ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Система санкціонованого доступу користувачів до каналів передачі інформації 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 ТУНІК

Виконав: здобувач вищої освіти групи СЗДМ 61
Олександр ТУНІК

Керівник: ___ГАВРИЛЕНКО Олексій_____
к.т.н. (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2025

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

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___125-Кібербезпека та захист інформації_____
Освітньо-професійна програма Технічні системи інформаційного та кібернетичного захисту

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр ТУРОВСЬКИЙ

«____» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Туніку Олександру Олександровичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Система санкціонованого доступу користувачів до каналів передачі інформації на об'єкті фінансової діяльності»
керівник кваліфікаційної роботи ГАВРИЛЕНКО Олексій, к.т.н.,

затверджені наказом Державного університету інформаційно-комунікаційних технологій
від « 15 » жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи 20.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи: способи та засоби захисту інформації в банківських установах, стандарти та способи захищеного збору та обробки інформації; опорна локальна захищена банківська мережа збору та обробки інформації.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
4.1. Провести огляд процесу забезпечення інформаційної безпеки банківської установи;
4.2. Проаналізувати методи захисту інформації від несанкціонованого доступу в банківській установі;
4.3. Розробити практичні рекомендацій що підвищення ефективності захисту інформації в банківській установі

5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання _____20.10.2024 ___

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 ТУНІК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олексій ГАВРИЛЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Кваліфікаційна робота складається з: вступу, трьох розділів, висновків та переліку використаних джерел. Обсяг роботи складає 84. Список використаних джерел містить 30 джерел.

Метою роботи є підвищення ефективності захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.

В кваліфікаційній роботі було розглянуто банківську установу, наведено її організаційну побудову та технічне оснащення, проаналізовано канали можливого витоку інформації та запропоновано заходи для запобігання несанкціонованого доступу до інформації, яка циркулює в банківській установі. Розглянуто інформацію про банківську інформаційну систему, основні загрози несанкціонованого доступу до конфіденційної інформації банківської установи.

Підсумком роботи є розробка рекомендацій по удосконаленню система захисту інформації в банківській установі, обґрунтування варіанту підбору комплекту технічних засобів для створення системи захисту інформації від несанкціонованого доступу

Об’єкт дослідження. Процес обробки інформації в інформаційно-комунікаційних каналах об’єкту фінансової діяльності.

Предмет дослідження. Система захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.

Апробація:

О.О. Тунік, Б.І. Цимбал, В.С. Бойко. Оцінка інформаційних ризиків банківської діяльності. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 03 листопада 2024 року, Київ: РВЦ ДУІКТ. – 024. С.94-95. https://duikt.edu.ua/uploads/p_2661_93669247.pdf

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

ABSTRACT

The qualification work consists of: introduction, three sections, conclusions and a list of sources used. The volume of the work is 79. The list of sources used contains 30 sources.

The purpose of the work is to increase the effectiveness of information protection from unauthorized access at the object of financial activity.

The qualification work considered a banking institution, presented its organizational structure and technical equipment, analyzed the channels of possible information leakage and proposed measures to prevent unauthorized access to information circulating in the banking institution. Information about the banking information system, the main threats of unauthorized access to confidential information of a banking institution were considered.

The result of the work is the development of recommendations for improving the information protection system in a banking institution, substantiation of the option of selecting a set of technical means for creating a system for protecting information from unauthorized access

Object of research. The process of processing information in the information and communication channels of the object of financial activity.

Subject of research. Information protection system against unauthorized access at the financial activity facility.

O.O. Tunik, B.I. Tsymbal, V.S. Boyko. Assessment of information risks of banking activities. All-Ukrainian scientific and practical conference: Current problems of security of information and telecommunication systems. Kyiv, November 3, 2024, Kyiv: RVC DUIKT. – 024. P.94-95.

https://duikt.edu.ua/uploads/p_2661_93669247.pdf

Keywords: ACCESS CONTROL AND MANAGEMENT SYSTEM, INFORMATION PROTECTION DEVICES, INFORMATION PROTECTION, BANKING INSTITUTION, MAIN INFORMATION THREATS OF BANKING INSTITUTION

ЗМІСТ

СПИСОК УМОВНИХ 7
ВСТУП 8
РОЗДІЛ 1. СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ УСТАНОВИ 9
1.1 Банківська систем 9
1.2 Доступ до банківської інформації 15
1.3 Банківська безпека 22
1.4 Канали поширення і витоку інформації 33
1.5 Засоби запобігання витоку інформації 38
1.6 Висновки по розділу 42

РОЗДІЛ 2. ОЦІНКА РИЗИКІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ 44
2.1 Огляд ризиків банківської діяльності та їх характеристика 44
2.2 Оцінка ризиків банківської діяльності 56
2.3 Висновки по розділу 64

РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ УСТАНОВІ З ВИКОРИСТАННЯМ СУЧАСНИХ ЗАСОБІВ 65
3.1 Опис об’єкту банківської діяльності 65
3.2 Вибір та обґрунтування технічних засобів запобігання несанкціонованого доступу до інформації 65
3.3 Склад обладнання проектованої системи контролю і управління доступом банківської установи 72
3.4 Економічний розрахунок 73
3.5 Висновок по розділу 74
ВИСНОВКИ 75
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 76
ДОДАТКИ 78

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 українські банки мають певну систему безпеки своєї діяльності, яку можна розглядати як стійкий стан життя, реалізацію фундаментальних інтересів, основних цілей банків, захист від зовнішніх і внутрішніх дестабілізуючих факторів, гарантія самостійної діяльності. Основним критерієм ефективності банківської безпеки є стабільність економічного та фінансового стану банку.

Враховуючи велику залежність банківської справи від надійності інформаційних технологій, які вона використовує, інформаційна безпека стає одним із фундаментальних принципів банківської системи загалом. Одним з основних напрямків інформаційної безпеки для будь-якої банківської установи є захист банківської таємниці.

Метою роботи є підвищення ефективності захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.

Тому для захисту об’єкту установка СКУД, є найбільш необхідним та важливим в структурах будь-якого приміщення. Добре організований СКУД дозволить вирішувати цілий ряд завдань: контролювати доступ до приміщення, ідентифікувати та управляти користувачами, а також автоматизувати виробничі процеси. Сучасні системи контролю та управління доступом представлені різноманітними технологіями: безконтактні карти, біометричні системи, електронні замки, системи енергозбереження і т.д.

Завданням дипломної роботи є захист інформації в банківських системах з використанням сучасних засобів.

Об’єкт дослідження. Процес обробки інформації в інформаційно-комунікаційних каналах об’єкту фінансової діяльності.

Предмет дослідження. Система захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.

РОЗДІЛ 1.
СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ УСТАНОВИ

1.1 Банківська система

Банки є найважливішим елементом банківської системи країни. У науковому середовищі думки експертів при визначенні терміну банк йдуть від розуміння банку як кредитної установи до визначення банку як фінансового посередника, що пропонує клієнтам (фізичним та юридичним особам) широкий спектр різноманітних фінансових послуг з точки зору зберігання, переказу, валютно-обмінними операціями, продаж золота та інших банківських металів тощо.

В Україні банки є важливою частиною фінансової системи та становлять основу особливої категорії компаній, відомих як «фінансові посередники». Історично українські банки займали домінуюче положення серед інших фінансових посередників і здійснюють більшість фінансових операцій в країні.

Виходячи з цього, слід зазначити, що в сучасних умовах розвитку інформаційної економіки сутність такого явища, як банківська справа, зміниться, а тому необхідно уточнити значення терміну банк. У цьому контексті пропонується таке визначення цього терміна: банк – це юридична особа-фінансовий посередник, що здійснює прямий (контактний) або продаж на відстані (безконтактний) всіх фінансових продуктів клієнтам (іншим юридичним та фізичним особам) та послуги не заборонені законодавством, інші правові операції, спрямовані на досягнення максимальної прибутковості в інтересах їх власників (акціонерів), які підлягають широкому нагляду та контролю з боку центрального банку.

Таке визначення терміну банківської справа звертає вашу увагу: по-перше, на сутність, об'єкт та основну мету банківської діяльності, без детального опису операційної діяльності; по-друге, розширює «класичний» спектр банківських функцій у розвитку інформаційної економіки і, по-третє, підкреслює роль

нагляду та контролю банківської діяльності за допомогою контролюючого органу.

Усі банки країни складають її банківську систему. Банківська система є однією з найважливіших і комплексних структур ринкової економіки і складається з низки різноманітних спеціалізацій та правових форм установ (фінансових посередників), які діють протягом певного періоду в межах єдиної фінансової системи та грошово-кредитного механізму. За іншим визначенням, банківська система — це чітко структурована, законодавчо визначена та підпорядкована група фінансових посередників, які здійснюють конкретну банківську діяльність та функціонально пов’язані в самостійну структуру.

Процес створення сучасної банківської системи, що відповідає умовам ринкової економіки в Україні, триває і триватиме ще довго. Це тому, що українська економіка ще не зазнала необхідної трансформації, вона ще не стала справжньою ринковою.

Проте вже зараз можна стверджувати, що в Україні були створені основи ринкової банківської системи.

Національний банк виконує майже всі функції, притаманні центральному банку ринкової держави. Він використовує такі ринкові інструменти монетарного регулювання, як обов’язкове резервування коштів комерційних банків, політика кредитування та рефінансування комерційних банків, операції з державними цінними паперами на відкритому ринку тощо.

Комерційні банки поступово домінують над методами комерційних банків у країнах, де в системі економічних відносин домінують ринкові принципи.

В останні роки вітчизняна економічна література поповнилася монографічними виданнями, які узагальнюють світовий досвід банківської системи та враховують особливості її становлення в Україні. Зокрема, у серії робіт досить детально розкривається техніка ведення бізнесу комерційних банків. Водночас відсутня навчальна література, яка б розглядала діяльність центрального банку, характер його монетарного регулювання економіки.

Термін «система» часто використовується при вивченні різних явищ природи та суспільного розвитку. Ознакою сучасного мислення вважається системний підхід. Термін «система» часто вживають не лише вчені та філософи, а й діячі культури та мистецтва, організатори виробництва та банківських операцій.

Однак терміни «система» та «банківська система» визначають не лише склад банків. Значення терміну «банківська система» ширше і включає:

- сукупність елементів;
- достатність елементів, що утворюють певну цілісність;
- взаємодія елементів.

Банківська система специфічна, вона виражає властивості, які її характеризують, на відміну від інших систем, що діють у народному господарстві. Своєрідність банківської системи визначається її складовими та зв’язками, що виникають між ними. Тому характер банківської системи впливає на склад і характер окремих її елементів.

У світовій практиці існує кілька типів банківських систем:

- централізована розподільча банківська система;
- ринкова банківська система;
- перехідна система.

На відміну від системи розподільчої, ринкова банківська система характеризується відсутністю державної банківської монополії. Утворити банк може будь-який об'єкт виробництва, будь-якої форми власності (не тільки державний).

В умовах ринкової економіки існує багато банків з децентралізованою системою управління. Між ними розподілені емісійні та кредитні функції. Тема присвячена центральному банку, а кредити компаніям і фізичним особам здійснюють різні комерційні банки: комерційні, інвестиційні, інноваційні, іпотечні, ощадні та інші.

Комерційні банки не відповідають за зобов'язаннями держави, так само як держава не відповідає за зобов'язаннями комерційних банків; Комерційні банки

підпорядковуються раді директорів свого банку, а не адміністративному органу держави.

Тому сучасна банківська система України є перехідною системою. Вона виступає як ринкова модель, яка поділена на два рівні. До першого рівня належать установи Національного банку України, які здійснюють емісію грошових одиниць в обіг (емісію), забезпечують стабільність гривні, здійснюють нагляд і контроль за діяльністю комерційних банків.

Другий рівень складають різноманітні комерційні банки, метою яких є обслуговування клієнтів (компаній, організацій, фізичних осіб) та надання їм різноманітних послуг (кредитні, розрахунково-готівкові, депозитні та обмінні операції). Тому банківська система України перебуває у стані потрясінь. Він включає компоненти ринкової банківської системи, але їх взаємодія ще недостатньо розвинена. Тому у складі емітентів банківської системи та в процесі їх взаємодії необхідно враховувати особливості та умови ринкової економіки.

Діяльність банківських установ та інших суб'єктів господарювання в ринкових умовах носить продуктивний характер. І хоча результати цієї діяльності не отримують безпосереднього матеріалу в традиційному розумінні (наприклад, продукти промисловості чи сільського господарства), вони мають свою цінність через соціальну вартість.

Основним продуктом комерційного банку є різноманітні послуги у вигляді кредитів, розрахунків, управління майном і вартістю, гарантій, індосаментів, консультацій тощо. Основою для цього є торгівля грошима як особливим товаром, передумовою забезпечення економіки достатніми платіжними засобами.

Основні функції комерційних банків мають вирішальне значення для природи банківського продукту. Особливістю діяльності банківських установ є те, що їх продуктом є, з одного боку, надання різноманітних послуг за допомогою активних, пасивних та комісійних посередницьких операцій, а з іншого – створення безготівкових платіжних засобів, які в т.ч. значною мірою це результат тих самих операцій.

Комерційні банки створюють безготівкові засоби платежу в рамках видачі депозитів на основі позик і рахунків клієнтів, що призводить до загального розширення грошової маси. Із зростанням попиту на банківські кредити сучасний механізм емісії дає змогу збільшити кількість грошей, а при зменшенні попиту – зменшити. Тому здатність комерційних банків генерувати гроші є важливою для економіки.

Другу складову банківського продукту складають різноманітні комерційні банківські послуги: депозити, кредити, розрахунки, готівка, інвестиції, довірена особа, валютні, консультаційні та інші. При цьому важливо отримати чіткі термінологічні формулювання для уточнення сутності та особливостей банківського продукту. Результатом банківської діяльності є надання послуг клієнтам. З цією метою банки здійснюють різні види бізнесу. Іншими словами, реальна «послуга» - це кінцевий результат, готовий продукт банку, а «операції» - це його виробничий процес.

Класифікацію цього процесу необхідно проводити з урахуванням особливостей формування та розміщення ресурсів комерційного банку, що зводиться до здійснення трьох великих груп операцій: пасиву, активів та комісіонера. Пасивна торгівля призначена для тимчасового залучення вільних грошей для розвитку ваших ресурсів.

Ведучи активний бізнес, банки вкладають отримані ресурси для отримання прибутку. Комісійні брокерські операції здійснюються банком від імені та на користь клієнта за плату. В останньому йдеться не про формування та розподіл ресурсів, а про переказ коштів від клієнтів, які вже є у банку в їхньому розпорядженні, або інші операції, які безпосередньо не пов’язані з грошовим потоком (так звані послуги поза балансом).

В результаті цих трьох бізнес-груп комерційні банки пропонують своїм клієнтам різноманітні послуги, які разом утворюють банківський продукт. Однак є деякі винятки. Це означає, що пасивні операції в комерційному банку, які здійснюються з метою формування капіталу, а також активні операції в інвестиційній сфері (у визначеному вище терміні) не можуть вважатися

банківським продуктом. Скоріше, це послуги комерційного банку для себе: у першому випадку вони відображають залучення капіталу, а в другому — його пропозицію.

Розвиток новітніх технологій у банківській справі та посилення конкуренції на фінансових ринках спонукають до постійного пошуку нових видів банківських продуктів і, як наслідок, розширення складу банківського бізнесу та збільшення його глобального обсягу. Це виражається у все активнішому проникненні банків у нетрадиційні сфери діяльності (страхування, туризм тощо). Однак, враховуючи поточну різноманітність банківського спектру, кожен з них можна віднести до однієї з трьох визначених груп: пасивного, активного або комісійного брокера.

Загалом результати банківської діяльності є однозначно продуктивними. Проводячи депозитні операції, банки тимчасово акумулюють вільні гроші і перетворюють їх у капітал, тобто «неопераційні» ресурси змушені працювати на благо окремих учасників ринку, а також економіки в цілому.

Використання банківського кредиту у виробництві є необхідною умовою процесу покращення відтворення, а споживчий кредит підвищує платоспроможний попит, що також сприяє економічному зростанню. Своєчасна організація та обробка банками створює умови для безперервної торгівлі та створює можливості для ефективного потоку капіталу в економіку. Реалізація інших банківських послуг також створює умови для нормальної ділової діяльності в різних галузях економіки та забезпечує гідний рівень життя.

Чітке розуміння цих питань особливо важливо з огляду на поширену політичну упередженість щодо «непродуктивної» роботи комерційної банківської системи в нашій країні.

Попередні нормативно-правові акти могли б допомогти подолати негативний стереотип банківських установ як «надбудови» у виробничому секторі національної економіки, оскільки значною мірою залежить усвідомлення громадськістю важливої ролі фінансового ринку та банків як його основних суб’єктів. Міра успішності заходів щодо подолання економічної рецесії та

формування всебічного розвитку повноцінної ринкової економіки, здатної гарантувати гідний рівень життя в Україні та наблизити її до економічно розвинутих країн світу.

Ключовою функцією банківської системи є її здатність маніпулювати грошовими потоками відповідно до потреб економіки. Кожен банк видає платіжні засоби. У банківській системі цей потенціал є більш суттєвим і розширеним. Випуск валюти має значний вплив на стабільність грошової маси та ефективність виробництва й обігу товарів.

Центральний банк здійснює первинну емісію шляхом видачі готівки, позик уряду та комерційним банкам, купівлі акцій, золота та іноземної валюти. Комерційні банки здійснюють вторинні випуски за допомогою позичково-розрахункових операцій, де банки збільшують свої кошти за допомогою механізму мультиплікації.

Виконання функцій гарантується відповідними законами та нормативно-правовими актами, що регулюють роботу всіх ланок банківської системи та створенням відповідного механізму контролю та контролю за дотриманням чинного законодавства та банківських операцій.

1.2 Доступ до банківської інформації

Інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Суб'єкт відносин у сфері інформації може вимагати усунення порушень його права та відшкодування майнової і моральної шкоди, завданої такими правопорушеннями.[4] Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.[5]

Для уточнення терміну «банківська інформація» необхідно визначити тих осіб, які уповноважені здійснювати діяльність, пов’язану з розкриттям інформації, і на цій підставі визначити органи, на які покладається здійснення діяльності, пов’язаної з обігом банківської інформації. Відповідно до ст. 7 Закону України «Про інформацію», суб’єктами, тобто особами, які потенційно можуть

бути учасниками інформаційних відносин, є: громадяни України, юридичні особи, держава. Крім того, аналіз цього закону дозволяє іншим державам, їх громадянам та юридичним особам, міжнародним організаціям та особам без громадянства бути також об’єктом інформаційних відносин. А учасниками інформаційних відносин є безпосередні громадяни, юридичні особи або держава, які набувають прав та обов'язків, передбачених законом у контексті інформаційної діяльності. Стаття 42 встановлено, що основними учасниками інформаційних відносин є: автори, споживачі, розповсюджувачі, зберігачі інформації. При цьому під Законом України «Про інформацію» розуміється інформаційна діяльність як комплекс заходів, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб та держави.

Основними видами інформаційної діяльності чинне законодавство розглядає отримання, використання, поширення та зберігання інформації. Отримання інформації — це набуття, придбання, накопичення відповідно до чинного законодавства України документально оформленої або публічно оприлюдненої інформації громадянами, юридичними особами або державою. Використання інформації служить задоволенню інформаційних потреб громадян, юридичних осіб та держави. Розповсюдження інформації – це поширення, оприлюднення, продаж документованої або публічно оприлюдненої інформації відповідно до вимог законодавства. Зберігання інформації служить для забезпечення належного стану інформації та її матеріального забезпечення.

Аналіз чинного законодавства в Україні показує, що існує два основних види інформації, а саме інформація відкритого доступу та інформація з обмеженим доступом. Доступ до відкритої інформації гарантується: її систематичним опублікуванням в офіційних друкованих виданнях (бюлетені, збірники); його поширення через засоби масової інформації; надання безпосереднього доступу зацікавленим громадянам, державним органам та юридичним особам.

Інформація з обмеженим доступом відповідно до її правових норм поділяється на конфіденційну та таємну. Таким чином, під конфіденційною

інформацією розуміється інформація, яка знаходиться у володінні, користуванні чи розпорядженні фізичними або юридичними особами і будуть розповсюджуватися на ваш запит відповідно до встановлених ними умов. А таємна інформація визначається як інформація, що містить відомості, що становлять державну та іншу передбачену законом таємницю, розголошення якої є шкідливим для особи, суспільства та держави.

На основі вищезазначених основних положень щодо інформаційної діяльності, закріплених чинним законодавством України, спробуємо дати визначення терміну «банківська інформація», виділити ознаки та виділити її види.

Дивлячись на визначення інформації як документованої або публічно оприлюдненої інформації про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі, виникає питання, яку інформацію, події чи явища слід вважати банківською інформацією. Перш за все, слід зазначити, що інформація, яка може бути визнана банком, має бути пов’язана з діяльністю цієї компанії як банку. Оскільки банк є юридичною особою, яка за ліцензією Національного банку України має виключне право здійснювати поєднання таких операцій: залучати вклади фізичних та юридичних осіб та розміщувати ці кошти на своє ім’я, на власних умовах та на власний ризик відкриття та обслуговування банківських рахунків фізичних та юридичних осіб. Банківська справа – це запит коштів у фізичних та юридичних осіб та розміщення зазначених коштів на своє ім’я, на їх умовах та на власний ризик, відкриваючи та ведучи банківські рахунки фізичних та юридичних осіб, можна зробити висновок, що інформація, яка кваліфікується як банківська, має стосуватися діяльності банків, які здійснюють банківську діяльність. При цьому об’єктивується документування відомостей у нормативно-правових документах банківських установ, документах, що підтверджують факт здійснення банківських операцій, документах, що підтверджують здійснення операцій, не заборонених законом, та ін. Рекламна інформація, що розповсюджується банківською установою за власною ініціативою, вважається оприлюдненою.

У світлі цього поняття «банківська інформація» може бути визначена як інформація, що міститься в банківських документах або оприлюднена банківською установою у порядку, встановленому чинним законодавством України, та пов’язана з її діяльністю в її банківських операціях.

Враховуючи, що основними видами інформаційної діяльності, чинне законодавство визнає отримання, використання, поширення та зберігання інформації, а також те, що основними видами інформаційної діяльності у сфері банківської інформації є отримання банківської інформації, використання банківської інформації, розповсюдження та зберігання банківської інформації.

Виходячи з визначення поняття «банківська діяльність», отримання банківської інформації можна визначити як діяльність банківської установи, в якій здійснюється збір інформації, пов’язаної з банківською інформацією. Використання банківської інформації – це процес задоволення інформаційних потреб зацікавлених осіб у порядку, встановленому чинним законодавством України, шляхом ознайомлення з банківською інформацією. Розповсюдження банківської інформації – це процес розповсюдження банківської інформації серед зацікавлених осіб у порядку, встановленому чинним законодавством України. Зберігання банківських даних є обов’язком, покладеним чинним законодавством України на органи, уповноважені поширювати банківські дані, лише у випадках, прямо передбачених законом.

Слід також зазначити, що, оскільки банківська справа є діяльністю, яка розвивається та вдосконалюється, можна продовжити попередній перелік інформації, що стосується банківської справи. Однак із вищесказаного можна зробити висновок, що до категорії банківської інформації відноситься інформація, яка має інший спосіб доступу та має певні характеристики діяльності. Очевидно, що банк сам зацікавлений у поширенні одних відомостей як учасник банківських відносин, у випадку інших банківська установа зобов’язана зберігати та захищати цю інформацію.

З цього можна зробити висновок, що при здійсненні банківської діяльності банківська установа працює з двома видами інформації, а саме:

- відкрита банківська інформація;

- Банківська інформація з обмеженим доступом.

Аналіз чинного банківського законодавства в Україні свідчить про те, що відкрита банківська інформація може містити інформацію, що стосується діяльності банківських установ, і не вважається банківською таємницею. Такою інформацією може бути інформація, у розкритті якої зацікавлений банк, та інформація, яку банк зобов'язаний розкрити.

Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку, є банківською таємницею.[6]

Зокрема, банківська таємниця – це:

- відомості про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;

- операції, що здійснюються для або від імені клієнта;

- економічне та фінансове становище клієнтів;

- банківські системи та системи захисту клієнтів;

- відомості про організаційно-правову структуру юридичної особи: клієнт, його керівник, діяльність;

- Інформація про комерційну діяльність клієнтів або комерційну таємницю, проекти, винаходи, зразки продукції та іншу комерційну інформацію;

- відомості про окремі банківські звіти, за винятком тих, що підлягають оприлюдненню;

- коди, які використовуються банками для захисту інформації;

- інформація про особу, яка має намір укласти договір споживчого кредиту, отримана шляхом перевірки кредитоспроможності.

Інформація про банки або клієнтів, зібрана в рамках банківського нагляду, є банківською таємницею.

Інформація про банки або клієнтів, яку Національний банк України отримує від органу банківського нагляду іншої країни на підставі міжнародного договору або відповідно до принципу взаємності для використання в

банківському нагляді або задля запобіганню відмиванню грошей або фінансування тероризму – це являється банківською таємницею. Положення статті не поширюються на інформацію, що підлягає опублікуванню. Перелік інформації, яка підлягає оприлюдненню, складається Національним банком України, а також самим банком на власний розсуд.

Національний банк України видає нормативно-правові акти з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, та надає роз'яснення щодо застосування таких актів.[6]

Комерційна таємниця повинна включати відомості, що характеризують нові банківські технології, роботу у сфері нових послуг, плани розвитку банку його мережі та іншу інформацію про прибуток.

Склад і обсяг відомостей, що становлять комерційну таємницю, а також порядок її захисту визначаються директором банку самостійно з урахуванням вимог Постанови Кабінету Міністрів України № 611 від 09.08.93р. "Про перелік відомостей, що не складають комерційну таємницю".

Розголошення інформації, що становить комерційну таємницю, є важливою частиною системи заходів банку щодо захисту вашої фінансової безпеки. І ми повинні враховувати такі характеристики інформації, яка віднесена до комерційної таємниці:

- не є державною таємницею;
- не підпадає під положення постанови Кабінету Міністрів України №611 від 09.08.93р.;
- не містить відомої інформації;
- належать банку та підключені до банківського виробництва;
- має будь-яке значення або потенціал для розвитку банку;
- має систему розповсюдження прав доступу;
- містить інформацію про технологію, виробництво, управління та операції банку.

Методика віднесення певної інформації до комерційної таємниці в нашій країні ще не розроблена.

Правила про комерційну таємницю та порядок доступу до них можуть складатися з розділів:

- права та обов'язки посадових осіб щодо доступу виконавців до документів та інформації, що містять комерційну таємницю;

- права та обов'язки відділів безпеки банку щодо доступу співробітників до документів, що містять комерційну таємницю;

- повноваження посадових осіб на доступ до документів, що містять комерційну таємницю;

- зареєструвати доступ виконавців до документів та відомостей, що містять комерційну таємницю;

- порядок надання документів, що містять комерційну таємницю;

- процедури доступу до секретної інформації;

- порядок доступу виконавців до документів оперативної кореспонденції;

- порядок розмноження та розсилання документів, що становлять комерційну таємницю, для зовнішніх організацій;

- порядок доступу до документів, що містять комерційну таємницю розголошених осіб;

- порядок доступу до нарад і конференцій, на яких обговорюються питання комерційної таємниці банку.

Встановлення достовірності інформації, яка є комерційною таємницею, дуже важливо, оскільки це допоможе знизити витрати на її захист.

Отже, з вищесказаного можна зробити наступні висновки.

Банківська інформація – інформація, що міститься в банківських документах або оприлюднена банківською установою в порядку, встановленому чинним законодавством України, та пов’язана з її діяльністю в її банківських операціях.

Залежно від режиму доступу ви можете розрізняти банківські реквізити з відкритим доступом і банківські реквізити з обмеженим доступом. Банківську інформацію з відкритим доступом, у свою чергу, можна поділити на банківську інформацію, у розголошенні якої зацікавлений банк, та банківську інформацію,

за розкриття якої несе від Канали поширення і витоку інформації повідальність банк.

1.3 Банківська безпека

Політика інформаційної безпеки банку включає: знання всіх інформаційних потоків; зрозуміти структуру інформації в системі; призначення критичних процесів (технічний захист), областей в інформаційних системах; розподіл користувачів на категорії та групи з чітким визначенням їхніх прав; можливість зафіксувати факт несанкціонованого доступу або атаки.

Оскільки основним каналом несанкціонованого доступу є комп'ютерна мережа (банківська, корпоративна, глобальна), то основна увага приділяється системі безпеки на рівні підтримки мережі (роутер, брандмауери, FTP, електронна пошта, мережева файлова система, браузер тощо).

Слабкими місцями мережевої інфраструктури є незахищені канали зв'язку з можливістю неіснуючих платежів, перехоплення та несанкціонованого використання платіжних даних, інших проявів шахрайства та зловживань. Такі випадки траплялися в Інтернеті. Є дві можливості захисту передачі інформації: ізоляція платіжної мережі, тобто використання приватних мереж, і шифрування даних.

Сучасні криптографічні системи базуються на наступних ідеях:

- діапазон значень ключа шифрування повинен бути таким, щоб ваш звичайний пошук в сучасних комп'ютерних техніках був неефективним (на це йшли місяці, роки, іншими словами, швидке розшифрування вимагає нескінченних ресурсів комп'ютера);

- вартість ресурсів, що використовуються для розшифровки даних без знання ключа, не може бути меншою за вартість самих даних;

- секретний алгоритм шифрування (дешифрування), ключ шифрування;

- навіть незначні зміни даних (до шифрування) або самого ключа шифрування повинні призвести до значних змін у зашифрованому файлі даних (таким чином, у процесі шифрування не можна буде розпізнати шаблон).

Із загальних рекомендацій (принципів) теорії інформації випливає, що при меншій надлишковості (ентропії) даних для шифрування зменшується також довжина ключа і навпаки. Тому особливо необхідно зашифрувати та попередньо заархівувати дані.

Алгоритми шифрування поділяються на:

- власне шифри, які розглядають дані як набір бітів незалежно від їх лексичної структури;

- спеціальні коди, що враховують лексичну структуру даних (на практиці це тексти), виділення слів, словосполучень тощо.

У системах електронної комерції всі транзакції (наприклад, платежі) є досить короткими та мають просту структуру, яка очевидна для таких даних, атрибутів платежу, банківських рахунків тощо. Тому коротку та прозору інформацію легше розшифрувати в її структурі. . Упакування цих транзакцій дозволяє легко уникнути природної «структури» даних. Така ситуація типова для архітектури клієнт-сервер з віддаленим доступом до бази даних. Майже всі бази даних компанії є реляційними. Результатом реляційного запиту (на основі SQL-запиту, як це відбувається на практиці) знову буде відношення (таблиця), тобто добре структуровані дані. Хороші системи шифрування повинні враховувати цю властивість.

Методи шифрування поділяються на 2 основні групи.

Симетричні процедури засновані на принципі, що сторони, що надсилає (шифрує) і отримує (дешифрує), використовують ключ. Зрозуміло, що тривале використання ключа збільшує ризик розпізнавання ключа; Тому його слід регулярно міняти. Ця ситуація сама по собі представляє проблему, коли новий ключ потрібно передати віддаленій системі або людині, тобто зміна є важливою операцією. Симетричні методи найчастіше використовуються для шифрування файлових систем і менш підходять для таких систем, як електронна пошта.

Урядові та військові органи використовують лише методи симетричного шифрування.

Якийсь симетричний метод також використовується, коли ключ розбивається на дві частини, кожна з яких не дозволяє розшифрувати дані, що загалом підвищує надійність секрету ключа. Типові алгоритми симетричного шифрування: DES, Triple DES, IDEA, B-Crypt, Lucifer, Skpjack, FEAL-1, RC2, RC4.

Асиметричні процедури або (стандартні) процедури з відкритим (загальним) ключем використовуються за такою схемою:

- У одержувача є 2 ключі, які неможливо отримати один від одного: відкритий і закритий. Відкритий ключ вільно поширюється (навіть публікується, публікується на веб-сайтах);

- відправник шифрує дані відкритим ключем; секретний секретний ключ знає тільки система шифрування;

- сторона-отримувач розшифровує отримані дані та зашифровує їх за допомогою приватного ключа.

Асиметричні алгоритми пропонують значну економію (до мільйонів доларів) на запуску служб безпеки для великих банків і корпорацій. Симетрична робота з відносно короткими клавішами, асиметрична, з довгими клавішами. Тому симетричні методи швидші (приблизно в 1000 разів). На практиці також використовуються змішані методи шифрування.

Шифрування файлів також використовується для підтвердження того, що автор не змінював і не створював файли. Ця техніка називається цифровим підписом. Останні можуть супроводжувати як зашифровані, так і відкриті повідомлення. Цифровий підпис повинен гарантувати: авторство, тобто його не можна підробити або використовувати повторно; неможливо змінити «підписаний» документ.

Загальновизнано, що асиметричні алгоритми шифрування пропонують більш високий рівень надійності та безпеки. Найпоширенішим є шифрування з відкритим ключем. Для розшифровки використовуються секретні ключі.

Кількість можливих комбінацій, які підходять для розшифровки інформації, зашифрованої відкритим ключем, залежить від довжини ключа в бітах. Використання більш довгих послідовностей у ключовій функції дозволяє передбачити можливості сучасних комп'ютерів і забезпечити надійний захист критичної інформації. Донедавна найпоширенішим використанням 40-бітних ключів в Інтернеті був захист інформації. Однак ці ключі виявити було легко (слід зазначити, що використання такого ненадійного інструменту стало результатом дуже жорстких обмежень на експорт високопродуктивних засобів шифрування зі Сполучених Штатів). В даний час в Інтернеті широко поширені ключі розміром 1024 біт або навіть більше, що робить їх практично невпізнанними.

Важливим завданням платіжних систем є ідентифікація учасників платежу (аутентифікація). Це зроблено для обмеження доступу до платіжних інструментів, надання права на цей доступ лише їх власникам, а також для того, щоб сповіщення отримували лише ті, кому спрямована платіжна операція. Довірена аутентифікація також сприяє підвищенню взаємної довіри між учасниками електронної комерції. Зараз в Інтернеті використовується широкий спектр засобів аутентифікації. Це включає персональний ідентифікаційний код (PIN), який необхідно ввести перед здійсненням фінансової операції. Але невелика довжина таких кодів дозволяє шахраям легко обійти ці методи захисту.

Для захисту більш ефективним є використання комп'ютерних паролів, які є довшими та складнішими, тому їх важко вгадати. Цей метод широко використовується в Інтернеті, оскільки він контролює доступ до локальних систем за допомогою паролів, але надійний результат можна отримати лише за умови його правильного використання.

Технологія цифрових сертифікатів ідентифікує користувача при доступі до даних через різні мережі. У програмах електронної комерції користувачі реєструють свої цифрові сертифікати в банку, який випускає кредитні картки. Щоразу, коли користувач намагається здійснити транзакцію, браузер, який

використовує протокол Secure Electronic Transaction (SET), надсилає копію сертифіката продавцеві, щоб перевірити дійсність кредитної картки користувача.

SET — це процедурна та технологічна, розроблена Visa і MasterCard. Протокол підтримується Verisign, Cybercash і First Virtual, які контролюють повноваження користувачів для продавців і банків. SET є основним протоколом безпеки для використання банківських карт на WWW, але це лише специфікація, а не повний продукт для безпеки.

Ще одним важливим елементом захисту є технологія шифрування. Він заснований на додаванні відкритих і закритих ключів, які використовуються, коли відправник (користувач) передає (отримує) дані для кодування та декодування даних. Алгоритми кодування використовуються в смарт-картках, кредитних картках із закодованим процесором або випадково згенерованим кодом, налаштованим для користувачів.

Відсутність протоколу забезпечення безпеки розрахунків пластиковими картками вже давно є основною перешкодою для розвитку електронної комерції. І лише влітку 1997 року довгоочікуваний протокол було остаточно узгоджено.

Його створенню передувала розробка ряду більш-менш поширених методів захисту фінансової інформації. Де-факто стандартом є протокол SSL (Security Socket Layer), який забезпечує шифрування інформації на рівні каналу на основі алгоритму RSA. Він сумісний з популярними веб-браузерами. Часто використовуються такі протоколи, як S/MIME і S-HTTP. Проте всі вони мають одну спільну рису: вони не дозволяють ідентифікувати особу покупця чи продавця.

Через відсутність єдиного стандарту з’явилося багато закритих власних протоколів шифрування для фінансових операцій з різним ступенем стабільності. Усі вони не відповідали головній вимозі, що відображає специфіку Інтернету: вимозі відкритості. Ситуація змінилася лише з приходом протоколу SET. Він дозволяє здійснювати безпечні платежі пластиковими картками у відкритих мережах. Розробка SET почалася в 1996 році, а в червні 1997 року були опубліковані специфікації його останньої версії SET 1.0. Сьогодні по всьому

світу існують десятки систем електронної комерції, які працюють на основі протоколу SET і пов’язують сотні банків, магазинів і процесингових центрів.

Протокол SET є основним протоколом інформаційної безпеки. Підтримка набору більшості платіжних систем (VISA, EuroCard, MasterCard, American Express, Diners Club, JCB, Cyber Cash і Digi Cash) і основних IT-груп (AT&T, HP, IBM, Microsoft, Northen Telekom, RSA) автоматично користується високою довірою мільйонів клієнтів.

Протокол пропонує:

- конфіденційність інформації, що передається та отримується за допомогою одночасного використання кількох алгоритмів шифрування та системи цифрових сертифікатів. Цифрові сертифікати видаються спеціальними органами (органами сертифікації) покупцям, продавцям і фінансовим центрам людей або компаній;

- гарантувати цілісність переданої інформації;

- взаємна автентифікація покупця та продавця. Покупець може бути впевнений, що продавець саме той, за кого себе видає, і має право прийняти його картку до оплати. Продавець має можливість переконатися, що власник картки є законним користувачем номера рахунку, прив’язаного до платіжної картки;

- сумісність шляхом поєднання продуктів SET від різних виробників, що працюють на будь-якій апаратній та програмній платформі;

- надійність обміну даними незалежно від механізмів безпеки, які використовуються в каналі зв'язку.

Стандарт регламентує прийом і форматування цифрових сертифікатів, форм замовлень і авторизованих повідомлень, порядок обміну повідомленнями та використання алгоритмів шифрування. Інші деталі реалізації залежать від розробників конкретних програм. Слід зазначити, що протокол SET дозволяє використовувати різні методи шифрування інформації, які визначені регіональними стандартами та відповідають вимогам протоколу.

Дуже ефективним засобом захисту є електронний підпис. Його використання вимагає, щоб той, хто перевіряє цей підпис, мав відкритий ключ,

який відповідає особистому ключу (підпису), який використовується відправником електронного документа. Однак отримання зазначеного відкритого ключа не виключає шахрайства, яке призводить до передачі підробленого відкритого ключа, який автентифікує підроблені повідомлення. Щоб цього уникнути, використовується практика сертифікації (підтвердження) відкритих ключів уповноваженою та довіреною установою чи організацією. Зазначена установа або організація називається сертифікатором і використовує свій електронний підпис у відкритих ключах, які надаються користувачам платіжної системи. Відкритий ключ центру сертифікації має надаватися через надійно захищені канали. Ця установа сертифікує відкриті ключі учасників системи тільки після того, як їх ідентичність буде перевірена за допомогою захищених каналів або інших процедур, які гарантують достатній рівень безпеки, і тільки ті відкриті ключі, які були підтверджені, вважаються дійсними.

Захист банківської інформації в СЕП включає ряд заходів, пов'язаних із шифруванням інформації, яка циркулює в платіжній системі. Шифруванню підлягають усі файли СЕП: початкові та платіжні файли, файли квитанцій, файли звітів, файли лімітів, відповідні файли виписок, файли офіційної інформації.

Перед виходом з банку всі платіжні документи СЕП обробляються за допомогою апаратно-програмного забезпечення захисту інформації, що забезпечує відповідність наступним вимогам інформаційної безпеки:

- інформація, що передається, має бути закритою, тобто повідомлення можуть прочитати лише ті, кому воно адресоване;

- цілісність: під час прийому виявляється випадкове або навмисне пошкодження повідомлення на етапі його передачі;

- автентичність відправника (при отриманні повідомлення можна чітко визначити, хто його надіслав).

Крім основних вимог, зазначених вище, необхідно провести ряд допоміжних заходів, які дозволять більш детально проаналізувати можливі нетипові ситуації:

- засобом захисту інформації є зашифрований арбітражний журнал, в якому зберігаються записи обробки інформації, а також вміст оброблених файлів;

- зашифроване повідомлення містить поля для дати та часу обробки.

Найважливішим засобом захисту інформації СЕП є апаратне забезпечення. Таємність ключів, що містяться в ньому, технічно гарантується:

– ключі зберігаються на спеціальній електронній картці, прочитати їх можна лише за допомогою спеціального блоку, який виконує процес шифрування інформації. Читати ключі іншим способом неможливо;

- електронна картка видається банку з тимчасовим посиланням на певний блок шифрування цього ж банку; втрачена або вкрадена картка не працює в іншому блоці шифру (наприклад, на комп'ютері іншого банку);

- у разі викрадення як пристрою, так і картки в конкретному банку, передбачено виключення цього пристрою зі списку користувачів СЕП; Після вирішення юридичних та фінансових проблем, пов'язаних із втратою обладнання та отриманням нового комплексу, банк може продовжити роботу з СЕП.

Найслабшим з точки зору безпеки є зона підготовки платежів працівниками банку, які беруть участь у СЕП. Усі більш-менш успішні зареєстровані спроби НСД були зроблені представниками банків, що призводило до розкрадання коштів з власного банку, а не з державного чи інших банків. У всіх цих випадках одержувачі НСД мали легальний доступ до системи захисту та обробки платіжної інформації та були перевищені їхні повноваження (доступ до багатьох або навіть усіх банківських ресурсів банку).

Апаратно-програмні засоби криптографічного захисту інформації в СЕП забезпечують автентифікацію одержувача та відправника міжбанківських електронних облікових документів та офіційних повідомлень СЕП, гарантують їх достовірність і цілісність від неможливості фальсифікації або фальсифікації документів у зашифрованому вигляді або за наявності ЕЦП.

Криптографічний захист інформації має охоплювати всі етапи обробки електронних банківських документів від моменту їх створення до моменту їх зберігання в архіві банку. Використання різних криптографічних алгоритмів на різних етапах обробки електронних банківських документів дозволяє забезпечити безперервний захист інформації в інформаційній мережі, а також роздільну обробку інформації для різних комп'ютерних завдань Національного банку.

Основною метою криптографічного захисту інформації є гарантування конфіденційності та цілісності електронної банківської інформації, а також сувора аутентифікація учасників СЕП та спеціалістів банківських установ, які беруть участь у створенні та обробці електронних банківських документів.

Для забезпечення вирішення завдань жорсткої аутентифікації банківських установ, підключених до інформаційної мережі, розроблено систему ідентифікації користувачів, яка є основою системи розподілу ключів криптографічного захисту.

З точки зору захисту інформації, кожна банківська установа має ідентифікатор довжиною трьох байтів, першим символом якого є літера відповідної території, на якій розташована банківська установа; другий і третій символи є унікальним ідентифікатором банківської установи в цій області. Ці ідентифікатори збігаються з адресами в системі ЕП і є унікальними в українській банківській системі.

Трибайтні ідентифікатори є основою для визначення робочих місць у банківських установах та ключовими ідентифікаторами для всіх робочих місць у банківській установі. Ідентифікатор ключа роботи складається з шести цифр, з яких перші три – ідентифікатор банку, четверта – тип роботи (оператор, бухгалтер тощо), а п'ята та шоста – ідентифікатор конкретної роботи (тобто , для обробки посадових осіб, відповідальних за платіжну інформацію на цьому робочому місці). Трибайтний ідентифікатор банку вбудований у програму генерації ключів і не може бути змінений в банку, захищаючи від підробки ключів з боку інших банків.

Відповідні ідентифікатори ключів записуються на електронних картках, які є носіями ключової інформації для апаратного шифрування.

З метою забезпечення захисту інформації від змін і, водночас, суворої аутентифікації та постійного захисту платіжної інформації з моменту її створення, система захисту СЕП та інших інформаційних завдань включає механізми навчання/верифікації ЕЦП на основі асиметричного RSA алгоритму.

Для забезпечення роботи цього алгоритму кожна банківська установа отримує від служб захисту інформації місцевої влади генератор персональних ключів із вбудованим ідентифікатором цієї банківської установи. За допомогою цього генератора ключів банк може генерувати ключі для всіх робочих станцій, які працюють з електронними банківськими документами. Щоб гарантувати захист ключової інформації (тобто відкритих ключів) від підробок та підробок, відкриті ключі ЕЦП необхідно надіслати до служби захисту інформації Національного банку для сертифікації (за винятком ключів для роботи оператора та інших, які використовуються тільки в САБ).

Технологія накладання/верифікації ЕЦП в СЕП розроблена таким чином, що посадова особа не може надіслати електронний міжбанківський розрахунковий документ. При створенні електронного міжбанківського розрахункового ваучера на робочому місці оператора посадова особа, яка створила цей документ, повинна накласти на документ ЕЦП зі своїм секретним ключем. При створенні файлу з електронними міжбанківськими бухгалтерськими документами на АРМ бухгалтера на цей файл накладається ЕЦП, що забезпечує захист від змін до всього файлу. Сформований таким чином платіжний файл обробляється АРМ-НБУ, при цьому ЕЦП оператора перевіряється в кожному міжбанківському електронному розрахунковому документі та накладається на ЕЦП АРМ-НБУ, яку можуть перевірити всі банківські установи, які беруть участь у СЕП. При обробці платіжних файлів на АРМ-2 перевіряються підписи всього файлу і після створення відповідних платіжних файлів ЕЦП застосовується до всього файлу із секретним ключем файлу АРМ-2.

При генеруванні ключів секретний ключ записується на дискету або картку пам'яті. Відкриті ключі, які використовуються в банку (наприклад, ключ оператора), записуються в іменований каталог як файли змін у таблиці відкритих ключів. Відкриті ключі АРМ, електронний цифровий підпис яких перевірено в СЕП, а саме відкриті ключі АРМ-3 та АРМ лічильника, записуються у вигляді файлів атестації у зазначеному довіднику. Ці файли подаються до Служби захисту інформації НБУ для сертифікації, щоб перед розповсюдженням через СЕП ви могли переконатися, що вони належать цьому абоненту СЕП і що вони не були створені кимось іншим від імені цього абонента та що всі вимоги до відкритого ключа алгоритму СЕП. Після успішної сертифікації відкриті ключі учасника СЕП надсилаються на робочу станцію у вигляді файлів змін у таблицях відкритих ключів на основі технології перевірки електронного підпису (АРМ-3 та АРМ-2).

Правові основи та нормативні документи НБУ мають створити правове середовище для захисту електронних міжбанківських розрахунків із визначенням юридичних осіб та осіб, відповідальних за операції в системі, прав та обов’язків учасників системи. , гарантія транзакцій і конфіденційність інформації в обігу, що пропонується в системі. Особлива увага в нормативних документах НБУ та підзаконних актах приділяється розгляду спірних питань і порядку ведення арбітражних справ між учасниками системи електронних міжбанківських розрахунків, опису обов'язків учасників системи щодо збереження та своєчасного надання арбітражної інформації, яка створюється засобами криптозахисту програмних комплексів системи та зберігається зашифрованою.[11]

Нормативними документами НБУ визначено низку адміністративних заходів, спрямованих на гарантування захисту підготовки, передачі, обробки та зберігання інформації про електронні фінансові операції для кожного учасника системи; Визначені правила доступу та фізичного захисту вузлів збору, обробки та зберігання даних. Положення НБУ також регламентують генерацію, передачу, розповсюдження, оновлення та використання ключів криптографічного захисту

в системі. Спеціальні інструкції НБУ суворо регламентують порядок роботи спеціалістів банківських установ із засобами захисту, використання та зберігання криптографічних ключів, розподіл повноважень з питань захисту інформації в банківській установі.

На основних вузлах збору, обробки та зберігання інформації в системі (центральний розрахунковий центр, регіональні розрахункові центри тощо) слід вжити заходів щодо захисту інформації від витоку інформації через технічні канали. У всіх приміщеннях, де розташовані сервери системи, в тому числі телекомунікаційні, дотримання певних організаційно-технічних заходів щодо процедури перевірки цих приміщень для контролю витоку інформації через технічні канали (лінії електропередач, заземлення, допоміжне технічне обладнання, електромагнітне випромінювання комп'ютера) постійно контролюється. Особливі вимоги до дотримання умов режиму в об’єктах банківських установ-учасників СЕП, де обробляються, експлуатуються та зберігаються засоби захисту, встановлені «Положенням про міжбанківський процесинг в Україні» та обов’язкові для виконання всіма банківськими установами. Усі посадові особи, які здійснюють електронні розрахунки, повинні суворо дотримуватися цих вимог. Відповідальність за дотримання зазначених вимог покладається на директорів банківських установ.

1.4 Канали поширення і витоку інформації

Витоком інформації вважається незаконне поширення інформації, що виходить за межі кола довірених осіб або організації, яка зберігала цю інформацію. Витік — це незаконне вилучення інформації у третіх осіб, незалежно від того, як дані були отримані.

Витік інформації може статися в результаті випадкового розкриття даних або коли зловмисник спеціально намагається шпигувати за чужою інформацією, яка прихована від сторонніх осіб.

Що стосується термінології, то слід розрізняти витік інформації та перехоплення. Перехоплення є незаконним способом отримання інформації

технічними засобами. Витік інформації – це її втрата, коли вона поширюється через канали зв’язку та фізичний простір з різного роду причин, включаючи перехоплення та перенаправлення. Навмисно створений витік інформації через технічні канали передбачає встановлення на шляху її поширення різних пристроїв, які її перехоплюють.

Цей термін частіше вживається в професійній сфері, на практиці це визначення стосується всіх видів витоків, заснованих як на людських, так і на технічних факторах. Найпоширенішим методом крадіжки є незаконний акт запису інформації, що містить захищену законом таємницю, на зовнішньому носії та вилучення її з корпоративного середовища. Сучасні системи DLP налаштовані насамперед для загроз від корпоративного користувача, а не для зовнішніх атак.

Прикладом такої ситуації стала ситуація, коли група Google подала до суду на Uber, який найняв колишнього співробітника компанії. Топ-менеджер незаконно скопіював майже всі дані про розробку безпілотного автомобіля під його керівництвом. Система безпеки, яка існує в одній з найбільших корпорацій світу, не змогла запобігти крадіжці інформації одним із її топ-менеджерів. При цьому судові перспективи відшкодування завданих збитків туманні, оскільки, вочевидь, не було досягнуто згоди між підприємством та працівником, що визначатиме механізм відшкодування у цій справі. Uber був обраний відповідачем і став бенефіціаром крадіжки. Можливо, файли були повернуті, але інформація, яку вони містили, могла бути використана для отримання конкурентної переваги.

Цей випадок говорить про те, що незалежно від рівня компанії, ризик втрати інформації однаковий для всіх.

Найпоширенішими причинами витоку інформації є такі версії:

- неналежний захист даних інших людей (організацією або довіреною особою);

- неналежне поводження з пристроями, які зберігають інформацію (з технічних причин).

Все це відбувається за умов, які дозволяють виникнути ситуації витоку:

- некомпетентність персоналу із захисту даних, нерозуміння ним важливості процесу та недбале поводження з інформацією загалом;

- використання неліцензійних інструментів або несертифікованих програм для захисту клієнтів та збереження їх конфіденційності;

- низький рівень контролю за засобами захисту інформації;

- постійна зміна працівників, які займаються захистом персональних даних.

Дуже часто провину за витік інформації покладають на співробітників компанії та їх керівників. Ви можете захистити себе від будь-якого зловмисника, якщо ваш персонал готовий і обізнаний. Є фактори, які не залежать від компанії:

- великі катастрофи;

- стихійні лиха;

- аварії на технічних станціях, вихід з ладу обладнання;

- погані погодні умови.

Системи зв'язку служать основою для передачі інформації будь-якого роду. Найпростіші системи складаються з носія інформації, приймача та одержувача інформації, а також каналу передачі. Кожен сигнал може передаватися наступними способами:

- світлові промені;

- метод електромагнітної передачі;

- звукові хвилі;

Основне завдання всієї ланцюжка пристроїв - передавати інформацію в конкретну точку без спотворень. Ряд пристроїв, які використовуються для передачі інформації називають системою зв'язку, а частина, яка передає інформацію, називається каналом передачі даних.

Кожен канал передачі інформації має ряд властивостей:

- положення початку і кінця;

- форма передачі інформації;

- компоненти або структура каналу;

- швидкість, кількість відправки та отримання даних;

- тип каналу та спосіб передачі (як перетворюється сигнал);

- продуктивність ланцюга;

- пропускна здатність каналу.

Ці системи і канали використовуються саме для передачі інформації. Однак бувають випадки, коли канал з’являється в іншому місці, він не є явним, і тому його називають каналом витоку інформації. Канал з'являється незалежно від джерела інформації та способу передачі.

Існує чотири основні групи технічних методів організації витоку інформації:

- візуальний, що дозволяє перехопити або копіювати інформацію у візуальній формі, йдеться про документи, інформацію, яка відображається на моніторі комп’ютера;

- акустично слухати переговори або телефонні розмови, що відбуваються в кімнаті;

- електромагнітний, дозволяє приймати дані, виражені у вигляді випромінювання електромагнітних хвиль, декодування яких також може надати необхідну інформацію;

- матеріали, пов'язані з аналізом об'єктів, документів і відходів, отриманих від діяльності компанії.

У будь-якому випадку технічного каналу витоку конкуренти використовують найсучасніші методи отримання та обробки інформації, і лише знання про наявність таких варіантів має допомогти знизити рівень ризику. Щоб повністю усунути загрозу, необхідно звернутися до фахівців, які здатні визначити найцінніші набори даних, які є об’єктами можливих атак, і запропонують повний спектр засобів захисту.

Візуально-оптичні носії. Якщо через вікно офісу видно екран монітора або деякі документи на столі, є ризик витоку. Будь-який світловий потік, що виходить від джерела інформації, може бути перехоплений. Для боротьби з цим методом в більшості випадків потрібні прості технічні засоби:

- зниження відбивних властивостей і зниження освітленості предметів;

- монтаж різноманітних перешкод і покриттів;

- використання світловідбиваючого скла;

- розташування об'єктів таким чином, щоб їх світло не потрапляло в діапазон можливого перехоплення.

Але існує і більш типовий ризик витоку інформації про види: вилучення документів із приміщення для фотографування, інші форми копіювання, скріншоти екранів бази даних із важливою інформацією та інші методи. Основні заходи боротьби з цими ризиками стосуються виключно адміністративно-організаційної сфери, хоча існують програмні засоби, які, наприклад, не дозволяють переглядати дані, що відображаються на екрані.

Акустичні канали. Інформація у вигляді звуку більш схильна до перехоплення та витоку. Звук в ультрачастотному діапазоні (понад 20 000 герц) легко поширюється. Якщо на її шляху є перешкода, звукова хвиля викликає в ній вібрації, які зчитуються спеціальними приладами. Цю звукову властивість слід враховувати вже на етапі планування будівлі або офісу, якщо дизайн інтер’єру буде продуманий архітекторами таким чином, щоб втрата інформації була неможлива. Якщо цей спосіб нездійсненний, то для оформлення приміщення доведеться вдатися до технічних засобів і використовувати матеріали, що відбивають звук, наприклад, пористу штукатурку. Для оцінки рівня безпеки використовуються стетоскопи.

Якщо не вдається досягти максимального звукопоглинання, можна використовувати генератори шума, які можна встановити по периметру незахищених від слуху стін основної будівлі або в кімнатах для переговорів.

Використання диктофонів під час переговорів також дозволяє витоку акустичної інформації. Для виявлення їх наявності використовуються спеціальні прилади. Установка пристроїв для захоплення голосового сигналу в телефонах (жучки) сьогодні практично не використовується, цифровий трафік перехоплюється іншими способами, навіть через телефонного оператора чи інтернет-провайдера. Цей рівень ризику також необхідно враховувати,

наприклад, створюючи спеціальні інструкції щодо цієї конфіденційної інформації, яку можна обговорити по телефону.

Електромагнітні канали та канали зв'язку. Перехоплення інформації, що міститься в електромагнітних перешкодах, також небезпечно. Електромагнітні хвилі, які поширюються на коротку відстань в межах електромагнітного поля, також можуть бути перехоплені. Ви можете прийти з:

- мікрофони телефонні та домофонні;
- основних заземлювальних та силових кіл;
- з аналогової телефонної лінії;
- волоконно-оптичні канали зв'язку;
- з інших джерел.

Перехопити та розшифрувати їх не складно за допомогою сучасних технічних засобів.

Технології дозволяють підключати вбудовані пристрої ПЕМВН безпосередньо до електричних ланцюгів або встановлювати їх у монітор чи корпус комп’ютера, при цьому вони можуть перехоплювати дані через внутрішні з’єднання плат. схема:

- відображається на екрані монітора;
- вводиться через клавіатуру;
- кабельний вихід на периферійні пристрої (принтер);
- записані на жорсткий диск та інші пристрої.

У цьому випадку бойові методи полягають у заземленні кабелів, екрануванні найбільш очевидних джерел електромагнітного випромінювання, ідентифікації маркерів або використанні спеціального програмного та апаратного забезпечення для ідентифікації маркерів. Однак інформація, що передається через Інтернет, може бути перехоплена. З крадіжками можна боротися як за допомогою апаратного, так і програмного забезпечення.

Матеріальні та речові канали. Звичайне сміття або промислові відходи можуть бути цінним джерелом даних. Хімічний аналіз відходів, які залишають контрольовану територію, може стати важливим джерелом інформації про склад

продукту або технологію виробництва. Розробка системи боротьби з цим ризиком вимагає комплексного рішення, яке передбачає використання технологій переробки відходів.

Всі перераховані вище способи витоку інформації (крім матеріальних і речових) вимагають територіальної доступності джерела для злодія, дальність дії звичайного пристрою для перехоплення звукової або візуальної інформації не перевищує кількох десятків метрів. Установка інтегрованих пристроїв для уловлювання електромагнітного випромінювання та акустичних коливань має вимагати прямого проникнення в об’єкт. Також необхідні знання дизайну, для цього може знадобитися найняти співробітника. Хоча більшість об’єктів оснащені камерами відеоспостереження, зараз ці методи використовуються лише у вкрай рідкісних випадках.

Найбільшу загрозу становлять сучасні методи крадіжки, які використовують можливості Інтернету і з його допомогою отримують доступ до файлів, даних або голосового трафіку.

1.5 Засоби запобігання витоку інформації

Витоком існують певні принципи, на яких має базуватися комплексна система заходів для захисту конфіденційної інформації від витоку:

- безперервність системи в просторі і часі. Застосовані методи захисту повинні контролювати весь периметр матеріалу та інформації 24 години на добу, щоб уникнути виникнення певних пробілів або зниження рівня контролю;

- багатозонний захист. Інформація повинна бути класифікована відповідно до її важливості, а для її захисту слід використовувати методи з різним впливом;

Розстановка пріоритетів. Не вся інформація однаково важлива, тому для найбільш цінної інформації слід використовувати найсуворіші запобіжні заходи;

- інтеграція. Усі компоненти системи повинні співпрацювати один з одним і перебувати під контролем з єдиного центру. Якщо компанія є холдинговою

компанією або кількома філіями, необхідно налаштувати управління інформаційними системами материнської компанії;

- розмноження. Усі важливі комунікаційні блоки та системи повинні бути продубльовані, щоб у разі просування або руйнування одного із захисних з'єднань воно замінювалося контрольним.

Будівельні системи такого рівня не завжди потрібні невеликим комерційним компаніям, але вкрай необхідні великим компаніям, особливо тим, які працюють з державним замовником.

Відповідальність за дотримання має відповідати керівник підприємства та один із його заступників, який відповідає за службу безпеки. Майже 70% загального рівня інформаційної безпеки залежить саме від адміністративно-технічних заходів, оскільки в діяльності служб промислового шпигунства використання службових справ про хабарництво відбувається набагато частіше, ніж використання спеціальних технічних засобів.

Засоби викрадення інформації, що вимагає високого рівня кваліфікації, та надання інформації третім особам, які не беруть безпосередньої участі в конкурсі.

Усі нормативні акти організації щодо захисту комерційної таємниці та іншої інформації повинні відповідати більш жорстким вимогам до подібних документів, необхідних для отримання ліцензії. Це пов’язано не тільки з тим, що вони є найскладнішими, а й тому, що якісна підготовка даного виду документації дає можливість у майбутньому зайняти позицію компанії в спорах через витік інформації.

Персонал є найслабшою ланкою в будь-якій системі захисту від витоку даних. Тому при роботі з ним слід приділяти максимум уваги. Для компаній, які працюють з державною таємницею, діє система авторизації. Інші організації повинні зробити кілька кроків, щоб забезпечити обмеження можливості роботи з конфіденційними даними. Перелік відомостей, що становлять комерційну таємницю, необхідно скласти та відобразити як додаток до трудового договору.

При роботі з інформацією, що міститься в базі даних, слід розробляти системи доступу.

Вам потрібно обмежити всі параметри копіювання та доступ до зовнішньої електронної пошти. Усі працівники повинні бути ознайомлені з інструкціями щодо поводження з інформацією, що містить комерційну таємницю, і повинні підтвердити це письмово в журналах. Це дозволяє притягнути їх до відповідальності в разі потреби.

Існуючий режим доступу на об'єкт має включати не тільки захист даних усіх відвідувачів, а й роботу тільки з охоронними компаніями, які також дотримуються всіх вимог безпеки. Ситуація, коли працівник приватної охоронної компанії чергує на об'єкті вночі, де персонал набирає свої паролі та залишає їх на столі для зручності системного адміністратора, може бути так само небезпечною, як і робота від професійного хакера чи закладки встановлені в технічних приміщеннях.

Часто винуватцями інформаційних порушень стають не відвідувачі, а співробітники компанії. Це численні консалтингові та бухгалтерські фірми, які надають послуги з розробки та обслуговування інформаційних систем. Як курйозний, але суперечливий приклад можна навести ситуацію в Україні, коли кільком дочірнім компаніям 1С заборонили працювати за підозрою у можливих крадіжках конфіденційної бухгалтерської інформації їх співробітниками. Така ж небезпека випливає з поширених сьогодні хмарних CRM-систем, що пропонують послуги хмарного зберігання даних. З мінімальною відповідальністю за безпеку довіреної їм інформації ніхто не може гарантувати, що вся база дзвінків клієнтів, зареєстрована в системі під час інтеграції з IP-телефонією, відразу не стане здобиччю конкуренції. Цей ризик слід класифікувати як дуже серйозний. Вибираючи між серверними чи хмарними програмами, слід вибрати першу. За даними Microsoft, цього року кількість кібератак на хмарні ресурси зросла на 300%.

Так само обережно ставляться до всіх контрагентів, які вимагають передачі даних, що становлять комерційну таємницю. Усі договори повинні містити

умови, які передбачають відповідальність за їх розкриття. Дуже часто сертифікати на нерухоме майно та оцінки акцій, аудит та консультативні розслідування перепродаються конкуруючим організаціям.

При плануванні архітектури приміщення, в якому ведуться переговори або розміщується інформація, що підлягає захисту, слід дотримуватися всіх вимог ДСТУ до способів захисту. Зали для переговорів мають пройти необхідну сертифікацію, використовувати всі сучасні методи екранування, звукопоглинаючі матеріали, використовувати генератори шуму.

Щоб захистити інформацію від втрати або крадіжки, потрібно багато апаратних і технічних заходів. Сучасні технічні засоби поділяються на три групи:

- машинобудування. Ця категорія захисних засобів використовується при реалізації архітектурно-планувальних рішень. Це пристрої, які фізично блокують несанкціонований доступ до охоронюваних об’єктів, систем відеоспостереження, сигналізації, електронних замків та подібних технічних пристроїв;

- апаратні засоби. Сюди входять вимірювальні прилади, аналізатори, технічні пристрої, що дозволяють визначити місце розташування вбудованих пристроїв, все, що дозволяє виявити існуючі канали витоку інформації, оцінити ефективність вашої роботи, суттєві характеристики та роль у ситуації з можливістю ідентифікації або втрата інформації, що сталася. До них належать польові індикатори, високочастотні вимірювальні прилади, нелінійні локаційні пристрої, пристрої для перевірки аналогових телефонних ліній. Для ідентифікації диктантів використовуються детектори, що розпізнають електромагнітне побічне випромінювання, за таким же принципом працюють детектори відеокамер;

- програмне забезпечення. Це найважливіша група, оскільки вона запобігає проникненню сторонніх осіб в інформаційні мережі, блокує атаки хакерів, запобігає перехопленню інформації. Серед них слід звернути увагу на спеціальні програми, що пропонують захист системної інформації. Саме такі системи DLP і SIEM найчастіше використовуються для створення комплексних механізмів

інформаційної безпеки. DLP (Data Leak Prevention, запобігання витоку даних) забезпечує повний захист від втрати конфіденційної інформації. Сьогодні вони в основному налаштовані на роботу із загрозами всередині периметра, тобто загрозами, які походять від користувачів корпоративної мережі, а не від хакерів. Системи використовують широкий спектр методів для визначення точок втрати або перетворення інформації і можуть блокувати будь-який несанкціонований вхід або передачу даних шляхом автоматичної перевірки всіх каналів її передачі. Вони аналізують трафік електронної пошти користувачів, вміст локальної папки, повідомлення миттєвих повідомлень і блокують спроби передачі даних, якщо вони виявлені.

Системи управління інформацією та подіями безпеки SIEM (Security Information and Event Management) керують інформаційними потоками та подіями в мережі, а подія — це будь-яка ситуація, яка може вплинути на мережу та її безпеку. Якщо це станеться, система самостійно запропонує рішення для усунення загрози.

Програмне обладнання може вирішувати окремі проблеми та забезпечувати комплексну безпеку мережі;

- криптографічні. Ця категорія пропонує алгоритми шифрування для всієї інформації, що передається по мережах або зберігається на сервері. Навіть якщо він програється, він не зацікавить гіпотетичного конкурента.

Комплексне застосування всього спектру методів захисту може виявитися непотрібним. Тому для організації систем захисту інформації в конкретній компанії необхідно створити власний проект, оптимальний з точки зору ресурсів.

1.6. Висновки по розділу

В першому розділі було розглянуто основні відомості про банківську систему, банківську інформацію її безпеку та основні загрози.

Розглянуто канали витоку інформації та засоби запобігання витоку інформації.

Розділ 2.

ОЦІНКА РИЗИКІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

2.1 Огляд ризиків банківської діяльності та їх характеристика

У міжнародній банківській практиці процес управління ризиками є центральною сферою фінансового менеджменту. Велика увага приділяється вивченню зон ризику та основних видів ризиків, пошуку ефективних методів їх оцінки, контролю та моніторингу, створенню адекватних систем управління.

Банківські ризики – це ймовірність того, що очікувані або несподівані події можуть негативно вплинути на капітал та/або дохід банку.

З точки зору банку, ризик – це потенційна втрата доходу або зниження ринкової вартості капіталу банку через негативні зовнішні чи внутрішні фактори. Такі збитки можуть бути прямими (втрата доходу або капіталу) або непрямими (обмежує можливості банку для досягнення бізнес-цілей).

В економічній літературі та практиці термін «ризик» використовується часто і має різне значення залежно від контексту, оскільки визначення ризику є складним. У широкому сенсі ризик визначається як невизначеність щодо того, як певна подія відбудеться в майбутньому.

Ризик вимірюється ймовірністю того, що очікувана подія не відбудеться і що це призведе до небажаних наслідків. У банківській справі, як і в інших видах бізнесу, ризик пов’язаний переважно з фінансовими втратами, які виникають при реалізації певних ризиків. Оскільки ризиків не можна і не потрібно повністю уникнути, ними можна і потрібно управляти свідомо, враховуючи, що всі види ризиків взаємопов’язані і що їх рівень постійно змінюється під впливом динамічного середовища.

Загалом, банківський сектор є більш ризикованим, ніж інші види діяльності. Ця функція зумовлена специфікою функцій, які виконує кожен комерційний банк. У банків багато партнерів, клієнтів, позичальників, фінансове становище яких безпосередньо впливає на їхнє становище. Діяльність банку дуже різноманітна і включає збір коштів, випуск і купівлю цінних паперів, кредити, факторинг, лізинг,

надання готівкою клієнтам тощо. Здійснення будь-якого банківського бізнесу передбачає можливість здійснення кількох ризиків.

У зв'язку з тим, що банк веде як активний, так і пасивний бізнес, виникають додаткові ризики, такі як ризик незбалансованої ліквідності, ризик розриву часу в зборі та розміщенні коштів, валютний ризик. Це спонукає до пошуку особливих підходів для обмеження його наслідків, які називаються «управлінням банківськими активами та пасивами». Діяльність операційних підрозділів, обов'язкове використання високотехнологічних інформаційно-телекомунікаційних систем, необхідність постійного моніторингу, виконання маркетингових функцій супроводжуються низкою функціональних банківських ризиків, яких можуть уникнути інші компанії. Адже банківська система більшості країн світу підлягає жорсткому регулюванню з боку держави та спеціальному нагляду. Як наслідок, банк піддається зовнішнім ризикам у своїй діяльності, деякі з яких, наприклад, ризик невиконання державних нормативних актів, є надзвичайно важливими в банківському секторі.

Хоча банківська діяльність пов'язана з багатьма ризиками, саме банки повинні включати надійність і безпеку. Оскільки банкіри працюють переважно з чужими грошима, їм варто навіть більше за інших підприємців намагатися знизити ризик своєї діяльності. Тому ризик-менеджмент вважається одним із важливих напрямків фінансового менеджменту банку.

Проблемі економічного ризику присвячено багато робіт і наукових досліджень, які показують різні підходи до класифікації ризиків. Класифікація ризиків базується на основній класифікаційній характеристикі, але різноманітність таких явищ, як ризик, створює основу для різноманітних підходів до вирішення цієї проблеми, хоча навряд чи вона буде повністю охоплена.

Банківські ризики поділяються на зовнішні та внутрішні, які, у свою чергу, поділяються на фінансові та функціональні та являють собою цілісну систему, яку комерційні банки можуть використовувати для практичного застосування залежно від особливостей банківської діяльності у разі виникнення ризику. Ризик може бути

різним, він існує при кожній операції. Для банків важливо не уникати ризиків, а передбачати та мінімізувати їх.

Зовнішні ризики включають зміни, пов’язані зі змінами зовнішнього середовища банку і не пов’язані безпосередньо з його діяльністю. Це політичні, правові, соціальні та макроекономічні ризики, які виникають внаслідок загострення економічної кризи в країні, політичної нестабільності, війни, заборони виплати за кордоном, консолідації боргу, ембарго, ембарго, відкликання імпортних ліцензій, стихійних лих (пожежі, повені, землетруси), приватизації, націоналізації, неналежне правове регулювання тощо. Вплив зовнішніх ризиків на діяльність банку дуже високий, керувати цими ризиками найважче, а іноді й неможливо. Для його оцінки в основному використовуються методи логічного аналізу.

До внутрішніх ризиків належать ризики, що виникають безпосередньо в результаті діяльності конкретного банку. Чим ширший спектр клієнтів, партнерів, банківських відносин, банківських операцій та послуг, тим більше внутрішніх ризиків супроводжує вашу роботу. Порівняно із зовнішніми ризиками, внутрішні ризики легше ідентифікувати та визначити кількісно. Завдання управління складаються з постійного виявлення, оцінки, мінімізації та моніторингу внутрішніх ризиків з використанням відповідних методів.

Внутрішні ризики легше визначити, ніж зовнішні.

Якісна класифікація банківських ризиків повинна базуватися на впливі зовнішніх і внутрішніх факторів ризику. Цінність якісної класифікації банківських ризиків полягає в доцільності їх використання для пошуку внутрішніх резервів з метою підвищення ефективності управління ризиками банківських операцій.

Внутрішні ризики поділяються на фінансові та функціональні залежно від сфери виникнення.

Фінансові ризики становлять найбільшу групу банківських ризиків. Вони визначаються ймовірністю грошових збитків і пов’язані з непередбаченими змінами обсягу, прибутковості, вартості та структури активів і зобов’язань банку.

Фінансові ризики можуть бути безпосередньо пов’язані з діяльністю підприємства (наприклад, вибір виду фінансового активу та часу його придбання

(продажу), кількість придбаних (проданих) активів тощо) і можуть існувати об’єктивно самостійно. побажань підприємства та виникають у результаті змін в економіці (наприклад, внаслідок циклічного розвитку економіки, заходів урядової фінансової та монетарної політики тощо).

Класифікація ризиків та уточнення форми їх прояву дають змогу визначити найбільш небезпечні сфери фінансового інвестування та розробити рекомендації щодо управління ризиками. Концепція розрахунку фактора ризику — це об’єктивна оцінка його рівня з метою забезпечення формування необхідної прибутковості бізнесу фінансового ринку та розробки системи заходів, що мінімізують його негативні фінансові наслідки для учасників фінансового ринку.

У світовій фінансовій практиці використовуються наступні методи контролю та мінімізації ризиків, конкретні комбінації яких залежать від особливостей конкретного сегмента фінансового ринку:

– фондові біржі і, зокрема, органи зберігання та компенсації пред’являють мінімальні вимоги до професійного складу учасників, їх матеріального становища та навіть репутації. Чим надійніший кожен з учасників системи, звісно, тим менший ризик для всіх інших учасників, але в той же час не всі вони зможуть задовольнити ці вимоги. У цьому випадку система дуже надійна, але неефективна через малу кількість учасників. Тому завдання організаторів ринкової інфраструктури — знайти прийнятний компроміс між надійністю системи та її розмірами;

- біржі та клірингові організації можуть встановлювати різні ліміти для транзакцій учасників. Чим суворіші ліміти, тим нижча взаємна заборгованість учасників і менші ризики. Проте занадто жорсткі обмеження призводять до зниження обсягів торгів та стагнації ринку. Тому потрібен компроміс між надійністю та розміром ринку;

- вкладники та клірингові організації впроваджують методи розподілу ризиків між усіма учасниками системи, зокрема використання «клірингових» та «інноваційних» методів;

- учасники переговорів можуть створити спеціальний резервний фонд, який компенсує збитки від невиконання або несвоєчасного виконання угод окремими учасниками, яким зазвичай керують депозитарій та клірингова організація;

- за допомогою зберігача та розрахункової палати учасники ринку можуть створити систему розподілу збитків, якщо вони виникають внаслідок невиконання окремими учасниками своїх зобов'язань за угодами;

- розрахункова палата депозитарію або учасники переговорів через клірингову палату використовують механізм акредитації боржників, які мають тимчасові труднощі з оплатою. Кредиторами за свій рахунок або за рахунок учасників можуть бути як самі учасники, так і клірингова організація.

Найбільш складні та небезпечні за своїми фінансовими наслідками ризики страхуються спеціальними страховими компаніями шляхом укладання відповідного договору. Йдеться про страхування професійних учасників бізнесу. В основному це так зване комплексне страхування банків і страхових компаній від електронних та комп’ютерних злочинів. Далі слід страхування від пошкодження цінностей, у тому числі цінностей.

Для банків актуальне страхування ломбарду. Проте, як і на українському фондовому ринку, операції з кредитами під заставу цінних паперів, які звичайні лише для рефінансування банківських операцій комерційних банків НБУ за державні облігації, пізніше планують проводити подібні операції з корпоративними цінними паперами. І якщо НБУ виступає зберігачем (відповідає за фізичну доступність даних ОВДП) в операціях з рефінансування в рамках ОВДП, то при рефінансуванні корпоративних цінних паперів НБУ та комерційні банки, які здійснюють операції з кредитування під заставу, за цінними паперами співпрацюють не лише з зберігачі. , а й з реєстраторами. І, як ми вже знаємо з практики, мають місце випадки незаконних дій реєстраторів щодо переоформлення майнових прав на цінні папери за підписами представників власника, який на момент передачі документів не був уповноважений підписувати ці документи, випадки втрата або знищення записів. І в результаті цих дій втрата застави та неповернення кредиту.

Слід згадати про інший вид страхування, наприклад страхування директорів та відповідальності керівництва, яке використовують організації, які виходять на західні ринки зі своїми цінними паперами.

Останнім часом все більшого поширення набуває страхування підприємницьких ризиків. Цей вид страхування фактично є страхуванням кримінальної та професійної відповідальності.

Діяльність на фінансовому ринку також потребує спеціальних портфельних стратегій, спеціально підібраних фінансових інструментів, які знижують цей ризик. Одним із дієвих механізмів нейтралізації ризиків операцій фінансового ринку є диверсифікація, яка захищає інвестиції від негативного впливу циклічних коливань в економіці, довгострокових галузевих тенденцій та ослаблення кредитних позицій. окремі компанії. Високий ступінь диверсифікації дозволяє знизити або навіть повністю виключити всі види ризиків, за винятком системних.

Фінансові ризики включають валютний, кредитний, інвестиційний, ринковий ризик, ризик ліквідності, ризик процентної ставки, інфляцію, базисний ризик тощо.

Кредитний ризик – це ймовірність фінансових збитків через невиконання зобов'язань позичальником. Важливою складовою кредитного ризику є галузевий ризик, який виникає через невизначеність перспектив розвитку галузі позичальника. Одним із методів вимірювання галузевого ризику є системний або бета-ризик. Бета-ризик показує кількість коливань або розбіжностей у продуктивності галузі щодо загального розвитку ринку або економіки в цілому. У галузі з бета-версією 1 спостерігаються коливання прибутків, які повторюють рух ринку. Менш нестабільна галузь має бета меншу за одиницю, а більш нестабільна галузь має бета більшу за одиницю. Очевидно, що вища бета-версія означає вищий галузевий ризик. Визначення рівня бета-версії для кожної галузі вимагає надійної бази даних протягом тривалого періоду часу.

При визначенні кредитного ризику потрібно враховувати географічний ризик, який поділяється на регіональний та країновий – місцезнаходження позичальника. Останній супроводжує позики іноземним позичальникам і зумовлений факторами, характерними для країни, в якій проживає позичальник.

Виходячи з поняття кредитного ризику комерційного банку, слід розрізняти такі терміни:

-Кредитний ризик позичальника: ймовірність того, що позичальник (боржник) не зможе виконати свої зобов'язання перед банком щодо сплати боргу за умовами договору (угоди);

- Кредитний ризик при отриманні кредитів: ймовірність того, що банк не використає гарантію своєчасно і в повному обсязі для покриття можливих збитків;

- Кредитний ризик кредитного договору: ймовірність того, що позичальник (боржник) не виконає свої зобов'язання перед банком щодо погашення заборгованості за договорами (контрактами) і банк не використає гарантію по кредиту вчасно та в повному обсязі, щоб покрити будь-які збитки. Визначення кредитного ризику можна розглядати з різних сторін. По-перше, його можна визначити як ймовірність того, що банк зазнає збитків у разі невиконання позичальником певного кредитного договору. По-друге, кредитний ризик можна охарактеризувати як максимальну суму збитків і незароблених доходів, які є результатом непогашення позичальником повністю або частини основного боргу та/або відсотків.

Регіональний ризик – це ризик, пов’язаний з діяльністю в певному регіоні в конкретній країні. Ризик, пов’язаний з веденням бізнесу в країні, іноді називають ризиком країни.

Регіональний ризик визначається особливостями даної адміністративно-географічної території, яка характеризується умовами, що відрізняються від середніх умов по всій країні. Відмінності можуть бути пов’язані з кліматичними, національними, політичними, правовими та іншими специфічними для регіону факторами, які впливають на становище позичальника і тому стають частиною кредитного ризику. Кредитний ризик притаманний не лише прямим кредитним операціям, а й супроводжує оформлення лізингу, факторингу, гарантій та процес створення портфеля цінних паперів.

Ризик дисбалансу ліквідності пов'язаний з імовірністю того, що банк не зможе вчасно виконати свої зобов'язання або втратить частину доходу від надмірно високоліквідних активів. Ризик незбалансованої ліквідності можна розглядати як два

різних ризики: ризик недостатньої ліквідності та ризик надлишкової ліквідності. Виміряти ризик ліквідності дуже складно, оскільки на цей показник впливає багато факторів, більшість з яких банк не може контролювати самостійно. На практиці для контролю ліквідності використовуються спеціальні індикатори, більшість з яких регулюються центральними банками країн.

У той же час практика управління ризиком ліквідності кредитними спілками вважається недосконалою, оскільки не враховує ризик довгострокового дисбалансу ліквідності, що суттєво впливає на платоспроможність. та фінансової стабільності установи. Для цього необхідно використовувати табличні методи оцінки ліквідності: структура позиції ліквідності (як окрема форма звітності кредитної спілки) та матриця фінансування мінімального ризику ліквідності.

Ризик інфляції — це ймовірність майбутнього знецінення вартості готівки, тобто втрати її купівельної спроможності. Інфляційні процеси більш-менш властиві більшості економічних систем. Це загальне економічне явище, і тому банки не можуть суттєво впливати. Проте банки можуть скористатися високою інфляцією для підвищення прибутковості свого бізнесу. Враховуючи специфіку своєї діяльності, банки мають реальні шанси опинитися серед тих, хто отримує вигоду від швидкої інфляції через різке збільшення грошової маси та вплив кредитного мультиплікатора на кредити клієнтів. Проте негативний вплив має і ризик інфляції, що проявляється у знеціненні активів банку та коштів власників банків – власного капіталу.

Ризик інфляції – це ризик того, що інфляція підірве ефективність інвестицій, вартість активів або купівельну спроможність потоків доходів. Дивлячись на фінансові результати без інфляції – це номінальна прибутковість. Цінність, про яку слід турбувати інвестора, — це купівельна спроможність, яка відома як фактична прибутковість. Інфляція – це зниження купівельної спроможності грошей з часом, і непередбачувані зміни інфляції несуть ризик того, що прибуток від здійснених інвестицій або майбутня вартість активу будуть нижчими, ніж очікувалося.

Будь-який потік грошей або грошовий дохід потенційно піддається інфляційному ризику, оскільки його вартість знецінюється прямо пропорційно зменшенню купівельної спроможності грошей. Позика з фіксованою сумою для

додаткового погашення у вигляді фіксованої суми є класичним прикладом активу, який піддається ризику інфляції, оскільки повернуті гроші можуть коштувати значно менше за залучені гроші. Фізичні активи та акції менш чутливі до ризику інфляції і навіть можуть отримати вигоду від непередбачуваної інфляції.

Ризик неплатоспроможності – це ймовірність того, що банк не зможе виконати свої зобов’язання, навіть якщо його швидко продати. Ризик неплатоспроможності тісно пов'язаний з ризиком ліквідності та ризиком банкрутства та випливає з інших ризиків. Тому процес управління базується на постійному моніторингу глобального ризику банку.

Значне місце серед фінансових ризиків займає група цінових ризиків, пов'язаних з можливістю зміни показників або вартості активів і зобов'язань банку. Ціновий ризик визначається ймовірністю зміни ринкових цін на фінансові та фізичні (матеріальні) активи, відображені на балансі банку або на позабалансових рахунках. Під фінансовими інвестиціями розуміються грошові кошти, валюта та цінні папери; До фізичних активів належать дорогоцінні метали, твори мистецтва, нафта, крупи, кольорові метали тощо. Це фінансові інструменти або активи, які можуть обліковуватись як на активних, так і на пасивних банківських рахунках, а також позабалансові статті. Отже, зміна ринкової ціни цих активів призводить до зміни вартості активів, зобов’язань або позабалансових зобов’язань банку. Наслідки цінового ризику найбільш очевидні, коли банк оцінює вартість статей балансу на основі ринкових цін на кінець кожного робочого дня. При цьому будь-яка зміна ринкових цін негайно відображається на балансі банку. Несвоєчасний облік прибутків або збитків створює додаткові проблеми, оскільки незнання факторів ризику не означає їх відсутність. Трьома основними банківськими ризиками цієї групи є ризик зміни процентних ставок, ризик обмінних курсів і ризик зміни вартості цінних паперів.

Ризик процентної ставки (відсотковий ризик) — це ймовірність фінансових збитків через мінливість процентних ставок на ринку протягом майбутнього періоду. Процентний ризик супроводжує діяльність позичальників, кредиторів, власників цінних паперів, інвесторів.

Валютний ризик визначається ймовірністю збитків у зв'язку зі зміною курсу однієї валюти щодо іншої. Ризики обмінного курсу виникають у компаній, які мають на балансі активи, зобов’язання або позабалансові статті в іноземній валюті.

Ризик зміни вартості цінних паперів (ризик власного капіталу) — це ймовірність фінансового збитку внаслідок зміни ринкової ціни цінних паперів або інших торговельних інструментів. Цей ризик притаманний всім учасникам біржі: інвесторам, трейдерам, емітентам цінних паперів.

Базовий ризик визначається ймовірністю структурних змін різних процентних ставок. Іншими словами, цей ризик виникає через асиметрію динаміки окремих процентних ставок (порівняльних характеристик) на відміну від процентного ризику, який пов’язаний із зміною рівня процентної ставки в часі. (динамічні характеристики). Наприклад, якщо ставки за кредитами визначаються на основі міжбанківських ринкових ставок і депозитні ставки не пов’язані безпосередньо з цим ринком, будь-яка розбіжність у зміні двох різних базових ставок може призвести до додаткових прибутків або збитків, що означає основний ризик.

При управлінні ціновими ризиками банки використовують спеціальні методи, які спільно називають хеджуванням. Механізм хеджування компенсує фінансові втрати, які виникають у результаті зміни ринкової ціни інструмента для однієї позиції та доходу для іншої (компенсаційної) позиції. За допомогою хеджування ви можете значно зменшити або навіть уникнути цінових ризиків.

Значний вплив на діяльність банків мають функціональні ризики. Причинами його виникнення є неможливість здійснювати повний і своєчасний контроль за фінансово-господарською діяльністю банку. Функціональні ризики пов'язані з процесами створення та впровадження нових банківських продуктів і послуг, збору, обробки, аналізу та передачі інформації, навчання кадрів та виконання інших адміністративно-комерційних операцій.

Ці ризики важче визначити, визначити кількісно та кількісно, ніж фінансові ризики. Однак функціональні ризики не менш небезпечні, ніж інші види банківського ризику, і в кінцевому підсумку також призводять до фінансових втрат. Банки намагаються знизити функціональні ризики шляхом удосконалення систем

внутрішнього аудиту, розвитку систем документообігу, розробки внутрішніх методів, надання технічної та фінансової підтримки окремих операцій. Добре продумана ресурсна, логістична та кадрова політика також допомагає зменшити ці ризики.

Технологічний ризик (ризик відмови системи) пов'язаний із використанням у діяльності банку високотехнологічних технічних засобів, пристроїв і технологій. Цей вид ризику виникає внаслідок помилок у використанні комп'ютерних програм, математичних моделей, формул і розрахунків. Це також трапляється, якщо менеджерів не інформують вчасно або неналежним чином через недоліки в підсистемах інфраструктури, перебої в мережах або комунікаціях. Фінансові втрати банку виникають внаслідок помилок і збоїв, а також додаткових витрат на їх усунення. Типовим проявом технологічного ризику є збій електронної платіжної системи. Однією з обов'язкових умов доступу банків до міжнародних клірингово-інформаційних систем є усунення несправностей обладнання протягом певного періоду часу (зазвичай 2 години).

Ризик зловживання – це можливість збитків для банку в результаті шахрайства, марнотратства, несанкціонованого доступу до важливої інформації співробітників або клієнтів банку, відмивання грошей, несанкціонованих операцій.

Документаційний ризик – це можливість випадкової помилки в документації, яка може мати негативні наслідки: невиконання положень договору, подання позову, відмова від попередніх зобов'язань тощо, покращення документообігу, автоматизація процесу документування та покращення роботи співробітника. навички можуть бути значно знижені.

Ризик операції супроводжує укладення та реєстрацію контракту, розрахунки, підписання контрактів, поставку цінних паперів або валюти. Цей вид ризику тісно пов'язаний з технологічними, документальними та операційними ризиками. Типовим прикладом є оплата зустрічних платежів, коли час переказу грошей не синхронізовано. Одна зі сторін повинна здійснити операцію раніше, що піддає ризику операції.

Операційний ризик визначається ймовірністю невідповідності операційних витрат банку та його ефективності. Процес управління операційними ризиками в

банку набагато складніший, ніж в інших сферах бізнесу. Витрати включають як відсоткові, так і непроцентні (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. Основними проблемами є неправильне формулювання цілей і стратегій банку, помилки при розробці стратегічного плану, недостатність ресурсів для реалізації стратегій, неправильне використання ризик-менеджменту в банківській практиці. Амбітна мета з недостатнім штатом чи фінансовими ресурсами може призвести до втрат або навіть втрати репутації банку. Класичними прикладами стратегічних ризиків є надмірні інвестиції в нерухомість або невиправдано швидке розширення мережі філій без ретельного дослідження ринку.

Ризик запуску нового продукту – це ймовірність того, що запланований рівень окупності нових банківських продуктів, послуг, операцій або технологій не буде досягнутий. У банківській справі, як і в інших видах бізнесу, існує постійна конкуренція за клієнтів і ринки за найвигідніші умови. На цей процес істотно впливають численні маркетингові ризики, які виражаються, серед іншого, у ризику впровадження нових продуктів.

Ризик репутаційного збитку виникає через можливу неспроможність банку зберегти свою репутацію як надійної та ефективної установи. Високий рівень залежності від зовнішнього капіталу робить банки особливо схильними до цього ризику. Втрата довіри вкладників до банку може призвести до відтоку готівки та банкрутства. Керівництво банку має приділяти особливу увагу дотриманню нормативних вимог, постійному моніторингу ліквідності та загального рівня ризику банківських операцій.

2.2 Оцінка ризиків банківської діяльності

Банки піддаються ризику, коли вони здійснюють банк з наміром отримати прибуток. Тому рівень ризику необхідно належним чином керувати та контролювати. Банківські ризики також необхідно оцінювати з точки зору їх важливості. Цю оцінку слід проводити на постійній основі.

Відповідно до концепції ризик-орієнтованого нагляду, відповідальність за контроль ризиків покладається на керівництво банку та наглядову раду банку. Національний банк визначає, наскільки банк керує ризиками протягом певного періоду часу, а не лише оцінює ситуацію в певний момент. У нагляді, що ґрунтується на оцінці ризиків, Banco Nacional діє більше як наглядовий орган, ніж як аудитор. Нагляд, орієнтований на ризики, дозволяє Національному банку здійснювати превентивний нагляд, зосереджуючи увагу на ризиках окремих банків та системних ризиках банківської системи.

У контексті банківської системи нагляд на основі ризиків визначає сфери діяльності, які разом узяті можуть становити неприйнятний ризик для банківської системи. У разі високоризикової діяльності або такої, яка стала особливо ризикованою внаслідок ринку, Національний банк має намір здійснювати адекватний вплив на банківську систему шляхом взаємодії з останньою шляхом прямого нагляду та за допомогою відповідних нормативних актів. Національним. банк. У ситуаціях, коли певний банк неадекватно керує своїми ризиками, Banco Nacional вживає відповідних заходів для впливу на керівництво банку, щоб узгодити свої дії з основними принципами надійного банківського обслуговування.

Деякі ризики є невід'ємною частиною банківської діяльності. Банківський сектор володіє широкими знаннями щодо того, як ідентифікувати, вимірювати, керувати та відстежувати ці притаманні банківські ризики. Нагляд, орієнтований на ризики, визнає існування цих ризиків і намагається якомога ефективніше використовувати ресурси нагляду. Наприклад, параметри ризику базуються на результатах обмежених тестів під час інспекцій, щоб забезпечити наявність відповідних засобів контролю. Це підтверджує перші результати визначення

параметрів ризику та сприяє розробці програм нагляду на основі параметрів ризику окремих банків. Процес визначення параметрів ризику є важливим для розробки циклів моніторингу та вибору інструментів моніторингу. Ризики для банківського сектору різноманітні та складні. Найбільш важливі та складні ризики вимагають кращих інструментів контролю та моніторингу як з боку Банку, так і з боку Національного банку. Banco Nacional намагається зосередити свої найкращі ресурси на цих складних і зростаючих ризиках, коли вони фактично або потенційно становлять значну загрозу для банківської системи.

Через різні ринкові умови та банківські структури не існує системи управління ризиками, прийнятної для всіх банків. Кожна установа повинна розробити власну програму та системи управління ризиками відповідно до своїх потреб та обставин. Наприклад, більший банк з більш складними операціями та відділеннями в різних географічних районах повинен мати більш витончену та витончену систему управління ризиками. Проте всі ефективні системи управління ризиками мають ряд ключових характеристик. Наприклад, ефективні системи управління ризиками повинні бути незалежними від діяльності з високим ризиком. Будь-яка система управління ризиками, незалежно від її структури, повинна включати такі елементи:

- оцінка ризиків. Правильна ідентифікація ризиків передусім полягає у розпізнаванні та розумінні існуючих ризиків або ризиків, які можуть виникнути у зв’язку з новими бізнес-ініціативами. Ідентифікація ризику має бути безперервним процесом, який має здійснюватися як на рівні окремих операцій, так і на рівні портфеля;

- вимірювання ризику. Точне та своєчасне вимірювання ризику є надзвичайно важливою частиною ефективного управління ризиками. Банк, який не має системи вимірювання ризиків, має лише обмежені можливості для контролю або моніторингу ризиків. Крім того, розробка інструментів управління ризиками, що використовуються банком, повинна відповідати складності та рівню ризиків. Банк повинен періодично перевіряти надійність приладів обліку,

які він використовує. Відповідні системи вимірювання ризику включають оцінку окремих операцій;

- контроль ризиків. Банк повинен встановити обмеження та довести їх до контрагентів за допомогою правил, стандартів та/або процедур, які визначають відповідальність та повноваження працівників. Ці ліміти контролю мають бути ефективними інструментами управління, які можна уточнити як зміни умов або толерантності до ризику. Банк визначає послідовність процедури видачі дозволів на виключення або зміну лімітів ризику, якщо це є обґрунтованим;

- моніторинг ризиків. Банки повинні відстежувати ризики, щоб забезпечити своєчасний моніторинг рівнів ризиків та винятків із певних правил. Подальші звіти мають бути регулярними, своєчасними, точними та інформативними та мають бути доступними для відповідних посадових осіб, щоб вони могли вжити необхідних заходів.

Для ефективного управління ризиками необхідна участь спостережної ради банку. Наглядова рада банку має визначити стратегічний напрямок діяльності банку. Важливою частиною стратегічного керівництва є визначення готовності банку йти на ризик шляхом усного або письмового схвалення відповідних положень. Завдяки належним чином розробленим системам моніторингу наглядова рада банку може притягнути керівництво банку до відповідальності за ведення бізнесу в межах визначеного допустимого ризику.

Оцінюючи систему управління ризиками, керівники враховують положення, процеси, персонал та системи контролю. Значні недоліки в одному або кількох із цих компонентів вважаються недоліками в управлінні ризиками. Усі ці системи є важливими, але розвиток та складність кожної з них відрізняються залежно від складності діяльності банку. Менші банки, які не ведуть складного бізнесу, як правило, мають менш формалізовані правила, процеси та системи контролю, ніж великі банки. Однак це не означає, що системи ризик-менеджменту менш важливі для банків із простими операціями. Це означає лише те, що формалізація процесу менш виражена. Усі банки повинні мати можливість чітко визначити та продемонструвати ефективність власної

системи управління ризиками. Для ефективного управління ризиками потрібні єдині правила, процеси, кваліфікований персонал та системи контролю:

- резерви відображають намір банку досягти бажаних результатів. Вони визначають стандарти та заходи, які необхідно застосовувати для виконання певних конкретних завдань. Ретельно розроблені правила базуються на правильно сформульованих місіях, цінностях та принципах банку. Вони також чітко визначають толерантність банку до ризику. Необхідно створити механізми для зміни правил у разі зміни характеру діяльності банку або його толерантності до ризику. Положення мають бути написані в письмовій формі з урахуванням складності операції, впливу організаційної структури тощо. Положення мають бути чітко сформульовані та втілені в життя;

- процеси – це процедури, програми та практики, які визначають, як банк виконує свої завдання. Процеси визначають, як здійснюється поточна діяльність банку. Належним чином розроблені процеси базуються на рекомендаціях банку, є ефективними та їх функціонування базується на відповідних повноваженнях виконавчого органу;

- співробітники: це працівники та керівники, які фактично здійснюють процеси або контролюють їх роботу. Співробітники та керівники повинні бути кваліфікованими та компетентними та належним чином виконувати свої завдання. Ви повинні розуміти місію, цінності, позиції та процеси банку. Програми оплати праці в банку повинні бути розроблені таким чином, щоб забезпечити придбання та утримання кваліфікованих працівників та їх безперервний професійний розвиток;

- системи контролю – це інструменти та інформаційні системи, які керівники банку використовують для оцінки діяльності працівників, підрозділів та банку в цілому, прийняття рішень та визначення ефективності існуючих процесів у банку. Вони засновані на принципі зворотного зв’язку і повинні бути своєчасними, точними та інформативними. Вони дозволяють оцінити діяльність банку та приймати рішення.

Кількість ризику і якість управління ризиком мають оцінюватися незалежно одна від одної. Тому, визначаючи рейтинги окремих факторів оцінки за системою оцінки ризиків, необхідно пам'ятати, що якою б високою або низькою не була якість управління ризиком, вона не повинна впливати на оцінку кількості ризику. Крім того, значний розмір капіталу або високі показники фінансової діяльності не повинні розглядатися як пом'якшувальні фактори для неадекватної системи управління ризиками. Наглядовці не повинні робити висновок, що "високий" рівень ризику - це погано, а "низький" рівень ризику - це добре. Кількість ризику просто відображає рівень ризику, який банк бере на себе в процесі здійснення своєї діяльності, і добре це чи погано - залежить від того, чи забезпечують системи управління ризиками банку виявлення, вимірювання, моніторинг і контроль цієї кількості ризику.[23]

Оцінка ефективності, комплексності та адекватності, створеної банком системи управління ризиками здійснюється уповноваженими працівниками Національного банку шляхом: аналізу діяльності банку, внутрішньобанківських документів, результатів самооцінювання з боку банку; перевірки процесів, операцій, інструментів з управління ризиками; проведення інтерв'ю з керівниками банку та іншими працівниками банку; оцінки взаємодії ради банку і частоти проведення зустрічей із головним ризик-менеджером та головним комплаєнс-менеджером.[24]

Банк використовує ефективні моделі та інструменти для оцінки (вимірювання) ризиків, як тих, що підлягають кількісному виміру в повній мірі, так і тих, що підлягають кількісному виміру в меншій мірі, уключаючи ризик репутації, стратегічний ризик. Банк має право використовувати тільки інструменти оцінки ризиків для тих ризиків, що підлягають кількісному виміру в меншій мірі.[24]

Банк під час обрання моделей та інструментів оцінки ризиків ураховує:

1) особливості своєї діяльності, характер, обсяг операцій, профіль ризику;

2) бізнес-потреби;

3) припущення, що є основою для моделей та інструментів;

4) наявність коректних та повних вхідних даних;

5) можливості інформаційної системи банку щодо управління ризиками;

6) досвід та кваліфікацію персоналу. [24]

Банк перевіряє моделі/інструменти, розроблені як банком, так і зовнішніми організаціями.

Банк не перевіряє жодну міжнародну модель/інструмент розповсюдження (а також метод аналізу тривалості, аналіз GAP), доки вони стандартизовані, а інформація про їх компоненти, переваги та недоліки є загальнодоступною та банк не може змінювати результати його перевірки.

Банк не проводить валідацію розроблених Національним банком моделей/інструментів оцінки ризиків, складові яких базуються на агрегованих статистичних даних, зібраних Національним банком з усієї банківської системи України та використовуються банками для розрахунку мінімальних нормативних вимог.

Перевірка моделі/інструменту оцінки ризику повинна бути незалежною від дизайну моделі чи вибору інструменту та його використання. Перевірка повинна виконуватися окремою філією банку (окрім організації, яка створює та/або використовує модель чи інструмент) або зовнішньою організацією, включаючи передачу валідації моделі/інструменту на аутсорсинг цій організації. Субпідрядник може створити модель, якщо банк відповідає вимогам незалежності для перевірки цієї моделі.

Ризик-менеджер забезпечує, щоб рада директорів банку та комітет з управління ризиками були належним чином поінформовані про сильні та слабкі сторони моделей та інструментів ризику, припущення та обмеження, властиві моделям, з метою використання їх при перегляді результатів ризику оцінки та своєчасної підготовки до врахування та відповідних управлінських рішень.

Банк регулярно, з періодичністю, визначеною цим Положенням, здійснює стрес-тестування з метою оцінки ризиків та визначення своєї спроможності протистояти потрясінням та загрозам, на які банк наражається під час своєї діяльності, або які можуть виникнути в майбутньому.[24]

Банк розробляє єдиний внутрішньобанківський документ або окремі розділи щодо стрес-тестування у відповідних документах щодо кожного з видів ризиків про порядок здійснення/проведення стрес-тестування (програма проведення стрес-тестування), який визначає:

1) методологію та моделі, що використовуються для здійснення стрес-тестування;

2) періодичність здійснення різних типів стрес-тестування;

3) перелік, функції та порядок взаємодії учасників процесу здійснення стрес-тестування, їх повноваження і відповідальність з чітким визначенням структури підпорядкування;

4) перелік видів ризиків, за якими здійснюється стрес-тестування;

5) перелік факторів ризиків, що використовуються під час здійснення стрес-тестування;

6) перелік припущень, що використовуються під час здійснення стрес-тестування;

7) інформаційну систему щодо управління ризиками, за допомогою якої банк здійснює стрес-тестування;

8) порядок розгляду результатів здійснення стрес-тестування та доведення їх змісту до відома ради банку, комітету з управління ризиками та правління банку з метою прийняття своєчасних та адекватних управлінських рішень щодо зниження рівня ризиків.[24]

Для кожного з основних видів ризику банк самостійно визначає методи стрес-тесту з урахуванням власного досвіду. Залежно від ситуації банк скористається одним або кількома з наступних методів:

1) Аналіз чутливості портфеля активів до зміни факторів ризику, який складається з моделювання наслідків зміни фактора ризику або групи тісно пов'язаних факторів ризику, але без змін інших факторів ризику;

2) Аналіз сценарію, який складається з моделювання наслідків зміни кількох факторів ризику одночасно на основі історичних та гіпотетичних подій. Зіткнувшись з надзвичайною (екстремальною) подією, але водночас імовірною,

метод дозволяє оцінити можливий вплив одночасного виникнення кількох факторів ризику на комерційну діяльність банку. При розробці сценаріїв банк використовує фактори ризику з найбільшим негативним впливом, які можуть призвести до подій, які можуть призвести до того, що банк зазнає найбільших збитків і розробить варіанти гіршого;

3) зворотні стрес-тести, які полягають у знаходженні такої комбінації значень факторів ризику та визначенні сценарію, при якому банк отримає заздалегідь визначений негативний результат (порушення капіталу та/або інших нормативів, встановлених Національним банком, втрата ліквідність, банкрутство тощо негативні наслідки для банку). Пошук можна здійснювати за допомогою експертних методів і статистичних моделей.

Менеджер з ризиків забезпечує, щоб рада директорів банку та комітет з управління ризиками були належним чином проінформовані про сильні та слабкі сторони методів стрес-тестування та стрес-сценаріїв, щоб вони були враховані під час перегляду результатів та здійснення своєчасного та адекватного управління рішення.

Банк використовує результати стрес-тесту для розробки/перегляду/коригування бізнес-плану та стратегії банку, стратегій управління ризиками, політики та процедур, планів відновлення, безперервності бізнесу та фінансування кризи.

2.3 Висновки по розділу

В другому розділі було розглянуто ризики банківської діяльності та подана методика її оцінки.

Розділ 3.
РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ УСТАНОВІ З ВИКОРИСТАННЯМ СУЧАСНИХ ЗАСОБІВ

3.1 Опис об’єкту банківської діяльності

Офіс банку (рисунок 3.1) займає приміщення площею 307,59 кв. м. В офісі 14 робочих приміщень: операційний зал (приміщення №2), кабінет для переговорів (приміщення №4), кабінет заступника директора (приміщення №5), кабінет директора (приміщення №6), сейфова кімната (приміщення №7), передсейфове приміщення (№8), каса 1 (приміщення №11), каса 2 (приміщення №12), каса 3 (приміщення №13), кабінет менеджерів (приміщення №14), кабінет технічного персонала (приміщення №14), секретний відділ, архів (приміщення №16). Також приміщення банкоматів (приміщення №1) та приміщення охорони (приміщення №3).

Вікна приміщень (№4, №5, №6) обладнанні металевими жалюзямі, а вікно приміщення №2 обладнано захисною плівкою. Усі двері, де використовується пропуск за Wiegand картою, відбитком пальця є броньованими. Висота стелі в усіх приміщень 2.5м.

Організація працює з 9-00 до 18-00 з обідньою перервою з 13-00 до 14-00. На час роботи відвідувач ам відкриті двері. В неробочий час та в час перерви на обід знаходження відвідувачів всередині приміщення організації не допускається.

По закінченню робочого дня, охоронник має закрити всі жалюзі та двері на замок, аналогічно відбувається і процес відкриття.

3.2 Вибір та обґрунтування технічних засобів запобігання несанкціонованого доступу до інформації

В даному розділі за характеристиками обладнання буде обрано найбільш оптимальні варіанти, які будуть використано в проектованій системі.

Для СКУД зазвичай використовуються IP-камери, тому на рис 3.2 зображено камери, які були використанні для порівняння.

В табл 3.1 порівнюються основні технічні характеристик вище зображених 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-підствітка	+	+	+	+	+
Живлення	DC 12B/PoE	DC 12B/PoE	DC 12B/PoE	DC 12B/PoE	DC 12B/PoE
Захист	IP66	IP67	IP66	IP67	IP67
Розширення	2 Мп	2Мп	2Мп	2Мп	4Мп

Після проведення аналізу характеристик неповоротних IP-камер виводимо кінцевий результат, який відповідає тому, що найкращим варіантом для цієї розробки є камера Hikvision DS-2CD1721FWD-IZ (2.8-12mm). Тим же чином проводимо вибір інших компонентів для створення системи.

В табл 3.2 порівнюються основні технічні характеристик вище зображених 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	1/2.7 CMOS	1/2.7 CMOS	1/3 CMOS	1/3 CMOS

	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 проведення аналізу характеристик поворотних IP-камер виводимо кінцевий результат, який відповідає тому, що найкращим варіантом для цієї розробки є камера Wi-Fi IP Камера 4Мп Reolink E1 Pro.

В таблиці 3.3 наведено найважливіші технічні характеристики для контроллерів.

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

Після проведення аналізу характеристик зчитувачів з відбитком пальця виводимо кінцевий результат, який відповідає тому, що найкращим варіантом для цієї розробки є зчитувач Dahua ASI1202M.

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	+	+	+	+	+
Струм споживання,мА	30	100	30	30	35
Дальність зчитування,см	10	1-8	10	10	7
Робочий діапазон температур, °С	-45-+60	-30-+60	-40-+60	-40-+60	-10-+60
Живлення, В	9-16	9-15	9-12	9-24	9-18
Ціна, грн	270 грн	952	390 грн	540 грн	450 грн

Після проведеного дослідження найкращим варіантом є зчитувач карт ATIS PR-82 EM.

Таблиця 3.6.

Характеристики зчитувачів карт з клавіатурою, що використовувались для порівняння

Характеристика	U-Prox KeyPad	Iron Logic Matrix-IV EH Keys	Hikvision DS-K1102MK	Dahua DHI-ASR1201D
Тип карт	EM-Marine	EM-Marine	EM-Marine	EM-Marine
Струм споживання,мА	40	150	150	100
Дальність зчитування,см	10	6 -10	3-5	6-8
Робочий діапазон температур, °С	0-+55	0-+50	-40-+70	-30-+60
Живлення, В	9-16	8-18	12	9-15
Ціна, грн	1405 грн	1938 грн	1201 грн	1260 грн

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 жорского 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 х 45 х 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°

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

Генератор акустичного «білого» шуму (2 канали «вібро» + 1 канал «акусто»). Призначений для захисту периметра приміщення від знімання інформації через стетоскопи, контактні мікрофони. Може створювати перешкоду для диктофонів і закладок всередині приміщення. Смуга частот 250-5000 Гц. Має канал зворотного зв'язку для налаштування рівня. Сертифікований ДЦВ ТЗІ України.

DNG-2300 призначений для захисту конфіденційної інформації від витоку через закладні пристрої, які неможливо визначити традиційними пошуковими приладами. І захисту від пристроїв встановлених по периметру приміщень, які захищаються або взагалі поза приміщеннями - провідних мікрофонів, контактних мікрофонів, передавачів, що використовують для передачі інформації мережу 220 В та інші.

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

В третьому розділі було розглянуто генеральний план об’єкту, здійснено вибір обладнання для системи захисту даного об’єкту.

Були використані зчитувачі Wiegand карток, зчитувач по відбитку пальця та IP-камери. Було зроблено аналіз технічних характеристик кожного пристрою в даній розробці.

Також було проведено економічний розрахунок засобів захисту данної банківської системи. Розрахунки показали, що окупність даної системи складуть приблизно 2 роки.

ВИСНОВКИ

В даній магістерській роботі подано систему захисту інформації на об’єкті фінансової діяльності з використанням сучасних засобів контролю та запобігання витоку інформації.

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

– проведено огляд процесу забезпечення інформаційної безпеки банківської установи;

– проаналізовано методи захисту інформації від несанкціонованого доступу в банківській установі;

– розроблено практичні рекомендацій що підвищення ефективності захисту інформації в банківській установі.

1. В першому розділі було розглянуто основні відомості про банківську систему, банківську інформацію її безпеку та основні загрози. А також розглянуто канали витоку інформації.

2. В другому розділі було розглянуто ризики банківської діяльності та її оцінка.

3. В третьому розділі було розглянуто генеральний план об’єкту, здійснено вибір обладнання для системи захисту даного об’єкту. Були використані зчитувачі Wiegand карток, зчитувач по відбитку пальця та IP-камери. Було зроблено аналіз технічних характеристик кожного пристрою в даній розробці.

Також було проведено економічний розрахунок засобів захисту даної банківської системи. Розрахунки показали, що окупність даної системи складуть приблизно 2 роки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. https://niss.gov.ua/publikacii/monografii/bankivska-bezpeka-derzhavi-v-umovakh-rozvitku-informaciynoi-ekonomiki
2. https://ru.osvita.ua/vnz/reports/bank/19767/
3. https://financial.lnu.edu.ua/wp-content/uploads/2020/11/Blashchuk_Petyk_13_end.pdf
4. ст. 200 Цивільного кодексу України
5. ст. 21 Закону України "Про інформацію"
6. ст. 60 Закону України "Про Банки і банківську діяльність"
7. https://goo.su/9oVO
8. https://biem.sumdu.edu.ua/images/stories/docs/K_CPD/Starinskii_s_015.pdf
9. https://ru.osvita.ua/vnz/reports/bank/19731/
10. https://ru.osvita.ua/vnz/reports/bank/20375/
11. https://xreferat.com/33/3607-1-metodi-zahistu-platezh-v-v-merezh-nternet.html
12. https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/
13. https://searchinform.ru/analitika-v-oblasti-ib/utechki-informatsii/sposoby-predotvrascheniya-utechki-informatsii/
14. https://buklib.net/books/27458/
15. https://old.bank.gov.ua/control/uk/publish/article?art_id=123614
16. http://global-national.in.ua/archive/16-2017/140.pdf
17. https://pidru4niki.com/81389/finansi/finansovi_riziki_sutnist_vidi_sposobi_kontrolyu_minimizatsiyi
18. http://www.economy.in.ua/pdf/12_2015/12.pdf
19. https://buklib.net/books/24194/
20. http://www.economy.in.ua/pdf/9_2010/19.pdf
21. https://ua.nesrakonk.ru/inflationrisk/
22. https://ips.ligazakon.net/document/PB04001
23. постанова Правління Національного банку України від 15 березня 2004 року N 104 "Про схвалення Методичних вказівок з інспектування банків "Система оцінки ризиків"

24. постанова Правління Національного банку України від 11 червня 2018 року № 64 "Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах"
25. https://xreferat.com/22/9945-1-bezpeka-bank-vs-ko-d-yal-nost-v-ukra-n.html
26. https://ukrreferat.com/chapters/finansy/finansova-bezpeka-bankivskoi-diyalnosti-referat.html
27. https://www.dssl.ru/publications/stati/kak-vybrat-ip-kameru/
28. https://nadzor.ua/
29. https://servak.com.ua/
30. https://www.bezpeka-shop.com/

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

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

СИСТЕМА САНКЦІОНОВАНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ НА ОБ’ЄКТІ ФІНАНСОВОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Олександр ТУНІК

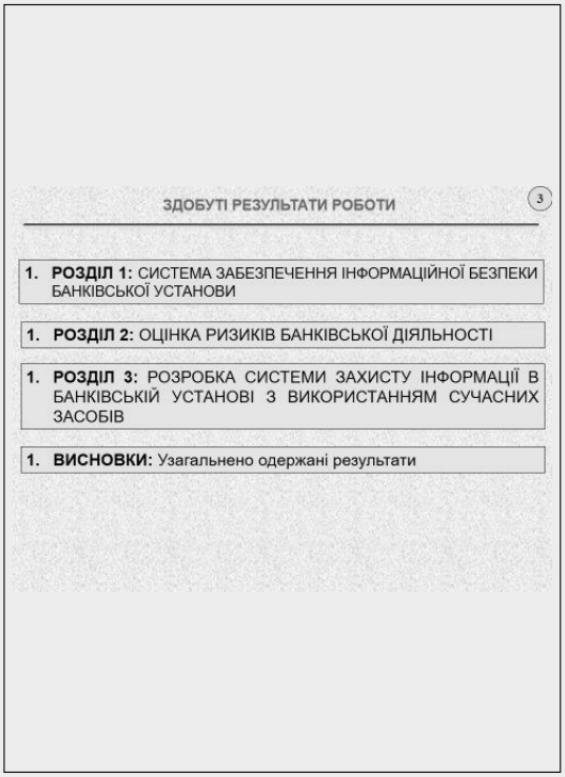
Керівник: к.т.н. Олексій ГАВРИЛЕНКО

Київ - 2025

АКТУАЛЬНІСТЬ, МЕТА ТА ЗАВДАННЯ РОБОТИ

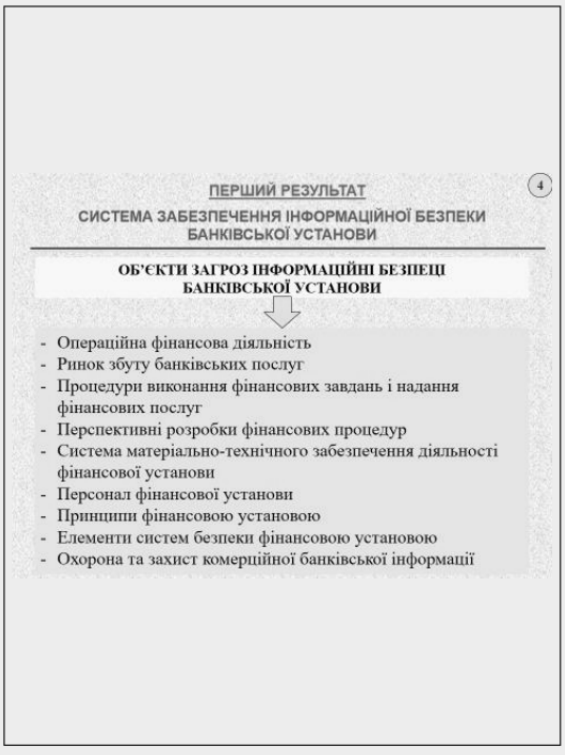
- Актуальність теми обумовлена необхідністю забезпечення захисту інформації в банківських установах від несанкціонованого доступу до каналів передачі даних.
- Мета роботи - підвищення ефективності захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.
- Об’єкт дослідження - процес обробки інформації в інформаційно-комунікаційних каналах об’єкту фінансової діяльності.
- Предмет дослідження - система захисту інформації від несанкціонованого доступу на об’єкті фінансової діяльності.
- Основні завдання: огляд інформаційної безпеки банківської установи; аналіз методів захисту; розроблення практичних рекомендацій щодо підвищення ефективності захисту.

ЗДОБУТІ РЕЗУЛЬТАТИ РОБОТИ



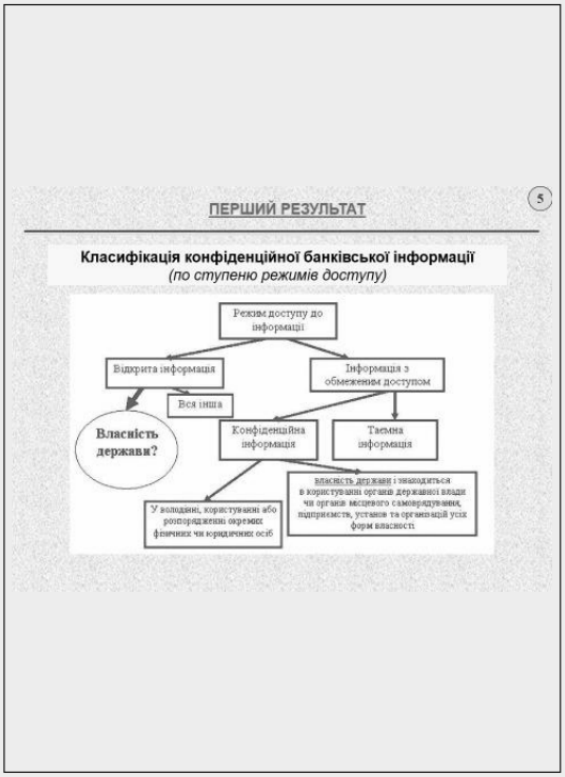
- У першому розділі розглянуто систему забезпечення інформаційної безпеки банківської установи.
- У другому розділі виконано оцінку ризиків банківської діяльності.
- У третьому розділі запропоновано систему захисту інформації з використанням сучасних засобів.
- Підсумком є формування рекомендацій щодо удосконалення системи контролю та управління доступом.

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ УСТАНОВИ



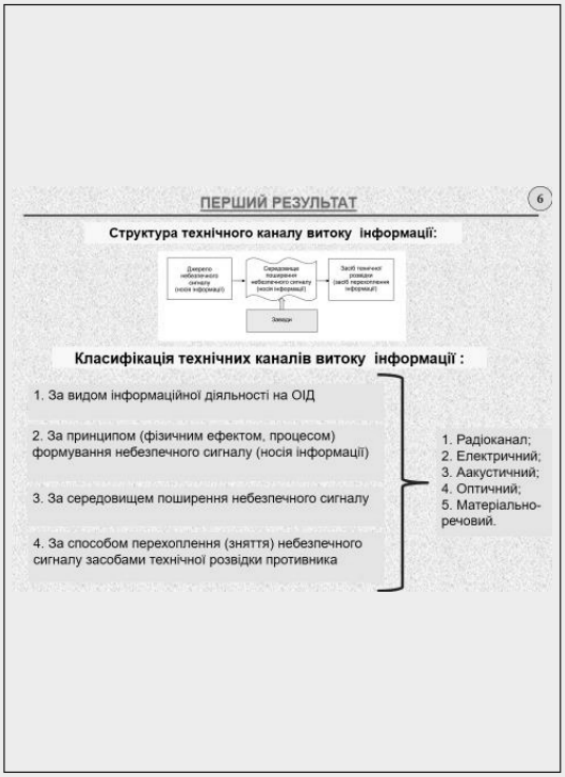
- Захист інформації банківської установи розглядається як сукупність організаційних, правових і технічних заходів.
- Особливу увагу приділено захисту банківської таємниці, платіжної інформації, персональних даних і службової інформації.
- У роботі проаналізовано криптографічні механізми, електронний підпис, контроль доступу та технології захищених каналів.

КЛАСИФІКАЦІЯ КОНФІДЕНЦІЙНОЇ БАНКІВСЬКОЇ ІНФОРМАЦІЇ



- Банківська інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.
- До інформації з обмеженим доступом належать банківська таємниця, комерційна та службова інформація.
- Виділення категорій інформації дає змогу визначити необхідний рівень захисту та режим доступу користувачів.

КАНАЛИ ПОШИРЕННЯ І ВИТОКУ ІНФОРМАЦІЇ

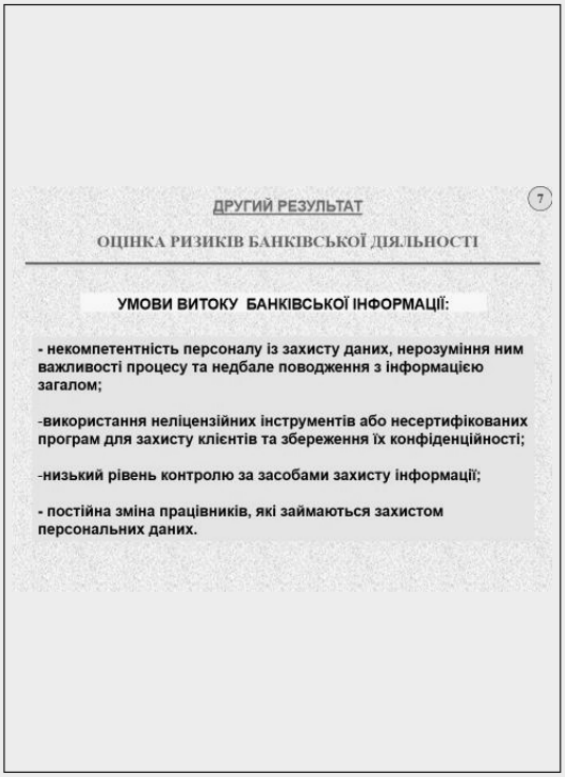


- У роботі розглянуто радіоканали, електромагнітні, акустичні, матеріально-речові та візуальні канали витоку інформації.
- Канали витоку можуть бути пов’язані з технічними засобами, приміщеннями, персоналом і мережевими каналами передачі даних.
- Для їх перекриття потрібне поєднання технічного контролю, організаційного режиму та засобів обмеження доступу.

ЗАСОБИ ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ

- Криптографічний захист забезпечує конфіденційність і цілісність інформації під час її передавання та зберігання.
- Електронний цифровий підпис використовується для автентифікації користувача та підтвердження цілісності електронного документа.
- Захищені протоколи та механізми сертифікації відкритих ключів підвищують надійність електронних фінансових операцій.
- Система контролю і управління доступом дозволяє обмежити доступ до приміщень, обладнання та інформаційних ресурсів.
- Організаційні заходи включають регламентацію прав доступу, облік користувачів, контроль персоналу та аудит дій.

ОЦІНКА РИЗИКІВ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ



- Ризики банківської діяльності пов’язані з можливістю фінансових втрат, порушенням конфіденційності даних і зниженням довіри клієнтів.
- У роботі виділено умови витоку банківської інформації та чинники, які підвищують імовірність реалізації загроз.
- Оцінка ризиків є основою для вибору адекватних технічних і організаційних засобів захисту.

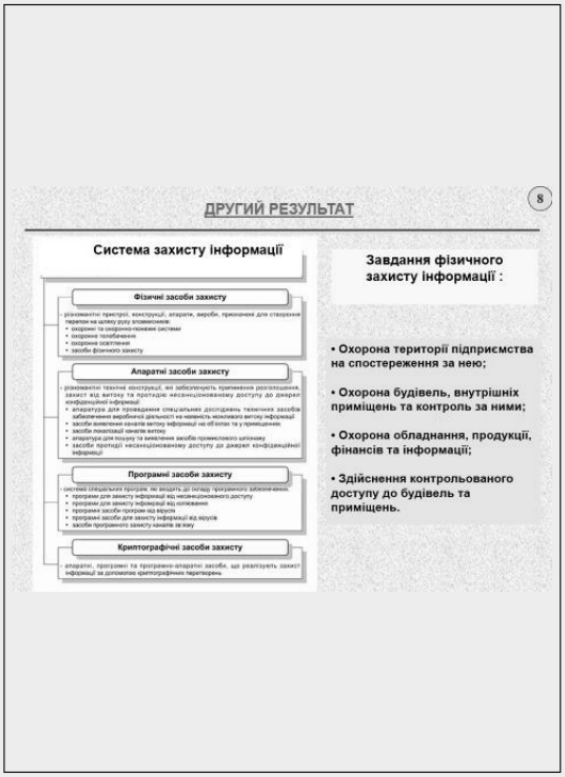
МЕТОДИКА УПРАВЛІННЯ РИЗИКАМИ ТА ДОСТУПОМ

Ідентифікація користувач / носій / зона → **Автентифікація** перевірка прав доступу → **Авторизація** дозвіл або заборона → **Контроль** реєстрація подій → **Аудит** аналіз і реагування

Логіка побудови системи санкціонованого доступу

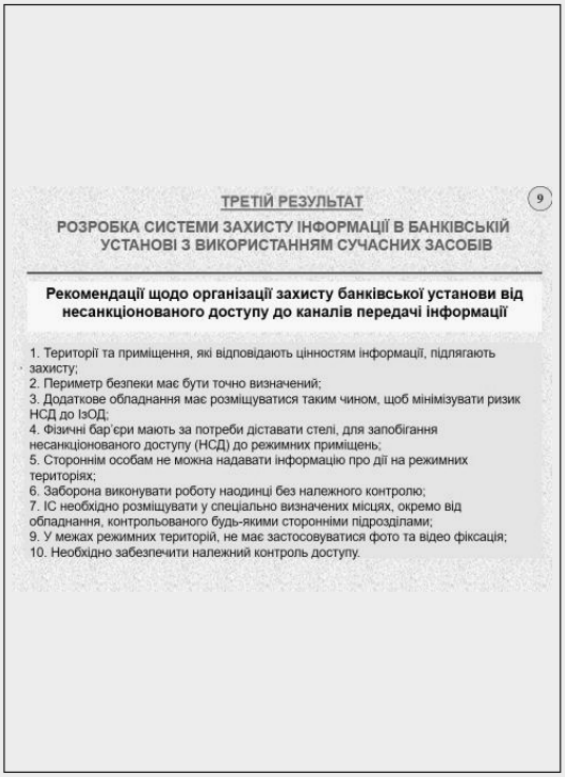
- централізоване управління правами користувачів та контроль фізичного доступу;
- виявлення інформаційних ризиків банківської установи та формування пріоритетів захисту;
- комплексне поєднання організаційних, технічних і програмних заходів безпеки.

ЗАВДАННЯ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТА ДОСТУПУ



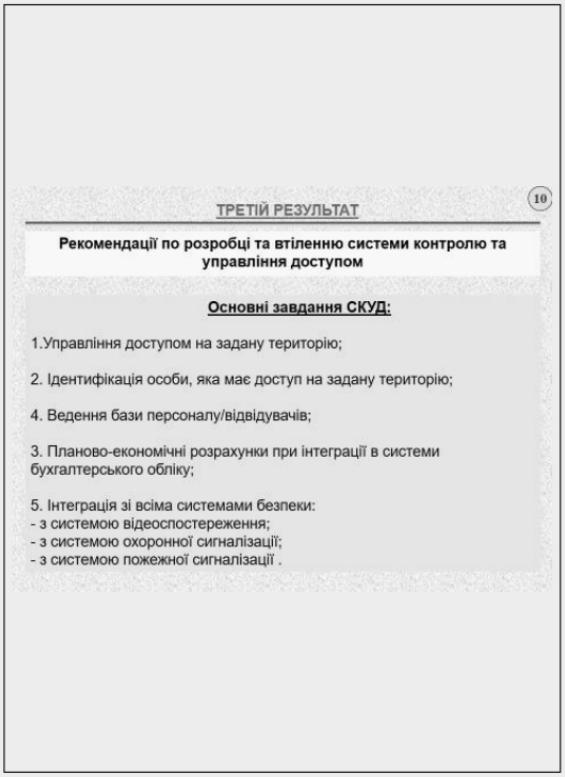
- Фізичний захист спрямований на запобігання несанкціонованому доступу до приміщень, носіїв інформації та технічних засобів.
- Система захисту передбачає формування контрольованих зон, реєстрацію проходів і розмежування прав доступу.
- Застосування СКУД дає змогу поєднати технічні засоби контролю з організаційними вимогами банківської безпеки.

РЕКОМЕНДАЦІЇ ЩОДО ОРГАНІЗАЦІЇ ЗАХИСТУ БАНКІВСЬКОЇ УСТАНОВИ



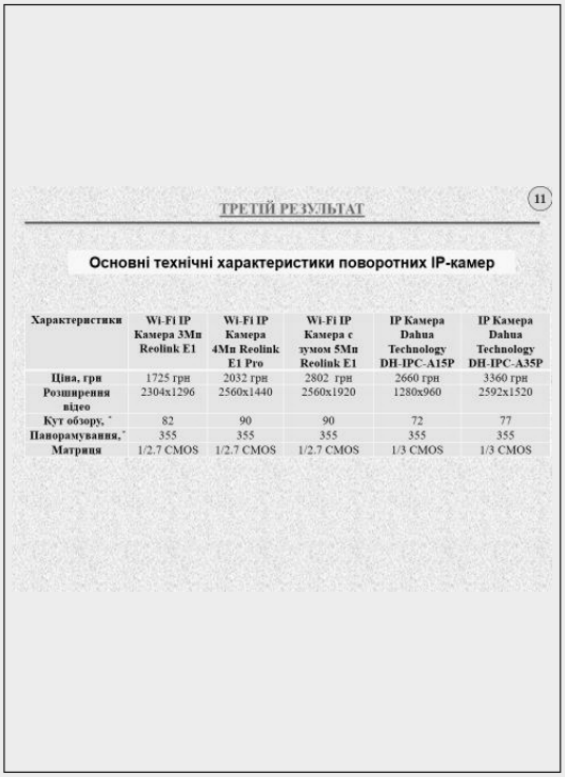
- Запропоновано рекомендації щодо організації захисту банківської установи від несанкціонованого доступу до каналів передачі інформації.
- Рекомендації охоплюють контроль території, приміщень, серверних зон, робочих місць і процедур доступу персоналу.
- Особливе значення мають регулярний аудит, навчання працівників і підтримання актуальності технічних засобів захисту.

РЕКОМЕНДАЦІЇ ПО РОЗРОБЦІ ТА ІНТЕГРАЦІЇ СКУД



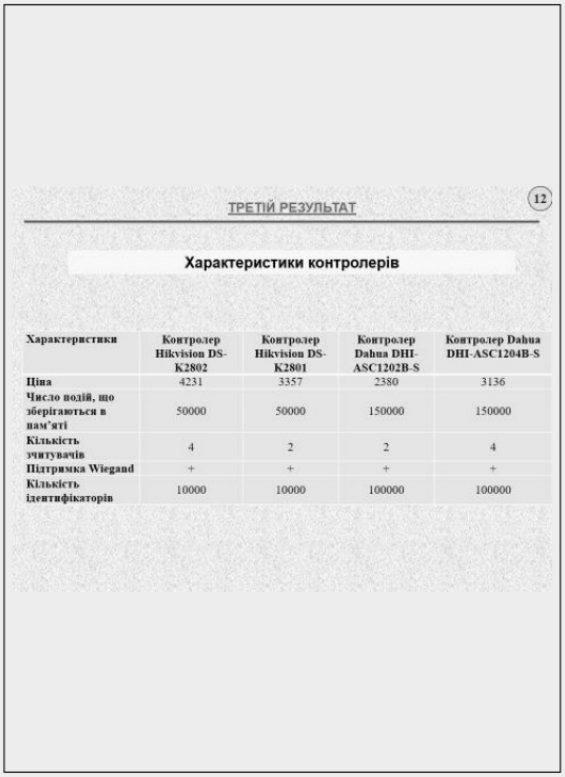
- Основні завдання СКУД: управління доступом на задану територію, ідентифікація користувачів, ведення бази персоналу та контроль подій.
- Система повинна інтегруватися з відеоспостереженням, охоронною сигналізацією та системами оповіщення.
- Для банківської установи важлива централізована реєстрація доступу та оперативне блокування прав користувачів.

ОСНОВНІ ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ПОВОРОТНИХ ТУРНІКЕТІВ



- У роботі наведено порівняльні характеристики технічних засобів контролю проходу.
- Під час вибору обладнання враховувалися ширина проходу, кількість напрямків, енергоспоживання, ресурс роботи та температурний діапазон.
- Обґрунтований вибір обладнання забезпечує надійне функціонування СКУД у режимах інтенсивної експлуатації.

ХАРАКТЕРИСТИКИ КОНТРОЛЕРІВ СКУД



- Контролер є центральним елементом СКУД, який забезпечує обробку ідентифікаторів, керування точками проходу та журналювання подій.
- Для банківської установи доцільно застосовувати контролери з підтримкою мережевого обміну, автономної роботи та достатньої кількості користувачів.
- Технічні параметри контролерів мають відповідати вимогам масштабованості та надійності системи.

ВИСНОВКИ

- Проаналізовано процес забезпечення інформаційної безпеки банківської установи та визначено основні канали можливого витоку інформації.
- Розглянуто загрози несанкціонованого доступу до конфіденційної інформації і виконано оцінку ризиків банківської діяльності.
- Запропоновано практичні рекомендації щодо підвищення ефективності захисту інформації в банківській установі.
- Обґрунтовано варіант підбору комплекту технічних засобів для побудови системи контролю та управління доступом.
- Результати роботи апробовано у матеріалах Всеукраїнської науково-практичної конференції з проблем безпеки інформаційно-телекомунікаційних систем.

ДЯКУЮ ЗА УВАГУ!

Доповідь підготував здобувач вищої освіти Олександр ТУНІК

а: «Система санкціонованого доступу користувачів до каналів передачі інформа

Київ - 2025