

МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА
на тему:

Технології електронних фондів, архівів та бібліотек

Здобувача вищої освіти першого (бакалаврського) рівня,
4 курсу, групи КБ-19-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології (за галузями)»


(підпис)

Данилка Ігоря Костянтиновича
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Філоненко Михайло
Миколайович, к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Керівник освітньо-
професійної програми


(підпис)

Федотова - Півень Ірина
Миколаївна, к.т.н, доцент
(прізвище, ім'я, по батькові, науковий ступінь,
вчене звання)

Допущено до захисту за рішенням кафедри
протокол від «26» травня 2023 № 13

Завідувач кафедри


(підпис)

Філоненко Михайло Миколайович
к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вче
звання)

Реєстрація № 30

06.06.2023
(дата)


(підпис відповідальної особи)

Результати перевірки

до захисту
(до захисту, на доопрацювання)

06.06.2023
(дата)


(підпис)

Результат захисту

4 (добре)
(оцінка)

15.06.2023
(дата)


(підпис)

Голова комісії:


(підпис)

В.М. Франчук

Члени комісії:


(підпис)

М.М. Філоненко


(підпис)

О.В. Редич


(підпис)

Є.В. Котух

БЛАНК ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	26		15.06.2023 Франчук В.М.  Філоненко М.М.  Редич О.В.  Котух Є.В.  Суховерхівка Л.П. 
2. Дотримання вимог щодо оформлення	від 0 до 10	7		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	4		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	41		

Оцінювання кваліфікаційної роботи науковим керівником - 41 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
82	B	4 (добре)	15.06.2023	Франчук В.М.  Філоненко М.М.  Редич О.В.  Котух Є.В.  Суховерхівка Л.П. 

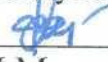
ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	
50-59	E	3 (задовільно)
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
 Кафедра комп'ютерних та інформаційних технологій і систем
 Галузь знань: 12 «Інформаційні технології»
 Спеціальність: 122 «Комп'ютерні науки»
 Освітня програма: «Інформаційні управляючі системи і технології (за галузями)»

Затверджую

Завідувач кафедри

 Філоненко

М.М.

«16» 11 2022

**Завдання на кваліфікаційну роботу
 здобувачу вищої освіти**

Данилка Ігоря Костянтиновича

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи

Технології електронних фондів, архівів та бібліотек.

Затверджена наказом ректора від «15» листопада 2022 № 1205

2. Строк здачі закінченої роботи «26» травня 2023

3. Цільова установка застосування знань, вмінь та навичок, здобутих під час навчання на першому (бакалаврському) рівні за спеціальністю 122 «Комп'ютерні науки»

Мета роботи Аналіз та розгляд технологій електронних фондів, архівів та бібліотек, їх огляд та функціонування

Об'єкт дослідження Процес і функціонал електронних технологій

Предмет дослідження Вивчення та огляд роботи технологій в електронних фондах, архівах та бібліотеках.

4. Вихідні дані до роботи Технології в електронних фондах. Архівах та бібліотеках

5. Перелік графічного матеріалу 2 рисунки

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	4
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	До 15.11.2022	15.11.2022
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	01.02.2023	01.02.2023
3	II розділ (аналіз експериментальної частини про методики досліджень)	03.04.2023	04.04.2023
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	10.05.2023	09.05.2023
5	Висновки	15.05.2022	15.05.2022
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	26.05.2023	26.05.2023
7	Отримання відгуку керівника	06.06.2023	06.06.2023
8	Отримання зовнішньої рецензії	08.06.2023	08.06.2023

8. Дата видачі завдання «16» листопада 2022

9. Керівник випускної кваліфікаційної роботи


 (підпис)

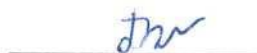
 Філоненко М.М.
 (прізвище, ініціали)

10. Керівник освітньо-професійної програми


 (підпис)

 Федотова-Півень І
 (прізвище, ініціали)

11. Завдання до виконання отримав здобувач вищої освіти


 (підпис)

 Данишко І.К.
 (прізвище, ініціали)

АНОТАЦІЯ

Технології електронних фондів, архівів та бібліотек

Метою даного дослідження є аналіз та розгляд технологій електронних фондів, архівів та бібліотек. Їх огляд та функціонування.

Завдання роботи включає

- аналіз та визначення методів і інструментів;
- визначення особливостей державного регулювання банківської системи;
- практичне застосування методів та інструментів фінансового механізму банківської діяльності.

Предметом дослідження є вивчення та огляд роботи технологій в електронних фондах, архівах та бібліотеках.

Об'єктом дослідження є процес і функціонал технологій.

За результатами дослідження розроблено модель роботи технологій в електронних фондах, архівах та бібліотеках.

Кваліфікаційна робота містить 44 сторінки, 2 рисунки, список використаних джерел 44 найменування.

Ключові слова технології, бібліотеки та архіви, фонди, безпека.

Рік виконання кваліфікаційної роботи: 2023 р.

Рік захисту роботи: 2023 р.

ABSTRACT

Technologies of electronic funds, archives and libraries

The aim of the study is to analyze and consider the technologies of electronic funds, archives and libraries. Their review and functioning.

The task of work includes

- analysis and definition of methods and tools;
- determination of features of state regulation of the banking system;
- practical application of methods and tools of the financial mechanism of banking activity.

The subject of research is the study and review of the operation of technologies in electronic funds, archives and libraries..

The object of the study is the process and functionality of technologies.

According to the results of the research, a model of the operation of technologies in electronic funds, archives and libraries was developed.

The qualification work contains 44 pages, 2 images, a list of 44 references.

Keywords technologies, libraries and archives, funds, security.

Year of qualification work: 2023.

Year of job protection: 2023

Зміст

ВСТУП.....	9
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ЗДІЙСНЕННЯ ЗАХИСТУ ОСІБ У ФІНАНСОВІЙ СФЕРІ АО «ПриватБанк».....	11
1.1. Підходи до вивчення сутності та характеристика процесу захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері у роботах банківських систем, електронних фондів, архівів та бібліотеках.....	11
1.2. Методологія дослідження здійснення захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері діяльності АО «ПриватБанк».....	18
РОЗДІЛ 2. АНАЛІЗ СТАНУ ТА ТЕНДЕНЦІЇ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ЗДІЙСНЕННЯ ЗАХИСТУ ФОНДІВ, АРХІВІВ ТА БІБЛІОТЕК.....	23
2.1. Ефективність та сучасні тенденції розвитку підходів до захисту електронних фондів, архівів та бібліотек АО «ПриватБанк».....	23
2.2. Передумови удосконалення процесу захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері банку АО «ПриватБанк».....	27
РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ ОСІБ ПІДОЗРЮВАНИХ У ВЧИНЕННЯ ЗЛОЧИНІВ У ФІНАНСОВІЙ СФЕРІ АО «ПриватБанк».....	34
3.1 Розвиток системи захисту підозрюваних осіб.....	34
3.2 Вдосконалення служби безпеки банку.....	37
ВИСНОВКИ.....	39
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	40

ВСТУП

Поглиблення зміни електронних фондів, архівів та бібліотек банківської системи в Україні розглядається як одне з пріоритетних завдань економічної політики на сучасному етапі. Для ринкової системи важливим елементом є розвиток діяльності банків та їх сфера діяльності, розширення сфери банківських послуг та операцій, що потребує відповідного контролю та нагляду з боку державних органів грошово-кредитного регулювання.

В Україні такі функції реалізує Національний банк України через інструменти відповідної грошово-кредитної політики. Функціонування банківської системи свідчить про те, що банки не можуть існувати незалежно від процесів, що відбуваються в реальному секторі економіки, оскільки саме тут здійснюється використання грошових капіталів.

Визначення і практичне застосування методів та інструментів фінансового механізму державного регулювання банківської діяльності повинні бути адекватні стану фінансової системи, електронних фондів, архівів та бібліотек та економіки загалом. Забезпечення фінансової стійкості та стабільного функціонування банківської діяльності при одночасному захисті інтересів клієнтів, є головною метою регулювання банківської діяльності.

Актуальність дослідження проблеми регулювання банківської діяльності визначається також і тим, що електронних фондів, архівів та бібліотек до певного часу в Україні у банківській практиці фактично не існувало поняття “регулювання банківської діяльності”.

Для забезпечення електронних фондів, архівів та бібліотек стабільності банківської діяльності зумовило постійну увагу дослідників до його різних аспектів.

Регулюванню банківської діяльності, грошового обігу та кредиту присвячені роботи багатьох вітчизняних вчених, зокрема У. Грудзевича, І. Д’яконової, В. Коваленка, О. Козьменка, Т. Васильєва, Л. Конопатської, М. Савлука, С. Мочерного та багатьох інших.

Метою даної роботи є визначення особливостей державного регулювання

банківської системи. Відповідно до мети виділено наступні завдання:

- визначити будову та функції банківської системи;
- з'ясувати механізм реалізації банківського нагляду;
- ознайомитись з світовим досвідом здійснення банківського нагляду;
- визначити сучасний стан, проблеми та перспективи розвитку вітчизняної

банківської системи;

- підходи до вивчення сутності та характеристика процесу захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері у роботах банківських систем, електронних фондів, архівів та бібліотеках;

- методологія дослідження здійснення захисту;
- ефективність та сучасні тенденції розвитку;
- удосконалення процесу захисту;
- перспективи розвитку системи захисту.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ЗДІЙСНЕННЯ ЗАХИСТУ ОСІБ У ФІНАНСОВІЙ СФЕРІ АО «ПриватБанк»

1.1. Підходи до вивчення сутності та характеристика процесу захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері у роботах банківських систем, електронних фондів, архівів та бібліотеках.

Сучасний етап розвитку українського суспільства характеризується стратегічним курсом на створення суверенної незалежної демократичної правової держави. В країні здійснюються радикальні соціально-економічні реформи, йде процес демократизації усіх сторін суспільного життя, який неможливий без закріплення законності і правопорядку, забезпечення надійної охорони конституційних прав і свобод громадян. Разом з тим в останні роки при загальному скороченні крадіжок, пограбувань та розбійних нападів зростає кількість розкрадань грошових сум з банків та інших кредитно-фінансових закладів, кас підприємств, організацій тощо. Дестабілізуючи вплив на обстановку в країні набирає сили організована злочинність, яка в останні роки поряд із вчиненням загально-кримінальних злочинів інтенсивно інтегрується в економічну сферу з метою отримання високих незаконних прибутків, зливаючись при цьому з економічною злочинністю. У зв'язку з цим відбувається процес розширення масштабів злочинних проявів, який характерний практично для усіх галузей економіки України. Особливе занепокоєння в цьому плані викликає факт виникнення та розвитку в Україні нового виду злочинних посягань, раніше невідомих вітчизняній юридичній науці та практиці, пов'язаних з використанням засобів комп'ютерної техніки та інформаційно-обробної технології – комп'ютерних злочинів.

Банківська система України – один з найважливіших елементів її фінансової системи. Як і вся економіка України, банківська система сьогодні зазнає кардинальних змін, які торкаються структурної і функціональної її частини. Зміни фіксуються банківським законодавством, розробка якого здійснюється на основі міжнародного досвіду та економічних реформ, які проходять в Україні, а також сучасних уявлень про суть та призначення

банківських установ. Економічна природа банків розкривається в їх специфічній функції: виконувати на економічному ринку роль особливих фінансових посередників. В такій ролі банки залучають вільні грошові кошти, які звільнюються в процесі господарської діяльності одних суб'єктів – держави, господарюючих структур, фізичних осіб – та надаються на умовах забезпеченості, повернення, строковості, платності та цільової направленості на тимчасове користування іншим. Саме система банків акумулює величезний фонд грошових коштів як в готівковій, так і в безготівковій формі.

Класифікації загроз інформації в автоматизованих системах приділялась значна увага у роботах провідних фахівців. У науковій літературі запропоновані різні визначення загроз в залежності від їх специфіки, середовища прояву, результатів їх впливу, нанесеного збитку тощо. Під загрозами будемо розуміти цілеспрямовані та випадкові дії, що підвищують уразливість зберігання, обробки та передачі інформації в автоматизованій банківській системі. Впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій зумовило поширення великих масивів інформації в обчислювальних та інформаційних мережах на значних територіях. За відсутності вітчизняних конкурентоспроможних інформаційних технологій надається перевага технічним засобам обробки інформації та засобам зв'язку іноземного та спільного виробництва, які здебільшого не забезпечують достатній захист інформації.

Стаття 1. Визначення інформації Під інформацією цей Закон розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Стаття 2. Мета і завдання Закону Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Стаття 3. Сфера дії Закону Дія цього Закону поширюється на інформаційні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави

при одержанні, використанні, поширенні та зберіганні інформації.

Стаття 5. Основні принципи інформаційних відносин Основними принципами інформаційних відносин є: гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об'єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації.

Стаття 7. Суб'єкти інформаційних відносин Суб'єктами інформаційних відносин є: громадяни України; юридичні особи; держава. Суб'єктами інформаційних відносин відповідно до цього Закону можуть бути також інші держави, їх громадяни та юридичні особи, міжнародні організації та особи без громадянства.

Стаття 8. Об'єкти інформаційних відносин Об'єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах.

Стаття 9. Право на інформацію Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Стаття 12. Визначення інформаційної діяльності Інформаційна діяльність — це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави. З метою задоволення цих потреб органи державної влади та органи місцевого і регіонального самоврядування створюють інформаційні служби, системи, мережі, бази і банки даних. Порядок їх створення, структура, права та обов'язки визначаються Кабінетом Міністрів України або іншими органами державної влади, а також органами місцевого і регіонального самоврядування.

Стаття 13. Основні напрями інформаційної діяльності Основними напрямками інформаційної діяльності є: політичний, економічний, соціальний, духовний, екологічний, науково-технічний, міжнародний тощо. Держава

зобов'язана постійно дбати про своєчасне створення, належне функціонування і розвиток інформаційних систем, мереж, банків і баз даних у всіх напрямках інформаційної діяльності. Держава гарантує свободу інформаційної діяльності в цих напрямках всім громадянам та юридичним особам в межах їх прав і свобод, функцій і повноважень.

Стаття 14. Основні види інформаційної діяльності Основними видами інформаційної діяльності є одержання, використання, поширення та зберігання інформації. Одержання інформації – це набуття, придбання, накопичення відповідно до чинного законодавства України документованої або публічно

Банківський сектор повинен утримувати у досить стабільному стані грошово-кредитну систему, створювати умови для розвитку економіки, сприяти конвертованості національної валюти, навчати клієнтуру рахувати гроші[40, С.132]..

Дуже часто в літературі банківську систему трактують як просту сукупність банків, що функціонують в країні. При такому підході до визначення сутності банківської системи вона являє собою механічне об'єднання банків, що немає заздалегідь окреслених цілей, специфічних рис і не виконує самостійних функцій і ролі на грошовому ринку.

Комунікаційне обладнання іноземного виробництва, яке використовується у мережах зв'язку, передбачає дистанційний доступ до його апаратних та програмних засобів, у тому числі з-за кордону, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються. Прогрес у різних галузях науки і техніки, призвів до створення компактних та високоефективних технічних засобів, за допомогою яких можна підключатись до ліній телекомунікацій та різноманітних технічних засобів обробки інформації вітчизняного та іноземного виробництва з метою отримання, пересилання та аналізу розвідувальних даних. Для цього може використовуватись апаратура радіо-, радіотехнічної, оптико-електронної, радіо-теплової, акустичної розвідок.

Усі потенційні загрози несанкціонованого доступу до інформації інформаційних систем розподіляються на цілеспрямовані та випадкові.

Потенційні загрози і канали несанкціонованого доступу до інформації в ПЕОМ залежать, насамперед, від умов її експлуатації – чи використовується ПЕОМ одним користувачем, чи групою. В першому випадку необхідний захист тільки від стороннього користувача, в другому – від будь-якого з користувачів, які працюють на одній ПЕОМ. Коли на ПЕОМ працює один користувач і відсутні засоби захисту, потенційними каналами несанкціонованого доступу можуть бути: – термінал, кінцеві модулі, пристрої користувача (клавіатура і засоби відбиття інформації); – засоби документування інформації; – засоби завантаження ПЗ; – носії інформації (машинні, паперові); – внутрішній монтаж ПЕОМ; – побічне електромагнітне випромінювання і наводки (ПЕМВН); – відходи в корзині сміття та інше.

Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як: необґрунтована відмова від надання відповідної інформації; надання інформації, що не відповідає дійсності; несвоєчасне надання інформації; навмисне приховування інформації; примушення до поширення або перешкоджання поширенню інформаційних сигналів такого роду збільшується. Несанкціоноване підключення порушником ТЗІ приймальної апаратури та спеціальних датчиків до ланцюгів електроживлення і заземлення, інженерних комунікацій та до каналів зв'язку також дозволяє несанкціоноване одержання інформації, а несанкціоноване під'єднання до каналів зв'язку в трактах передачі даних може призвести до модифікації та порушенню цілісності інформації в обчислювальних мережах 1. Тому на підставі вищевикладеного можна виділити ще одну класифікацію каналів витоку інформації – за фізичною природою: – радіоканали (електромагнітні випромінювання в радіодіапазоні); – акустичні (поширення звукових коливань у будь-якому звукопровідному матеріалі); – електричні (напруги і струми в різних струмопровідних комунікаціях); – візуально-оптичні (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій ділянці спектра); – матеріально-речові (папір, фото, магнітні носії, відходи тощо) (Рис. 1.1). Фізичні процеси, що відбуваються в технічних засобах при їх функціонуванні, створюють у навколишньому просторі побічні випромінювання,

що у тій чи іншій мірі пов'язані з оброблюваною інформацією.



Рис. 1.1. Технічні канали витоку інформації.

1.2 Методологія дослідження здійснення захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері діяльності АО «ПриватБанк»

Джерелом утворення акустичного каналу витоку інформації є вібруючі тіла чи механізми, такі як голосові зв'язки людини, рухомі елементи машин, телефонні апарати, звукопосилюючі системи, гучномовні засоби зв'язку, засоби звукозапису і звуковідтворення і навіть ПЕОМ, що працює в режимі вводу, виводу й обробки звукової інформації¹. Електричні канали витоку інформації це ланцюги живлення і заземлення. Візуально-оптичні канали утворюються як оптичний шлях від об'єкта конфіденційних устремлінь до зловмисника. Для утворення візуально- оптичних каналів необхідні певні просторові, енергетичні і тимчасові умови і відповідні засоби на стороні зловмисника.

Переважним правом на одержання інформації користуються громадяни, яким ця інформація необхідна для виконання своїх професійних обов'язків. Стаття 30. Інформація з обмеженим доступом Інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну і таємну. Конфіденціальна інформація – це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов.

Банківська система – законодавчо визначена, чітко структурована та субординована сукупність фінансових посередників, які здійснюють банківську діяльність на постійній професійній основі і функціонально взаємозв'язані в самостійну економічну структуру[14, С.563-564].

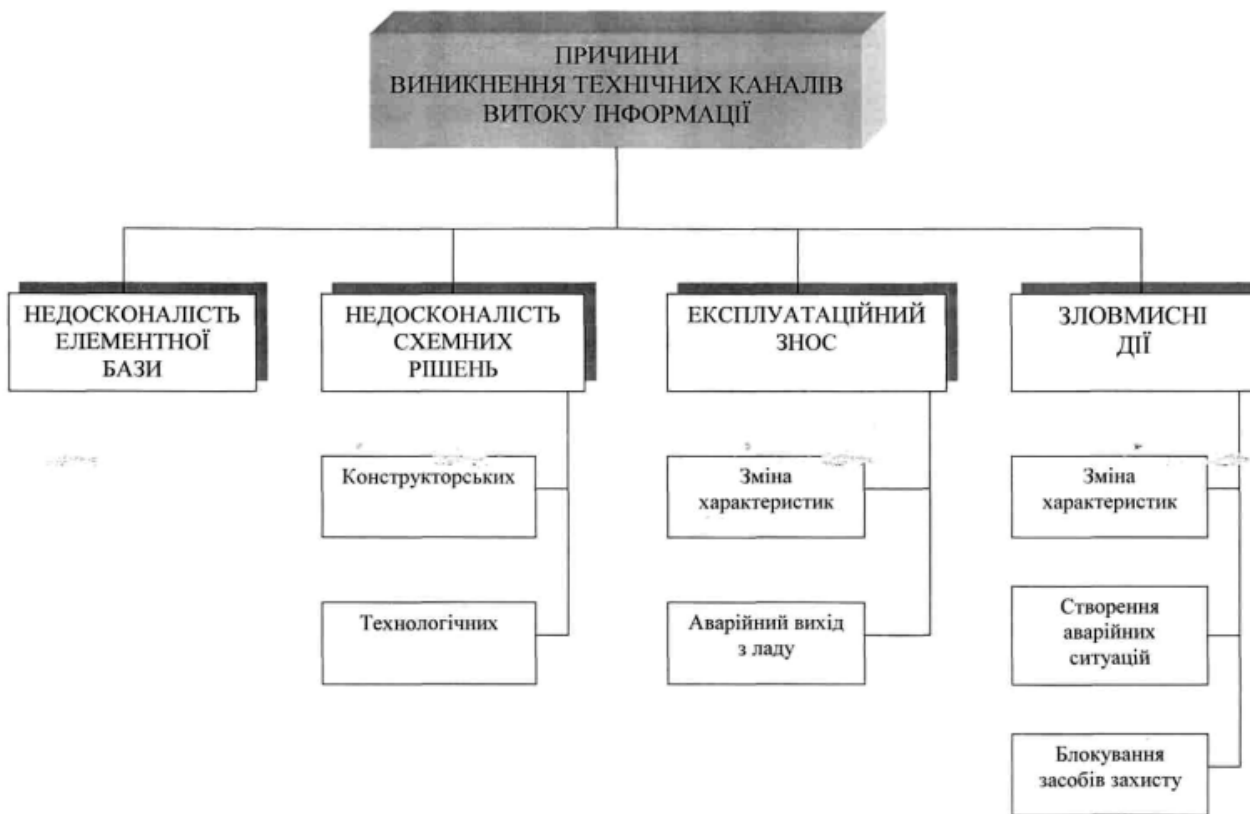


Рис. 1.2 Причини витоку інформації.

На перше місце в банківській системі виходять такі цілі:

- забезпечення суспільного нагляду і регулювання банківської діяльності з метою узгодження інтересів окремих банків із загальносуспільними інтересами;
- забезпечення надійності і стабільності функціонування банківської системи в цілому з метою стабілізації грошей та безперебійного обслуговування економіки;
- забезпечення ефективної взаємодії банків з органами державної влади та міжнародних фінансових інституцій з метою узгодження інтересів усіх учасників цих взаємовідносин

Розгляд названих цілей дає підстави стверджувати, що всі вони можуть бути виконані тільки сукупністю банків, що поєднуються в банківську систему[11, С.30].

Проте в більшості країн світу створена та діє дворівнева банківська система. Така система складається з головного або Центрального банку країни, що є емісійним центром в державі та всієї сукупності інших банків, що обслуговують юридичних та фізичних осіб[11, С.29].

На другому рівні банківської системи перебуває решта банків, які в Україні прийнято називати комерційними банками. У зарубіжних країнах комерційними називають тільки частину банків другого рівня. Переважно це банки, що виконують весь комплекс базових операцій і створені на акціонерній основі. Крім комерційних, у кожній країні виділяється цілий спектр інших банків - кооперативних, приватних, спеціалізованих тощо.

Банки другого рівня відносно один одного є економічно самостійними, рівноправними, такими, що конкурують між собою на грошовому ринку. Вони юридичне й економічно відокремлені і будують свою діяльність на комерційних засадах з метою одержання прибутку. Заради прибутку вони обслуговують своїх клієнтів, зазнаючи при цьому великих ризиків: кредитних, процентних, валютних тощо.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей. До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до закону про цю інформацію. Порядок обігу таємної інформації та її захисту визначається відповідними державними органами за умови додержання вимог, встановлених цим Законом. Порядок і терміни обнародування таємної інформації визначаються відповідним законом. Стаття 38. Право власності на

інформацію Право власності на інформацію – це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження інформацією. Інформація є об'єктом права власності громадян, організацій (юридичних осіб) і держави. Інформація може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Власник інформації щодо об'єктів своєї власності має право здійснювати будь-які законні дії. Підставами виникнення права власності на інформацію є: створення інформації своїми силами і за свій рахунок; договір на створення інформації; договір, що містить умови переходу права власності на інформацію до іншої особи.

Кримінально-правового значення розглянемо більш розгорнуто. Більшість фахівців поділило комп'ютерні злочини на два типи:

1. Злочини, в яких об'єктом їх здійснення є ЕОМ: – знешкодження або заміна даних, програмного забезпечення та обладнання; – розкрадання вхідних, вихідних даних, програмного забезпечення та обладнання; – економічне шпигунство та розголошення відомостей, які складають державну чи комерційну таємницю; – інші злочинні діяння цього виду.

2. Протизаконні акції, для здійснення яких ЕОМ використовується як знаряддя в досягненні злочинної мети: – комп'ютерний саботаж; – вимагання та шантаж; – розтрата; – розкрадання коштів; – обман споживачів, інвесторів чи користувачів; – інші злочини. До категорії «інші злочинні діяння» віднесено несанкціоноване використання комп'ютеру в особистих цілях.

На мій погляд, під комп'ютерною злочинністю слід розуміти суспільно-небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинити збитки майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським формуванням і громадянам, а також правам особи.

На підставі вищевикладеного можна зробити такі висновки: Криміналістична характеристика незаконного втручання в роботу ЕОМ банківської установи, відрізняється специфікою, особливостями й містить у собі:

дані про предмет злочинного посягання, відомості про способи підготовки, вчинення й приховання злочину; дані про обстановку вчинення злочину, дані про особу злочинця, а так само відомості про «слідову картину». Вище проаналізовані елементи криміналістичної характеристики дозволяють запропонувати такі новації, пропозиції і рекомендації. 1. Способи вчинення незаконного втручання в роботу ЕОМ банку доцільно поділяти на дві групи: 1) способи безпосереднього доступу до ЕОМ; 2) способи віддаленого доступу до ЕОМ. Існування двох принципово різних за своїм характером способів незаконного втручання в роботу ЕОМ, кожний з яких має певну специфіку, обумовлює особливості пошукової слідчої діяльності по кожному з них. 2. Інформацію латентного характеру можна одержати, вивчаючи типові способи протидії розслідуванню по розглянутій категорії справ. Основне інформаційне навантаження несе спосіб приховання слідів злочину. Приховування слідів злочину, пов'язаних з незаконним втручанням у роботу ЕОМ банківської установи, може виражатися в знищенні, утаюванні, маскуванні, фальсифікації, як традиційно досліджуваними криміналістикою способами (маскування зовнішності, дача неправдивих свідчень тощо), так і специфічними способами, пов'язаними з комп'ютерним обладнанням, програмним забезпеченням та інформацією (маскування й фальсифікація програмних продуктів, маскуванні місцезнаходження злочинця при віддаленому доступі до ЕОМ банківської установи, відновлення нормальної працездатності комп'ютера тощо). 3. Незаконне втручання в роботу ЕОМ банківської установи сьогодні в п'ять разів частіше вчинюється чоловіками, але прогностичні дані свідчать, що в майбутньому жінки зможуть їх потіснити. Більшість суб'єктів злочину мають вищу або незакінчену вищу технічну освіту, а також іншу вищу або незакінчену вищу освіту. Серед них переважають особи у віці від 20 до 40 років.

РОЗДІЛ 2. АНАЛІЗ СТАНУ ТА ТЕНДЕНЦІЇ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ЗДІЙСНЕННЯ ЗАХИСТУ ФОНДІВ, АРХІВІВ ТА БІБЛІОТЕК

2.1 Ефективність та сучасні тенденції розвитку підходів до захисту електронних фондів, архівів та бібліотек АО «ПриватБанк»

Банківська система – це не єдиний банк, що керується з одного офісу (центрального банку), а специфічна економічна та організаційно-правова структура, що забезпечує функціонування грошового ринку та економіки в цілому.

Вона покликана виконувати такі функції:

- трансформаційну;
- створення платіжних засобів та регулювання грошової маси;
- забезпечення сталості банківської діяльності і грошового ринку.

Трансформаційна функція зумовлена посередницькою місією банків. Мобілізуючи вільні грошові кошти одних суб'єктів ринку і передаючи їх різними способами іншим суб'єктам, банки мають можливість змінювати (трансформувати) строки грошових капіталів, їх розміри та фінансові ризики.

Функція створення грошей і регулювання грошової маси полягає в тому, що банківська система оперативно змінює масу грошей в обігу, збільшуючи чи зменшуючи її відповідно до зміни попиту на гроші. Іншими словами банківська система управляє пропозицією грошей.

Проблеми банківського нагляду в Україні привертають велику увагу. Це пояснюється тим, що політика Національного банку України здійснює вплив на конкретні операції банків.

Суть контролю полягає в тому, що суб'єкт управління здійснює облік і перевірку того, наскільки об'єкт управління виконує його настанови. Контроль у банках має загальноприйняті форми – попередній, поточний, наступний – та методи – економічний аналіз, перевірка та ревізія [35, С.409].

Для того, щоб банківський нагляд був ефективним, його завдання мають бути чіткими, зрозумілими всім, хто визначає економічну політику, а також тим, хто безпосередньо контролює діяльність банків. Органи банківського регулювання та нагляду передусім мають керуватися принципами розумного,

обачливого ставлення до банків, тобто вони не повинні вимагати від банків здійснення операцій, які могли б послабити їхній фінансовий стан, порушити свободу діяльності банків [27, С.10].

З метою розвитку електронного документообігу та спрощення ведення архівної справи у банківській системі України Національний банк оновив Перелік документів, що утворюються в діяльності Національного банку та банків України, із зазначенням строків їх зберігання.

Відповідний перелік затверджений постановою Правління Національного банку України від 20 червня 2019 року № 80, що набере чинності з 01 липня 2019 року.

У документі враховано пропозиції Державної архівної служби України та Міністерства юстиції України щодо вилучення типової документації (оптимізація становить 41% – 245 статей), яка міститься в Переліку типових документів.

Це дає можливість українським банкам:

- спростити процес організації ведення архівної справи;
- автоматизувати процеси систематизації та архівного зберігання документів;
- впровадити єдиний підхід під час побудови електронних архівів.

Крім того, Правління Національного банку прийняло постанову від 20 червня 2019 року № 81, якою встановлено:

- єдині правила приймання-передавання документів (справ) банків, що припиняють банківську діяльність (зокрема, виведенням з ринку яких займається Фонд гарантування вкладів фізичних осіб), на архівне зберігання до Національного банку;
- єдині стандарти щодо роботи з архівними документами таких банків.

Система захисту охоплює всі етапи розроблення, впровадження та експлуатації програмно-технічних комплексів СЕП та інформаційних задач і визначає чіткий розподіл відповідальності на кожному етапі підготовки, оброблення та виконання електронних банківських документів на всіх рівнях.

Службові особи організації, які відповідають за захист електронних банківських документів, зобов'язані надавати письмові або усні відомості про

стан засобів захисту та їх використання, а також про стан захисту інформації в програмному забезпеченні САБ (у тому числі системи "клієнт-банк", а також інших систем, на які поширюються вимоги Національного банку щодо інформаційної безпеки), технологію оброблення електронних банківських документів в організації та систему захисту інформації під час їх оброблення на вимогу Департаменту інформаційної безпеки або його регіональних підрозділів.

Організація, яка отримала засоби захисту, не має права передавати їх іншим організаціям або особам, у тому числі й іншим організаціям однієї юридичної особи.

Система захисту інформації Національного банку створена для забезпечення конфіденційності та цілісності електронної інформації, а також суворої автентифікації учасників СЕП, учасників інформаційних задач і фахівців організацій, які беруть участь у підготовці й обробленні електронних документів.

Для здійснення суворої автентифікації організації застосовується система ідентифікації користувачів, яка є основою системи розподілу ключової інформації.

Організація для забезпечення захисту інформації має трибайтний унікальний ідентифікатор, перший знак якого є літерою відповідної території, на якій він розташований, другий і третій є унікальними ідентифікаторами організації у межах цієї території.

Трибайтний ідентифікатор має бути узгоджений з адресою системи ЕП і бути унікальним для кожної організації. Трибайтний ідентифікатор організації записується в ПМГК та АКЗІ, який надається організації та не може бути нею змінений, що забезпечує захист від підроблення ключової інформації від імені іншої організації.

Трибайтний ідентифікатор організації є складовою частиною ідентифікатора ключа криптографічного захисту, що складається із шести символів, з яких перші три є ідентифікаторами організації, четвертий визначає тип робочого місця учасника СЕП (операціоніст, бухгалтер тощо) або тип інформаційної задачі, п'ятий і шостий - ідентифікатор робочого місця або відповідальної особи.

АРМ-СЕП/АРМ-НБУ забезпечує конфіденційність електронних банківських документів, що містять конфіденційну інформацію, за допомогою апаратного/програмного шифрування всіх файлів/пакетів, які обробляються.

АРМ-СЕП і АРМ-НБУ є єдиними програмно-апаратними комплексами, які забезпечують обмін електронною інформацією в СЕП та інформаційних задачах.

Організація зобов'язана виконувати системні вимоги до ПЕОМ та інструкції щодо налаштування комплексів АРМ-СЕП і АРМ-НБУ.

Основні завдання банківського регулювання та нагляду:

- забезпечення стабільності та надійності банківської системи з метою сприяння економічному піднесенню;
- захист вкладників і кредиторів банку, що передбачає захист клієнтів від неправомірної діяльності банківських установ і забезпечення професійного поведіння з клієнтами та кредиторами банку [27, С.11];
- створення конкурентного середовища у банківському секторі, завдяки якому знижуються відсоткові ставки за кредитами, підвищуються відсоткові ставки за депозитами, розширюється спектр банківських послуг, запроваджуються нові банківські технології;
- забезпечення відкритості політики та діяльності банківського сектору в цілому і в кожному банку зокрема;
- підтримання необхідного рівня стандартизації та професіоналізму в банківській системі, забезпечення ефективної діяльності банків і запровадження технологічних нововведень в інтересах споживачів банківських послуг.

2.2 Передумови удосконалення процесу захисту осіб підозрюваних у вчиненні злочинів у фінансовій сфері банку АО «ПриватБанк»

Відповідно до Концепції економічної безпеки України, економічна безпека – це спроможність національної економіки вільно й незалежно розвиватися, утримувати стабільність громадянського суспільства та його інститутів, мати достатній оборонний потенціал країни за будь-яких несприятливих умов і варіантів розвитку подій, а також здатність Української держави до захисту

національних економічних інтересів від зовнішніх і внутрішніх загроз. Складовими економічної безпеки є фінансова, енергетична, продовольча, аграрна, демографічна та інші види безпеки. Зазначені складові тісно пов'язані між собою та доповнюють одна одну. Наприклад, не може бути продовольчої безпеки без стійкого забезпечення держави фінансовими ресурсами, водночас не може йтися про продовольчу або фінансову безпеку, якщо не забезпечено енергетичну складову.

Особливе занепокоєння у правоохоронних органів викликають зловживання посадових осіб банківських установ щодо розкрадання грошей з рахунків клієнтів банку з подальшим переведенням їх на рахунки фіктивних підприємств та подальшою легалізацією через мережу «конвертаційних» центрів. Вказана злочинна схема відбувається за допомогою електронної системи дистанційного банківського обслуговування (Internet-banking, «Клієнт-Банк» тощо), яка потребує удосконалення засобів захисту. Серед основних проблем, які суттєво впливають на боротьбу зі злочинами у сфері електронного обслуговування клієнтів банку можна виділити наступні. По-перше, це системи і технології у сфері діяльності банків, що неудосконалені з точки зору інформаційної безпеки та захисту даних:

1) 5 використання користувачами комп'ютерної техніки неліцензійного програмного забезпечення, що з великою долею ймовірності може містити в собі шкідливе програмне забезпечення, яке використовується злочинцями;

2) недостатній захист комп'ютерних мереж та приватних ПК та інше. По-друге, недостатня урегульованість нормативно-правових документів щодо вимог до захищеності систем дистанційного банківського обслуговування клієнтів.

Так, багато вчених сходяться на думці, що законодавством України чітко не визначено поняття ключових термінів «кіберпростір», «кібербезпека», «кіберзахист», «кібератака», «кібервійна», «кібертерризм», «кіберзброя», а лише узагальнене поняття злочинів і правопорушень, які вчиняються з використанням комп'ютерних систем та мереж. Слід зазначити, що даний напрямок протидії злочинним посяганням на ресурси банку ще залишається недостатньо дослідженим. Зокрема, на перший погляд здається, що крадіжки з рахунків

клієнтів банку за допомогою систем дистанційного обслуговування (напр. з банківських кредитних карток) вчиняються злочинцями - «хакерами», які не мають відношення до банківської установи. Дійсно, така практика має місце. Але більш масштабні збитки для кредитно-фінансової установи мають факти, коли до подібних дій причетні представники банків. У цьому випадку і схеми злочинної діяльності більш складні, і виявити такі зловживання досить важко з огляду на закритий характер банківської діяльності та обізнаність злодіїв як якісно сховати сліди злочинів та протидіяти розслідуванню. Практика вказує, що серед обвинувачених – учасників технологій злочинного збагачення у сфері банківської діяльності за подібними категоріями кримінальних проваджень дуже рідко фігурують представники банківського сектору. Хоча, досить часто, саме завдяки їх безпосередньої участі відбувається процес несанкціонованого доступу до б рахунків клієнтів банку та подальшого розкрадання коштів. З цього приводу переважна більшість (82%) опитаних нами слідчих та оперативних працівників по боротьбі з економічною та організованою злочинністю стверджує, що на практиці довести причетність банківських службовців до подібного роду зловживань вкрай важко¹ . Труднощі, на які посилаються опитані, викликані відсутністю методичних розробок, в яких мають бути розкриті зміст злочинної діяльності працівників банку в структурі технологій злочинного збагачення, особливості розкриття та розслідування комплексу економічних злочинів у цій сфері.

Національний банк України продовжує здійснювати заходи щодо застосування єдиних міжнародних стандартів електронного документообігу та створення додаткових можливостей для подальшого впровадження безпаперових технологій у фінансовій системі України.

На сьогодні завершено дослідно-промислову експлуатацію інформаційної системи "Електронний архів Національного банку України", яка тривала з грудня 2021 року. Упровадження системи забезпечить автоматизацію основних функцій архіву, оцифрування архівних документів, легкість та зручність доступу до них працівників.

Надалі Національний банк планує поширення цієї інформаційної системи в банках і фінансових установах з метою інтеграції й поліпшення їх взаємодії з

регулятором, іншими органами державної влади. Область банківської діяльності пов'язана з осередком суттєвих матеріальних цінностей та економічних механізмів, що впливають на підприємницьку активність суб'єктів господарювання та всіх сфер економіки. Непостійність фінансової діяльності та скорочення керованості нею з боку держави значно послаблюють банківську концепцію, роблячи її дуже чутливою для протизаконних посягань [30].

У зв'язку з цим пильну увагу приділяється останнім часом саме злочинності у сфері банківської діяльності. Слід зазначити, що саме держава є головним гарантом безпеки банківської діяльності, основні функції якого можна визначити так:

1. Розвиток надійної законодавчої основи, що стабілізує банківську діяльність та її захищеність.
2. Включення безпеки банківської сфери в єдиний порядок, забезпечується у країні належними органами та установами.
3. Формування законного механізму, що координує функціонування вищезгаданих органів з діяльністю інших державних структур[5, с.115].

Національна монополія на банківську справу, перевага управлінських функцій кредитних інститутів над домашніми господарюваннями, суворе регулювання банківських угод, крім того, жорстка дисципліна, що відрізняла кредитні установи радянського етапу, вважалися умовою, що обмежує на формування злочинності у цій галузі.

Подальші кроки щодо розвитку та вдосконалення інформаційної системи "Електронний архів Національного банку України" з долученням банківської спільноти та учасників ринку небанківських фінансових послуг включатимуть:

- проведення пілотного проєкту з Укрдержархівом, Міністерством юстиції України та Мінцифри щодо взаємодії/обміну електронними архівними документами;
- вивчення можливості обміну спільно з Фондом гарантування вкладів фізичних осіб архівних документів в електронній формі на зберігання через наявні електронні канали зв'язку шляхом створення нового онлайн-модуля "Особистий кабінет фондоутворювачів";

- доопрацювання інформаційної системи "Електронний архів Національного банку України" у частині вдосконалення механізмів опрацювання та захисту архівних документів, що містять інформацію з обмеженим доступом;
- налагодження взаємодії/обміну досвідом з банками, які мають або створюють електронні архіви, а також у частині інтеграції та взаємодії з органами державної влади та установами;
- вивчення можливості спільно з банками, учасниками ринку небанківських фінансових послуг, які не мають відповідних рішень, запровадження онлайн-кабінету з доступом для передавання електронних архівних документів постійного/тривалого зберігання, а в перспективі – побудови Галузевого державного архіву Національного банку України;
- розроблення з долученням банківської спільноти та учасників ринку небанківських фінансових послуг нової редакції Правил застосування переліку документів, що утворюються в діяльності НБУ та банків України*, які поширюватимуться на небанківські установи, державне регулювання і нагляд за якими здійснює Національний банк.

Національний банк готовий дослухатися до пропозицій банківської спільноти та учасників небанківського фінансового сектору щодо розбудови та упровадження проєкту "Електронний архів Національного банку України".

Нагадаємо, у 2018 році Правління НБУ затвердило проєкт "Електронний архів Національного банку України (1 етап)" та включило його реалізацію до стратегічних цілей Стратегії Національного банку України до 2025 року та Стратегії розвитку фінансового сектору України до 2025 року.

Безліч злочинців застосовують найпростіші шахрайські схеми скоєння такого роду злочинів. До них можна віднести дзвінки клієнтам банку з проханням назвати пароль від кредитної картки чи CVV, тобто код автентифікації картки. Також, ймовірно, шахраї використовують спосіб підроблення офіційного сайту банку або ж діють від нього особи у мережі Інтернет[49].

На першому етапі організації зловмисники завантажують веб-сайт банку, проводять повний його аналіз та вносять зміни до коду сторінок, потім відбувається розміщення модифікованої версії сайту на новому веб-хостингу з

ідентичним ім'ям банку. Часто зловмисниками створюється анонімний сайт для крадіжки даних або шкідливе посилання нібито від імені співробітника банку, що веде до сторінки із зараженим програмним забезпеченням. У разі потрапляння на анонімний сайт кредитної організації зростає ризик втрати персональних ідентифікаційних даних, а також даних своїх банківської картки. При переході за зараженим посиланням діє вже інший спосіб атаки, пов'язаний із захопленням керування комп'ютером чи іншим пристроєм користувача. Вже із захопленого комп'ютера шахрай проводить незаконні трансакції, має можливість списувати кошти клієнта, а також використовувати дані для подальших злочинів.

Найбільш поширеними видами кібершахрайства, які мають місце бути у банківській сфері є:

1. «Скіммінг» (англ. *skimming* – швидко переглядати). На банкоматах або POS-терміналах у торгових точках шахраї встановлюють спеціальні пристрої, які зчитують дані з кредитних карток. За допомогою цього виду шахрайства зловмисники зчитують ПІН-код картки шляхом копіювання її магнітної смуги. Шахраї виготовляють фальсифіковану пластикову картку на основі отриманих злочинним шляхом даних. На основі отриманих даних вони виготовляють підроблену пластикову картку, при використанні якої гроші списуються з оригіналу. Для захисту від скіммінгу банкіри рекомендують використовувати картки тільки в тих місцях, які заслуговують на довіру та охороняються. Тому що камери та різні пристрої на банкоматах клієнт може просто не помітити.

2. "Фішинг" (англ. *fishing* - рибалка). Фішинг - один з різновидів соціальної інженерії, яка ґрунтується на тому, що користувач не знає основ мережевої безпеки. Злочинці отримують інформацію про картку дистанційно. Для цього шахраї, підписуючись співробітниками банку, надсилають підроблену Інтернет-сторінку банку. На ній, за допомогою різних психологічних прийомів, просять запровадити свої логін та інші конфіденційні дані, наприклад номер картки, CVV-код, Пін код. Отримуючи всю необхідну інформацію, кібершахраї отримують доступ до акаунтів та банківських рахунків.

3. Шкідливі програмні забезпечення. Найпоширеніший спосіб - це зараження комп'ютера співробітника банку шкідливим програмним

забезпеченням з метою отримати повний контроль над машиною. В даному випадку злочинець опановує цілісну банківську систему, де має можливість не тільки відстежувати, а й робити великі операції від імені користувача [46].

Аргументовані фактори збільшення поодиноких різновидів правопорушень у банківській області, які мають характер кібершахрайства, які в свою чергу завдають безпосереднього удару по банківській діяльності та безпеки клієнтів банку. Вивчено ключові проблеми забезпечення економічної безпеки в галузі банківської діяльності в умовах формування нових та збільшення старих загроз на основі розгляду сучасного стану злочинності у банківській сфері.

РОЗДІЛ 3. ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ ОСІБ ПІДОЗРЮВАНИХ У ВЧИНЕННЯ ЗЛОЧИНІВ У ФІНАНСОВІЙ СФЕРІ АО «ПриватБанк»

3.1 Розвиток системи захисту підозрюваних осіб

Банківська система є невід’ємною частиною економіки. Вона розвивається, трансформується і адаптується до тієї системи фінансових відносин, яка склалася в державі. Практична роль банківської системи визначається її участю в управлінні системою платежів і розрахунків, інвестиціях і кредитних операціях, що дозволяє банкам разом із іншими фінансовими посередниками акумулювати заощадження усіх суб’єктів фінансового ринку

Будучи найважливішою складовою фінансово-кредитної сфери держави банківська система є частиною забезпечення фінансової безпеки країни. По суті саме стан банківського сектора визначає рівень фінансово-кредитної безпеки, а тому певною мірою і рівень фінансової безпеки держави. Формування економіки ринкового типу зумовлює потребу у створенні надійного та фінансово стійкого банківського сектора до впливу зовнішніх та внутрішніх загроз в умовах посилення макроекономічної нестабільності. Одним з напрямів вирішення цього завдання є забезпечення фінансової стійкості банків.

Фінансова безпека банку передбачає такий стан банківської системи в цілому, зокрема окремого банку, який характеризується здатністю протистояти можливим зовнішнім та внутрішнім загрозам банківської діяльності для

забезпечення нормального функціонування та розвитку в умовах дестабілізуючого впливу оточуючого середовища та захищеності фінансових інтересів зацікавлених сторін. Функціонування банківського сектору пов'язане з ризиками банківської діяльності, що включають в себе не лише ризики фінансових втрат банків, але й ризики, на які наражаються пов'язані з їх діяльністю економічні агенти.

Об'єктом фінансової безпеки банків є фінансова діяльність банку в цілому та її окремі елементи:

- прибуток;
- фінансові ресурси;
- грошові потоки;
- доходи та витрати;
- фінансовий потенціал;
- валютні цінності тощо.

Суб'єктами забезпечення фінансової безпеки банку є:

- зовнішні – центральний банк, органи державної влади, фонд гарантування вкладів фізичних осіб, клієнти, контр– агенти ;
- внутрішні – власники банку, топ–менеджери та банківський персонал. Метою забезпечення фінансової безпеки банківської установи є забезпечення фінансової стійкості банку та захист його фінансових інтересів від дії зовнішніх і внутрішніх загроз та фінансових ризиків для забезпечення ефективного розвитку в поточному та довгостроковому періоді.

Усі чинники впливу на банківську систему поділяються на дві категорії (зовнішні та внутрішні) й є взаємопов'язаними. Категорія внутрішніх чинників впливу напряду залежить від ефективності управлінської системи банків, установа може здійснювати на них вплив відповідними інструментами.

Складніша ситуація із впливом зовнішніх чинників, оскільки банк не може на них впливати, а це призводить до складності їх прогнозування, врахування тощо.

Методи та інструменти усунення загроз фінансової безпеки банків можна поділити:

1)внутрішні - банк, як і будь-який інший господарюючий суб'єкт, має економічну самостійність і може самостійно вживати певних заходів, спрямованих на досягнення фінансової безпеки. До основних внутрішніх методів забезпечення фінансової безпеки банку належать:

- фінансове планування;
- фінансовий аналіз;
- фінансове регулювання;
- фінансовий контроль.

2)зовнішні - діяльність банку підлягає втручанню з боку держави, яка має інструменти впливу на діяльність банківських установ. Основними зовнішніми методами забезпечення фінансової безпеки банку є:

- банківське регулювання;
- банківський нагляд;
- банківський контроль. Основним внутрішнім методом забезпечення фінансової безпеки банку є управління фінансами – фінансовий менеджмент.

Сплеск майнових злочинів правоохоронні органи пояснюють розвитком інтернет-технологій, які дозволяють виробляти розкрадання коштів, не виходячи їх удома. Але регіональна влада прямо пов'язують зростання крадіжок із нинішньою економічною кризою. Відсутність легальних доходів часто штовхає громадян на злочин у сфері [47].

Тому досить важливо підбирати на посаді банківської сфери. не тільки кваліфікованих, а й відповідальних співробітників – знайти грамотного фінансового директора, який має позитивні відгуки від колишніх роботодавців, банківських працівників, професійні та особисті якості яких не викликають сумнівів у керівника тощо.

У наш електронний вік, коли дуже розвинена електронна культура та з'являються все більше банківських послуг та продуктів, зростає і кількість всіляких загроз та кіберзлочинів. Тому необхідна серйозна захист банківського сектора. Так, це вимагатиме чималих витрат, як із боку самих банківських структур, і держави.

Слід провести розробку пропозицій щодо вдосконалення економічної безпеки у банківській сфері з метою збільшення ефективності виявлення та припинення правопорушень. Оскільки раніше у роботі було розглянуто такий вид злочинів, як кібершахрайство, то на основі раніше проведених аналізів можна виробити ряд заходів щодо протидії даного правопорушення у сфері банківської діяльності.

3.2 Вдосконалення служби безпеки банку

Для вдосконалення діяльності служби безпеки банку з точки зору протидії кібершахрайству пропонуються такі заходи щодо підвищення економічної безпеки:

1. Розробка та створення службою безпеки банку спеціальних навчальних програм із забезпечення безпеки, зниження загроз та ризиків наступу протиправних діянь щодо використання електронних засобів платежу.

Завдяки таким програмам, до яких буде забезпечено вільний доступ лише для клієнтів банку в режимі відстеження користувачів спеціалістами служби безпеки банку, значно підвищиться рівень фінансової грамотності населення, а, отже, знизиться кількість злочинів у галузі кібершахрайства, і зрештою, підвищиться економічна безпека банку.

2. Запровадження службою безпеки проекту створення міжбанківського інформаційного ресурсу, який би забезпечував закритий канал обміну даними щодо інцидентів з платіжними картками та інформаційною безпекою. Цей проект дозволить банкам обмінюватися фактичними навичками у сфері протидії кібершахраям, а також стрімко та точно виявляти ділянки компрометації карток. Тобто. банки зможуть обмінюватися актуальною інформацією галузі комп'ютерних злочинів.

3. Розробка та впровадження службою безпеки системи збору даних про пристрій, які є своєчасним виявленням шахрайських схем в інтернет-банкінгу. Ця система повинна не тільки знижувати ризик виникнення кібершахрайства, але й виявляти всілякі факти виникнення загроз.

Розблокувати цю систему та карту можна буде у будь-якому найближчому відділенні банку, де слід заповнити певні документи та пояснити причину введення неправильних даних.

4. Виділення у службі безпеки окремих фахівців із забезпечення інформаційно-економічної безпеки, безперервного фінансового моніторингу та внутрішнього контролю з метою протидії кібершахрайству, а також зниження ризику розвитку протизаконних діянь.

5 . Забезпечення службою безпеки технічних заходів щодо захисту грошових коштів від розкрадань банку з банкоматів, які включають обладнання всіх банкоматів антискіммінгові пристрої. Дані апарати підключаються до пристрою, що регулює напругу в банкоматі, при знятті якого прийняття картки стає неможливим. Тут слід зважити на той факт, що кожен банк обирає собі пристрій, який вважає ефективним і надзатратним. На сьогодні існує маса антискімлингових пристроїв, які відрізняються один від одного виробниками, якістю, формою та ціною.

ВИСНОВКИ

Отже, ефективність банківської роботи із залучення додаткових грошових коштів та забезпечення його конкурентоспроможності на фінансовому ринку залежать від впровадження банківськими інститутами нових депозитних продуктів. Однак важливим є поєднання традиційного обслуговування клієнтів з сучасними інноваційними системами та продуктами. Постійний моніторинг, впровадження та підтримка ефективної депозитної політики дозволить підвищити надійність національних банків та розширить шляхи євроінтеграційних перетворень цілої банківської системи України. Таким чином, сучасна депозитна політика вітчизняних банків потребує постійного вдосконалення. Основними напрямками підвищення ефективності вважаємо:

1. Посилення захисту депозитних коштів фізичних та юридичних осіб, через удосконалення та посилення жорсткості у питаннях законодавчого та нормативно-правового регулювання.
2. Втілення у систему відкриття та обслуговування депозитних рахунків принцип простоти, надійності, доступності та лояльності.
3. Посилення контролю щодо правдивості, своєчасності та доступності інформації про фінансовий стан банків через контролюючі та регулюючі органи банківської системи.
4. Зміна підходу до якості обслуговування клієнтів через запровадження та оновлення сучасних нових інформаційних технологій у банківській сфері, а також підвищення кваліфікації працівників банку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрушко П.П. Проблеми кримінальної відповідальності за втручання в роботу автоматизованих систем // Правове, нормативне та метрологічне

- забезпечення системи захисту інформації в автоматизованих системах України. – К., 2000. – С. 50-53.
2. Афанасьєв А.Ю. Проблеми попередження крадіжок грошових засобів з використанням пластикових карток і інших засобів електронного доступу // – 2003. – №4. – С. 31-35.
3. Баєв О.Я. Тактика слідчих дій. – Одеса, 1992. – 208с.
4. Бажанов М.И. Кримінальне право України. Загальна частина. – Дніпропетровськ, 1992. – 166 с.
5. Банківське право України / А.О. Селіванов, В.Л. Кротюк, Л.Н. Заруденко. – К.: Видавничий дім “Ін Юре”, 2000. – 368 с.
6. Банківське право: навчальний посібник / Упорядник М.П. Кучерявенко. – Х.: Торсінг, 1999. – 784 с.
7. Банківське право: українське та європейське: навчальний посібник / П.Д. Біленчук, О.Г. Диннік, І.О. Лютий, О.В. Скороход. – К.: Атіка, 1999. – 398 с.
8. Банківська справа / Під ред. О.И. Лаврушина. – ТОО “ЭКОС”, 1992. – 428 с.
8. Баранов О.А. Кримінологічні проблеми комп’ютерної злочинності http://geocities.com/beta_fly/texts/s1.htm
9. Бахін В.П., Біленчук П.Д., Зубань М.А. Алгоритми вирішення слідчих дій. Навчальний посібник. – К.: Українська академія внутрішніх справ, 1995. – 93 с.
10. Бахін В.П., Весельський В.К. Тактика допиту. Навчальний посібник. (Серія “Навчально-практичне видання.”). – Київ: НВТ “Правник”, 1997. – 64 с.
11. Безпека комп’ютерних систем. Злочинність у сфері комп’ютерної інформації та її попередження. / ЗЮІ МВС, НАВСУ. – Запоріжжя, 1998. – 315 с.
12. Білецький В.И. Методика розслідування крадіжок грошових засобів // Криміналістика і судова експертиза: – К., 1982, – Вип. 24.
13. Біленчук П.Д., Борисова Л.В., Паніотов Є.К. Взаємодія правоохоронних органів України та країн світу при розслідуванні електронних високотехнологічних транснаціональних злочинів // Право і безпека. – 2003. – №1. – С. 54-59.
14. Біленчук П.Д. Криміналістичне дослідження обвинуваченого. – К.: УАВС, 1995. – 128 с.

15. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінологіко-криміналістичні аспекти: Навч. посіб. – К.: Українська академія внутрішніх справ, 1994. – 71 с.
16. Біленчук П.Д., Котляревський О.І. Портрет комп'ютерного злочинця: Навч. посібник. – К: В&В, 1997. – 48 с.
17. Біленчук П.Д., Романюк Б.В., Цимбалюк В.С. та ін. Комп'ютерна злочинність. Навчальний посібник. – Київ: Атіка, 2002. – 240 с.
18. Борисова Л.В. Використання спеціальних знань при проведенні розслідування злочинів у сфері комп'ютерної інформації: стан проблеми та перспективи дослідження / Сучасні судово-експертні технології в кримінальному і цивільному судочинстві: Матеріали міжнар. науково- практич. конф. (м. Харків, 14-15 березня 2003 р.). – Х.: Вид-во Нац. ун-ту внутр. справ, 2003. – С. 48-55.
19. Борисова Л.В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження: Автореф. дис. ... канд.юр.наук: 12.00.09. – К., 2007. – 16 с.
20. Буцан О.П. Криміналістична характеристика і основні положення розслідування злочинів, зкоюваних кредитними банківськими картками: Дис. ... канд. юр. наук: 12.00.09. – Х., 1995. – 210 с.
21. Васильєв А.Н. Тактика окремих слідчих дій. – 1981. – 112 с.
22. Васильєв А.Н., Яблоков Н.П. Предмет, система і теоретичні основи криміналістики. – М., 1984. – 143 с.
23. Вехов В.Б. Особливості розслідування злочинів, зкоюваних з використанням засобів електронно-обчислювальної техніки: навч.-метод, посібник. – 1998. – 72 с.
24. Вехов В.Б., Голубев В.А. Розслідування комп'ютерних злочинів в країнах СНГ / Під ред. Б.П. Смагоринського. – 2004. – 304 с.
25. Вехов В.Б., Попова В.В., Ілюшин Д.А. Тактичні особливості розслідування злочинів в сфері комп'ютерної інформації: Наук.- практ. посібник. – 2004. – 160 с.
26. Вехов В.Б. Документи на машинних носіях // Законність. – 2004. – №2. – С. 18-20.
27. Вертузаєв М., Попов А. Запобігання комп'ютерним злочинам та їх розслідування // Право України. – 1998. – №1. – С. 101.

28. Вертузаєв М.С. Проблеми взаємодії оперативних підрозділів органів внутрішніх справ зі службами безпеки банків в попередженні злочинних посягань з використанням пластикових платіжних засобів // Бизнес и безопасность. – 2002. – № 5. – С. 2-3.
29. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. Посібник / За ред. С.Г. Лаптева. – К.: Вид-во Європ.ун-ту, 2001. – 321 с.
30. Волеводз А.Г. Сліди злочинів, зкоюваних в комп'ютерних мережах – 2002. – №1. – С. 4-12.
31. Волобуєв А.Ф. Предмет розкрадання майна у сфері підприємництва як елемент криміналістичної характеристики злочинів даного виду // Вісник Одеського інституту внутрішніх справ. – 1998. – Вип.3. – С.39-43.
32. Волобуєв А.Ф. Загальні положення криміналістичної методики: Лекція. – Х., 1996. – 36 с.
33. Волобуєв А.Ф. Комплексна методика розслідування економічних злочинів // Вісник прокуратури. – 2003. – № 6 (24). – С. 53-56.
34. Волобуєв А.Ф. Особливості розслідування розкрадань грошових коштів, що здійснюються з використанням комп'ютерної техніки // Вісник Луганського інституту внутрішніх справ. – 1998. – № 2. – С. 179-185.
35. Голубєв В.О. Програмно-технічні засоби захисту інформації від комп'ютерних злочинів / Під ред. О.П. Снігерьова. – Запоріжжя, 1998. – 144 с.
36. Гончаренко В.И., Кушнір Г.А., Підпалый В.Л. Поняття криміналістичної характеристики злочинів // Криміналістика і судова експертиза. – К., 1986, – Вип. 33. – С. 15-19.
37. Гончаров Д. Кваліфікація крадіжок, зкоєних з використанням комп'ютерних технологій // Законність. – 2001. – № 11. – С. 31-33.
38. Городиський О.М. Криміналістична характеристика та основні положення розслідування злочинів, пов'язаних з приховуванням валютних цінностей: Автореф. дис. ... канд.юр.наук: 12.00.09. – Х., 1998. – 18 с.
39. Гриненко А.В., Каткова Т.В., Кожевніков Г.К., Коновалова В.Е., Шепитько В.Ю. Руководство по расследованию злочинів. Кримінальна процедура.

Криміналістична техніка. Тактика виробництва слідчих дій. Ккспертиза: Наук.-практ. Посібник. – Х.: «Консум», 2001. – 608 с.

40. Гудков Г.П. Комп'ютерні злочини в сфері економіки // Актуальні проблеми боротьби з корупцією і організованою злочинністю в сфері економіки. – М.: 1995. – С. 142- 144.

41. Гуцалюк М.С. Координація боротьби з комп'ютерною злочинністю // Право України. – 2002. – № 5. – С. 21-26.

42. Дзюблюк О.В. Організація грошово-кредитних відносин суспільства в умовах ринкового реформування економіки. – К.: Поліграфкнига, 2000. – 512 с.

43. Дідковська С.П., Клименко Н.И., Лисиченко В.К. Підготовка і проведення окремих видів судової експертизи: Навчальний посібник. – К., 1977. – 79 с.

44. Домарев В.В. Захист інформації і безпека комп'ютерних систем. – К.: ДіаСофт, 1999. – 480 с.