаслідок намагання реалізувати велику кількість економічних інтересів різних суб'єктів, крім того, існують чисельні об'єктивні обставини, що можуть бути несприятливими, - природні, техніко-технологічні, інформаційні чинники тощо, то різноманітні загрози виникають і діють постійно, обумовлюючи необхідність досягнення й підтримання стану безпеки.

Економічна безпека фінансово-кредитних установ забезпечує їхню стійкість до виявлених загроз, характеризує здатність до самовідтворення та самоорганізації для забезпечення задоволення потреб зовнішніх і внутрішніх стейкхолдерів. Саме у виявленні загроз, протидії ним, нейтралізації, а, за можливістю, і ліквідації їх полягає, на наш погляд, гарантування безпеки.

Грамотно ж протидіяти можна лише тому, що розпізнано і вивчено. Саме цим визначається важливість ідентифікації загроз економічній безпеці фінансово-кредитних установ.

Крім того, незважаючи на те, що загрози існують постійно, їх склад та інтенсивність впливу періодично змінюються. Зокрема, у даний час вітчизняні фінансово-кредитні установи стикаються з такими видами загроз, які ще декілька років тому не могли б бути передбачені навіть гіпотетично.

Відповідно, появляються нові види ризиків, а традиційні набувають більшої інтенсивності. Актуальність цих питань потребує звернення уваги на сутність загроз, виявлення їх класифікаційних ознак та джерел виникнення.

Поняття загрози вже достатньо тривалий час є об'єктом вивчення вітчизняної безпекології і досить часто у наукових доробках зустрічається використання понять ризик, небезпека та загроза. Незважаючи на це, досі у наукових колах існує широкий спектр точок зору щодо визначення суті зазначених понять. Правильне розуміння цих понять дозволяє сформувати відповідну на них реакцію і в першу чергу це стосується ефективності забезпечення економічної безпеки.

Аналіз наведених трактувань свідчить, що майже у кожному з них відображено небезпеку нанесення чи заподіяння певної шкоди суб'єкту, створення перепон у реалізації його інтересів, досягненні його цілей та констатований негативний вплив на стабільну діяльність. Узагальнюючи, можна сказати, що загрози безпеці - це фактично будь-які внутрішні або зовнішні умови та фактори, які здійснюють негативний вплив на процес розвитку й для його відновлення потребують зниження своїх кількісних або зміни (пом'якшення) якісних характеристик. При цьому, на думку Варналія З. С. , найзагальнішими ознаками загроз виступають конкретність, реальність, дійсність, створення економічної небезпеки.

Втім, варто звернути увагу на певну відносність характеристик загроз.

Одні і ті ж події або чинники в одному випадку (для одного суб'єкта) можуть бути сприятливими, а за інших умов (для іншого суб'єкта) – зовсім ні. Так, зміцнення національної валюти становить загрозу економічним інтересам експортерів, означає для них недоотримання запланованого фінансового результату, у той же час сприятливо для імпортерів, а також зменшує валютний еквівалент державного боргу, що позитивно впливає на боргову безпеку держави. Крім того, те, що у короткостроковому періоді здається небезпекою, загрозою – наприклад, посилення конкуренції на фінансовому ринку внаслідок появи FinTech компаній, – на довгостроковому горизонті може розглядатися як позитивна можливість – шлях інноваційного розвитку фінансово-кредитних установ через створення з ними стратегічних альянсів.

Вивчаючи наукову літературу з безпекових питань, можна знайти і багато точок зору вчених на сутність і зміст економічної безпеки на рівні суб'єкта господарювання/фінансово-кредитної установи.

Погоджуємось з Козаченко Г.В. й Погореловим Ю.С., що відсутність чіткого визначення змісту поняття "загроза" провокує виникнення помилкового прирівняння наслідків реалізації загроз та загроз як таких, що зумовлює помилки у визначенні векторів та орієнтирів безпекозабезпечувальної діяльності суб'єкта господарювання.

У результаті аналізу наведених визначень можна сказати, що трактування загроз безпеці для господарюючих суб'єктів, що пропонуються І.П. Мігус й Орлик О.В., є дещо узагальненим, оскільки не містять уточнення стосовно змісту подій, що відбуваються, та характеру їх впливу на діяльність суб'єкта, що є визначальним у процесі оперативної ідентифікації загроз.

На нашу думку, більшість процесів і явищ у зовнішньому середовищі фінансово-кредитних установ, що є результатом діяльності великої кількості

суб'єктів, які переслідують свої інтереси, - зокрема, макроекономічні процеси, за своєю природою є індиферентними по відношенню до функціонування ФКУ і не можуть однозначно розглядатися як загрози або сприятливі фактори. І лише певний внутрішній стан ФКУ, особливості її ресурсної бази, активів, бізнес-процесів, технічного забезпечення, персоналу тощо змушує ідентифікувати певні з них саме як загрози. При зміні характеристик стану установи такі події або явища можуть втратити свій загрозливий характер.

Використовуючи попередній приклад зі зміною курсу національної валюти, можемо констатувати, що знецінення гривні під час фінансової кризи 2008-2009 років стало загрозою для діяльності більшості вітчизняних банків, які мали портфель валютних іпотечних кредитів, оскільки суттєво знизило платоспроможність позичальників. Для попередження таких ситуацій у майбутньому у середині 2009 року на законодавчому рівні в Україні було заборонено видачу всіх видів валютних кредитів фізичним особам (отже, відбувалася зміна стану активів). Ті ж банки, що на початок кризи мали велику довгу позицію в іноземних валютах, навпаки, отримали додаткові прибутки за рахунок зростання їх курсу.

Інша справа – свідомі дії суб'єктів зовнішнього середовища, які мають пряму чи опосередковану взаємодію з фінансово-кредитними установами, атому впливають на їх діяльність (держава, регулятори, конкуренти, партнери, клієнти тощо). Тут джерелом загроз можуть стати не лише такі прямі агресивні дії, як спроба рейдерського захоплення або інформаційна атака, а і об'єктивні розбіжності економічних інтересів цих суб'єктів і ФКУ. Щодо внутрішнього середовища фінансово-кредитних установ, то тут джерелом загроз переважно є некваліфікований менеджмент, а також навмисні та ненавмисні дії персоналу.

Більшість науковців характеризують загрозу як реальну чи потенційну подію, що є, безумовно, доцільним. Специфіка загроз економічній безпеці

фінансово-кредитної установи полягає саме у тому, що явища зовнішнього та внутрішнього середовища можуть бути як реальними, що реалізуються з певною ймовірністю, так і потенційними, що не відбуваються в дійсності (зокрема: чутки про злиття або придбання установ; розгляд законопроекту, що містить посилення норм діяльності або заборону певної діяльності; передбачення аналітиків щодо динаміки макроекономічних процесів тощо), але провокують панічні настрої, волатильність на фінансовому ринку і також призводять до певних негативних наслідків, навіть не будучи реалізованими.

Розмежування цих джерел загроз має практичне значення, оскільки заходи, застосовані щодо протидії ним й нейтралізації, повинні бути дещо різними.

На наш погляд, однією зі складнощів, пов’язаних з нейтралізацією загроз, розробкою ефективних захисних заходів, є різнохарактерний прояв їх сутності.

Практично будь-який елемент поза або всередині організації, з точки зору забезпечення економічної безпеки, може виступати в різних ролях:

- суб’єкта (засобу, способу, інструмента) забезпечення безпеки;

- об’єкта забезпечення економічної безпеки (елемент, що захищається);

- джерела (суб’єкта або об’єкта) загрози.

При цьому під елементами тут можуть розумітися будь-які об’єкти, живі і неживі, матеріальні і нематеріальні, зокрема, персонал підрозділу установи, окремий працівник, кошти, договір, клієнт, розрахунковий документ, операція, бізнес-процес тощо.

Особливо важливим є акцентування на негативному характері впливу зазначених дій чи подій на фінансово-кредитну установу, насамперед, через неможливість реалізації її економічних інтересів, заподіяння фінансових збитків або матеріальної шкоди, втрату капіталу. Втім, підтримуємо думки Гребенюк Н.О. та Зубка М.І., що для ФКУ не менше руйнівними можуть бути наслідки нефінансового або іміджевого, морального характеру: зниження репутації, втрата

клієнтів, звільнення провідних співробітників, збої у роботі інформаційних систем тощо, які з плином часу також відображаються на фінансових результатах.

Узагальнення підходів науковців до поняття “загроза” дозволило сформувати таке його визначення: під загрозою економічній безпеці фінансово-кредитної установи слід розуміти такі явища, процеси або дії/бездіяльність, які відбуваються у зовнішньому та внутрішньому середовищі її діяльності та прямо або опосередковано підвищують ймовірність порушення стабільного функціонування ФКУ, недосягнення нею своїх цілей через нанесення фінансово-кредитній установі будь-якого виду збитків.

Відповідно до положень сучасної безпекології, спорідненими до поняття загрози є такі поняття, як “небезпека” і “ризик”. Аналізу співвідношення цих термінів, виходячи з різноманітних трактувань їх сутності, присвячено ряд наукових публікацій, вивчення яких дозволило зробити нижченаведені узагальнення.

Щодо поняття “небезпека”, то у літературі існують, як мінімум, три точки зору на його зміст:

- небезпека, виходячи з етимології цього слова, трактується як ситуація, протилежна безпеці, тобто як відсутність безпеки; отже, вони виступають протилежними за значенням: стан незахищеності інтересів суб’єкта та, відповідно, стан захищеності;

- небезпека розглядається як потенційна загроза, стадія зародження останньої, як певна негативна ситуація, що сама по собі не наносить шкоди.

Небезпека набуває негативного прояву при відповідних умовах, за яких вона трансформується у загрозу і набуває посилу до негативної дії; отже, загроза тлумачиться як стадія переходу небезпеки зі статусу “можливість” у статус “дійсність”;

- небезпека вважається конкретною, вищою формою прояву загрози, коли починає спостерігатися руйнівний вплив останньої на діяльність економічного суб'єкта; таким чином, небезпечною ситуація стає у тому випадку, коли загроза набуває реальних форм прояву.

Саме остання точка зору нам видається найбільш прийнятною, оскільки вона відображає реальну динаміку процесу, рух від безпеки до небезпеки через посилення загроз діяльності економічного суб'єкта.

Стосовно розуміння поняття "ризик" також існує велика кількість різних підходів. Ми погоджуємось з тим, що ризик є об'єктивною характеристикою діяльності будь-якого суб'єкта підприємництва, що притаманна будь-яким управлінським рішенням в умовах невизначеності. За даного розуміння ризик вимірюється ймовірністю неотримання передбачуваних результатів. У цьому випадку мається на увазі імовірність упущення вигоди, матеріальних чи фінансових втрат, неотримання прибутку. Іманентність комерційній діяльності такої ознаки як ризикованість підкреслюється навіть законодавчим визначенням підприємництва як самостійної, систематичної, на власний ризик діяльності. Аналогічно, стосовно банків, одна з їх базових операцій полягає у розміщенні від свого імені залучених у вклади коштів, на власний ризик та з власними умовами. Отже, ризик є формою функціонування суб'єктів підприємництва у динамічному, ймовірнісному середовищі.

Невизначеність середовища як раз і полягає у наявності дестабілізуючих факторів, загроз, небезпек, які можуть не проявитися або діяти більш або менш інтенсивно. Якщо вони не вплинули на певний процес або операцію, то ризик не реалізується і очікувані суб'єктом результати досягаються: сприятливі умови дозволяють досягнути поставлених цілей та отримати прибуток. І навпаки, вплив загрози – це ризикована ситуація, що почала реалізовуватися за небажаним варіантом.

Отже, можна зазначити, що загрози існують об’єктивно, а ризик дозволяє надати оцінку ступеня впливу загрози на стан та результати діяльності фінансово-кредитної установи. Якщо загроза – це ймовірна можливість перешкоди економічним інтересам ФКУ, то ризик у свою чергу є рівнем цієї загрози і дає математичне уявлення виразу можливості настання перешкод.

Проілюструвати ці міркування можна на прикладі спільної для всіх досліджуваних фінансово-кредитних установ операції – видачі кредиту фізичній особі. При наданні позики у ФКУ виникає кредитний ризик, що полягає у можливості часткового або повного неповернення кредиту та несплати відсотків. Реалізація негативного сценарію залежить від факту переходу загроз, які, у цілому, відомі (зниження платоспроможності позичальника, суттєве погіршення стану його здоров’я, спроби шахрайства, зниження вартості застави тощо) з потенційного стану у реальний (зокрема, внаслідок втрати позичальником роботи). Отже, ймовірність фінансових втрат ФКУ зростає, але вона може бути мінімізована за рахунок нейтралізації загрози (опосередковано – отриманням позичальником допомоги по безробіттю, або прямим шляхом – реалізацію предмета застави). І лише при зростанні загрози до рівня небезпеки (доходів немає, предмет застави втрачено) кредитний ризик реалізується повною мірою, кредит переходить у стан непрацюючого, проблемного, що викликає необхідність формування резервів і зменшує капітал фінансово-кредитної установи. За умови нереалізації загроз ризик не проявляється, і ФКУ отримує очікувані фінансові результати.

Наше уявлення щодо взаємозв’язку понять “загроза”, “безпека”, “ризик” візуалізовано на рис. 3.1.

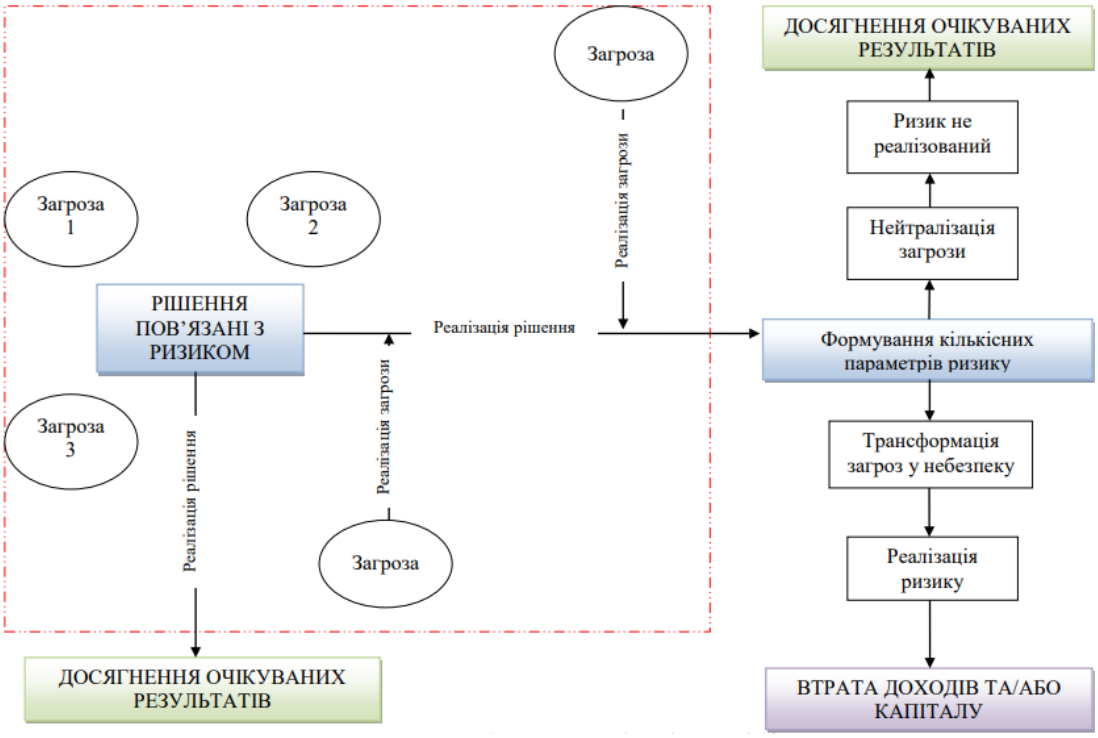

Рис. 3.1. Взаємозв'язок загроз, небезпек та ризиків у діяльності фінансово-кредитних установ

Процес забезпечення економічної безпеки фінансово-кредитних установ починається саме з ідентифікації загроз їх стабільному функціонуванню.

Ідентифікація (від лат. identicus – тотожний), відповідно до словника іншомовних слів, означає ототожнення, прирівнювання, уподібнення, тобто встановлення тотожності певного об'єкта відомому на підставі збігу ознак.

Майже аналогічний зміст має і термін "діагностика" (з грец. diagnosis – розпізнання). Основними завданнями ідентифікації (діагностики) загроз економічній безпеці є своєчасне їх виявлення, дослідження характеру, напряму впливу на економічні інтереси фінансово-кредитної установи, оцінка ймовірності реалізації та попередження потенційних кризових станів.

Для проведення ідентифікації використовуються різноманітні методи, які входять у наступні чотири класифікації:

1. Методи експертних оцінок, які достатньо докладно описані у літературі. Нагадаємо лише, що ці методи поділяються на дві великі групи: індивідуальні

(персональні) експертні оцінки, які передбачають отримання думок від окремих, ізольованих один від одного експертів, та групові (колективні) оцінки, коли оцінки експертів певним чином зв'язані між собою.

Формами проведення індивідуальних експертиз є інтерв'ю та аналітична записка, а колективних – метод комісії й метод Дельфі. Експертами у ситуації ідентифікації загроз економічній безпеці виступають провідні працівники фінансово-кредитної установи, а також зовнішні фахівці. Основними вимогами до них є високий рівень кваліфікації, компетентність, індиферентність до результату, психологічна незалежність.

2. Економіко-статистичні методи полягають в аналізі статистичних даних при забезпеченні економічної безпеки ФКУ. З використанням цих методів здійснюється моніторинг зовнішнього та внутрішнього середовища, оцінка впливу загроз, вибір серед них найбільш суттєвих. До них відносяться метод кореляції, регресійний аналіз, індексний метод тощо.

3. Математичні методи є дослідженням економічних процесів за допомогою математичних моделей. Зрозуміло, що їх застосування потребує високої кваліфікації і досвіду фахівців, тому доцільно лише у комерційних банках. До таких методів відносяться теорія ігор, теорія нечітких множин, методи оптимізації, метод ієрархій та ін.

4. Економічні методи, що є способами дослідження економічних показників, процесів і систем у нерозривному зв'язку один з одним.

Використовуються, зокрема, для оцінки суми збитків, які фінансово-кредитна установа може отримати внаслідок реалізації загрози. До таких методів діагностики відносяться: трендовий аналіз, факторний аналіз, метод коефіцієнтів та інші. Для ідентифікації загроз варто застосовувати і відомі методи стратегічного аналізу: SWOT-аналіз, PEST-аналіз, SNW (абревіатура від англ. strength, neutral, weakness) – для аналізу внутрішнього середовища ФКУ.

З точки зору кількості та рівня небезпеки загроз, зовнішнє середовище для діяльності фінансово-кредитної установи може у "чистому вигляді" характеризуватися таким чином:

- нейтральне середовище, яке практично не впливає на функціонування установи; така ситуація складається, коли інтереси економічних суб'єктів не перетинаються і вони діють відносно незалежно один від одного;

- сприятливе середовище, яке полегшує розвиток економічних суб'єктів, привносить позитивні зміни в їхнє функціонування;

- вороже середовище характеризується сукупним негативним впливом на установу, її економічні інтереси, викликає стагнацію і занепад організації.

Погоджуємось з думкою З.С. Варналія стосовно того, що зміст загрози безпосередньо пов'язаний з її формою. Згідно з науковго погляду, під формою загрози варто розуміти її способи зовнішнього вираження. Форма зумовлює межі загрози та надає її змісту фактичної визначеності в об'єктивному світі.

Загроза набуває статусу доступної для дослідження та оцінки саме завдяки формі. Загрози економічній безпеці фінансово-кредитних установ є надзвичайно різноманітними, вони постійно виникають і зникають у часі, видозмінюються і трансформуються, тому в основу їх ідентифікації повинна бути покладена науково обґрунтована класифікація. Для її формування, на наш погляд, доцільно використовувати і класифікації загроз, що пропонуються науковцями, які здійснюють дослідження економічної безпеки суб'єктів різного різня (держави, регіону, підприємств, банків, фінансових установ), оскільки підходи до виділення класифікаційних ознак є достатньо загальними.

Насамперед, учені одностайні у тому, що за джерелами походження (сферою виникнення) загрози поділяються на зовнішні, що генеруються у зовнішньому середовищі фінансово-кредитної установи, та внутрішні, що є результатом організації та функціонування установи. Втім, у подальшому, перелік і пояснення змісту цих загроз суттєво відрізняються у залежності від спрямованості досліджень, що, безумовно, не є недоліком і свідчить про практично нескінчену кількість видів загроз, що можна ідентифікувати. У зв'язку з тим також відмітимо, що, на нашу думку, вдосконалення класифікації повинно полягати не стільки у додаванні нових ознак, скільки у критичному аналізі й більш чіткому трактуванні вже існуючих.

Так, автори підручника “Безпека банківської діяльності”, розуміючи під загрозами потенційні чи реальні дії певних суб’єктів, здатні завдати конкретному банку матеріальної або моральної шкоди, розглядають види загроз за сферою виникнення саме з “суб’єктної” точки зору. Джерелами зовнішніх загроз називаються конкуренти; особи, які провадять кримінальну діяльність, кримінальні угруповання; клієнти банків, потенційні та наявні партнери; контрольно-наглядові органи; засоби масової інформації та ін. Згадуються також політичні загрози, стихійні лиха та техногенні аварії і катастрофи.

Внутрішні загрози банку, на думку Зубка М.І. та Яременко С.М., зумовлені непрофесійною роботою працівників, недобросовісним відношенням та конфліктністю, незаконними діями та злочинною поведінкою. Окрім зазначених аспектів, внутрішні загрози можуть виникнути в результаті використання в роботі недосконалих чи неефективних технологій банківського виробництва та інформаційного супроводження, неадекватного банківського внутрішньооб’єктового режиму діяльності в установах.

У свою чергу, Зверяков М.І., Коваленко В.В., Сергєєва О.С., аналізуючи управління фінансовою стійкістю банків, виділяють такі зовнішні загрози їхній безпеці, як глобальні банківські кризи, особливості застосування монетарних інструментів з боку НБУ, недосконаліть банківського нагляду та регулювання, суспільна недовіра до банківської та грошової систем, конкурентне середовище, процеси легалізації злочинних доходів та фінансування тероризму, несприятливі макроекономічні умови. До внутрішніх загроз автори відносять: недосконаліть системи фінансового менеджменту; недосконаліть організації проведення основних банківських операцій; недотримання ліквідності банківською установою; слабкість маркетингової політики банку; недостатня кваліфікація і чесність персоналу банку та ін.

Деякі види зовнішніх і внутрішніх загроз безпеці фінансово-кредитних установ, визначених Базельським комітетом з банківського нагляду, відображено у додатку Г.

Додатковий вид загроз за сферою виникнення пропонують Манцуров І.І. й Нусінова О.В, поділяючи зовнішні загрози на “загрози зовнішнього тиску”, що виникають поза межами економічного суб’єкта без його участі, і “репутаційні загрози”, пов’язані із формуванням негативної думки про підприємство у зовнішніх контрагентів; вони виникають поза межами підприємства, але зумовлені його діями та результатами діяльності.

Враховуючи, що репутаційні загрози є надзвичайно небезпечними для фінансово-кредитних установ, вважаємо за доцільне включати їх як підвид зовнішніх загроз діяльності ФКУ.

Багато науковців поряд з поділом загроз економічній безпеці на зовнішні і внутрішні зазначають і такі їх види, як об’єктивні та суб’єктивні, називаючи цю ознаку “за ставленням до загроз”, “за причиною виникнення”, “за джерелом походження”. Загрози пояснюються як такі, що виникають поза волею і без участі економічного суб’єкта (об’єктивні), та такі, що створюються внаслідок дій такого суб’єкта (суб’єктивні). Є також думка, що об’єктивні загрози є природними, а суб’єктивні – штучними. На наш погляд, такі трактування цієї ознаки практично дублюють зміст ознаки “за сферою виникнення”, оскільки об’єктивні загрози виступають зовнішніми по відношенню до суб’єкта, а суб’єктивні – внутрішніми. Крім того, об’єктивними є лише дія економічних законів та настання природних явищ, все інше – політика, законодавство, механізми управління тощо є результатом свідомих дій людей.

Далі, практично у всіх класифікаціях зустрічається поділ загроз на потенційні і реальні, при цьому як ознака зазначається: за можливістю здійснення, за рівнем сформованості, за формою прояву. Думається, що виходячи з попередніх міркувань щодо взаємозв’язку загроз і ризиків, найдоцільніше буде назвати цю ознаку “за формою існування”. Загроза може вважатися вже існуючою, якщо сформульована її сутність і вона мається на увазі при прийнятті комерційних рішень. Інша справа, що до певного часу вона не чинить впливу на

процеси, зокрема, фінансово-кредитної установи і є потенційною; відповідно, при її активізації вона стає реальною (наприклад, загроза невизнання неприбуткового статусу вітчизняних кредитних спілок стала реальністю внаслідок прийняття змін до Податкового кодексу України.

Деякими науковцями пропонується поділяти загрози на приховані та явні, але, на наш погляд, такий поділ є тотожнім за змістом вищенаведеній ознаці.

Важливою і часто згадуваною є ознака загроз економічній безпеці, що характеризується як "за природою виникнення", "за сферою спрямування", "за видом", "за сутністю" і за якої вони поділяються на економічні, політичні, соціальні, правові (законодавчі), інформаційні, технологічні, екологічні та ін. Пропонуємо цей критерій назвати "за природою походження", що, на наш погляд, точніше передає сутність зазначених видів загроз. Крім того, замість правових загроз варто розглядати інституційні як такі, що відображають вплив не лише правових норм, а і діяльності різноманітних інститутів (організацій). Серед загроз, виділених за сферою виникнення, особливо актуальними для фінансово-кредитних установ є економічні, інституційні та інформаційні.

Практично всі автори у тій чи іншій формі згадують ознаку загроз, пов'язану з тривалістю їх дії, але як види вказують або тимчасові і постійні, або з більш докладною градацією у часі – коротко-, середньострокові тощо. Наш погляд, під час ідентифікації загроз, у зв'язку зі швидкоплинністю середовища, дуже важко визначити час їх дії на майбутнє. Тому говорити про якісь більш або менш тривалі проміжки часу недоцільно, отже, варто залишити у класифікації такі види загроз, як тимчасові й постійні.

До цієї ознаки тісно примикає поділ загроз за систематичністю прояву. Незважаючи на безумовну наявність певного смислового відтинку, автори такої точки зору пояснюють систематичні загрози як такі, що існують постійно (чи досить тривалий час), а несистематичні – як ті, що впливають на діяльність

суб'єкта стохастично або з визначеним періодом виникнення, тобто фактично ототожнюють їх з постійними і тимчасовими.

За ознакою передбачуваності виділяють прогнозовані загрози, які можна передбачити та вчасно локалізувати їхні наслідки, або хоча б бути готовими до них, а також непрогнозовані (в інших варіантах класифікації – передбачувані та форс-мажорні). Прогнозування загроз проводиться за результатами моніторингу економічної безпеки фінансово-кредитної установи для подальшого формування та застосування управлінських заходів стратегічного, тактичного і оперативного характеру. Непрогнозовані загрози, як уже зрозуміло, неможливо попередити, оскільки вони з'являються зненацька, що надзвичайно ускладнює процес їх нейтралізації.

Доволі часто у проаналізованих класифікаціях зустрічається ознака "за характером спрямування", "характером впливу" або "механізмом впливу", за якою загрози поділяється на прямі та непрямі (опосередковані). У нашому трактуванні, прямі загрози безпеці фінансово-кредитній установі безпосередньо зачіпають її економічні інтереси і можуть формуватися, у тому числі, адресною навмисною діяльністю інших суб'єктів. Непрямі загрози створюють несприятливе середовище функціонування для багатьох економічних агентів і опосередковано впливають на діяльність ФКУ (зокрема, негативна динаміка макроекономічних показників – обсягу ВВП, рівня інфляції, доходів населення тощо). Більш точною назвою ознаки вважаємо – за характером впливу.

Ще однією класифікаційною ознакою науковці зазначають ступінь небезпеки або значущість загроз. Погоджуємось, що загрози економічній безпеці можуть чинити більш або менш потужний вплив на її рівень, що встановлюється під час ідентифікації загроз ФКУ. Втім, достатньо складно до моменту реалізації загрози визначити міру її реального впливу, тому, на нашу думку, варто використовувати такі орієнтовні види, як небезпечні та особливо небезпечні,

приналежність ідентифікованих загроз до яких визначається на основі попереднього досвіду діяльності.

Далі потрібно зупинитися на наявних у літературі класифікаційних ознаках, в яких, на наш погляд, дещо змішуються сутність загроз та їх наслідки, а також загрози і ризики, що підтверджує вже згадувану думку Козаченко Г.В. й Погорелова Ю.С. Так, при застосуванні ознак “за масштабами збитків” (незначні, значні, катастрофічні), “за ступенем тяжкості наслідків” (незначний збиток, граничний збиток, значний збиток), “за ступенем впливу на безпеку” (значний, допустимий, мінімальний) фактично характеризується не сама загроза, а наслідки її реалізації. Аналіз здійснюється по факту настання несприятливої події, вже за результатами негативного впливу, оскільки неможливо спрогнозувати ступінь значимості заподіяної шкоди заздалегідь.

Науковцями пропонується таку класифікаційну ознаку, як “за мірою керованості” або “за можливістю запобігання”, виділяючи керовані та некеровані загрози. На думку цих авторів, ця ознака характеризує здатність менеджменту організації до самостійної локалізації наслідків. Тут варто зазначити, що загрозами об’єктивно неможливо керувати, їм можна лише протидіяти, а наслідки їх реалізації у будь-якій ситуації становлять відповідальність фінансово-кредитної установи, за виключенням випадків передачі ризиків третім особам, що є складовою управління не загрозами, а ризиками.

Отже, на наш погляд, для відображення основних характеристик загроз безпеці фінансово-кредитних установ необхідно і достатньо використовувати ознаки, відображені у табл. 3.1.

Таблиця 3.1

Класифікація загроз економічній безпеці фінансово-кредитних установ

Ознака	Види загроз
За сферою виникнення	Зовнішні (у т.ч. репутаційні), внутрішні
За формою існування	Потенційні, реальні
За природою походження	Економічні, політичні, соціальні, інституційні, інформаційні, технологічні, екологічні та ін.
За тривалістю дії	Тимчасові, постійні
За характером впливу	Прямі, непрямі (опосередковані)
За ступенем небезпеки	Небезпечні, особливо небезпечні
За можливістю передбачення	Прогнозовані, непрогнозовані

Результатом проведення діагностики загроз економічній безпеці фінансово-кредитної установи є оцінка рівня захищеності установи загалом і у розрізі окремих складових безпеки, виявлення найбільш вразливих бізнеспроцесів, підрозділів і ресурсів. Далі постає питання розробки механізму попередження й нейтралізації загроз, який є основою стабільного і поступального розвитку ФКУ. Для того, щоб була сформована дієва протидія загрозам, фінансово-кредитна установа має спиратися на достовірні інформаційні дані, різнобічні результати аналізу зовнішнього та внутрішнього середовища діяльності. Саме належне інформаційно-аналітичне забезпечення економічної безпеки фінансово-кредитних установ є необхідною основою прийняття обґрунтованих управлінських рішень.

3.2 Методика динамічного розподілу сил та засобів захисту інформації

Вибір конкретних методів та моделей може залежати від конкретних вимог і потреб вашої організації. Проведемо загальний огляд методів:

1. Методи розподілу доступу:

- Рольовий доступ: Призначення прав користувачам відповідно до їхніх ролей у системі.
- Мандатний доступ: Використання правил і обмежень, щоб керувати доступом користувачів до ресурсів.
- Багаторівневий доступ: Класифікація інформації на різні рівні чутливості та надання доступу лише на підставі необхідності.

2. Методи захисту:

- Шифрування: Застосування алгоритмів шифрування для захисту конфіденційності даних.
- Фізичний захист: Заходи для фізичного захисту обладнання та інфраструктури.
- Аутентифікація та авторизація: Визначення і перевірка ідентичності користувачів та контроль їхнього доступу.

3. Математичне моделювання:

- Моделі доступу: Опис правил і механізмів, що регулюють отримання доступу користувачами до ресурсів.
- Моделі загроз: Визначення імовірних загроз і розробка стратегій їхнього запобігання та реагування.
- Математичні методи шифрування: Використання алгоритмів шифрування для забезпечення конфіденційності.

Класифікація підходів і положень методології і математичного моделювання розподілу доступу та захисту КІУСКЗ наведена на рис. 3.3.

Рис. 3.3 Структурна схема класифікації і взаємозв'язку підходів та положень методології і математичного моделювання розподілу доступу та захисту КІУСКЗ

Методи розподілу доступу

Цей метод передбачає призначення конкретних ролей користувачам і призначення відповідних прав доступу до ресурсів, що відповідають їхнім обов'язкам та функціям у організації.

Цей метод передбачає призначення конкретних ролей користувачам і призначення відповідних прав доступу до ресурсів, що відповідають їхнім обов'язкам та функціям у організації.

Мандатний доступ

Заснований на наборі формальних правил і обмежень, які визначають, хто має доступ до якої інформації або ресурсів.

Ефективний для забезпечення відповідності стандартам та правилам, а також для врахування індивідуальних обмежень доступу.

Багаторівневий доступ.

Класифікація інформації на різні рівні чутливості, зазвичай за допомогою літер категорій або класів, і надання доступу тільки на підставі необхідності.

Забезпечує диференційований доступ до інформації, що є особливо важливим для організацій з конфіденційною інформацією.

Методи захисту.

Використання математичних алгоритмів для перетворення зрозумілої інформації в незрозумілу форму (шифровану).

Забезпечує конфіденційність даних, особливо під час передачі чи зберігання інформації.

Фізичний захист.

Використання фізичних засобів, таких як контроль доступу, відеоспостереження, системи сигналізації, щоб забезпечити безпеку обладнання та інфраструктури.

Запобігання фізичному доступу до обладнання та зменшення ризику втрат чи пошкоджень.

Аутентифікація та авторизація

Визначення і перевірка ідентичності користувачів, а потім надання або відмова в доступі відповідно до їхніх прав.

Забезпечення того, що лише вповноважені користувачі мають доступ до системи та ресурсів.

Моделі доступу

Визначення правил та механізмів, за якими користувачі отримують доступ до ресурсів

Допомагає у визначенні та реалізації системи контролю доступу.

Моделі загроз.

Визначення потенційних загроз та інцидентів, що можуть виникнути, та розробка стратегій їхнього запобігання та реагування.

Забезпечення захисту системи від потенційних атак і загроз.

Розробка та використання математичних алгоритмів для шифрування та дешифрування даних.

Забезпечення конфіденційності даних та зменшення ризику несанкціонованого доступу.

Ці підходи є загальними та можуть бути адаптовані відповідно до специфічних потреб та контексту вашої організації. Зверніть увагу, що для критично важливих інформаційних установ і систем важливо враховувати велику

кількість факторів, таких як ступінь чутливості інформації, рівень ризику, регулятивні вимоги та технічні можливості.

Ці підходи і методи можуть бути використані окремо або в комбінації, в залежності від конкретних потреб і ризиків вашої організації. Розуміння контексту та урахування вимог конкретної області важливі для ефективного застосування цих підходів.

Висновок до третього розділу

Результати методики прогнозування інформаційних загроз у процесі розвитку рейдерського захоплення вказують на можливості передбачення та уникнення потенційних загроз.

Методика динамічного розподілу сил та засобів захисту інформації свідчить про можливість ефективного використання ресурсів при реагуванні на інформаційні загрози.

РОЗДІЛ 4
ОРГАНІЗАЦІЙНО-ПРАКТИЧНІ РЕКОМЕНДАЦІЇ З РЕАЛІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ СТРУКТУРНИМ ПІДРОЗДІЛАМ КРЕДИТНО-ФІНАНСОВОЇ УСТАНОВИ

4.1 Пропозиції щодо організаційно-функціональної структури органів захисту інформації кредитно-фінансової установи

Організаційно-функціональна структура органів захисту інформації для кредитно-фінансової установи повинна бути спеціалізованою, ефективною та гнучкою, щоб відповідати унікальним вимогам цього сектору. Ось кілька рекомендацій щодо створення такої структури:

1. Відділ Інформаційної Безпеки:

- Керівництво Інформаційної Безпеки: Відповідає за стратегічне управління інформаційною безпекою, розробку політики та взаємодію з вищим рівнем керівництва.
- Безпека Даних та Конфіденційність: Відповідає за захист фінансової інформації та здійснення заходів щодо конфіденційності даних.

2. Відділ Кібербезпеки та Захисту Від Кібератак:

- Мережева Безпека та Захист Периметру: Забезпечує захист мережевої інфраструктури, моніторинг трафіку та виявлення аномалій.
- Інцидентний Реагування та Відновлення Після Інцидентів: Відповідає за виявлення, реагування та відновлення після кібератак та інших інцидентів.

3. Відділ Управління Доступом:

- Управління Ідентифікацією та Доступом: Встановлює системи ідентифікації користувачів, контроль доступу та аутентифікацію.

4. Відділ Фізичної Безпеки та Контролю:

- Фізична Безпека: Відповідає за заходи безпеки для забезпечення фізичного захисту обладнання та інфраструктури.
- Контроль Доступу: Управління фізичним доступом до приміщень і об'єктів.

5. Відділ Управління Інцидентами та Безпеки Програмного Забезпечення:

- Виявлення та Реагування на Інциденти: Забезпечує моніторинг та реагування на можливі інциденти.
- Безпека Програмного Забезпечення: Розробка та впровадження стандартів безпеки в процес розробки програм.

6. Внутрішній Аудит та Контроль Безпеки:

- Аудит Інформаційної Безпеки: Забезпечує проведення внутрішніх аудитів безпеки для визначення ефективності заходів та виявлення можливих слабких місць.

7. Відділ Навчання та Свідомості Користувачів:

- Навчання з Кібербезпеки: Відповідає за регулярне навчання персоналу щодо правил безпеки та виявлення соціально-інженерних атак.

Ця структура може слугувати базою, але важливо адаптувати її до конкретних потреб і контексту вашої кредитно-фінансової установи, враховуючи ризики та вимоги вашого бізнесу. Забезпечення ефективного взаємодії між різними відділами та підвищення рівня свідомості персоналу є ключовими компонентами успішного захисту інформації.

Зважаючи на специфіку кредитно-фінансової установи, яка має великий обсяг конфіденційної інформації та підвищений ризик фінансових загроз, ось альтернативний варіант організаційно-функціональної структури для органів захисту інформації:

1. Відділ Кібербезпеки та Захисту Фінансової Інформації:

- Мережева Безпека та Виявлення Атак: Забезпечення захисту мережевої інфраструктури та моніторингу на предмет кібератак.

- Захист Фінансових Транзакцій: Розробка та впровадження заходів безпеки для забезпечення цілісності та конфіденційності фінансових операцій.

2. Відділ Управління Ризиками та Захисту Даних:

- Оцінка Ризиків та Контроль: Аналіз потенційних загроз та розробка стратегій зменшення ризиків.
- Захист Конфіденційних Даних: Визначення та впровадження політик та процедур для захисту конфіденційних фінансових даних.

3. Відділ Аналізу та Виявлення Інцидентів:

- Моніторинг Інцидентів: Постійний моніторинг та аналіз подій для виявлення можливих інцидентів безпеки.
- Реагування на Інциденти: Розробка та впровадження процедур швидкого реагування на кібератаки та інші інциденти безпеки.

4. Відділ Управління Доступом та Аутентифікації:

- Ідентифікація та Аутентифікація: Управління системами ідентифікації та процесами аутентифікації користувачів.
- Управління Доступом: Реалізація систем контролю доступу та визначення рівнів доступу.

5. Відділ Безпеки Програмного Забезпечення та Аудиту Коду:

- Аудит Програмного Забезпечення: Аналіз коду для виявлення потенційних вразливостей та недоліків.
- Безпека Розробки: Запровадження стандартів безпеки під час розробки нового програмного забезпечення.

6. Відділ Навчання та Свідомості Користувачів:

- Навчання з Кібербезпеки: Регулярне навчання персоналу з питань кібербезпеки та обізнаності щодо соціально-інженерних атак.

Ця структура розміщена на акцентуванні специфічних аспектів безпеки фінансової інформації. Важливо також враховувати законодавчі вимоги та стандарти безпеки відповідно до сектору фінансів.

4.2 Організаційно-практичні рекомендації щодо реалізації захисту інформації кредитно-фінансової установи

До основних рекомендацій що до захисту інформації кредитно-фінансової установи відносяться:

1. Провести регулярні аудити безпеки інформації для ідентифікації слабких місць та потенційних загроз.
2. Встановити сучасне обладнання для моніторингу мережі та виявлення аномальних активностей, що можуть свідчити про рейдерські загрози.
3. Провести навчання та тренінги для персоналу щодо виявлення соціально-інженерних атак та інших загроз безпеці інформації.
4. Забезпечити своєчасне встановлення патчів та оновлень для всього програмного забезпечення та обладнання для усунення вразливостей.

Аудит безпеки інформації є ключовим елементом в системі захисту кредитно-фінансових установ від рейдерських загроз. Цей процес дозволяє виявити потенційні вразливості та ризики в інформаційній інфраструктурі та приймати заходи для їх ефективного усунення. Нижче наведено кроки та етапи, які можна включити в аудит безпеки інформації кредитно-фінансової установи:

1. Збір Інформації:

Отримання повного списку інформаційних ресурсів, програмного забезпечення, обладнання та персоналу, що використовуються в установі.

2. Оцінка Загроз та Ризиків:

Аналіз ідентифікованих ресурсів для визначення потенційних загроз безпеці та оцінка ризиків для кожного.

3. Оцінка Заходів Захисту:

Перевірка існуючих заходів безпеки, таких як антивірусне програмне забезпечення, файрволи, системи виявлення вторгнень, та їх ефективності.

4. Перевірка Аутентифікації та Авторизації:

Аналіз систем аутентифікації та авторизації, визначення сильних та слабких сторін.

5. Перевірка Фізичної Безпеки:

Оцінка рівня фізичної захищеності серверних кімнат, централізованих баз даних та інших важливих об'єктів.

6. Тестування Захисту Даних:

Проведення тестів на проникнення для виявлення можливостей несанкціонованого доступу до інформації.

7. Оцінка Політик та Процедур:

Перевірка чіткості та відповідності політик безпеки та процедур вимогам безпеки інформації.

8. Аудит Співпрацівників:

Перевірка рівня обізнаності персоналу щодо політик безпеки та їхньої відповідальності.

9. Оцінка Захисту Від Внутрішніх Загроз:

Вивчення можливостей виявлення та запобігання внутрішнім загрозам з боку власного персоналу.

10. Створення Звіту та Рекомендацій:

Підготовка звіту із зазначенням виявлених проблем, ризиків та рекомендацій щодо вдосконалення системи захисту.

11. Постійне Вдосконалення:

Впровадження рекомендацій та постійне вдосконалення системи захисту на основі вивчених навчень та змін в інформаційному середовищі.

Аудит безпеки інформації повинен проводитися періодично та враховувати нові технології та вектори атак для ефективного захисту від рейдерських загроз.

Ефективний моніторинговий інструментарій в сфері інформаційної безпеки є ключовим компонентом для виявлення та відповіді на потенційні загрози, включаючи рейдерські загрози. Основна мета моніторингу - це оперативна реакція на події та аномалії, а також виявлення незвичайної або підозрілої

активності. Нижче подані ключові елементи ефективного моніторингового обладнання:

1. Системи Виявлення Вторгнень (IDS) та Системи Попередження Вторгнень (IPS):

Використання IDS для виявлення аномальних активностей у мережі та IPS для блокування атак та попередження їхнього поширення.

2. Системи Журналювання та Аналізу Журналів (SIEM):

Збір, агрегація та аналіз журналів подій з різних джерел для виявлення аномалій та розслідування інцидентів.

3. Антивірусні та Антималware Системи:

Моніторинг файлових та системних операцій на предмет підозрілої активності та виявлення вірусів чи шкідливих програм.

4. Системи Виявлення Аномальної Активності:

Використання алгоритмів та машинного навчання для виявлення змін у звичайному патерні активності, що може свідчити про атаку.

5. Мережеві Аналізатори та Сканери:

Використання мережевих аналізаторів для моніторингу трафіку та виявлення незвичайних підключень чи активності.

6. Системи Керування Угрозами (Threat Intelligence):

Використання інформації з джерел інтелектуальної безпеки для оцінки та виявлення потенційних загроз.

7. Системи Аналізу Поведінки Користувачів:

Моніторинг поведінки користувачів для виявлення надто прискіпливого доступу або надмірних привілеїв.

8. Моніторинг Систем Файлових та Папкових Доступів:

Виявлення незвичайних змін в правах доступу до файлів та папок.

9. Системи Керування Захистом Кінцевих Точок (EPP та EDR):

Моніторинг та захист кінцевих точок на рівні обладнання та програмного забезпечення.

10. Моніторинг Систем Ідентифікації та Аутентифікації:

Виявлення невдалих спроб аутентифікації та надто активних сеансів користувачів.

11. Розподілені Системи Запису та Аналізу Трафіку:

Збір та аналіз трафіку на різних точках мережі для виявлення аномалій.

12. Системи Керування Конфігурацією та Вразливостей:

Моніторинг конфігурацій та виявлення вразливостей в інфраструктурі.

Використання цих інструментів у сполученні із стратегіями аналізу та виявлення загроз може забезпечити комплексний підхід до моніторингу безпеки, необхідний для захисту кредитно-фінансової установи від рейдерських загроз.

Розробка та впровадження ефективної освітньої програми для персоналу є важливим кроком у забезпеченні високого рівня інформаційної безпеки в кредитно-фінансовій установі. Враховуючи рейдерські загрози, освітня програма повинна бути спрямована на збільшення усвідомленості персоналу щодо можливих ризиків та надання їм засобів для протидії атакам. Ось деякі ключові елементи такої програми:

1. Оцінка Ризиків та Усвідомлення Загроз:

Вивчення персоналом потенційних ризиків, пов'язаних з рейдерськими загрозами та іншими видами кібератак.

2. Соціально-Інженернінгові Атаки та Захист Від Них:

Тренінги щодо розпізнавання та уникнення соціально-інженерних атак, які можуть бути використані рейдерами.

3. Безпечне Використання ІТ-Ресурсів:

Вказівки щодо безпеки в роботі з електронною поштою, веб-сайтами, соціальними мережами та іншими інтернет-ресурсами.

4. Захист Від Фішингу та Малваре:

Навчання персоналу розпізнавати фішингові атаки та уникати встановлення шкідливого програмного забезпечення.

5. Створення Сильних Паролів та Керування Ідентифікацією:

Інструкції щодо створення та управління безпечними паролями та використанням методів двофакторної аутентифікації.

6. Безпечне Підключення до Мережі:

Інформація про безпечне використання публічних Wi-Fi, віртуальних приватних мереж (VPN) та інших мережевих засобів.

7. Безпека Мобільних Засобів:

Засоби захисту інформації на мобільних пристроях, захист від втрати чи крадіжки.

8. Свідоме Керування Електронною Поштою:

Правила взаємодії з електронною поштою, розпізнавання підозрілих повідомлень та атак.

9. Поведінка в Інтернеті:

Освіта щодо безпечної поведінки в Інтернеті, обережність при використанні соціальних мереж та інтернет-ресурсів.

10. Стратегії Реагування на Інциденти:

Навчання персоналу ефективним стратегіям реагування на інциденти та співпраці з відділом безпеки.

11. Постійне Оновлення та Тренінги:

Регулярні оновлення освітніх матеріалів та проведення тренінгів для забезпечення актуальності та ефективності програми.

12. Тестування Щоденної Уваги до Безпеки:

Проведення тестів та вправ для перевірки здатності персоналу використовувати отримані знання в щоденній роботі.

Ця освітня програма повинна бути динамічною, адаптованою до змін у сфері кібербезпеки та враховувати конкретні ризики та потреби кредитно-фінансової установи. Освічений персонал грає критичну роль у забезпеченні безпеки інформації в умовах рейдерських загроз.

Ефективне управління актуальними патчами та оновленнями важливо для забезпечення безпеки інформації та запобігання рейдерським загрозам у банківських установах. Цей процес дозволяє підтримувати актуальність програмного забезпечення та зменшує ризик використання вразливостей. Ось ключові елементи управління актуальними патчами та оновленнями:

1. Інвентаризація Програмного Забезпечення:

Створення повного списку всього програмного забезпечення, що використовується в організації, включаючи операційні системи, бази даних, веб-сервери та інші додатки.

2. Оцінка Вразливостей:

Використання інструментів для сканування та оцінки вразливостей для ідентифікації слабких місць у встановленому програмному забезпеченні.

3. Планування та Пріоритизація:

Розробка плану впровадження патчів та оновлень на основі критичності вразливостей та важливості систем.

4. Тестування Патчів:

Перед впровадженням патчів, їх тестування в ізольованому середовищі для визначення можливих впливів на функціональність систем.

5. Автоматизація Процесу:

Використання систем автоматизації для виявлення, завантаження та впровадження актуальних патчів.

6. Моніторинг та Журналювання:

Постійний моніторинг стану оновлень та журналювання процесу впровадження для виявлення можливих проблем.

7. Захист Завдань Адміністраторів:

Захист завдань адміністраторів та обмеження їхніх привілеїв для запобігання зловживанням або помилковим діям.

8. Регулярні Аудити та Звіти:

Проведення регулярних аудитів для перевірки відповідності стану оновлень стандартам безпеки, а також генерація звітів.

9. Ефективна Комунікація:

Повідомлення про зміни та оновлення, встановлення ефективного механізму комунікації зі всіма відповідальними сторонами.

10. Впровадження Процесів Відкату:

Розробка та впровадження процесів відкату для вирішення проблем, які можуть виникнути під час впровадження патчів.

11. Постійна Освіта Кадрів:

Навчання персоналу важливості вчасного оновлення та використання найновіших патчів для захисту від загроз.

12. Системи Моніторингу Безпеки:

Використання систем моніторингу безпеки для виявлення неавторизованого доступу та надзору за процесами оновлення.

13. Впровадження Політик Безпеки:

Запровадження жорстких політик безпеки, що визначають терміни впровадження оновлень та патчів.

Ефективне управління патчами та оновленнями потребує цілеспрямованості, систематичності та співпраці всіх відділів в організації. Це важливий елемент в захисті від рейдерських загроз та інших кіберзагроз.

Узагальнюючи регулярні аудити безпеки інформації є необхідним елементом для виявлення та адресації слабких місць та потенційних загроз. Рекомендується впровадження систематичного підходу до аудитів, включаючи аналіз інцидентів, оцінку ризиків та взаємодію з експертами з безпеки. Сучасне обладнання для моніторингу мережі та виявлення аномальних активностей є ключовим компонентом системи безпеки. Рекомендується впровадження інтелектуальних систем, здатних розпізнавати зміни у звичайних патернах та швидко реагувати на потенційні загрози. Навчання персоналу стосовно виявлення соціально-інженерних атак та інших загроз безпеці є ефективним засобом забезпечення “людського елементу” в системі безпеки. Рекомендується проведення регулярних тренінгів та оновлення програм для відображення нових загроз та технік. Своєчасне встановлення патчів та оновлень є критичним для усунення вразливостей у програмному та апаратному забезпеченні. Рекомендується впровадження систем автоматизації для швидкого та ефективного розгортання патчів.

4.3 Оцінка ефективності запропонованої методики динамічного розподілу сил та засобів захисту інформації кредитно-фінансової установи

Введення ключових показників ефективності (KPIs) є важливим етапом в забезпеченні моніторингу та оцінки успішності заходів з інформаційної безпеки. Для кредитно-фінансової установи, яка ставить перед собою завдання захисту від рейдерських загроз, важливо визначити та впровадити KPIs, які відображають ключові аспекти безпеки. Ось деякі потенційні KPIs:

Час Реакції на Загрози:

KPI: Середній час реакції на виявлення загрози або інциденту.

Пояснення: Визначає ефективність системи виявлення та реагування на потенційні атаки.

Виявлення та Усунення Вразливостей:

KPI: Кількість виявлених та усунених вразливостей за період часу.

Пояснення: Відображає ефективність процесів усунення слабких місць у безпеці.

Рівень Захисту Інформації:

KPI: Рівень відповідності заходів безпеки до стандартів та регуляцій.

Пояснення: Вказує на те, наскільки добре організація відповідає вимогам забезпечення безпеки.

Кількість Фішингових Атак Виявлено:

KPI: Кількість виявлених та запобігтих фішингових атак.

Пояснення: Визначає рівень осведомленості персоналу та ефективність систем виявлення фішингу.

Тривалість Навчання та Оновлення Персоналу:

KPI: Середній час тривалості навчань для персоналу та частота їх оновлення.

Пояснення: Вказує на регулярність та ефективність освітніх програм.

Своєчасне Встановлення Патчів:

KPI: Відсоток оновлених систем та програм за визначений період.

Пояснення: Визначає ефективність управління патчами та вразливостями.

Результативність Моніторингового Обладнання:

KPI: Кількість виявлених аномальних активностей та викритих загроз.

Пояснення: Оцінює ефективність систем моніторингу та виявлення інцидентів.

Важливо пам'ятати, що KPIs повинні бути конкретними, вимірюваними, досяжними та відповідати стратегічним цілям організації. Регулярний аналіз цих показників допоможе оцінити ефективність та вчасно вживати заходів для удосконалення системи безпеки.

Проведення тестів імітації рейдерського захоплення є важливою частиною стратегії забезпечення інформаційної безпеки для кредитно-фінансової установи. Ці тести дозволяють випробувати реальні процеси та заходи захисту в умовах сценарію рейдерської атаки. Ось деякі ключові аспекти тестів імітації рейдерського захоплення:

Розробка Сценаріїв:

Розробка реалістичних сценаріїв рейдерського захоплення, які можуть включати соціально-інженерні атаки, технічні вразливості та внутрішні загрози.

Визначення Цілей та Об'єктів Тестування:

Визначення конкретних цілей та об'єктів тестування для оцінки відповідності процесів захисту.

Моделювання Сценаріїв:

Моделювання та виконання імітаційних сценаріїв з максимальним наближенням до реальних обставин.

Включення Учасників:

Залучення персоналу та інших зацікавлених сторін для участі в імітаційних тестах.

Оцінка Реакції та Відновлення:

Оцінка ефективності системи виявлення, реакції на інциденти та відновлення після рейдерського захоплення.

Визначення Вразливостей та Недоліків:

Виявлення вразливостей, слабких місць та недоліків в системах безпеки.

Оцінка Комунікації та Співпраці:

Оцінка ефективності комунікації та співпраці між різними відділами та відповідальними сторонами в умовах кризової ситуації.

Створення Звітів та Рекомендацій:

Після завершення тестів розробка докладних звітів і рекомендацій для вдосконалення систем безпеки.

Послідовне Покращення:

Використання результатів тестів для постійного покращення стратегій, процесів та технічних заходів безпеки.

Тести імітації рейдерського захоплення допомагають організації підготуватися до реальних загроз та визначити області, які вимагають додаткового удосконалення. Регулярне проведення таких тестів є важливим елементом циклу безпеки, спрямованого на підвищення стійкості організації до різних форм кіберзагроз, включаючи рейдерські атаки.

Постійне вдосконалення є ключовим принципом в сфері інформаційної безпеки та стратегії боротьби з рейдерськими загрозами для кредитно-фінансових установ. Цей процес передбачає постійний аналіз, оновлення та удосконалення заходів безпеки для відповіді на нові технологічні та кіберзагрози. Ось кілька ключових аспектів постійного вдосконалення:

Аналіз Інцидентів та Використання Звітів:

Ретельний аналіз інцидентів, включаючи імітаційні тести рейдерських захоплень, та використання звітів дозволяє визначити слабкі місця та вдосконалити відповідні стратегії.

Стале Оновлення Стратегій та Політик Безпеки:

Адаптація стратегій та політик безпеки до нових загроз, технологічних та регуляторних змін.

Участь У Постійних Тренінгах та Навчаннях:

Забезпечення персоналу регулярними тренінгами та навчаннями, орієнтованими на виявлення та протидію рейдерським загрозам.

Аудит та Оцінка Відповідності:

Регулярні аудити та оцінка відповідності заходів безпеки до внутрішніх стандартів та регуляцій.

Вдосконалення Моніторингу та Виявлення Інцидентів:

Розробка та впровадження нових методів моніторингу та виявлення інцидентів для швидшої та ефективнішої реакції.

Вдосконалення Технічних Заходів Безпеки:

Оновлення та удосконалення технічних заходів безпеки, включаючи системи виявлення, захисту та реагування на інциденти.

Співпраця з Експертами та Галузевими Організаціями:

Здійснення активної співпраці з експертами та галузевими організаціями для обміну досвідом та отримання консультацій.

Тестування Бізнес-Критичних Процесів:

Регулярне тестування та оцінка безпеки бізнес-критичних процесів для визначення їхньої стійкості до різних атак.

Адаптація до Нових Загроз:

Адаптація стратегій та заходів безпеки до появи нових кіберзагроз та еволюції технологій.

Залучення Всього Колективу:

Залучення всього колективу до культури безпеки та постійного вдосконалення.

Постійне вдосконалення є процесом, що вимагає систематичного підходу та активної участі всього колективу організації у забезпеченні інформаційної безпеки.

На основі наданої інформації, можна провести оцінку методів, описаних у роботі “Технології захисту інформації при спробі рейдерського захоплення банківської установи”. Оцінка включає такі аспекти:

1. Аналіз Стану та Можливостей Комплексних Систем Захисту:

Оцінка: Метод виявлення та аналізу стану і можливостей системи захисту є важливим кроком для розуміння потенційних загроз та ризиків.

2. Комплекс Моделей Системи Захисту:

Створення комплексу моделей, включаючи динамічні середовища та моделі захисту, є високорівневим підходом до проектування системи безпеки.

3. Методика Організації Динамічного Захисту:

Розробка методики для прогнозування та динамічного розподілу сил та засобів в разі рейдерського захоплення дозволяє ефективно реагувати на нові загрози.

4. Організаційно-Практичні Рекомендації:

Пропозиції щодо організаційно-функціональної структури та реалізації захисту інформації можуть служити основою для ефективного впровадження заходів безпеки.

5. Аудит Безпеки Інформації:

Оцінка: Проведення регулярних аудитів для ідентифікації слабких місць та потенційних загроз є ключовим елементом стратегії безпеки.

6. Моніторингове Обладнання:

Використання сучасного обладнання для моніторингу мережі є необхідним для виявлення аномальних активностей та реагування на рейдерські загрози.

7. Освітня Програма для Персоналу:

Навчання персоналу щодо виявлення соціально-інженерних атак є важливим елементом захисту від рейдерських загроз.

8. Керовані Актуальні Патчі та Оновлення:

Забезпечення своєчасного встановлення патчів та оновлень важливо для усунення вразливостей.

Загальна Оцінка:

Методи, описані в роботі, виглядають цілеспрямованими та комплексними, спрямованими на розбудову стійкої системи захисту від рейдерських загроз. Важливо враховувати, що ефективність будь-якої стратегії безпеки залежить від регулярного оновлення та адаптації до змін у загрозах та технологіях.

Висновок до четвертого розділу

Організаційно-функціональна структура органів захисту інформації кредитно-фінансової установи потребує вдосконалення та адаптації для ефективності заходів захисту.

Рекомендації щодо реалізації захисту інформації кредитно-фінансової установи вказують на конкретні заходи та процеси, які слід впроваджувати для підвищення безпеки.

Оцінка ефективності методики динамічного розподілу сил та засобів захисту інформації підтверджує її придатність для практичного використання та реалізації.

ВИСНОВКИ

Кваліфікаційна робота “Технології захисту інформації при спробі рейдерського захоплення кредитно-фінансової установи” представляє комплексний аналіз стану та можливостей захисту інформації в кредитно-фінансових установах, зокрема при рейдерському захопленні. Дослідження включає аналіз банківської системи України, інформаційної структури кредитно-фінансових установ, загроз інформаційній безпеці, нормативно-правової бази, а також існуючої системи захисту.

У розділі 2 роботи визначено комплекс моделей системи захисту інформації кредитно-фінансової установи, включаючи модель динамічного середовища інформаційних загроз рейдерського захоплення, модель формування структури загроз і модель захищеності інформаційного вузла. Ці моделі спрямовані на ефективний захист інформації в умовах рейдерської загрози.

У розділі 3 розглядається методика організації динамічного захисту інформації кредитно-фінансової установи при спробі рейдерського захоплення. Прогнозування інформаційних загроз та динамічний розподіл сил і засобів захисту є ключовими аспектами цієї методики.

У розділі 4 подаються організаційно-практичні рекомендації для реалізації захисту інформації в структурних підрозділах кредитно-фінансової установи. Пропонуються вдосконалення організаційно-функціональної структури органів захисту інформації, рекомендації для реалізації захисту і ефективності методики динамічного розподілу сил і засобів захисту.

В цілому, робота пропонує системний підхід до захисту інформації в умовах рейдерського захоплення фінансово-кредитноїї установи, враховуючи специфіку банківської системи України та існуючі загрози. Рекомендації і методики, включені до роботи, можуть слугувати практичним керівництвом для підвищення ефективності захисту інформації в банківських установах перед потенційними рейдерськими загрозами.

СПИСОК ПОСИЛАНЬ

1. William Stallings. “Network Security Essentials” : монографія / Pearson /William Stallings. Boston: Pearson, 2019. 512 с.

2. Bruce Schneier. “Applied Cryptography: Protocols, Algorithms, and Source Code in C” :монографія / John Wiley & Sons / Bruce Schneier. New York: Wiley, 2018. 784 с.

3. Gary McGraw, Bruce Schneier. “Exploiting Online Games: Cheating Massively Distributed Systems” : монографія / Addison-Wesley / Gary McGraw, Bruce Schneier. Boston: Addison-Wesley, 2017. 384 с.

4. Kevin D. Mitnick, William L. Simon. “The Art of Deception: Controlling the Human Element of Security” : монографія / Wiley / Kevin D. Mitnick, William L. Simon. Indianapolis: Wiley, 2022. 368 с.

5. Cory Doctorow. “Little Brother” : роман / Tor Teen / Cory Doctorow. New York: Tor Teen, 2018. 382 с.

6. Hacking Team. “Hacking Team: The Commercialization of Cyberespionage” : звіт / Citizen Lab / Hacking Team. Toronto: Citizen Lab, 2015. 78 с.

7. Shon Harris, Allen Harper. “Gray Hat Hacking: The Ethical Hacker's Handbook” : монографія / McGraw-Hill / Shon Harris, Allen Harper. New York: McGraw-Hill, 2023. 656 с.

8. Dan Kaminsky. “Serious Cryptography: A Practical Introduction to Modern Encryption” : монографія / No Starch Press / Dan Kaminsky. San Francisco: No Starch Press, 2017. 336 с.

9. Mark Stamp. “Information Security: Principles and Practice” : підручник / Wiley / Mark Stamp. Hoboken: Wiley, 2022. 616 с.

10. Ross J. Anderson. “Security Engineering: A Guide to Building Dependable Distributed Systems” : монографія / Wiley / Ross J. Anderson. Hoboken: Wiley, 2020. 1080 с.

11. Adam Shostack. “Threat Modeling: Designing for Security” : монографія / Wiley / Adam Shostack. Hoboken: Wiley, 2022. 624 с.

12. Charlie Miller, Dino Dai Zovi. “The iOS Hacker's Handbook” :/монографія / Wiley / Charlie Miller, Dino Dai Zovi. Hoboken: Wiley, 2022. 408 с.

13. Bruce Sterling. “The Hacker Crackdown: Law and Disorder on the Electronic Frontier” : документальний нарис / Bantam Books / Bruce Sterling. New York: Bantam Books, 2022. 336 с.

14. Peter Szor. “The Art of Computer Virus Research and Defense” : монографія / Addison-Wesley / Peter Szor. Boston: Addison-Wesley, 2019. 744 с.

15. Jonathan Zittrain. “The Future of the Internet and How to Stop It” : монографія / Yale University Press / Jonathan Zittrain. New Haven: Yale University Press, 2018. 352 с.

16. Cory Doctorow. “Homeland” : роман / Tor Teen / Cory Doctorow. New York: Tor Teen, 2018. 400 с.

17. Joseph Menn. “Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet” : журналістське дослідження / PublicAffairs / Joseph Menn. New York: PublicAffairs, 2018. 320 с.

18. Michael Sikorski, Andrew Honig. “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” : практичний посібник / No Starch Press / Michael Sikorski, Andrew Honig. San Francisco: No Starch Press, 2022. 800 с.

19. Kim Zetter. “Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon” : журналістське дослідження / Crown / Kim Zetter. New York: Crown, 2019. 448 с.

20. Steven Levy. “Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age” : історичний нарис / Viking / Steven Levy. New York: Viking, 2021. 368 с.

21. Richard Bejtlich. “The Practice of Network Security Monitoring: Understanding Incident Detection and Response” : монографія / No Starch Press / Richard Bejtlich. San Francisco: No Starch Press, 2021. 376 с.

22. Nitesh Dhanjani, Billy Rios, Brett Hardin. “Hacking: The Next Generation” : монографія / O'Reilly Media / Nitesh Dhanjani, Billy Rios, Brett Hardin. Sebastopol: O'Reilly Media, 2019. 298 с.

23. Michael Goodrich, Roberto Tamassia. “Algorithmic Foundations of Cybersecurity” : монографія / Springer / Michael Goodrich, Roberto Tamassia. New York: Springer, 2017. 569 с.

24. Peter J. Stavroulakis. “Network Security Essentials: Applications and Standards” : підручник / Prentice Hall / Peter J. Stavroulakis. Upper Saddle River: Prentice Hall, 2016. 552 с.

25. Neil Daswani, Anmol Misra, David C. Strohecker. “Foundations of Security: What Every Programmer Needs to Know” : підручник Apress / Neil Daswani, Anmol Misra, David C. Strohecker. Berkeley: Apress, 2017. 384 с.

26. Jeremiah Grossman, Trey Ford. “Web Application Security: A Beginner's Guide” : практичний посібник / McGraw-Hill / Jeremiah Grossman, Trey Ford. New York: McGraw-Hill, 2021. 352 с.

27. E. Eugene Schultz, Jim D. Shackleford. “Dictionary of Information Security” : словник \ Syngress / E. Eugene Schultz, Jim D. Shackleford. Burlington: Syngress, 2016. 352 с.

28. Thomas J. Holt, Adam M. Bossler. “Cybercrime and Digital Forensics: An Introduction” : підручник / Routledge / Thomas J. Holt, Adam M. Bossler. New York: Routledge, 2018. 300 с.

29. Gary Bahadur, Jason Inasi, Alex de Carvalho. “Securing the Clicks Network Security in the Age of Social Media” : монографія / McGraw-Hill / Gary Bahadur, Jason Inasi, Alex de Carvalho. New York: McGraw-Hill, 2021. 304 с.

30. David Seidl, Michael G. Solomon. “Fundamentals of Information Systems Security” : підручник / Jones & Bartlett Learning / David Seidl, Michael G. Solomon. Burlington: Jones & Bartlett Learning, 2019. 560 с.

31. Andrew S. Tanenbaum. “Computer Networks” : підручник / Prentice Hall / Andrew S. Tanenbaum. Upper Saddle River: Prentice Hall, 2020. 912 с.

32. Vincent Nestler, Russell Osborn, Timothy J. Shimeall. “Computer and Information Security Handbook” : довідковий посібник / Morgan Kaufmann / Vincent Nestler, Russell Osborn, Timothy J. Shimeall. Boston: Morgan Kaufmann, 2018. 978 с.