Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Деркача Дениса Олеговича*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему ***Обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
розділів:				
спеціальний				
економічний				

Рецензент				

Нормоконтролер				

Дніпро, 2020

ЗАТВЕРДЖЕНО:

завідувач кафедри

безпеки інформації та телекомунікацій

_____ д.т.н., проф. Корнієнко В.І.

«___» _____ 20__ року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавра

студенту ***Деркачу Д. О.*** **академічної групи** ***125м-19-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації _____

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від №

Розділ	**Зміст**	**Термін виконання**

Завдання видано _____ _____

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ ***Деркач Д. О.***

РЕФЕРАТ

Пояснювальна записка: 97 с., 1 табл., 4 додатків, 6 рис., 44 джерел.

Об’єкт: фінансово-технологічні застосунки на прикладі банківської системи.

Предмет: захист інформації у фінансово-технологічних застосунки на прикладі банківської системи.

Мета кваліфікаційної роботи: обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках на прикладі банківської системи.

В першому розділі розглянуті питання актуальності захисту інформації, використання технології блокчейн, стану фінансових технологій та їх використання у банківській сфері задля захисту інормації. Виконано постановку задач кваліфікаційної роботи.

В другому розділі описані та проаналізовані методи та засоби вирішення задачі, проаналізовано захист інформації в банківській сфері. Розглянуто питання використання технології блокчейн та її використання у фінансово-технологічних застосунках. Були надані методичні рекомендацій щодо захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках.

В третьому розділі визначено економічну доцільність впровадження методики. Проведено розрахунки капітальних витрат, поточних витрат, оцінки величини збитку та загальний ефект від впровадження методики.

ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА БЕЗПЕКА ФІНАНСОВО-ТЕХНОЛОГІЧНИХ ЗАСТОСУНКІВ, ЗАХИСТ ІНФОРМАЦІЇ У БАНКІВСЬКІЙ СФЕРІ, БЛОКЧЕЙН, БЛОКЧЕЙН У ФІНАНСОВО-ТЕХНОЛОГІЧНИХ ЗАСТОСУНКАХ, ФІНАНСОВІ ТЕХНОЛОГІЇ.

ABSTRACT

An explanatory note: 97 p., 1 table., 4 applications, 6 pic., 44 sources.

Object: financial and technological applications on the example of the banking system.

Subject: protection of information in financial and technological applications on the example of the banking system.

The purpose of the qualification work: substantiation of the method of information protection based on the use of blockchain technology in financial and technological applications on the example of the banking system.

The first part discusses the relevance of information security, the use of blockchain technology, the state of financial technologies, and their use in the banking sector. The tasks of qualification work have been set.

The second part describes and analyzes the methods and means of solving the problem, analyzes the protection of information in the banking sector. The use of blockchain technology and its use in financial and technological applications are considered. Methodical recommendations on information protection based on the use of blockchain technology in financial and technological applications were provided.

The third part identifies the economic feasibility of implementing the methodology. Calculations of capital costs, current costs, estimates of the amount of damage, and the overall effect of the implementation of the methodology.

PROTECTION OF INFORMATION, INFORMATION SECURITY OF FINANCIAL AND TECHNOLOGICAL APPLICATIONS, INFORMATION SECURITY IN THE BANKING, BLOCKCHAIN, BLOCKCHAIN IN FINANCIAL AND TECHNOLOGICAL APPLICATIONS, FINANCIAL TECHNOLOGIES.

РЕФЕРАТ

Пояснительная записка: 97 с., 1 табл., 4 приложений, 6 рис., 44 источников.

Объект: финансово-технологические приложения на примере банковской системы.

Предмет: защита информации в финансово-технологические приложения на примере банковской системы.

Цель квалификационной работы: обоснование методики защиты информации на основе использования технологии блокчейн в финансово-технологических приложениях на примере банковской системы.

В первом разделе рассмотрены вопросы актуальности защиты информации, использование технологии блокчейн, состояния финансовых технологий и их использования в банковской сфере. Выполнена постановка задач квалификационной работы.

Во втором разделе описаны и проанализированы методы и средства решения задачи, проанализированы защите информации в банковской сфере. Рассмотрены вопросы использования технологии блокчейн и ее использование в финансово-технологических приложениях. Были предоставлены методические рекомендации по защите информации на основе использования технологии блокчейн в финансово-технологических приложениях.

В третьем разделе определена экономическая целесообразность внедрения методики. Проведены расчеты капитальных затрат, текущих расходов, оценки величины ущерба и общий эффект от внедрения методики.

ЗАЩИТА ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО-ТЕХНОЛОГИЧЕСКИХ ПРИЛОЖЕНИЙ, ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКОЙ СФЕРЕ, БЛОКЧЕЙН, БЛОКЧЕЙН В ФИНАНСОВО-ТЕХНОЛОГИЧЕСКИХ ПРИЛОЖЕНИЯХ, ФИНАНСОВЫЕ ТЕХНОЛОГИИ.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АКА – автоматичний касовий апарат

АС – автоматизована система

АСОД – автоматизована система обробки даних

АСОІ – автоматизована система обробки інформації

АНБ – Агентство національної безпеки

АР – аналіз ризику

АРМ – автоматизоване робоче місце

ЕОТ – електронно-обчислювальна техніка

НСД – несанкціонований доступ

ПК – приховані канали

ШП – шкідливі програми

АТС – автоматизована електронна станція

ВПБ – виборча політика безпеки

ВУД – виборче управління доступом

ГК – головний ключ

ГПВЧ – генератор псевдовипадкових чисел

ГР – гарячий резерв

ДК – дебетова картка

ДОБ – достовірна обчислювальна база

ЕБС – електронна банківська система

ЕОМ – електронна обчислювальна машина

ЕП – електронні платежі

ЕПД – електронні платіжні документи

ЗАЗ – засекречена апаратура зв'язку

ЗМІ – засоби масової інформації

ІК – інтелектуальна картка

ІБ – інформаційна безпека

ІТС – інформаційно-телекомунікаційна система

КСЗІ – комплексна система захисту інформації

КК – кредитна картка

КАП – код автентифікації повідомлень

КЦ – контроль цілісності

КД – контроль доступу

ЛОМ – локальна обчислювальна мережа

МД – матриця доступу

НВІС – надвелика інтегральна схема

НБУ – національний банк України

ОЕД – обмін електронними документами

ОІД – об'єкт інформаційної діяльності

ОС – операційна система

ПБ – політика безпеки

ПВЧ – псевдовипадкові числа

ПЕОМ – персональна електронно- обчислювальна машина

ППБ – повноважна політика безпеки

ТЗППІ – технічні засоби переробки та передачі інформації

ЦРК – центр розповсюдження ключів

ЯБ – ядро безпеки

DES – Data Encryption Algorythm – криптосистема з секретним ключем

DSA – Digital Signature Algorythm – алгоритм цифрового підпису

MAA – Message Autentification Algorythm – стандарт для захисту цілісності даних

MAC – Message Autentification Code – код перевірки достовірності даних

MASTER CARD – кредитна картка

PC - персональний комп'ютер

PIN – персональний ідентифікаційний номер POS – розрахунок в точці продажу

RSA – (Rivest, Shamir, Adleman)– криптосистема з відкритими ключами

SKIPJACK – криптосистема з секретним ключем

SWIFT – (The Society for Worldwide inter- bank Financial Telecomunication) – система електронних платежів

VISA – кредитна картка

ЗМІСТ

ВСТУП

У сучасному суспільстві процес інформатизації набув глобального значення. Інформатизація охоплює весь спектр сучасних та майбутніх проблем - економічний, організаційний, соціальний, культурний та освітній розвиток, діяльність усіх рівнів соціального управління. Це сприяє національним інтересам, покращує керованість економікою, розвиток наукового виробництва та високих технологій, підвищує продуктивність праці та покращує соціально-економічні відносини.

Майже всі інформаційні системи містять інформацію, розголошення якої третій стороні може завдати шкоди її власнику або особі, до якої інформація стосується. Питання інформаційної безпеки (ІБ) стає особливо актуальним для підприємств та організацій, які обробляють інформацію з обмеженим доступом.

Швидкий розвиток інформатики призвів до зростання відносної важливості певних аспектів суспільного життя. Сьогодні однією з головних цінностей для суспільства та особистості загалом була інформація.

З розвитком комерційної та підприємницької діяльності зросла кількість спроб несанкціонованого доступу (НСД) до ІзОД, а проблеми її захисту суттєво збільшили потребу у фахівцях з інформаційної безпеки.

Мільйони компаній у всьому світі витрачають багато грошей на інформаційну безпеку. Це пов’язано з поступовим підвищенням рівня інформаційної злочинності.

1 ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ, ПОСТАНОВКА ЗАДАЧІ

1.2 Захист інформації

1.2.1 Поняття інформаційної безпеки

Інформаційна безпека - це “системний комплекс взаємопов’язаних запобіжних заходів запезпечення національнії інтересів у свері інформації та інформаційної діяльності; захисту інформаційного сівернітету та інформаційного простору України”. [1]

У найзагальнішому випадку інформаційна безпека -це захищеності інформаційного середовища суспільства, який забезпечує його проектування, використання та розвиток на благо громадян, організацій та держави.

В інформаційному середовищі дізнайтеся про сферу діяльності суб’єктів, які беруть участь у створенні, перетворенні та використанні інформації. Інформаційне середовище умовно поділяється на три основні частини:

- створення і розповсюдження вихідної та похідної інформації;
- формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг;
- споживання інформації; та дві забезпечувальні предметні частини:
- створення і застосування інформаційних систем, інформаційних технологій і засобів їхнього забезпечення;
- створення і застосування засобів і механізмів інформаційної безпеки.

В залежності від виду загроз інформаційній безпеці інформаційну безпеку можна розглядати наступним чином:

- як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації;
- інформації та інформаційних ресурсів від неправомірного впливу сторонніх осіб;
- інформаційних прав і свобод людини і громадянина. [2]

Сьогодні у визначенні інформаційної безпеки можна спостерігати дві тенденції. Представники правоохоронних органів рекомендують поширити інформаційну безпеку майже на всі питання та відносини в інформаційній сфері, а також представники гуманітарної сфери - з інститутом секретності.

1.2.2 Принципи інформаційної безпеки, їх характеристики

Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність. [3]

Неможливо створити систему, захист якої не можна порушити, головним принципом є створення такого механізму захисту, який буде дорожче зламати, ніж інформація, яку можна отримати. виконуючи захисні функції. За словами експерта з кібербезпеки Дмитра Ганжело: "Усунення наслідків кібератак часто обходиться в кілька разів дорожче, аніж профілактика боротьби з ними." У сучасних умовах, не гарантуючи належного захисту інформації, неможливо забезпечити стабільний економічний розвиток окремих підприємств та держави. [4]

Основними принципами забезпечення інформаційної безпеки України є:

- пріоритет прав людини;
- верховенство права;
- пріоритет договірних (мирних) засобів у вирішенні інформаційних конфліктів;
- адекватність заходів захисту національних інтересів України в інформаційній сфері реальним та потенційним загрозам;
- громадський контроль за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки України;
- додержання балансу інтересів особи, суспільства, держави, їх взаємна відповідальність;

- чітке розмежування повноважень та функцій органів державної влади в системі забезпечення інформаційної безпеки України.

В Україні забезпечення ІБ здійснюється шляхом захисту інформації — у випадку, коли необхідність захисту інформації визначена законодавством в галузі ЗІ. Для реалізації захисту інформації створюється Комплексна система захисту інформації (КСЗІ). Або, якщо суб'єкт інформаційної безпеки бажає реалізувати розробку та реалізацію політики інформаційної безпеки і може реалізувати її, не порушуючи вимог законодавства:

- міжнародними стандартами ISO: ISO/IEC 17799:2005, ISO/IEC 27001:2013 та ін. — для підтримки рішень на основі ITIL та COBIT і виконання вимог англ. Sarbanes-Oxley Act (акту Сербайнза-Оклі про відповідальність акціонерів за обізнаність про стан своїх активів). Тоді на підприємстві створюється Система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ.
- власними розробками.

Функцій забезпечення ІБ підприємств:

- розробка методів аналізу загроз, оцінки рівня інформаційної безпеки підприємства і систем її забезпечення;
- організація і здійснення діяльності із захисту інформації;
- експлуатація технічних засобів захисту інформації;
- аудит і контроль функціонування системи інформаційної безпеки підприємства. [5]

Методи забезпечення ІБ згідно рисунку 1.1:

- теоретичні методи:

  1) формалізація процесів, пов'язаних із забезпеченням ІБ;

  2) обґрунтування коректності та адекватності систем забезпечення ІБ;

– організаційні методи:

1) керування ІБ на підприємстві;

– правові методи:

1) відповідальність;

2) робота с держтаємницею;

3) захист авторських прав;

4) ліцензування та сертифікація;

– інженерно-технічні методи:

1) захист від несанкціонованого зняття інформації під час передачі технічними каналами;

– сервіси мережевої безпеки:

1) ідентифікація і аутентифікація;

2) розмежування доступу;

3) протоколювання і аудит;

4) засоби захисту периметра;

5) криптографічні засоби захисту;

Рисунок 1.1 — Методи забезпечення ІБ

1.3 Технологія блокчейн

1.3.1 Загальні відомості та принцип роботи

Останнім часом технологія блокчейн (Blockchain) активно обговорюється у всьому світі. Наша країна не є винятком. Тому ця технологія привернула увагу українських професіоналів (і не лише програмісти, представники технічних професій, а й державні діячі, нотаріуси, великі компанії готові йти в ногу з часом). [6]

Блокчейн - це структурована база даних, "блокчейн", де кожен блок пов’язаний з попереднім. Блок містить серію записів (інформації). Кожен новий блок інформації додається до кінця ланцюжка. Це створює своєрідний регістр даних, в якому дані вводяться в суворому порядку. Кількість блоків необмежена. Вміст блоку може містити будь-яку інформацію: операції, особи, предмети, операції, серійні номери, видані позики тощо.

Іншими словами, блокчейн - це розподілений загальнодоступний запис, заснований на сучасних криптографічних алгоритмах, який містить базу даних усіх раніше виконаних транзакцій, децентралізовану та розміщену на загальнодоступних ресурсах Мережі. Це структурована система, яка містить певні правила побудови ланцюгів транзакцій та доступу до інформації.

На думку розробників, ця система виключає крадіжки, шахрайство, порушення прав власності тощо. Факти, що зберігаються в блокчейні, не можна втратити. Вони залишаться там назавжди. Крім того, ланцюжок блоків зберігає не тільки кінцевий стан, але і всі попередні стану. Тому кожен може перевірити правильність остаточного стану, перераховуючи факти з самого початку.

Блокчейн працює зі складною системою шифрування (ключами). Кожен блок має свій унікальний ключ. Неможливість "розірвати ланцюг", тобто змінити блок або додати блок, забезпечується, серед іншого, тим, що коди (хеші) попереднього та наступного блоків пов'язані, і модифікація одного блоку робить це негайно, а всі інші блок за ним недійсний, що автоматично з'являється на екрані.

Хеш (hash) – це унікальний код, який змінюється, коли змінюється навіть символ у тексті, розрахований за складною математичною формулою, і завжди буде однаковим для тієї самої інформації. Отже, ви не можете мати два різних хеша для абсолютно однакової інформації. Вони використовують таку систему, особливо для захисту своєї інформації, своїх грошей, бо зрозуміло, що з ними відбувається. Це принцип: неможливо витратити більше грошей, ніж у вас, що також дозволяє контролювати всі операції, що відбуваються, де, коли і скільки витрачено. Зокрема, є пропозиції щодо використовувати хеш-кодування для забезпечення безпечної експлуатації, такі як кардіостимулятори, роботи, літаки, автономні транспортні засоби, що унеможливлюють їх розбиття. Зрештою, як кажуть прихильники впровадження системи, легше зламати центральний сервер і

отримати доступ до всієї інформації разом, змінити чи видалити її, ніж перервати децентралізовану систему. [7]

1.3.2 Переваги та надоліки

Ми можемо назвати як переваги блокчейну, так і проблеми, пов'язані з його використанням. Перевагами використання блокчейн-системи є:

- децентралізація, тобто вони використовують всю мережу, а не комп'ютер (організацію, особу тощо). У цьому випадку, навіть якщо один або кілька комп'ютерів (фізичних осіб) не можуть виконувати жодної функції (ліквідація, арешт тощо), Інші зберігають цю інформацію, що ускладнює хакерам атаку та фальсифікацію інформації (хоча ніхто від неї не захищений);
- перевіреність кожної транзакції: усі транзакції, записи тощо. є криптографічне підтвердження Зокрема, ключі бувають приватними (належать певній особі) та відкритими (якими можуть користуватися всі користувачі мережі), тобто якщо є людина або комп'ютер;
- прозорість (загальнодоступний): кожен може в будь-який час побачити, які операції були проведені;
- безпека: інформація зберігається в шифруванні;
- неможливість зміни «підписаного» блоку: інформація, введена в блокчейні, сканує перевірку, а якщо перевірка успішна, проставляється оригінальний «штамп» і ці дані синхронізуються між усіма учасниками, з цього моменту інформацію не можна змінити;
- обчислювальна логіка: цифрова природа реєстру працює таким чином, що транзакції блокчейну можуть бути пов'язані з обчислювальною логікою і фактично запрограмовані, що дозволяє користувачам налаштовувати алгоритми та правила для автоматичного виконання транзакцій між вузлами;

Перевага	Сутність переваги	Значення переваги для систем кібербезпеки банків
Децентралізація	Відсутність єдиного головного серверу зберігання даних; всі записи зберігаються у кожного учасника системи, на кожному її вузлі.	Сучасні системи кібербезпеки банків є централізованими, мають головні сервери даних, що породжує їх основну вразливість. Блокчейн-технологія дозволить під час атаки одного вузла зберегти дані на інших вузлах.
Повна прозорість системи	Всі транзакції, які відбуваються в системі, можуть відстежуватися на всіх вузлах системи.	Технологія блокчейн у банківській системі надасть можливість аналізувати всі транзакції на кожному окремому вузлі. При цьому, кожна наступна транзакція перед її виконанням перевіряється всіма вузлами системи, і не може бути здійснена при виявленні найменшої невідповідності до усіх попередньо здійснених транзакцій.
Конфіденційність	Всі дані зберігаються в зашифрованому вигляді. Користувач, відслідковуючи всі транзакції, не може розпізнати окремі дані про них, а для здійснення операцій потрібний унікальний ключ доступу.	Застосування в банківських системах блокчейнів дозволить захистити від зовнішніх кіберзлочинців та інсайдерів-співробітників особисті дані клієнтів, про їх банківські рахунки, оскільки, маючи всю історію транзакцій, злочинці не зможуть нею скористатись та ідентифікувати дані.
Захищеність від несанкціонованого доступу	Будь-яка спроба внесення несанкціонованих змін автоматично відхиляється системою через невідповідність численним копіям даних, розміщених на різних вузлах системи. Для легального внесення змін в систему та здійснення транзакцій необхідно мати спеціальний унікальний код, який видається та підтверджується системою.	Зловмисники часто здійснюють маніпуляції та фальсифікації даних в системі банку, доступ до якої отримують обхідним шляхом, використовуючи вразливості системи. Якщо зловмисник заволодіє спеціальним унікальним кодом системи, що малоймовірно, в системі завжди зберігатиметься інформація про кожну транзакцію. Будь-яке зловживання правами в системі буде відоме всім іншим її членам, і зловмисник не матиме можливості приховати сліди власного злочину.
Компроміс	Компроміс реалізується шляхом попередньої перевірки кожним членом системи даних, які додаються до неї. Прийняття рішення щодо додавання нового блоку відбувається за умови згоди всіх учасників. Досягнення консенсусу здійснюється у відповідності до одного протоколу консенсусу з урахуванням особливостей та специфіки системи.	З погляду кібербезпеки банківських операцій, проведення процедури перевірки кожної транзакції іншими вузлами системи створює додатковий бар'єр для реалізації атак. Будь-яка спроба підміни даних в одному з вузлів системи буде заблокована іншими вузлами системи, які мають свої копії усіх даних в системі. Цей механізм може захистити банківську систему від таких типів афер, як підміна кредитної історії, реквізитів рахунків, махінації із банківською звітністю тощо.

Рисунок 1.4.1 — Переваги застосування технології блокчейн у системах кібербезпеки банків [10, 11]

Коли ми говоримо про класичний тип контракту, завжди існує ймовірність того, що одна сторона порушить його. Тепер, щоб «заохотити» сторони конвенції поводитись чесно, держава використовує правові механізми, судову систему, яка забирає багато часу, грошей і рішення не завжди справедливі. Використання блокчейну прискорює, спрощує та зменшує витрати на процедуру, оскільки для укладення контракту потрібна участь обох сторін, а систему (блокчейн) не можна обдурити вже визначеними параметрами контракту. З цього випливає наступний позитив реалізації та використання блокчейну:

- економія часу (робота системи 24 години на добу, 7 днів на тиждень);
- економія ресурсів (зокрема, державних коштів).

Хоча блокчейн-технології мають значний потенціал для вирішення багатьох фінансово-економічних питань у різних секторах економіки, на практиці існують

певні нюанси впровадження таких технологій. Наприклад, технологія вимагає унікального організаційного рівня - компанії повинні погодитись на впровадження нових ресурсомістких технічних, функціональних та правових механізмів. Рисунок 1.4.1 схематично ілюструє загальні потенційні ризики, які можуть виникнути під час впровадження технології блокчейн.

Рисунок 1.4.2 — Загальні ризики пов'язані з впровадженням блокчейну [26]

Технологічні ризики. Ефективна розробка та впровадження рішень на основі блокчейну потрібно визначити та вирішити перелік технологічних ризиків та проблем. Список включає конфіденційність даних та транзакцій блокчейну, ризики безпеки, обмеження продуктивності базової платформи блокчейнів та проблеми інтеграції з іншими корпоративними системами.

Операційні ризики. Впровадження програм, заснованих на блокчейні, особливо в консорціумі кількох організацій, є складним і передбачає вирішення

ряду питань операційного ризику, таких як управління, контроль, контроль транзакцій блокчейну та посилення власності на активи.

Правові та регулятивні ризики. Блокчейн, як технологія може не регулюватися, але програми, побудовані за технологією блокчейн, повинні дотримуватися відповідних норм, таких як «Загальний регламент Європейського Союзу про захист даних (GDPR)», що стосується захисту даних та конфіденційності. Юридичні та регуляторні ризики включають невизначеність щодо норм між юрисдикційних норм, антимонопольних порушень, використання smart-контрактів, протидії відмиванню грошей (відмивання грошей) та захисту клієнтів (KYC) та захисту інтелектуальної власності (IC).

Стратегічні ризики. Інтеграція технологій блокчейну та бізнес-моделей є стратегічним вибором для організацій. Таким чином, це порушує низку стратегічних питань, таких як визначення застосовних пропозицій щодо вартості, управління брендом та репутацією та управління змінами.

Фінансові ризики. Загальною метою реалізації блокчейну є спрощення передачі значень. При розробці таких блокчейн-додатків, платформ та інфраструктури слід враховувати різні фінансові ризики, такі як ризик потенційних фінансових втрат, остаточне врегулювання транзакцій, ризики, пов'язані з фінансуванням консорціуму та захистом інтелектуальної власності. Крім того, необхідно розглянути низку питань бухгалтерського обліку та звітності, залежно від приміток до фінансових операцій та інформації, що використовується у фінансовій звітності.

Підводячи підсумок, блокчейн - це справді революційна технологія, яка дозволяє розподіленому світу досягти свого роду «консенсусу» без посередників, які можуть бути використані у всіх сферах суспільного життя (охорона здоров’я, фінанси, засоби масової інформації тощо.), оскільки:

– «народжуються» нові бізнес-моделі;

– знижується рівень шахрайства;спрощуються процеси (робота) між бізнес-агентами.

Дослідження зарубіжних центрів, що вивчають впровадження таких нових технологій, показують, що ланцюжок блоків може застосовуватися у таких сферах, як фінанси (33%), уряд (29%), охорона здоров'я (27%) та інші.

Враховуючи тенденції у цій галузі та можливість їх реалізації, можна припустити, що весь блокчейн буде використовуватися у нашому житті через 10-15 років, і лише за умови адаптації національного законодавства до нових реалій використання ІТ.

У той же час прогнози в галузі, що швидко розвивається, інформатики невдячні, і процес може бути значно прискорений. Своєрідне «тестування» впровадження технології блокчейну в нашій країні зараз відбувається в різних галузях, і їх успіх залежить від загального світогляду.

Зокрема, для забезпечення конфіденційності, ми рекомендуємо, щоб блокчейн зберігав лише виписку, а не всю інформацію про транзакцію. Крім того, безпеку цієї технології можна частково гарантувати, використовуючи відкритий, а також приватний ключ. [8, 9]

1.3.3 Механізми досягнення консенсусів

Блокчейн не тільки економічно доцільний, але і може стати плацдармом у будь-якій сфері «розумних» контрактів. Як і всі технології, блокчейн не є на 100% досконалим, тому користувачі можуть атакувати його.

Блокчейн виконує функції надійної системи, він повинен бути надійним, стабільним і захищеним, забезпечуючи такі функції, як доступність, надійність, безпека, конфіденційність, цілісність тощо.

Протокол блокчейну забезпечує це шляхом тиражування даних та операцій за допомогою декількох вузлів. Реплікація може грати багато ролей, але блокчейн копіює дані лише для стабільності, а не для масштабування. Усі вузли в принципі

підтверджують інформацію, що додається до ланцюжка блоків; ця функція стимулює впевненість усіх вузлів у тому, що блокчейн в цілому працює належним чином.

При оцінці протоколу блокчейну важливо визначити основні припущення моделі довіри або безпеки. Це визначає середовище, для якого розроблений протокол і в якому він відповідає своїм гарантіям. Такі припущення повинні охоплювати всі елементи системи, включаючи мережу, наявність синхронізованих годинників та очікувану (некоректну) поведінку вузлів.

Для кращого розуміння причин помилок необхідно визначити, наскільки процеси та канали зв'язку, що складають систему, можуть бути некоректними для даної моделі системи.

Для дослідження задачі консенсусу розподілену систему зазвичай представляють як статичну, обмежену кількість процесів П = {□1, □2, .., □□}, де зв'язок між процесами відбувається шляхом передачі повідомлень за допомогою надійного каналу точка-точка (англ. point-to-point). Процес є абстрактною частиною розподіленої системи, яка здатна виконувати обчислення [2].

Термін коректно використовується, лише якщо впродовж усього терміну виконання конкретної компоненти, такої як процес або зв’язок між процесами, не буде жодної помилкової поведінки або відхилення від встановлених правил протоколу.

Для кращого розуміння причин помилок необхідно визначити, яким чином процеси та комунікаційні канали зв’язку, що складають систему, можуть фактично некоректними за певною моделі системи. Назвемо протокол □–стійким, якщо він допускає не більше ніж □ некоректних процесів з усіх □ процесів системи. Наступний список є певним узагальненням типів збоїв або помилок (але неповним), які можуть виникати під час функціонування системи:

- Повний вихід з ладу (англ. crash failure). Найпростіша модель помилки, за якої компонента системи зазнає збою і вже ніколи не відновиться.
- Відмова виконання (англ. omission failure). За такої моделі некоректні компоненти можуть не виконувати дії, такі як надсилання повідомлень або виконання обчислень. Компоненти зі здатністю відновлення після помилки також потрапляють до цієї категорії.
- Невиконання термінів (англ. timing failure). Помилки невиконання термінів виникають при порушенні припущень щодо синхронізації. В асинхронній системі цей тип помилок не має значення.
- Візантійська відмова (англ. Byzantine failure). Візантійська відмова (яку іноді також називають довільною помилкою) дозволяє компоненту довільно відхилятись від очікуваної поведінки, 2 а отже, і робити зловмисні дії. Ця категорія включає копіювання або модифікацію вмісту повідомлень, надсилання небажаних повідомлень та тимчасову або постійну імітацію будь-якого типу із зазначених раніше відмов. [10]

1.4 Фінансові технології

1.4.1 Основні поняття та принципи

Фінансові технології, або Фінтех (англ. “FinTech”), – галузь, що складається з компаній, що використовують технології та інновації, щоб конкурувати з традиційними фінансовими організаціями в особі банків і посередників на ринку фінансових послуг. [11]

Під фінансовими технологіями слід розуміти технології, які використовуються у фінансовій галузі для оптимізації витрат, збільшення доданої вартості у своїх продуктах, швидкодії проходження всіляких процесів, без- пеки тощо.

Фінансові технології включають майже будь-яку технічну / програмну інтерпретацію фінансових процесів.

Сьогодні фінансові технології активно використовуються організаціями, які прагнуть вдосконалити та оптимізувати надання фінансових послуг. У той же час існуючі фінансові установи конкурують з так званими стартапами FinTech, які використовують комбінацію технологій, сервіс, орієнтований на клієнта, та гнучкі бізнес-структури для зменшення витрат, розширення клієнтської бази та збільшення частки ринку. Із занепадом банківського сектору та зниженням довіри населення до банківської системи України з'являється значний потенціал для розвитку галузі FinTech.

Згідно з даними опитування компанії "Pricewaterhouse Coopers" 83% компаній, що представляють традиційний сектор фінансових послуг (до них компанія відносить комерційні банки, страхові та інвестиційні компанії, брокерів та інші організації), роблять висновок, що вони можуть втратити частку бізнесу, яка може перейти до конкурентів, а саме фінансово-тех- нологічних компаній. «В разі з банками показник виявиться ще більш значущим і досягне 95%», як відзначено у звіті "PwC". [12]

У порівнянні з традиційними установами фінансових послуг, компанії FinTech мають ряд споживчих переваг. Вони розширюють можливості клієнтів, надаючи нові послуги за допомогою нових технологічних додатків. Нові цифрові фінансові технології дозволяють клієнтам отримувати доступ до інформації в будь-який час і в будь-якому місці. А онлайн-послуги здатні максимально зручно задовольнити свої потреби, що не стосується традиційних фінансових радників, які працюють за регулярним графіком "дев'ять-шість".

Компанії, що працюють у цій галузі, можна розділити на дві групи:

- стартапи, які пропонують технічні рішення для існуючих фінансових компаній;
- стартапи, які працюють безпосередньо зі споживачами фінансових послуг.

Фінтех-компанії працюють у наступних сферах:

- Управління особистими фінансами, тобто впровадження мобільних і десктопних програм, що дають змогу стежити за рухами особистих коштів, отримувати докладні звіти і припущення про майбутні витрати на основі предик- тивного аналізу.
- Платежі – напрям фінансових технологій, що пропонує суттєво прогресивніші підходи до фінансових транзакцій.
- Кредитування P2P (peer-to-peer) – стартапи у сфері кредитування без участі банківської установи на основі розподілених техноло- гій. P2P-кредитування передбачає отримання/ надання кредитів від людини до людини без участі фінансових установ.
- Інвестиційні платформи – напрям фінансових технологій, що пропонує автоматизацію інвестування із застосуванням предиктивного аналізу на основі великих даних. Інновації на цьому напрямі полягають в автоматизації процесу прийняття рішень. Створюються спеціальні фінансові сервіси, а саме роботи-консультанти (robots-advisors), які в режимі онлайн автоматично генерують інвестиційні рішення, сформовані на основі обробки інформації за певним алгоритмом. Робот-консультант оцінює інформацію про потенційного інвестора для визначення цілей інвестування та його схильності до ризику. Після оброблення даних про клієнта і доступної інформації з фондового ринку робот-консультант пропонує способи формування оптимального інвестиційного портфеля.
- Колективне фінансування (краудфандінг) – вид фінансування за допомогою збору коштів на реалізацію будь-якого проекту через Інтернет. Сьогодні найбільш популярними майданчиками для отримання венчурного фінансування лишаються Kickstarter і Indiegogo. Однак ринок відкритий для нових ідей, безліч компа- ній пропонують свої рішення, що дають змогу інвесторам і стартаперам знайти один одного.

- Безпека – надання сервісу для банківських установ на основі спрощення та автоматизації питання аутентифікації клієнтів та розроблення заходів щодо боротьби з шахрайством.
- B2B-фінтех – окремий напрям фінтеху, що вирішує проблеми розрахунків та обміну даними в бізнесі. Останнім перспективним трендом цієї діяльності є розробка смарт-контрактів на основі блокчейна.
- Грошові перекази. На відміну від стартапів у сфері платежів, компанії цього напряму працюють над інноваціями, що дають змогу переказувати грошові кошти без участі банківських установ. Як правило, технологія передбачає просту і зрозумілу мобільну платформу та використання альтернативних підходів до аутентифікації клієнтів (наприклад, через соціальні мережі).
- Аналіз Великих даних, тобто наборів інформації (як структурованої, так і неструктурованої) настільки великих розмірів, що традиційні способи та підходи (здебільшого засновані на рішеннях класу бізнесової аналітики та системах управління базами даних) не можуть бути застосовані до них. Великі дані дають можливість проаналізувати кредитоспроможність позичальника, зменшити час розгляду кредитних заявок. За допомогою Великих даних можна проаналізувати операції конкретного клієнта і запропонувати відповідні саме йому банківські послуги.
- РегТех – унікальний напрям інновацій, що дає змогу швидко та автоматизовано адаптувати бізнес до змін законодавства та умов ринку.
- InsureTech – стартап у сфері страхових технологій, що пропонує ринку повністю автоматизовані страхові продукти, зокрема мобільні додатки, взаємодію на рівні Інтернету речей, P2P-страхування, автоматизацію регрес- них виплат. Сучасному користувачу вже пропонується не тільки сервіс для дистанційного укладання договору через сайт страхової компанії, але й нові види страхування та різні додаткові можливості, наприклад короткострокове страхування через мобільні пристрої, онлайн-доступ до баз даних для зберігання інформації про застраховане майно.

- Штучний інтелект – впровадження рішень, які дають змогу скоротити найбільш значні витрати фінансових компаній, тобто витрати на персонал.
- Необанки (банкичеленджери) – це повністю онлайн-банки (без філіальної мережі), побудовані з чистого аркуша на нових технологічних платформах, на відміну від застарі- лої інфраструктури традиційних банків. Як правило, необанки пропонують більш високі процентні ставки, низький рівень комісій (або взагалі їх відсутність) і більш високий клас обслуговування та підтримки.
- Криптовалюта – вид цифрових грошей, в якому використовуються розподілені мережі та публічно доступні журнали реєстрації угод, а ключові ідеї криптографії поєднані в них з грошовою системою заради можливості створити безпечну, анонімну та потенційно стабільну віртуальну валюту До фінтестартапів у сфері криптовалюти відносяться криптобіржі, обмінники, майнінгові компанії, інвестиційні та ICO- майданчики.
- Блокчейн – це розподілена база даних, у якій зберігається інформація про кожну транзакцію, вироблену в системі. Використання блокчейн-рішень можливе в будь-якій сфері, зокрема у фінансових технологіях. Найбільш відомим рішенням в банківських транзакціях є платформа Ripple. [13]

Зазначимо, що наведена класифікація є досить умовною, оскільки інноваційні підходи постійно змінюються.

Якщо взяти до уваги аналітичні дані про діяльність Fintech, то в першій половині 2020 року інвестиції в цю галузь перевищили 20 мільярдів доларів. [14]

Фахівці стверджують, що в українському FinTech-секторі вже виявлено понад 100 стартапів різної складності, причому 77% українських FinTech-компаній засновані у 2012–2017 роках; серед засновників компаній є банкіри, інженери, IT-фахівці. При цьому 65% компаній фінансуються засновниками, а топ-менеджмент сформований з колишніх співробітників «ПриватБанку», «ПУМБ», «Райффайзен Банку Аваль», «Універсал Банку». Згідно з дослідженням

73% FinTech-компаній створюють сервіси для масового сегменту, 19% – для середнього та малого бізнесу, 8% – інші; 38,5% всіх сервісів розвиваються в напрямі платежів та грошових переказів, 19% – кредитування та мікрокредитування для P2P, B2C, P2B. [15]

Було встановлено, що одним із визначальних факторів розвитку сучасної фінансової системи є впровадження фінансових технологій та діяльність компаній FinTech. Зосереджуючись на сегменті, який не охоплюється банківськими послугами та використовує сучасні цифрові канали, він не лише швидко збільшує участь громадськості у фінансовому секторі, але й досить швидко розширює бізнес українських фальшивих компаній.

1.4.2 Блокчейн та фінансові технології

Одним з нових інноваційно платіжних інструментів є технологія блокчейн, тому вплив використання цієї технології на фінансову безпеку потребує досліджень. Поглиблення високотехно логічної технології сприяє економічному розвитку країни. Блокчейн сприятиме роз- витку інноваційних технологій та цифрової економіки знань в Україні. Потребують впровадження відповідні цифрові технології, послуги та системи, які будуть здатні протидіяти сучасним загрозам та гаранту- вати фінансову безпеку держави. Поширення блокчейну є найбільшою подією, що відбувається у сфері розвитку валютно-фінансових відносин та приведе до глибинних змін у банківській системи. У фінансовій сфері настає час технології блокчейн. Глобалізація та вдосконалення технології на базі блокчейну приводить до структурних змін у валютно-фінансових та кредитних відносинах. Це приводить до децентралізації фінансової сфери, зміни ролі держави, центрального банку, а валютно-фінансові відносини позбуваються національної належності та стають дійсно глобальними.

Головною умовою функціонування економічно стійкої та соціально стабільної країни є забезпечення стабільності фінансової безпеки. Темпи розвитку соціально-економічного прогресу держави значною мірою залежать від стану

сформованості фінансової безпеки країни. Отже, фінансова безпека є забезпеченням розвитку фінансової системи та процесів в економіці задля створення необ- хідних умов для соціально-економічної стабільності та збереження цілісності фінансової системи. Фінансова безпека виконує роль регулятора стійкості економічного розвитку країни, платіжної системи, а також дає змогу нейтралізувати вплив світових фінансових криз на національну систему держави. На жаль, сьогодні валютна складова фінансової безпеки України перебуває під впливом певних проблем, таких як геополітична ситуація, вплив діяльності міжнародних організацій, інфляційні процеси, відсутність чіткої нормативно-правової бази.

Отже, зростає потреба підвищення рівня валютної безпеки України через зростання негативних тенденцій в динаміці платіжного балансу, страху світової кризи та девальваційних очікувань. Головною метою валютного регулювання є набуття таких характеристик, як спрощеність, захищеність, зростання довіри, зрозумілість валют- ного регулювання. Нині прослідковується втрата впевненості громадян у фінансовій системі, адже довіра вкладників до банків знижується. Задля досягнення названої мети необхідно створити технологію, яка б відповідала певним вимогам. [16]

У 2009 році з'явилась технологія блокчейн, яка полягає в записі цифрових тран- закцій на основі величезної бази даних. Блокчейн-технологія – це спосіб зберігання даних у вигляді взаємопов'язаного ланцюга блоків. Шифрування здійснює велика кількість комп'ютерів, що працюють в одній мережі. Кожен блок пов'язаний з попереднім та містить набір записів. Нові блоки завжди додаються в кінець ланцюжка. Тільки-но утворюється новий блок, реєстр оновлюється, тому блок вже не може бути змінений, що унеможливлює його підробку. Слід зазначити, що реєстр оновлюється на всіх комп'ютерах в мережі одночасно. [17]

Технологія блокчейн має багато способів використання: від проведення платежів та створення цифрових гаманців до бірж криптовалюти та блокчейн-

платформ. Блокчейн дійсно може суттєво змінити світову економіку, як свого часу її змінив комп'ютер. [18]

В Азійсько-Тихоокеанському регіоні зосереджена значна частина потужностей з майнінгу криптовалюти. Цей регіон зазнав суттєвих змін, адже відбулося зростання промисловості та руху товарів між країнами. Отже, тут є всі передумови поширення технології блокчейн. У грудні 2016 року центральний банк Китайської Народної Республіки протестував власну цифрову валюту, а саме цифровий юань. Нині Китай планує перевести на блокчейн національний фонд соціального страхування, в управлінні якого перебуває близько $250 млрд. В результаті запровадження національної цифрової валюти в Китаї центральний банк отримає інформацію про те, як працює економіка, виникає можливість регулювання інфляції, зниження операційних витрат, використання різних нових додатків, а також з'являються нові можливості універсального контролю з боку держави. [19, 20]

Ще одним прикладом використання технології блокчейн є проект земельного кадастру на основі блокчейн для Грузії у 2016 році. Це дасть можливість підвищити рівень безпеки та прискорити процес оформлення документів, а також сприятиме зниженню вартості реєстрації прав на землю з 50–200$ до 5–10 центів. [21]

Отже, блокчейн є інноваційним продуктом багатьох світових інституцій та держав- них регуляторів, який дає змогу не тільки комплексно модернізувати застарілі сис- теми, але й ефективно боротися з корупцією та кіберзлочинністю. Європейський Союз інвестував понад $6 млн. в стартапи, які розробляють або вивчають застосування технології блокчейн через програму "Horizon 2020". [22]

З 2018 року державна Третьяковська гале- рея оцифровує свою колекцію на приватні пожертвування в рамках блокчейн-проекту "My Tretyakov". Механізм оцифрування матиме такий вигляд: спочатку особа або компанія жертвує гроші на оцифрування експоната, що перебуває в галереї, та стає його патроном. При

цьому система випадковим чином вибирає одиницю зберігання, яка прикріплюється за цим патроном та зв'язує його ім'я з предметом. Саме такий зв'язок імені або назви компанії з оцифрованим експонатом закріплюється за допомогою блокчейн-технології, розробленої австрійською компанією "Riddle & Code". Метою проекту є здолання географічних обмежень задля зближення осіб, що цікавляться мистецтвом. Це нововведення залучить молоду аудиторію, кожен матиме інформацію про «опікуваний» їм експонат, а також зможе розміщувати його у своїй галереї для інших користувачів. [23]

Останнім з нововведень у галузі технології блокчейн є відкриття Центру блокчейну в Женеві швейцарською компанією "WISeKey". Центр блокчейну надаватиме підтримку різних стартапів, які працюють на основі технології блокчейн, а також дасть змогу просу- вати цю технологію розподіленого реєстру. Компанія "WISeKey" сприятиме прийняттю технології блокчейну як у державному секторі, так і в приватному. Ця компанія займається розробленням безпечної авторизації та ідентифікації особистості. Відкриття нового центру стало частиною спільного проекту з Інститутом дослідження блокчейну (BRI). Планується відкриття центрів в інших країнах (США, Китай, Індія, Африка). Кожен центр буде спеціалізуватись на певній галузі. Центр блокчейну в Женеві спеціалізується на фінансових технологіях. Головною метою такої мережі центрів виступатиме координація цих компаній за рахунок навчання практичним знанням щодо застосування технології блокчейн та обміну ними. [24]

Отже, технологія блокчейн є багатофункціональною та багаторівневою інформаційною технологією, адже охоплює всі сфери економічної діяльності та застосовується в багатьох галузях. Блокчейн дає нові можливості з пошуку, організації, оцінювання та передачі будь-яких дискретних одиниць. Директор Міжнародного валютного фонду Крістін Лагард висловила свою думку про нові технології. Вона стверджує, що блокчейн очікує таке ж майбутнє, як Інтернет, адже ця технологія запевняє у відсутності потреби у фінансових посередниках або центральних банках, що докорінно змінює банківську діяльність та створює

альтернативу національним грошам. Населення віддаватиме перевагу віртуальній валюті, адже це є швидшим, простішим та безпечнішим способом, ніж одержання паперових грошей. З огляду на важливість технології блокчейну для людства її подальший розвиток бажано проводити на принципах державно-приватного партнерства. [25]

Отже, можна стверджувати, що технологія блокчейн справді здатна суттєво вплинути на подальший розвиток фінансового сектору. Основна перевага технології блокчейн полягає у відсутності необхідності в централізованому органі. Ця особливість кидає виклик традиційним фінансовим інститутам, адже використання технології блокчейн дасть змогу позбутись як централізованих посередників, так і зовнішнього контролю. Сучасні проекти дають змогу значно скоротити трансакційні витрати на міжбанківські платежі, здійснення клірингу та розрахунків щодо фінансових інструментів.

Таким чином, вважаємо що технологія блокчейн має достатню кількість переваг як економічного, так технологічного характеру. Проте існує певна кількість ризиків через відсутність практичних навичок використання цієї технології, несприйняття нововведення, виникнення способів злому криптографічних шифрів, а також зловживання технологією через підробку децентралізованих систем централізованими. Також існує загроза використання цієї технології через незначний досвід використання, недостатню базу розробок кібербезпеки для технології, неможливість скасування транзакції після підтвердження, складність адаптації до інших розрахункових систем.

Розглянувши переваги та недоліки використання цієї технології, ми звертаємо увагу на те, що блокчейн справді максимально сильно вплине на фінансовий сектор. З 2022 року, згідно з даними іспанського банку “Santander”, впровадження блокчейну може зменшити банківські витрати на інфраструктуру в секторі міжнародних платежів, операцій з цінними паперами та дотримання вимог регулюючих органів на $15–20 млрд. [26]

Особливий вплив технологія блокчейн здійснить на банківську сферу, адже дасть змогу захистити клієнтів банків від шахраїв, підвищити довіру до банків, зберігати інформацію про кредитні історії клієнтів та їх рахунки, а створення систем smart-контрактів прискорить швидкість документообігу, розширить асортимент послуг банку та зменшить витрати на інкасацію.

Отже, технологія блокчейн справді суттєво вплине на підтримання безпеки, знизивши ризики та скоротивши витрати банків, оскільки зникає можливість виникнення помилок, зловживань та збільшується швидкість проведення транзакцій. Усвідомлюючи потенціал блокчейну, більше 40 банків по всьому світі вже інвестували певну кількість грошей у впровадження цієї технології у свої системи, адже вони розуміють, що існує можливість працювати без посередника, а це приведе до заощаджень цих банків на суму в мільярди доларів. Заощаджені кошти тепер можна буде ефективно інвестувати в реалізацію бізнес-проектів задля отримання більших прибутків. [27]

Технологія блокчейн може вплинути не лише на фінансову безпеку країни, але й на інші галузі, особливо людську діяльність. Впровадження технології блокчейн дає можливість усунути взаємну недовіру населення, викликану відсутністю достатньої прозорості. Банківська діяльність, державне управління, суспільні відносини повинні бути побудовані на взаємній довірі.

Отже, слід зазначити, що використання блокчейн-технології суттєво збільшить швидкість, прозорість та ефективність фінансових систем. Довіра населення до цієї технології буде ґрунтуватись на тому, що блокчейн стає найпрозорішим засобом зв'язку між державою та населенням, виключаючи будь-які посередницькі інститути. Технологія блокчейн забезпечує прозорість усіх транзакцій, адже проводиться їх ретельний запис, здійснюються аналіз та збереження. Отже, серед учасників блокчейну є довіра, адже не потрібно нічого підтверджувати або надавати сертифікати про учасників транзакцій. Проте багато людей поки що просто не розуміють силу цієї технології. [28]

Основою безпеки технології блокчейн також є його децентралізація, яка забезпечить зростання безпеки інформації, адже здебільшого шахраї атакують централізовані вузли управління для отримання необхідної інформації. Проте у блокчейні кожен вузол мережі має свою копію бази даних з усіма транзакціями. При цьому окремі вузли розташовані по всій планеті, що й виступає 100% гарантією безпеки блоків даних. Ця технологія дасть змогу підвищити безпеку в такому напрямі, як автентифікація банківських посвідчень, отже, за допомогою блокчейна можна автентифікувати користувачів без використання паролів та із забезпеченням безпеки внутрішніх комунікацій від кібершпигунства та витоку інформації.

З огляду на най- більш актуальні проблеми фінансової без- пеки України постає необхідність застосування технології блокчейн у бюджетній системі. Отже, можемо зробити висновок, що потенціал блокчейну є багатообіцяючим, адже ця технологія дає можливість користувачам записувати інформацію та обмінюватись нею. Блокчейн викликає справжню довіру, коли незалежні учасники зберігають власні копії важливої інформації завдяки розподіленим блокчейн-системам. Також відсутня необхідність єдиного органу управління процесом, адже тільки учасники транзакції можуть бачити інформацію та вносити зміни. Застосування цієї технології на практиці дасть змогу покращити контроль за дотриманням норм нормативно-правового регулювання, спростити видачу документа ції щодо транзакцій, підвищити прозорість функціонування фінансової системи.

Слід сказати про еволюційне значення блокчейну, який дійсно вплине на стан фінансової безпеки країни, перш за все на банківську сферу, для якої цінною є безпека зберігання та оброблення електронних даних. Фахівці іспанського банку “Santander” зробили підрахунки, що до 2022 року світові банки за допомогою технології блокчейн зможуть зменшити витрати на $15–20 млрд. Із соціальної точки зору ця технологія дасть поштовх для глобальних змін в організації суспільства. Біль- шість установ потребує певного часу для усвідомлення переваг

блокчейну, але мало хто залишиться осторонь від перетворень на основі цієї технології, адже вона істотно полегшить платежі та онлайн-транзакції, повністю змінить уявлення суспільства про побудову довірчих відносин. Метою технології блокчейну є створення прозорої та доступної системи запису та кодування транзакцій, що значно підвищить інвестиційну привабливість країни.

1.5 Постановка задачі

Метою є обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках на прикладі банківської системи.

Завдання:

- аналіз захисту інформації банківських систем;
- аналіз банківських операцій, їх автоматизації та захисту;
- характеристика принципів захисту інформації в банківських системах та їх особливості;
- існуючі методики захисту інформації у банківських системах;
- розробка методичних рекомендацій на основі використання технології блокчейн;

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз захист інформації в банківській сфері

Стрімкий розвиток інформаційних технологій, розширення глобального інформаційного середовища, широке застосування засобів обміну інформацією, всеохоплююча комп'ютеризація всіх сфер життєдіяльності зумовлюють актуальність дослідження питань безпеки інформаційної інфраструктури. Забезпечення ефективного захисту інформації є надзвичайно актуальним і для установ банківської сфери, де щоденно оброблюється великий обсяг інформації різного рівня конфіденційності. Ця інформація в більшості випадків і виступає

об'єктом дій конкурентів, що і обумовлює загострення питань захисту інформації від її незаконного використання і несанкціонованого доступу до неї. Застосування сучасних інформаційних технологій в банківських системах розширює можливості для різних зловживань, пов’язаних з використанням обчислювальної техніки (так званих комп'ютерних злочинів). Щорічні втрати від злочинів в цій сфері складають в світі, по різних оцінках, від 170 млн. до 10 млрд. Дол.» [29]

Не можна не погодитися з тезою, що «одним із найважливіших критеріїв функціонування банківської системи є інформаційна безпека як всієї системи, так і її частин: центрального і комерційних банків». [30]

Під інформаційною безпекою банку будемо розуміти стан інформаційної інфраструктури банку, за якого забезпечуються умови стабільного функціонування, максимізації прибутку, оптимального використання ресурсів банку, а також забезпечується захищеність клієнтів, співробітників і керівництва банку від зовнішніх і внутрішніх загроз.

Законодавчо-нормативне регулювання захисту інформаційних ресурсів банківських установ представлено нормами Закону України «Про банки і банківську діяльність» і Закону України «Про інформацію». Окрім того в питаннях інформаційної безпеки банківських установ важливе місце займають і вимоги нормативно-правових актів НБУ з питань організації та управління інформаційною безпекою. Так, з метою підвищення рівня інформаційної безпеки установ банківської сфери з 2010 р. в Україні (відповідно до Постанови НБУ No474 від 28.10.2010р.) діють стандарти НБУ: СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності Система управління інформаційною безпекою. Вимоги» (ISO / IES 27001:2005, MOD); СОУ Н НБУ 65.1 СУІБ 2.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO / IES 27002:2005, MOD). [31]

Важливим документом є також «Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки

ризиків відповідно до стандартів Національного банку України від 01.03.2011р.». [32]

Ці методичні рекомендації розроблені на основі міжнародного стандарту ISO/IEC 27003:2010 з урахуванням особливостей банківської діяльності, стандартів та вимог Національного банку України з питань інформаційної безпеки.

На сьогодні в питаннях інформаційної безпеки прийняті, зокрема, такі міжнародні стандарти:

- серія ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою»: ISO/IEC 27000:2009. Визначення і основні принципи; ISO/IEC 27001:2005. Інформаційні технології – Методики безпеки – Системи менеджменту інформаційної безпеки – Вимоги (BS 7799-2:2005); ISO/IEC 27002:2005. Інформаційні технології – Методики безпеки – Практичні правила управління інформаційною безпекою; ISO/IEC 27003:2010. Настанова з впровадження системи управління інформаційною безпекою; ISO/IEC 27005:2008. Інформаційні технології – Методика безпеки – Управління ризиками інформаційної безпеки (на основі стандарту BS 7799-3:2006); ISO/IEC 27006:2007. Інформаційні технології – Методики безпеки – Вимоги до організації, що провадять аудит і сертифікацію систем менеджменту інформаційної безпеки; ISO/IEC 27011:2008. Керівництво з менеджменту інформаційної безпеки для телекомунікацій; ISO/IEC 15408. Загальні критерії оцінки безпеки інформаційних технологій;
- серія ISO 13335 «Міжнародні стандарти безпеки інформаційних технологій»: ISO 13335-1:2004. Інформаційні технології – Керівництво по управлінню IT безпекою – Концепції і моделі для управління безпекою інформаційних і телекомунікаційних технологій; ISO 13335-3:1998. Інформаційні технології – Керівництво по управлінню IT безпекою – Методи управління IT безпекою; ISO 13335-4:2000. Інформаційні технології

– Керівництво по управлінню IT безпекою – Вибір механізмів захисту; ISO 13335-5:2001. Інформаційні технології – Керівництво по управлінню IT безпекою – Керівництво по управлінню мережевою безпекою.

Основними характеристиками інформаційної безпеки банків виступають:

- об'єктами безпеки є: інформація про персонал (керівництво, відповідальні виконавці, співробітники); інформація щодо технологій, які використовуються банком; інформаційні ресурси (інформація щодо діяльності та фінансового стану клієнта, що стала відома банку у процесі обслуговування; інформація щодо всіх операцій банку та фінансова звітність банку; конфіденційні електронні мережі банку);
- головною метою системи інформаційної безпеки є забезпечення стійкого функціонування банку і запобігання погроз його безпеці, захист від протиправних посягань, розголошення, утрати, витоку, перекручування і знищення службової інформації, порушення роботи технічних засобів, забезпечення виробничої діяльності, включаючи і засоби інформатизації;
- до основних завдань, які повинна вирішувати інформаційна безпека банку, належать: забезпечення доступу керівництва банку до конфіденційної ринкової інформації; запобігання витоку і руйнуванню конфіденційної банківської інформації; забезпечення поширення у зовнішньому середовищі вигідної для банку «конфіденційної» інформації [33]

Окремо зупинимося на питанні попередження, виявлення та мінімізації загроз банківській інформаційній безпеці. Останні за своєю суттю представляють собою сукупність внутрішніх та зовнішніх умов, які направлені на порушення нормальних умов функціонування інформаційної інфраструктури банку та можуть нанести шкоду інтересам його власників, співробітників та клієнтів.

Узагальнюючи дослідження вітчизняних та зарубіжних вчених- економістів можна виділити наступні види загроз інформаційній безпеці банківських установ: протиправне збирання інформації та її використання; порушення технології і

правил опрацювання інформації; впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби; розроблення і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем банківських установ; несанкціонований доступ до інформації, що є в банківських установах і їхніх базах даних; перехоплення інформації, що циркулює в засобах і системах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу до інформації та навмисних технічних впливів на них в процесі обробки та зберігання; підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях. [34, 35]

Всі загрози можна згрупувати наступним чином:

- випадкові загрози: помилки, а також події, що не залежать від людини (природні явища або викликані діяльністю людини);
- навмисні загрози: можуть реалізуватися учасниками процесу обробки інформації (копіювання і крадіжка програмного забезпечення; несанкціоноване введення даних; зміна або знищення даних на магнітних носіях; крадіжка інформації; несанкціоноване використання ресурсів комп'ютерів; несанкціоноване використання банківських автоматизованих систем; несанкціонований доступ до інформації високого рівня секретності; знищення інформації);
- перекручення інформації: зміна її змісту, порушення її цілісності, в тому числі і часткове знищення. [36]

Цікавими є результати дослідження спецслужбами факторів, які створюють умови витоку інформації:

- надмірна балакучість співробітників банків (32%);
- прагнення працівників банків заробляти гроші будь-яким способом і будь-якою ціною (24%);

- відсутність у банку системи заходів, спрямованих на захист інформації (14%);
- звичка співробітників банків ділитись один з одним почутими новинами, чутками, інформацією (12%);
- безконтрольне використання інформаційних систем (10%);
- наявність передумов для виникнення серед співробітників конфліктних ситуацій (8%). [37]

Виокремлення численних видів загроз інформаційній безпеці практично повністю повторює існуючу класифікацію ризиків інформаційної безпеки:

- загроза – це такий розвиток подій, дія (бездіяльність), в результаті яких з'являється можливість або підвищується ймовірність порушення нормального функціонування підприємства й недосягнення ним своїх цілей, зокрема нанесення підприємству будь-якого виду збитку;
- ризик – це ведення діяльності в умовах невизначеності або ж взагалі сама невизначеність умов і результатів діяльності, а загроза – це вже цілком певний негативний розвиток подій. Отже, загроза – це заздалегідь відомий сценарій несприятливого розвитку подій, що почав реалізовуватися за небажаним варіантом, і який відповідно виходить за рамки поняття нормальної невизначеності умов господарської діяльності.

Існування ризикових факторів обумовлює необхідність раціонального управління ними, ґрунтовно та адекватно оцінювати структуру й міру ризику, намагаючись знизити ступінь ризику до допустимого. [38]

Метою заходів щодо забезпечення інформаційної безпеки є скорочення можливих економічних і моральних збитків банківської установи, пов'язаних з пошкодженням або неправомірним використанням інформаційних ресурсів, а саме:

- захистити інформацію з обмеженим доступом від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності);
- забезпечити цілісність і доступність інформації, що обробляється, зберігається, в системах та комп'ютерних мережах банківської установи;
- протидіяти поширенню недостовірної, заздалегідь неправдивої інформації про банківську установу, здійсненню негативних інформаційних впливів на її керівництво.

Таким чином, забезпечення інформаційної безпеки банківських установ є актуальним та нагальним питанням їх функціонування та розвитку, оскільки воно має потенціал для збереження та ефективного використання фінансових, матеріальних та інформаційних ресурсів банків, своєчасного виявлення та нейтралізації реальних та потенційних загроз та створення умов для банків. їх стратегічні інтереси.

Під безпекою АСОІ для банківських систем (і не тільки) розуміють здатність протидіяти спробам завдання шкоди її власникам та користувачам при здійсненні різних (навмисних чи ненавмисних) дій на неї.

Безпека АСОІ досягається забезпеченням конфіденційності інформації, що нею обробляється, а також цілісності та доступності компонентів і ресурсів системи.

Конфіденційність - це властивість інформації, яка може бути відома лише тим, хто допускається, і тим, хто дотримується контролюючих (авторизованих) суб'єктів системи (користувачів, програм, процесів тощо). Ця інформація є конфіденційною для інших суб'єктів системи.

Цілісність системного компонента (ресурсу) - його властивості (у семантичному сенсі) незмінні в процесі роботи системи.

Наявність одного із компонентів (ресурсів) системи - можливість того, що авторизовані сутності системи доступні в будь-який час.

Розрізняють зовнішню та внутрішню безпеку АСОІ. Зовнішня безпека передбачає захист АСОІ від стихійних лих та від проникнення зловмисників з-зовні з метою розкрадання, одержання доступу до носіїв інформації чи виведення системи з ладу. Предметом внутрішньої безпеки є забезпечення надійної та коректної роботи системи, цілісності її програм та даних.

Усі зусилля щодо забезпечення внутрішньої безпеки АСОІ зосереджуються на створенні надійних і зручних механізмів регламентації діяльності всіх її користувачів і обслуговуючого персоналу, дотриманні встановленої в організації дисципліни – прямого або непрямого доступу до ресурсів системи та до інформації.

Відомі два підходи до забезпечення безпеки АСОІ – "фрагментарний" і комплексний. "Фрагментарний" підхід орієнтується на протидію суворо визначеним погрозам за певних умов. Прикладами реалізації такого підходу є, наприклад, спеціалізовані антивірусні засоби, окремі засоби реєстрації та управління, автономні засоби шифрування тощо. Головна особливість "фрагментарного" підходу – відсутність єдиного захищеного середовища обробки інформації.

Перевагою "фрагментарного" підходу є його висока вибірковість щодо конкретної погрози, яка зумовлює також основний його недолік – локальність дії. Навіть невелика зміна погрози призводить до втрати ефективності захисту. Поширити дію таких заходів на всю АСОІ практично неможливо.

Особливістю комплексного підходу є створення захищеного середовища обробки інформації в АСОІ, яка об'єднує різні заходи протидії погрозам (правові, організаційні, програмно-технічні). Захищене середовище обробки інформації формується на основі розроблених для конкретної АСОІ правил обробки критичної інформації.

Організація захищеного середовища обробки інформації дає змогу гарантувати (в межах розробленої політики безпеки) рівень безпеки АСОІ.

Комплексний підхід застосовують для захисту великих АСОІ або невеликих АСОІ, які обробляють інформацію, що дорого коштує, чи виконують відповідальні завдання.

Система захисту АСОІ – це сукупність правових та морально-етичних норм, організаційних, адміністративних і програмно-технічних засобів, спрямованих на протидію загрозам АСОІ з метою зведення до мінімуму можливих втрат користувачів та власників системи.

Етап аналізу можливих погроз АСОІ потрібний для фіксування на певний момент часу стану АСОІ (конфігурації апаратних та програмних засобів, технології обробки інформації) і визначення можливих дій на кожний компонент системи. Із всієї множини можливих дій треба вибрати лише ті, які можуть реально відбутися та завдати значної шкоди користувачам і власникам системи.

На етапі планування формується система захисту як єдина сукупність заходів протидії різної природи. Відомо не так багато універсальних способів захисту АСОІ від різних впливів на неї. Ними є:

- ідентифікація і автентифікація суб'єктів АСОІ;
- контроль доступу до ресурсів АСОІ;
- реєстрація і аналіз подій, що відбуваються в АСОІ;
- контроль цілісності об'єктів АСОІ;
- шифрування даних;
- резервування ресурсів і компонентів АСОІ.

Ці універсальні методи можуть використовуватися в різних варіаціях та комбінаціях у конкретних методах та засобах контролю.

Результатом етапу планування є план захисту – документ, який містить перелік захищених компонентів АСОІ і можливого впливу на них, вартість

захисту інформації в АСОІ, правила обробки інформації в АСОІ, що забезпечують захист її від різних взаємодій, а також опис розробленої системи захисту інформації.

Суть етапу впровадження системи захисту інформації полягає у розробці та розробці засобів захисту, необхідних для реалізації правил обробки інформації, викладених у плані захисту.

Сформувались два основних способи реалізації механізмів захисту:

- "Доданий" захист, де засоби захисту – це доповнення до основних програмних та апаратних засобів АСОІ. Подібного підходу в забезпеченні безпеки дотримується, наприклад, фірма IBM.
- "Вбудований" захист, який полягає в тому, що механізми захисту є невід'ємною частиною АСОІ, розробленою та реалізованою з урахуванням певних вимог безпеки. Механізми захисту можуть бути реалізовані у вигляді окремих компонентів АСОІ і розподілені по інших компонентах системи. При цьому засоби захисту становлять єдиний механізм, який відповідає за забезпечення безпеки всієї АСОІ. Цей спосіб використовувався компанією DEC при розробці системи VAX/VMS.

Обидва описані способи мають свої переваги і недоліки. "Доданий" захист більш гнучкий, його механізм можна додавати або вилучати в міру необхідності. У тому разі, коли "додані" засоби захисту не підтримуються "вбудованими" механізмами АСОІ, вони не забезпечать необхідного рівня безпеки.

Основна перевага "вбудованого" захисту – надійність та оптимальність. Засоби захисту розроблялись та реалізовувались одночасно з самою АСОІ. Проте "вбудований" захист має жорстко фіксований набір функцій, не даючи змоги розширювати чи скорочувати його. Деякі функції можна тільки відключити.

Обидва препарати в рідкісній формі зустрічаються рідко. Зазвичай використовуються їх комбінації, які дозволяють поєднувати переваги та компенсувати недоліки.

Комплексний захист АСОІ можна реалізувати як з допомогою “доданого”, так і “вбудованого” захисту. Забезпечення захисту АСОІ – це ітеративний процес, що закінчується тільки з завершенням життєвого циклу всієї системи.

2.2. Аналіз банківських операцій, їх автоматизації та захисту

В АСОІ зберігається і обробляється конфіденційна інформація. Її підробка або витік можуть призвести до серйозних наслідків. Через це електронні банківські системи приречені залишатися відносно закритими, працювати під керуванням специфічного програмного забезпечення і приділяти більше уваги своїй безпеці.

Другою особливістю ЕБС є підвищення вимогливості та надійності апаратного і програмного забезпечення. Це дає змогу здійснювати безперервну обробку інформації.

Можна виділити два класи задач, які розв’язує ЕБС.

- Аналітичні (прогнозування, планування, аналіз рахунків тощо). Результати їхнього розв’язання можуть справляти вплив на політику банків. Внаслідок цінності результатів їхній захист має бути постійним.
- Щоденні (виконання платежів і коригування розрахунків). Для їхнього розв’язання звичайно потрібно набагато більше ресурсів, ніж для аналітичних задач. Звичайно досить забезпечити захист безпосередньо в момент його здійснення. При цьому захист самого процесу обробки інформації та кінцевих результатів має бути постійним.

Вісімдесят вісім відсотків опитаних організацій мають політику безпеки. Різні організації приділяють все більшу увагу захисту збереженої та обробленої інформації. Лише 66 відсотків організацій, що мають менше 100 працівників.

вони мають політику безпеки, тоді як для організацій, що мають понад 5000 працівників, частка таких організацій сягає 94 відсотків. 88 відсотків організацій, які мають політику безпеки, мають спеціальні підрозділи для реалізації.

У плані захисту особливу увагу приділяють захисту великих ЕОМ (82 відсотки), відновленню інформації після аварій і катастроф (73 відсотки), захисту від комп'ютерних вірусів (72 відсотки), захисту персональних ЕОМ (69 відсотків).

До особливостей організації захисту мереж ЕОМ в фінансових установах можна віднести широке використання комерційного програмного забезпечення для управління доступом до мережі (82 відсотки, в державному секторі – 71 відсоток), захист точок підключення до систем через комутовані лінії зв'язку (69 відсотків, в державному секторі – 51 відсоток). Інші способи захисту, такі як використання антивірусних засобів, кінцеве канальне шифрування даних, що передаються, автентифікація повідомлень, використовуються менше, ніж у 50 відсотках організацій. Велика увага приділяється захисту приміщень, у яких розміщені комп'ютери.

Захист ЕБС має розроблятися для кожної системи індивідуально відповідно до загальних правил і включати:

- аналіз ризику, що завершується розробкою проекту системи захисту і планів захисту, безперервної роботи і відновлення;
- реалізацію системи захисту (СЗ) на основі результатів аналізу ризику;
- постійний контроль за роботою СЗ і АСОІ в цілому.
- кожну систему обробки інформації потрібно розробляти індивідуально, враховуючи такі особливості: організаційну структуру банку;
- обсяг і характер інформаційних потоків (усередині банку в цілому, усередині відділів, між відділами, зовнішніх);
- кількість і характер виконуваних операцій: аналітичних і щоденних (один з ключових показників

- активності банку – число банківських операцій за день); кількість і функціональні обов'язки персоналу; кількість і характер клієнтів;
- графік добового навантаження.

Захист повинен відповідати принципам організації мережі: якщо мережа централізована, захист повинен бути централізованим, якщо мережа розподілена, захист також повинен бути розподілений.

Топологія "зірка" найкраще підходить для централізованої обробки; розподілений - для "загальної шини", що характеризується високою швидкістю передачі даних і відносно швидким доступом до вузла.

Доступ до мережі на комутованих лініях вважається потенційно найнебезпечнішим. Ви повинні аутентифікувати логін по телефону (захист паролем, перевірте опис списку дозволених номерів).

Є сенс використовувати цю методологію захищених АСОІ в тому разі, якщо витрати на реалізацію менші, ніж вартість інформації, що може бути втрачена. Найреальнішим об'єктом використання цієї методології є великі АСОІ чи АСОІ, що обробляють дорогу інформацію або розв'язують відповідальні задачі.

З часу своєї появи банки незмінно притягували до себе злочинців. У наші дні банки перетворились на обладнані за останнім словом техніки бастіони, що ховають в своїх надрах мільярди. Проте прогрес у техніці злочинців йшов не менш швидкими темпами, ніж розвиток банківських технологій. У наші дні значна частка всіх злочинів пов'язана з використанням АСОІ банку. Отже, при створенні АСОІ банку потрібно приділяти велику увагу забезпеченню їхньої безпеки.

Необхідність захисту банківських систем: тенденції та факти. Комп'ютерні системи є абсолютно новим джерелом досі невідомих загроз, а саме:

- втрати банків від впливу на їхні системи обробки близько 3 млрд. дол. на рік;

- обсяг втрат, пов'язаних з використанням пластикових карток, приблизно дорівнює 2 млрд. дол. на рік, що становить 0,5–10 відсотків від загального обсягу платежів.

Варто також звернути увагу на значне збільшення вірусних загроз і числа НСД до інформації, яка спільно використовується в мережі ЕОМ. 10 відсотків порушень скоєні скривдженими та невдоволеними службовцями АСОІ банку, 10 – з корисливих мотивів персоналом системи, 50–55 відсотків – результат ненавмисних помилок.

Особливості злочинів у фінансовій сфері такі:

- Більшість комп'ютерних злочинів є дрібними. Збитки від них становлять 10 000 – 50 000 дол.
- Комп'ютерні злочини, як правило, потребують великої кількості банківських операцій (до кількох сотень). Проте великі суми можуть пересилатися всього лише за кілька транзакцій.
- Більшість злочинців – клерки.
- Комп'ютерні злочини не завжди високо технологічні.
- Багато зловмисників пояснюють свої дії тим, що вони начебто беруть позику в банку з наступним поверненням.

Одним з найвразливіших місць ОЕД є пересилання платіжних та інших повідомлень між банком і банкоматом або між банком і клієнтом.

При цьому виникають такі проблеми: взаємодія одержувача і відправника документів здійснюється опосередковано – через канал зв'язку. Це породжує 3 типи проблем:

- взаємного розпізнавання абонентів (проблема автентифікації при з'єднанні);
- захист документів, які передаються каналами зв'язку (забезпечення їхньої цілісності та конфіденційності);

- захист самого процесу обміну документами (проблема доведення факту відправки (отримання) документа).

У системах ОЕД мають бути реалізовані механізми, що забезпечують реалізацію функцій захисту на окремих вузлах системи ОЕД, та на рівні протоколів високого рівня:

- автентифікація абонентів;
- неможливість відмови від авторства повідомлення;
- контроль цілісності повідомлення;
- забезпечення конфіденційності повідомлення;
- управління доступом на кінцевих системах;
- гарантії доставки повідомлення;
- неможливість відмови від вжиття заходів за отриманим повідомленням;
- реєстрація послідовності повідомлень;
- контроль цілісності послідовності повідомлень;
- забезпечення конфіденційності потоку повідомлень.

Повнота вирішення цих проблем багато в чому залежить від правильного вибору системи шифрування. Система шифрування (або криптографічна система) - це сукупність алгоритмів шифрування та методів розподілу ключів.

Правильний вибір системи шифрування допомагає:

- приховати зміст документа від сторонніх осіб завдяки шифруванню його змісту;
- забезпечити спільне використання документа групою користувачів системи ОЕД в результаті
- криптографічного розмежування інформації та відповідного протоколу розповсюдження ключів. При цьому для осіб, які не входять до групи, документ є недоступним;

- своєчасно виявити перекручення, підробку документа введенням криптографічної контрольної ознаки (імітовставки);
- переконатися в тому, що абонент, з яким відбувається взаємодія в мережі, є дійсно тим, за кого себе видає (автентифікація абонента / джерела даних).

Слід зазначити, що при захисті ОЕД (і для електронних платежів зокрема) велике значення має не стільки шифрування документа, скільки забезпечення його цілісності та автентифікації джерела даних при проведенні сеансу зв'язку.

Надійність криптографічної системи в цілому залежить від механізму передачі (розподілу) ключів між учасниками взаємодій. Основними підходами до надсилання ключів є:

- метод базових (сеансових) ключів (master / session keys). Вводиться ієрархія ключів (головний ключ (ГК), ключ шифрування ключів (КК), ключ шифрування даних (КД)). Ієрархія може бути дворівневою (КК /КД), або трирівневою (ГК /КК /КД). При цьому старший ключ в ієрархії розповсюджується між учасниками взаємодії неелектронним шляхом, що виключає його перехоплення та (або) компрометацію. Стандарт визначає 3 способи розповсюдження ключів: безпосередня, з використанням центру розповсюдження, з використанням центру трансляції ключів. Стандарт не застосовується для розповсюдження ключів між спеціалізованими банківськими пристроями, такими як банкомати і пристрої розрахунків у точці продажу;
- метод відкритих ключів (public keys). Базується на односторонніх перетвореннях, за яких частина ключа залишається відкритою і може бути передана лініями зв'язку у відкритому вигляді. Це звільняє від дорогої процедури розповсюдження ключів як шифрування неелектронним способом;
- метод виведеного ключа (derived key). Застосовується для захисту інформації, яка передається між терміналом системи розрахунку в точці

продажу і комп'ютером банку. При цьому методі ключ для шифрування кожної наступної трансакції обчислюється одностороннім перетворенням попереднього ключа і параметрів трансакцій;

- метод ключа трансакцій (transaction key). Також застосовується для захисту інформації, що передається між терміналом системи розрахунку в точці продажу і комп'ютером банку. Він відрізняється від методу виведеного ключа тим, що при обчисленні ключа для наступної трансакції не застосовуються її параметри.

Особливу увагу слід приділити захисту терміналів, підключених до електронних платіжних систем.

Якщо банк виконує операції з високим ризиком, впроваджені процедури безпеки повинні включати захист паролем, багаторівневу авторизацію користувачів, контроль транзакцій та реєстрацію системи. Слід розрізняти доступ користувача до терміналів та інші зовнішні пристрої, які повинні бути фізично захищені.

Криптографічні методи повинні використовуватися для захисту даних, що передаються по лініях зв'язку.

Система безпеки центральної АСОІ має включати багаторівневий контроль доступу до периферійних пристроїв і центральної бази даних.

Задачі з безпеки визначаються для кожного конкретного випадку індивідуально в процесі аналізу ризику.

Найвідоміша система електронних платежів SWIFT (The Society for Worldwide inter – bank Financia / Telecommunication) – безприбуткове кооперативне міжнародне співтовариство, метою якого є організація міжнародних банківських розрахунків по всьому світу. Вона об'єднує 3200 користувачів з 84 країн світу, прямий доступ користувачів до своїх кореспондентів по всьому світу 20 хв., доставка термінового повідомлення – 5 хв.

Розглянемо способи розрахунку фізичних осіб з фінансовими закладами – так звані персональні платежі, а також способи їх захисту.

Домашнє (телефонне) обслуговування. Розпорядження можуть бути віддані як голосом спеціальному службовцю банку або електронній системі, так і в електронній формі безпосередньо банківському комп'ютеру.

Введення даних для платежу (ідентифікатор, номер рахунку, розмір платежу) здійснює клієнт з клавіатури телефона.

Особлива увага приділяється первинному ідентифікації та верифікації абонента. Наприклад, для автентифікації можна використовувати десятисимвольний пароль, який встановлюється замовником і відомий лише замовнику. Перевірити абонента можна при зверненні до оператора. На початку завдання оператор випадковим чином просить один або кілька листів від пароля користувача. Крім того, клієнт отримує кодове слово, яке використовується в цій процедурі.

Майбутнє цього типу послуг залежить від розвитку розпізнавання мови та створення надійних і відносно недорогих пристроїв з прийнятними характеристиками такого розпізнавання.=

Автоматичні касові апарати (АКА). АКА (банкомат) – спеціалізований пристрій, призначений для обслуговування клієнта за відсутності банківського персоналу. Він призначений в основному для видачі готівки. Крім цієї функції, АКА може виконувати ряд додаткових, а саме:

- перевірка стану рахунку клієнта;
- зміна параметрів рахунку клієнта;
- здійснення різноманітних платежів;
- надання інформації про страховий поліс клієнта, котирування цінних паперів на фондовому ринку, купівлю й продаж акцій, обмінні курси валют тощо.

Взаємодія клієнта з АКА здійснюється за допомогою пластикової картки, на якій записана потрібна інформація, виносної клавіатури і мікродисплея. Фактично АКА являють собою ПЕОМ, яка має до 16 Мбайт ОП, до 100 Мбайт дискової пам'яті, нагромаджувач на гнучких магнітних дисках, дисплей, принтер та інші периферійні пристрої. Шифрування конфіденційної інформації при передачі каналами зв'язку або записуванні на диск здійснюється на основі стандарту DES. Станом на 1989 р., у різних країнах світу встановлено понад 200000 АКА, загальні вклади в індустрію АКА становили 3 млрд. дол.

Розрахунок у точці продажу (POS). В основному всі термінали, підключені до цих систем, розміщені на підприємствах торгівлі. Більшість таких терміналів встановлено в супермаркетах, на автозаправних станціях тощо.

Системи POS забезпечують такі послуги:

- перевірку і підтвердження чеків;
- перевірку і обслуговування дебетових і кредитних карток;
- використання системи електронних розрахунків.

Дані, необхідні для платежу, передаються через термінали системи POS банківському комп'ютеру, проводиться платіж і гроші переводяться з рахунку покупця на рахунок продавця.

PIN – це послідовність цифр (звичайно 4-6, але може бути до 12), яка використовується для ідентифікації клієнта. За способом призначення можна виділити такі типи PIN:

- призначені виведені (derived);
- призначені випадкові (random);
- вибрані користувачем.

У зв'язку з тим, що PIN призначений для ідентифікації та автентифікації клієнта, його значення має бути відомим тільки клієнту.

Алгоритм ідентифікації клієнта. Є два основні способи перевірки PIN: алгоритмічний і неалгоритмічний.

Алгоритмічний спосіб перевірки полягає в тому, що у користувача запитується персональний ідентифікатор PIN, який перетворюється за певним алгоритмом з використанням таємного ключа, а потім порівнюється з значенням PIN, що зберігається на картці. Переваги цього методу:

- відсутність копії PIN на головному комп'ютері, що виключає його розкриття персоналом банку;
- відсутність передачі PIN між АКА та головним комп'ютером банку, що виключає його перехоплення зловмисниками чи нав'язування результатів порівняння.

Генерація PIN з номера рахунку. Спочатку номер рахунку клієнта доповнюється нулями або іншою константою до 16 шістнадцятиричних цифр (8 байтів). Потім одержані 8 байтів шифруються з використанням таємного ключа за алгоритмом DES. З одержаного шифртексту (8 байт), починаючи з молодших байтів, виділяються по 4 біти. Якщо значення числа, утвореного цими бітами, менше за 10, то одержана цифра включається в PIN, інше значення відкидається. Отже, обробляються всі 8 байтів (64 біти). Якщо в результаті обробки не вдалося одержати необхідну кількість десяткових цифр, з невикористаних комбінацій віднімається 10.

Використання систем POS і АКА поставило вимогу появи деякого носія інформації, який би міг ідентифікувати користувача та зберігати деякі облікові дані. У ролі таких носіїв стали виступати пластикові картки.

Тепер у світі випущено 600 млн. пластикових карток. Найбільш відомими з них є такі:

- кредитні картки VISA (більше ніж 200 млн.) та Master Card (148 млн.);
- міжнародні чекові гарантії Eurochegue і Postchegue;

- картки для оплати подорожей і розваг American Expresse (40 млн.) і Diners Club.

Відповідно до принципу дії можна розрізняти пасивні та активні пластикові картки. Пасивні засоби зберігають інформацію лише на певному носії. Активні карти характеризуються наявністю вбудованого чіпа. Карту мікропроцесора називають смарт-картою.

Кредитні та дебетові картки можна розрізнити за характером оплати пластиковими картками.

За характером використання картки вони поділяються на корпоративні та особисті.

Інтелектуальні картки (ІК). Цей тип карток винайдений та запатентований Роланом Мореном у Франції і набув найбільшого поширення в США. Серцем таких карток є не просто мікропроцесор, а мікроЕОМ, оскільки в постійний запам'ятовуючий пристрій, встановлений на картці, "прошивається" спеціальний набір програм, що називається Операційною Системою Картки.

Ці картки забезпечують різноманітний набір функцій:

- можливість роботи із захищеною файловою системою (доступ до файлів потребує повноважень по читанню (запису) інформації);
- шифрування даних з використанням різних алгоритмів;
- ведення ключової системи тощо.

Деякі картки забезпечують режим "самоблокування" при спробі НСД.

ІК дає змогу суттєво спростити процедуру ідентифікації клієнта. Для перевірки PIN використовується алгоритм, що реалізується мікропроцесором на картці.

Водночас ІК мають і суттєві недоліки, які зумовили обмежене поширення їх:

- висока вартість виготовлення картки;
- збільшена, порівняно з стандартом, товщина, через що вона не може бути прочитана звичайним АКА.

Для читання таких карток потрібна установка спеціальних зчитувачів.

Кредитні картки (КК). КК – найпоширеніший тип пластикових карток. До них належать VISA та Master Card, American Exprese та AmEx'S Optima, картки Discovery Card фірми Sears, місцеві та регіональні картки універсальних магазинів. КК пред'являється для оплати товарів і послуг. При оплаті з допомогою КК банк відкриває покупцю кредит на суму покупки і потім через деякий час (звичайно 25 днів) надсилає рахунок поштою. Покупець повертає оплачений чек назад до банку.

Дебітові картки (ДК). Це пластикові картки, що використовуються для дебітових розрахунків. Вони багато в чому аналогічні кредитним. Для дебітових трансакцій найчастіше використовується АКА. Дебітові картки призначені для заміни готівки та персональних чеків.

Головна її відмінність від КК полягає в тому, що з її допомогою можна вносити гроші на свій рахунок. ДК в основному застосовуються для одержання готівки через АКА.

Захист пластикових карток від підробки. До банківських карток висуваються дві головні вимоги: унікальність і необоротність.

Перша вимога означає, що серед усіх випущених банком карток не повинно бути однакових за характеристиками.

Згідно з другою вимогою не може бути відновлена первісна інформація на картці.

Існує два основних способи захисту від підробки - магнітні водяні знаки та метод "сендвіч". Метод магнітних водяних знаків полягає у нанесенні спеціального малюнка на магнітну стрічку, розміщену на картці.

Метод "сендвіч" полягає в тому, щоб одна зі смужок містила ділянки різної намагніченості. Сучасні пластикові картки мають кілька рівнів захисту. Наприклад, картки VISA мають 7.

2.3. Існуючі методики захисту інформації у банківських системах

Інформація є одним з найважливіших джерел процвітання будь-якої держави, банку чи компанії. Недарма кажуть: "Той, хто має інформацію, належить світові". Кожне управлінське рішення ґрунтується на інформації, на якій воно приймається, і вартує його.

Витоки можуть завдати серйозної шкоди банку, його економічному становищу та іміджу, часто дозволяючи конкурентам зайняти провідні позиції на ринку, а іноді і призвести до банкрутства.

Відповідно до законів про підприємництво попит породжує пропозицію. Ось чому на сучасному ринку засобів захисту інформації з'являється все більше різноманітних та потужних інструментів. Цей процес став особливо активним в останні роки.

Іноземні компанії, виробники таких пристроїв та систем, здійснюють помітне різке вторгнення на цей ринок.

Дослідимо деякі питання інформаційної безпеки та доцільність використання іноземного програмного забезпечення для інформаційної безпеки в Україні.

Цільове електронне відстеження банків та компаній з найбільшими перспективами розвитку з метою отримання інформації про їх заплановану продукцію, технології, фінансові та комерційні операції. Одним із способів отримання такої інформації є контроль каналів для обміну інформацією. Незалежність держави сильно залежить від незалежності та надійності інформаційних баз даних та каналів. Їх контроль над державою, її банками та компаніями залежить від того, хто контролює і знає весь прогрес. Одним із

способів управління інформаційними каналами є електронні та програмні «закладки».

“Електронні закладки” (“жучки” тощо) вже давно використовуються спецслужбами для промислового шпигунства. За допомогою цих “жучків” можна перехопити не лише акустичну, але і спеціальну електронну інформацію. Припустимо, одна фірма продала іншій комп’ютер, ксерокс, телефон, факс, і “продавець” тепер знає все, що робиться у “покупця”. “Жучок” справно поставляє своєму господарю інформацію радіоканалом чи, наприклад, через комп’ютерну мережу. І звичайно ж, продавець точно знає, кому дістанеться ця техніка. Отже, витрати на “жучка” швидко відшкодовуються.

Як дешевший, але не менш ефективний спосіб отримання інформації з комп’ютерів використовують зняття з них електромагнітного випромінювання. Окремі види навіть побутової телевізійної техніки дають змогу отримати “картинку” з екрана дисплея комп’ютера на своїх екранах. Уявіть собі, що в машині, припаркованій недалеко від банку сидять “електронні хакери” і спостерігають по телевізору, що відбувається на банківському комп’ютері. Однак таке можливе лише з звичайним, незахищеним від випромінювання комп’ютером.

Фірми, які надають подібні послуги зі “зняття” інформації, уже з’явилися в Києві, Москві, і успіх їхньої діяльності зумовлений тим, що у нас поки що або зовсім не захищаються, або захищаються непрофесійно.

Іншим ефективним способом промислового шпигунства є проникнення в комп’ютерні мережі, електронні бази даних банків, компаній тощо. У розвинених країнах збитки від таких запасів становлять десятки мільярдів доларів.

Якщо ж такі проникнення плануються заздалегідь, то для полегшення роботи “зломщику” до програми, яка поставляється клієнтові, розробник вносить “програмну закладку”, яка дає можливість легко увійти в комп’ютерну систему того, у кого вона буде стояти. У зв’язку з цим у воєнній галузі з’явився новий термін – “інформаційна зброя”.

Існує багато прикладів впровадження «програмних закладок» в інформаційні системи різних фінансових та комерційних структур. Тільки ефективність такої закладки може бути такою, що призведе до повного знищення власника інформаційної системи або через витік конфіденційної інформації, або через несанкціонований вплив розробника на саму систему. Ці ефекти особливо широко використовуються в країнах з розвиненими комп'ютерними системами, де розробник все ще може «віддалено» впливати на роботу своєї програми, спілкуючись з ним по мережі. Однак подібні випадки вже були зареєстровані в Угорщині.

Уряд США вважає за необхідне контролювати розповсюдження криптографічних систем. Тому в середині квітня 1993 р. Президент США запропонував прийняти криптографічну систему Clipper як стандарт США замість стандарту DES. Уряд США зберігає контроль над криптографічними ключами в криптографічній системі Clipper. Ключ розділений на дві частини, і кожна частина зберігається в окремій організації, обраній Генеральним прокурором. Після прослуховування дозволу суду правоохоронні органи отримають обидві частини ключа та розшифрують надану інформацію.

Основою нової системи шифрування стане секретний криптоалгоритм Skipjack АНБ США. Секретність ключа шифрування системи Clipper заснована на принципі розділеного і депонованого ключа.

Крипточип Capstone є розширеним варіантом крипточипа Clipper і містить, крім інших елементів, додатково схему реалізації алгоритму цифрового підпису DSA (Digital Signature Algorithm), запропоновану національним інститутом стандартів і технологій NIST (США). Цей алгоритм використовуватиметься замість алгоритму цифрового підпису RSA.

Слід враховувати доцільність використання іноземного програмного забезпечення для захисту інформації в Україні та створення та використання вітчизняних систем безпеки.

На сьогоднішній день банківський сектор справив позитивний вплив завдяки впровадженню сучасних технологій автоматизованої обробки інформації та пов'язаному з цим розширенню спектру послуг, що надаються, а також прискоренню обороту коштів та неминучим негативним ефектам, а саме:

- частішають спроби крадіжок грошових коштів, в тому числі за допомогою засобів комп'ютерної техніки;
- не завжди ефект від впровадження передових технологій адекватний витратам;
- не всі послуги надаються на досить якісному рівні.

Уже сьогодні потребують негайного вирішення такі проблеми:

- забезпечення безпеки обміну інформацією між відділами банків, що працюють в режимі єдиного кореспондентського рахунку в Національному банку України. Оскільки більше ніж 70 відсотків платежів у таких банках становлять внутрішньосистемні (міжфілійні) платежі, очевидно, наскільки актуальна ця задача. За Промінвестбанком України, що працює в цьому режимі, на нього будуть переходити й інші банки (організація взаємодії за принципом "кожен з кожним");
- безпеки інформації, що циркулює у відомчих мережах передачі даних. Уже існує відомча мережа передачі даних банку "Україна";
- відсутності нормативно-правової бази, яка дає змогу вирішувати питання електронного грошового обігу як між відділами банків, так і між банками і їхніми клієнтами (в системах "Клієнт–Банк");
- відсутності єдиних стандартів галузі як найпоширеніших алгоритмів, так і термінології;
- на сьогоднішній день ніякими засобами, крім досить слабких, які входять до складу найпопулярніших мережевих операційних систем, не забезпечується безпека інформації, що обробляється всередині відділу

банку. Водночас 70–90 відсотків усіх крадіжок грошових коштів в автоматизованих системах здійснюють співробітники банків;

– сертифікації програмних і апаратних засобів. З однієї сторони, НБУ справедливо вимагає використання для захисту банківської інформації лише сертифікованих програмних і апаратних засобів, з іншої – система державної сертифікації таких засобів ще реально не функціонує, а спроби НБУ виступати в ролі сертифікаційної організації не зовсім законні.

Без комплексного вирішення цих та інших питань потрібно створити надійну електронну платіжну систему, а доступ зробити простим та зручним для всіх учасників - завдання недосяжне.

В даний час темпи зростання кількості банків, що працюють в Україні, сповільнюються. Цей процес буде замінений процесом підвищення якості та кількості послуг, що надаються, в тому числі в галузі автоматизації електронних платежів. Прикладами є використання кредитних карток у багатьох банках, активний обмін фінансовою інформацією між банківськими підрозділами за допомогою телекомунікацій та запровадження різних автоматизованих систем обробки фінансової інформації в банках. І останнє, але не менш важливе, серед таких нововведень є електронні платіжні системи "Клієнт-Банк", які дозволяють клієнтам банку - юридичним особам - здійснювати операції зі своїм банківським рахунком безпосередньо з офісу. Ми аналізуємо проблеми, пов'язані із забезпеченням захисту інформації, що обробляється в таких системах, та надаємо деякі рекомендації щодо їх реалізації.

Це вимагає аналізу всіх етапів процесу взаємодії клієнта з банком, виявлення потенційних загроз безпеці та вибору методів захисту від них.

Одну з можливих технологічних схем функціонування системи “Клієнт–Банк” наведено на рисунку 2.3.1.

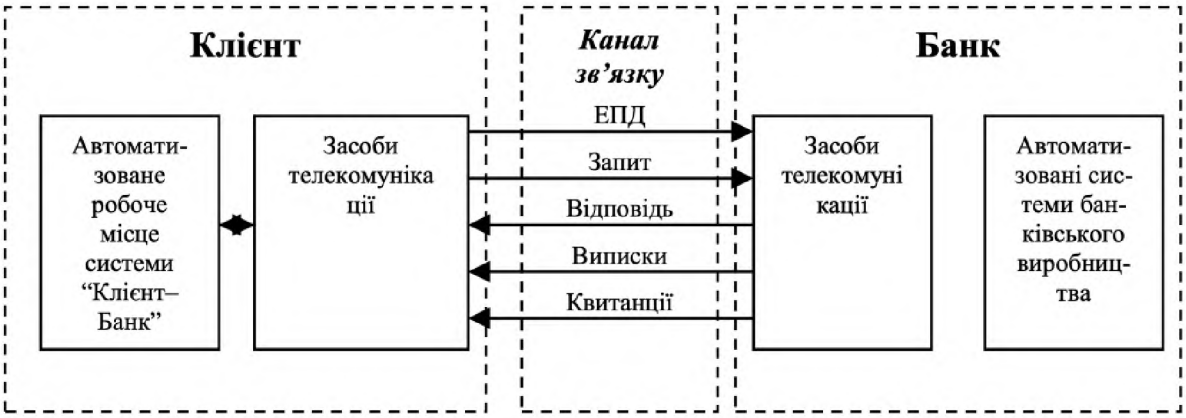

Рисунок 2.3.1 - Технологічна схема функціонування системи "Клієнт–Банк"

Така схема використовується, наприклад, в АПБ "Україна", подібна – в кількох інших банках. Клієнт на своєму автоматизованому робочому місці (АРМ) виконує підготовку електронних платежів документів (ЕПД). ЕПД за допомогою програмно-технічних засобів телекомунікації (модему і відповідного програмного забезпечення) передаються до банку, де приймаються також через телекомунікаційні засоби, що функціонують на спеціально впровадженому комп'ютері (зв'язному сервері), включеному до локальної обчислювальної мережі (ЛОМ) банку. У цій ЛОМ функціонує програмний комплекс автоматизованої системи банківського виробництва (АСБВ), який називають комплексом операційного дня банку (ОДБ). Прийняті зв'язним сервером (ЗС) електронні платежі документів каналами ЛОМ передаються в АСБВ, де здійснюється їх подальша обробка. Після прийняття ЕПД і обробки АСБВ формує квитанцію і передає її на ЗС для наступної передачі клієнту. Протягом операційного дня і після його завершення АСБВ формує і передає на ЗС повідомлення про рух на рахунку клієнта (поточні та кінцеві виписки).

З точки зору забезпечення безпеки в цій технології можна виділити три групи проблем:

- Такі, що виникають при обробці інформації всередині організації-відправника ЕПД.

- Пов’язані з забезпеченням захисту ЕПД при пересиланні їх між клієнтом і банком.
- Ті, що виникають у процесі обробки документа в банку і прийняття рішень про зміну стану рахунку клієнта (про переказ коштів).

Проблеми першої групи пов’язані в основному з такими причинами:

- необхідністю забезпечення юридичної значимості сформованого документа для установи банку (проблема автентифікації виконавця документа);
- блокуванням можливості внесення зловмисником змін в уже сформовані та підготовлені до відправки ЕПД (проблема автентифікації або захисту цілісності документа);
- захистом цілісності використовуваних при підготовці ЕПД програмних засобів для блокування можливостей несанкціонованого формування (відправки) ЕПД (проблема автентифікації або захисту цілісності програмних засобів).

Одне з вразливих місць – пересилання документів між клієнтом і банком. Це породжує три типи проблем, пов’язаних з необхідністю:

- взаємного розпізнавання абонентів (проблема автентифікації при встановленні зв’язку);
- захист документів, які передаються каналами зв’язку (забезпечення цілісності та конфіденційності документів);
- захист самого процесу обміну документами (проблема доведення факту відправлення (доставки) документа).

У банку в процесі обробки прийнятого ЕПД можуть виникнути такі проблеми:

- підтвердження цілісності та юридичної значимості прийнятого документа (ідентифікація та автентифікація відправника, а також автентифікація повідомлення);

- забезпечення захисту від несанкціонованої модифікації вже прийнятого ЕПД або від нав'язування хибноъ інформації зловмисником всередині відділення банку;
- захист цілісності використовуваних при обробці ЕПД в банку програмних засобів для блокування можливостей несанкціонованого доступу і модифікації інформації про стан рахунків клієнта;
- оскільки клієнт і банк юридично незалежні, існує проблема недовіри – чи будуть вжиті щодо прийнятого документа відповідні дії.

Отже, для забезпечення надійності роботи системи "Клієнт–Банк" засоби захисту мають забезпечувати:

- ідентифікацію та автентифікацію клієнта–відправника ЕПД з однозначною авторизацією документа; автентифікацію ЕПД;
- автентифікацію програмного забезпечення, яке функціонує у клієнта в банку;
- автентифікацію абонентів у процесі встановлення зв'язку і передачі повідомлення;
- приховування смислового змісту повідомлення, що передається;
- захист сформованих ЕПД від несанкціонованого доступу (НСД) як у клієнта, так і в банку;
- фіксацію фактів прийому (передачі) документів з веденням відповідних архівів і журнальних файлів; чітку регламентацію обов'язків клієнта і банку стосовно один одного.

Розглянемо методи та алгоритми, які можна використовувати для вирішення описаних проблем.

Способом ідентифікації та автентифікації відправника ЕПД, а також авторизації самого документа є застосування цифрового підпису документа, що виконується за допомогою несиметричних криптоалгоритмів. Існує кілька алгоритмів для виконання цифрового підпису. Серед них алгоритм RSA і

алгоритм Ель-Гамаля. В Україні стандарту на алгоритм цифрового підпису поки що немає.

Для автентифікації та приховування смислового змісту повідомлень звичайно застосовують симетричні криптоалгоритми, наприклад, DES, Clipper або діючий на території колишнього СРСР, в тому числі в Україні, ГОСТ 28147-89.

Проблему автентифікації абонента при встановленні з'єднання можна вирішити двома методами: простою та суворою автентифікацією. Проста процедура автентифікації - це, як правило, обмін паролями. Для суворої автентифікації використовуються асиметричні криптографічні алгоритми. Це позбавляє від необхідності заздалегідь міняти секретні паролі, що значно підвищує стабільність системи.

Захисту ЕПД під час обробки в клієнтських та банківських автоматизованих системах неможливо досягти без контролю за правами операторів на запуск програмного забезпечення та доступ до даних.

Для того, щоб реєструвати отримання (передачу) повідомлень за допомогою системи безпеки, слід підтримувати ведення архівів отриманих та переданих документів, і доступ до цих архівів повинен бути обмежений як програмно, так і організаційно. Усі повідомлення про спроби виявлення інформації про НСД, виявлені системами безпеки, повинні реєструватися в спеціальних журналах.

Починати використовувати систему “Клієнт–Банк” можна тільки після укладання між клієнтом і банком угоди, в якій чітко зафіксовані зобов’язання сторін стосовно одна одної, а також їхня згода підкорятися вимогам, викладеним у “Положенні про порядок використання засобів цифрового підпису”, вирішувати всі спірні питання у відповідній експертній організації та підкорятися її рішенням.

Звідси випливає, що система захисту “Клієнт–Банк” має бути комплексом програмно-апаратних засобів, що функціонують у банку і у клієнта. Можливі

схеми включення цих засобів до поданої на рисинку 2.3.2 технології наведено на рисунку 2.3.2 та рисунку 2.3.3.

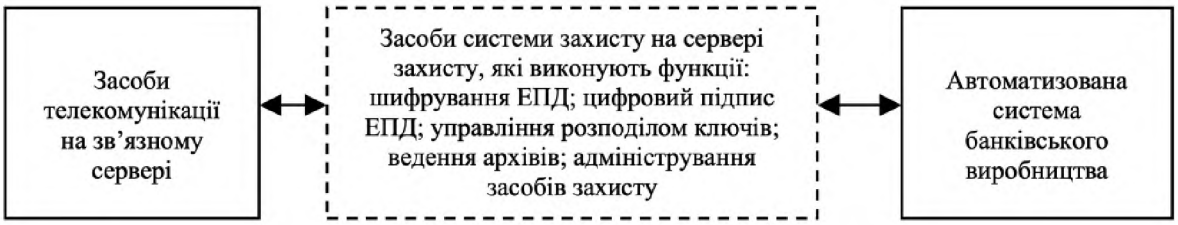

Рисунок 2.3.2 - комплексні програмно-апаратниі засоби

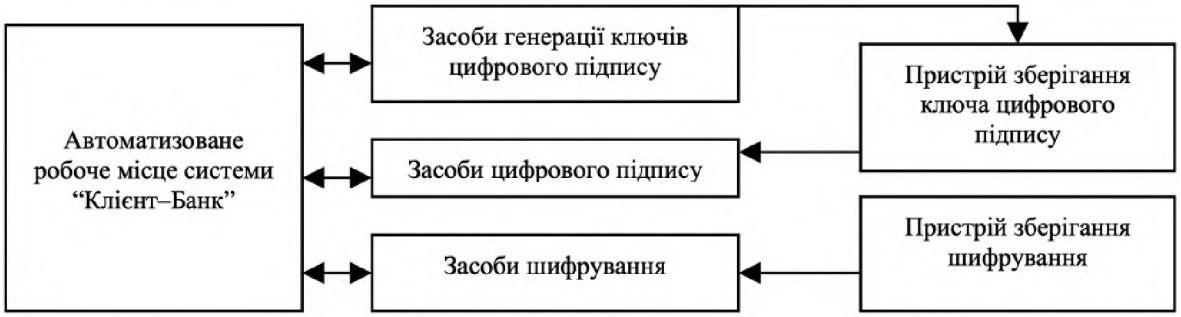

Рисунок 2.3.3 - комплексні програмно-апаратниі засоби

Засоби захисту в клієнта містять програмні або апаратні засоби шифрування інформації, цифрового підпису, генерації ключів цифрового підпису.

Неодмінний компонент системи захисту – програмно-апаратні засоби захисту комп'ютерів від НСД, які обов'язково мають встановлюватися в банку, але можуть бути встановлені також у клієнта.

Слід зазначити, що, на жаль, сьогодні на ринку України практично немає систем, які задовольняють наведені вимоги. Є лише окремі їх компоненти, що реалізують, як правило, функції шифрування і цифрового підпису. При цьому абсолютно не продумані питання інтеграції засобів захисту з АСБВ і забезпечення надійного і безпечного їх взаємозв'язку. Мабуть, єдиним винятком з цього правила є система "Піраміда-К", розроблена на замовлення банку "Україна".

2.4 Розробка методичних рекомендацій на основі використання технології блокчейн

Стандартні банківські процеси складаються з таких процесів, як кредитування, іпотека, операції та платіжні послуги. Більшість із цих послуг реалізуються із застосуванням застарілих методів та технологій. Наприклад, між перевіркою інформації, кредитним рейтингом, обробкою кредитів та розподілом коштів фізичним особам придбання іпотечного кредиту займає 30–60 днів, а для малих та середніх підприємств - 60–90 днів. Blockchain може оптимізувати банківські та кредитні послуги, зменшуючи ризик контрагента та скорочуючи час розрахунків. Це дозволяє:

- звіряти документацію та дані клієнтів, зменшуючи операційні ризики та дозволяючи перевіряти фінансові документи у режимі реального часу;
- оптимізувати ринки кредитного прогнозування та кредитного скорингу, миттєво отримання інформації шляхом зіставлення активності користувачів та даних по всій мережі;
- автоматизувати формування синдикату, андерайтинг і виплату коштів, тобто виплату основного боргу і відсотків, зниження вартості та затримок;
- полегшення забезпеченості активами, оскільки технологія дозволяє у режимі реального часу управляти активами, відстежувати і забезпечувати дотримання регулятивних заходів контролю. [39]

Інновації у фінансових технологіях багато в чому змінюють світ грошових переказів. Але поки що блокчейн не використовується в обробці будь-яких великих платежів. Одним з пояснень цього є нездатність технології підтримувати кілька транзакцій одночасно. Для порівняння: SWIFT може обробляти до 24 мільйонів транзакцій кожні 24 години, а Visa може обробляти 65 000 транзакцій в секунду. Блокчейн Bitcoin, з іншого боку, може обробляти тільки близько 2000 платежів за десять хвилин в день.

Технічні експерти повністю усвідомлюють обмеження блокчейну. До тих пір, поки вони не зможуть збільшити розмір блоків для розміщення більшої

кількості транзакцій, платформи блокчейну не зможуть скласти конкуренцію MasterCard, PayPal та іншим гігантам обробки платежів.

Однак, те, що може просунути блокчейн і криптовалюта до масового використання, це Facebook Libra. Цей спірний проект спрямований на створення децентралізованої мережі платежів за межами традиційної фінансової системи. Засобом обміну у Libra є Stablecoin. Асоціація Libra, як орган створений для управління грошима, буде контролювати резерв для підтримки стабільної вартості цифрової монети. Якщо майже два з половиною мільярди користувачів Facebook почнуть використовувати Libra для того, щоб купувати речі й відправляти гроші іншим людям, платіжна мережа Libra буде здатна зруйнувати грошову систему і розорити світові ринки. Якщо Libra виявиться успішною, це дасть титану соціальних мереж і його інвесторам фінансовий та політичний вплив, досить значний, щоб просувати свої ідеї в уряді. [40]

З огляду на серйозність кіберзагроз сектору фінансових послуг, банки та інші організації фінансового сектору інвестують набагато більше, ніж інші галузі, у створення та розвиток власних систем кібербезпеки. Сучасні системи кібербезпеки банків досить складні та багаторівневі, враховуючи природу та механізми формування ризику в кіберпросторі. Їм потрібно враховувати постійно зростаючу тенденцію поширення кіберзагроз, наявність багатьох відомих та невідомих потенційних каналів атаки. Слід зазначити, що джерелом кіберзагроз може бути не лише зовнішнє, а й внутрішнє, що включає інтеграцію різних різноспрямованих механізмів захисту. [41]

Основним завданням наявних систем кібербезпеки є максимальна протидія усім можливим кібератакам, за допомогою яких могли би бути здійснені кіберзло чини. В ідеалі системи кіберзахисту повинні не тільки виступати бар'єром для всіх відомих видів кіберзагроз, але і вміти ідентифікувати досі невідомі види кібератак до того, як вони могли б завдати шкоди банку та його клієнтам. Зазвичай система кібербезпеки банку являє собою комплексне програмне

рішення, яке базується на низці технологій, здатних захистити інформаційний простір банку від окремих видів та типів загроз залежно від їх характеру дії та сфери виникнення. Використання цілого портфелю технологій дає змогу максимально мінімізувати наявний загальний рівень кіберризику, оскільки немає єдиної технології, яка б ефективно спрацьовувала проти усіх можливих типів загроз. [42]

В даний час найбільш передовими технологіями забезпечення кібербезпеки банків є технології штучного інтелекту та машинного навчання. Їх основною перевагою є можливість поєднувати різні канали, такі як цифровий банкінг, аутентифікація, банківська справа на відкритому банку. За допомогою технології штучного інтелекту він може обробляти величезні обсяги інформації з різних каналів в одному місці, що дозволяє більш ефективно відстежувати та виявляти кібератаки, одночасно аналізуючи складну картину всіх транзакцій, доступних на різних каналах. Аналіз діяльності на кожному каналі часто не може встановити жодного підозрюваного злочину. Кібератаки зазвичай здійснюються шляхом виконання ряду операцій по різних каналах. Не кожен вчинок може викликати підозру, але відстеження всієї серії дій може визначити сценарій злочинних кібератак. Багато експертів у галузі банківської справи та кібербезпеки вважають, що використання технологій штучного інтелекту буде провідною тенденцією для постачальників фінансових послуг.

Поряд з технологіями, які вже активно використовуються в системах кібербезпеки, ми можемо виділити технологію блокчейн, яка є відносно новою та перспективною. Поки він не набув поширення, але, на наш погляд, його використання в системах кібербезпеки банку може суттєво підвищити їх ефективність. Блокчейн став широко відомим завдяки активному розвитку криптовалют, які в основному базуються на цій технології. Сьогодні багато стартапів у всьому світі намагаються впровадити та протестувати концепції для різноспрямованих проектів, заснованих на технології блокчейн. Зокрема, вони починають використовуватися для розробки вдосконалених систем електронного

голосування, ведення різних глобальних реєстрів (наприклад, реєстрів нерухомості, земельних реєстрів), систем маркетингу, систем управління ланцюгами поставок тощо. [42]

Технологія блокчейн, яку ще називають технологією розподілених реєстрів, є досить універсальним інструментом, який може бути використаним для вирішення широкого спектру завдань. До основних її переваг відносять децентралізованість, повну прозорість, конфіденційність, захищеність від несанкціонованого доступу та реалізацію компромісу. Всі вищенаведені переваги можуть бути спрямованими на вирішення наявних проблем забезпечення кібербезпеки банків. Тому їх було перекладено на площину проблематики кібербезпеки банків (таблиця 2.3.1).

Перевага	Сутність переваги	Значення переваги для систем кібербезпеки банків
Децентралізація	Відсутність єдиного головного серверу зберігання даних; всі записи зберігаються у кожного учасника системи, на кожному її вузлі.	Сучасні системи кібербезпеки банків є централізованими, мають головні сервери даних, що породжує їх основну вразливість. Блокчейн-технологія дозволить під час атаки одного вузла зберегти дані на інших вузлах.
Повна прозорість системи	Всі транзакції, які відбуваються в системі, можуть відстежуватися на всіх вузлах системи.	Технологія блокчейн у банківській системі надасть можливість аналізувати всі транзакції на кожному окремому вузлі. При цьому, кожна наступна транзакція перед її виконанням перевіряється всіма вузлами системи, і не може бути здійснена при виявленні найменшої невідповідності до усіх попередньо здійснених транзакцій.
Конфіденційність	Всі дані зберігаються в зашифрованому вигляді. Користувач, відслідковуючи всі транзакції, не може розпізнати окремі дані про них, а для здійснення операцій потрібний унікальний ключ доступу.	Застосування в банківських системах блокчейнів дозволить захистити від зовнішніх кіберзлочинців та інсайдерів-співробітників особисті дані клієнтів, про їх банківські рахунки, оскільки, маючи всю історію транзакцій, злочинці не зможуть нею скористатись та ідентифікувати дані.
Захищеність від несанкціонованого доступу	Будь-яка спроба внесення несанкціонованих змін автоматично відхиляється системою через невідповідність численним копіям даних, розміщених на різних вузлах системи. Для легального внесення змін в систему та здійснення транзакцій необхідно мати спеціальний унікальний код, який видається та підтверджується системою.	Зловмисники часто здійснюють маніпуляції та фальсифікації даних в системі банку, доступ до якої отримують обхідним шляхом, використовуючи вразливості системи. Якщо зловмисник заволодіє спеціальним унікальним кодом системи, що малоймовірно, в системі завжди зберігатиметься інформація про кожну транзакцію. Будь-яке зловживання правами в системі буде відоме всім іншим її членам, і зловмисник не матиме можливості приховати сліди власного злочину.
Компроміс	Компроміс реалізується шляхом попередньої перевірки кожним членом системи даних, які додаються до неї. Прийняття рішення щодо додавання нового блоку відбувається за умови згоди всіх учасників. Досягнення консенсусу здійснюється у відповідності до одного протоколу консенсусу з урахуванням особливостей та специфіки системи.	З погляду кібербезпеки банківських операцій, проведення процедури перевірки кожної транзакції іншими вузлами системи створює додатковий бар'єр для реалізації атак. Будь-яка спроба підміни даних в одному з вузлів системи буде заблокована іншими вузлами системи, які мають свої копії усіх даних в системі. Цей механізм може захистити банківську систему від таких типів афер, як підміна кредитної історії, реквізитів рахунків, махінації із банківською звітністю тощо.

Таблиця 2.3.1 - Переваги застосування технології блокчейн у системах кібербезпеки банків

Аналізуючи переваги, можна стверджувати, що застосування технології блокчейн в інформаційних системах банків може суттєво підвищити рівень їхньої захищеності від кібератак різного роду. Також використання технології блокчейн здатне усунути основні вразливості сучасних банківських систем, які роблять можливим здійснення таких основних типів кібератак, як Malware, веб-атаки, DOS, атаки зловмисних інсайдерів, зловмисний код та ін. [43]

Непрозорість банківських інформаційних систем створює суттєві перешкоди під час ідентифікації злочинних сценаріїв кібератак. За таких умов навіть системи штучного інтелекту та машинного навчання не можуть працювати максимально ефективно. Також непрозорість банківських систем створює сприятливі умови для шахрайств з боку співробітників банків. Відомо, що близько 48% кібератак на банківські установи здійснюється саме зловмисними інсайдерами. Саме атаки з їхнього боку вважаються найбільш небезпечними та призводять до найбільших грошових втрат. Але в умовах інформаційної системи, що функціонує на базі блокчейн, жоден співробітник не зміг би внести зміни до системи, будучи непоміченим, а всі його маніпуляції з системою постійно фіксувалися б та зберігалися в кожній копії реєстру даних на кожному вузлі. За таких умов будь-яка спроба перевищення службових повноважень досить швидко стає відомою на всіх вузлах системи. [44]

Враховуючи всі вищезазначені переваги та перспективи технології блокчейн, можна сказати, що майбутні напрямки її застосування в банківських системах цілком передбачувані. Якщо порівняти можливості технологій штучного інтелекту та блокчейнів, які широко використовуються сьогодні, ми можемо впевнено стверджувати, що ці два варіанти не взаємозамінні, оскільки вони спрямовані на вирішення різних проблем. Але їх поєднання можливо і доповнює, тому має сенс підвищити рівень інтересу до них з боку різних підприємств, включаючи банківські установи. [44]

Якщо порівняти технологію блокчейну з іншими технологіями, що використовуються в системах кібербезпеки, можна сказати, що вона не менш ефективна і деякі технології можна успішно замінити. Технологія блокчейн може вирішити ті самі проблеми, які в даний час вирішуються за допомогою таких технологій, як розширена автентифікація та контроль доступу, технології шифрування, запобігання втраті даних, автоматичне управління політикою тощо. Ланцюжок транзакційних блоків, кожен із хешем даних попередніх транзакцій, може реєструвати кожні незначні зміни в системі та зберігати історію змін у системі на кожному вузлі. І якщо розслідування кіберзлочинів сьогодні триває від кількох місяців до року, використання технології блокчейн може пришвидшити, а то й десятки разів, розслідування злочинів.

Технологія блокчейн має значний потенціал в інформаційних системах кібербезпеки банків. Аналіз таких ключових переваг, як децентралізація, прозорість, конфіденційність, захист від несанкціонованого доступу та компроміси, показав, що їх можна використовувати для широкого кола питань кібербезпеки в банках. Впровадження технології блокчейн у банківські системи може усунути багато основних уразливих місць кібербезпеки. Результати аналізу даних Google Trends показали, що інтерес до кібербезпеки та банківських додатків є досить значним порівняно з технологією штучного інтелекту, яка вже широко використовується в цих сферах, хоча безпека є кращою при впровадженні комп'ютерних додатків, які це пов’язано з ефективністю штучного інтелекту та ефективністю інвестування в нього. Більшість економічно та технологічно розвинених країн світу виявляють значний інтерес до використання технології блокчейн у банківській діяльності, що призводить до появи та розвитку значних перспектив практичної реалізації її потенціалу. Можна припустити, що технологія блокчейн не менш ефективна у боротьбі з кіберзлочинністю, ніж інші, що використовуються в даний час у банківських інформаційних системах, і може доповнювати існуючі системи для вирішення кіберзагроз.

2.5 Порівняння методики з вже впровадженими

Нині найбільш прогресивними технологіями, які застосовуються для забезпечення кібербезпеки банків, є технології штучного інтелекту та машинного навчання. Основною їхньою перевагою є можливість об'єднання різних каналів, таких як цифровий банкінг, аутентифікація, картковий банкінг та відкритий банкінг. За допомогою технології штучного інтелекту можна в одному місці опрацьовувати величезні обсяги інформації з різних каналів, що дає змогу набагато ефективніше моніторити та виявляти кібератаки, аналізуючи при цьому комплексну картину усіх наявних транзакцій у різних каналах. Аналіз активності в окремих каналах часто не здатен ідентифікувати окрему підозрілу злочинну транзакцію. Зазвичай кібератаки реалізуються шляхом здійснення низки дій із застосуванням різних каналів. Кожна така окрема дія може не викликати жодних підозр, але відстежування цілої послідовності дій може ідентифікувати злочинний сценарій кібератаки. Багато спеціалістів в сфері банкінгу та кібербезпеки вважають, що саме застосування технології штучного інтелекту стане передовою тенденцією для постачальників фінансових послуг.

Поряд із технологіями, які вже активно використовуються у системах кібербезпеки, можна виділити технологію блокчейн, яка є відносно новою та перспективною. Допоки вона не знайшла широкого розповсюдження, але її використання, на нашу думку, в системах забезпечення кіберзахисту банку змогла б суттєво підвищити рівень їхньої ефективності. Блокчейн став широко відомим завдяки активному розвитку криптовалют, більшість з яких базується саме на цій технології. Нині по всьому світі вже є низка стартапів, які намагаються реалізовувати та тестувати концепції різноспрямованих проектів на базі технології блокчейн. Зокрема, її починають використовувати під час побудови прогресивних систем електронного голосування, ведення різних глобальних реєстрів (наприклад, реєстрів нерухомості, земельних ділянок), у маркетингових системах, у системах управління ланцюгами поставок тощо.

2.6 Переваги методики

Можна назвати як переваги методики, так і проблеми, що виникають у зв'язку з її використанням. До переваг можна віднести:

- децентралізацію, тобто використовується вся мережа, а не один комп'ютер (організація, людина тощо). У такому випадку, навіть якщо один або декілька комп'ютерів (осіб) не може виконувати ніяких функцій (ліквідований, арештований тощо), – інші зберігають цю інформацію, що ускладнює хакерські атаки та підробку інформації (хоча від цього і ніхто не застрахований);
- доказовість кожної трансакції: є криптографічне підтвердження кожної трансакції, запису тощо. Зокрема, ключі є приватні (що належать конкретній особі) і публічні (які можуть бути використані всіма користувачами цієї мережі), тобто якщо є одна особа чи один комп'ютер;
- прозорість (загальний доступ): будь-хто і будь--коли може побачити, які саме операції проводилися;
- безпека: інформація зберігається із застосуванням криптографії;
- неможливість внесення змін у «підписаний» блок: інформація, яка попала в блокчейн, проходить перевірку і якщо перевірку пройдено – ставиться своєрідна «печатка» і ці дані синхронізуються між всіма учасниками, з цього моменту інформацію змінити не можна;
- обчислювальна логіка: цифрова природа реєстру працює таким чином, що трансакції у блокчейні можуть бути прив'язані до обчислювальної логіки і фактично їх можна програмувати, що дає можливість користувачам налаштовувати алгоритми і правила автоматичного виконання трансакцій між вузлами;

Якщо говорити про класичний вид договору, то завжди є імовірність, що одна зі сторін його порушить. Зараз для «мотивування» учасників договору вести себе чесно держава використовує юридичні механізми, судову систему, на що витрачається багато часу, коштів і рішення не завжди є справедливими.

Використання блокчейну дозволить прискорити, спростити і здешевити процедуру, адже для укладення контракту необхідна участь обох сторін, і ні одна, ні друга не можуть обдурити систему (блокчейн) з уже заданими параметрами виконання договору. З цього випливають наступні «позитиви» впровадження та використання блокчейну:

- економія часу (робота системи 24 години на добу, 7 днів на тиждень);
- економія ресурсів (зокрема, державних коштів).

2.7 Недоліки методики

В той же час, використання методики має низку недоліків:

- технологічна недосконаліть системи – поломки обладнання та хакерські атаки;
- швидкість функціонування, яка значно поступається існуючим стстемам;
- в угодах, які не потребують високого рівня надійності, методика може створювати додаткові складнощі;
- відсутність законодавчої бази, яка б дозволяла регулювати спірні питання, що виникають у процесі роботи з методикою та технологією;
- відсутність кваліфікованого персоналу або перекваліфікація існуючого;
- як і в багатьох можливих варіантах використання, існують деякі перешкоди пов'язані із застосуванням даної технології в рамках цифрової ідентифікації. Можливо найскладнішою проблемою є той факт, що ці системи як і раніше будуть уразливі для типу шахрайських дій, які також відомі як синтетичне розкрадання персональних даних;

2.8 Висновки результатів використання методики

У розділі були описані та проаналізовані методи та засоби вирішення задачі, проаналізовано захист інформації в банківській сфері. Розглянуто питання використання технології блокчейн та її використання у фінансово-технологічних

застосунках. Були надані методичні рекомендацій щодо захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках.

Підсумовуючи викладене у розділі, можна констатувати, що методика з використання блокчейн є дійсно революційною, він дає змогу в розподіленому світі прийти до свого роду «консенсусу», обібитися без посередників, що може бути використано у всіх сферах суспільного життя (охорона здоров'я, фінанси, медіа тощо). Можна стверджувати, що використання методики і технології блокчейн справді здатне суттєво вплинути на подальший розвиток фінансового сектору. Основна перевага технології блокчейн полягає у відсутності необхідності в централізованому органі. Ця особливість кидає виклик традиційним фінансовим інститутам, адже використання технології дасть змогу позбутись як централізованих посередників, так і зовнішнього контролю. Сучасні проекти дають змогу значно скоротити трансакційні витрати на міжбанківські платежі, здійснення клірингу та розрахунків щодо фінансових інструментів.

3 ЕКОНОМІЧНА ЧАСТИНА

Мета цього розділу — обґрунтування економічної доцільності проектування та впровадження методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках на прикладі банківської системи. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

- річні експлуатаційні витраті на придбання і налагодження складових системи інформаційної безпеки або витрати, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;
- річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;
- річний економічний ефект від впровадження об'єкта проектування;
- визначення та аналіз показників економічної ефективності запропонованого в дипломному проекті проектного рішення.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.1.1. Визначення витрат на створення програмних засобів захисту інформації

Техніко-економічні розрахунки мають містити:

- визначення трудомісткості розробки та опрацювання ПЗ;
- розрахунок витрат на створення програмного продукту;
- оцінку швидкодії та надійності роботи програмного продукту.

3.1.1.1 Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві

Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві здійснюється, виходячи з тривалості кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = tmз + tв + ta + tmехн + tр + tп + tс + tвпр, \text{ годин,} \qquad (3.1)$$

де $tmз$ – тривалість складання технічного завдання на розробку додаткових рекомендацій та посадових інструкцій, $tmз$ = 16 год.;

$t_в$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $t_в$ = 32 год.;

$t_а$ – тривалість аналізу нормативно-правової бази України, $t_а$ = 48 год.;

$t_{техн}$ – тривалість аналізу технології резервування даних, $t_{техн}$ = 40 год.;

$t_р$ – тривалість складання моделі ризику, $t_р$ = 32 год.;

$t_п$ – тривалість складання моделі порушника, $t_п$ = 32 год.;

$t_с$ – тривалість розробки додаткових рекомендацій та посадових інструкцій, $t_с$ = 64 год.;

$t_{впр}$ – тривалість впровадження резервування даних, $t_{впр}$ = 48 год.

Тоді:

$$t = t_{тз} + t_в + t_а + t_{пр} + t_{опр} + t_д =$$

= 16 + 32 + 48 + 40 + 32 + 32 + 64 + 48 = 312 год.

3.1.1.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення ***Ззп*** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК ***Змч***:

$$K_{пз} = З_{зп} + З_{мч}. \qquad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування) і визначається за формулою:

$$З_{зп} = t \cdot З_{пр}, \text{ грн.}, \qquad (3.3)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн./годину.

За формулою (3.3) визначається заробітна плата виконавця з урахуванням середньогодинної заробітної плати з нарахуваннями у розмірі 200,50 грн./годину.

$$З_{зп} = 312 \cdot \ 200{,}50 = 62556 \text{ грн},$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot C_{мч} + t_{д} \cdot C_{мч} \text{ , грн.,} \qquad (3.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою (3.4):

$$З_{мч} = 13{,}50 \cdot \ 5{,}7 + 4{,}2 \cdot \ 5{,}7 = 100{,}89 \text{ грн}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \ \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} \text{ , грн.,} \qquad (3.5)$$

де P – встановлена потужність ПК (P = 0,8 кВт);

C_e – тариф на електричну енергію (C_e = 1,64 грн./кВт за годину);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік ($Ф_{зал}$ = 3997 грн.);

H_a – річна норма амортизації на ПК (H_a = 0,1 частки одиниці);

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення ($H_{апз}$ = 0,2 частки одиниці);

$K_{лпз}$ – вартість ліцензійного програмного забезпечення ($K_{лпз}$ = 1827 грн.);

F_p – річний фонд робочого часу (за 40-годинного робочого тижня (F_p = 1920 годин).

Вартість 1 години машинного часу ПК визначається за формулою (3.5):

$$C_{мч} = 0,8 \cdot 1 \cdot 1,64 + \frac{3997 \cdot 0,1}{1920} + \frac{1827 \cdot 0,2}{1920} = 2,85 \text{ грн.}$$

Витрати на створення програмного продукту $К_{пз}$ визначаються за формулою (3.2)

$$K_{пз} = 15639+24,19=15663,19 \text{ грн.}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість створення програмного забезпечення *Кпз* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Вартість безстрокової ліцензії Exiland Backup Standard для юридичних осіб при закупівлі її на 2-15 ПК складає 650 грн. Програмне забезпечення встановлюється на 3 ПК.

Таким чином, капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, (3.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки ($К_{пр}$=15663,19 грн.);

$К_{зпз}$ –вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), ($К_{зпз}$ = 650*3=1950 грн.);

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки визначаються за формулою (3.6):

$$К = 15663,19 + 1950 = 17613,19 \text{ грн.}$$

Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad \text{грн.} (3.7)$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в$ = 0);

$С_к$ - витрати на керування системою в цілому обчислюються за формулою (3.8);

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (3.8)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 0 грн.).

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій.

Амортизації підлягає програмне забезпечення Exiland Backup Standard загальною вартістю 1950 грн. з припустимим строком дії користування 2 роки. Таким чином, річні амортизаційні відрахування за прямолінійним методом нарахування складуть:

$$С_а = 1950 / 2 = 975 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.15)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного системного адміністратора на місяць складає 15000 грн. Додаткова заробітна плата –8% від основної заробітної плати. Отже,

$$С_з = 15000*12 + 15000*12*0,08= 194400 \text{ грн.}$$

З 01.01.2016 року ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 194400*0,22 = 42768 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,} \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р = 0,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою (3.16):

$$С_{ел} = 0,8*1920*1,64 = 2519,04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% ($С_{тос}$ = 17613,19*0,01=176,13 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою (3.8):

$$С_к = 975 + 194400 + 42768 + 2519,04 + 176,13= 481676,34 \text{ грн.}$$

Річні поточні витрати на функціонування системи інформаційної безпеки визначаються за формулою (3.9):

$$C = 481676{,}34 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості збитку застосовуємо спрощену модель оцінки.

Необхідні вхідні дані для розрахунку:

де $t_п$ – час простою вузла внаслідок атаки ($t_п$ = 12 годин);

$t_в$ – час відновлення після атаки персоналом ($t_в$ = 8 годин);

$t_{ві}$ – час повторного введення загубленої інформації співробітниками атакованого сегменту мережі ($t_{ві}$ = 7 годин);

$З_о$ – заробітна плата обслуговуючого персоналу ($З_о$ = 8000 грн. на місяць);

$З_с$ – заробітна плата співробітників атакованого вузла ($З_с$ = 10000 грн. на місяць);

$Ч_о$ – чисельність обслуговуючого персоналу ($Ч_о$ = 2 особи);

$Ч_с$ – чисельність співробітників атакованого сегменту мережі ($Ч_с$ = 2 особи);

О – обсяг продажів атакованого сегменту мережі, (О = 260000 грн. на рік);

$П_{зч}$ – вартість заміни устаткування або запасних частин, ($П_{зч}$ = 0 грн.);

I – число атакованих вузлів (I = 3);

N – середнє число атак на рік (N = 30).

Упущена вигода від простою атакованого вузла становить:

$$U = П_п + П_в + V, \quad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн.;

$П_в$ – вартість відновлення працездатності сегмента мережі, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

Упущена вигода від простою атакованого вузла визначається за формулою (3.10):

$$U = 681,82 + 761,37 + 3375 = 4818,19 \text{ грн.}$$

Втрати від зниження продуктивності співробітників атакованого сегмента мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п$$

$$Пп=\sum ЗсF \cdot \ tп \ ,(3.11)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить F = 176 годин).

Втрати від зниження продуктивності співробітників атакованого сегмента мережі визначаються за формулою (3.18):

$$П_п = \frac{10000}{176} \cdot 12 = 681,82 \text{ грн.}$$

$$Пп=\sum ЗсF \cdot \ tп$$

Витрати на відновлення працездатності сегмента мережі включають кілька складових:

$$П_в = П_{ві} + П_{пв} + П_{зч},(3.12)$$

де $П_{ві}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення сегмента мережі, грн.;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн..

Витрати на відновлення працездатності сегмента мережі визначаються за формулою (3.12):

$$П_в = 397,73 + 363,64 = 761,37 \text{ грн.},$$

Витрати на повторне введення інформації $П_{ві}$ розраховуються, виходячи з розміру заробітної плати співробітників атакованого сегмента мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ві}$:

$$П_{ві} = \frac{\sum Зс}{F} \cdot t_{ві} \quad .(3.13)$$

Витрати на повторне введення інформації визначаються за формулою (3.13):

$$П_{ві} = \frac{10000}{176} \cdot 7 = 397{,}73 \text{ грн.}$$

Витрати на відновлення сегмента мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу:

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \quad .(3.14)$$

Витрати на відновлення сегмента мережі визначаються за формулою (3.14):

$$П_{пв} = \frac{8000}{176} \cdot 8 = 363{,}64 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого сегмента мережі визначаються виходячи із середньогодинного обсягу продажів типового підприємства і сумарного часу простою атаковано сегмента мережі:

$$V = \frac{O}{Fp} \cdot (t_п + t_в + t_{ві}) \text{, грн.(3.15)}$$

де $F_р$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько ($F_р$ = 2080 годин).

Втрати від зниження очікуваного обсягу продажів типового підприємства визначаються за формулою (3.15):

$$V = \frac{260000}{2080} \cdot (12 + 8 + 7) = 3375 \text{ грн.},$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \Sigma_i \Sigma_n U = 3*30*4818,19=867274,2 \text{ грн} \quad (3.16)$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.}, \quad (3.17)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (95%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і визначається за формулою (3.17):

$$E = 867274,2*0,95 – 481676,34 = 342234,16 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \quad (3.18)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI визначається за формулою (3.18):

$$ROSI = \frac{171117,075}{17619,19} = 9,71, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100), \quad (3.19)$$

де $N_{деп}$ – річна депозитна ставка, (18 %);

$N_{інф}$ – річний рівень інфляції, (13%).

Розрахункове значення коефіцієнта повернення інвестицій визначається за формулою (3.19):

$$35,86 > (18 - 13)/100 = 9,71 > 0,05.$$

Термін окупності капітальних інвестицій T_o визначається за формулою (3.20) та показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{9,71} = 0,1 \text{, років.} \quad (3.20)$$

3.4 Висновок

Результатом проведеної роботи в даному розділі є обґрунтування економічної доцільності проектування та впровадження методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках на прикладі банківської системи.

Розраховані капітальні витрати, які складають 35238,38 грн., поточні витрати на експлуатацію системи інформаційної безпеки, що становлять 481676,34 грн. Визначена величина економічного ефекту складає 342234,16 грн. Коефіцієнт повернення інвестицій складає 9,71 та швидкість повернення - 0,1 року.

Аналіз проведених розрахунків дозоляє зробити висновок про економічну доцільність впровадження запропонованої методики.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було розглянуто питання актуальності захисту інформації, використання технології блокчейн, стану фінансових технологій та їх використання у банківській сфері задля захисту інформації.

У другому розділі були описані та проаналізовані методи та засоби захисту інформації у фінансово-технологічних застосунках на прикладі банківської системи, проаналізовано захист інформації в банківській сфері. Розглянуто питання використання технології блокчейн та її використання у фінансово-технологічних застосунках. Були надані методичні рекомендацій щодо захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках.

В третьому розділі визначено економічну доцільність впровадження методики. Проведено розрахунки капітальних витрат, поточних витрат, оцінки

величини збитку та загальний ефект від впровадження методики. Тому, в даному випадку, ці методичні рекомендації використовувати доцільно.

ПЕРЕЛІК ПОСИЛАНЬ

1. Шадрин И. П. Подготовка и принятие управленческого решения / И. П. Шадрин. — Якутск, 1970. — 123 с.
2. «Інформаційна безпека особистості», «Поняття інформаційної безпеки». URL: https://sites.google.com/site/infobezosob/
3. Князев А. А. Информационная война Архівовано 26 березень 2014 у Wayback Machine. // Энциклопедический словарь СМИ. — Бишкек: Издательство КРСУ, 2002
4. AlexandraSokolenko1 (2019-02-15). Кибербезопасность. Дмитрий Ганжело.
5. Северина, С. В. (2016). Інформаційна безпека та методи захисту інформації
6. Давидова Ірина Віталіївна ТЕХНОЛОГІЯ БЛОКЧЕЙН: ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ
7. «Просто о технологии и ее применении в отрасли». URL: http://my-trade-group.com
8. «Блокчейн – рождение новой экономики». URL: https://www.youtube.com/watch?v=kqhuWGjJ8_Q
9. Давидова Ірина Віталіївна ТЕХНОЛОГІЯ БЛОКЧЕЙН: ПЕРСПЕКТИВИ РОЗВИТКУ В УКРАЇНІ
10. Introduction to reliable and secure distributed programming / Christian Cachin, Rachid Guerraoui, and Luis Rodrigues.
11. Финансовые технологии. URL: https://ru.wikipedia.org/wiki
12. Третьяков Д.Е. Тенденции развития банковского и финан- сово-технологического сектора на основе использования высоких технологий. Креативная экономика. 2017. Т. 11. No 8. С. 893–89

13. ПаперникС.М.Щотакефінтех. URL: http://www.management.com.ua/notes/what-is-fintech.html.
14. Инвестиции в FinTech: сколько денег вложили в инновационный сектор в 2020 году - investment.24tv.ua
15. FinTech Ukraine 2017: матеріали конференції. URL: https:// mind.ua/publications/20178132-fintech-v-ukrayini-yak-jomu-obijti-banki-ta-na-chomu-zaroblyati
16. Блокчейн в Україні: що це за технологія і чим вона ко- рисна. URL: https://112.ua/statji/blokcheyn-v-ukraine- chto-eto-za-tehnologiya-i-chem-ona-polezna-417161.Html
17. Сфери застосування блокчейн-технологій. URL: http://cryptocurrency.co.ua/blockchain/primenenie.html
18. Технології, які змінюють світ: blockchain. URL: http://biz.nv.ua/ukr/experts/prazdnikov_m/tehnologiji- jakizminjujut-svit-blockchain-2008567.html
19. Народний банк Китаю тестує власну цифрову ва- люту. URL: http://coinews.io/ua/category/1-kripto/ article/256-narodnij-bank-kitaju-testu%D1%94-vlasnu- cifrovu-valjutu
20. Потенчук Г. Фінансові технології: сутність та регу- лювання. URL: http://www.economyandsociety.in.ua/ journal/13_ukr/200.pdf.
21. Блокчейн-проект в Грузії. URL: https://bitnovosti.com/ tag/bitfury-blokchejn-proekt-v-gruzii
22. Як технологія блокчейн змінить світовий фі- нансовий ринок. URL: https://minfin.com.ua/ ua/2018/07/02/34184749
23. Третьяковська галерея запустить блокчейн-проект. URL: https://www.interfax.ru/culture/637938
24. Швейцарська компанія “WISeKey” відкрила Центр блокчейну в Женеві. URL: https://proexpress.com. ua/uk/shveicarskaia-kompaniia-wisekey-otkryla-centr- blokcheina-v-jeneve

25. Глава Міжнародного валютного фонду (МВФ) Крістін Лагард. URL: https://bloomchain.ru/blockchain-fintech/ kristin-lagard-predlozhila-borotsya-s-kriptovalyutami-s- pomoshhyu-blokchejna
26. Як блокчейн змінить фінансовий ринок. URL: https://busines.in.ua/yak-blokchejn-zminyt-finansovyj- rynok
27. Великі банки по всьому світі переходять на використання технології блокчейну. URL: https://mind.ua/news/20177207-veliki-banki-po- usomu-svitu-perehodyat-na-vikoristannya-tehnologiyi- blokchejnu
28. Рузакова О., Гринь Є. Застосування технології Blockchain до систематизації результатів інтелекту- альної діяльності. Вісник Пермського університету. Юридичні науки. 2017. No 38. С. 508–520.
29. Козаченко І.П. Загальні принципи захисту банківської комп'ютерної інформації / І.П. Козаченко, В.О. Голубєв / Центр дослідження проблем комп'ютерної злочинності. URL: http://www.crime-research.ru/library/Koz_gol.htm.
30. Пичугина П.А. Проблемы обеспечения информационной безопасности в банковских информационных системах / П.А. Пичугина. URL: http://www. tvvlibrary.narod.ru/papers/2011/6-11.pdf.
31. Ролдугіна Ю.В. Особливості інформаційної безпеки банків / Ю.В. Ролдугіна, І.В. Ковальова // Актуальні проблеми економічного і соціального розвитку регіону. – 2011. – С.283-287.
32. Засадна Х.О. Стандарти управління інформаційною безпекою / Х.О. Засадна // Фінансовий простір. – 2011. – No3 (3). – С.60-64.
33. Бодюл Є.М. Інформаційна безпека банку / Є.М. Бодюл // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст] : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С.53-55.

34. Бєлоусова К.І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи / К.І. Бєлоусова, Я.І. Бєлоусов // Науковий вісник ДУІКТ. – 2010. – С.33-38.
35. Марущак А.І. Інформаційна безпека банківської установи: структура та система забезпечення / А.І. Марущак // Протидія злочинам, які вчиняються з використанням комп'ютерних мереж [Текст] : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». – Суми : ДВНЗ «УАБС НБУ», 2010. – С.21-24.
36. Козаченко І.П. Загальні принципи захисту банківської комп'ютерної інформації / І.П. Козаченко, В.О. Голубєв / Центр дослідження проблем комп'ютерної злочинності. – [Електронний ресурс]. – Режим доступу: http:// www.crime-research.ru/library/Koz_gol.htm.
37. Зубок М.І. Безпека банківської діяльності / М.І. Зубок: Навч. посібник. – К.: КНЕУ, 2002. – 190 с.
38. Гапоненко В.Ф. Экономическая безопасность предприятий. Подходы и принципы / В.Ф. Гапоненко, А.Л. Беспалько, А.С. Власков. – М.: Издательство «Ось-89», 2007. – 208с.
39. How does blockchain impact banking and lending? URL: https://consensys.net/blockchain-use-cases/finance/#banking
40. Joe Light, Benjamin Bain, Olga Kharif. Facebook Weighs Libra Revamp to Address Regulatory Concerns. URL: https://www.bloomberg.com/news/articles/2020-03-03/facebook-weighs- libra-revamp-to-win-over-reluctant-regulators?srnd=technology-vp
41. Culp S., Kim F., Gomes R. Banking Risk: Evolving ecosystem, evolving threats. Accenture URL: https://www.accenture.com/us-en/insights/financial-services/banking-global-risk-study (дата звернення: 15.06.2020).

42. Casino F., Dasaklis T.K., Patsakis C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics. 2019. Vol. 36. P. 55–81. URL: https://doi.org/10.1016/j.tele.2018.11.006.
43. Bahou A.J. Blockchain and Applications in Information Security. Information Systems Security Association URL: https://issa-midtn.org/resources/Documents/AJ%20Bahou%20-%20Blockchain%20Applications%20in%20Information%20Security.pdf
44. Building confidence: solving banking`s cybersecurity conundrum. Accenture URL: https://www.accenture.com/_ acnmedia/pdf-44/accenture-building-confidence-solving-banking-cybersecurity-conundrum.pdf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	3	
3	А4	Зміст	2	

4	А4	Вступ	1	
5	А4	1 Розділ	24	
6	А4	2 Розділ	40	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

1. ПОЯСНЮВАЛЬНА ЗАПИСКА - Деркач.docx
2. Презентація - Деркач.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник розділу _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук

на кваліфікаційну роботу магістра на тему:

“Обґрунтування методики захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках”

студента групи 125м-19-1

Деркача Дениса Олеговича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __джерела та __ додатка.

Актуальність теми полягає в необхідності підвищення захищеності інформації з обмеженим що циркулює у банківських системах.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було описано та проаналізовано методи та засоби вирішення задачі, проаналізовано захист інформації в банківській сфері. Розглянуто питання використання технології блокчейн та її використання у фінансово-технологічних застосунках. Були надані методичні рекомендацій щодо захисту інформації на основі використання технології блокчейн у фінансово-технологічних застосунках.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому кваліфікаційна робота задовольняє усім вимогам і може бути допущена до захисту, а її автор ***Деркач Денис Олегович*** заслуговує на оцінку «_____».

Керівник кваліфікаційної роботи,

_____

Керівник спец. част.

_____