ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО
ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система захисту технічних каналів передачі інформації від несанкціонованого доступу на об’єкті фінансової діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

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

Виконав: здобувач вищої освіти групи СЗДМ 62
Олександр ЛИХОГОД

Керівник: АВЕРІЧЕВ Ігорь .
к.е.н., (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

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

Кафедра Технічних систем кіберзахисту
Ступінь вищої освіти магістр
Спеціальність Кібербезпека та захист інформації
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____ Олександр ТУРОВСЬКИЙ

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лихогоду Олександру Ігоровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система захисту технічних каналів передачі інформації від несанкціонованого доступу на об'єкті фінансової діяльності»
керівник кваліфікаційної роботи Ігорь АВЕРІЧЕВ, к.е.н.

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: об'єкт банківської діяльності, технічні канал витоку інформації, вимоги до захисту інформації в банківській установі, технічні канали витоку інформації банківської установи.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Проаналізувати систему роботи банківської установи та канали можливого витоку інформації;
4.2. Проаналізувати ризики банківської діяльності;
4.3. розробити систему захисту інформації в банківській системі з використанням сучасних засобів.

5. Перелік графічного матеріалу: Презентаційний матеріал на слайдах

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Олександр ЛИХОГОД
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Ігорь АВЕРІЧЕВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи складається з: вступу, чотирьох розділів, висновків та переліку використаних джерел. Обсяг роботи складає 80 сторінки. Список використаних джерел містить 30 джерел.

Метою роботи є підвищення ефективності захисту технічних каналів передачі інформації від несанкціонованого доступу на об'єкті фінансової діяльності.

В кваліфікаційній роботі було розглянуто банк, наведено його будову та технічне оснащення, проаналізовано місця можливого витоку інформації та запропоновано план дій для унеможливлення несанкціонованого доступу до інформації, яка циркулює в банку. Також розглянуто інформацію про банківську систему, основні загрози банківської діяльності.

Об'єкт дослідження – банківська установа.

Предмет дослідження – система захисту інформації банківської установи

Підсумком роботи є розроблена система захисту інформації в банківській системі, зроблено підбір оптимальної техніки для створення даної системи захисту.

Апробація:

Ю.В. Жеребок, І.В. Довбня, О.І. Лихогод, Особливості функціонування та завдання системи захисту технічних каналів передачі інформації об'єктів банківської діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.32-33. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

Ключові слова: СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ, ПРИСТРОЇ ЗАХИСТУ ІНФОРМАЦІЇ, ЗАХИСТ ІНФОРМАЦІЇ, БАНКІВСЬКА СИСТЕМА, ОСНОВНІ ЗАГРОЗИ БАНКІВСЬКОЇ СИСТЕМИ.

ABSTRACT

Qualification work consists of: introduction, four sections, conclusions and a list of sources used. The volume of work is 80 pages. The list of sources used contains 30 sources.

The purpose of the work is to increase the efficiency of information security in the banking system using modern means.

The qualification work examined the bank, presents its structure and technical equipment, analyzes the locations of possible leakage of information and proposed a plan of action to prevent unauthorized access to information circulating in the bank. Information on the banking system, the main threats of banking activity is also considered.

The object of study is a banking institution.

The subject of research is a system of information security of a banking institution

The result of the work is the developed system of information protection in the banking system, the selection of optimal equipment to create this protection system is made.

ACCESS CONTROL AND MANAGEMENT SYSTEM, INFORMATION PROTECTION DEVICES, INFORMATION PROTECTION, BANKING SYSTEM, MAIN THREATS TO THE BANKING SYSTEM.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

СКУД – Система контролю та управління доступом

СЕП – Система електронних платежів

ЕЦП – електронний цифровий підпис

НБУ – Національний банк України

АРМ – автоматизоване робоче місце

ПЕМВН – побічні електромагнітні випромінювання та наведення

ДСТУ – державний стандарт України

ОВДП – облігації внутрішніх державних позик України

ОІД – об’єкти інформаційної діяльності

АТС – автоматична телефонна станція

НСД – несанкціонований доступ

ВСТУП

Сьогодні банківський сектор України має надійну систему безпеки, яку можна вважати основою стабільної діяльності банку, досягнення його фундаментальних інтересів та першочергових цілей, захисту від внутрішньої та зовнішньої нестабільності, а також гарантією його незалежного функціонування. Основним критерієм ефективності безпеки банку є стабільність економічного та фінансового стану банку.

Враховуючи високу залежність банківського сектору від надійності його інформаційних технологій, інформаційна безпека стала одним з фундаментальних принципів усієї банківської системи. Для будь-якої банківської установи одним з основних напрямків інформаційної безпеки є захист банківської таємниці.

Тому встановлення систем контролю доступу в будь-якому місці є найважливішим заходом для захисту банківських установ. Комплексна система контролю доступу може вирішити численні проблеми: контроль доступу персоналу, ідентифікацію та управління користувачами, автоматизацію виробничих процесів. Сучасні системи контролю та управління доступом використовують різні технології: безконтактні картки, біометричні системи, електронні замки, системи енергозбереження тощо.

Завданням цієї роботи є захист інформаційної безпеки в банківських системах за допомогою сучасних інструментів.

РОЗДІЛ 1.
БАНКІВСЬКА СИСТЕМИ ТА ЇЇ БЕЗПЕКА

1.1 Банківська система

Банки є найважливішим компонентом національної банківської системи. В академічних колах експерти розходяться в думках щодо визначення поняття «банк», причому одні визначають його як кредитну установу, а інші – як фінансового посередника, який надає різні фінансові послуги клієнтам (фізичним та юридичним особам), включаючи зберігання, перекази, обмін валюти, а також купівлю-продаж золота та інших дорогоцінних металів [1,2,3].

В Україні банки є життєво важливою частиною фінансової системи та основою спеціальної категорії «фінансових посередників». Історично українські банки домінували на ринку фінансових посередників, здійснюючи більшість фінансових операцій країни.

З огляду на це, варто зазначити, що характер банківської справи в сучасній інформаційній економіці змінюється, що вимагає уточнення значення терміна «банк». З огляду на це, ми пропонуємо таке визначення банківської справи: Банк – це юридична особа, тобто фінансовий посередник, який продає всі фінансові продукти та послуги (не заборонені законом) безпосередньо (контактно) або дистанційно (безконтактно) клієнтам (іншим юридичним та фізичним особам), а також здійснює інші законні операції, спрямовані на максимізацію прибутку для своїх власників (акціонерів), та підлягає широкому нагляду та контролю з боку центрального банку [1,2,3]. Це визначення має на меті підкреслити такі моменти: по-перше, воно уточнює природу, цілі та основну мету банківських операцій без деталізації їхньої конкретної операційної діяльності; по-друге, воно розширює обсяг «традиційних» функцій банківських операцій у контексті інформаційної економіки; та по-третє, воно підкреслює наглядову та контрольну роль регуляторних органів за банківською діяльністю [1,2,3].

Усі банки в країні разом утворюють банківську систему цієї країни. Банківська система є однією з найважливіших і найскладніших структур у ринковій економіці, що складається з численних установ (фінансових посередників) з різним ступенем спеціалізації та правовими формами, що функціонують у рамках єдиної фінансової системи та монетарного механізму протягом певного періоду часу. Інше визначення розглядає банківську систему як добре структуровану, юридично визначену та взаємозалежну групу фінансових посередників, які здійснюють специфічну банківську діяльність та функціонально пов'язані між собою, утворюючи незалежну структуру [1,2,3].

В Україні процес побудови сучасної банківської системи, що відповідає умовам ринкової економіки, триває і триватиме ще довго. Це пояснюється тим, що українська економіка ще не завершила необхідну трансформацію і не стала по-справжньому ринковою.

Однак можна сказати, що Україна заклала основу для ринкової банківської системи.

Національний банк України виконує майже всі функції центрального банку в ринковій економіці. Він використовує ринкові інструменти монетарного коригування для виконання своїх обов'язків.Обов'язкові резервні вимоги комерційних банків, їхня політика кредитування та рефінансування, а також торгівля державними облігаціями на відкритому ринку [1,2,3].

У країнах, де ринкові принципи домінують в економічних відносинах, методи роботи комерційних банків поступово стають домінуючими.

За останні роки у вітчизняній економічній літературі з'явилася велика кількість монографій, що узагальнюють досвід світової банківської системи та розглядають особливості формування банківської системи України. Зокрема, серія робіт детально описує методи роботи комерційних банків. Тим часом наразі відсутня навчальна література, що обговорює діяльність центральних банків та регуляторний характер їхньої монетарної політики щодо економіки.

Термін «система» часто використовується для вивчення різних явищ природного та соціального розвитку. Системний підхід вважається відмінною

рисою сучасного мислення. Термін «система» використовують не лише вчені та філософи, а й діячі культури та мистецтва, організатори виробництва та банківські керівники.

Однак терміни «система» та «банківська система» визначають не лише складові банку. Термін «банківська система» має ширше значення, яке включає [3,4]:

- Сукупність елементів;
- Достатність елементів, що складають певну цілісність;
- Взаємодію між елементами.

Банківська система має унікальні характеристики, демонструючи атрибути, відмінні від інших систем, що функціонують у національній економіці. Ця унікальність залежить від її компонентів та взаємозв'язків між ними. Тому характер банківської системи впливає на склад та характер її окремих елементів.

У світовій практиці існує кілька типів банківських систем:

- Централізовані розподільчі банківські системи;
- Ринкові банківські системи;
- Перехідні системи.

На відміну від розподільчих систем, ринкові банківські системи характеризуються відсутністю державної банківської монополії. Будь-яке виробниче підприємство будь-якої форми власності (не обмежуючись державними підприємствами) може створити банк.

У ринковій економіці існує безліч банків з децентралізованим управлінням. Емісійні та кредитні функції розподілені між ними. Ця тема в першу чергу зосереджена на центральному банку, тоді як кредити підприємствам та фізичним особам надаються різними типами комерційних банків, включаючи комерційні банки, інвестиційні банки, інноваційні банки, іпотечні банки, ощадні банки тощо.

Комерційні банки не беруть на себе державний борг, так само як держава не бере на себе борг комерційних банків; комерційні банки підпорядковуються їхнім радам директорів, а не державним адміністративним органам [3,4,5].

Таким чином, сучасна банківська система України є перехідною системою. Вона функціонує за ринковою моделлю та поділена на два рівні. Перший рівень включає підпорядковані установи Національного банку України, які відповідають за емісію грошових одиниць (емісію), забезпечення стабільності гривні, а також за нагляд та управління діяльністю комерційних банків.

Другий рівень складається з різних комерційних банків, метою яких є обслуговування клієнтів (компаній, організацій, фізичних осіб) та надання їм різноманітних послуг (кредитні, розрахункові, готівкові, депозитні та валютні операції). Таким чином, банківська система України перебуває в постійному руслі. Вона містить компоненти ринкової банківської системи, але взаємодія між цими компонентами ще не повністю розвинена. Тому при побудові емісійних установ та взаємодії всередині банківської системи необхідно враховувати характеристики та умови ринкової економіки.

Діяльність банківських установ та інших комерційних структур за ринкових умов є за своєю суттю продуктивною. Хоча результати цієї діяльності не є прямими матеріальними продуктами в традиційному розумінні (наприклад, промислова чи сільськогосподарська продукція), їхня цінність відображається в соціальній цінності [3,4,5].

Основними продуктами комерційних банків є надання різних форм послуг, включаючи кредитування, розрахунки, управління активами та вартістю, гарантії, індосаменти та консалтинг. Це базується на обміні грошей як особливого товару, що є передумовою для забезпечення достатніх платіжних засобів для економіки.

Основні функції комерційних банків відіграють вирішальну роль у характері їхніх банківських продуктів. Характеристики банківської діяльності полягають у тому, що, з одного боку, вони надають різноманітні послуги через

активні, пасивні та комісійні посередницькі операції; з іншого боку, вони створюють безготівкові методи оплати, які значною мірою є результатом вищезгаданих операцій.

Комерційні банки створюють безготівкові методи оплати, випускаючи депозити на основі позик та рахунків клієнтів, що призводить до загального розширення грошової маси. Зі зростанням попиту на банківські кредити сучасний механізм емісії грошей може збільшити грошову масу; навпаки, зі зменшенням попиту він може зменшити грошову масу. Тому здатність комерційних банків створювати гроші має вирішальне значення для економіки.

Другим компонентом банківських продуктів є різні комерційні банківські послуги: депозити, позики, розрахунки, готівка, інвестиції, трасти, обмін валюти, консалтинг тощо. Чітка термінологія є важливою для пояснення їхньої природи та характеристик.

Банківські продукти. Кінцевим результатом банківських операцій є надання послуг клієнтам. З цією метою банки займаються різними видами бізнесу. Іншими словами, справжня «послуга» – це кінцевий результат, готовий продукт банку, тоді як «операція» – це його виробничий процес.

Класифікуючи цей процес, необхідно враховувати характеристики формування та розподілу ресурсів комерційного банку, які можна узагальнити у три основні категорії: зобов'язання, активи та комісійні послуги. Пасивні операції спрямовані на тимчасове залучення вільних коштів для розвитку власних ресурсів банку.

Активний бізнес стосується інвестування ресурсів банком для отримання прибутку. Комісійний бізнес стосується збору банком комісій та надання послуг від імені клієнтів. Останній не передбачає формування та розподіл ресурсів, а скоріше переказ існуючих коштів клієнтів або інший бізнес, не пов'язаний безпосередньо з грошовим потоком (тобто так звані позабалансові послуги).

За допомогою цих трьох категорій бізнесу комерційні банки надають клієнтам різні послуги, які разом складають банківські продукти. Однак є

винятки. Це означає, що пасивний бізнес, який здійснюють комерційні банки з метою накопичення капіталу, та активний бізнес у сфері інвестицій (визначений вище) не можуть вважатися банківськими продуктами. І навпаки, це послуги, що надаються самими комерційними банками: перший відображає залучення капіталу, а другий – його пропозицію.

Досягнення новітніх банківських технологій та загострення конкуренції на фінансових ринках спонукали банки постійно шукати нові продукти, тим самим розширюючи склад свого банківського бізнесу та збільшуючи свій глобальний масштаб. Це відображається у все більш проактивному проникненні банків у нетрадиційні сфери бізнесу (страхування, туризм тощо). Однак, враховуючи сучасну диверсифікацію банківських операцій, кожен банк можна класифікувати за одним із трьох типів: пасивний бізнес, активний бізнес або комісійне брокерство.

Загалом, результат банківських операцій, безсумнівно, прибутковий. Займаючись прийманням депозитів, банки тимчасово накопичують вільні кошти та перетворюють їх на капітал, тобто дозволяють «неопераційним» ресурсам створювати цінність для окремих учасників ринку та економіки в цілому.

Застосування банківського кредиту у виробництві є необхідною умовою для підвищення ефективності відтворення, тоді як споживчий кредит може підвищити ефективний попит, тим самим сприяючи економічному зростанню. Своєчасна організація та обробка банками створюють умови для продовження торгівлі та можливості для ефективного припливу капіталу в економіку. Здійснення інших банківських послуг також створює умови для нормального функціонування різних секторів економіки та забезпечує гідний рівень життя.

З огляду на поширену в моїй країні негативну політичну упередженість щодо «непродуктивної» ролі комерційної банківської системи, чітке розуміння цих питань є особливо важливим.

Попередні нормативно-правові документи допоможуть розвіяти негативні стереотипи щодо банківських установ як частини «надбудови» виробничого

сектору національної економіки, оскільки від цього значною мірою залежить сприйняття громадськістю важливої ролі фінансового ринку та його основних учасників — банків. Оцінка ефективності цих заходів має вирішальне значення для оцінки їхньої здатності подолати економічну рецесію та досягти всебічного розвитку, який гарантує гідний рівень життя українського народу та наближає його до зрілих ринкових економік розвинених країн.

Ключовою функцією банківської системи є її здатність регулювати грошові потоки відповідно до економічних потреб. Кожен банк випускає платіжні інструменти. Цей потенціал є більш значним і поширеним у банківській системі. Емісія валюти має значний вплив на стабільність грошової маси та ефективність виробництва та обігу товарів.

Центральний банк здійснює емісію первинної валюти шляхом випуску готівки, надання кредитів уряду та комерційним банкам, а також купівлі акцій, золота та іноземної валюти. Комерційні банки випускають вторинну валюту через операції кредитування та розрахунків, використовуючи механізм множення капіталу для збільшення своїх фондів.

Відповідні закони та нормативні акти захищають нормальне функціонування банківської справи та встановлюють відповідні механізми для нагляду та контролю за дотриманням банківською діяльністю чинних законів та нормативних актів.

1.2 Доступ до банківської інформації

Інформація – це будь-яка інформація та/або дані, які можуть зберігатися на матеріальному носії або відображатися в електронній формі. Суб'єкти інформаційних відносин можуть вимагати усунення будь-якого порушення своїх прав та відшкодування майнової та моральної шкоди, завданої таким порушенням. [4] Інформація з обмеженим доступом стосується конфіденційної інформації, секретної інформації та службової інформації. [5]

Для уточнення значення терміна «банківська інформація» необхідно визначити, хто має право здійснювати діяльність, пов'язану з розкриттям інформації, та на основі цього визначити орган, відповідальний за здійснення діяльності, пов'язаної з потоком банківської інформації. Згідно зі статтею 7 Закону України «Про інформацію», суб'єктами інформаційних відносин, тобто особами, які можуть брати участь в інформаційних відносинах, є: громадяни України, юридичні особи та держава. Крім того, аналіз законодавства вказує на те, що суб'єктами інформаційних відносин можуть бути також інші країни, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства. Учасниками інформаційних відносин є громадяни, юридичні особи або держава, які безпосередньо беруть участь в інформаційній діяльності та які відповідно до закону користуються правами на інформаційну діяльність та несуть відповідні обов'язки. Стаття 42 визначає, що основними учасниками інформаційних відносин є: автори інформації, споживачі інформації, розповсюджувачі інформації та зберігачі інформації. Тим часом, Закон України «Про інформацію» розуміє інформаційну діяльність як сукупність заходів, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави. Основні види інформаційної діяльності, передбачені чинним законодавством, включають отримання, використання, поширення та зберігання інформації. Отримання інформації стосується громадян, юридичних осіб та держави, які набувають, купують або накопичують записану або загальнодоступну інформацію відповідно до чинного законодавства України. Використання інформації спрямоване на задоволення інформаційних потреб громадян, юридичних осіб та держави. Поширення інформації — це розповсюдження, публікація або продаж записаної або загальнодоступної інформації відповідно до вимог законодавства. Зберігання інформації спрямоване на забезпечення належного стану інформації та її фізичних носіїв.

Аналіз чинного законодавства України показує, що інформація в основному поділяється на дві категорії: інформація з відкритим доступом та інформація з обмеженим доступом. Механізми забезпечення доступу до

відкритої інформації включають: систематичну публікацію через офіційні друковані видання (бюлетені, антології); поширення через засоби масової інформації; та забезпечення каналів прямого доступу для зацікавлених громадян, державних органів та юридичних осіб.

Відповідно до правових норм, інформація з обмеженим доступом поділяється на конфіденційну інформацію та секретну інформацію. Таким чином, конфіденційна інформація стосується інформації, що знаходиться у володінні таких суб'єктів: Фізичні або юридичні особи можуть використовувати або розпоряджатися цією інформацією, яка буде розповсюджена відповідно до ваших вимог та встановлених вами умов. Секретна інформація – це інформація, що становить державну таємницю, та інша інформація, класифікована законом як таємна, розголошення якої завдасть шкоди особам, суспільству та державі.

Виходячи з основних положень чинного законодавства України щодо інформаційної діяльності, ми спробуємо визначити термін «банківська інформація», виділивши його характеристики та розрізнивши його види.

Враховуючи, що інформація визначається як зафіксована або публічно розкрита інформація щодо подій та явищ, що відбуваються в суспільстві, державі та навколишньому середовищі, виникає питання: яку інформацію, події чи явища слід вважати банківською інформацією? По-перше, слід зазначити, що інформація, яку може ідентифікувати банк, повинна бути пов’язана з банківською діяльністю компанії. Це пояснюється тим, що банк – це юридична особа, уповноважена Національним банком України, яка має виключні права: приймати депозити від фізичних та юридичних осіб та вносити ці кошти до банку від свого імені, на своїх умовах та на свій ризик; а також відкривати та вести банківські рахунки для фізичних та юридичних осіб. Банківська діяльність полягає у запиті коштів у фізичних та юридичних осіб та внесенні цих коштів на банківські рахунки від свого імені, на своїх умовах та на свій ризик. Тому інформація, що вважається банківською, повинна бути пов'язана з діяльністю банку, який здійснює банківську діяльність. У цьому контексті інформація, зафіксована в нормативно-правових документах банківських

установ, документи, що підтверджують ведення банківської діяльності, та документи, що підтверджують, що ведення бізнесу не є незаконним, належать до категорії банківської інформації. Рекламна інформація, що проактивно розголошується банківськими установами, також вважається публічною інформацією.

Таким чином, поняття «банківська інформація» можна визначити як інформацію, що міститься в банківських документах або розголошується банківськими установами відповідно до процедур, передбачених чинним законодавством України, що стосуються їхньої банківської діяльності.

Враховуючи основні види інформаційної діяльності, чинне законодавство визнає отримання, використання, розповсюдження та зберігання інформації, а основними видами інформаційної діяльності у сфері банківської інформації є отримання, використання, розповсюдження та зберігання банківської інформації.

Виходячи з визначення «банківської діяльності», отримання банківської інформації можна визначити як діяльність банківської установи зі збору інформації, пов'язаної з банківською інформацією. Використання банківської інформації стосується процесу, за допомогою якого відповідні сторони, відповідно до процедур, передбачених чинним законодавством України, задовольняють свої інформаційні потреби шляхом доступу до банківської інформації. Поширення банківської інформації стосується процесу, за допомогою якого відповідні сторони, відповідно до процедур, передбачених чинним законодавством України, поширюють серед них банківську інформацію. Зберігання банківських даних є обов'язком згідно з чинним законодавством України для установ, уповноважених поширювати банківські дані, але лише у випадках, прямо передбачених законом.

Слід також зазначити, що, оскільки банківські операції є процесом, що постійно розвивається та вдосконалюється, вищезгаданий перелік інформації, пов'язаної з банківською діяльністю, може продовжувати розширюватися. Однак, як видно з вищезазначеного, категорії банківської інформації

включають інформацію з різними методами доступу та специфічними характеристиками діяльності. Очевидно, що банки, як учасники банківських відносин, навмисно поширюють певну інформацію; тоді як щодо іншої інформації банківські установи зобов'язані зберігати та захищати цю інформацію.

Тому банківські установи обробляють два типи інформації під час здійснення банківської діяльності:

- Загальнодоступна банківська інформація;

- Банківська інформація з обмеженим доступом.

Аналіз чинного українського банківського законодавства показує, що загальнодоступна банківська інформація може містити інформацію, пов'язану з діяльністю банківських установ, але не вважається конфіденційною банківською інформацією. Цей тип інформації може бути інформацією, яку банки навмисно розкривають, або інформацією, яку банки зобов'язані розкривати.

Інформація, отримана банком щодо діяльності клієнтів та їх фінансового стану під час надання банківських послуг, а також інформація щодо відносин, встановлених з клієнтами або третіми особами під час надання банківських послуг, вважається конфіденційною інформацією банку. [6] Зокрема, конфіденційна інформація банку включає:

- Інформацію про банківський рахунок клієнта, включаючи агентський рахунок банку в Національному банку України;

- Операції, здійснені від імені або для клієнтів;

- Економічний та фінансовий стан клієнта;

- Банківську систему та систему захисту прав клієнтів;

- Інформацію про організаційно-правову структуру юридичних осіб: клієнтів, їх керівників, господарську діяльність;

- Інформація про ділову діяльність клієнтів або комерційні таємниці, проекти, винаходи, зразки продукції та інша бізнес-інформація;

- Інформація індивідуальної банківської звітності, крім інформації, яка підлягає розкриттю;

- Коди, що використовуються банком для захисту інформації;

- Персональна інформація, отримана в результаті кредитних розслідувань щодо запропонованих договорів споживчого кредитування.

Інформація про банк або його клієнтів, зібрана в рамках банківського нагляду, вважається банківською конфіденційною інформацією.

Інформація про банк або його клієнтів, отримана Національним банком України від банківських регуляторів інших країн відповідно до міжнародних договорів або принципу взаємності, з метою банківського нагляду або запобігання відмиванню грошей чи фінансуванню тероризму, вважається банківською конфіденційною інформацією. Це положення не поширюється на інформацію, яка підлягає розкриттю. Перелік інформації, яка підлягає розкриттю, складається Національним банком України, а банки також можуть самостійно вирішувати його складання.

Національний банк України публікує нормативно-правові документи щодо зберігання, захисту, використання та розкриття банківської конфіденційної інформації та тлумачить застосування цих правових документів. [6] Комерційна таємниця повинна включати інформацію, що відображає характеристики нових банківських технологій, роботу в нових сферах обслуговування, плани розвитку банку та його мережі, а також іншу інформацію, пов'язану з прибутковістю. Склад та обсяг інформації, що становить комерційну таємницю, а також процедури її захисту визначаються президентом банку відповідно до вимог Постанови Кабінету Міністрів України від 9 серпня 1993 року № 611 «Про перелік інформації, що не становить комерційної таємниці».

Розкриття інформації, що становить комерційну таємницю, є важливою складовою системи заходів банку щодо захисту фінансової безпеки клієнтів. Необхідно враховувати такі характеристики інформації, класифікованої як комерційна таємниця:

- Вона не є державною таємницею;

- Вона не підпадає під дію Постанови Кабінету Міністрів України від 9 серпня 1993 року № 611;

- Вона не містить відомої інформації;

- Вона належить банку та пов'язана з банківськими операціями;

- Вона має будь-яке суттєве значення або потенційну цінність для розвитку банку;

- Вона має систему контролю доступу;

- Містить інформацію щодо технологій, виробництва, управління та операцій банку.

У нашій країні ще не встановлено метод класифікації певної інформації як комерційної таємниці.

Нормативні акти щодо комерційної таємниці та процедур її отримання можуть включати такі частини:

- Права та обов'язки посадових осіб щодо доступу керівного персоналу до документів та інформації, що містять комерційну таємницю;

- Права та обов'язки банківських служб безпеки щодо доступу співробітників до документів, що містять комерційну таємницю;

- Повноваження посадових осіб щодо доступу до документів, що містять комерційну таємницю;

- Права доступу виконавця до документів та інформації, що містять комерційну таємницю;

- Процедури надання документів, що містять комерційну таємницю;

- Процедури отримання секретної інформації;

- Процедури отримання виконавцем документів про ділові операції;

- Процедури копіювання та розповсюдження документів, що становлять комерційну таємницю, зовнішнім організаціям;

- Процедури отримання документів, що містять комерційну таємницю, від розкритого персоналу;

- Процедури участі в нарадах та семінарах, на яких обговорюються питання комерційної таємниці банків.

Визначення достовірності інформації, що становить комерційну таємницю, має вирішальне значення, оскільки допомагає зменшити витрати на її захист.

Таким чином, з вищезазначеного можна зробити такі висновки:

Банківська інформація – це інформація, що міститься в банківських документах або розголошується банківськими установами відповідно до процедур, передбачених чинним законодавством України, що стосуються їхньої банківської діяльності.

За способом доступу банківську інформацію можна розділити на загальнодоступну банківську інформацію та банківську інформацію з обмеженим доступом. Канали публічного розкриття банківської інформації можна розділити на інформацію, яку банки мають намір розкрити, та інформацію, яку банки зобов'язані розкрити. Канали поширення та витоку інформації.

1.3 Банківська безпека

Стратегія інформаційної безпеки банку включає: розуміння всіх інформаційних потоків; розуміння інформаційної структури в системі; визначення критичних процесів (технічний захист) та зон інформаційної системи; категоризацію користувачів на різні групи та чітке визначення їхніх дозволів; а також можливість реєструвати події несанкціонованого доступу або атаки.

Оскільки основним каналом несанкціонованого доступу є комп'ютерні мережі (банківські мережі, корпоративні мережі, глобальні мережі), основна увага приділяється безпеці рівнів підтримки мережі (маршрутизатори, брандмауери, FTP, електронна пошта, мережеві файлові системи, браузери тощо).

Слабкою ланкою мережевої інфраструктури є незахищені канали зв'язку, що може призвести до неіснуючих платежів, перехоплення платіжних даних та несанкціонованого використання, а також до інших шахрайств та зловживань. Такі інциденти є поширеним явищем в Інтернеті. Існує два рішення для захисту передачі інформації: ізоляція платіжних мереж (тобто використання виділених мереж) та шифрування даних.

Сучасні криптографічні системи базуються на таких принципах:

- Діапазон можливих значень ключів шифрування повинен бути достатньо великим, щоб звичайний пошук з використанням сучасних обчислювальних технологій був неефективним (потенційно займав місяці або навіть роки; іншими словами, швидке розшифрування вимагає необмежених обчислювальних ресурсів);

- Вартість ресурсів для розшифрування даних без знання ключа не повинна бути меншою за вартість самих даних;

- Секретний алгоритм шифрування (розшифрування) та ключ шифрування;

- Навіть незначні зміни в даних (перед шифруванням) або в самому ключі шифрування повинні призвести до значної зміни зашифрованого файлу даних (тому шаблони повинні бути нерозпізнаваними під час шифрування).

Відповідно до загальних принципів теорії інформації, чим менша надлишковість (ентропія) зашифрованих даних, тим коротша довжина ключа, і навпаки. Тому шифрування та попереднє архівування даних є особливо необхідними.

Алгоритми шифрування поділяються на:

- Практичну криптографію, яка трактує дані як набір бітів та ігнорує їх лексичну структуру;

- Спеціальне кодування, яке враховує лексичну структуру даних (фактично посилання на текст), таке як виділення слів, фраз тощо.

У системах електронної комерції всі транзакції (такі як платежі) є дуже короткими та структурно простими; структура цього типу даних (таких як

атрибути платежу, банківські рахунки тощо) легко очевидна. Тому лаконічну та прозору інформацію легше інтерпретувати. Однак, упаковка цих транзакцій може легко не помітити природну «структуру» даних. Це поширене явище в клієнт-серверних архітектурах, які використовують віддалений доступ до бази даних. Майже всі бази даних компанії є реляційними. Результатом реляційного запиту (на основі SQL-запитів, що є поширеним явищем на практиці) залишається відношення (таблиця), тобто добре структуровані дані. Гарна система шифрування повинна враховувати цю характеристику.

Методи шифрування в основному поділяються на дві категорії.

Програми симетричного шифрування базуються на принципі, що відправник (шифрувальник) і одержувач (дешифрувальник) використовують один і той самий ключ. Очевидно, що використання одного й того ж ключа протягом тривалого часу збільшує ризик неправильної ідентифікації ключа; тому ключі необхідно періодично змінювати. Сама заміна ключа є проблематичною, коли новий ключ потрібно передати віддаленій системі або особі, оскільки це значна операція. Методи симетричного шифрування найчастіше використовуються для шифрування файлових систем і менш підходять для таких систем, як електронна пошта. Урядові та військові установи зазвичай використовують лише симетричні методи шифрування.

Деякі методи симетричного шифрування поділяють ключ на дві частини, кожна з яких не може розшифрувати дані. Це загалом підвищує надійність конфіденційності ключа. Типові алгоритми симетричного шифрування включають: DES, Triple DES, IDEA, B-Crypt, Lucifer, Skpjack, FEAL-1, RC2 та RC4.

Асиметричне шифрування або (стандартні) програми шифрування, що використовують відкритий ключ (спільний ключ), використовуються наступним чином:

- Одержувач має два несумісні ключі: відкритий ключ і закритий ключ. Відкриті ключі можуть вільно поширюватися (навіть публічно публікуватися на веб-сайтах);

- Відправник використовує відкритий ключ для шифрування даних; закритий ключ відомий лише системі шифрування;

- Одержувач розшифровує отримані дані, а потім шифрує їх за допомогою закритого ключа.

Асиметричні алгоритми шифрування можуть заощадити великим банкам та підприємствам значні витрати на служби безпеки (до мільйонів доларів). Симетричне шифрування використовує відносно короткі ключі, тоді як асиметричне шифрування використовує довші ключі. Тому симетричне шифрування набагато швидше (приблизно в 1000 разів швидше). На практиці також часто використовуються гібридні методи шифрування.

Шифрування файлів також використовується для перевірки того, що автор не змінював і не створював файл. Цей метод називається цифровими підписами. Цифрові підписи можна використовувати як для зашифрованих, так і для відкритих текстових повідомлень. Цифровий підпис повинен гарантувати: особу автора, тобто його не можна підробити або використати повторно; і що «підписаний» документ не можна змінити.

Асиметричні алгоритми шифрування зазвичай вважаються такими, що мають вищу надійність і безпеку. Шифрування з відкритим ключем є найпоширенішим. Розшифрування використовує закритий ключ. Кількість комбінацій, які можна використовувати для розшифрування інформації, зашифрованої відкритим ключем, залежить від бітової довжини ключа. Використання довших послідовностей ключів може витримувати високу продуктивність сучасних комп'ютерів та забезпечувати надійний захист критичної інформації. Донедавна в інформаційній безпеці в Інтернеті найчастіше використовувалися 40-бітні ключі. Однак ці ключі легко виявляються (варто зазначити, що використання таких ненадійних інструментів пов'язане з дуже суворими обмеженнями США на експорт високопродуктивних інструментів шифрування). Наразі в Інтернеті широко використовуються 1024-бітні та навіть довші ключі. Це робить їх практично невпізнанними.

Найважливішим завданням платіжних систем є ідентифікація учасників платежів (автентифікація). Це робиться для обмеження доступу до платіжних інструментів, гарантуючи, що доступ мають лише їхні власники, а сповіщення отримує лише призначений одержувач платіжної транзакції. Довірена автентифікація також допомагає зміцнити взаємну довіру між учасниками електронної комерції. Наразі в Інтернеті використовуються різні методи автентифікації, включаючи персональні ідентифікаційні номери (PIN-коди), які користувачі повинні вводити перед проведенням фінансових транзакцій. Однак через коротку довжину цих кодів шахраї можуть легко обійти ці захисти.

Для захисту користувачів використання довших і складніших комп'ютерних паролів є ефективнішим, оскільки їх важче вгадати. Цей метод широко використовується в Інтернеті, оскільки він використовує паролі для контролю доступу до локальних систем, але надійні результати досягаються лише за умови правильного використання.

Технологія цифрових сертифікатів використовується для ідентифікації користувачів, коли вони отримують доступ до даних у різних мережах. У програмах електронної комерції користувачі реєструють свої цифрові сертифікати у банках-емітентах своїх карток. Щоразу, коли користувач намагається здійснити транзакцію, браузер, що використовує протокол безпечних електронних транзакцій (SET), надсилає копію сертифіката продавцю для перевірки дійсності кредитної картки користувача.

SET – це програмний та технологічний протокол, розроблений Visa та MasterCard. Цей протокол підтримується такими компаніями, як Verisign, Cybercash та First Virtual, які керують обліковими даними користувачів у продавців та банках. SET – це основний протокол безпеки для використання банківських карток у Всесвітній мережі, але це лише специфікація, а не повний продукт безпеки.

Ще одним важливим елементом безпеки є технологія шифрування. Заснована на комбінації відкритих та закритих ключів, вона кодує та декодує дані за допомогою цих ключів, коли відправник (користувач) передає (отримує)

дані. Алгоритми шифрування застосовуються до смарт-карт, кредитних карток із кодами, закодованими процесором, або випадково згенерованими кодами тощо.

Спеціально розроблено для користувачів.

Протягом тривалого часу відсутність протоколу для забезпечення безпеки платежів банківськими картками була головною перешкодою для розвитку електронної комерції. Лише влітку 1997 року довгоочікуваний протокол нарешті було узгоджено.

До цього були розроблені різні методи захисту фінансової інформації, більш-менш універсальні. Фактичним стандартом був протокол SSL (Secure Sockets Layer), який забезпечує шифрування на канальному рівні на основі алгоритму RSA та сумісний з основними браузерами. Також часто використовувалися такі протоколи, як S/MIME та S-HTTP. Однак усі вони мали одну спільну рису: вони не могли ідентифікувати особи покупця та продавця.

Через відсутність єдиного стандарту з'явилося багато закритих, власницьких протоколів шифрування для фінансових транзакцій з різним ступенем стабільності. Жоден з цих протоколів не відповідав ключовій вимозі, унікальній для Інтернету: відкритості. Ця ситуація змінилася з появою протоколу SET. Він дозволив здійснювати безпечні платежі за допомогою банківських карток через відкриті мережі. Розробка протоколу SET розпочалася в 1996 році, а специфікація його останньої версії, SET 1.0, була випущена в червні 1997 року. Сьогодні десятки систем електронної комерції по всьому світу працюють на базі протоколу SET, що з'єднує сотні банків, магазинів та процесингових центрів.

Протокол SET є провідним протоколом інформаційної безпеки. Він підтримує більшість платіжних систем (VISA, EuroCard, MasterCard, American Express, Diners Club, JCB, Cyber Cash та Digi Cash) та основні IT-групи (AT&T, HP, IBM, Microsoft, Northern Telekom, RSA), заслуживши таким чином довіру мільйонів клієнтів.

Протокол забезпечує такі функції:

- Забезпечує конфіденційність переданої та отриманої інформації, використовуючи одночасно кілька алгоритмів шифрування та систем цифрових сертифікатів. Цифрові сертифікати видаються спеціалізованими органами (центрами сертифікації) покупцям, продавцям та фінансовим установам фізичних осіб або компаній;

- Гарантує цілісність переданої інформації;

- Взаємну автентифікацію між покупцями та продавцями. Покупці можуть бути впевнені в особі продавця та мають право приймати платежі зі своїх банківських карток. Продавці мають можливість перевірити, чи є власник картки законним власником рахунку, пов'язаного з платіжною карткою;

- Висока сумісність, що дозволяє комбінувати продукти SET від різних виробників та працювати на будь-якій апаратній та програмній платформі;

- Надійність обміну даними не залежить від механізмів безпеки, що використовуються в каналі зв'язку.

Цей стандарт визначає отримання та формат цифрових сертифікатів, повідомлень про замовлення та авторизацію, порядок обміну повідомленнями та використання алгоритмів шифрування. Інші деталі реалізації залежать від конкретних розробників програми. Важливо зазначити, що протокол SET дозволяє використовувати різні методи шифрування інформації, які визначені регіональними стандартами та відповідають вимогам протоколу.

Електронні підписи є високоефективним засобом захисту. Використання електронного підпису вимагає перевірки того, що підписувач володіє відкритим ключем, що відповідає закритому ключу (підпису), який використовує відправник електронного документа. Однак отримання зазначеного відкритого ключа не повністю виключає можливість шахрайства; шахраї можуть надсилати підроблені відкриті ключі для перевірки неправдивої інформації. Щоб уникнути цього, поширеною практикою є автентифікація (верифікація) відкритого ключа уповноваженою та довіреною установою або організацією. Ця установа або організація називається Центром сертифікації (ЦС), і вона використовує свій електронний підпис на відкритому ключі, наданому

користувачам платіжної системи. Відкритий ключ ЦС має бути наданий через надійний та безпечний канал. ЦС автентифікує свій відкритий ключ лише після перевірки особи учасників системи через безпечний канал або інші процедури, що гарантують достатній рівень безпеки, і лише автентифіковані відкриті ключі вважаються дійсними.

Заходи захисту банківської інформації в SEP (План об'єкта безпеки) включають низку заходів, пов'язаних із шифруванням інформації, що циркулює в платіжній системі. Усі документи SEP повинні бути зашифровані: включаючи початкові документи та платіжні документи, документи про квитанції, звітні документи, лімітні документи, пов'язані з рахунками виписки та офіційні інформаційні документи.

Усі платіжні документи SEP обробляються за допомогою апаратних та програмних систем захисту інформації перед тим, як залишити банк, щоб забезпечити дотримання наступних вимог інформаційної безпеки:

- Передана інформація має бути закритою, тобто лише одержувач може прочитати інформацію;

- Цілісність: Випадкове або навмисне пошкодження інформації під час передачі має бути виявлено під час отримання;

- Автентичність відправника (відправника можна чітко ідентифікувати після отримання інформації).

На додаток до вищезазначених основних вимог, вживаються деякі додаткові заходи для більш детального аналізу потенційних аномалій:

- Захист інформації досягається за допомогою зашифрованого журналу арбітражу, який використовується для зберігання записів обробки інформації та вмісту оброблених документів;

- Зашифрована інформація включає поля дати та часу обробки.

Найважливішим заходом захисту інформації для SEP є апаратне забезпечення. Конфіденційність ключів, що містяться в ньому, технічно гарантована:

- Ключі зберігаються на спеціальній електронній картці та можуть бути прочитані лише спеціалізованим модулем, який виконує процес шифрування інформації. Зчитати ключ будь-яким іншим способом неможливо;

- Електронна картка видається банком і встановлює тимчасовий зв'язок з певним модулем шифрування цього банку; втрачену або вкрадену картку не можна використовувати на інших модулях шифрування (наприклад, на комп'ютері іншого банку);

- Якщо і пристрій, і картку вкрадено в межах певного банку, пристрій буде вимкнено. Зі списку користувачів SEP; після вирішення юридичних та фінансових питань, пов'язаних із втраченим обладнанням та отриманням нової системи, банки можуть продовжувати використовувати SEP.

З точки зору безпеки, найслабшою ланкою є зона підготовки платежів для банківських працівників, залучених до SEP. Усі більш-менш успішні спроби NSD були ініційовані представниками банків, що призводило до крадіжки коштів, а не державних банків чи інших банків. У всіх цих випадках одержувачі NSD мали легітимний доступ до системи захисту та обробки платіжної інформації, і їхні повноваження були перевизначені (доступ до багатьох або навіть усіх ресурсів банку).

Апаратні та програмні засоби, що використовуються в SEP для захисту зашифрованої інформації, автентифікують одержувачів та відправників міжбанківських електронних бухгалтерських документів та офіційних повідомлень SEP, забезпечуючи їхню автентичність та цілісність, запобігаючи підробці або втручанню в зашифровані форми чи документи з електронними підписами.

Захист зашифрованої інформації повинен охоплювати всі етапи обробки електронних банківських документів, від створення документа до зберігання в архівах банку. Використання різних алгоритмів шифрування на різних етапах обробки електронних банківських документів забезпечує безперервний захист інформації в інформаційній мережі та дозволяє здійснювати незалежну обробку інформації для різних комп'ютерних завдань національного банку.

Основною метою захисту зашифрованої інформації є захист конфіденційності та цілісності інформації електронного банку, а також ретельна автентифікація учасників SEP та банківських фахівців, що беруть участь у створенні та обробці електронних банківських документів.

Для забезпечення ретельної автентифікації банківських установ, які мають доступ до інформаційної мережі, ми розробили систему ідентифікації користувачів, яка є основою системи розподілу зашифрованих ключів.

З точки зору захисту інформації, кожна банківська установа має трибайтовий ідентифікатор, перший символ якого – це літера, що представляє відповідний регіон.

Розташування банківської установи; другий та третій символи є унікальними ідентифікаторами для банківських установ у цьому регіоні. Ці ідентифікатори відповідають адресам у системі ЕР та є унікальними в межах банківської системи України.

Трибайтовий ідентифікатор є основою для ідентифікації посад у банківській установі та є ключовим ідентифікатором для всіх посад в установі. Ключовий ідентифікатор посади складається з шести цифр, де перші три – це ідентифікатор банку, четверта – тип посади (наприклад, оператор, бухгалтер тощо), а п’ята та шоста – ідентифікатори, характерні для посади (наприклад, співробітник, який обробляє платіжну інформацію для цієї посади). Трибайтовий ідентифікатор банку вбудований у програму генерації ключів і не може бути змінений внутрішньо банком, що запобігає підробці ключів іншими банками.

Відповідний ключовий ідентифікатор записується на електронній картці, яка є носієм апаратно зашифрованої ключової інформації.

Щоб забезпечити захист інформації від несанкціонованого доступу, сувору автентифікацію та безперервний захист з дати створення платіжної інформації, система захисту SEP та інші інформаційні завдання включають механізм навчання/верифікації EDS на основі асиметричного алгоритму RSA.

Для забезпечення роботи цього алгоритму кожна банківська установа отримує від відділу захисту інформації місцевої влади спеціалізований генератор ключів із вбудованим у нього власним ідентифікатором. Банки можуть використовувати цей генератор ключів для генерації ключів для всіх робочих станцій, що обробляють документи електронного банкінгу. Щоб забезпечити захист ключової інформації (тобто відкритого ключа) від підробки та несанкціонованого доступу, відкритий ключ EDS має бути надісланий до Департаменту захисту інформації Національного банку для автентифікації (за винятком робочих ключів оператора та інших ключів, що використовуються лише в SAB).

Технічна конструкція системи накладання/верифікації EDS у SEP гарантує, що жодна посадова особа не може надсилати розрахункові документи електронного банкінгу. Коли розрахунковий документ електронного банкінгу створюється на робочому місці оператора, посадова особа, яка створює документ, повинна додати до документа електронний код безпеки даних (EDS), що містить її закритий ключ. Коли на бухгалтерському робочому місці створюється документ, що містить бухгалтерські документи електронного банку, до цього документа також додається ЕЦП, щоб запобігти підробці всього документа. Платіжні документи, сформовані таким чином, обробляються робочими місцями Національного банку України (НБУ). Одночасно в кожному розрахунковому документі електронного банку перевіряється ЕЦП оператора та додається до ЕЦП НБУ, який можуть перевірити всі банки-учасники СЕП. Під час обробки платіжних файлів на робочому місці НБУ система перевіряє підпис усього файлу та після створення відповідного платіжного файлу застосовує ЕЦП до всього файлу, використовуючи закритий ключ файлу НБУ.

Під час генерації ключів закритий ключ записується на дискету або карту пам'яті. Відкритий ключ, який використовується банком (наприклад, ключ оператора), записується як файл змін у таблиці відкритих ключів до призначеного каталогу. Відкриті ключі ARM, електронні підписи яких були перевірені в SEP (Самовдосконаленій системі електронних платежів), а саме

відкриті ключі ARM-3 та ARM лічильника, записуються як документи-підтвердження до призначеного каталогу. Ці документи подаються до Департаменту захисту інформації Національного банку України (НБУ) для автентифікації, щоб переконатися, що вони належать користувачеві SEP, не створені кимось іншим від його імені та відповідають усім вимогам відкритого ключа алгоритму SEP перед розповсюдженням через SEP. Після успішної автентифікації відкритий ключ учасника SEP надсилається на робочу станцію як файл змін у таблиці відкритих ключів на основі технологій перевірки електронних підписів (ARM-3 та ARM-2).

Нормативна база та нормативні документи Національного банку України (НБУ) повинні створювати правове середовище для захисту електронних міжбанківських розрахунків, чітко визначаючи права та обов'язки юридичних та фізичних осіб, відповідальних за операції в системі, права та обов'язки учасників системи, гарантії транзакцій та конфіденційність інформації, що циркулює в системі. Нормативні документи та статут НБУ приділяють особливу увагу врегулюванню спорів та процедурам арбітражних справ між учасниками системи електронних міжбанківських розрахунків, а також описують зобов'язання учасників системи щодо зберігання та оперативного надання арбітражної інформації. Ця арбітражна інформація генерується під криптографічним захистом програмного комплексу системи та зберігається в зашифрованому вигляді. [11]

Нормативні документи НБУ встановлюють низку управлінських заходів, спрямованих на забезпечення безпеки підготовки, передачі, обробки та зберігання електронної інформації про фінансові операції для кожного учасника системи; та встановлюють правила доступу та фізичного захисту вузлів збору, обробки та зберігання даних. Нормативні документи НБУ також регулюють генерацію, передачу, розповсюдження, оновлення та використання ключів шифрування в системі. Спеціальні директиви Національного банку України (НБУ) суворо регламентують процедури роботи банківських фахівців

щодо захисту, використання та зберігання ключів шифрування, а також розподіл повноважень щодо захисту інформації в банківських установах.

На основних вузлах збору, обробки та зберігання інформації системи (центральний розрахунковий центр, регіональний розрахунковий центр тощо) повинні вживатися заходи щодо запобігання витоку інформації через технічні канали. У всіх місцях розташування серверів системи, включаючи телекомунікаційні споруди, повинні дотримуватися певних організаційних та технічних заходів, а також встановлюватися відповідні процедури перевірки для контролю витоку інформації через технічні канали (лінії електропередач, заземлення, допоміжне технічне обладнання, електромагнітне випромінювання комп'ютерів).Електронні платежі підлягають постійному моніторингу. Банки, що беруть участь у Системі безпечних електронних платежів (СЕП), повинні дотримуватися конкретних інституційних умов, передбачених у «Положенні про обробку міжбанківських платежів в Україні», які є обов’язковими для всіх банківських установ, у місцях, де обробляються, застосовуються та зберігаються засоби безпеки. Весь персонал, задіяний у електронних платежах, повинен суворо дотримуватися цих вимог. Керівники банківських установ несуть відповідальність за забезпечення дотримання цих вимог.

1.4 Канали поширення і витоку інформації

Витік інформації стосується несанкціонованого поширення інформації поза межами довірених осіб або організацій, які зберігають цю інформацію. Витік стосується несанкціонованого отримання інформації від третьої сторони, незалежно від того, як дані були отримані.

Витік інформації може статися через випадкове розголошення даних або навмисне викрадення прихованої інформації зловмисником.

Термінологічно необхідно розрізняти витік інформації та перехоплення. Перехоплення стосується несанкціонованого отримання інформації за допомогою технічних засобів. Витік інформації стосується втрати інформації

внаслідок її поширення через канали зв'язку та фізичний простір з різних причин, включаючи перехоплення та перенаправлення. Навмисне спричинення витоку інформації через технічні канали передбачає встановлення різних пристроїв для перехоплення шляху інформації.

Цей термін частіше використовується у професійних сферах; на практиці визначення застосовується до всіх видів витоків, заснованих на людських та технічних факторах. Найпоширенішим методом викрадення є несанкціонований запис юридично захищеної конфіденційної інформації на зовнішні носії та її видалення з корпоративного середовища. Сучасні системи запобігання втратам даних (DLP) в першу чергу налаштовані на вирішення внутрішніх загроз корпоративним користувачам, а не зовнішніх атак.

Прикладом цього є справа позову Google проти Uber. Uber найняв колишнього співробітника Google, керівник якого незаконно скопіював майже всі дані, пов'язані з безпілотними автомобілями, розробкою яких він керував. Системи безпеки однієї з найбільших компаній світу не змогли запобігти крадіжці інформації керівником. Крім того, оскільки, очевидно, між компанією та співробітником не було угоди про встановлення механізму компенсації, можливість звернення до суду за спричиненими збитками була вкрай неясною. Uber було обрано відповідачем і став бенефіціаром крадіжки. Хоча документи могли бути повернуті, інформація, що міститься в них, могла бути використана для отримання конкурентної переваги.

Цей випадок демонструє, що ризик втрати даних однаковий для всіх, незалежно від розміру компанії.

Найпоширеніші причини витоків даних такі:

- Недостатній захист даних інших осіб організаціями або довіреним персоналом;

- Неправильна експлуатація пристроїв, що зберігають інформацію (з технічних причин).

Все це відбувається за умов, які легко призводять до витоків інформації:

- Недостатня кількість персоналу з питань захисту даних, недостатня обізнаність про важливість процесів та поширена недбалість у обробці інформації;

- Використання неавторизованих інструментів або несертифікованих процедур для захисту клієнтів та збереження їхньої конфіденційності;

- Недостатній нагляд за інструментами захисту інформації;

- Часта плинність персоналу, відповідального за захист персональних даних.

У витоках інформації часто звинувачують співробітників компанії та їхніх керівників. Якщо ваші співробітники добре підготовлені та обізнані, вони можуть захистити себе від будь-якого зловмисника. Деякі фактори знаходяться поза контролем компанії:

- Великі катастрофи;

- Стихійні лиха;

- Технічні аварії на об'єкті, відмови обладнання;

- Суворі погодні умови.

Системи зв'язку є основою для передачі різних типів інформації. Найпростіша система складається з носія інформації, приймача інформації та каналу передачі. Кожен сигнал може передаватися такими способами:

- Світлом;

- Електромагнітною передачею;

- Звуковими хвилями;

Основним завданням усього ланцюга обладнання є передача інформації без втрат до визначеної точки. Кілька пристроїв, що використовуються для передачі інформації, називаються системою зв'язку, а частина, яка передає інформацію, називається каналом передачі даних.

Кожен канал передачі інформації має такі атрибути:

- Початкова та кінцева точки;

- Формат передачі інформації;

- Склад або структура каналу;

- Швидкість, обсяг надісланих та отриманих даних;

- Тип каналу та метод передачі (метод перетворення сигналу);

- Характеристики схеми;

- Пропускна здатність каналу. Ці системи та канали спеціально розроблені для передачі інформації. Однак іноді ці канали можуть з'являтися в інших місцях і не мають чіткого визначення, звідси й термін «канали витоку інформації». Канали існують незалежно від джерела інформації чи методу передачі.

Технічні засоби витоку інформації можна загалом розділити на чотири типи:

- Візуальний витік: перехоплення або копіювання інформації у візуальній формі, такої як документи чи інформація, що відображається на моніторі комп'ютера;

- Підслуховування: прослуховування розмов або телефонних дзвінків у кімнаті;

- Електромагнітний витік: отримання даних, представлених у вигляді електромагнітного випромінювання, яке можна декодувати для отримання потрібної інформації;

- Аналіз матеріалів, таких як предмети, документи та відходи, що утворюються під час діяльності компанії.

Незалежно від існування технічних каналів витоку, конкуренти використовуватимуть найсучасніші методи збору та обробки інформації. Тільки розуміючи існування цих каналів, можна ефективно зменшити ризики. Щоб повністю усунути загрозу, необхідно звернутися до експертів, які можуть визначити найцінніші набори даних, що можуть стати цілями атаки; вони забезпечать комплексні заходи захисту.

Візуальні оптичні носії. Якщо вікно офісу дозволяє бачити екран монітора або документи на столі, існує ризик витоку інформації. Будь-яке світло, що виходить від джерела інформації, потенційно може бути

перехоплене. Для вирішення цієї ситуації в більшості випадків потрібні лише прості технічні заходи:

- Зменшення відбивної здатності та яскравості об'єкта;

- Встановлення різних бар'єрів та покриттів;

- Використання відбивного скла;

- Відрегулюйте положення об'єктів таким чином, щоб їхнє світло не потрапляло в зону можливого перехоплення.

Однак існує більш поширений ризик витоку інформації: наприклад, винесення документів з кімнати для фотографування, створення інших форм копіювання, створення скріншотів баз даних, що містять важливу інформацію, тощо. Основні заходи щодо вирішення цих ризиків обмежуються адміністративним та організаційним рівнями, хоча деякі програмні засоби можуть перешкоджати перегляду даних, що відображаються на екранах.

Акустичні канали. Інформація у вигляді звуку легше перехоплюється та просочується. Звук надвисокої частоти (понад 20 000 Гц) поширюється дуже швидко. Якщо на шляху звукових хвиль є перешкода, це призведе до вібрації перешкоди, і ці коливання можна виявити за допомогою спеціального обладнання. Якщо архітектори врахували цю акустичну характеристику під час проектування інтер'єру, то це слід врахувати на етапі планування будівлі чи офісу, щоб гарантувати, що інформація не буде втрачена. Якщо цей метод неможливий, то в дизайні приміщення необхідно використовувати технічні засоби, використовуючи звукопоглинальні матеріали, такі як пориста штукатурка. Для оцінки рівня безпеки використовується стетоскоп.

Якщо максимального звукопоглинання неможливо досягти, можна використовувати генератори шуму, встановлені навколо стін у головній будівлі, які не обладнані засобами захисту слуху, або в кімнатах для переговорів.

Використання записуючих пристроїв під час переговорів також може призвести до витоку акустичної інформації. Для виявлення наявності таких пристроїв потрібне спеціалізоване обладнання. У наш час встановлення підслуховуючих пристроїв у телефонах використовується рідко; цифровий

зв'язок зазвичай перехоплюється іншими засобами, наприклад, через телефонних операторів або інтернет-провайдерів. Цей ризик необхідно враховувати; наприклад, для обговорень, що проводяться по телефону, можуть бути розроблені спеціальні рекомендації щодо обробки конфіденційної інформації.

Електромагнітні та комунікаційні канали. Перехоплення інформації, що міститься в електромагнітних перешкодах, також дуже небезпечне. Електромагнітні хвилі, які поширюються на короткі відстані в електромагнітних полях, також можуть бути перехоплені. Ці перешкоди можуть виникати з:

- Телефонних та раційних мікрофонів;
- Головних заземлювальних та силових кіл;
- Аналогових телефонних ліній;
- Оптоволоконних каналів зв'язку;
- З інших джерел.

Перехоплення та декодування цих даних за допомогою сучасних технологій не є складним.

Існуючі технології дозволяють вбудовані пристрої PEMVN безпосередньо підключати до схем або встановлювати їх у монітори чи корпуси комп'ютерів, при цьому вони можуть перехоплювати дані через внутрішні з'єднання друкованої плати. Методи передачі:

- Відображення на екрані монітора;
- Введення через клавіатуру;
- Виведення на периферійні пристрої (принтер) через кабель;
- Запис на жорсткий диск та інші пристрої.

У цьому контексті контрзаходи включають заземлення кабелів, екранування найочевидніших джерел електромагнітного випромінювання, ідентифікаційне маркування або використання спеціалізованого обладнання та програмного забезпечення для ідентифікаційного маркування. Однак інформація, що передається через Інтернет, може бути перехоплена. Боротьба з

крадіжками може бути досягнута за допомогою поєднання апаратних та програмних підходів.

Фізичні та матеріальні канали. Звичайне сміття або промислові відходи можуть стати цінними джерелами даних. Хімічний аналіз відходів, що залишають контрольовані зони, може бути значним джерелом інформації про склад продукту або виробничі процеси. Розробка систем для вирішення цього ризику вимагає комплексного рішення, що включає застосування технологій управління відходами.

Усі вищезгадані методи витоку інформації (за винятком фізичних та матеріальних каналів) вимагають від злодіїв можливості підійти до джерела інформації, тоді як ефективна дальність традиційних пристроїв перехоплення аудіо- або відеоінформації зазвичай обмежена кількома десятками метрів. Встановлення інтегрованих пристроїв для захоплення електромагнітного випромінювання та акустичних коливань вимагає безпосереднього проникнення до цільового об'єкта. Крім того, потрібні знання проектування, а також може знадобитися найм персоналу. Хоча більшість об'єктів оснащені камерами відеоспостереження, ці методи наразі використовуються лише в дуже обмеженій кількості випадків.

Найбільшу загрозу становлять сучасні методи крадіжки, які використовують можливості Інтернету для отримання документів, даних або голосового трафіку.

1.5 Засоби запобігання витоку інформації

Отже, комплексна система запобігання витоку конфіденційної інформації повинна базуватися на таких принципах:

- Безперервність системи в просторі та часі. Використані методи захисту повинні цілодобово контролювати всі матеріали та інформацію, щоб запобігти будь-яким порушенням або зниженню рівнів контролю;

- Багатозонний захист. Інформацію слід класифікувати за важливістю та захищати за допомогою різних методів;

- Пріоритезація. Не вся інформація однаково важлива; тому найціннішу інформацію слід захищати найсуворішими заходами;

- Інтеграція. Усі компоненти системи повинні співпрацювати та контролюватися з однієї центральної точки. Якщо компанія є холдинговою компанією або має кілька філій, необхідне управління інформаційними системами материнської компанії;

- Резервне копіювання. Усі критичні комунікаційні модулі та системи повинні мати резервні копії, щоб резервне з'єднання можна було негайно використовувати для заміни втраченого або пошкодженого з'єднання.

Малому бізнесу не завжди потрібно створювати систему такого рівня, але це критично важливо для великих компаній, особливо тих, які працюють з державними клієнтами.

Відповідальність за дотримання вимог має нести керівник компанії та один з його заступників, відповідальний за служби безпеки. Майже 70% загальної інформаційної безпеки залежить від адміністративних та технічних заходів, оскільки підкуп посадових осіб набагато поширеніший, ніж спеціалізовані технічні засоби в промисловому шпигунстві.

Викрадення інформації вимагає вузькоспеціалізованих навичок та передбачає її надання третім особам без прямого конкурентного зв'язку.

Усі організаційні положення щодо захисту комерційної таємниці та іншої інформації повинні відповідати суворішим вимогам, ніж документація, необхідна для подання заявок на отримання ліцензії. Це пов'язано не лише з тим, що ці документи є найскладнішими, але й з тим, що високоякісна документація допомагає компаніям вирішувати майбутні суперечки, що виникають внаслідок порушень інформації.

Персонал є найслабшою ланкою в будь-якій системі захисту даних. Тому під час обробки такої інформації необхідно бути надзвичайно обережним. Для компаній, що займаються державною таємницею, створено системи авторизації.

Інші організації повинні вживати численні заходи для забезпечення обмеженого доступу до конфіденційних даних. Перелік інформації, що становить комерційну таємницю, має бути складений та доданий до трудових договорів. Під час обробки інформації в базах даних слід створити відповідні системи контролю доступу.

Потрібно обмежити всі дозволи на копіювання та доступ до зовнішніх електронних листів. Усі співробітники повинні бути ознайомлені з інструкціями щодо роботи з інформацією, що містить комерційну таємницю, та письмово підтверджувати їх у своїх журналах. Це дозволяє за необхідності нести відповідальність.

Існуючі політики доступу до об'єктів повинні включати не лише захист усіх даних відвідувачів, але й гарантувати, що співпраця здійснюється лише з охоронними компаніями, які відповідають усім вимогам безпеки. Якщо співробітники приватних охоронних компаній чергують на об'єкті вночі, і вони залишають паролі на своїх столах для зручності системних адміністраторів, ризик не менший, ніж від професійної хакерської атаки або закладок, встановлених у серверній кімнаті.

Часто винуватцями інформаційних порушень є не відвідувачі, а співробітники компанії. До цих співробітників належать багато консалтингових та бухгалтерських фірм, які надають послуги з розробки та обслуговування інформаційних систем. Помітним, але суперечливим прикладом є випадок в Україні: кільком дочірнім компаніям 1С було заборонено працювати через підозру у крадіжці співробітниками конфіденційної бухгалтерської інформації. Такий самий ризик існує і з широко використовуваними хмарними CRM-системами, оскільки вони надають послуги хмарного зберігання даних. Через надзвичайно низьку відповідальність за безпеку довіреної інформації немає гарантії, що всі бази даних дзвінків клієнтів, записані в системі, не стануть одразу мішенями для конкурентів під час інтеграції з системами IP-телефонії. Цей ризик слід класифікувати як дуже серйозний. Вибираючи між серверними

та хмарними рішеннями, слід надавати пріоритет першим. За даними Microsoft, кількість кібератак, спрямованих на хмарні ресурси, цього року зросла на 300%.

До всіх підрядників, які запитують передачу даних, що становлять комерційну таємницю, слід ставитися з однаковою обережністю. Усі контракти повинні містити пункти щодо відповідальності за порушення. Така інформація, як сертифікати на нерухомість, оцінки акцій, аудиторські та консалтингові дослідження, часто перепродається конкурентам.

Під час планування кімнат для переговорів або зберігання захищеної інформації необхідно дотримуватися всіх вимог захисту DSTU (Управління телекомунікаційної безпеки Нідерландів). Кімнати для переговорів повинні бути належним чином сертифіковані, використовувати всі сучасні методи екранування, звукопоглинальні матеріали та бути оснащені генераторами шуму.

Для запобігання втраті або крадіжці інформації необхідні різні апаратні та технічні заходи. Сучасні технічні засоби поділяються на три категорії:

- Машинобудування. Цей тип захисту використовується при реалізації архітектурних та планувальних схем. До них належать пристрої, що фізично запобігають несанкціонованому доступу до охоронюваних зон, системи відеоспостереження, сигналізація, електронні замки та подібні пристрої;

- Апаратне забезпечення. Це включає вимірювальні прилади, аналізатори, технічне обладнання тощо. Ці пристрої можуть допомогти вам знайти вбудовані пристрої, виявити існуючі канали витоку інформації, оцінити операційну ефективність та визначити ключові характеристики та функції пристроїв у ситуаціях, коли можливий витік інформації або ідентифікація. До цих пристроїв належать польові індикатори, високочастотне вимірювальне обладнання, пристрої нелінійного позиціонування та обладнання для тестування аналогових телефонних ліній. Детектори електромагнітного випромінювання можуть використовуватися для ідентифікації голосового введення, а детектори відеокамер працюють за тим самим принципом.

- Програмне забезпечення. Програмне забезпечення є найважливішим заходом безпеки, що запобігає вторгненню неавторизованого персоналу в інформаційні мережі, блокує хакерські атаки та запобігає перехопленню інформації. Слід звернути особливу увагу на спеціалізовані програми, які забезпечують захист системної інформації. Системи запобігання втраті даних (DLP) та управління інформацією та інцидентами безпеки (SIEM) зазвичай використовуються для побудови складних механізмів інформаційної безпеки. Запобігання втраті даних (DLP) забезпечує комплексний захист конфіденційної інформації. Сьогодні вони в основному використовуються для вирішення внутрішніх загроз — загроз, що походять від користувачів корпоративної мережі, а не від хакерів. Ці системи використовують кілька методів для виявлення точок втрати або передачі інформації та блокування будь-якого несанкціонованого доступу до даних або їх передачі шляхом автоматичної перевірки всіх каналів передачі. Вони аналізують трафік електронної пошти користувачів, вміст локальних папок та миттєві повідомлення, блокуючи будь-які виявлені спроби передачі даних.

Системи управління інформацією та подіями безпеки (SIEM) керують потоком інформації та подій у мережі. Подія – це будь-яка ситуація, яка потенційно може вплинути на мережу та її безпеку. Якщо така подія трапляється, система автоматично пропонує рішення для зменшення загрози.

Програмне забезпечення може вирішувати окремі проблеми та забезпечувати комплексний захист безпеки мережі;

- Шифрування. Такі системи забезпечують алгоритми шифрування для шифрування всієї інформації, що передається мережею або зберігається на серверах. Навіть якщо інформація втрачена, вона не приверне уваги потенційних зловмисників.

Застосування всіх методів захисту комплексно може бути не обов'язковим. Тому побудова системи захисту інформації для конкретної компанії вимагає створення власного проекту та його оптимізації на основі доступних ресурсів.

1.6. Висновки по розділу

У першій частині розглядається основна інформація про банківські системи, банківську інформацію, їхню безпеку та основні загрози.

Крім того, обговорюються канали витоку інформації та методи запобігання витоку інформації.

РОЗДІЛ 2.
РИЗИКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ ТА ЇЇ ОЦІНКА

2.1 Ризики банківської діяльності

У міжнародній банківській практиці управління ризиками є ключовою сферою фінансового менеджменту. Велике значення надається вивченню сфер ризику та основних типів ризиків, пошуку ефективних методів оцінки, контролю та моніторингу ризиків, а також встановленню відповідних систем управління.

Банківський ризик стосується можливості того, що очікувані або неочікувані події можуть негативно вплинути на капітал та/або дохід банку.

З точки зору банку, ризик стосується потенційної втрати доходу або зниження ринкової вартості капіталу банку через несприятливі зовнішні або внутрішні фактори. Такі втрати можуть бути прямими (втрата доходу або капіталу) або непрямими (обмеження здатності банку досягати своїх бізнес-цілей).

Термін «ризик» часто використовується в економічній літературі та практиці, і через складність його визначення його значення змінюється залежно від контексту. У широкому сенсі, ризик визначається як невизначеність того, як відбудеться майбутня подія.

Міра ризику – це ймовірність того, що очікувана подія не відбудеться і що це призведе до несприятливих наслідків. Як і в інших галузях, ризик банківської галузі насамперед проявляється у фінансових збитках, що виникають внаслідок реалізації конкретних ризиків. Оскільки ризику не можна і не слід повністю уникати, ним можна і потрібно свідомо керувати, враховуючи взаємозв'язок усіх видів ризиків та той факт, що їхні рівні постійно змінюються через динамічне середовище. Загалом, банківська діяльність несе вищі ризики, ніж діяльність в інших галузях. Це випливає з унікального характеру функцій, що виконуються кожним комерційним банком. Банки

мають численних партнерів, клієнтів та позичальників, фінансові умови яких безпосередньо впливають на власні умови банку. Банківські операції є дуже диверсифікованими, включаючи залучення капіталу, випуск та купівлю цінних паперів, кредитування, факторинг, лізинг та надання готівки клієнтам. Будь-яка банківська діяльність може бути пов'язана з різноманітними ризиками.

Оскільки банки займаються як активною, так і пасивною діяльністю, виникають додаткові ризики, такі як ризик дисбалансу ліквідності, ризик затримки надходжень та платежів коштів, а також ризик обмінного курсу. Це спонукає до пошуку конкретних методів пом'якшення їх наслідків, відомих як «управління активами та пасивами банку». Операційна діяльність, обов'язкове використання високотехнологічних інформаційно-комунікаційних систем, необхідність постійного моніторингу та виконання маркетингових функцій сприяють низці функціональних банківських ризиків, які можуть пом'якшити інші компанії. Зрештою, банківські системи більшості країн світу підлягають суворому національному регулюванню та спеціалізованому нагляду. Тому банки стикаються із зовнішніми ризиками у своїй діяльності, деякі з яких, такі як ризик недотримання національних правил, є особливо значними в банківській галузі.

Незважаючи на численні ризики, властиві банківським операціям, банки повинні бути гарантами надійності та безпеки. Оскільки банкіри переважно розпоряджаються чужими коштами, вони повинні прагнути пом'якшувати бізнес-ризики ретельніше, ніж інші підприємці. Тому управління ризиками вважається однією з найважливіших сфер фінансового менеджменту банків.

Економічний ризик був у центрі уваги численних публікацій та наукових досліджень, у яких запропоновано різні методи класифікації ризиків. Класифікація ризиків базується на його основних характеристиках, але різноманітність ризикових явищ надає численні шляхи вирішення цього питання, хоча навряд чи вона повністю охоплює всі ризики.

Банківські ризики поділяються на зовнішні та внутрішні. Внутрішні ризики далі поділяються на фінансові та функціональні ризики, утворюючи

цілісну систему. Комерційні банки можуть застосовувати цю систему до своїх операцій, коли виникають ризики, виходячи з характеристик власного бізнесу. Ризики різноманітні та існують у кожному аспекті бізнесу. Для банків важливо не уникати ризику, а максимально його передбачати та мінімізувати.

Зовнішні ризики – це ризики, пов'язані зі змінами у зовнішньому середовищі банку, ризики, які безпосередньо не пов'язані з його підприємницькою діяльністю. Ці ризики включають політичні, правові, соціальні та макроекономічні ризики, що виникають через такі фактори, як ескалація внутрішньої економічної кризи, політична нестабільність, війна, заборони на іноземні платежі, реструктуризація боргу, ембарго, анулювання ліцензій на імпорт, стихійні лиха (пожежі, повені, землетруси), приватизація, націоналізація та невідповідні закони та нормативні акти. Зовнішні ризики мають значний вплив на банківські операції, ними надзвичайно важко керувати, а іноді навіть неможливо контролювати. Оцінка цих ризиків переважно використовує методи логічного аналізу. Внутрішні ризики стосуються ризиків, що безпосередньо виникають з власної діяльності конкретного банку. Чим ширший спектр клієнтів, партнерів, банківських відносин, банківських операцій та обсягу послуг банку, тим з більшою кількістю внутрішніх ризиків він стикається. Порівняно із зовнішніми ризиками, внутрішні ризики легше ідентифікувати та кількісно оцінити. Завдання управління включають використання відповідних методів для постійного виявлення, оцінки, пом'якшення та моніторингу внутрішніх ризиків.

Внутрішні ризики легше ідентифікувати, ніж зовнішні.

Якісна класифікація банківських ризиків повинна ґрунтуватися на впливі як зовнішніх, так і внутрішніх факторів ризику. Цінність якісної класифікації банківських ризиків полягає в її здатності виявляти внутрішні резерви, тим самим підвищуючи ефективність управління ризиками в банківських операціях.

Внутрішні ризики можна класифікувати на фінансові та функціональні ризики залежно від сфери їх виникнення.

Фінансовий ризик становить найбільшу категорію банківських ризиків. Фінансовий ризик залежить від ймовірності валютних втрат і пов'язаний з непередбаченими змінами в розмірі, прибутковості, витратах та структурі активів і пасивів банку.

Фінансовий ризик може бути безпосередньо пов'язаний з діяльністю компанії (наприклад, вибір типів фінансових активів та терміни їх придбання (продажу), кількість придбаних (проданих) активів тощо), або може існувати об'єктивно незалежно від намірів компанії та бути спричиненим економічними змінами (наприклад, циклічний економічний розвиток, заходи урядової фіскальної та монетарної політики тощо).

Уточнення класифікацій ризиків та їх проявів допомагає визначити найнебезпечніші сфери фінансових інвестицій та розробити рекомендації щодо управління ризиками. Концепція розрахунку факторів ризику полягає в об'єктивній оцінці їх рівнів для забезпечення необхідної прибутковості операцій на фінансовому ринку та розробці системи заходів для мінімізації їх негативного фінансового впливу на учасників фінансового ринку.

У світовій фінансовій практиці зазвичай використовуються такі методи контролю та мінімізації ризиків, причому конкретна комбінація залежить від характеристик конкретного сегмента фінансового ринку:

– Фондові біржі, особливо зберігачі цінних паперів та клірингові палати, встановлюють мінімальні вимоги до професійного складу, фінансового стану та навіть репутації учасників. Звичайно, чим вища надійність кожного учасника системи, тим нижчий ризик для інших учасників; проте не всі учасники можуть відповідати цим вимогам. У цьому випадку, хоча система є високонадійною, її ефективність низька через невелику кількість учасників. Тому завданням організаторів ринкової інфраструктури є пошук прийнятного балансу між надійністю системи та масштабом;

– Біржі та клірингові палати можуть встановлювати різні ліміти на торгівлю учасників. Чим суворіші ліміти, тим нижчі міжпартнерські зобов'язання та нижчий ризик. Однак надмірно суворі ліміти можуть призвести

до зменшення обсягу торгів та стагнації ринку. Тому необхідно знайти баланс між надійністю та розміром ринку;

- Депоненти та клірингові палати впроваджують методи диверсифікації ризиків серед усіх учасників системи, зокрема використовуючи «кліринговий» та «інноваційний» підходи;

- Сторони переговорів можуть створити спеціальний резервний фонд для компенсації збитків, спричинених невиконанням або затримкою виконання окремими учасниками своїх зобов'язань за угодою. Цей фонд, як правило, управляється зберігачем та клірингової палатою.

- За допомогою зберігача та клірингової палати учасники ринку можуть створити систему розподілу збитків, спричинених невиконанням окремими учасниками своїх зобов'язань за угодою.

- Клірингова палата зберігача або сторони, що ведуть переговори через клірингову палату, можуть використовувати механізм автентифікації боржника для автентифікації боржників, які тимчасово не можуть здійснювати платежі. Кредитором може бути сам учасник або клірингова палата, і може взяти на себе борг самостійно або від імені учасника.

Щодо фінансових наслідків, то найскладніші та найнебезпечніші ризики страхуються спеціалізованими страховими компаніями через відповідні угоди. Це належить до категорії страхування для професійних учасників бізнесу. По суті, це те, що банки та страхові компанії називають комплексним страхуванням від електронних та комп'ютерних злочинів. Далі йде страхування від втрати цінностей (включаючи цінні речі).

Страхування ломбардів пов'язане з банками. Однак, подібно до кредитування під цінні папери, поширеного на українському фондовому ринку (наразі обмеженого рефінансуванням банківських операцій комерційних банків), Національний банк України (НБУ) планує в майбутньому запустити аналогічні кредитні операції під корпоративні цінні папери. Якщо Національний банк України виступатиме зберігачем (відповідальним за фізичне зберігання даних про державні облігації) під час рефінансування державних

облігацій, то під час рефінансування корпоративних цінних паперів Національний банк України та комерційні банки, що здійснюють кредитування під цінні папери, повинні будуть співпрацювати не лише зі зберігачем, але й з агентством з реєстрації цінних паперів. З практики ми дізналися, що агентства з реєстрації цінних паперів займаються незаконною діяльністю, такою як перереєстрація права власності на цінні папери з підписом неуповноважених представників під час передачі, а також втрата або пошкодження записів. Ці дії зрештою призводять до втрати застави та неможливості повернення кредитів.

Варто зазначити, що існує ще один вид страхування, такий як страхування відповідальності директорів та менеджерів, яке часто використовується установами, що виводять цінні папери на західні ринки.

В останні роки страхування комерційних ризиків стає все більш популярним. Цей вид страхування фактично включає страхування кримінальної відповідальності та страхування професійної відповідальності.

Діяльність на фінансовому ринку також вимагає спеціальних портфельних стратегій, а саме ретельного вибору фінансових інструментів, які можуть знизити ризик. Диверсифікація є одним із ефективних механізмів пом'якшення операційних ризиків на фінансових ринках. Вона може захистити інвестиції від негативного впливу коливань економічного циклу, довгострокових галузевих тенденцій та погіршення кредитоспроможності окремих компаній. Високо диверсифіковані інвестиції можуть зменшити або навіть повністю усунути всі ризики, крім системного ризику.

Фінансові ризики включають валютний ризик, кредитний ризик, інвестиційний ризик, ринковий ризик, ризик ліквідності, ризик процентної ставки, інфляційний ризик та базисний ризик.

Кредитний ризик стосується можливості фінансових втрат через невиконання позичальником своїх боргових зобов'язань. Значною складовою кредитного ризику є галузевий ризик, що виникає через невизначеність перспектив розвитку галузі позичальника. Одним із методів вимірювання галузевого ризику є системний ризик або бета-ризик. Бета-ризик відображає

ступінь волатильності або відхилення показників галузі відносно ринку або загального рівня економічного розвитку. Галузь зі значенням бета, що дорівнює 1, зазнає коливань прибутку синхронно з ринковими тенденціями. Галузі з нижчою волатильністю мають значення бета менше 1, тоді як галузі з вищою волатильністю мають значення бета більше 1. Очевидно, що чим вище значення бета, тим більший галузевий ризик. Визначення значення бета для кожної галузі вимагає довгострокової, надійної бази даних.

Під час визначення кредитного ризику необхідно враховувати географічний ризик, який далі поділяється на регіональний ризик та ризик країни, тобто місцезнаходження позичальника. Останній стосується позик, наданих іноземним позичальникам, і залежить від факторів, характерних для країни/регіону позичальника.

Виходячи з концепції кредитного ризику в комерційному банківському секторі, слід розрізняти такі терміни:

- Кредитний ризик позичальника: Можливість того, що позичальник (боржник) не зможе виконати своє зобов'язання щодо погашення боргу перед банком відповідно до умов договору (угоди);

- Кредитний ризик за кредитом: Можливість того, що банк не зможе своєчасно та достатньо використати забезпечення за кредитом для покриття потенційних збитків;

- Кредитний ризик за кредитною угодою: Можливість того, що позичальник (боржник) не зможе виконати своє зобов'язання щодо погашення боргу перед банком відповідно до угоди (контракту), а банк не зможе своєчасно та достатньо використати забезпечення за кредитом для покриття будь-яких збитків. Визначення кредитного ризику можна тлумачити з різних точок зору. По-перше, кредитний ризик можна визначити як ймовірність того, що банк зазнає збитків, коли позичальник не виконає певну кредитну угоду. По-друге, кредитний ризик можна визначити як максимальні втрати та нереалізований дохід, що виникають внаслідок нездатності позичальника повернути всю або частину основної суми боргу та/або відсотків.

Регіональний ризик стосується ризику, з яким стикаються під час ведення бізнесу в певному регіоні певної країни. Ризик, з яким стикаються під час ведення бізнесу в країні, іноді також називають країновим ризиком.

Регіональний ризик залежить від конкретних обставин певного адміністративно-географічного регіону, що характеризується умовами, що відрізняються від середніх показників по країні. Ці відмінності можуть бути пов'язані з такими факторами, як клімат, країна та політика. Правові фактори та інші регіонально специфічні фактори, що впливають на стан позичальників, є частиною кредитного ризику. Кредитний ризик існує не лише в операціях прямого кредитування, але й в лізингу, факторингу, гарантіях та формуванні портфеля.

Ризик дисбалансу ліквідності стосується можливості того, що банк може бути не в змозі вчасно виконати свої зобов'язання або втратити частину доходів через надмірно ліквідні активи. Ризик дисбалансу ліквідності можна розділити на два типи: ризик недостатньої ліквідності та ризик надмірної ліквідності. Вимірювання ризику ліквідності є дуже складним, оскільки на цей показник впливає багато факторів, більшість з яких знаходяться поза незалежним контролем банку. На практиці для контролю ліквідності зазвичай використовуються спеціалізовані показники, і ці показники здебільшого регулюються центральними банками різних країн.

Тим часом практика управління ризиком ліквідності кредитних спілок вважається недосконалою, оскільки вона не враховує ризик довгострокових дисбалансів ліквідності, які можуть суттєво вплинути на платоспроможність установи та фінансову стабільність. Тому необхідно використовувати табличний підхід для оцінки ліквідності: структуру стану ліквідності (як незалежний звіт для кредитних спілок) та матрицю фінансування мінімального ризику ліквідності.

Інфляційний ризик стосується можливості знецінення готівки в майбутньому, тобто можливості зниження купівельної спроможності. Інфляція більш-менш притаманна більшості економічних систем. Це поширене

економічне явище, і тому банки мають над ним мало контролю. Однак банки можуть використовувати високу інфляцію для підвищення прибутковості свого бізнесу. Враховуючи специфічний характер своїх операцій, банки, ймовірно, будуть серед бенефіціарів швидкої інфляції через різке збільшення грошової маси та вплив кредитного мультиплікатора на кредитування клієнтів. Однак інфляційний ризик також має негативні наслідки, проявляючись у знеціненні банківських активів та власного капіталу власників банків (тобто власного капіталу).

Інфляційний ризик стосується ризику того, що інфляція погіршить ефективність інвестицій, вартість активів або купівельну спроможність потоків доходів.

Без урахування інфляції, фінансовий результат – це номінальна дохідність. Інвестори повинні зосередитися на купівельній спроможності або реальній дохідності. Інфляція – це зниження купівельної спроможності грошей з часом, а непередбачуваний характер інфляції створює ризик того, що інвестиційна дохідність або майбутня вартість активів не виправдають очікувань.

Будь-який грошовий потік або грошовий дохід схильні до інфляційного ризику, оскільки їхня вартість безпосередньо знецінюється зі зниженням купівельної спроможності грошей. Фіксована сума кредиту плюс додатковий платіж у фіксованій сумі – типовий приклад активу, на який впливає інфляційний ризик, оскільки сума погашення може бути набагато меншою за суму кредиту. Реальні активи та акції менш чутливі до інфляційного ризику і навіть можуть отримати вигоду від непередбачуваної інфляції.

Ризик банкрутства – це можливість того, що банк, навіть якщо його швидко продати, не зможе виконати свої боргові зобов'язання. Ризик банкрутства тісно пов'язаний з ризиком ліквідності та несе інші ризики. Тому основою процесів управління банком є постійний моніторинг загального банківського ризику. Ціновий ризик відіграє значну роль у фінансовому ризику, оскільки він пов'язаний з ймовірністю зміни вартості банківських активів та

пасивів. Ціновий ризик залежить від ймовірності зміни ринкових цін фінансових активів та фізичних активів, відображених у балансі банку або на позабалансових рахунках. Фінансові інвестиції включають готівку, валюту та цінні папери; фізичні активи включають дорогоцінні метали, твори мистецтва, нафту, зерно та кольорові метали. Ці фінансові інструменти або активи можуть бути враховані на активних та пасивних рахунках банку, а також у позабалансових статтях. Тому зміни ринкових цін на ці активи призведуть до змін вартості активів, зобов'язань або позабалансової заборгованості банку. Вплив цінового ризику є найбільш значним, коли банк оцінює вартість статей балансу на основі ринкових цін на кінець кожного робочого дня. Крім того, будь-які зміни ринкових цін негайно відображаються у балансі банку. Нездатність своєчасно врахувати прибутки та збитки може спричинити подальші проблеми, оскільки незнання факторів ризику не означає, що ризик не існує. До цих видів банківських ризиків насамперед належать ризик процентної ставки, ризик обмінного курсу та ризик вартості цінних паперів.

Ризик процентної ставки стосується можливості фінансових збитків через коливання ринкових процентних ставок протягом майбутнього періоду. Позичальники, кредитори, власники цінних паперів та інвестори можуть зіткнутися з ризиком процентної ставки.

Ризик обмінного курсу стосується можливості збитків через зміни обмінного курсу однієї валюти відносно іншої. Валютний ризик існує на балансі компанії для активів, зобов'язань або позабалансових статей, деномінованих в іноземній валюті.

Акціонерний ризик стосується можливості фінансових втрат через зміни ринкових цін на цінні папери або інші торгові інструменти. З цим ризиком стикаються всі учасники біржі (інвестори, трейдери, емітенти цінних паперів).

Базисний ризик залежить від можливості структурних змін різних процентних ставок. Іншими словами, цей ризик випливає з асиметрії (порівняльної характеристики) динамічних змін різних процентних ставок, що відрізняється від процентного ризику (динамічної характеристики, пов'язаної зі

змінами рівнів процентних ставок з часом). Наприклад, якщо кредитні ставки визначаються на основі міжбанківських ринкових ставок, тоді як депозитні ставки безпосередньо не пов'язані з цими ринковими ставками, будь-яка різниця в змінах цих двох різних базових ставок може призвести до додаткових прибутків або збитків – це базисний ризик.

В управлінні ціновим ризиком банки використовують специфічні методи, які разом називають хеджуванням. Механізми хеджування використовуються для компенсації фінансових втрат, що виникають внаслідок змін ринкових цін фінансових інструментів в одній позиції, та для отримання прибутку в іншій позиції (компенсаційний прибуток). За допомогою хеджування можна значно зменшити або навіть уникнути цінового ризику.

Функціональний ризик має значний вплив на діяльність банку. Функціональні ризики виникають через відсутність у банків комплексного та своєчасного контролю над їхньою фінансово-господарською діяльністю. Ці ризики включають такі процеси, як створення та впровадження нових банківських продуктів і послуг, збір, обробка, аналіз та передача інформації, навчання персоналу та виконання інших адміністративних та комерційних операцій.

Порівняно з фінансовими ризиками, ці ризики важче ідентифікувати, кількісно оцінити та оцінити. Однак функціональні ризики не менш шкідливі, ніж інші види банківських ризиків, і зрештою призводять до фінансових втрат. Банки пом'якшують функціональні ризики шляхом удосконалення систем внутрішнього аудиту, розробки систем управління документами, удосконалення внутрішніх процесів, а також надання технічної та фінансової підтримки різним бізнес-операціям. Добре розроблена ресурсна, логістична та кадрова політика також допомагає зменшити ці ризики.

Технічні ризики (ризики системних збоїв) тісно пов'язані з використанням високотехнологічних засобів, обладнання та технологій у банківських операціях. Ці ризики виникають через помилки в комп'ютерних програмах, математичних моделях, формулах та розрахунках. Крім того, вони також

можуть виникати, якщо керівництво не отримує відповідну інформацію своєчасно або неналежним чином через дефекти в підсистемах інфраструктури, збої в мережі чи зв'язку тощо. Фінансові втрати банку виникають не лише через ці помилки та збої, але й через додаткові витрати, понесені на їх усунення. Одним із типових проявів технологічного ризику є збій електронних платіжних систем. Необхідною умовою для доступу банків до міжнародних клірингових та інформаційних систем є здатність виправляти несправності обладнання протягом певних термінів (зазвичай дві години).

Ризик зловживання стосується можливості збитків для банків через шахрайство, марнотратство, несанкціонований доступ до важливої інформації банківських співробітників або клієнтів, відмивання грошей або несанкціоновані транзакції.

Документальний ризик стосується можливості неочікуваних помилок у документах, що призводить до негативних наслідків, таких як невиконання договірних умов, судові позови або відмова від попередніх зобов'язань. Удосконалення процесів обробки документів, автоматизація процесів обробки документів та підвищення кваліфікації співробітників можуть значно зменшити цей ризик.

Транзакційний ризик супроводжує процеси укладання та реєстрації договорів, розрахунків, підписання договорів та передачі цінних паперів або валюти. Цей тип ризику тісно пов'язаний з технологічними, документальними та операційними ризиками. Типовим прикладом є те, що на взаємозалік платежів може вплинути переказ коштів у різний час. Вимога про те, щоб одна сторона завершила транзакцію раніше терміну, наражає транзакцію на ризик.

Операційний ризик залежить від ймовірності невідповідності між операційними витратами банку та його ефективністю. Процеси управління операційними ризиками в банку набагато складніші, ніж в інших сферах бізнесу. Витрати включають процентні та непроцентні витрати (комісійні та інші операційні витрати), які не завжди можна точно передбачити. Тому

керівникам банків важче, ніж іншим підприємцям, визначити вплив нефінансових витрат на чистий прибуток.

Стратегічний ризик пов'язаний з помилками у реалізації функцій стратегічного управління. Ключові проблеми включають невідповідні цілі та стратегії банку, недосконале стратегічне планування, недостатні ресурси для реалізації стратегії та неправильне застосування управління ризиками в банківській практиці. Надмірно амбітні цілі в поєднанні з недостатніми людськими або фінансовими ресурсами можуть призвести до збитків і навіть шкоди репутації банку. Типовими прикладами стратегічного ризику є надмірне інвестування в нерухомість або необґрунтовано швидке розширення мережі філій без належного дослідження ринку.

Ризик запуску нового продукту стосується можливості того, що нещодавно запущені банківські продукти, послуги, бізнеси чи технології можуть не досягти очікуваної рентабельності інвестицій. Як і інші галузі, банківський сектор стикається з жорсткою конкуренцією за клієнтів та частку ринку, прагнучи до найвигідніших умов. На цей процес суттєво впливають численні ринкові ризики, включаючи ризик запуску нового продукту.

Репутаційний ризик виникає з потенційної нездатності банку підтримувати свою репутацію надійної та ефективної установи. Висока залежність від зовнішнього капіталу робить банки особливо вразливими до цього ризику. Втрата довіри вкладників може призвести до відтоку капіталу та навіть банкрутства. Керівництво банку повинно приділяти особливу увагу дотриманню нормативних вимог, постійному моніторингу ліквідності та загальному рівню ризику банківської операції.

2.2 Оцінка ризиків банківської діяльності

Банки, які працюють з метою отримання прибутку, неминуче стикаються з ризиками. Тому рівні ризиків повинні належним чином управлятися та контролюватися. Також необхідно оцінювати серйозність банківських ризиків, і ця оцінка має бути постійною.

Відповідно до ризик-орієнтованого регуляторного підходу, відповідальність за контроль ризиків лежить на керівництві та наглядовій раді банку. Національний банк зосереджується на рівні управління ризиками протягом певного періоду, а не просто оцінює ризикову ситуацію в певний момент часу. Згідно з ризик-орієнтованою моделлю регулювання, Національний банк діє радше як регулятор, ніж як аудитор. Ця модель дозволяє Національному банку проводити превентивний нагляд, зосереджуючись як на ризиках окремих банків, так і на системних ризиках у банківській системі.

Щодо банківської системи, ризик-орієнтована регуляторна модель спрямована на визначення сфер діяльності, які в поєднанні можуть становити неприйнятні ризики для банківської системи. Щодо діяльності з високим рівнем ризику або діяльності, яка стає особливо ризикованою через ринкові фактори, Національний банк має намір взаємодіяти з банківською системою шляхом прямого нагляду та відповідних регуляторних заходів для здійснення належного впливу. Якщо управління ризиками банку є неадекватним, Національний банк вживатиме відповідних заходів, щоб спрямувати керівництво банку на узгодження своїх дій з фундаментальними принципами надійної банківської справи.

Деякі ризики є невід'ємною частиною банківських операцій. Банківський сектор має великий досвід у виявленні, вимірюванні, управлінні та моніторингу цих притаманних ризиків. Регулювання на основі ризиків визнає їх існування та прагне максимально ефективно використовувати регуляторні ресурси.

Наприклад, параметри ризику базуються на результатах обмеженого тестування, проведеного під час перевірок, щоб забезпечити наявність належних засобів контролю. Це підтверджує початкові результати визначення параметрів ризику та допомагає у розробці регуляторних підходів на основі параметрів ризику кожного банку. Процес визначення параметрів ризику має вирішальне значення для розробки циклів моніторингу та вибору інструментів моніторингу. Ризики, з якими стикається банківський сектор, різноманітні та складні. Найбільш значущі та складні ризики вимагають більш ефективних заходів контролю та моніторингу як з боку банків, так і з боку національного банку. Коли ці складні та зростаючі ризики становлять значну фактичну або потенційну загрозу для банківської системи, Національний банк Іспанії зосереджує свої ресурси на їхньому вирішенні. Через відмінності в ринкових умовах та банківських системах не існує універсальної системи управління ризиками, що застосовується до всіх банків. Кожна установа повинна розробити власний план та систему управління ризиками, адаптовані до її конкретних потреб та обставин. Наприклад, більші банки зі складнішими операціями та філіями, розташованими в різних географічних регіонах, в ідеалі повинні мати більш комплексні та просунуті системи управління ризиками. Однак усі ефективні системи управління ризиками мають деякі спільні ключові характеристики. Наприклад, ефективна система управління ризиками повинна бути незалежною від діяльності з високим рівнем ризику. Будь-яка система управління ризиками, незалежно від її структури, повинна включати такі елементи:

- Оцінка ризиків. Правильна ідентифікація ризиків передбачає, перш за все, ідентифікацію та розуміння існуючих ризиків або потенційних ризиків, пов'язаних з новими бізнес-ініціативами. Ідентифікація ризиків має бути безперервним процесом, що проводиться одночасно на рівні окремого бізнесу та на рівні портфеля;

- Вимірювання ризиків. Точне та своєчасне вимірювання ризиків є надзвичайно важливим компонентом ефективного управління ризиками. Банки

без системи вимірювання ризиків мають дуже обмежені можливості контролю та моніторингу ризиків. Крім того, інструменти управління ризиками, що використовуються банком, повинні бути розроблені відповідно до складності та рівня ризику. Банки повинні регулярно переглядати надійність інструментів бухгалтерського обліку, які вони використовують. Відповідна система вимірювання ризиків включає оцінку окремих транзакцій;

- Контроль ризиків. Банки повинні встановлювати ліміти ризиків та повідомляти їх контрагентам за допомогою правил, стандартів та/або процедур, чітко визначаючи обов'язки та повноваження співробітників. Ці контрольні ліміти повинні бути ефективними інструментами управління та можуть коригуватися відповідно до змін обставин або толерантності до ризику. Банки повинні встановити процедуру затвердження винятків або змін лімітів ризику, коли це доцільно.

- Моніторинг ризиків. Банки повинні відстежувати ризики, щоб забезпечити своєчасний моніторинг рівнів ризику та винятків з певних правил. Звіти про подальші дії повинні бути регулярними, своєчасними, точними та інформативними, і повинні надаватися відповідному персоналу, щоб вони могли вжити необхідних заходів.

Ефективне управління ризиками вимагає участі наглядової ради банку. Наглядова рада повинна визначати стратегічний напрямок діяльності банку. Вирішальним компонентом стратегічного управління є визначення готовності банку брати на себе ризики та досягнення цього шляхом усного або письмового затвердження відповідних умов. За допомогою добре розробленої системи моніторингу наглядова рада може забезпечити, щоб керівництво банку діяло в межах встановлених лімітів толерантності до ризику. Під час оцінки системи управління ризиками менеджери враховують політику, процеси, людей та системи контролю. Значні недоліки в одному або кількох із цих компонентів вважаються недоліками в управлінні ризиками. Усі ці системи є важливими, але рівень їх розвитку та складність відрізнятимуться залежно від складності банківського бізнесу. Менші банки з менш складними операціями часто мають

менш стандартизовані правила, процеси та системи контролю, ніж більші банки. Однак це не означає, що системи управління ризиками неважливі для банків з простішими операціями; це просто означає, що стандартизація процесів нижча. Усі банки повинні мати можливість чітко визначити та продемонструвати ефективність своїх систем управління ризиками. Ефективне управління ризиками вимагає послідовних правил, процесів, кваліфікованого персоналу та систем контролю:

- Нормативні акти відображають намір банку досягти поставлених цілей. Вони визначають стандарти та заходи, яких необхідно дотримуватися для виконання конкретних завдань. Добре розроблені правила базуються на чіткій місії, цінностях та принципах банку та чітко визначають толерантність банку до ризику. Слід створити відповідні механізми для коригування правил, коли змінюється характер банківського бізнесу або толерантність до ризику. Нормативні акти повинні розроблятися з урахуванням таких факторів, як складність бізнесу та вплив організаційної структури, і повинні бути чітко визначені та забезпечувати їх виконання.

- Процеси стосуються процедур, планів та практик, які визначають, як банк виконує свої завдання. Процеси визначають, як здійснюється поточна діяльність банку. Добре розроблені процеси повинні базуватися на рекомендаціях банку, функціонувати ефективно та виконуватися в межах відповідних повноважень виконавчого органу;

- Персонал: стосується працівників та керівників, які фактично виконують або контролюють процеси. Працівники та керівники повинні мати відповідну кваліфікацію та здібності для ефективного виконання своїх обов'язків. Вони повинні розуміти місію, цінності, позиціонування та процеси банку. Система компенсації банку повинна забезпечувати залучення та утримання кваліфікованих працівників і сприяння їхньому подальшому кар'єрному розвитку;

- Системи контролю стосуються інструментів та інформаційних систем, що використовуються керівниками банку для оцінки ефективності роботи

працівників, відділів та банку в цілому, прийняття рішень та визначення ефективності існуючих процесів банку.

Ґрунтуючись на принципі зворотного зв'язку, вони повинні бути своєчасними, точними та інформативними. Вони допомагають оцінити діяльність та рішення банку.

Кількість ризиків та якість управління ризиками слід оцінювати незалежно один від одного. Тому, визначаючи рівень кожного фактора оцінки в рамках системи оцінки ризиків, необхідно пам'ятати, що якість управління ризиками не повинна впливати на оцінку кількості ризиків. Крім того, великі обсяги капіталу або відмінні фінансові показники не слід розглядати як компенсуючі фактори для недосконалостей системи управління ризиками. Регулятори не повинні робити висновок, що «високий» рівень ризику – це погано, а «низький» рівень ризику – це добре. Кількість ризику лише відображає рівень ризику, який банк бере на себе у своїй діяльності, а її якість залежить від того, чи може система управління ризиками банку ідентифікувати, вимірювати, моніторити та контролювати цю кількість ризику. [23]

Національні банки уповноважують своїх співробітників оцінювати ефективність, комплексність та адекватність системи управління ризиками банку шляхом: аналізу діяльності банку, внутрішніх документів та результатів самооцінки; перевірки процесів, операцій та інструментів управління ризиками; проведення співбесід з керівниками банку та іншими співробітниками; та оцінка взаємодії ради директорів банку та частоти зустрічей з головним менеджером з управління ризиками та головним менеджером з комплаєнсу. [24]

Банки використовують ефективні моделі та інструменти для оцінки (вимірювання) ризиків, включаючи повністю кількісно вимірювані ризики та менш кількісно вимірювані ризики, такі як репутаційні та стратегічні ризики. Банки мають право використовувати інструменти оцінки ризиків лише для менш кількісно вимірюваних ризиків. [24]

Вибираючи моделі та інструменти оцінки ризиків, банки враховують такі фактори:

1) Конкретні обставини, характер, обсяг та профіль ризику банківського бізнесу;

2) Потреби бізнесу;

3) Основні припущення моделей та інструментів;

4) Точність та повнота вхідних даних;

5) Можливості інформаційної системи управління ризиками банку;

6) Досвід та кваліфікація персоналу. [24]

Банки перевіряють моделі/інструменти, розроблені ними самими та зовнішніми установами.

Банки не перевірятимуть міжнародні моделі/інструменти розподілу (а також методи аналізу тривалості та аналізу розривів), якщо вони стандартизовані, їхні компоненти, переваги, недоліки тощо є загальнодоступними, і банк не може змінювати результати їхньої валідації.

Банки не перевірятимуть моделі/інструменти оцінки ризиків, розроблені Національним банком, компоненти яких базуються на агрегованих статистичних даних, зібраних Національним банком з усієї банківської системи України. Банки повинні розраховувати мінімальні регуляторні вимоги.

Валідація моделей/інструментів оцінки ризиків повинна бути незалежною від розробки моделі або вибору та використання інструменту. Валідацію має виконувати незалежне відділення банку (не та організація, яка створила та/або використовує модель чи інструмент) або зовнішня організація, включаючи аутсорсинг валідації моделі/інструменту цій організації. Якщо банк відповідає вимогам незалежності для валідації моделі, модель може бути створена субпідрядником.

Ризик-менеджери повинні забезпечити, щоб рада директорів банку та комітет з управління ризиками мали повне розуміння сильних та слабких сторін моделей та інструментів ризику, притаманних припущень та обмежень моделей, щоб їх можна було використовувати під час перегляду результатів оцінки ризиків та бути готовими своєчасно розглядати та приймати відповідні управлінські рішення.

Банки повинні періодично проводити стрес-тести з частотою, зазначеною в цьому Положенні, для оцінки ризиків та визначення їхньої здатності протистояти шокам та загрозам, з якими вони стикаються або можуть виникнути в їхній діяльності. [24]

Банки повинні розробити внутрішній документ або створити окремий розділ про стрес-тестування у відповідних документах для кожного типу ризику, щоб регулювати процедури впровадження/виконання (програму стрес-тестування) для стрес-тестування. План повинен визначати:

1) методи та моделі стрес-тестування;

2) частоту проведення різних стрес-тестів;

3) перелік учасників процесу стрес-тестування, їхні функції та процедури взаємодії, а також їхні повноваження та обов'язки, та уточнювати їхні підпорядковані відносини;

4) перелік типів ризиків для стрес-тестування;

5) перелік факторів ризику, що використовуються в стрес-тестуванні;

6) перелік припущень, що використовуються в стрес-тестуванні;

7) інформаційну систему управління ризиками, яка використовується банком для проведення стрес-тестування;

8) процедури перегляду результатів стрес-тестування та процедури повідомлення результатів тестування раді директорів банку, комітету з управління ризиками та управлінському комітету, щоб своєчасно приймати відповідні управлінські рішення та знижувати рівень ризику. [24]

Для кожного основного типу ризику банк самостійно визначатиме метод стрес-тестування на основі власного досвіду. Залежно від конкретних обставин банк застосовуватиме один або декілька з наступних методів:

1) аналіз чутливості портфеля до змін факторів ризику, тобто моделювання впливу змін одного фактора ризику або групи тісно пов'язаних факторів ризику (але без урахування змін інших факторів ризику);

2) сценарний аналіз, тобто моделювання впливу одночасних змін кількох факторів ризику на основі історичних та гіпотетичних подій. За умови високої

ймовірності екстремальних подій цей метод може оцінити потенційний вплив кількох факторів ризику, що виникають одночасно, на ділову діяльність банку. Під час побудови сценаріїв банки вибирають фактори ризику з найбільшим негативним впливом, які можуть призвести до найбільших збитків, та будують найгірший сценарій.

3) Зворотне стрес-тестування передбачає визначення комбінацій факторів ризику та визначення сценарію, за яким банк зіткнеться із заздалегідь визначеними негативними наслідками (наприклад, порушення національних стандартів капіталу банку та/або інших стандартів, втрата ліквідності, банкрутство тощо, що негативно впливає на банк). Це дослідження може використовувати експертні методи та статистичні моделі.

Ризик-менеджери повинні забезпечити, щоб рада директорів банку та комітет з управління ризиками повністю розуміли переваги та недоліки методологій стрес-тестування та стресових сценаріїв, щоб їх можна було враховувати під час розгляду результатів та прийняття своєчасних та ефективних управлінських рішень.

Банки використовують результати стрес-тестування для розробки/перегляду/коригування своїх бізнес-планів та стратегій, стратегій управління ризиками, політик та процедур, планів відновлення, забезпечення безперервності бізнесу та кризового фінансування.

2.3 Висновки по розділу

У другій частині досліджуються ризики банківської діяльності та пропонуються методи оцінки цих ризиків.

РОЗДІЛ 3.

РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СИСТЕМІ З ВИКОРИСТАННЯМ СУЧАСНИХ ЗАСОБІВ

3.1 Опис об’єкту

Офісна будівля банку (Рис. 3.1) займає площу 307,59 квадратних метрів. Вона містить 14 робочих зон: операційну (кімната 2), кімнату для переговорів (кімната 4), кабінет віце-президента (кімната 5), кабінет президента (кімната 6), сховище (кімната 7), передсховище (кімната 8), кімнату касира 1 (кімната 11), кімнату касира 2 (кімната 12), кімнату касира 3 (кімната 13), кабінет керівника (кімната 14), кабінет технічного персоналу (кімната 14) та кімнату конфіденційного відділу та архіву (кімната 16). Крім того, є кімната банкоматів (кімната 1) та кімната охорони (кімната 3). Вікна кімнат 4, 5 та 6 оснащені металевими жалюзі, а вікно кімнати 2 покрите захисною плівкою. Усі двері з використанням карток Wiegand та системою контролю доступу за відбитками пальців є броньованими. Висота стелі у всіх кімнатах становить 2,5 метра.

Наш робочий час: з 9:00 до 18:00, обідня перерва з 13:00 до 14:00. Протягом робочого часу всі двері відчинені для відвідувачів. Відвідувачам заборонено входити до приміщення поза робочим часом та обідньою перервою.

В кінці робочого дня співробітники служби безпеки повинні закрити всі жалюзі та двері; процедура відкриття дверей така ж, як і в кінці робочого дня.

3.2 Вибір та обґрунтування зразків обладнання

У цьому розділі буде обрано оптимальне рішення на основі характеристик обладнання, яке буде використовуватися в проектованій системі.

IP-камери зазвичай використовуються в системах контролю доступу (СКУД); тому на рисунку 3.2 показано камери, що використовуються для порівняння.

У таблиці 3.1 порівнюються основні технічні характеристики вищезгаданих неповоротних IP-камер.

Таблиця 3.1.

Основні технічні характеристики неповоротних IP-камер

Характеристики	**ATIS ANVD-2MIRP-20W/2.8A**	Hikvision DS-2CD1721FWD-IZ (2.8-12mm)	ATIS ANVD-2MVFIRP-30W/2.8-12 Prime	Hikvision DS-2CD2T23G0-I8(4mm)	Uniview IPC2324EBR-DP
Ціна, грн	1620 грн	3300 грн	1950 грн	4038 грн	5740 грн
Розширення відео	1920x1080	1920x1080	1920x1080	1920x1080	2592x1520
Кут обзору, °	105	111	101	86	91
Матриця	1/2.9 CMOS	1/2.8 CMOS	1/2.8 CMOS	1/2.8 CMOS	1/3 CMOS
ІЧ-підсвітка	+	+	+	+	+
Живлення	DC 12В/PoE	DC 12В/PoE	DC 12В/PoE	DC 12В/PoE	DC 12В/PoE
Захист	IP66	IP67	IP66	IP67	IP67
Розширення	2 Мп	2Мп	2Мп	2Мп	4Мп

Проаналізувавши характеристики неповоротних IP-камер, ми дійшли висновку, що камера Hikvision DS-2CD1721FWD-IZ (2.8-12 мм) була найкращим вибором для цього проєкту. Інші компоненти для побудови системи ми обрали таким самим чином. У таблиці 3.2 порівнюються основні технічні характеристики вищезгаданих поворотних IP-камер.

Таблиця 3.2.

Основні технічні характеристики поворотних IP-камер

Характеристики	Wi-Fi IP Камера 3Мп Reolink E1	Wi-Fi IP Камера 4Мп Reolink E1 Pro	Wi-Fi IP Камера с зумом 5Мп Reolink E1 Zoom	IP Камера Dahua Technology DH-IPC-A15P	IP Камера Dahua Technology DH-IPC-A35P
Ціна, грн	1725 грн	2032 грн	2802 грн	2660 грн	3360 грн
Розширення відео	2304x1296	2560x1440	2560x1920	1280x960	2592x1520
Кут обзору, °	82	90	90	72	77
Панорамування, °	355	355	355	355	355
Матриця	1/2.7 CMOS	1/2.7 CMOS	1/2.7 CMOS	1/3 CMOS	1/3 CMOS
ІЧ-підсвітка	+	+	+	+	+
Живлення	DC 12В/PoE	DC 12В/PoE	DC 12В/PoE	DC 5В/2А	DC 5В/2А
Розширення	3 Мп	4 Мп	5 Мп	1.3 Мп	3 Мп

Після аналізу характеристик обертових мережевих камер ми вважаємо, що мережева Wi-Fi камера Reolink E1 Pro 4MP є найбільш підходящою для цього проєкту розробки.

У таблиці 3.3 наведено основні технічні характеристики контролера.

Таблиця 3.3.

Характеристики контролерів, що використовувались для порівняння

Характеристики	Контролер Hikvision DS-K2802	Контролер Hikvision DS-K2801	Контролер Dahua DHI-ASC1202B-S	Контролер Dahua DHI-ASC1204B-S
Ціна	4231	3357	2380	3136
Число подій, що зберігаються в пам'яті	50000	50000	150000	150000
Кількість зчитувачів	4	2	2	4
Підтримка Wiegand	+	+	+	+
Кількість ідентифікаторів	10000	10000	100000	100000

Після проведеного дослідження найкращим варіантом є Контролер

Dahua DHI-ASC1204B-S.

В таблиці 3.4 наведено найважливіші технічні характеристики для контролерів з відбитком пальця.

Таблиця 3.4.

Основні технічні характеристики зчитувачів з відбитком пальця

Характеристики	Зчитувачі Dahua ASI1202M	Зчитувачі FoxKey FK-F-2	Зчитувачі Trinix TRR-1000W	Зчитувачі Trinix TRR-1000F
Ціна	4760	2755	1844	9000
Число подій, що зберігаються в пам'яті	150000	10000	6000	10000
Підтримка Wiegand	+	+	+	-
Кількість ідентифікаторів	30000	1000	3000	1000

Проаналізувавши характеристики зчитувачів відбитків пальців, ми дійшли висновку, що зчитувач Dahua ASI1202M був найкращим вибором для цієї розробки.

Таблиця 3.5.

Характеристики зчитувачів карт, що використовувались для порівняння

Характеристика	ATIS PR-08 EM-W	Dahua DHI-ASR1100A-D	ATIS PR-82-EM	ATIS PR-06 EM-W	ATIS PR-80-EM
Тип карт	EM-MARINE	EM-MARINE	EM-MARINE	EM-MARINE	EM-MARINE
Підтримка Wiegand	+	+	+	+	+

Після проведеного дослідження найкращим варіантом є зчитувач карт з

клавіатурою Dahua DHI-ASR1201D.

В таблиці 3.7 наведено найважливі технічні характеристики для систем безпеки.

Таблиця 3.7.

Характеристики систем безпеки, що використовувались для порівняння

Характеристики	Axxon Next	Milestone Systems	DSSL	Kipod
Ціна, грн	*5000*	7000	6500	4500
Кількість камер	*необмежено*	*необмежено*	128	8000
Кількість серверів	*необмежено*	*необмежено*	4	30
Підтримка різних типів камер	+	+	-	+
Підтримка різних модулів	+	+	+	+
Пробна безкоштовна версія	+	-	-	-
Автозум	+	+	-	-
Пошук в архіві	Зручний	Зручний	Немає	Зручний
Детектор руху	Чудовий	Нормальний	Чудовий	Нормальний

Після проведеного дослідження найкращим варіантом є система безпеки Axxon Next.

В таблиці 3.8 наведено найважливіші технічні характеристики для серверів.

Таблиця 3.8.

Характеристики серверів, що використовувались для порівняння

Характеристики	HP ProLiant DL360e Gen8	HP ProLiant DL380p Gen8	Dell R720	Cisco UCS C220 M3 LFF
Ціна, грн	23119 грн	25219 грн	24917 грн	8993 грн
Об'єм оперативної пам'яті, Гб	16	16	16	16
Частота процесора, ГГц	2,40-2,80	2,00-2,50	2,00-2,50	2,00-2,50
Об'єм жорсткого диску, Гб	1200	600	1200	-
Потужність блоку живлення, Вт	750	750	750	650
Гарантія, міс.	24	24	24	24

Після проведеного дослідження найкращим варіантом є сервер HP ProLiant DL360e Gen8.

Таблиця 3.9

Характеристики електромагнітного замка

Принцип роботи	Магнітна взаємодія
Сила утримання	240 кг
Матеріал корпусу	Алюміній
Живлення	12 В
За відсутності струму	Відкритий
Розміри	186 x 45 x 30 мм

Таблиця 3.10

Характеристики доводчика дверей

Тип дверного доводчика	Класичний дверний доводчик з ліктьовою тягою
Вага двері	До 80 кг
Ширина двері	До 1100 мм
Тип важілю	Колінчастий важіль
Кут відкриття двері	180°

PBK-814A(LED) - кнопка виходу з нержавіючої сталі, використовується для монтажа в системах контроля доступа.

Генератор акустичного "білого шуму" (2 канали "вібрації" + 1 канал "акустичного"). Призначений для запобігання прослуховуванню через стетоскопи та контактні мікрофони в приміщенні. Може перешкоджати роботі диктофонів та закладок у приміщенні. Діапазон частот 250-5000 Гц. Має канал зворотного зв'язку для регулювання гучності. Сертифіковано Центральним управлінням розвідки України.

DNG-2300 призначений для запобігання витоку конфіденційної інформації вбудованими пристроями, які неможливо виявити традиційним пошуковим обладнанням. Крім того, він захищає від прослуховування пристрої, встановлені навколо або за межами захищених зон, такі як дротові мікрофони, контактні мікрофони та передавачі, що використовують мережі 220 В..

3.3 Склад обладнання проектованої системи контролю і управління доступом банківської установи

Систему захисту банку сформуємо в складі нижчеподаного обладнання:

- 20 неповоротних IP-камер Hikvision DS-2CD1721FWD-IZ (2.8-12mm) (характеристики наведені в таблиці 3.1);
- 2 поворотні Wi-Fi IP Камери 4Мп Reolink E1 Pro (характеристики наведені в таблиці 3.2);

- 4 зчитувача з відбитком пальців Dahua ASI1202M (характеристики наведені в таблиці 3.4);
- 4 зчитувача карт ATIS PR-82 EM (характеристики наведені в таблиці 3.5);
- 3 зчитувача карт з клавіатурою Dahua DHI-ASR1201D (характеристики наведені в таблиці 3.6);
- 9 генераторів шуму DNG2300 (характеристики наведені в розділі 3);
- 3 контролера Dahua DHI-ASC1204B-S (характеристики наведені в таблиці 3.3);
- 16 доводчиків дверей GEZE TS 1500 (характеристики наведені в таблиці 3.10);
- 11 електромагнітних замків VIZIT-ML240-40 (характеристики наведені в таблиці 3.9);
- 11 кнопка виходу PBK-814A(LED);
- 1 система безпеки Axxon Next (характеристики наведені в таблиці 3.7);
- 4 сервери HP ProLiant DL360e Gen8 (характеристики наведені в таблиці 3.8).

3.4 Економічний розрахунок

В економічній частині буде розраховано повну вартість комплексної системи захисту інформації у приміщенні з обмеженим доступом.

Таблиця 3.11.

Вартість складових системи захисту

Складова системи захисту	Ціна,грн	Кількість	Вартість, грн
Камера Hikvision DS-2CD1721FWD-IZ	3300	20	66 000
Камера Wi-Fi IP Камера 4Мп Reolink E1 Pro	2032	2	4 064
Зчитувач з відбитком пальців Dahua ASI1202M	4760	4	19 040
Зчитувача карт ATIS PR-82 EM	390	4	1 560
Зчитувач карт з клавіатурою Dahua DHI-ASR1201D	1260	3	3 780
Генератор шуму DNG2300	22752	9	204 768
Контролер Dahua DHI-ASC1204B-S	3136	3	9 408
Доводчик дверей GEZE TS 1500	743	16	11 888
Електромагнітний замок VIZIT-ML240-40	1000	11	11 000
Кнопка виходу PBK-814A(LED)	330	11	3 630
Система безпеки Axxon Next	5000	1	5 000
Сервер HP ProLiant DL360e Gen8	23119	4	92 476
Загальна вартість системи захисту, грн			366 680

¶

Розрахунок:

Загальна вартість комплексної системи захисту = 66 000 + 4 064 + 19 040 + 1 560 + 3 780 + 204 768 + 9 408 + 11 888 + 11 000 + 3 630 + 5 000 + 92 476 = = **366 680 грн.**

Було проведено оцінку собівартості розробленої комплексної системи захисту конфіденційної інформації в банку.

Вартість системи склала **366 680 грн.**

Таким чином, повна окупність даної системи захисту можлива за 2 роки.

3.5 Висновок по розділу

У третій частині розглядалося загальне планування об'єкта та обрано обладнання для його системи безпеки.

Було використано зчитувачі карток Wegener, сканери відбитків пальців та IP-камери. Технічні характеристики кожного пристрою були проаналізовані в процесі розробки.

Також було проведено економічні розрахунки заходів безпеки для банківської системи. Розрахунки показали, що термін окупності системи становить приблизно два роки.

ВИСНОВКИ

У цій магістерській роботі розроблено систему захисту інформації для банківської системи з використанням сучасних заходів контролю та запобігання витоку інформації.

Під час написання цієї роботи було виконано такі завдання:

– Аналіз процесу забезпечення безпеки банківської системи;

– Аналіз можливостей та характеристик методів захисту інформації з обмеженим доступом у банківській інформаційній системі;

– Дослідження напрямків підвищення ефективності захисту інформації в банківській системі;

1. У першій частині представлено основну інформацію про банківську систему, банківську інформацію, її безпеку та основні загрози, а також проаналізовано канали витоку інформації.

2. У другій частині проаналізовано ризики банківської діяльності та їх оцінку.

3. У третій частині розглянуто загальне планування об'єкта та вибрано обладнання, необхідне для системи захисту об'єкта. Використовувалися зчитувачі карток Wiegand, сканери відбитків пальців та IP-камери. Було проаналізовано технічні характеристики кожного розробленого пристрою.

Крім того, було розраховано економічну ефективність заходів захисту банківської системи. Результати розрахунків показують, що термін окупності інвестицій у систему становить приблизно 2 роки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Council of Europe Convention on Access to Official Documents, Tromso, 2009 / / CETS № 205.

2. Charter of the United [Електронний ресурс]. — Режим доступу: http://www.un.orglen/documents/charter/.].

3. Sullivan, G. (2011). «The Bribery Act 2010 : Part One: an overview». Criminal Law Review. 2011 (2). ISSN 0011-135X. С. 46

5. Андреев В.І., Хорошко В.О., Чередниченко В.С., Шелест М.Є Основи кібербезпеки / За ред. проф. В.О. Хорошка. вид., доп. і перероб. — К. : Вид. ДУІКТ, 2009. — 292 с.

6. Максименко Ю.Є. Теоретико-правові засади забезпечення кібербезпеки України : дис.… канд. юрид. наук :12.00.01 / Ю.Є. Максименко. — К., 2007. — 186 с.

7. Марущак А.І. Кібербезпека як об’єкт дослідження правової науки / А.І. Марущак // Актуальні проблеми управління кібербезпекою держави : зб. матер. наук.- прак. конф., 17 березня 2010 року м. Київ. — К. : Наук. вид. відділ НА СБ України, 2010. — С. 36−41

8. Марущак А.І. Інформаційне право : Доступ до інформації : Навч. посіб. / А. І. Марущак. — К., 2007. — 280 с.

9. Марущак, А. І. Інформаційне право: регулювання інформаційної діяльності : Навчальний посібник. К. : Видавничий дім «Скіф», КНТ, 2008. — 344 с

10. Арістова, І.В. Державна інформаційна політика : організаційно-правові аспекти : Монографія / І.В. Арістова. —
Х. : Вид-во ун-ту внутр. справ, 2000. — 368 с.

11. Hells U., Karras A., Scherer K.R. Multichannel communication of emotion: synthetic signal production // Facets of
Emotion. Recent research / Ed. K.R.Scherer/ — Hillsdate,

N.J. — 1988. — P. 162

12. Sullivan, G. (2011). «The Bribery Act 2010 : Part One: an overview». Criminal Law Review. 2011 (2). ISSN 0011-135X. C. 46

13. Charter of the United [Електронний ресурс]. — Режим доступу: http://www.un.orglen/documents/charter/.].

14. Шутов, Р. Глиняний фундамент кібербезпеки — [Електронний ресурс] — Режим доступу:
http://osvita.mediasapiens.ua/media_law/law/koli_sosud_napivporozhniy_scho _robiti_z_kontseptsieyu_informatsiynoi_bezpeki/.

15. Цимбалюк В.С. Сутність кібербезпеки в умовах входження України до глобальної кіберцивілізації / В. Цимбалюк // Науковий вісник академії ДПС України. —2007. — № 4. — С. 174–178.

16. Цимбалюк В.С. Інформаційне право (основи теорії і практики) / В.С. Цимбалюк. Монографія. — К. : «Освіта України», 2010. — 388 с.

17. What is Authorization? [Електронний ресурс] // auth0 bu Okta. – 2022. – Режим доступу до ресурсу: https://auth0.com/intro-to-iam/what-is-authorization.

18. API Reference [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://stripe.com/docs/api/errors.

19. Krawczyk H. HMAC: Keyed-Hashing for Message Authentication [Електронний ресурс] / H. Krawczyk, M. Bellare // IBM. – 1997. – Режим доступу до ресурсу: https://www.rfc-editor.org/rfc/rfc2104.

20. Лужецький В. А. ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ / В. А. Лужецький, А. Д. Кожухівський, О. П. Войтович. – Вінниця: ВНТУ, 2009. – 268 с.

21. Аліпов Ілля Миколайович. Методи захисту інформації при її передаванні : Автореф. дис... канд. техн. наук: 05.13.08 / Харківський держ. технічний ун-т радіоелектроніки. - Х., 1997. - 22с

22. Богуш Володимир Михайлович, Мухачов Владислав Андрійович. Криптографічні застосування елементарної теорії чисел : Навч. посібник /

Державний ун-т інформаційно-комунікаційних технологій. - К. : ДУІКТ, 2006. – 126 с.

23. Ємець Володимир, Мельник Анатолій, Попович Роман. Сучасна криптографія: Основні поняття . - Л. : БаК, 2003. - 144с. : рис., табл. - (Захист інформації в комп'ютерних та телекомунікаційних мережах). - Бібліогр.: с. 128.

24. Hung-JenLiao. Intrusion detection system: A comprehensive review / Hung-JenLiao, Kuang-YuanTunga. // Journal of Network and Computer Applications. – 2013. – №36. – С. 16–24.

25. Snort IDS and IPS Toolkit [Електронний ресурс]. – 2007. – Режим доступу до ресурсу: https://www.amazon.com/Snort-Toolkit-Beales-SourceSecurity/dp/1597490997.

26. Polymorphic Blending Attacks [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: https://www.usenix.org/legacy/event/sec06/tech/full_papers/fogla/fogla.pdf.

27. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с.

28. Економічний ризик : методи оцінки та управління : навч. посіб. / за ред. Т. А. Васильєвої. Суми : ДВНЗ «УАБС НБУ», 2015. 208 с.

29. Traffic Inspector Next Generation [Електронний ресурс] // Smart-Soft. – 2014. – Режим доступу до ресурсу: https://www.evraas.com/upload/iblock/ead/eadf098bb265b5bce1e4ebd0db73c51b.pdf.

30. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння [Електронний ресурс]. – 2002. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68769.

31. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Поправка [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=65314.

32. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. З поправкою [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66229.

33. Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z2227-13#Text.

ДОДАТКИ

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

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

СИСТЕМА ЗАХИСТУ ТЕХНІЧНИХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОБ’ЄКТІ ФІНАНСОВОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Олександр ЛИХОГОД

Керівник: к.е.н. Ігор АВЕРІЧЕВ

Київ - 2026

АКТУАЛЬНІСТЬ ТЕМИ ДОСЛІДЖЕННЯ

- Банківські та фінансові установи обробляють інформацію з обмеженим доступом, банківську та комерційну таємницю.
- Технічні канали витоку інформації можуть формуватися через мережеві, акустичні, електромагнітні, візуально-оптичні та організаційні чинники.
- Несанкціонований доступ до інформації в банку створює ризики фінансових втрат, порушення роботи установи та компрометації клієнтських даних.
- Актуальним є побудова комплексної системи захисту, що поєднує організаційні, технічні та програмно-апаратні засоби.

МЕТА, ОБ’ЄКТ, ПРЕДМЕТ І ЗАВДАННЯ РОБОТИ

- Мета роботи - підвищення ефективності захисту технічних каналів передачі інформації від несанкціонованого доступу на об’єкті фінансової діяльності.
- Об’єкт дослідження - банківська установа як об’єкт фінансової діяльності.
- Предмет дослідження - система захисту інформації банківської установи.
- Основні завдання: проаналізувати банківську систему та її інформаційні потоки; визначити канали витоку; оцінити ризики; обґрунтувати склад технічних засобів захисту.

БАНКІВСЬКА ІНФОРМАЦІЯ ТА РЕЖИМИ ДОСТУПУ

- Банківська інформація охоплює дані, що містяться у документах банку або розкриваються установою відповідно до вимог чинного законодавства.
- За режимом доступу вона поділяється на загальнодоступну інформацію та інформацію з обмеженим доступом.
- До інформації з обмеженим доступом належать дані про рахунки клієнтів, операції, фінансовий стан клієнтів, банківські коди, внутрішні процедури та системи захисту.
- Захист таких даних потребує контролю доступу, обмеження поширення, журналювання подій та технічного блокування каналів витоку.

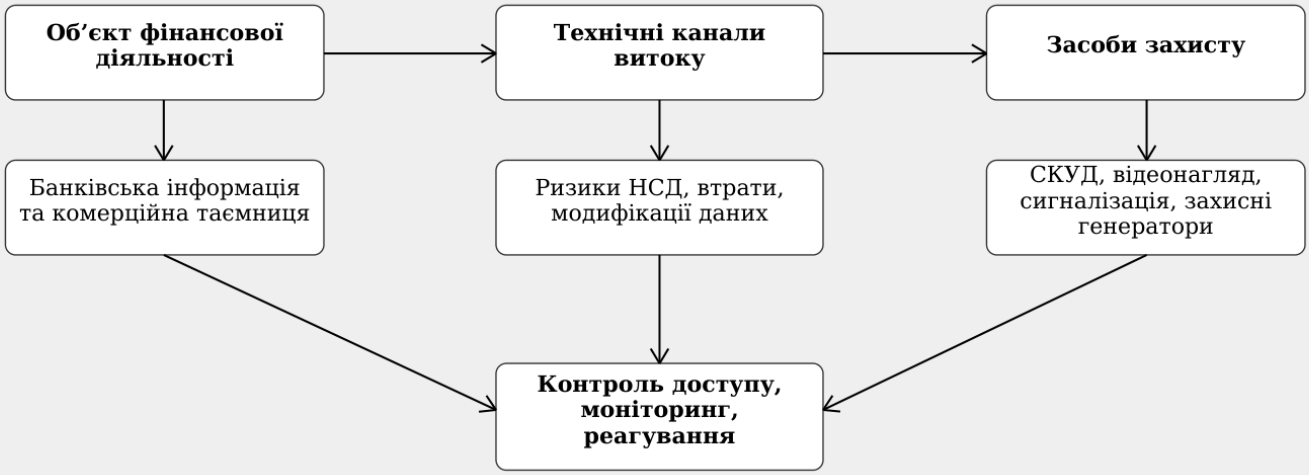
КАНАЛИ ПОШИРЕННЯ ТА ВИТОКУ ІНФОРМАЦІЇ

- Канали витоку інформації можуть виникати під час зберігання, обробки, передавання та відображення даних.
- Для банківської установи критичними є технічні канали, пов’язані з приміщеннями, обладнанням, комунікаційними мережами та засобами зв’язку.
- Окрему небезпеку становлять побічні електромагнітні випромінювання та наведення, акустичні сигнали, оптичне спостереження й несанкціонований фізичний доступ.
- Усунення каналів витоку повинно здійснюватися через зонування приміщень, контроль доступу та застосування спеціалізованих технічних засобів захисту.

РИЗИКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

- Ризики банківської діяльності охоплюють операційні, інформаційні, фінансові та організаційні загрози.
- Ключовими наслідками реалізації ризиків є витік банківської таємниці, втручання в роботу автоматизованих систем, блокування бізнес-процесів та несанкціоноване використання даних.
- Оцінювання ризиків дає змогу визначити пріоритетність заходів захисту, обрати адекватні технічні рішення та сформувати економічно обґрунтований склад системи.
- Для об’єкта фінансової діяльності система захисту має бути превентивною, контрольованою та здатною до фіксації інцидентів.

СТРУКТУРНА МОДЕЛЬ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ



ЗАСОБИ КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ

- Система контролю та управління доступом забезпечує ідентифікацію користувачів, обмеження проходу до захищених зон та фіксацію подій доступу.
- До складу системи можуть входити контролери, зчитувачі, електрозамки, датчики стану дверей та програмне забезпечення адміністрування.
- Вибір обладнання виконується з урахуванням функціональності, кількості контрольованих точок, вартості та можливості інтеграції з іншими підсистемами.

Основні технічні характеристики поворотних IP-камер

Характеристики	Wi-Fi IP Камера 3Мп Reolink E1	Wi-Fi IP Камера 4Мп Reolink E1 Pro	Wi-Fi IP Камера с зумом 5Мп Reolink E1 Zoom	IP Камера Dahua Technology DH-IPC-A15P	IP Камера Dahua Technology DH-IPC-A35P
Ціна, грн	1725 грн	2032 грн	2802 грн	2660 грн	3360 грн
Розширення відео	2304x1296	2560x1440	2560x1920	1280x960	2592x1520
Кут обзору, °	82	90	90	72	77
Панорамування, °	355	355	355	355	355
Матриця	1/2.7 CMOS	1/2.7 CMOS	1/2.7 CMOS	1/3 CMOS	1/3 CMOS
ІЧ-підсвітка	+	+	+	+	+
Живлення	DC 12В/PoE	DC 12В/PoE	DC 12В/PoE	DC 5В/2А	DC 5В / 2А
Розширення	3 Мп	4 Мп	5 Мп	1.3 Мп	3 Мп

ІНТЕГРАЦІЯ ДАТЧИКІВ ТА ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ

Характеристики контролерів, що використовувались для порівняння¶

Характеристики	Контролер Hikvision DS-K2802	Контролер Hikvision DS-K2801	Контролер Dahua DHI-ASC1202B-S	Контролер Dahua DHI-ASC1204B-S
Ціна	4251	3327	2380	3136
Число подій, що зберігаються в пам'яті	50000	50000	150000	150000
Кількість зчитувачів	4	2	2	4
Підтримка Wiegand	+	+	+	+
Кількість ідентифікаторів	10000	10000	100000	100000

- Для захисту приміщень банку застосовуються датчики відкривання, руху, пожежної та тривожної сигналізації.
- Інтеграція датчиків із центральним контролером дозволяє оперативно виявляти порушення режиму охорони.
- Технічні засоби охорони доповнюють СКУД і забезпечують контроль стану приміщень у неробочий час.

ЗАХИСТ ВІД АКУСТИЧНИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

- Акустичні канали витоку можуть виникати в місцях проведення переговорів, роботи з клієнтами та оброблення конфіденційних даних.
- Для протидії застосовуються генератори акустичного або віброакустичного зашумлення.
- Підбір таких засобів виконується за параметрами ефективності, зони дії, енергоспоживання, вартості та умов експлуатації.

Основні технічні характеристики зчитувачів з відбитком пальця¶

Характеристики	Зчитувачі Dahua ASI1202M	Зчитувачі FoxKey FK-F-2	Зчитувачі Trinix TRR-1000W	Зчитувачі Trinix TRR-1000F
Ціна	4760	2755	1844	9000
Число подій, що зберігаються в пам'яті	150000	10000	6000	10000
Підтримка Wiegand	+	+	+	-
Кількість ідентифікаторів	30000	1000	3000	1000

ЗАХИСТ ВІД ЕЛЕКТРОМАГНІТНИХ КАНАЛІВ ВИТОКУ

Характеристики серверів, що використовувались для порівняння

Характеристики	HP ProLiant DL360e Gen8	HP ProLiant DL380p Gen8	Dell R720	Cisco UCS C220 M3 LFF
Ціна, грн	23119 грн	25219 грн	24917 грн	8993 грн
Об'єм оперативної пам'яті, ГБ	16	16	16	16
Частота процесора, ГГц	2,40-2,80	2,00-2,50	2,00-2,50	2,00-2,50
Об'єм жорсткого диску, ГБ	1200	600	1200	-
Потужність блоку живлення, Вт	750	750	750	650
Гарантія, міс.	24	24	24	24

- Побічні електромагнітні випромінювання та наведення можуть створювати умови для дистанційного зняття інформації.
- Захист реалізується шляхом екранування, заземлення, фільтрації, використання генераторів завад і контролю технічних засобів.
- Такі заходи є необхідними для приміщень з автоматизованими робочими місцями та обладнанням обробки конфіденційної інформації.

ЗАХИСТ ДВЕРЕЙ, ВХІДНИХ ЗОН І ПЕРИМЕТРА

- Фізичний периметр банківської установи повинен бути захищений від несанкціонованого проникнення та прихованого доступу.
- Для цього використовуються захисні двері, електромеханічні замки, датчики відкривання, турнікети та засоби відеоконтролю.
- Комплексний підхід забезпечує поєднання механічної стійкості, електронного контролю та оперативного реагування.

Характеристики доводчика дверей

Тип дверного доводчика	Класичний дверний доводчик з ліктьовою тягою
Вага двері	До 80 кг
Ширина двері	До 1100 мм
Тип важіль	Колінчастий важіль
Кут відкриття двері	180°

ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ОБРАНОЇ СИСТЕМИ ЗАХИСТУ

Складова системи захисту	Ціна, грн	Кількість	Вартість, грн
Камера Hikvision DS-2CD1721FWD-IZ	3300	20	66 000
Камера Wi-Fi IP Камера 4Мп Reolink E1 Pro	2032	2	4 064
Зчитувач з відбитком пальця Dahua ASI1202M	4760	4	19 040
Зчитувача карт ATIS PR-82 EM	390	4	1 560
Зчитувач карт з клавіатурою Dahua DHI-ASR1201D	1260	3	3 780
Генератор шуму DNG2300	22752	9	204 768
Контролер Dahua DHI-ASC1204B-S	3136	3	9 408
Доводчик дверей GEZE TS 1500	743	16	11 888
Електромагнітний замок VIZIT-ML240-40	1000	11	11 000
Кнопка виходу PBK-814A(LED)	330	11	3 630
Система безпеки Axxon Next	5000	1	5 000
Сервер HP ProLiant DL360e Gen8	23119	4	92 476
Загальна вартість системи захисту, грн			366 680

- У роботі виконано підбір обладнання для побудови системи захисту об’єкта фінансової діяльності.
- Вартість системи визначається кількістю компонентів, типом засобів контролю доступу, сигналізації, відеоконтролю та захисту технічних каналів.
- Економічний розрахунок підтверджує можливість практичного впровадження запропонованого комплексу технічних засобів.

ОЧІКУВАНИЙ РЕЗУЛЬТАТ ВПРОВАДЖЕННЯ СИСТЕМИ

- Зниження імовірності несанкціонованого доступу до приміщень і технічних засобів банківської установи.
- Підвищення рівня захисту банківської інформації, комерційної таємниці та інформації з обмеженим доступом.
- Блокування або зменшення ефективності основних технічних каналів витоку інформації.
- Формування умов для централізованого контролю подій безпеки та оперативного реагування на інциденти.
- Підвищення загальної стійкості об’єкта фінансової діяльності до внутрішніх і зовнішніх загроз.

ВИСНОВКИ ЗА РЕЗУЛЬТАТАМИ РОБОТИ

- Проаналізовано особливості функціонування банківської установи та визначено склад інформації, що потребує захисту.
- Встановлено основні канали можливого витоку інформації та напрями несанкціонованого доступу до банківських даних.
- Розглянуто ризики банківської діяльності та обґрунтовано необхідність застосування комплексної системи технічного захисту.
- Запропоновано склад сучасних засобів захисту, який включає СКУД, охоронну сигналізацію, засоби контролю доступу, захисту технічних каналів та організаційні заходи.
- Виконано підбір обладнання та економічне обґрунтування запропонованої системи.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Олександр ЛИХОГОД

Тема: система захисту технічних каналів передачі інформації

Київ - 2026