Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра інформаційної безпеки та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)

магістр
(ступінь вищої освіти)

на тему Аналіз сучасного стану кібербезпеки банківської та фінансової структури України
(назва теми)

Виконав: студент 6 курсу, групи БКз-812м
Спеціальності 125 Кібербезпека
(код і найменування спеціальності)
Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних мереж
НІКУЛІН С.А.
(ПРІЗВИЩЕ та ініціали)

Керівник: НЕЛАСА Г.В.
(ПРІЗВИЩЕ та ініціали)

Рецензент НІКУЛІЩЕВ Г.І.
(ПРІЗВИЩЕ та ініціали)

2023

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Освітній ступінь магістр
Спеціальність 125 Кібербезпека
(код і найменування)

Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних мереж

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри ІБтаН
Андрій КОРОТУН
« 04 » вересня 2023 року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

НІКУЛІНА Сергія Анатолійовича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз сучасного стану кібербезпеки банківської та фінансової структури України
Analysis of the Current State of Cybersecurity in the Banking and Financial Structure of Ukraine

керівник проєкту (роботи): к.т.н., доцент, НЕЛАСА Ганна Вікторівна
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по-батькові)

затверджені наказом закладу вищої освіти від «28» 11 2023 року № 476

2. Строк подання студентом проєкту (роботи): « 11 » 12 2023 року
3. Вихідні дані до проєкту (роботи): Нормативно правові та законодавчі акти України, періодичні видання, науково – методичні розробки вітчизняних та зарубіжних авторів.
4. Зміст розрахунково – пояснювальної записки (перелік питань, які потрібно розробити):
Огляд сучасної банківської та фінансової сфери
Методи захисту в банківських та фінансових установах
Порівняльний аналіз методів захисту персональних даних в банківських та фінансових установах
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
Презентація доповіді (в MS PowerPoint), 15 слайдів.

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1 – 4	НЕЛАСА Г. В., доцент кафедри ІБтаН	04.09.2023	05.12.2023
Нормоконтроль	КОРОЛЬКОВ Р. Ю., доцент кафедри ІБтаН		08.12.2023

7. Дата видачі завдання : « 04 » вересня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1.	Аналіз літературних джерел за тематикою дослідження	04.09.2023 – 15.09.2023	виконано
2.	Збір інформації	16.09.2023 – 10.10.2023	виконано
3.	Аналіз даних та їх класифікація	11.10.2023 – 21.10.2023	виконано
4.	Написання теоретичної частини дипломної роботи	22.10.2023 – 10.11.2023	виконано
5.	Написання аналітичної частини дипломної роботи	11.11.2023 – 25.11.2023	виконано
6.	Перевірка чернетки дипломної роботи та внесення змін до неї керівником	26.11.2023 – 28.11.2023	виконано
7.	Оформлення матеріалів магістерської роботи	29.11.2023 – 05.12.2023	виконано
9	Підготовка до захисту в ДЕК	06.12.2023 – 10.12.2023	виконано

Студент _____ Сергій НІКУЛІН
(підпис) (Ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Ганна НЕЛАСА
(підпис) (Ім'я, ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 83 с., 2 табл., 2 рис., 40 джерел.

БАНК, ІНФОРМАЦІЙНА БЕЗПЕКА, ЕЛЕКТРОННИЙ ЦИФРОВИЙ ПІДПИС, СИМЕТРИЧНЕ ШИФРУВАННЯ, АВТОМАТИЗОВАНА БАНКІВСЬКА СИСТЕМА

Актуальність теми. Кібербезпека банківської та фінансової структури України є одним із найважливіших питань національної безпеки. У сучасних умовах зростання кіберзагроз, які можуть призвести до серйозних фінансових втрат, порушення роботи банківських систем та навіть до дестабілізації фінансової системи країни, забезпечення кібербезпеки банків та фінансових установ є пріоритетним завданням для держави та бізнесу.

Об’єкт дослідження – банківська та фінансова структури України.

Предмет дослідження – кібербезпека банківської та фінансової структури України.

Мета роботи – проаналізувати сучасний стан кібербезпеки банківської та фінансової структури України.

Задачі дослідження – охарактеризувати основні кіберзагрози, яким піддається банківська та фінансова структура України, проаналізувати стан кібербезпеки банків та фінансових установ в Україні, розробити пропозиції щодо підвищення кібербезпеки банківської та фінансової структури України.

Наукова новизна. Робота включає аналіз нормативно-правової бази, організаційних та технічних заходів, що застосовуються для забезпечення кібербезпеки банківської та фінансової структури. Проведено порівняльний аналіз кібербезпеки банківської та фінансової структури України з іншими країнами світу.

ABSTRACT

Explanatory note to the master's thesis: 83 pp., 2 tables, 2 figures, 40 sources.

BANK, INFORMATION SECURITY, ELECTRONIC DIGITAL SIGNATURE, SYMMETRICAL ENCRYPTION, AUTOMATED BANKING SYSTEM

Actuality of theme. Cybersecurity of the banking and financial structure of Ukraine is one of the most important issues of national security. In today's conditions of growing cyber threats, which can lead to serious financial losses, disruption of banking systems and even destabilization of the country's financial system, ensuring the cyber security of banks and financial institutions is a priority task for the state and business.

The object of the study is the banking and financial structure of Ukraine.

The subject of the study is cyber security of the banking and financial structure of Ukraine.

The purpose of the work is to analyze the current state of cyber security of the banking and financial structure of Ukraine.

The objectives of the research are to characterize the main cyber threats to which the banking and financial structure of Ukraine is exposed, to analyze the state of cyber security of banks and financial institutions in Ukraine, to develop proposals for improving the cyber security of the banking and financial structure of Ukraine.

Scientific novelty. The work includes an analysis of the legal framework, organizational and technical measures used to ensure the cyber security of the banking and financial structure. A comparative analysis of the cyber security of the banking and financial structure of Ukraine with other countries of the world was conducted.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

НБУ – Національний банк України;

ДСТУ – Державний стандарт України;

ЕЦП – Електронний цифровий підпис;

СЕП – Системи електронних платежів;

ПЗ – Програмне забезпечення;

АБС – Автоматизована банківська система;

ІБ – Інформаційна безпека;

AES – Advanced Encryption Standard (вдосконалений стандарт шифрування);

СБ – служба безпеки;

СУБД – система управління базою даних;

ОС – операційні системи;

DES – Data Encryption Standard;

NAT – Network Address Translation.

ВСТУП

Сучасний світ характеризується швидкими темпами розвитку інформаційних технологій, що істотно змінює всі сфери суспільного життя, в тому числі і фінансову. Банківський сектор України є однією з найбільш цифровізованих галузей економіки, що робить його вразливим до кібератак. Банківський та фінансовий сектор є особливо вразливим до кіберзлочинності, оскільки він обробляє величезні обсяги чутливих даних.

За останні роки в Україні спостерігається зростання кількості кібератак на фінансові установи. Так, у 2022 році було зафіксовано понад 1000 таких атак, що призвело до збитків на суму понад 1 мільярд гривень. під час російської агресії, кібератаки на українські банки та фінансові установи стали частиною гібридної війни Росії проти України. За даними Національного банку України, у 2022 році кількість кібератак на банки та фінансові установи зросла на 70%.

Актуальність даної теми обумовлена наступними факторами:

– зростанням можливостей обчислювальної техніки;

– посилення кібератак на банківський та фінансовий сектор України;

– важливість банківського та фінансового сектору для національної безпеки України;

– необхідність підвищення рівня кібербезпеки банківського та фінансового сектору України.

Основними завданнями банку або фінансової установи щодо забезпечення інформаційної безпеки є:

– виявлення потенційних загроз інформаційній безпеці і вразливостей;

– запобігання інцидентам інформаційної безпеки;

– нейтралізація або мінімізація загроз інформаційній безпеці банку або фінансовій установі.

Структура інформаційної безпеки банківської та фінансової установи складається з таких основних складових:

– забезпечення безпеки інформаційних ресурсів;

– забезпечення безпеки інформаційної інфраструктури;

– забезпечення безпеки інформаційного поля.

Інформаційні ресурси – це інформація, яка циркулює в інформаційній системі банківської та фінансової установи, яка зберігається на різноманітних носіях, і яка належить банківській та фінансовій установі. Тому основною метою безпеки даних ресурсів є збереження такої інформації від несанкціонованого витоку, використання у зловмисних цілях, або порушення її конфіденційності.

Інформаційна інфраструктура. Її безпека полягає у збереженні такого стану захищеності ЕОМ (комп'ютерів), електронних систем та мереж і мереж електрозв'язку банківської та фінансової установи, яка повністю гарантує цілісність і доступність інформації, яка в них проходить обробку (зберігається чи циркулює).

Щодо забезпечення безпеки «інформаційного поля» банківської або фінансової установи, то вона полягає у контролі тих потоків інформації, які є несистематизованими і оприлюднюються різними учасниками інформаційних відносин, а саме теле і радіо-організаціями, друкованими та інтернет-виданнями, конкурентами, органами державної влади і місцевого самоврядування тощо.

Методика дослідження – це сукупність методів і прийомів, які застосовуються для досягнення поставленої мети дослідження.

У дипломній магістерській роботі на тему "Аналіз сучасного стану кібербезпеки банківської та фінансової структури України" будуть використані такі методи дослідження:

– аналітичний метод – це метод дослідження, який полягає в розчленуванні об'єкта дослідження на складові частини та вивченні їхніх взаємозв'язків. Аналітичний метод буде використаний для дослідження основних кіберзагроз, яким піддається банківська та фінансова структура України, а також для аналізу стану кібербезпеки банків та фінансових установ в Україні;

– статистичний метод – це метод дослідження, який полягає в збиранні, обробці та аналізі статистичних даних. Статистичний метод буде використаний для аналізу даних про кількість і характер кібернападів на банки та фінансові установи;

– метод експертних оцінок – це метод дослідження, який полягає в отриманні інформації від експертів у відповідній галузі. Метод експертних оцінок буде використаний для отримання інформації про думку експертів щодо стану кібербезпеки банків та фінансових установ в Україні.

Вибір методів та інструментів дослідження залежить від мети та завдань дослідження. У дипломній магістерській роботі на тему "Аналіз сучасного стану кібербезпеки банківської та фінансової структури України" поставлені такі завдання:

– охарактеризувати основні кіберзагрози, яким піддається банківська та фінансова структура України;

– проаналізувати стан кібербезпеки банків та фінансових установ в Україні;

– розробити пропозиції щодо підвищення кібербезпеки банківської та фінансової структури України.

Для досягнення першого завдання буде використаний аналітичний метод дослідження. Для цього будуть проаналізовані нормативно-правові акти, наукові статті, звіти про дослідження тощо.

Для досягнення другого завдання будуть використані аналітичний та статистичний методи дослідження. Для цього будуть проаналізовані дані про кількість і характер кібернападів на банки та фінансові установи в Україні.

Для досягнення третього завдання будуть використані аналітичний, статистичний та метод експертних оцінок. Для цього буде проведено аналіз існуючих заходів щодо підвищення кібербезпеки банків та фінансових установ, а також буде отримано інформацію від експертів у відповідній галузі.

Для проведення дослідження будуть використані такі інструменти:

– книги, статті, звіти про дослідження – для аналізу нормативно-правових актів, наукових статей, звітів про дослідження тощо;

– дані про кількість і характер кібернападів на банки та фінансові установи в Україні – для аналізу статистичних даних;

– наукові статті та думки експертів з кібербезпеки – для отримання інформації від експертів у відповідній галузі.

Методика дослідження, яка буде використана в дипломній магістерській роботі на тему "Аналіз сучасного стану кібербезпеки банківської та фінансової структури України", є обґрунтованою та адекватною поставленим завданням. Вона дозволить отримати достовірну інформацію, яка буде використана для розробки пропозицій щодо підвищення кібербезпеки банківської та фінансової структури України.

1 ОГЛЯД СУЧАСНОЇ БАНКІВСЬКОЇ ТА ФІНАНСОВОЇ СФЕРИ

1.1 Кіберзагрози та ризики

У сучасному світі, де інформаційні технології відіграють вирішальну роль у фінансовій сфері, питання кібербезпеки стали однією з найбільш актуальних та важливих проблем. Банківська система, яка зберігає та обробляє величезний обсяг фінансової інформації, стала основним об'єктом для кіберзлочинців. Серйозні загрози з боку хакерів, вірусів, фішингових атак, та інших кіберзагроз щодня тестують захищеність банківських та фінансових структур.

Банківська сфера є невід'ємною частиною сучасного світу та глобальної економіки. Банки виконують важливі функції в системі фінансового обігу, забезпечуючи надійність зберігання грошей, надання кредитів, обслуговування платежів та багато інших фінансових послуг. Діяльність банків впливає на стабільність економіки країни та життя її громадян.

Банки виконують наступні ключові функції:

– забезпечення фінансової стабільності: банки допомагають підтримувати стабільність економіки, забезпечуючи ліквідність та фінансову підтримку підприємств та населення;

– зберігання грошей: банки є безпечними місцями для зберігання грошей та цінних паперів, надійно захищаючи їх від втрати чи крадіжки;

– надання кредитів: банки надають позики та кредити підприємствам і громадянам, що сприяє розвитку бізнесу та особистим фінансовим цілям;

– платіжні послуги: банки обробляють та забезпечують безпечний обмін грошей між різними особами та організаціями, дозволяючи здійснювати різноманітні платежі;

– управління активами: банки допомагають клієнтам у розміщенні та управлінні їхніми фінансовими активами, такими як інвестиції та портфелі.

Структура банківської сфери.

Банківська система України складається з двох рівнів:

– перший рівень – Національний банк України (НБУ). НБУ є центральним банком країни, який здійснює регулювання та контроль банківської діяльності;

– другий рівень – комерційні банки. Комерційні банки є юридичними особами, які здійснюють банківську діяльність з метою одержання прибутку.

Комерційні банки поділяються на:

– Державні банки;

– приватні банки – банки, статутний капітал яких належить фізичним та/або юридичним особам, які не є державою;

Процеси, що відбуваються у банках

У банках відбуваються такі основні процеси:

– приймання вкладів. Фізичні та юридичні особи розміщують свої гроші у банках у вигляді вкладів. Вклади можуть бути строковими або безстроковими, депозитними або поточними;

– надання кредитів. Банки надають кредити фізичним та юридичним особам на різні цілі. Кредити можуть бути забезпеченими або не забезпеченими;

– проведення платежів. Банки здійснюють платежі за дорученням своїх клієнтів. Платежі можуть бути внутрішньобанківськими або міжбанківськими;

– інші послуги. Банки надають своїм клієнтам широкий спектр інших послуг, таких як валютний обмін, страхування, консультування тощо.

Банківська сфера є однією з найцінніших цілей для кіберзлочинців. Банки зберігають величезну кількість чутливої інформації про своїх клієнтів, а також мають доступ до значних фінансових ресурсів. Це робить їх привабливими цілями для атак, які можуть призвести до серйозних фінансових збитків, порушення конфіденційності та навіть крадіжки особистих даних.

Відмінність банківської і фінансової структури України.

Банківська і фінансова структури в Україні є важливими складовими фінансової системи країни, і хоча вони взаємодіють і мають спільні елементи, є деякі відмінності між ними.

Складові банківської структури:

– комерційні банки, які надають різноманітні фінансові послуги, такі як розрахунково-касове обслуговування, кредитування, зберігання коштів, інвестиційні послуги тощо;

– небанківські фінансові установи: сюди входять страхові компанії, лізингові компанії, інвестиційні фонди тощо.

Складові фінансової структури:

– комерційні банки, але не обмежується лише ними. Вона охоплює всі види фінансових установ, включаючи банки, страхові компанії, пенсійні фонди, лізингові компанії, інвестиційні фонди, ринок цінних паперів тощо;

– фінансові послуги: фінансова структура також включає надання різних фінансових послуг, які не обов'язково пов'язані з банківською діяльністю. Це може включати страхування, інвестування в цінні папери, пенсійне забезпечення тощо.

Регулювання і нагляд.

– банки: банківська діяльність суворо регулюється Національним банком України (НБУ), який виступає як головний регулятор і наглядач в банківській сфері;

– фінансові установи: фінансові установи також піддаються регулюванню, але це може залежати від конкретного типу установи і від регулюючого органу (НБУ, Комісія з цінних паперів та фондового ринку України, Державна служба фінансового моніторингу тощо).

Цільове призначення.

– банки: основне завдання банків – надання фінансових послуг, зокрема управління коштами клієнтів, видача кредитів тощо;

– фінансові установи: фінансові установи можуть мати більший спектр діяльності, включаючи страхування ризиків, управління інвестиціями, пенсійне забезпечення тощо.

Важливо відзначити, що банки є складовою частиною фінансової структури, але фінансова структура більш широка і охоплює різні види фінансових установ і послуг.

Основні види кіберзагроз.

До основних видів кіберзагроз, які ставлять під загрозу банківську та фінансову сфери, відносяться:

– зловмисне програмне забезпечення – це програмний код, який розроблений з метою завдати шкоди комп'ютеру або його користувачам. Зловмисне програмне забезпечення може використовуватися для крадіжки особистих даних, розкрадання фінансових коштів або зараження комп'ютерної системи;

– фішинг – це вид шахрайства, при якому зловмисники намагаються отримати особисту інформацію про жертву, такі як логін, пароль або номер кредитної картки. Фішингові атаки часто здійснюються за допомогою електронних листів або веб-сайтів, які виглядають як офіційні веб-сайти банків або інших фінансових установ;

– злом – це процес несанкціонованого доступу до комп'ютерної системи або мережі. Зловмисники, які зламують комп'ютерну систему банку,

можуть отримати доступ до чутливої інформації, такої як дані клієнтів або фінансові дані;

– DDoS-атака – це атака, при якій зловмисники намагаються зробити веб-сайт або службу недоступними для користувачів. DDoS-атаки часто здійснюються шляхом надсилання великої кількості запитів до веб-сайта або служби, що може призвести до їх завантаження;

– соціальна інженерія, яка включає в себе маніпуляцію людьми, щоб отримати доступ до конфіденційної інформації або фінансових ресурсів. Це може включати в себе використання соціальних мереж, фішингових листів або телефонних обманів.

Наслідки Кібератак.

Фінансові втрати. Кібератаки можуть призвести до серйозних фінансових втрат для банків. Наприклад, великі суми грошей можуть бути вкрадені або вимагатися у вигляді викупу в обмін на розкодування зашифрованих даних.

Втрата довіри клієнтів .Кібератаки можуть призвести до втрати довіри клієнтів банку, оскільки вони можуть втратити доступ до своїх рахунків або стати жертвами шахрайства.

Пошкодження репутації. Пошкодження репутації може бути серйозним наслідком кібератак для банку. Втрата довіри клієнтів та публічне викриття недоліків у системах безпеки може негативно вплинути на репутацію банку та призвести до втрати бізнесу.

Юридичні проблеми. Кібератаки можуть призвести до юридичних проблем для банку, включаючи відповідальність за порушення конфіденційності та безпеки даних клієнтів.

Кіберзагрози становлять серйозну загрозу для банківської сфери. Розуміння різних видів кіберзагроз та їх можливих наслідків є важливим для розробки та впровадження ефективних стратегій кібербезпеки в банківській сфері. У наступних розділах будуть розглянуті сучасні методи та технології

кіберзахисту, які допоможуть зменшити ризики та підвищити рівень безпеки в цій галузі.

1.2 Заходи з кібербезпеки

Кіберзахист передачі даних.

Шифрування даних є однією з основних стратегій кіберзахисту. Банки повинні використовувати сучасні протоколи шифрування для захисту конфіденційної інформації, яка передається через мережі. Зашифровані канали зв'язку допоможуть уникнути перехоплення та зламу даних під час передачі.

Двофакторна аутентифікація.

Впровадження двофакторної аутентифікації для клієнтів банку може допомогти уникнути несанкціонованого доступу до облікових записів. Цей метод вимагає від користувача надання двох різних видів ідентифікації, таких як пароль і SMS-код.

Моніторинг та виявлення вторгнень.

Банки повинні встановити системи моніторингу та виявлення вторгнень для постійного відстеження активності на своїх мережах та серверах. Це дозволить вчасно виявляти аномальні дії та вторгнення та реагувати на них.

Безпека мобільних додатків.

З огляду на поширеність мобільних банкінгових додатків, банки повинні приділяти особливу увагу їх кіберзахисту. Це включає в себе захист додатків від вразливостей, вимоги до безпеки на рівні програмного забезпечення та контроль доступу.

Навчання та підвищення свідомості.

Навчання співробітників та клієнтів щодо кібербезпеки є важливою частиною стратегії з кіберзахисту. Банки повинні проводити регулярні тренінги та надавати інформацію щодо найновіших загроз та методів захисту.

Резервне копіювання та відновлення даних.

Резервне копіювання даних є необхідним для забезпечення можливості відновлення інформації після кібератаки або інших подій. Банки повинні мати плани резервного копіювання та відновлення, які допоможуть відновити нормальну роботу після інциденту.

Взаємодія з кіберполіцією та іншими агентствами.

Банки повинні співпрацювати з правоохоронними органами та іншими агентствами з метою виявлення та припинення кіберзагроз. Ця взаємодія допомагає у розслідуванні інцидентів та притягненні зловмисників до відповідальності.

Заходи з кібербезпеки є критичними для забезпечення безпеки банківської та фінансової сфери в умовах постійних кіберзагроз і вони повинні бути системними. Банки і фінансові установи повинні приділяти велику увагу захисту своїх клієнтів та даних, а також підтримувати актуальність своїх заходів з кібербезпеки перед сучасними загрозами. У наступному розділі будуть розглянуті приклади сучасних методів кіберзахисту, які можуть бути використані в банківській та фінансовій сфері.

1.3 Правові засади інформаційної безпеки в банківській та фінансовій сферах

Правові засади інформаційної безпеки в банківській та фінансовій сферах України визначаються Конституцією України, законами України "Про Національний банк України", "Про банки і банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про

основні засади забезпечення кібербезпеки України" та іншими нормативно-правовими актами.

Конституція України визначає, що держава забезпечує захист прав і свобод людини і громадянина, в тому числі права на інформацію. Закони України "Про Національний банк України" та "Про банки і банківську діяльність" передбачають, що Національний банк України є центральним банком України, який здійснює регулювання та нагляд за банківською системою України, у тому числі за забезпеченням інформаційної безпеки банків.

Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" визначає правові та організаційні засади захисту інформації в інформаційно-телекомунікаційних системах, у тому числі в банківських та фінансових системах. Закон України "Про основні засади забезпечення кібербезпеки України" визначає правові та організаційні засади забезпечення кібербезпеки в Україні, у тому числі в банківській та фінансовій сферах.

Основними принципами інформаційної безпеки в банківській та фінансовій сферах України є:

- законність;
- комплексність;
- системність;
- відповідальність;
- своєчасність.

Забезпечення інформаційної безпеки в банківській та фінансовій сферах України покладається на Національний банк України, банки, інші фінансові установи та фізичних осіб.

Національний банк України здійснює регулювання та нагляд за банківською системою України, у тому числі за забезпеченням інформаційної безпеки банків. Національний банк України має право:

– встановлювати вимоги до інформаційної безпеки банків;

– здійснювати перевірку банків на відповідність вимогам законодавства з питань інформаційної безпеки;

– накладати штрафи на банки за порушення законодавства з питань інформаційної безпеки.

Банки зобов'язані:

– розробити та впровадити систему управління інформаційною безпекою;

– забезпечити захист інформації, яка використовується в їхній діяльності;

– проводити інформування працівників про заходи з забезпечення інформаційної безпеки.

Фізичні особи зобов'язані:

– не розголошувати конфіденційну інформацію, отриману від банків або інших фінансових установ;

– використовувати надійні паролі та інші засоби захисту інформації.

За порушення законодавства з питань інформаційної безпеки банків та інших фінансових установ, а також фізичних осіб передбачена відповідальність, встановлена законами України.

Для забезпечення інформаційної безпеки в банківській та фінансовій сферах України Національний банк України розробив і затвердив Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. Це Положення визначає порядок організації та здійснення заходів із забезпечення інформаційної безпеки в банківській системі України, у тому числі вимоги до системи управління інформаційною безпекою банків.

Система управління інформаційною безпекою банку повинна включати в себе такі основні елементи:

– політика інформаційної безпеки банку;

– організаційні заходи із забезпечення інформаційної безпеки;

– технічні заходи із забезпечення інформаційної безпеки;

– процедури реагування на інциденти інформаційної безпеки.

Політика інформаційної безпеки банку повинна визначати основні цілі та принципи забезпечення інформаційної безпеки в банку, а також повноваження та відповідальність працівників банку за забезпечення інформаційної безпеки.

Організаційні заходи із забезпечення інформаційної безпеки повинні спрямовуватися на створення ефективної системи управління інформаційною безпекою банку, у тому числі на:

– призначення відповідальної особи за забезпечення інформаційної безпеки в банку;

– розробку і впровадження внутрішніх документів з питань інформаційної безпеки;

– проведення навчання працівників банку з питань інформаційної безпеки.

Технічні заходи із забезпечення інформаційної безпеки повинні спрямовуватися на захист інформації, яка використовується в банківській діяльності, від несанкціонованого доступу, використання, розголошення, модифікації або знищення, а також на запобігання поширенню шкідливого програмного забезпечення.

Процедури реагування на інциденти інформаційної безпеки повинні визначати порядок дій працівників банку у разі виникнення інциденту інформаційної безпеки.

Забезпечення інформаційної безпеки в банківській та фінансовій сферах України є важливим завданням, яке спрямоване на захист прав і інтересів вкладників, кредиторів та інших учасників фінансових відносин.

Постановою правління Національного банку України визначено, що при застосуванні криптографічного захисту банк зобов'язаний використовувати:

а) асиметричні алгоритми:

– алгоритм Діффі – Геллмана (алгоритм DH та ECDH);

– алгоритм цифрового підпису (алгоритм DSA, ECDSA та ДСТУ 4145-2002);

– алгоритм Ривест – Шаміра – Адлемана (алгоритм RSA);

– алгоритми безпеки гешування SHA-224, SHA-256, SHA-384, SHA- 512;

б) алгоритми симетричного шифрування:

– алгоритм ―Advanced encryption standard‖ (AES) із довжиною ключа 128, 192 і 256 біт або більше;

– алгоритм криптографічного перетворення (ДСТУ ГОСТ 28147:2009;

– алгоритм ― Калина (ДСТУ 7624:2014.

Висновки до розділу 1.

В даному розділі дипломної роботи було викладено правові засади інформаційної безпеки в банківській та фінансовій сферах. Охарактеризовані основні можливі види кіберзагроз інформаційної і комунікаційної інфраструктури та можливі наслідки, які пов'язані з інформаційними технологіями, збитки та можливі втрати важливої та конфіденційної інформації, як фінансові втрати так і втрата довіри клієнтів і пошкоджена репутація банківської та фінансової установи. Виділено заходи з кібербезпеки для забезпечення безпеки банківської та фінансової сфери в умовах постійних кіберзагроз із зауваженням, що вони повинні бути системними.

2 МЕТОДИ ЗАХИСТУ В БАНКІВСЬКИХ ТА ФІНАНСОВИХ УСТАНОВАХ

2.1 Захист компьютерної мережі

В організації комплексної інформаційної безпеки банківських та фінансових установ важливу роль відіграє контроль дій службовців, які отримують доступ в Internet з локальної мережі банку.

Для активної взаємодії між філіальними підрозділами банків і фінансових установ з обміну конфіденційною інформацією необхідне забезпечення постійного і захищеного доступу в Internet. Також слід відзначити для здійснення міжбанківських операцій, організації доступу до загальних ресурсів, збору і обробки даних, доступу клієнтів до своїх рахунків в інтерактивному режимі та багатьох інших завдань використання специфічних Internet-додатків.

Якісна робота банківської або фінансової установи клієнтські сервіси яких багато в чому залежать від роботи Internet-каналу, їхнім співробітникам потрібно безперебійний і стабільний доступ в Internet. Як правило, для забезпечення безперервності процесів банківські та фінансові установи підключені до декількох провайдерів, що гарантує необхідну швидкість і якість доступу в Internet.

Для уникнення втрати інформації і простою в роботі банківських додатків при зміні провайдера, необхідно використовувати надійні рішення, які дозволять перевести роботу офісу і всіх сервісів банку з одного Internet-каналу на інший безболісно і без втрат. Для цього в програмному комплексі в рамках інструментарію для організації доступу в Internet повинна бути передбачена робота з двома і більше провайдерами. Наразі існує доволі багато продуктів, які підтримують функцію «Резервного каналу», що дозволяє автоматично переводити всіх користувачів на альтернативне підключення до Internet, якщо зв'язок через основне підключення відсутній.

Робота з основним каналом поновлюється також автоматично, що дозволяє забезпечити безперервний і безперебійний доступ співробітників до Internet-ресурсів та стабільну роботу всіх сервісів банку і фінансової установи.

Крім того, дана функція підтримки кількох каналів дозволяє, наприклад, надати доступ в Internet різним користувачам через різних провайдерів. Це допомагає оптимізувати навантаження на внутрішню мережу і правильно розподілити.

Віддалені філії банку або фінансової установи вимагають налагодженої і захищеної взаємодії для оперативного обміну інформацією та спільного доступу до корпоративних ресурсів. Рішенням для таких цілей є VPN (Virtual private network) – з'єднання до серверів баз даних, поштових серверів. Суть даної технології полягає в здатності захистити трафік будь-яких інформаційних внутрішньо-корпоративних та загальнодоступних систем, аудіо-та відео-конференцій і систем електронної комерції.

Проблема захисту мереж має двоїстий характером. З одного боку, мережа – це єдина система, яка має єдині правила обробки інформації, а з іншого, мережа це купа відокремлених систем, і кожна має свої власні правила обробки інформації.

На мережу атаки можуть здійснюватися з двох рівнів, а можливо і комбіновано:

– з верхнього, коли зловмисник намагається використати властивості мережі для проникнення на певний вузол і виконати певні несанкціоновані дії. Заходи, які вживаються для захисту повинні бути визначеними потенційними можливостями зловмисника і надійністю засобів захисту цих вузлів;

– з нижнього, коли зловмисник намагається використати властивості мережевих протоколів задля порушення конфіденційності або цілісності окремих повідомлень або потоку в цілому. Порушення потоку або повідомлень призводить до витоку інформації і навіть втрати контролю за

мережею. Використовувані протоколи повинні забезпечувати захист повідомлень та їх потоку в цілому.

Захист мережі планується як єдиний комплекс заходів, він охоплює всі особливості обробки інформації. В цьому випадку організація захисту мережі, розробка політики безпеки, її реалізація і керування захистом будуть підкорюватися загальним правилам. Однак потрібно враховувати те, що кожен окремий вузол загальної мережі повинен мати свій індивідуальний захист в залежності від того, які функцій він виконує і від можливостей мережі.

На кожному окремому вузлі необхідно окремо організовувати:

– контроль доступу до усіх файлів і іншим наборам даних, які доступні з інших мереж і з локальної мережі;

– контроль процесів, які активізовані з віддалених вузлів;

– контроль за всім мережевим трафіком;

– проведення ідентифікації та аутентифікації користувачів, які отримують доступ до даного вузла з мережі;

– контроль доступу до ресурсів локального вузла, який є доступним для використання користувачами мережі;

– контроль за поширенням інформації в межах локальної мережі та пов'язаних з нею інших мереж.

Функції захисту протоколів, відповідно до їх призначення:

– фізичний рівень – контролювати електромагнітні випромінювання ліній зв'язку та пристроїв, підтримувати комунікаційне обладнання у робочому стані. Захист на даному рівні забезпечується за допомогою пристроїв, які екранують, генерують перешкоди, засобів фізичного захисту передавального середовища;

– канальний рівень – збільшити надійність захисту даних, які передаються по каналу потрібно забезпечувати за допомогою шифрування. Шифруються всі передані дані, включно зі службовою інформацією;

– мережевий рівень – являє собою самий уразливий рівень з точки зору захисту. На цьому рівні відбувається формування всієї інформації, яка маршрутизується, стають явними відправник та одержувач, на ньому зокрема здійснюється управління потоком. Окрім того, за допомогою протоколів даного рівня, обробка пакетів відбувається на всіх маршрутизаторах, шлюзах і інших проміжних вузлах. Практично всі мережеві порушення відбуваються з використанням саме протоколів даного рівня (читання, модифікація, знищення, дублювання, переорієнтування деяких повідомлень чи всього потоку в цілому, маскування під деякий інший вузол та ін.). Захист від подібних загроз здійснюється за допомогою протоколів мережевого і транспортного рівнів, а також за допомогою засобів криптозахисту. Наприклад використовується вибіркова маршрутизація;

– транспортний рівень – на цьому рівні здійснюється контроль за тими функціями попереднього рівня, які відбуваються на приймальному і передавальному вузлах. За допомогою механізмів даного рівня перевіряється цілісність пакетів даних, їх послідовність, маршрут, який пройдений, час відправки та час доставки, ідентифікація та аутентифікація відправника і одержувача та інші функції. Саме на даному рівні всі активні загрози стають видимими. Цілісності даних та службової інформації досягається крипто захистом. Тільки ті хто мають секретний ключ відправника та одержувача можуть читати та змінювати інформацію і зміна залишається непоміченою. Проте навіть і всі ці заходи не зможуть запобігти загрозі знищення, переробки або затримки повідомлення. Паралельна доставка дублікатів іншими шляхами є захистом від таких загроз;

– верхні рівні – протоколами даних рівней забезпечується контроль взаємодії прийнятої або переданої інформації;

– сеансовий і представницький рівні – протоколи даних рівнів функції захисту не виконують;

– прикладний рівень – протоколами даного рівня виконується управління доступом до потрібних даних, проводиться також ідентифікація та аутентифікація користувачів, а також виконуються інші функції, які визначаються конкретним протоколом.

2.2 Технічний захист конфіденційної інформації

Технічний захист конфіденційної інформації в банківській та фінансовій сфері України є одним із найважливіших завдань для забезпечення стабільної роботи банківської та фінансової системи країни.

Заходи технічного захисту конфіденційної інформації в банківській та фінансовій сфері України регламентуються такими нормативно-правовими актами: Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", Постанова Правління Національного банку України "Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України", Державні стандарти України

Заходи технічного захисту конфіденційної інформації в банківській та фінансовій сфері України можна розділити на такі групи:

а) заходи фізичного захисту:

– використання спеціальних приміщень для зберігання інформації;

– обмеження доступу до приміщення, де зберігається інформація;

– застосування охоронних систем;

б) заходи логічного захисту:

– встановлення спеціальних програмних засобів захисту інформації;

– розробка та впровадження політики безпеки інформації;

– проведення навчання персоналу з питань інформаційної безпеки.

Заходи фізичного захисту спрямовані на запобігання несанкціонованому доступу до інформації шляхом фізичного обмеження доступу до неї. До таких заходів належать:

– розміщення інформації в спеціальних приміщеннях, які мають відповідну охорону;

– застосування механічних засобів захисту, таких як замки, двері, вікна, решітки тощо;

– застосування електронних засобів захисту, таких як відеокамери, датчики руху тощо.

Заходи логічного захисту спрямовані на запобігання несанкціонованому доступу до інформації шляхом використання технічних засобів. До таких заходів належать:

– встановлення спеціальних програмних засобів захисту інформації, таких як брандмауери, антивіруси, антиспам-фільтри тощо;

– розробка та впровадження політики безпеки інформації, яка визначає правила доступу до інформації, зберігання інформації та використання інформації;

– проведення навчання персоналу з питань інформаційної безпеки.

Шифрування інформації є одним із найефективніших методів технічного захисту конфіденційної інформації в банківській та фінансовій сфері України. Шифрування інформації дозволяє зробити її недоступною для несанкціонованого доступу.

Контроль цілісності інформації спрямований на запобігання несанкціонованому модифікуванню інформації. Контроль цілісності інформації здійснюється шляхом використання спеціальних алгоритмів, які дозволяють перевірити, чи була інформація змінена з моменту її останнього запису.

Резервне копіювання інформації спрямоване на забезпечення можливості відновлення інформації у разі її втрати або пошкодження. Резервне копіювання інформації здійснюється шляхом копіювання інформації на зовнішні носії.

Вибір заходів технічного захисту конфіденційної інформації в банківській та фінансовій сфері України залежить від таких факторів, як:

– складність та конфіденційність інформації;

– можливі кіберзагрози;

– фінансові можливості організації.

Для того щоб реалізувати всі ці функції застосовують різні технічні пристрої:

– джерела безперебійного живлення, пристрої стабілізації, які унеможливлюють стрибкоподібні перепади напруги, захищають від навантажень у мережі електроживлення у пікові години;

– екрануючі пристрої для апаратури, ліній зв’язку та приміщень, з комп’ютерною технікою;

– пристрої, які ідентифікують і фіксують термінали і користувачів при спробах несанкціонованого доступу до комп’ютерної мережі;

– засоби. які захищають порти комп’ютерної та мережевої техніки тощо.

Щодо технічної безпеки банківської та фінансової системи, то основні відмінності можна згрупувати наступним чином.

По-перше, банківські системи будуються звичайно на базі розподіленої системи або мультипроцесорної (тому що необхідно опрацьовування дуже великого потоку інформації).

По-друге, систему потрібно надійно захитити і відокремити, а зв’язок з іншими системами здійснити через спеціальні “шлюзи”.

По-третє, потрібно забезпечити робото спроможність системи навіть у разі виходу з ладу окремих вузлів.

Заходи технічного захисту конфіденційної інформації в банківській та фінансовій сфері України повинні бути комплексними та постійно вдосконалюватися. На сьогодні, системи автоматизації банківської діяльності впроваджуються зі значними проблеми захисту. Зважаючи на великі обсяги інвестицій, які потрібно вкладати в технічний захист, ці проблеми враховуються досить слабо, а якщо і враховуються, то не в повному обсязі. Це ускладнює виконання задачі забезпечення належного захисту інформації на етапах її створення, передачі та обробки. Більша увага приділяється захисту тієї інформації, яка виходить за межі банку, в той час, як внутрішня система банку залишається або повністю або частково незахищеною. Це зумовлено великою кількістю зовнішніх загроз і відсутністю статистики злочинів, технічної недосконалості банків.

Одним із основних напрямків розвитку технічного захисту конфіденційної інформації в банківській та фінансовій сфері України є впровадження штучного інтелекту та машинного навчання. Такі технології дозволяють автоматизувати процеси виявлення та реагування на кібератаки, а також підвищити ефективність заходів технічного захисту інформації.

Іншим важливим напрямком є розвиток нормативно-правової бази у сфері кібербезпеки. Важливо, щоб нормативно-правові акти в цій сфері були сучасними та відповідали актуальним загрозам.

Забезпечення ефективного технічного захисту конфіденційної інформації в банківській та фінансовій сфері України є важливою умовою для забезпечення стабільної роботи банківської та фінансової системи країни.

2.3 Програмний захист інформації

Програмні засоби захисту – це програмне забезпечення, яке використовується для захисту інформації від несанкціонованого доступу,

використання, розголошення, модифікації або знищення. Вони є одним із основних елементів системи управління інформаційною безпекою.

Програмні засоби за своїм функціональним призначенням розділяють на програмні засоби ідентифікації і аутентифікації користувачів.

Ідентифікація – це коли будь–якому об’єкту чи суб’єкту присвоюється унікальний образ, ім’я або число.

Аутентифікація – встановлення достовірності, яке полягає у перевірці, чи є перевіряємий об'єкт (суб'єкт) тим, за кого себе видає.

Кінцевою метою ідентифікації і аутентифікації в обчислювальній системі є допуск об’єкта до інформації. яка має обмеження у користуванні, у разі позитивного результату перевірки і відмова в допуску у іншому випадку.

Один з найпоширеніших способів аутентифікації – це присвоєння особі імені або числа – пароля, які є унікальними та зберігання їх значень в обчислювальні системі. При вході в систему користувач вводить свій код паролю, а обчислювальна система порівнює його значення з тим значенням, яке зберігається в пам’яті, якщо коди збігаються, то відкривається доступ до дозволеної функціональної задачі, а при не співпадінні – в доступі відмовляється.

За допомогою поділу коду доступу до об’єкта на дві частини, досягається доволі високий рівень безпеки інформації. Одну частину вводить користувач, а друга розміщується на деякому носії, який встановлюється на спеціальний зчитувальний пристрій, пов'язаний з терміналом.

До програмних засобів забезпечення інформаційної безпеки засобів зв'язку в обчислювальних мережах відносяться:

– програмно-апаратні шифратори мережевого трафіку;

– встановлення екранів, Firewall, реалізованих на базі програмно-апаратних засобів;

– захищені мережеві крипто протоколи;

– програмні засоби виявлення атак;

– програмні засоби аналізу захищеності;

– захищені мережеві операційні системи (ОС).

Програмно-апаратні шифратори мережевого трафіку.

Програмно-апаратні шифратори мережевого трафіку використовуються для забезпечення безпеки під час передачі даних через мережі. Ці пристрої поєднують в собі як апаратне, так і програмне забезпечення для шифрування та дешифрування трафіку, що проходить через них. Ось деякі аспекти та типи програмно-апаратних шифраторів мережевого трафіку:

а) VPN-шифрування:

– віртуальні приватні мережі (VPN) використовують шифрування для забезпечення приватності та безпеки під час обміну даними між вузлами мережі;

– VPN-шифрування може бути реалізоване на різних рівнях мережі, таких як мережевий (IPsec), транспортний (TLS/SSL), або додатковий (прикладний) рівень;

б) шифрування на рівні транспортного рівня:

– протоколи, такі як TLS/SSL, можуть бути впроваджені на рівні транспортного рівня для шифрування комунікації між клієнтом і сервером;

в) мережеві апаратні шифратори:

– деякі мережеві пристрої, такі як маршрутизатори та файрволи, можуть бути з вбудованим апаратним шифрування для підтримки безпечного трафіку через мережу;

г) шифрування на рівні додатків:

– деякі додатки мають вбудовані механізми шифрування для забезпечення конфіденційності даних під час їх передачі через мережу;

д) шифрування цільових пристроїв:

– деякі пристрої, такі як мережеві переходники або точки доступу Wi-Fi, можуть підтримувати апаратне шифрування для захисту трафіку на місці його виникнення;

– деякі облачні сервіси, що надають послуги сховища або обчислень, можуть використовувати шифрування для захисту даних на рівні пристроїв у краудсервісі;

е) шифрування у рамках промислового Інтернету речей (IIoT):

– в сфері промислового Інтернету речей, де велика кількість пристроїв може бути підключена до мережі, використовуються апаратні засоби шифрування для захисту комунікації та даних.

Забезпечення ефективної безпеки мережі включає в себе використання програмно-апаратних рішень, які враховують конкретні потреби та загрози конкретної мережі чи організації.

Встановлення екранів, Firewall, реалізованих на базі програмно-апаратних засобів.

Встановлення екранів (firewall) на базі програмно-апаратних засобів є важливим етапом в забезпеченні безпеки мережі. Файервол використовується для контролю та фільтрації мережевого трафіку, забезпечуючи безпеку та захист мережевої інфраструктури. Такі файерволи можуть бути реалізовані на різних рівнях мережі – на рівні мережевого рівня (маршрутизатор), транспортного рівня (файерволи, які працюють з TCP/UDP) та додатковому рівні (файерволи застосунків).

Основні кроки для встановлення програмно-апаратного файерволу включають наступне:

а) вибір відповідного обладнання:

– визначається, чи буде використовуватися спеціалізовані файерволи, які поєднують в собі апаратні та програмні компоненти, чи буде використовуватися програмний файервол на загальній мережевій платформі;

б) встановлення та конфігурація обладнання:

– встановлювати обладнання в потрібних точках мережі (наприклад, перед входом у мережу з Інтернету);

– потрібно налаштувати базові настройки, такі як IP-адреса, доступ до консолі, інтерфейси тощо;

в) обрання стратегії захисту:

– визначається стратегія захисту, тобто які типи трафіку будуть блоковані чи дозволені, які порти чи протоколи будуть використовуватися;

г) налаштування правил доступу:

– створюються правила доступу, які визначають, який трафік дозволяється або блокується;

– додаються правила для контролю вхідного та вихідного трафіку, враховуючи безпекові політики тієї чи іншої банківської та фінансової установи чи організації;

д) включення додаткових функцій:

– деякі файерволи мають додаткові функції, такі як інспекція глибокого пакету, виявлення вторгнень, VPN-підтримка тощо, включають та налаштовують ці функції відповідно до обраного варіанта використання;

е) моніторинг та журналювання:

– налаштування моніторингу для відстеження активності файерволу та виявлення можливих атак чи порушень політик безпеки;

– включення системи журналювання для збереження записів про події та аудита активності;

і) тестування та апробація:

– перевіряється файервол, переконуються, що правила фільтрації працюють вірно та не блокують легітимний трафік;

– проводиться аудит безпеки для виявлення можливих слабких місць;

ї) оновлення та підтримка:

– періодично потрібно оновлювати програмне забезпечення та апаратне забезпечення файерволу, щоб уникнути використання вразливостей;

– забезпечується регулярне апаратне обслуговування та резервне копіювання налаштувань.

Процес встановлення та конфігурації може варіюватися в залежності від конкретних вирішень файерволів та вимог мережі.

Захищені мережеві крипто протоколи.

Захищені мережеві крипто протоколи відіграють ключову роль у забезпеченні конфіденційності, цілісності та автентифікації даних, які передаються через мережі. Ось кілька таких протоколів:

а) Transport Layer Security (TLS) / Secure Sockets Layer (SSL):

– TLS та його попередник SSL є протоколами шифрування, які забезпечують безпеку передачі даних через Інтернет;

– вони використовують криптографічні алгоритми для шифрування даних та встановлення захищеного з'єднання між клієнтом і сервером;

б) Internet Protocol Security (IPsec):

– IPsec надає безпеку на рівні мережі, забезпечуючи конфіденційність, цілісність та аутентифікацію даних на рівні IP-пакетів;

– використовується для захисту трафіку між мережевими пристроями, такими як маршрутизатори та віддалені користувачі;

в) Secure Shell (SSH):

– SSH надає захищений канал для командного доступу та передачі даних між двома пристроями;

– забезпечує шифрування, аутентифікацію та захист від атак на мережевий рівень;

г) Pretty Good Privacy (PGP) / GNU Privacy Guard (GPG):

– PGP та GPG є криптографічними протоколами для шифрування та підпису електронних повідомлень;

– застосовуються для забезпечення безпеки електронної пошти та файлів.

д) WireGuard:

– WireGuard – сучасний VPN-протокол, який забезпечує прозорість та ефективність захисту мережі;

– відомий своєю простотою та високою швидкістю;

е) OpenVPN:

– OpenVPN є популярним протоколом для настройки віртуальних приватних мереж (VPN);

– використовується для захисту з'єднань між віддаленими користувачами та корпоративною мережею;

і) S/MIME (Secure/Multipurpose Internet Mail Extensions):

– S/MIME використовується для шифрування та цифрового підпису електронної пошти;

– забезпечує конфіденційність та автентифікацію у електронній пошті.

Важливо враховувати, що безпека мережевих крипто протоколів вимагає постійного вдосконалення через розвиток крипто аналітичних методів та появи нових загроз. Також слід дотримуватися найкращих практик забезпечення, таких як вчасне оновлення протоколів та використання безпечних конфігурацій.

Програмні засоби виявлення атак.

Програмні засоби виявлення атак (Intrusion Detection Systems - IDS) використовуються для виявлення аномальної або підозрілої поведінки в мережі чи на окремих системах. Ці засоби відіграють важливу роль у забезпеченні безпеки інформаційних систем, дозволяючи вчасно реагувати на потенційні загрози. Існують дві основні категорії IDS: системи виявлення вторгнень (IDS) та системи виявлення аномалій (Anomaly Detection Systems –

ADS). Ось кілька програмних засобів виявлення атак, які представляють обидві категорії:

а) системи виявлення вторгнень (IDS):

– Snort – відкрите програмне забезпечення для систем виявлення вторгнень (NIDS).Використовує правила для виявлення підозрілого трафіку;

– Suricata – IDS та IPS, яке також використовує правила для виявлення та блокування атак;

– Bro (тепер Zeek) – платформа для аналізу мережевого трафіку, яка може виявляти атаки та аномальні звільнення;

– Security Onion – дистрибутив Linux, який включає Snort, Suricata, Bro та інші інструменти для виявлення та аналізу вторгнень;

– Ossec – IDS, який також може використовуватися для системи виявлення вторгнень і відгуку на інциденти (IDR);

б) системи виявлення аномалій (ADS):

– Splunk – платформа для аналізу та моніторингу даних, яка може використовуватися для виявлення аномалій;

– ELK Stack (Elasticsearch, Logstash, Kibana) – засоби аналізу та візуалізації даних, які можуть використовуватися для виявлення аномального трафіку;

– AlienVault OSSIM – відкритий засіб, який включає IDS (Snort), систему логування, аналітику та інші компоненти для виявлення атак та аномалій;

– Darktrace – платформа машинного навчання для виявлення аномалій в мережевому трафіку;

– Cisco Stealthwatch – продукт для моніторингу мережі та виявлення аномалій з використанням різноманітних методів аналізу.

Ці інструменти допомагають виявляти атаки, які можуть включати в себе вторгнення, аномалії в системному або мережевому трафіку, а також інші підозрілі активності. Важливо визначити, який інструмент або

комбінацію інструментів використовувати, враховуючи конкретні потреби та характеристики мережі.

Програмні засоби аналізу захищеності.

Програмні засоби аналізу захищеності допомагають організаціям визначати та виправляти вразливості, виявляти слабкі місця в інфраструктурі та забезпечувати високий рівень безпеки інформаційних систем. Ось деякі інструменти для аналізу захищеності:

– Nessus – є популярним інструментом для сканування вразливостей. Він дозволяє виявляти слабкі місця в мережі, опрацьовувати різноманітні конфігурації та встановлювати патчі для виявлених вразливостей;

– OpenVAS – відкрите програмне забезпечення для сканування вразливостей, яке надає набір інструментів для виявлення проблем безпеки в мережевій інфраструктурі;

– Nexpose (Rapid7) – це інструмент від компанії Rapid7, який дозволяє аналізувати захищеність інфраструктури та виявляти потенційні вразливості;

– Qualys – хмарний сервіс для сканування вразливостей та аналізу захищеності, який надає широкий спектр функцій для контролю безпеки;

– Wireshark – інструмент для аналізу мережевого трафіку. Він дозволяє перехоплювати та аналізувати пакети для виявлення аномалій та підозрілого трафіку;

– Burp Suite – це набір інструментів для тестування безпеки веб-застосунків. Він включає в себе функції сканування вразливостей, аналізу трафіку та інші корисні інструменти;

– Acunetix – інструмент для автоматизованого сканування вразливостей в веб-застосунках та сервісах;

– Snort – інструмент для виявлення вторгнень (IDS), який може використовуватися для аналізу мережевого трафіку та виявлення потенційно шкідливих дій;

– OWASP ZAP (Zed Attack Proxy) – це інструмент для тестування безпеки веб-застосунків, який може виявляти вразливості та допомагати виправляти їх;

– Metasploit – це потужний інструмент для тестування на проникнення, який може використовуватися для аналізу захищеності та виявлення слабких місць в системах.

Ці інструменти можуть бути використані окремо або в поєднанні для створення повноцінної стратегії тестування та аналізу захищеності. Важливо регулярно використовувати ці інструменти для моніторингу захищеності та реагування на зміни в оточенні безпеки.

Захищені мережеві операційні системи (ОС).

Захищені мережеві операційні системи (МОС) розроблені з урахуванням високих вимог щодо безпеки та захисту мережевих ресурсів. Ці ОС мають вбудовані заходи безпеки, які допомагають у зменшенні ризиків виникнення загроз та атак на мережу. Ось деякі приклади захищених мережевих операційних систем:

– SELinux (Security-Enhanced Linux) – це розширення ядра Linux, яке надає політику безпеки, забезпечуючи контроль доступу на рівні ядра;

– Trusted Solaris — операційна система від Oracle, що має захищені компоненти, такі як Trusted Extensions, які надають удосконалену безпеку та контроль доступу;

– Windows Server (Enterprise Editions) – Enterprise-версії операційних систем Windows Server (наприклад, Windows Server 2019) надають додаткові функції безпеки, такі як BitLocker для шифрування дискового простору та Active Directory для управління доступом;

– AIX (Advanced Interactive eXecutive) – операційна система від IBM, яка включає різноманітні заходи безпеки, такі як аудит безпеки та інші;

– OpenBSD – продовження операційної системи BSD, яка відома своїм фокусом на безпеку. Має вбудовані інструменти, такі як PF (Packet Filter), які використовуються для контролю мережевого трафіку;

– Cisco IOS (Internetwork Operating System) — операційна система для мережевого обладнання Cisco, що має вбудовані засоби безпеки для мережевих пристроїв;

– Junos (Juniper Networks) – операційна система для маршрутизаторів та комутаторів Juniper Networks, яка надає безпеку на рівні мережі та системи;

– Qubes OS – операційна система, яка використовує віртуалізацію для ізоляції різних частин системи та має вбудовані заходи для забезпечення безпеки.

Ці операційні системи відомі своєю здатністю до захисту від різноманітних загроз та використовують різноманітні техніки безпеки, такі як шифрування, контроль доступу, аудит безпеки та вбудовані механізми виявлення та відгуку на інциденти. Важливо враховувати, що безпека системи – це комплексний процес, і необхідно дотримуватися найкращих практик безпеки та регулярно оновлювати системи для захисту від нових загроз.

Антивірусний захист важливої інформації.

Антивірусний захист важливої інформації в банківській та фінансовій установі є критичним елементом забезпечення інформаційної безпеки. Шкідливе програмне забезпечення може завдати шкоди важливій інформації, наприклад, шляхом її знищення, модифікації або розголошення.

Банки та фінансові установи використовують антивірусні програми для виявлення та видалення шкідливого програмного забезпечення.

Антивірусні програми працюють, аналізуючи файли та код на наявність ознак шкідливого програмного забезпечення.

Існує два основних типи антивірусних програм:

– програми сигнатурного виявлення використовують бази даних відомих шкідливих програм для виявлення шкідливого програмного забезпечення;

– програми поведінкового виявлення аналізують поведінку програм для виявлення шкідливого програмного забезпечення.

Банки та фінансові установи часто використовують комбінацію цих двох типів антивірусних програм для забезпечення максимальної безпеки. Антивірусний захист банківської та фінансової інформаційної системи будують за принципом ієрархії:

– корпоративний рівень;

– підрозділи або філії;

– кінцеві користувачі.

Служби всіх рівнів об’єднують в єдину мережу, чим утворюють єдину інфраструктуру за допомогою локальної обчислювальної мережі. Причому служби загально – корпоративного рівня повинні працювати в постійному режимі на безперервній основі .

Для управління і синхронізації взаємодії всіх рівнів, яке повинно здійснюється спеціальним персоналом, повинно бути передбачено засоби централізованого адміністрування.

Антивірусна система, яка буде відповідати всім вимогам безпеки, повинна надавати такі види сервісів на загально-корпоративному рівні:

– можливість отримувати оновлення ПЗ та антивірусних баз;

– своєчасне оновлення антивірусних баз;

– мати контроль за роботою системи в цілому (одержувати попередження про виявлення вірусу, формування комплексних звітів про роботу системи в цілому).

На рівні підрозділів – це проведення оновлення антивірусних баз для кінцевих користувачів, антивірусного ПЗ кінцевих користувачів, а також можливість управління локальними групами користувачів.

На рівні кінцевих користувачів – антивірусний захист даних користувача в автоматичному режимі.

Антивірусний захист повинен підтримувати такі функції:

– віддаленого управління;

– ведення журналів;

– сповіщення.

Важливим є можливість регулювати рівень навантаження від антивірусного забезпечення. Потрібно забезпечити можливість виявлення вірусів виконуваних файлів, макросів документів. Повинні бути передбачені механізми виявлення невідомого програмного забезпечення вірусів, постійний захист робочих станцій, який забезпечує перевірку файлів при їх відкритті і запису на зовнішній носій. Антивірусні бази повинні оновлюватися в автоматичному режимі.

Системи антивірусного захисту, їхні програмно – технічні компоненти повинні задовольняти наступним загальним принципам створення автоматизованих систем:

– надійність, повинна функціонувати в цілому, навіть при відмові функціонування окремих вузлів, мати засоби відновлення після відмови;

– масштабованість, антивірусний захист потрібно формувати із урахуванням збільшення числа об’єктів для захисту;

– відкритість, систему потрібно формувати, враховуючи можливість поповнення і оновлення її складу, не порушуючи при цьому функціонування обчислювального середовища в цілому;

– сумісність – повинна бути можливість підтримки антивірусним програмним забезпеченням максимальної кількості мережевих ресурсів. У

структурі та функціональних особливостях компонент повинні бути представлені засоби взаємодії з іншими системами;

– уніфікованість (однорідність) – всі складові антивірусного забезпечення повинні представляти собою стандартні системи та засоби, які мають широку сферу застосування й перевірені на практиці.

Всі компоненти банківської інформаційної системи, які пов’язані з транспортуванням інформації та/або її зберіганням: файл-сервери; робочі станції; робочі станції мобільних користувачів; сервера резервного копіювання; сервера електронної пошти повинні підлягати антивірусному захисту. Системними адміністраторами використовуються цілі комплекси програмного захисту від вірусів. Такими є програми – ревізори, фільтри.

Програми – ревізори вважаються одними з найнадійніших із засобів для захисту від вірусів. Вони запам’ятовують стан програм, каталогів і системних областей диска до зараження комп'ютера вірусом, а потім через певні проміжки часу або за бажанням користувача звіряють поточний стан з початковим.

Коли відбувається порівняння, то перевіряються довжина файлу, контрольна сума, дата і час модифікації і інші додаткові параметри. Ці програми мають досить розвинені алгоритми, вони виявляють stealth-віруси і можуть навіть очистити програми, що перевіряються, від змін, внесених вірусом. До програм-ревізорів належать широко поширені в Україні програми Adinf від «Діалогнаука» або WinsonarXP. Недоліком є те, що вони дуже сильно гальмують роботу комп’ютера.

Програми-фільтри представляють із себе невеликі резидентні програмами, вони виявляють підозрілі дії при роботі комп’ютера, що характерні для вірусів. Це спроби корекції файлів які мають розширення com, exe, зміна атрибутів файлу, прямий запис на диск за абсолютною адресою, запис в завантажувальні сектори диска, завантаження резидентної програми. Якщо якась програма проведе спроби провести вказані вище дії, то така програма надсилає користувачеві повідомлення, забороняє або робить

відповідну дію. Користь таких програм у здатності виявити вірус на найпершій стадії його існування і до розмноження. Прикладом програми-фільтру є програма Vsafe.

Proxy-сервери з ідентифікацією та аутентифікації, корпоративні мережі з "віртуальними" IP-адресами для захисту даних.

Proxy-сервери з ідентифікацією та аутентифікації.

Proxy-сервер – це сервер, який виступає посередником між клієнтом і сервером. Proxy-сервери використовуються для різних цілей, зокрема для захисту конфіденційності даних.

Proxy-сервери з ідентифікацією та аутентифікацією дозволяють контролювати доступ до певних ресурсів. Для цього користувач повинен пройти процес ідентифікації та аутентифікації, перш ніж йому буде дозволено отримати доступ до ресурсу.

У банківській та фінансовій сфері proxy-сервери з ідентифікацією та аутентифікацією можуть використовуватися для захисту таких ресурсів, як:

- сервери банківських систем;
- сервери клієнтських додатків;
- сервери баз даних;
- сервери електронної пошти.

Корпоративні мережі з "віртуальними" IP-адресами.

Корпоративні мережі з "віртуальними" IP-адресами використовують технологію NAT (Network Address Translation). NAT дозволяє використовувати один зовнішній IP-адресу для декількох внутрішніх IP-адрес.

Використання "віртуальних" IP-адрес у корпоративних мережах дозволяє підвищити безпеку даних. Це пов'язано з тим, що зовнішній IP-адрес не пов'язаний з конкретним внутрішнім комп'ютером. Таким чином, навіть якщо зловмисник отримає доступ до зовнішнього IP-адреси, він не зможе визначити, який внутрішній комп'ютер є джерелом атаки.

Обидва ці заходи дозволяють підвищити безпеку даних у банківській та фінансовій сфері.

Proxy-сервери з ідентифікацією та аутентифікацією дозволяють контролювати доступ до певних ресурсів. Це допомагає запобігти несанкціонованому доступу до конфіденційної інформації.

Корпоративні мережі з "віртуальними" IP-адресами допомагають приховати внутрішні IP-адреси комп'ютерів у мережі. Це ускладнює для зловмисників визначення джерела атаки.

Загалом, використання proxy-серверів з ідентифікацією та аутентифікації та корпоративних мереж з "віртуальними" IP-адресами є ефективним способом захисту даних у банківській та фінансовій сфері.

2.4 Криптографічний захист інформації

2.4.1 Криптографічні алгоритми.

Головною метою шифрування інформації є її захист від будь-якого несанкціонованого або неправомірного доступу.

В основі шифрування знаходяться два елементи – це криптографічний алгоритм і ключ.

Криптографічним алгоритмом є математична функція, що з’єднує текст або будь-яку іншу зрозумілу інформацію з числовим ланцюжком, який є ключем з метою отримання тексту, що стає шифрованим.

Спеціальні крипто алгоритми мають таємний алгоритм шифрування, а загальні крипто алгоритми є відкритими, а так звана крипто стійкість в свою чергу, визначається ключами шифрування. Спеціальні алгоритми часто використовуються в апаратних засобах крипто захисту.

Найчастіше загальні криптографічні алгоритми стають стандартами шифрування, якщо їх висока крипто стійкість доведена. Вони

оприлюднюються для обговорення, а також визначають премію за успішну спробу його зламати.

Криптографічні алгоритми поділяють на симетричні і асиметричні.

Симетричні криптографічні алгоритми – це такі алгоритми, у яких шифрування і розшифрування виконується однаковим ключем. Відправник і отримувач повідомлення користуються одним і тим самим ключем. Дані алгоритми відрізняються достатньо великою швидкість обробки як для апаратної, так і для програмної реалізації. Недоліком симетричних алгоритмів є труднощі, які пов'язані з безпечним розподілом ключів між обома абонентами.

Щодо асиметричних криптографічних алгоритмів, то шифрування і розшифрування виконується за допомогою різних ключів. Власник одного із ключів не зможе визначити парний для нього ключ. Ці алгоритми потребують набагато більше часу для їхнього обчислення, але при цьому, не має труднощів з розподілом ключів, тому що розподіл одного з ключів у відкритому доступі не зменшує крипто стійкості даного алгоритму і не дасть можливості відновлення парного йому ключа.

Насьогодні існує багато криптографічних алгоритмів.

Найпоширеннішими є стандарт шифрування даних DES (Data Encryption Standart), алгоритм RSA, названий за першими літерами прізвищ його розробників (Rivest, Shamir, Adleman),які розроблені у 1970-х роках. Ці два алгоритми є державними стандартами США. DES – це симетричний алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів напряму залежить від довжини ключа, який застосовується.

Ще одним алгоритмом, що широко застосовується, зокрема, в банківській системі, є алгоритм Діффі-Геллмана.

Алгоритм Діффі-Геллмана (Diffie–Hellman key exchange (D–H)) – є методом обміну криптографічними ключами. Цей алгоритм є одним із перших прикладів практичної реалізації з обміну ключами, який дозволяє

двом учасникам, які не мають ніяких попередніх даних один про одного, можливість отримувати спільний секретний ключ, використовуючи незахищені канали зв’язку.

Протокол Діффі-Геллмана являє собою анонімний протокол встановлення ключа, і не використовує автентифікацію, але в той же час він забезпечує базу для різних протоколів, які використовують автентифікацію.

Алгоритм DSA (Digital Signature Algorithm) – криптографічний алгоритм який використовує відкритий ключ щоб створювати електронний підпис, але не для шифрування. Підпис створюється таємно, але перевіряється публічно. Тільки один суб’єкт створює підпис повідомлення, але будь-хто може перевірити його коректність.

Алгоритм Advanced Encryption Standard (AES) – є симетричним алгоритмом блочного шифрування (розміри блока 128 біт, ключа 128/192/256 біт), прийнятий як американський стандарт шифрування урядом США.

2.4.2 Електронний цифровий підпис

При використанні асиметричних криптографічних алгоритмів формується додаткова інформацію, яка називається електронним цифровим підписом.

Електронний цифровий підпис (ЕЦП) – це криптографічний метод, який використовується для підтвердження автентичності та цілісності електронних документів. ЕЦП дозволяє відправнику електронного документа довести, що він є тим, за кого він видає себе, і що документ не був змінений з моменту його підписання. Накладання ЕЦП відбувається за допомогою особистого ключа, в той час як перевірка – за допомогою відкритого ключа.

При підписанні електронного документу не відбувається зміна його початкового змісту, просто до нього додається блок даних, він і є

електронним цифровим підписом. Отримання цього блоку розділяють на два етапи.

Перший етапі це – обчислення за допомогою програмного забезпечення і спеціальної математичної функції так званого «відбитку повідомлення» (message digest), який має такі особливості:

– фіксована довжина, у незалежності від довжини повідомлення;

– унікальність відбитку для кожного повідомлення;

– унеможливлена будь-яка можливість відновлення повідомлення по його відбитку.

Тому, будь-яка модифікація документа призведе до зміни і його відбитка, а це в свою чергу відобразиться при перевірці Електронного цифрового підпису.

Другий етап – відбиток документу шифрують за допомогою програмного забезпечення і особистого ключа автора.

Розшифровка ЕЦП і одержання початкового відбитка, який би відповідав документу, можлива тільки з використанням Сертифіката відкритого ключа автора.

Перевірка Електронного цифрового підпису (рис. 2.1) отриманого документу проводиться у декілька етапів:

– отримавши повідомлення, використовуючи програмне забезпечення, а також використовуючи сертифікат відкритого ключа автора розшифровується підписаний відбиток і одержується відбиток початкового документа;

– за допомогою спеціальної математичної функції, використовуючи програмне забезпечення, обчислюється його відбиток;

– перевіряється ЕЦП порівнюють відбитки початкового документа і того, який отримано. Результатом перевірки буде одна з відповідей: «вірний»/«невірний».

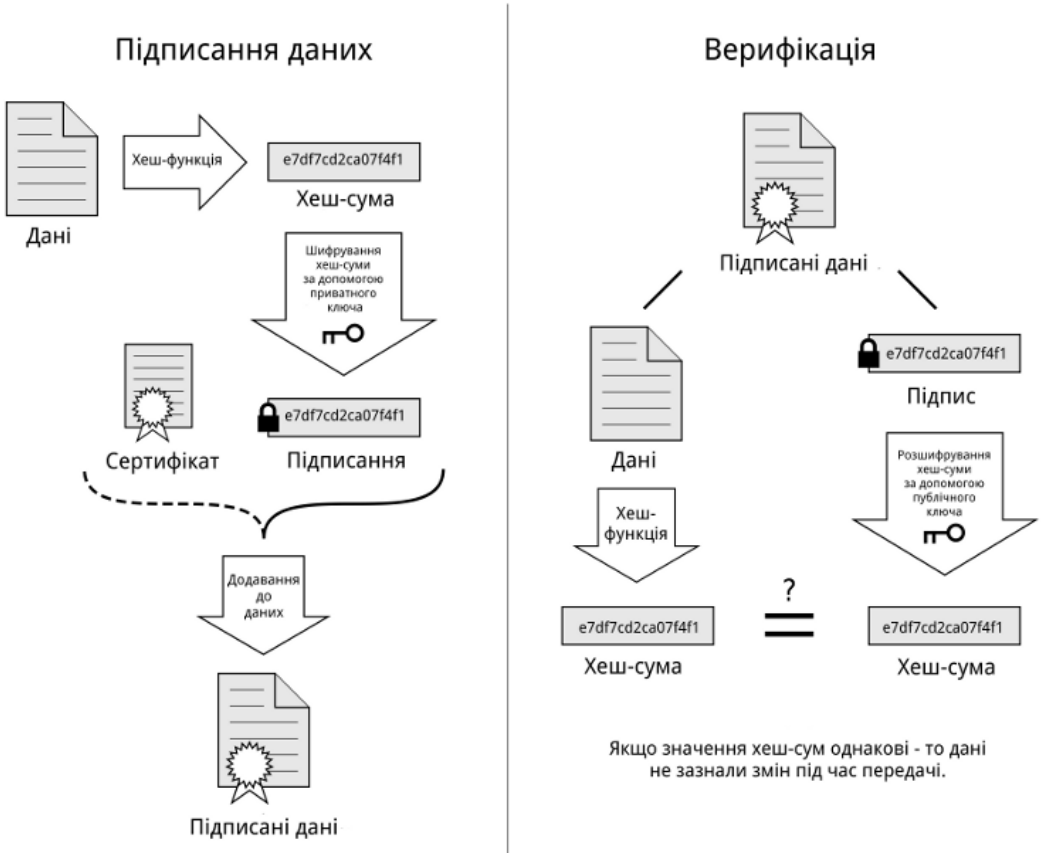

Рисунок 2.1 – Електронний цифровий підпис

2.4.3 Методи розподілу ключів

Від того наскільки безпечно проводиться розподіл ключів, залежить ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів.

Метод базових/сеансових ключів.

Цей метод описаний у стандарті ISO 8532, він застосовується для розподілу ключів симетричних алгоритмів шифрування. Це криптографічний метод, який використовується для забезпечення конфіденційності та цілісності даних, що передаються в мережі. Метод складається з двох етапів:

– обмін базовими ключами: на першому етапі відправник і одержувач обмінюються базовими ключами. Базові ключі – це довгі, стійкі до злому ключі, які зберігаються в секреті;

– шифрування даних сеансовим ключем: на другому етапі відправник використовує базовий ключ для шифрування сеансового ключа. Сеансовий ключ – це короткий, одноразовий ключ, який використовується для шифрування даних, що передаються.

Далі відправник використовує сеансовий ключ для шифрування даних, що передаються. Одержувач може розшифрувати дані, використовуючи базовий ключ, який він отримав від відправника.

Метод базових/сеансових ключів безпечний, тому що базові ключі зберігаються в секреті. Крім того, сеансові ключі є одноразовими, тому вони не можуть бути використані для злому даних, що передаються.

Метод базових/сеансових ключів використовується в різних сферах, включаючи:

– електронна комерція: метод використовується для захисту електронних платежів та інших чутливих даних, що передаються в Інтернеті;

– безпека мереж: метод використовується для захисту даних, що передаються в захищених мережах, таких як корпоративні мережі та військові мережі;

– шифрування електронної пошти: метод використовується для захисту електронної пошти від несанкціонованого доступу.

Метод базових/сеансових ключів є ефективним способом забезпечення конфіденційності та цілісності даних, що передаються в мережі.

Застосування такої схеми розподілу ключів потребує значного часу і значних витрат.

Метод відкритих ключів.

Даний метод описано у стандарті ISO 11166, він застосовується для розподілу ключів як для симетричного, так і для асиметричного шифрування.

Це криптографічний метод, який використовується для забезпечення конфіденційності, цілісності та автентичності даних. Метод заснований на використанні двох ключів: відкритого та закритого.

Відкритий ключ – це ключ, який може бути опублікований для всіх. Він використовується для шифрування даних, які можна розшифрувати лише за допомогою закритого ключа.

Закритий ключ – це ключ, який зберігається в секреті. Він використовується для розшифровування даних, які були зашифровані за допомогою відкритого ключа.

Метод відкритих ключів використовується для таких цілей:

– шифрування даних: метод використовується для шифрування даних, які потрібно захистити від несанкціонованого доступу;

– електронний цифровий підпис: метод використовується для створення електронних цифрових підписів, які дозволяють підтвердити автентичність та цілісність електронних документів;

– шифрування електронної пошти: метод використовується для шифрування електронної пошти від несанкціонованого доступу.

Метод відкритих ключів є ефективним способом забезпечення конфіденційності, цілісності та автентичності даних.

Переваги методу відкритих ключів:

– безпека: метод відкритих ключів є безпечним, тому що відкритий ключ не може бути використаний для розшифровування даних без закритого ключа;

– ефективність: метод відкритих ключів є ефективним, тому що він дозволяє шифрувати та розшифровувати дані швидко та легко;

– мобільність: метод відкритих ключів є мобільним, тому його можна використовувати в різних мережах і середовищах.

Недоліки методу відкритих ключів:

– вартість: впровадження методу відкритих ключів може бути дорогим;

– складність: метод відкритих ключів може бути складним для розуміння та використання.

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Забезпечити «абсолютний» захист інформації не гарантує жоден із цих методів, але при цьому, витрати «злому» у кілька разів перевищать вартість тієї інформації, яка зашифрована, що особливо важливо для банківського та фінансового сектору.

Для використання системи криптографії з відкритим ключем, потрібно згенерувати відкритий і особистий ключі. Після цього слід розповсюдити відкритий ключ. Найбільш надійним способом розповсюдження відкритих ключів є сертифікаційні центри, які призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат є підтвердженням справжності особи користувача, він також містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.

Сертифікаційні центри відповідають за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності.

2.4.4 Стандарти цифрового підпису

Стандарт цифрового підпису ECDSA над простим полем.

Алгоритм ECDSA є одним із національних стандартів електронного цифрового підпису. Цифровий підпис створюється за допомогою операцій над точками еліптичної кривої після хешування повідомлення. В якості хеш-

функції використовуються алгоритми класу SHA (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512), наприклад, SHA-1, хеш-образ якого дорівнює 160 біт.

Відкритими параметрами алгоритму є еліптична крива, базова точка кривої P з відомим простим порядком n. Відкритим ключем підписувача є точка еліптичної кривої Q, $Q = d \cdot P$, його секретним ключем є число d. Для забезпечення криптостійкості цифрового підпису порядок базової точки має бути досить великим: $2^{160} < n < 2^{511}$ або $n > 2^{512}$.

Цифровий підпис формується абонентом А за допомогою його секретного ключа, перевірка підпису здійснюється абонентом В з використанням відкритого ключа абонента А.

Загальносистемні параметри:

Еліптична крива над простим полем $GF(p)$

$y^2 = x^3 + ax + b \bmod p$;

P – базова точка кривої з великим простим порядком n.

Генерація ключів:

- генерується секретний та відкритий ключі абонента А;
- обирається випадкове число d, $2 \le d \le n - 2$;
- секретним ключем абонента А є число d;
- відкритим ключем абонента А є точка кривої $Q = d \cdot P$.

Формування цифрового підпису. Підписувач А обчислює хеш-образ повідомлення M за допомогою хеш-функції SHA. Отримане двійкове число $H(M)$ конвертується в десяткове число H. Потім обчислюється значення $h = H \bmod n$.

Нехай хеш-образу повідомлення M відповідає число h.

Оберемо випадкове число k, $2 \le k \le n - 2$.

Обчислимо точку $C = k \cdot P = (x_C, y_C)$ та число $r = x_C \bmod n$. (Число r не повинно бути 0.)

З використанням секретного ключа d та хеш-образу повідомлення h обчислимо значення s із співвідношення $s \cdot k = h + d \cdot r \bmod n$. (Число s не повинно бути 0.)

Цифровим підписом є пара чисел $\langle r, s \rangle$.

Підписане повідомлення має вигляд $\{M,\ \langle r, s \rangle,\ \text{текст}\}$. Поле «текст» є довільним, може містити ідентифікатори підписувача, або помітку часу, наприклад.

Перевірка цифрового підпису.

Для перевірки підписаного абонентом А повідомлення $\{M,\ \langle r, s \rangle,\ \text{текст}\}$ використовуються хеш-образ повідомлення M, відкриті загальносистемні параметри алгоритму ECDSA та відкритий ключ підписувача, тобто еліптична крива, базова точка P, її порядок n, десяткове число h, що відповідає хеш-образу повідомлення M, відкритий ключ абонента А – точка кривої Q.

Обчислимо два параметри

$u = \frac{h}{s} \bmod n$ та $v = \frac{r}{s} \bmod n$.

Знайдемо точку еліптичної кривої $u \cdot P + v \cdot Q = (x_0, y_0)$.

Параметр $r' = x_0 \bmod n$ повинен співпадати з параметром r.

Якщо $r' = r$, підпис признається справжнім.

Приклад.

Нехай відкритими параметрами алгоритму ECDSA є еліптична крива $y^2 = x^3 + 15x + 24 \bmod 43$, базова точка кривої $P = (0,14)$, порядок точки $n = 41$.

Для генерування асиметричної пари ключів абонента А оберемо випадкове число $d = 5$ та обчислимо точку $Q = 5 \cdot P = (3,15)$.

Відкритим ключем абонента А є точка кривої $Q = (3,15)$.

Секретним ключем абонента А є число $d = 5$.

Для формування підпису абонент А хешує повідомлення M та отримує відповідне десяткове число $h = 4$.

Далі абонент А обирає випадкове число $k = 2$ та обчислює точку $C = 2 \cdot P = (1,30)$. Звідси число $r = 1 \bmod 41 = 1$.

З використанням секретного ключа d та числа h абонент А обчислює параметр s: $s \cdot 2 = 4 + 5 \cdot 1 \bmod 41 = 9 = -32$. Звідси $s = -16 \bmod 41 = 25$.

Цифровим підписом є пара чисел $\langle 1,25 \rangle$.

Підписане повідомлення має вигляд $\{M,\ \langle 1,25 \rangle,\ \text{текст}\}$.

Для перевірки підписаного абонентом А повідомлення $\{M,\ \langle r,s \rangle,\ \text{текст}\}$ використовуються хеш-образ повідомлення M, відкрити загальносистемні параметри алгоритму ECDSA та відкритий ключ підписувача, тобто еліптична крива, базова точка $P = (0,14)$, її порядок $n = 41$, десяткове число $h = 4$, що відповідає хеш-образу повідомлення M, відкритий ключ абонента А – точка кривої $Q = (3,15)$.

Обчислимо значення $u = \frac{4}{25} \bmod 41 = \frac{4}{-16} = \frac{-1}{4} = 10$ і $v = \frac{1}{25} \bmod 41 = \frac{-40}{25} = \frac{-8}{5} = \frac{-90}{5} = -18 = 23$.

Знайдемо точку еліптичної кривої $10 \cdot P + 23 \cdot Q = (1,30)$ та параметр $r' = 1 \bmod 41 = 1$.

Оскільки $r' = r$, підпис визнається справжнім.

Український стандарт цифрового підпису ДСТУ 4145-2002.

Загальносистемні параметри:

Еліптична крива над розширеним полем $GF(2^m)$

$y^2 + xy = x^3 + ax^2 + b$;

де $a, b \in GF(2^m)$, $b \neq 0$, $a \in \{0,1\}$, $f(t)$ – незвідний многочлен степеню m; базова точка еліптичної кривої $P \neq O$ великого простого порядку n, $|n|$ – число двійкових розрядів в n; H – функція хешування ДСТУ 7564:2014 (або SHA-256).

Генерація ключів:

– згенеруємо секретний та відкритий ключі абонента А;

– оберемо випадкове число d, $2 \le d \le n-2$;

– обчислимо точку $Q = d \cdot P$;

– секретним ключем абонента А є число d;

– відкритим ключем абонента А є точка кривої Q.

Формування цифрового підпису. Підписувач А обчислює хеш-образ повідомлення M за допомогою обраної хеш-функції. Отримане двійкове число $H(M)$ конвертується в елемент поля $h \in GF(2^m)$. Для цього використовують m молодших бітів $H(M)$.

Оберемо випадкове число k, $1 < k \le n-1$.

Обчислимо точку $R = k \cdot P = (x_R, y_R)$ та елемент поля $y = h \cdot x_R \bmod f(t)$.

Молодші $|n|-1$ розряди елемента поля y формують десяткове число r. Число r не повинно бути 0.

З використанням секретного ключа d та хеш-образу повідомлення h обчислимо значення $s = k + d \cdot r \bmod n$. Число s не повинно бути 0.

Цифровим підписом є пара чисел $\langle r, s \rangle$.

Перевірка цифрового підпису.

Для перевірки підписаного абонентом А повідомлення $\{M, \langle r, s \rangle\}$ використовуються хеш-образ повідомлення M, відкриті загальносистемні параметри алгоритму ДСТУ 4145-2002 та відкритий ключ підписувача, тобто еліптична крива, базова точка P, її порядок n, елемент поля h, що відповідає хеш-образу повідомлення M, відкритий ключ абонента А – точка кривої Q.

Абонент В обчислює точку еліптичної кривої $s \cdot P + r \cdot Q = (x_0, y_0)$ та елемент поля $y = h \cdot x_0 \bmod f(t)$. Молодші $|n|-1$ розряди елемента поля y формують десяткове число r'.

Параметр r' повинен співпадати з параметром r.

Якщо $r' = r$, підпис визнається справжнім.

Висновки до розділу 2.

В даному розділі дипломної роботи було викладено методи захисту в банківських та фінансових установах. Розглянуто и охарактеризовано захист комп'ютерної мережі, технічний захист конфіденційної інформації, програмний захист, у тому числі захист від вірусної небезпеки, криптографічний захист інформації.

Оскільки діяльність і процвітання будь-якого банку, фінансової установи залежить безпосередньо від швидкості з якою здійснюється обмін інформації в середині банку або фінансової установи і на скільки добре побудована система безпеки. Сучасний захист інформації банківської та фінансової структури передбачає постійне вдосконалення системи у відповідності до зростання ризиків витоку, пошкодження та знищення інформації і реалізується такими методами:

– криптографічний захист конфіденційності при передачі інформації;

– управління інформаційними потоками, як у локальній мережі, так і при передачі каналами зв'язку на різні відстані;

– застосування механізмів обліку спроб доступу ззовні, подій у інформаційній системі та документів, що друкуються;

– забезпечення цілісності програмного забезпечення та інформації;

– здійснення фізичної охорони і обліку техніки та носіїв;

– створення спеціальних служб інформаційної безпеки.

Захист інформації у сучасних умовах потребує впровадження в систему безпеки наступних інструментів захисту:

– фізична перешкода;

– управління доступом;

– механізми шифрування;

– протидія атакам шкідливих програм і вірусів;

– апаратні засоби захисту;

– фізичні засоби захисту;

– програмні засоби захисту.

3 ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В БАНКІВСЬКИХ ТА ФІНАНСОВИХ УСТАНОВАХ

3.1 Кіберзахист банківської системи України в сучасних умовах цифрових трансформацій.

Як зазначалось раніше, фінансові установи та уся інфраструктура фінансового ринку піддаються кібератакам найбільше. Фінансові установи, зокрема банки, стають все більш привабливою мішенню для кіберзлочинців, зокрема тому що фінансовий сектор приваблює великих інвесторів, виділяючи значні фінансові ресурси.

На фоні повномасштабного вторгнення в Україні кібератаки стали невід'ємною складовою гібридної війни. Кіберзлочинці у свій час опановують все нові методи кібератак. А саме тому першочерговим завданням регуляторів є збереження системності у протидії кібератакам, а самому банківському та фінансовому секторам – інвестувати в кібербезпеку.

За даними НБУ, майже всі кібератаки на банківський і фінансовий сектор здійснювались хакерськими угруповуваннями, за якими стояла країна агресора. Це такі групи хакерів як Armageddon, Fancy Bears та інші. Наразі усі кібернапади, які проводилися кіберзлочинцями країни агресора зводились до двох напрямків: DDoS-атаки різного характеру, від яких страждає вся банківська система, та фішингові атаки різних типів (різні види шахрайства). Майже усі фішингові атаки, які спрямовані на банківську систему, є виманюванням коштів у клієнтів банків за різними схемами надання допомоги. Злочинці використовують найпростішу соціальну інженерію, різноманітні методи створення фейкових мобільних додатків та сторінок банків, де використовують айдентику справжніх банків.

На теперішній час ключовими трендами банківської цифровізації є:

– широке застосування і оптимізація віддаленої роботи працівників;

– значне зростання операцій онлайн;

– спрощення доступу до послуг банку;

– значний розвиток каналів дистанційного продажу;

– широке застосування технологій штучного інтелекту;

– перехід до управління на основі даних;

– програми тотальної персоніфікації;

– імпортозаміщення;

– розробка власного програмного забезпечення та зростання потреби в ІТ-фахівцях.

За даними звіту про фінансову стабільність за червень 2023 року від НБУ з початку 2022 року найбільш поширеним залишаються DDoS атаки, однак значну загрозу становлять і атаки на інформаційну інфраструктуру, зокрема за допомогою шкідливого програмного забезпечення.. Також новими цілями кіберзлочинців стають небанківські установи та розробники програмного забезпечення для банків та фінансових установ. Збої в роботі енергосистем призводять до затримок у роботі сервісів. Так клієнти можуть тимчасово втратити можливість користуватися онлайн-застосунками, здійснювати операції з картками чи знімати готівку в банкоматах.

За даними редакційних матеріалів журналу Forbes, які посилаються на прес-службу Державної служби спецзв'язку, у 2022 році кількість кіберінцидентів протягом 2022 року в Україні сталося майже втричі більше ніж у 2021 році. Протягом 2022 року Україна стикнулася з 7000 кібератак на інформаційну інфраструктуру. З 24 лютого і до кінці 2022 року урядова команда реагування на комп'ютерні надзвичайні події CERT-UA опрацювала 2194 кіберінціденти. З них 120 стосувалися фінансового сектору, 156 – комерційних організацій та 92 – сектору телекомунікацій і розробки програмного забезпечення. За перший квартал 2023 року фахівці CERT-UA

опрацювали 549 кібератак, серед яких 13 – на фінансовий сектор, 23 – на комерційний сектор і 11 – на розробників програмного забезпечення.

Цьогоріч, крім банків, кіберзлочинці атакують страхові компанії і розробників програмного забезпечення для банків, кажуть у НБУ. Також дуже високоефективними є кібератаки, спрямовані на викрадення коштів.

У Держспецзв'язку припускають, що збільшення фішингових атак та компрометації акаунтів, спрямованих на банківську і фінансову систему України, можуть свідчити про те, що росіяни планують зламати ресурси комерційних організацій та атакувати їх, щоб викрасти гроші і тим самим послабити їхній потенціал.

3.2 Порівняння практик та стратегій кібербезпеки в Україні з іншими країнами.

У публікації, підготовленій Офісом парламентської реформи в рамках проекту ЄС-ПРООН з парламентської реформи, зазначено, що за даними 2019 року за індексом NCSI, який являє собою глобальний індекс, який вимірює готовність країн до запобігання кіберзагрозам та управління кіберінцидентами, Україна посіла за рейтингом – 28 місце (2020 року – 26 місце, а у 2022 року – вже 25 місце). При цьому, країни, представлені в огляді, посідають такі місця за індексом NCSI: Естонія – 3 місце, Литва – 4 місце, Іспанія – 5 місце, Нідерланди – 10 місце, Сполучені Штати Америки – 14 місце, Велика Британія – 15 місце. NCSI – це також база даних із загальнодоступними матеріалами та інструментарієм для розбудови потенціалу національної кібербеспеки.

Міжнародний союз електрозв'язку розробив Глобальний індекс кібербезпеки – GCI (рис. 3.1). Рівень розвитку кожної країни аналізується за п'ятьма категоріями: правові заходи (рівень розробленості законодавчої бази

у сфері кібербезпеки), технічні заходи (рівень технічних можливостей кіберзахисту), організаційні заходи (національні стратегії кібербезпеки), розбудова потенціалу (інформаційне забезпечення, освіта та наявні стимули для розвитку потенціалу кибербезпеки) та співробітництво (рівень розвитку партнерства у сфері кібербезпеки).

За цим рейтингом у 2018 році США зайняли – 2 місце, Литва – 4 місце, Естонія – 5 місце, Іспанія – 7 місце, Нідерланди – 12 місце, Ізраїль – 39 місце. Для порівняння, Україна посіла у рейтингу GCI 2018 року 54 місце, а у 2021 році – 78 місце, втративши 24 позиції.

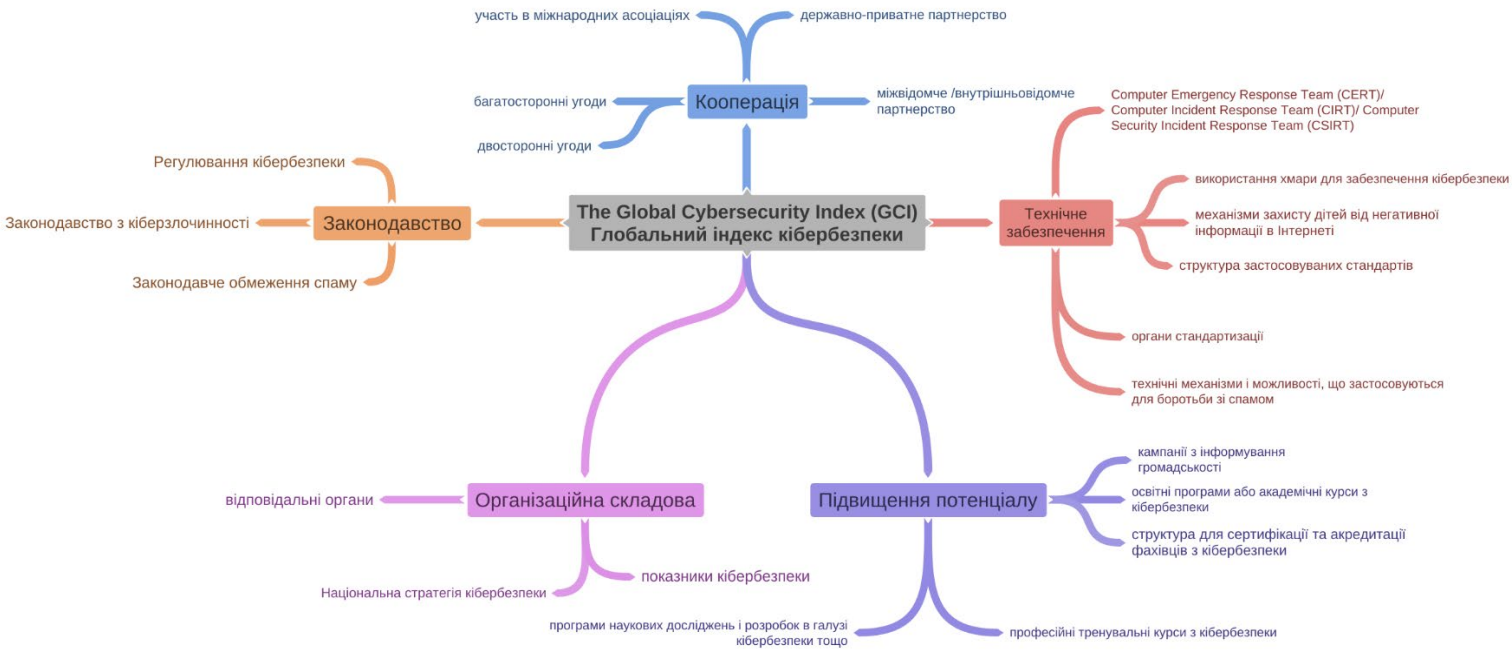

Рисунок 3.1 – Глобальний індекс кібербезпеки

З аналізу, зробленому Офісом парламентської реформи в рамках проекту ЄС-ПРООН з парламентської реформи, можна зробити деякі висновки. Так, країни з системами прецедентного права, а саме Велика Британія та США, використовують ризик – орієнтований підхід і на підставі оцінки ризиків та загроз готують стратегічні документи, плани їх реалізації, уточнюють повноваження інституцій відповідно до тих завдань, які ставить

національна стратегія. Ще одна особливість – відсутність на перших етапах регулювання окремого закону про кібербезпеку. Велика роль відводиться самим суб'єктам кібербезпеки, їх свідомому підходу, а також системі стандартизації. Найбільше від решти відрізняється підхід до кібербезпеки, який застосовується в Ізраїлі. Ізраїль постійно перебуває у ворожому середовищі, країна має високий відсоток виробництва високотехнологічної продукції, а це в свою чергу залежить від сталості цифрових послуг. Також експортується програмне забезпечення, тому вважається забезпечення кібербезпеки одним із завдань оборони країни. Ізраїль використовує мілітаризований підхід і досить обмежено інформує про заходи, що будуть вживатися. Окрім того, Ізраїль активно залучає науковий потенціал і широко співпрацює з бізнесом. При цьому залученість громадськості до формування політики кібербезпеки досить низька. Величезна роль відводиться державно – приватному партнерству у форматі наукових парків. Вони у свою чергу виробляють політику, заходи і також здійснюють аналіз ризиків.

Близькими до України за організацією управління кібербезпекою є країни колишнього СРСР (Литва, Естонія), які ухвалили відповідні закони про кібербезпеку, чітко визначили повноваження основних суб'єктів кібербезпеки та встановили відповідальність за невиконання заходів. Так, Закон про основи національної безпеки Литви визначає сектори національної економіки, які мають значення для національної безпеки: енергетика, транспорт, інформаційні технології та телекомунікації, інші високотехнологічні сфери, банківська та фінансова сфери.

У Литві стратегічні цілі та пріоритети політики кібербезпеки, а також заходи, необхідні для їх досягнення, визначає уряд, а не законодавчий орган чи Президент. Як найкращу практику регулювання в Україні можна адаптувати для застосування литовський закон про кібербезпеку, але з певними застереженнями, оскільки Литва як член ЄС визнає і без змін «переносить» Регламенти ЄС, що в Україні здійснити неможливо. Утім,

нашій державі все одно слід імплементувати як Директиви, так і Регламенти ЄС у цій сфері.

В Іспанії і Нідерландах до ухвалення рішень щодо формування та реалізації політики у сфері кібербезпеки залучені численні органи, а нормативно-правові акти вводяться в дію королівськими указами. У Нідерландах до системи забезпечення кібербезпеки включені також організації регіонального рівня.

Спільним для всіх країн (крім США, які наразі займаються цим питанням) є відведення великої ролі державно-приватному партнерству як складнику інституційного забезпечення управління кібербезпекою.

Державно-приватне партнерство реалізується за такими напрямами:

– підготовка пропозицій для розробки стратегічних документів у сфері кібербезпеки;

– участь у розробці стандартів, як національних, так і міжнародних;

– консультативно – дорадча функція;

– науково – технічне співробітництво (держава — наукові кола, наукові кола — бізнес);

– широкі консультації із заінтересованими сторонами в межах консультативно-дорадчих органів.

Слід зазначити, що в усіх країнах регулятори координують свою діяльність у сфері захисту персональних даних та у сфері кібербезпеки в частині інформування про інциденти, порушення цілісності систем, вироблення політики з метою уникнення дублювання повноважень тощо. Технічна частина системи захисту персональних даних регулюється законодавством у сфері кібербезпеки, а безпосередньо захист прав осіб — органом, що здійснює контроль у сфері захисту персональних даних.

Основними практиками кібербезпеки в Україні є:

– запровадження комплексу заходів із забезпечення кібербезпеки, який включає фізичний захист, логічний захист та технічний захист інформації;

– впровадження політики безпеки інформації, яка визначає правила доступу до інформації, зберігання інформації та використання інформації;

– проведення навчання персоналу з питань кібербезпеки;

– співпраця з міжнародними організаціями з питань кібербезпеки.

Основною стратегією кібербезпеки в Україні є стратегія, яка була затверджена Національним центром кібербезпеки в 2022 році. Стратегія визначає основні завдання та напрями діяльності України у сфері кібербезпеки.

Основними завданнями стратегії є:

– забезпечення стійкості та безпеки державних інформаційних і комунікаційних систем;

– забезпечення захисту критичної інфраструктури від кібератак;

– забезпечення захисту прав і свобод громадян у кіберпросторі.

Основними напрямами діяльності України у сфері кібербезпеки є:

– запровадження сучасних технологій і методів кібербезпеки;

– розвиток кадрового потенціалу у сфері кібербезпеки;

– співпраця з міжнародними організаціями та партнерами у сфері кібербезпеки.

Практики та стратегії кібербезпеки в Україні мають багато спільного з практиками та стратегіями кібербезпеки в інших країнах. Наприклад, у багатьох країнах світу існують закони, які визначають правові та організаційні основи захисту інформації в інформаційно-телекомунікаційних системах. Також у багатьох країнах світу існують державні органи, які відповідають за забезпечення кібербезпеки.

Однак, існують і деякі відмінності між практиками та стратегіями кібербезпеки в Україні та інших країнах. Наприклад, у деяких країнах світу

існують більш жорсткі вимоги до захисту інформації, ніж в Україні. Також у деяких країнах світу існують більш розвинені програми навчання та підготовки персоналу з питань кібербезпеки.

3.3 Комплексний підхід і практична реалізація кіберзахисту в банківській та фінансовій структурі.

3.3.1 Порівняння автоматизованих банківських систем.

Автоматизовані банківські системи (АБС) – це комплекси програмних і технічних засобів, які призначені для автоматизації діяльності банків. АБС дозволяють банкам автоматизувати такі процеси, як:

- відкриття та обслуговування рахунків;
- розрахунково-касове обслуговування;
- оформлення кредитів;
- оформлення депозитів;
- оформлення валютних операцій;
- оформлення операцій з цінними паперами;
- оформлення страхових операцій;
- оформлення інших банківських послуг.

Різноманітні модулі адміністрування дозволяють комплексу програмного забезпечення організувати доступність та безпеку банківської інформації. Різноманітні модулі дозволяють управляти доступом користувачів до будь-яких ресурсів системи, баз клієнтів, рахунків, операцій, функцій, документів, звітів.

АБС Б2 – це вітчизняна АБС, розроблена харківською компанією «CS». АБС Б2 є модульною системою, яка дозволяє банку адаптувати її під

свої потреби. АБС Б2 має широкий функціонал, який дозволяє банку автоматизувати всі основні банківські процеси.

АБС «Скрудж» - це також вітчизняна АБС, розроблена київською компанією «Лайм Системс». АБС «Скрудж» є масштабованою системою, яка дозволяє банку розширюватися без необхідності заміни АБС. АБС «Скрудж» має сучасний інтерфейс, який зручний для користувачів.

АБС Оракл ФлексКуб – це міжнародна АБС, розроблена американською компанією Oracle. АБС Оракл ФлексКуб має широкий функціонал і відповідає міжнародним стандартам. АБС Оракл ФлексКуб є однією з найпопулярніших АБС у світі.

Порівняння АБС Б2, АБС «Скрудж» і АБС Оракл ФлексКуб наведено в таблиці:

Таблиця 3.1 – Порівняння АБС Б2, АБС «Скрудж» і АБС Оракл ФлексКуб

Характеристика	АБС Б2	АБС «Скрудж»	АБС Оракл ФлексКуб
Розробник	CS (Україна)	Lime Systems (Україна)	Oracle (США)
Тип	Модульна	Масштабована	Міжнародна
Функціонал	Широкий	Сучасний	Широкий
Інтерфейс	Звичайне	Сучасний	Сучасний
Відповідність стандартам	Національні	Національні	Міжнародні
Популярність	Середня	Середня	Висока

Вибір АБС для банківської та фінансової структури залежить від таких факторів, як:

– розмір;

– сфера діяльност;

– фінансові можливості;
– потреби тієї чи іншої банківської та фінансової установи.

Для невеликих установ з обмеженими фінансовими можливостями АБС Б2 може бути хорошим варіантом. АБС Б2 є доступною за ціною і має широкий функціонал, який дозволяє автоматизувати основні банківські та фінансові процеси.

Для середніх і великих установ, які планують розширюватися, АБС «Скрудж» може бути хорошим варіантом. АБС «Скрудж» є масштабованою системою, яка дозволяє установі розширюватися без необхідності заміни АБС.

Для міжнародних установ, які працюють за міжнародними стандартами, АБС Оракл ФлексКуб може бути хорошим варіантом. АБС Оракл ФлексКуб має широкий функціонал і відповідає міжнародним стандартам.

3.3.2 Апаратно-програмний метод захисту даних

Зазвичай не усі співробітники усвідомлюють ступінь ризику та розмір шкоди, який може понести банк чи інша фінансова установа в разі втрати чи крадіжки зовнішніх носіїв інформації. Зважаючи на те, що більшість USB-накопичувачів знаходиться поза системою контролю чи управління служби безпеки, і на них не поширюється політика безпеки банківської та фінансової установи, це підвищує ризик несанкціонованого доступу до даних, витоку, пошкодженню або заміни даних і порушення вимог нормативно-правового законодавства.

Для вирішення подібних проблем розроблені комплекси – клієнт-серверні апаратно-програмні платформи (наприклад комплекс Microcrypt

Armorino Secure Storage (M.A.S.S.)). Дана технологія дозволяє будь-якому клієнту, приватному або корпоративному, забезпечити надійність і простоту в рішенні проблем, пов’язаних з безпечним зберіганням персональних або корпоративних даних. Складається комплекс з мобільного носія з апартною реалізацією шифрування, системи зберігання даних і програмного середовища з клієнт-серверною архітектурою.

Такі комплекси дозволяють:

– використовувати кілька типів розділів на одному пристрої;

– шифрувати всі дані, які використовуються на захищених розділах;

– розмежувати повноваження у використанні і делегувати різні права доступу;

– налаштовувати політики безпеки кожного користувача;

– використовувати інтегровані розширення, які, в свою чергу, використовують «захищене сховище» для зберігання своєї ключової інформації (такі як Windows Logon, Secure Virtual Drive, Microsoft Cryptographic Service Provider Next Generation, PKCS # 11 Module, IIT Client CSK- 1);

– використовувати пристрій для захищеного зберігання облікових записів;

– створювати локальні шифровані сховища на комп'ютері (папки, файли, диски) і, таким чином, забезпечити конфіденційність інформації на всіх етапах обробки в територіально-розподіленому робочому оточенні;

– мати можливість віддаленого скидання заблокованого пароля на основі одноразового пароля;

– використовувати інтегровану підтримку портативних версій ПЗ (браузер, поштовий клієнт, чат клієнт, Skype, антивірус, хранитель паролів і багато інших), які зберігають всю інформацію безпосередньо в зашифрованому розділі;

– використовувати функцію «Віртуальні диски» для зберігання «образу» будь-якого ПО (інформаційні бази даних, довідники і т.д.) на захищеному носії;

– зберігати резервні копії в зашифрованому вигляді;

– за потреби змінювати розміри розділів.

3.3.3 DLP як програмний метод захисту персональних даних

Абревіатура DLP означає Data Loss Prevention або «запобігання втраті даних». Це підхід або набір стратегій, що складаються з інструментів або процесів, за допомогою яких адміністратор мережі може забезпечити захист чутливих даних від несанкціонованого доступу, викрадення або втрати. Це унеможливлює надсилання користувачами чутливої або критичної інформації поза межі корпоративної мережі. Трапляється, що користувачі – через недбалість або злий намір – передають дані, а це може зашкодити банку чи фінансовій установі.

Причини для впровадження DLP-систем

Обсяг вкрадених даних зростає із кожним роком. Випадки витоку даних у своїй більшості супроводжуються публічним резонансом, і як наслідок негативно впливає на репутацію банку чи іншої фінансової установи, а часто і на її фінансове становище. А в останній час в умовах збільшення відсотку дистанційної роботи ситуація стає ще складнішою. Наприклад за даними дослідницької служби Ask Statista в США вартість наслідків середнього витоку даних оцінюється у 9,44 мільйонів доларів. DLP дозволяє вирішити три болісних питання в кібербезпеці банківської та фінансової установи: захист персональних даних/дотримання встановлених вимог, захист інтелектуальної власності та видимість даних. DLP-рішення є

також ефективними для протидії несанкціонованим діям користувачів, захисту даних Office 365, аналізу поведінки користувачів і структурних підрозділів банківської та фінансової установи та захисту від комплексних загроз.

Прикладом може слугувати програмний комплекс Symantec Data Loss Prevention. Цей комплекс може бути інтегрований в банк чи фінансову установу з невеликою кількістю користувачів, так і великих установ, кількість яких може перевищувати сотні тисяч.

Такий комплекс здатний захистити інформаційні дані банківської та фінансової установи на всіх ресурсах IT-інфраструктури:

– захист конфіденційних даних на робочих комп'ютерах і ноутбуках, навіть тих, що знаходяться за межами корпоративної мережі;

– виявлення конфіденційної інформації у відкритому доступі, в системах документообігу, поштового обміну, базах даних, на серверах і файлових сховищах;

– відстеження і блокування переміщення інформації усередині корпоративної мережі і за її межі;

– контроль веб-сервісів і хмарних сховищ, мобільних додатків, вхідних і вихідних повідомлень електронної пошти на мобільних пристроях.

3.3.4 Порівняльний аналіз розглянутих методів захисту

Зважаючи на вищезазначене, можна привести порівняльну таблицю методів захисту персональних та конфіденційних даних в банківській та фінансовій установі від витоків, пошкодження та розкрадання різними каналами.

Таблиця 3.2 – Порівняння методів захисту

	Апаратно-програмні платформи	DLP	Вбудовані методи АБС
Розмежування доступу	+	-	+
Ідентифікація і аутентифікація користувачів	+	-	+
Ведення детального протоколу дій	-	+	+
Безпечний перенос файлів на зовнішні носії	+	+\-	-
Забезпечення оффлайн-безпеки даних	+	-	-
Передача даних на мобільних пристроях	-	+	-
Захист даних на станціях за межами мережі	+	+	-
Легкість використання	+	-	+
Контроль впорядкованості файлів та даних	-	+	+
Контроль електронної пошти та месенджерів	-	+	-
Контроль за хмарними сховищами	-	+	-

З порівняння методів захисту можна виділити кілька особливостей:

– побудувати захист банківської та фінансової установи тільки апаратними чи тільки програмними методами неможливо, потрібен комплексний підхід;

– вбудовані методи АБС ведуть облік і контроль тільки базових каналів і джерел загроз, не забезпечуючи повного захисту персональних даних банківських та фінансових установ на належному рівні;

– системи DLP у свою чергу перекривають недоліки вбудованих в АБС методів захисту і контролю, забезпечуючи захист всіх можливих каналів витоку інформації, але не забезпечують захист файлів на електронних носіях, а тільки надають моніторинг за діями з даними носіями;

– можливі витоки і пошкодження носіїв виключають апаратно-програмні платформи (типу Armorino), які забезпечують надійний захист даних на флеш-носіях.

Висновки до розділу 3

В даному розділі дипломної роботи було зроблено порівняльний аналіз методів захисту персональних даних в банківських та фінансових установах, на основі якого можна зробити висновок, що жоден метод захисту персональних даних не може бути єдиним який використовується.

Проведено аналіз сучасних практик та стратегій кібербезпеки в Україні з іншими країнами.

Практики та стратегії кібербезпеки в Україні розвиваються в правильному напрямку. Україна впроваджує сучасні технології і методи кібербезпеки, розвиває кадровий потенціал у сфері кібербезпеки та співпрацює з міжнародними організаціями та партнерами у сфері кібербезпеки.

Однак, Україні необхідно продовжувати розвивати правову та технічну базу, розвивати кадровий потенціал у цій сфері, щоб забезпечити стійкість та безпеку державних інформаційних і комунікаційних систем, критичної інфраструктури та прав і свобод громадян у кіберпросторі.

ВИСНОВКИ

В дипломній роботі були охарактеризовані основні можливі види кіберзагроз інформаційної і комунікаційної інфраструктури та можливі наслідки, які вони несуть. Викладено правові засади інформаційної безпеки в банківській та фінансовій сферах.

Також в роботі викладено методи захисту в банківських та фінансових установах. Розглянуто и охарактеризовано захист комп'ютерної мережі, технічний захист конфіденційної інформації, програмний захист, у тому числі захист від вірусної небезпеки, криптографічний захист інформації.

Проведено порівняльний аналіз методів захисту персональних даних в банківських та фінансових установах, на основі якого можна зробити висновок, що жоден метод захисту персональних даних не може бути єдиним який використовується.

Проведено аналіз сучасних практик та стратегій кібербезпеки в Україні з іншими країнами.

Зазначено, що в Україні кібербезпека є одним із пріоритетних напрямів державної політики. У 2022 році Верховна Рада України прийняла Закон України "Про основні засади забезпечення кібербезпеки України", який визначає правові та організаційні основи забезпечення кібербезпеки в Україні.

Практики та стратегії кібербезпеки в Україні в цілому відповідають міжнародним стандартам. Однак, Україна все ще має певні недоліки в цій сфері, зокрема:

– недосконалість нормативно-правової бази у сфері кібербезпеки;

– недостатній рівень фінансування заходів із забезпечення кібербезпеки;

– недостатній рівень обізнаності населення про кібербезпеку;

Для подолання цих недоліків Україні необхідно продовжувати вдосконалювати своє законодавство, підвищувати рівень фінансування заходів із забезпечення кібербезпеки та проводити роз'яснювальну роботу серед населення про кібербезпеку.

Посилення законодавчої бази у сфері кібербезпеки передбачає розробку та затвердження нових нормативно-правових актів, які врахують сучасні загрози та ризики в цій сфері.

Основні напрями посилення законодавчої бази у сфері кібербезпеки включають:

– уточнення і конкретизація вимог до забезпечення кібербезпеки. Сучасні загрози кібербезпеці постійно змінюються і ускладнюються. Тому законодавчі вимоги до забезпечення кібербезпеки повинні бути такими, щоб вони могли ефективно протистояти цим загрозам;

– запровадження нових механізмів забезпечення кібербезпеки. Поряд з традиційними механізмами забезпечення кібербезпеки, такими як шифрування інформації, використання брандмауерів та антивірусного програмного забезпечення, необхідно впроваджувати нові механізми, які відповідають сучасним загрозам. До таких механізмів можна віднести, наприклад, використання штучного інтелекту для виявлення та протидії кібератакам;

– посилення відповідальності за порушення вимог законодавства у сфері кібербезпеки. Порушення вимог законодавства у сфері кібербезпеки може призвести до серйозних наслідків, таких як витоки конфіденційної інформації, фінансові втрати та навіть порушення роботи критичної інфраструктури. Тому відповідальність за такі порушення повинна бути посилена.

Конкретні заходи щодо посилення законодавчої бази у сфері кібербезпеки можуть включати:

– запровадження обов’язкового аудиту кібербезпеки для всіх банків та фінансових установ. Аудит повинен проводитися незалежними експертами та повинен включати оцінку стану кібербезпеки, виявлення та усунення уразливостей, а також розробку рекомендацій щодо підвищення рівня кібербезпеки;

– встановлення вимог до використання сучасних технологій та методів захисту інформації. До таких вимог можуть входити вимоги до шифрування інформації, використання брандмауерів та антивірусного програмного забезпечення, управління доступом до інформації, навчання персоналу з питань кібербезпеки;

– запровадження кримінальної відповідальності за кібератаки. Санкції за кібератаки повинні бути суворими та мати чітко визначений перелік;

– затвердження нового закону про кібербезпеку. Новий закон повинен визначити основні принципи і напрями забезпечення кібербезпеки в Україні, а також встановити вимоги до забезпечення кібербезпеки для різних суб'єктів;

– внесення змін до чинних законів, які стосуються кібербезпеки. Ці зміни повинні врахувати сучасні загрози та ризики в сфері кібербезпеки;

– розробка та затвердження нормативно-правових актів, які конкретизують вимоги до забезпечення кібербезпеки. Ці акти повинні визначати конкретні заходи, які повинні вжити суб'єкти для забезпечення кібербезпеки.

Крім того, необхідно провести гармонізацію українського законодавства у сфері кібербезпеки з міжнародними стандартами. Це дозволить Україні підвищити рівень кібербезпеки та узгодити свою політику у цій сфері з політикою інших країн.

Посилення законодавчої бази у сфері кібербезпеки є важливим кроком на шляху до підвищення рівня кібербезпеки в Україні.

Заходи технічного захисту конфіденційної інформації в банківській та фінансовій сфері України повинні бути комплексними та постійно вдосконалюватися. А на сьогодні, в системах автоматизації банківської діяльності проблеми захисту враховуються досить слабо, а якщо і враховуються, то не в повному обсязі. Це ускладнює забезпечення належного захисту інформації на етапах її створення, передачі та обробки. Найчастіше захищається та інформація, яка виходить за межі банку. Внутрішня система банку, зазвичай, незахищена. Це зумовлено великою кількістю зовнішніх загроз і відсутністю статистики злочинів, технічної недосконалості банків.

Одним із основних напрямків розвитку технічного захисту конфіденційної інформації в банківській та фінансовій сфері України є впровадження штучного інтелекту та машинного навчання. Такі технології дозволяють автоматизувати процеси виявлення та реагування на кібератаки, а також підвищити ефективність заходів технічного захисту інформації.

Наукова новизна магістерської роботи полягає в наступному:

– проведено аналіз сучасного стану кібербезпеки банківської та фінансової структури. Робота включає в себе аналіз нормативно-правової бази, організаційних та технічних заходів, що застосовуються в Україні для забезпечення кібербезпеки банківської та фінансової структури;

– проведено порівняльний аналіз кібербезпеки банківської та фінансової структури України з іншими країнами світу. У роботі показано, що Україна має ряд проблем у сфері кібербезпеки, які необхідно вирішити для забезпечення безпеки банківської та фінансової системи країни.

Основні результати дослідження:

– на основі проведеного аналізу встановлено, що нормативно-правова база України у сфері кібербезпеки банківської та фінансової структури є досить розвиненою. Однак, існує ряд проблем у її реалізації, зокрема, недостатнє фінансування заходів кібербезпеки, а також недостатній рівень інформованості банківських працівників про кіберзагрози;

– у роботі показано, що організаційні та технічні заходи, що застосовуються в Україні для забезпечення кібербезпеки банківської та фінансової структури, відповідають міжнародним стандартам. Однак, існує ряд проблем у їх реалізації, зокрема, недостатній рівень кваліфікації персоналу, а також недостатнє фінансування заходів кібербезпеки;

– у роботі показано, що рівень кібербезпеки банківської та фінансової структури України є нижчим, ніж у розвинених країнах світу. Це пов'язано з рядом проблем, зокрема, недостатнім фінансуванням заходів кібербезпеки, недостатнім рівнем інформованості банківських працівників про кіберзагрози, а також недостатнім рівнем кваліфікації персоналу.

Висновки та рекомендації.

Для підвищення рівня кібербезпеки банківської та фінансової структури України необхідно вжити наступних заходів:

– покращити нормативно-правову базу у сфері кібербезпеки;

– збільшити фінансування заходів кібербезпеки;

– покращити інформованість банківських працівників про кіберзагрози;

– підвищити рівень кваліфікації персоналу, що відповідає за забезпечення кібербезпеки.

Результати дослідження мають важливе практичне значення для підвищення рівня кібербезпеки банківської та фінансової структури України і можуть бути використані для підвищення рівня кібербезпеки банків і фінансових установ в Україні.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» / В.М.Ахрамович.; Державний університет телекомунікацій. – К.:ДУТ, 2019. – 163 с.

2. Банківська безпека: підручник / КорченкоА.О., Скачек Л.М, Хорошко В.О. – К.: ПВП «Задруга», 2014 – с.185.

3. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння: ДСТУ 4145: 2002. – [Чинний від 2002-03-13]. К.: Держстандарт України, 2002. – 38 с.: табл. – (Національний стандарт України).

4. Безпека банківських систем : навч. посіб. / П. С. Усік, К. О. Буравченко; М-во освіти і науки України, Центральноукр. нац. техн. ун-т.— Кропивницький: ЦНТУ, 2022. — 194 с.

5. Формування системи інформаційної безпеки в банківському секторі України / О.П. Степаненко// Моделювання та інформаційні системи в економіці. – 2015. – № 91. – С. 17-35.

6. Банківські технології і продукти : навчальний посібник./ Чайковський Я. І.; Тернопіль : ЗУНУ, 2021. 172 с.

7. Звіт про фінансову стабільність НБУ за червень 2023 року. URL: https://bank.gov.ua/ua/news/all/zvit-pro-finansovu-stabilnist-cherven-2023-roku.

8. Методичні рекомендації до виконання дипломних проектів для студентів спеціальності 125 “Кібербезпека” другого (магістерського) рівня / уклад. С. П. Євсеєв, А. А. Гаврилова, О.В. Мілов. – Харків : ХНЕУ ім. С. Кузнеця, 2021. – 63 с.

9. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с.

10. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

11. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". URL: https://zakon.rada.gov.ua/laws/show/681-20#Text.

12. Закон України «Про Національний банк України». URL: https://zakon.rada.gov.ua/laws/show/679-14#Text.

13. Закон України "Про основи національної безпеки". URL: https://zakon.rada.gov.ua/laws/show/964-15#Text.

14. Закон України «Про доступ до публічної інформації». URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

15. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

16. Закон України «Про захист інформації в автоматизованих системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

17. Закон України "Про електронні документи та електронний документообіг". URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

18. Закон України — «Про електронний цифровий підпис». URL: https://zakon.rada.gov.ua/laws/show/851-15#Text.

19. Закон України «Про банки і банківську діяльність». URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text.

20. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

21. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

22. Закон України «Про захист інформації в автоматизованих системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

23. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

24. Постанова Правління Національного банку України від 26 листопада 2015 року N 829 «Про затвердження нормативно-правових актів з питань інформаційної безпеки». URL: https://bank.gov.ua/ua/legislation/Resolution_26112015_829.

25. Правила оформлення Регламенту роботи центрів сертифікації ключів банків України (z1036-10), зареєстровані в Міністерстві юстиції України 04.11.2010 за N 1036/18331. URL: https://zakon.rada.gov.ua/laws/show/z1036-10#Text.

26. Правила реєстрації, засвідчення чинності відкритого ключа та акредитації центрів сертифікації ключів банків України в Засвідчувальному центрі Національного банку України (z1035-10), зареєстровані в Міністерстві юстиції України 04.11.2010 за N 1035/18330. URL: https://zakon.rada.gov.ua/laws/show/z1035-10#Text.

27. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17.

28. Положення про діяльність в Україні внутрішньодержавних і міжнародних платіжних систем // Постанова Національного банку України від 25.09.2007 р. № 348 зі змінами та доповненнями // [Електронний ресурс].— Режим доступу: www.rada.kiev.ua.

29. Положення про забезпечення безперервного функціонування інформаційних систем Національного банку та банків України, затверджене

постановою Правління Національного банку України від 17.06.2004 N 265 (z0857-04). URL: https://zakon.rada.gov.ua/laws/show/z1197-12#Text.

30. Положення про застосування Національним банком України заходів впливу за порушення банківського законодавства // Постанова Національного банку України від 28.08.2001 р. № 369 зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/z0845-01#Text.

31. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене Постановою Правління Національного банку України 28.09.2017 № 95 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/v0095500-17.

32. Положення про порядок формування, зберігання та знищення електронних архівів у Національному банку України і банках України, затверджене постановою Правління Національного банку України від 12.09.2006 N 163 357 (z1089-06), зареєстроване в Міністерстві юстиції України 03.10.2006 за N 1089/12963. URL: https://zakon.rada.gov.ua/laws/show/z1089-06#Text.

33. Постанова Правління Національного банку України "Про затвердження нормативно-правових актів з питань функціонування електронного цифрового підпису в банківській системі України" від 17.06.2010 N 284 (z1034-10), зареєстрована в Міністерстві юстиції України 04.11.2010 за N 1034/18329. URL: https://zakon.rada.gov.ua/laws/show/z1034-10#Text.

34. Правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затверджені постановою Правління Національного банку України від 02.04.2007 N 112 (z0419-07), зареєстровані в Міністерстві юстиції України 24.04.2007 за N 419/13686. URL: https://zakon.rada.gov.ua/laws/show/z0419-07#Text.

35. Правління Національного банку України. Постанова 04 грудня 2017 року м. Київ № 124. Про затвердження Змін до Правил зберігання, захисту, використання та розкриття банківської таємниці. URL : https://zakon.rada.gov.ua/laws/show/v0124500-17#Text.

36. Правління Національного банку України. Постанова 26.11.2015 № 829. Про затвердження нормативно-правових актів з питань інформаційної безпеки. URL: https://zakon.rada.gov.ua/laws/show/v0829500-15#Text.

37. Правління Національного банку України. Постанова. 04.07.2007 N 243. Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи. URL: https://zakon.rada.gov.ua/laws/show/z0955-07#Text.

38. Правління Національного банку України. Постанова. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17#Text.

39. Правління Національного банку України. Постанова 10 лютого 2016 року м. Київ № 63. Про затвердження Правил з організації захисту приміщень банків в Україні. URL: https://zakon.rada.gov.ua/laws/show/v0063500-16#Text.

40. Указ Президента України від 14.05.2021 № 96/2016 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» [Електронний ресурс]. – Режим доступу : https://www.president.gov.ua/documents/4472021-40013.