НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ»

Виконав: здобувач 4 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Закірко Юрій Олегович

Керівник: к.т.н., доцент
Кухаренко Сергій Вікторович

Рецензент: к.фіз.-мат.н., доцент
Черєвко Євген Володимирович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Закірко Юрію Олеговичу

1. Тема роботи: «Забезпечення захисту інформації в банківській сфері»
Керівник роботи: к.т.н, доцент Кухаренко Сергій Вікторович
затверджені наказом НУ ОЮА від «02» квітня 2024 року № 809-06
2. Строк подання здобувачем роботи «20» травня 2024 рік
3. Дата видачі завдання «15» вересня 2023 рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Забезпечення захисту інформації в банківській сфері» на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, за переліком посилань містить 21 літературне джерело. Робота виконана на 44 сторінках загального тексту та 35 сторінках основного тексту.

Метою роботи є вивчення сучасних методів та підходів до забезпечення інформаційної безпеки в банківській сфері, аналіз потенційних загроз і вразливостей, а також розробка рекомендацій щодо підвищення ефективності захисних систем. Особлива увага приділяється застосуванню інженерних заходів захисту, політикам доступу та методам криптографічного захисту даних.

У рамках дослідження були систематизовані основні категорії загроз і розроблені методи їх нейтралізації, а також представлені кейс-стадії з аналізу реальних інцидентів безпеки в банківських установах. Була розроблена модель оцінки ризиків та система моніторингу вразливостей, що дозволяє оперативно реагувати на можливі кіберзагрози.

Результати роботи можуть бути використані банківськими установами для удосконалення своїх систем інформаційної безпеки, підвищення рівня захисту клієнтських даних та фінансових активів. Рекомендації, розроблені в цій роботі, сприятимуть формуванню ефективних стратегій інформаційної безпеки, адаптованих до специфіки банківської діяльності.

Можливими напрямками подальших досліджень є розробка автоматизованих систем раннього виявлення інцидентів безпеки, вивчення міжнародного досвіду в області кібербезпеки банківських систем та адаптація найкращих практик з міжнародних стандартів безпеки до умов України.

ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЇ, БЕЗПЕКА ДАНИХ, АНАЛІЗ, БАНКІВСЬКА СФЕРА, СИСТЕМА, ВИТОК.

ABSTRACT

The qualification work on the topic "Ensuring the protection of information in the banking sector" for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, educational program: Cybersecurity, according to the list of references, contains 21 literary sources. The work was completed on 44 pages of the general text and 35 pages of the main text.

The objective of this study is to examine contemporary methodologies and approaches to information security in the banking sector. This entails the analysis of potential threats and vulnerabilities, as well as the formulation of recommendations for enhancing the efficacy of security systems. Particular emphasis is placed on the utilisation of engineering security measures, access policies, and cryptographic data protection techniques.

The study has sought to systematise the principal categories of threats and develop methods to neutralise them. Additionally, it has presented case studies of actual security incidents that have occurred in banking institutions. A risk assessment model and a vulnerability monitoring system have been developed that allows for a prompt response to possible cyber threats. The results of the work can be used by banking institutions to improve their information security systems, increase the level of protection of client data and financial assets. The recommendations developed in this paper will contribute to the formation of effective information security strategies adapted to the specifics of banking activities.

Further research may be conducted in the following areas: the development of automated systems for the early detection of security incidents; the study of international experience in the field of cybersecurity of banking systems; and the adaptation of best practices from international security standards to the conditions of Ukraine.

TECHNICAL PROTECTION OF INFORMATION, INFORMATION, DATA SECURITY, ANALYSIS, BANKING, SYSTEM, LEAK.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ – інформаційна безпека

ІББ – інформаційна безпека банку

УІБ – управління інформаційною безпекою

СУІБ – система управління інформаційною безпекою

АСУ – автоматизована система управління

ІСУ – інформаційна система управління

КС – комп’ютерна система

ОІД – об’єкт інформаційної діяльності

ТКВІ – технічний канал витоку інформації

ВСТУП

Банківська система є ключовим гравцем на фінансовому ринку, а її стабільність та ефективність є життєво важливими для розвитку національної економіки. У сучасних економічних умовах основною функцією банківського сектору є розподіл фінансових ресурсів між державою, суб'єктами господарювання та домогосподарствами з метою підтримки ключових секторів економіки.

Банківський сектор відіграє вирішальну роль у розвитку країни, концентруючи фінансові ресурси та спрямовуючи кредитні потоки у пріоритетні галузі економіки. Варто зазначити, що в Україні банківський сектор надає понад 90% усіх фінансових послуг. Операційне середовище банківського сектору було послаблене світовою фінансовою кризою, військовими подіями та несприятливим політичним розвитком, а також спадом виробництва та зниженням інвестиційної активності.

Проте банківська система України залишається ключовим гравцем у забезпеченні ефективних процесів відтворення підприємств та основним джерелом фінансових інвестицій в економіку країни. Крім того, банківська система України відіграє важливу роль у перерозподілі тимчасово вільних коштів між учасниками ринку на різних рівнях, тим самим сприяючи підвищенню конкурентоспроможності національної економіки та виступаючи ключовим фактором довгострокового зростання.

У зв'язку з цим важливо ретельно проаналізувати розвиток і стабільність банківської системи країни в поточних економічних умовах. У цьому контексті, особливе значення набуває питання інформаційної безпеки в банківській сфері. В умовах постійно зростаючих кіберзагроз та високої конкуренції на фінансових ринках, забезпечення захисту інформації стає не просто необхідністю, а критично важливим елементом стабільності та надійності будь-якої банківської системи. Враховуючи це, інформаційна безпека виступає як фундамент, на якому тримається довіра клієнтів та ефективність банківських операцій.

Отже, саме через те, що банківська сфера є одною з найголовніших гілок країни, її потрібно забезпечувати найновітнішими засобами захисту інформації та завжди їх оновлювати, щоб уникнути будь-яких атак.

Мета даної кваліфікаційної роботи є поглиблене вивчення та аналіз методів інженерного захисту інформації в контексті сучасних вимог кібербезпеки. Робота зосереджена на розробці комплексних рішень для захисту критично важливих даних у банківських організаціях, дослідженні ефективності існуючих систем безпеки та визначенні шляхів їх оптимізації. Акцент робиться на аналізі принципів технічного підходу до інформаційної безпеки та розробці методів застосування сучасних технологій захисту.

Об’єктом дослідження в роботі є процеси управління інформаційною безпекою в організаціях з використанням методів захисту інформації. Особливий акцент зроблено на використанні апаратних і програмних засобів захисту даних, включаючи шифрування, аутентифікацію та контроль доступу. Такий підхід дозволяє оцінити стан інформаційної безпеки та впровадити найбільш ефективні заходи захисту у банківську сферу.

Предметом дослідження є методи та технології інженерного захисту інформації, включаючи вивчення новітніх розробок у сфері шифрування даних, біометричних технологій та систем контролю доступу. Дослідження також включає аналіз можливостей застосування цих технологій у різних банківських системах, та оцінку їх ефективності у захисті чутливої інформації.

Практична значущість даної роботи полягає у покращенні рівня захисту інформації в організаціях через впровадження сучасних та ефективних методів інженерного захисту. Результати дослідження можуть бути використані для розробки рекомендацій по зміцненню і відновленню інформаційної безпеки, а також допоможуть формувати стратегії впровадження найновіших технологічних рішень. Ці знання будуть корисні для зміцнення захисту інформаційних систем від потенційних загроз та забезпечення їх стабільності в умовах зростаючих кібератак. Окрім того, пропозиції, розроблені на основі цієї роботи, можуть слугувати основою для законодавчих і нормативних змін у сфері інформаційної безпеки на

національному рівні. А також, їх можна використовувати для впровадження у банківські структури задля забезпечення більшої безпеки інформації в середині установи.

1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В БАНКІВСЬКІЙ СФЕРІ

1.1 Основні поняття та термінологія

Інформація – це будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

Захист інформації – це комплекс заходів, включаючи правові, адміністративні, організаційні та технічні гарантії, які забезпечують безпеку, точність і належний контроль доступу до інформації. Ці заходи впроваджуються з упевненістю та досвідом, щоб зменшити потенційні ризики та захистити конфіденційні дані.

Інформаційна безпека – це критично важливий аспект захисту життєво важливих інтересів особи, суспільства та держави. Вона необхідна для запобігання шкоди, спричиненої неповною, несвоєчасною або недостовірною інформацією, а також порушенням цілісності та доступності інформації, несанкціонованому розповсюдженню інформації з обмеженим доступом, негативному інформаційно-психологічному впливу та навмисному спричиненню негативних наслідків за допомогою інформаційних технологій. Застосовуючи ефективні заходи інформаційної безпеки, ми можемо забезпечити безпеку та захист наших цінних інформаційних активів.

Захист інформації в системі – це заходи, які спрямовані на запобігання несанкціонованому доступу до інформації, що міститься в ній.

Захист інформації поділяється на три основні складові, які є основними у кібербезпеці та сфері діяльності пов’язаній із захистом інформації:

– Доступність – це можливість одержати необхідну інформаційну послугу за прийнятий час.

Доступність є важливою складовою інформаційної безпеки, оскільки йдеться про можливість отримання необхідних інформаційних послуг у прийнятні строки. Інформаційні системи призначені для надання конкретних інформаційних послуг, і їхня нездатність може завдати шкоди всім суб’єктам інформаційних відносин. Хоча інші аспекти інформаційної безпеки є важливими, пріоритетним є

забезпечення доступності. Визнаючи її важливість, ми можемо гарантувати, що всі користувачі матимуть доступ до необхідної їм інформації.

– Цілісність – це актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни.

Цілісність є фундаментом інформаційної безпеки, особливо коли інформація слугує “керівництвом до дії”. Прикладами такої інформації є рецепти ліків, медичні процедури, специфікації та характеристики продуктів, а також хід технологічного процесу. Порушення цілісності такої інформації може мати серйозні наслідки, аж до людських жертв. Також важливо уникати викривлення офіційної інформації, чи то юридичний текст, чи то сторінка вебсервера урядової організації. Надаючи пріоритет цілісності та точності, ми можемо забезпечити безпеку та благополуччя окремих осіб і суспільства в цілому.

– Конфіденційність – це захист інформації від несанкціонованого доступу до неї.

Конфіденційна інформація присутня в багатьох організаціях, включаючи освітні установи. Наша організація зобов’язується зберігати дані про екзаменаційні питання та окремих користувачів, такі як паролі, приватними. Ми впевнені у своїй здатності підтримувати безпеку та конфіденційність цієї інформації.

Політика інформаційної безпеки банківської установи – це набір керівних принципів, що визначає ключові сфери, умови та процедури захисту інформації банку від несанкціонованого доступу. Ці настанови покликані забезпечити постійний захист інформації банку, а також усвідомлення всіма працівниками своїх обов’язків щодо підтримання безпеки цієї інформації [4].

Безпека банківської установи – це здатність банку, та його системи, протистояти спробам та діям, які можуть нанести шкоду середовищу та інтересам банку.

Заходи безпеки банківської діяльності поділяються на три групи, які мають перелік певних заходів, яких повинні дотримуватись банківські установи у своїй діяльності.

Розглянемо ці групи більш детальніше:

1. Проектні:

– оцінювання кредитоспроможності позичальників;

– дослідження рівня безпеки співпраці із клієнтами з використанням інформаційно-аналітичних методів;

– заходи комерційної розвідки.

2. Термінові:

– заходи щодо нейтралізації конкретних випадків промислового шпигунства;

– протидія недобросовісній конкуренції;

– зупинення витоку комерційної інформації.

3. Постійні загального характеру:

– співпраця з правоохоронними органами та службами безпеки;

– ретельний підбір персоналу;

– забезпечення безпеки банківських приміщень;

– захист інформації банку;

– створення позитивного іміджу банку.

Економічна безпека банківської установи – це стан захищеності захисту ресурсів, інтересів банку, його партнерів та клієнтів. Запобігаючи внутрішнім та зовнішнім загрозам, банк може забезпечити стабільну роботу та розширене відтворення з мінімальними втратами. Наша експертиза в цій сфері дозволяє нам впевнено орієнтуватися в потенційних ризиках та захищати інтереси всіх зацікавлених сторін.

DLP (Data Loss Prevention) – системи запобігання втраті даних, спрямовані на виявлення та запобігання витокам конфіденційної інформації за межі корпоративної мережі.

1.2 Основи безпеки банківської діяльності

Банківська діяльність, як одна з ключових ланок національної фінансової системи, передбачає особливо високий рівень безпеки через високий ризик обробки та збереження таємної інформації. Банківський сектор більшу частину часу працює з обробкою даних, це може бути особиста інформація клієнтів, всі види транзакцій або просто внутрішній документообіг чи стратегічне планування розвитку. Банки, як правило, мають захищену інформаційну систему, яка технічно захищена від хакерських атак [2].

В кожному банку є певна інформація, яку потрібно захищати від кіберзлочинців, а саме:

– інформація про персонал (співробітники, керівники, виконавці);

– інформаційні ресурси (інформація з обмеженим доступом, що містить конфіденційні дані, в тому числі банківську та комерційну таємницю, а також іншу конфіденційну інформацію в різних форматах);

– інформація про технології, які використовує банківська установа;

– конфіденційні електронні мережі банку;

– фінансова звітність банку та інформація щодо операцій банку;

– інформація про діяльність та фінансовий стан клієнту.

Задля збереження банківської безпеки існують основні принципи, яких дотримуються всі банківські структури. Фундаментальними принципами банківської безпеки є наступні:

– законність має першочергове значення, і всі заходи, що вживаються для забезпечення безпеки банку, повинні ґрунтуватися на чинній нормативно-правовій базі та здійснюватися без її порушення;

– ефективність також є ключовим фактором, оскільки витрати на заходи безпеки повинні бути меншими, ніж очікувані результати, і не повинні призводити до погіршення показників діяльності або безпеки банку, а також перешкоджати реалізації його інтересів;

– реалізація заходів безпеки здійснюватиметься професіоналами, які не принижуватимуть гідність і права персоналу та клієнтів;

– заходи безпеки та перевірка персоналу будуть конфіденційними та матимуть обмежений доступ;

– управління безпекою охоплюватиме всі види банківських операцій, внутрішні та зовнішні загрози, діяльність усіх структурних підрозділів;

– заходи безпеки реалізуються відповідно до стратегічних цілей та поточних завдань банку, визначених у затвердженій програмі безпеки;

– банк оперативно реагує на запобігання та нейтралізацію загроз безпеці;

– система управління безпекою побудована таким чином, щоб бути гнучкою та реагувати на зміни у зовнішньому середовищі;

– крім того, персонал банку добре навчений розпізнавати ознаки потенційних загроз безпеці [3].

1.3 Правова база забезпечення інформаційної безпеки в Україні та світі

Вкрай важливо досягти комплексного сприйняття та виконання правових інструментів, що регулюють інформаційну безпеку. У цій частині ми розглянемо ключові нормативно-правові акти, які створюють правила інформаційної безпеки, що застосовуються до українського банківського сектору, а також висвітлимо відповідні міжнародні стандарти [5].

Сфера інформаційної безпеки України базується на ключових документах, які були прийняті законодавством країни, а саме:

1. Закон України «Про інформацію» від 02.10.92 № 2657-XII, що визначає загальні засади отримання, використання та захисту інформації.

2. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, що регулює збір, обробку та захист персональних даних осіб.

3. Закон України “Про основи національної безпеки України” від 19.06.2003 № 964-IV, що включає положення про захист державної інформаційної інфраструктури.

4. Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX, що встановлює правила для забезпечення безпеки в сфері електронних комунікацій.

Завдяки цим документам формується фундамент для інформаційної безпеки України. Але з кожним роком, методи захисту інформації вдосконалюються через те, що з'являються нові методи зламів та атак, які наносять шкоду різним сферам діяльності в Україні.

На міжнародному рівні інформаційна безпека рядом є одним із головних предметів особливої уваги, що регулюється через комплекс, конвенцій, стандартів та рекомендацій, які були розроблені для створення гарантованої безпеки даних, незалежно від національних кордонів. Інформаційна безпека на міжнародному рівні регулюється такими стандартами:

– Загальний регламент про захист даних (GDPR) – це ключовий документ Європейського Союзу, який встановлює норми щодо збору та обробки персональних даних.

– Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) – міжнародний договір, спрямований на боротьбу з кіберзлочинністю.

– ISO/IEC 27001 – критично важливий міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою.

Всі ці міжнародні ініціативи та стандарти мають спільну мету: необхідно створити безпечну та надійну цифрову сферу, в якій життєво важливі дані будуть захищені, конфіденційність користувачів буде посилена, а ймовірність кіберзлочинів знижена. Формування та застосування таких стандартів є одним із ключових питань глобальної стратегії кібербезпеки, що, зрештою, змушує кожну державу, в тому числі й Україну, змінювати своє правове регулювання відповідно до високих міжнародних стандартів захисту інформації.

2 АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАХИСТУ ІНФОРМАЦІЇ У БАНКІВСЬКІЙ СФЕРІ

2.1 Системи технічного захисту інформації

Система технічного захисту інформації – це сукупність правових, організаційних і технічних заходів, спрямованих на забезпечення захисту інформації від несанкціонованого доступу, використання, розкриття, зміни або знищення. Вона включає нормативно-правову базу, інфраструктуру, матеріально-технічні засоби та інтелектуальні ресурси, необхідні для досягнення цілей захисту інформації. Система захисту інформації складається з трьох основних компонентів: нормативно-правової бази, організаційної інфраструктури та фізико-технічних засобів [6].

1. Нормативно-правова база

Нормативно-правова база включає в себе закони та нормативно-правові акти, які регулюють сферу технічного захисту інформації. В Україні до таких документів належать:

– Закони України, що регулюють загальні питання інформаційної безпеки.

– Нормативно-правові акти у сфері ТЗІ, які визначають вимоги та стандарти захисту інформації.

– Нормативні документи системи ТЗІ, які містять конкретні вказівки щодо впровадження заходів безпеки.

– ДСТУ у сфері захисту інформації, що встановлюють стандарти і вимоги до захисту інформації на різних рівнях.

2. Організаційна інфраструктура

Організаційна інфраструктура включає об'єкти захисту, органи, де здійснюється технічний захист інформації, та суб'єкти системи ТЗІ. До основних елементів організаційної інфраструктури належать:

– Об’єкти захисту, які містять конфіденційну або приватну інформацію, що потребує захисту.

– Органи, де здійснюється ТЗІ, тобто установи та відділи, відповідальні за впровадження та підтримку заходів безпеки.

– Суб’єкти системи ТЗІ, включаючи відповідальних осіб та підрозділи, які здійснюють контроль та моніторинг заходів безпеки.

3. Матеріально-технічна база

Матеріально-технічна база складається з засобів технічного захисту інформації, засобів спецзв’язку та засобів пошуку закладних пристроїв. Основні елементи цієї бази включають:

– Засоби ТЗІ, такі як системи шифрування, брандмауери, антивірусні програми та інші технічні засоби.

– Засоби спецзв’язку, що забезпечують захищену комунікацію між різними частинами організації.

– Засоби пошуку закладних пристроїв, які допомагають виявляти та нейтралізувати приховані пристрої для знімання інформації.

Для того, щоб створити ефективну систему інформаційної безпеки, необхідно виконати певні кроки, які допоможуть забезпечити загальний захист інформаційних активів організації. Цей процес включає низку загальних кроків, кожен з яких відіграє ключову роль у створенні надійної системи інформаційної безпеки:

1. Визначення й аналіз загроз для інформації: На цьому етапі здійснюється ідентифікація можливих загроз, аналіз ризиків і визначення вразливостей інформаційних систем.

2. Розробка політики безпеки та плану захисту інформації: Визначаються основні принципи та підходи до захисту інформації, формулюються політики та стратегії безпеки.

3. Розробка технічного завдання на створення системи (комплексу) захисту інформації: Документуються вимоги до системи захисту, визначаються технічні параметри та функціональні можливості.

4. Розробка проекту системи (комплексу) захисту інформації: Створюється детальний проект, який включає всі аспекти впровадження заходів безпеки.

5. Упровадження системи (комплексу) захисту інформації: Реалізуються заходи захисту відповідно до розробленого проекту, проводиться інсталяція необхідного обладнання та програмного забезпечення.

6. Оцінювання захищеності інформації (атестація, експертиза): Проводиться перевірка та оцінка ефективності впроваджених заходів, здійснюються експертні дослідження та атестація системи.

7. Введення системи (комплексу) захисту інформації в експлуатацію: Система захисту запускається в роботу, здійснюється її інтеграція в існуючі інформаційні процеси.

Після впровадження системи захисту інформації, необхідно забезпечити її постійний розвиток, оновлення та моніторинг. Це включає регулярні технічні та організаційні заходи, спрямовані на виявлення та блокування всіх можливих шляхів втечі з об'єкта. Крім того, для підтримання високого рівня безпеки необхідно постійно перевіряти нормальне функціонування та надійність технічних засобів захисту.

Іншим важливим аспектом є підготовка та навчання персоналу, залученого до захисту технічної інформації. Програми навчання та тренінгів допомагають забезпечити обізнаність персоналу про нові загрози та способи протидії їм. Це дозволить вам швидко реагувати на нові виклики та підвищити загальний рівень інформаційної безпеки у вашій організації.

Таким чином, система технічного захисту інформації – це комплексний підхід, що включає правові, організаційні та технічні заходи. Її впровадження та постійне вдосконалення забезпечує надійний захист ІТ-об'єктів від внутрішніх та зовнішніх загроз, а також зміцнює стабільність та безпеку банківської установи.

2.2 Види захисту ідентифікаційних карток

В наш час ідентифікаційні картки використовуються у багатьох сферах людської діяльності, включаючи студентський квиток, посвідчення особи, ліцензію на керування транспортним засобом, перепустку на режимні об’єкти. Вони

успішно замінили застарілі системи контролю, з їх допомогою стало можливим повністю автоматизувати систему обліку, перевірки та допуску серед організацій різних сфер діяльності та розмірів. Час на ідентифікацію співробітників скоротився до мінімуму. Ідентифікаційна картка має ряд переваг перед звичайним посвідченням особи. Однак, найбільш суттєвою перевагою є високий рівень захисту, який вона забезпечує як від підробки, так і від несанкціонованого доступу до персональної інформації. Особи, зацікавлені у створенні підроблених посвідчень особи, прагнуть бути в курсі розвитку галузі. Але приходять нові методи, якими можна зменшити ризики підробки шляхом впровадження надійних систем для друку захищених ідентифікаційних карток і використання новітніх технологій, які можуть знизити ризик підробки [7].

Старим але ефективним методом є технологія гильоше. Це використання багатобарвного малюнку з великою кількістю тонких ліній, що перетинаються, який створюється за допомогою математичного алгоритму.

Гильоше неможливо ідеально скопіювати, так само як і відбиток нашого пальцю, тому що товщина кожної лінії близько 40-70 мкм і їх кривизна постійно змінюється. Але для того, щоб забезпечити надійність ідентифікаційної картки паралельно використовують інші методи захисту.

Один з таких, є обов’язкова наявність фотографії власника карти на самій карточці. Це метод є цілком безпечним, адже використати таку картку може або її власник, або людина дуже схожа на нього. Але разом з цим приходять нові проблеми такі як зміна зовнішності протягом часу, тому і впроваджують періодичну заміну фотографій на картках, щоб вона була актуальна.

Існує дуже багато елементів захисту, як зберігають в собі зашифровану інформацію про власника. До прикладу, магнітна смужка, яка є одним за найпопулярніших методів кодування інформації на пластикових картках. За допомогою спеціальних приладів запису – кодувальник магнітної смуги, та зчитування – зчитувач магнітної смуги, на неї записують та зчитують інформацію, яка в ній міститься. Важливо зазначити, що в наш час виробляють карти з магнітними смугами HiCo (високий рівень коерцитивності) та LoCo (низький

рівень коерцитивності). Коерцітивність – це рівень магнітного поля, при якому може буде здійснений вплив на дані, зашифровані на магнітній смужці.

Також, дуже простим та популярним способом, є нумерування карток спеціальним порядковим або випадковим номером, який вноситься до бази даних інформаційної системи. Цей номер наноситься і на лицьову сторону картки, щоб його можливо було прочитати без зчитування чіпу спеціальними засобами.

Зараз почали використовувати технології захисту третього рівня, а саме нанесення на картку нанотексту, який неможливо прочитати неозброєним оком. Для того, щоб його побачити, потрібно застосовувати мікроскоп.

Також підвищує рівень захисту картки токенізація, яка замінює конфіденційні дані, такі як номери кредитних карт, унікальним ідентифікатором, або “токеном”, який не може бути використаний поза контекстом конкретної транзакції. Це значно знижує ризик використання даних зловмисниками у випадку їх витоку [8].

Значного прогресу було досягнуто в галузі технологій безпеки для ідентифікаційних карток. Процес виробництва ідентифікаційних карток тепер захищений від підробок, що фактично виключає можливість їх дублювання. На основі цього прориву державні та комерційні організації можуть створювати унікальні одно- або мультимодальні ID-картки. Комерційні організації також можуть створювати унікальні уні- або мультимодальні системи безпеки та обирати необхідний рівень безпеки. Зазвичай, посвідчення особи - це комбінація елементів усіх трьох рівнів безпеки. На це є дві причини. По-перше, чим більше елементів безпеки реалізовано в ідентифікаційній картці, тим складніше підробити таку картку. По-друге, включення унікальних елементів захисту, які відомі лише службі безпеки організації, полегшує перевірку та аутентифікацію карток.

2.3 Системи запобігання витоку інформації (DLP)

DLP (Data Loss Prevention) – це система та інші засоби, що захищають від витоків, перекривають або контролюють канали, за якими інформація може

залишити інформаційну систему, такі як мережеві з'єднання по різних протоколах, відчужувані носії інформації, мобільні комп'ютери, принтери тощо.

Банки часто не мають ресурсів і можливостей охопити всі можливі канали витоку інформації. Засоби масової інформації, які не перебувають під їхнім контролем, несуть відповідальність за значну частину ненавмисних витоків. Навмисні витоки є ще більш проблематичними. Внутрішні зловмисники, знаючи, які канали контролюються, намагаються обійти їх і передати конфіденційні дані вільним, незахищеним каналом. Отже, неповне перекриття того чи іншого параметру інформаційної системи не має суттєвого впливу на ймовірність навмисного витоку даних. Для ефективної протидії як випадковим, так і навмисним витокам, звичайно, необхідно, щоб DLP-система (підкріплена організаційними заходами) охоплювала всі без винятку канали (носії) [9].

DLP-системи засновані на аналізі потоків даних, що проходять через кордони захищеної інформаційної системи. У разі виявлення конфіденційної інформації в цьому потоці даних спрацьовує активний компонент системи та передача повідомлення (пакета, потоку даних, сесії) блокується. DLP-система, як самостійний програмний продукт, характеризується такими функціями:

– DLP-системи аналізують вихідний трафік,

– DLP-системи аналізують інформаційні потоки з використанням різних технологій.

DLP-системи також виконують глибокий аналіз змісту інформації та її категоризацію, організовують автоматичний захист конфіденційних даних в інформаційних ресурсах кінцевих точок, на рівні шлюзів даних і в статичних системах зберігання даних, а також ініціюють процедури реагування на інциденти для вжиття відповідних заходів. Комплексні DLP-системи зазвичай встановлюють на кінцевих точках, як-от робочі станції та обчислювальні сервери, і називають мережевими системами, призначеними для захисту корпоративної інформації від внутрішніх розкрадань. Існують також DLP-системи, які встановлюються на мережевому рівні і виступають як шлюзове рішення. Такі системи називаються хостовими DLP.

Типове рішення для DLP зазвичай включає сервер централізованого управління, який виконує такі функції:

– Об’єднує інші компоненти рішення в єдину систему.

– Ідентифікує дані, що містять конфіденційну інформацію.

– Створює, редагує та розповсюджує політики роботи з конфіденційними даними.

– Створює та розповсюджує інструкції для роботи з конфіденційними даними.

– Збирає, зберігає та обробляє інциденти, створює та поширює звіти.

– Надає співробітникам і співробітникам служби інформаційної безпеки рольовий доступ до управління системою.

Система DLP складається з трьох основних функцій: виявлення, ідентифікація та моніторинг. Отже:

– Виявлення – це процес виявлення конфіденційної інформації.

– Ідентифікація – це акт ідентифікації конфіденційної інформації.

– Моніторинг – це процес перевірки даних, що передаються, та виявлення порушень умов, визначених в інструкціях.

Ця функція може бути представлена різноманітними операціями. До них відносяться надсилання повідомлень у разі порушення правил безпеки, введення карантину та блокування передачі даних.

Можна казати що, впровадження систем запобігання витоку інформації (DLP) має першорядне значення для забезпечення інформаційної безпеки в банківському секторі. Оскільки кіберзагрози продовжують зростати, а інформаційні системи стають дедалі складнішими, впровадження ефективних DLP-систем є не просто захисним заходом, а стратегічною необхідністю. Ці системи не тільки допомагають банкам виявляти та запобігати несанкціонованому витоку конфіденційної інформації, але й дозволяють ретельно контролювати обробку та зберігання критично важливих даних.

Програмні рішення DLP забезпечують комплексний підхід до захисту даних, який включає моніторинг і блокування передачі конфіденційної інформації, а

також автоматизацію дотримання нормативних вимог. Такий підхід слугує зміцненню внутрішньої та зовнішньої довіри до банківської установи, знижуючи ризик потенційних фінансових та репутаційних збитків.

Успіх DLP у банківському секторі залежить від низки факторів, серед яких належна інтеграція системи в існуючу IT-інфраструктуру, адаптація політик безпеки до конкретних потреб установи та постійне навчання співробітників.

Банки, які впроваджують ці системи, повинні також забезпечити їхню адаптивність і здатність реагувати на мінливі ринкові умови та технологічні інновації. Таким чином, DLP не тільки підвищує рівень інформаційної безпеки банків, але й відіграє ключову роль у зміцненні довіри клієнтів та інвесторів, гарантуючи захист їхніх інвестицій та персональних даних у непередбачуваному цифровому світі [14].

2.4 Технічні канали витоку інформації та методи їх блокування

Технічний канал витоку інформації – сукупність джерела небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки [12].

Серед первинних джерел небезпечного сигналу на об’єкт інформаційної діяльності можемо виділити наступні:

– Технічні засоби та системи, які обробляють інформації;

– Монітори засобів електронно-обчислювальної техніки, екрани, секретні документи за надрукованим текстом, тощо, на яких відображається інформація;

– Людина, що озвучує інформацію або засоби відтворення або підсилення звуку.

Також можна виділити наступні середовища поширення небезпечного сигналу:

– Інженерні комунікації, які виходять за межі зони, що знаходиться під контролем;

– Комунікації допоміжних технічних засобів та систем (ДТЗС) та основних технічних засобів та систем (ОТЗС), що виходять за межі зони, яка знаходиться під контролем;

– Вільний простір.

Для розробки вимог та організації заходів із захисту інформації від витоків за допомогою технічних засобів виконано класифікацію таких витоків за певними критеріями. Виділено декілька основних типів технічних каналів витоку інформації (ТКВІ) залежно від:

– типу інформаційної активності в організації,

– основного принципу (фізичного ефекту чи процесу), який лежить в основі створення потенційно небезпечного сигналу,

– середовища, через яке цей сигнал розповсюджується,

– методу вилучення цього сигналу за допомогою технічних засобів військової розвідки [10].

Також, технічні канали витоку інформації поділяються за принципом функціонування та їх фізичними властивостями: акустичний; радіоелектронний; оптичний; електричний; матеріально-речовий. Розглянемо їх більш детально.

Акустичний канал – це канал витоку інформації завдяки акустичним сигналам, які надходять з носія цієї інформації за рахунок поширення механічних коливань у повітряному просторі, впливу звукових каналів на елементи й конструкції будинку, викликаючи їхню вібрацію, або впливу звукових коливань на технічні засоби обробки інформації.

Радіотехнічний канал – це найбільш інформативний канал, в якому носієм інформації є електромагнітне поле або електричний струм. Середовищем розповсюдження інформації через цей канал є атмосфера, безповітрянний простір та різні типи електричних проводів.

Оптичний канал – це канал в якому виток інформації утворюється випромінюванням, перевипроміннюванням та відбиванням в інфрачервоній, видимій та ультрафіолетовій областях спектру.

Електричний канал – це виток інформації за рахунок перехоплення магнітного поля, паразитної генерації, взаємних впливів, електромагнітних випромінювань, високочастотного нав’язування високочастотних засобів.

Матеріально-речовий канал – це збір інформації за допомогою обробки інформації одержуваної з різних відходів трудової діяльності об’єкта. Відходи можуть.

Щоб уникнути витоку інформації через усі можливі ТКВІ існує багато новітніх методів, які зараз використовують підприємства та держустанови. Для цього існує такий термін як технічний захист інформації (ТЗІ) або комплексний система захисту інформації (КСЗІ).

Способи захисту інформації поділяються умовно на три види: організаційний; інженерно-технічний; криптографічний.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі налаштування та експлуатації системи для забезпечення певного рівня інформаційної безпеки.

Відповідно до законів і нормативних актів, міністерства і компанії створюють спеціальні служби безпеки для захисту інформації. Ці служби зазвичай підпорядковуються керівництву установи. Керівник служби організовує створення та функціонування системи захисту інформації. Керівництво організації несе повну відповідальність за стан інформаційної безпеки.

На організаційному рівні вирішуються такі завдання щодо забезпечення інформаційної безпеки системи:

- Організація розробки систем інформаційної безпеки;
- Обмеження доступу до обладнання та системних ресурсів;
- Планування заходів;
- Підготовка документації;
- Навчання та тренінги обслуговуючого персоналу та користувачів;
- Атестація засобів захисту інформації;
- Авторизація діяльності у сфері інформаційної безпеки;
- Удосконалення систем захисту інформації;

– Оцінка ефективності системи захисту інформації;

– Перевірка дотримання встановлених правил експлуатації системи.

Організаційні методи є основою комплексної системи захисту інформації. Тільки за допомогою цих методів технічні, інформаційні та криптографічні засоби захисту інформації можуть бути об’єднані в комплексну систему на правовій основі.

Інженерно-технічний захист інформації – це діяльність, спрямована на запобігання порушенню цілісності, блокуванню та/або витоку інформації через технічні канали, та забезпечується комплексом програмних, технічних, організаційних та конструкторських заходів на всіх етапах їх створення й експлуатації.

Основними методами та засобами технічного захисту інформації з обмеженим доступом, що міститься в автоматизованих системах та комп’ютерній техніці, є

– використання захищених пристроїв;

– регламентація роботи користувачів, технічного персоналу, програмного забезпечення, елементів баз даних та конфіденційних носіїв інформації (розмежування доступу);

– регламентація архітектури автоматизованих систем та комп’ютерної техніки;

– проектування та забезпечення комунікаційних структур і пристроїв для функціонування автоматизованих систем та ІТ-обладнання;

– пошук, виявлення та блокування закладних пристроїв.

Криптографічний захист інформації – це вид захисту конфіденційної інформації, розголошення якої завдає (або може завдати) шкоди державі, суспільству чи особі. Здійснюється шляхом перетворення інформації з використанням спеціальних (ключових) даних для приховування (або відновлення) змісту інформації, перевірки її автентичності, цілісності, авторства тощо.

До засобів криптографічного захисту інформації належать апаратні, програмні та програмно-апаратні комплекси і кластери, які реалізують

криптографічні алгоритми перетворення інформації; захищають від нав’язування неправдивої інформації, у тому числі від засобів ідентифікації особи та електронного цифрового підпису; призначені для виготовлення та розповсюдження ключових документів, що використовуються в засобах криптографічного захисту інформації, незалежно від виду носія, на якому використовується ключова інформація [11].

Отже, існує дуже багато технічних каналів витоку інформації, але у нашій реальності вже з’явилось дуже багато способів захисту цієї інформації від її витоку та потрапляння у руки зловмисника. Саме для того, щоб конфіденційна інформація знаходилась у безпеці, потрібно завжди оновлювати засоби захисту інформації на актуальні зразки та використовувати тільки найновітніші технології, які в свою чергу повинні мати відповідні сертифікати.

3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СФЕРІ

3.1 Аналіз систем захисту на прикладі ПриватБанку

Для прикладу аналізу систем захисту інформації візьмемо систему технічного захисту інформації державного банку України – «ПриватБанк».

Сучасні банківські системи використовують у фізичних відділеннях найсучасніші методи захисту інформації, а у онлайн застосунку найбезпечніші методи аутентифікації.

В цій банківській системі володільцем персональних даних користувачів є АТ КБ «ПриватБанк» – банківська установа, якає зареєстрована в Україні. Для того, щоб користуватися їхніми послугами, споживач повинен надати свої дані, які цей банк обробляє. Серед них наступні:

– контактні дані: прізвище, ім’я та по батькові, контактний номер телефону, адреса електронної пошти;

– дані для оподаткування заохочень: паспортні або ID-дані, ідентифікаційний номер платника податків;

– дані переможців акції: повне ім’я та фото або відео переможця/переможців;

– дані для надсилання заохочень: поштова адреса (місто, вулиця, квартира, індекс).

Але для того, щоб банк здійснив обробку персональних даних повинна бути мета та підстава, які поділяються на групи [12]:

Правочин:

– надання клієнту можливості долучитися до участі у відповідній акції;

– зв’язок із переможцем (переможцями) акції;

– вручення (надсилання) заохочень.

Законні інтереси:

– публікація фото або відео переможця (переможців) акції;

– протидія шахрайству;

– забезпечення та покращення якості проведення акцій, розробка нових, надання доказів про спілкування з вами;

– аналіз аудиторії;

– знеособлення персональних даних;

– узагальнення статистики.

Закон:

– оподаткування заохочень.

Згода:

– надсилання вам повідомлень на електронну пошту щодо проведення нових акцій.

Варто розуміти, що банк може розповсюджувати конфіденційну інформацію своїх користувачів. Тому, існують деякі випадки, які прописані у політиці конфіденційності, коли банк може передати персональні дані третім особам:

1. Безпека, законні підстави, виконання закону. Передання персональних даних третім особам здійснюється з метою виконання офіційних вимог органів державної влади та місцевого самоврядування в межах їхньої компетенції, судового рішення чи відповідного закону, захисту банк від скарг третіх осіб без шкоди для ваших прав і свобод, сприяння попередженню та розслідуванню незаконних діянь, зокрема й шахрайства [16].

2. За вашою згодою. Умови та строк передання має бути обумовлено такою згодою.

3. Послуги третіх осіб. Час від часу банк може користуватися послугами третіх осіб для обробки персональних даних.

Кожен банк повинен використовувати комплекс систем захисту інформацій, який спрямовано на банківський сектор. Саме для цього було створено та затверджено Постанову «Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України» від 02.04.2007 № 112, яка визначає правила організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України [19].

Отже, захист інформації у ПриватБанку відбувається за допомогою певних систем, які діляться на відповідні категорії. Головною метою яких є захист інформації щодо електронних документів на переказ від несанкціонованого доступу, спотворення або знищення, та унеможливлення здійснення протиправних дій щодо інформації та інформаційних систем обслуговуючим персоналом.

Головними об’єктами такого захисту є:

– електронні документи на переказ та їх архіви;

– інформаційні повідомлення між Платіжною організацією, розрахунковим банком, операторами послуг платіжної інфраструктури, учасниками платіжної системи та іншими суб’єктами переказу коштів;

– інформація з обмеженим доступом, що зберігається в базах даних платіжної системи та резервних копіях;

– інформація про платників та отримувачів переказів;

– засоби оброблення та захисту інформації (програмно-технічні та криптографічні);

– серверне та мережеве обладнання задіяне для переказу коштів;

– криптографічні ключі, паролі та інша конфіденційна інформація, яка використовується для авторизації програмно-технічними засобами та користувачами.

Варто почати з оболонки, а саме заходів захисту з охорони приміщень, в яких знаходиться все серверне та мережеве обладнання, задіяне для переказу коштів в платіжній системі. Тому, це обладнання повинне знаходитись в приміщеннях дата-центрів та відповідати таким вимогам [16]:

– обладнання розташовано в окремій серверній стойці, яка зачиняється та опечатується;

– фізичний доступ до серверного та мережевого обладнання мають лише відповідальні за інформаційну безпеку особи;

– в приміщеннях з обладнанням ведеться цілодобове відеоспостереження;

– приміщення обладнане автоматизованою системою протипожежного захисту;

– приміщення знаходиться під цілодобовою охороною;

– серверне та мережеве обладнання забезпечене основним та резервним безперебійним живленням.

На програмному та апаратному рівні інформація захищається засобами мережевої безпеки. Ці інструменти забезпечують захист:

– серверного обладнання, що задіяне для переказу коштів в платіжній системі;

– внутрішніх мережевих сервісів;

– робочих місць адміністраторів;

– програмних застосунків на серверах та робочих місцях працівників.

Для запобігання порушень інформаційної безпеки та уникнення кіберінцидентів вживаються наступні заходи:

– встановлюється чіткий розподіл прав доступу до засобів захисту мережі, серверів та застосунків;

– всі технічні, службові та фінансові операції протоколюються шляхом ведення журналів реєстрації;

– забезпечується можливість відновлення до робочого стану всіх мережевих засобів захисту інформації та серверного обладнання у випадку збоїв.

Також, потрібно зазначити, що у банківську систему було впроваджено низку систем та механізмів, які забезпечують безпечне функціонування банку та захищене зберігання конфіденційної інформації. Серед них можна виділити наступні засоби захисту:

– засоби захисту мережі;

– антивірусних захист;

– криптографічні засоби захисту інформації;

– система керування ключами;

– вимоги до паролів;

– захист інформаційних систем;

– система багатофакторної автентифікації;

– захист архівів електронних документів.

Було виділено найосновніші методи, які використовую даний банк для захисту персональних даних своїх користувачів, але насправді їх значно більше, та з часом вони вдосконалюються та змінюються, для того, щоб забезпечити максимальну безпеку своїм користувачам.

3.2 Порівняння оцінки ефективності існуючих систем в інших банках

У сучасному світі, де кіберзагрози набувають все більшої складності та різноманітності, банківські установи виступають одними з найбільш привабливих цілей для кіберзлочинців. Підібравши та впровадивши найефективніші системи управління інформаційною безпекою в сучасні іноземні банки, важливим наступним кроком є оцінка їхньої ефективності в реальних умовах експлуатації. На цьому етапі ми прагнемо зрозуміти, наскільки впроваджені заходи відповідають поставленим цілям та чи вдається їм забезпечити необхідний рівень захисту критично важливих активів банку. Вивчення та аналіз зібраної інформації допоможе виявити потенційні прогалини в системах безпеки та внести корективи для подальшого зміцнення захисних механізмів.

Заходи іноземних банків включаються в себе низку переваг, від тренінгу персоналу до новітніх систем проти шкідливого впливу, кожна з яких, виконує свою роботу та захищає банк в своєму секторі. Задля покращення безпеки банку, варто використовувати весь комплекс спеціальних систем для захисту, тому що при окремому їх використанні банківська система не отримає потрібний результат [13].

Одним із найважливіших заходів є розмежування доступу для співробітників. Ця процедура дозволяє не тільки мінімізувати ризики несанкціонованого доступу до конфіденційної інформації, але й забезпечує дотримання принципу найменших привілеїв, згідно з яким співробітники отримують доступ лише до тих ресурсів, які необхідні для виконання їхніх робочих завдань. Такий підхід значно знижує ймовірність випадкових або умисних дій, які можуть призвести до витоку даних або інших безпекових інцидентів.

Крім того, систематичний перегляд та оновлення політик доступу є критично важливим для адаптації до змін у структурі компанії, змін у робочих процесах чи під час впровадження нових технологій. Це також включає ретельне відстеження і документування всіх присвоєнь, змін та анулювання прав доступу, що допомагає підтримувати високий рівень прозорості та контролю над мережевими ресурсами та даними.

Для розмежування доступу банки використовують Active Directory (AD), що є ключовим компонентом інфраструктури банку, що дозволяє централізовано управляти користувачами, групами, доступом до ресурсів та безпековими політиками. Оцінка ефективності AD полягає у перевірці здатності системи виконувати надійну аутентифікацію та авторизацію користувачів, а також у забезпеченні дотримання політик безпеки через Group Policy Objects (GPOs). Важливим є регулярний аудит і моніторинг подій AD для виявлення несанкціонованих дій або політик, що не відповідають стандартам безпеки.

Використання системи захисту електронної пошти банку допомагає банку ефективно фільтрувати спам, блокувати фішингові атаки та запобігати поширенню шкідливого програмного забезпечення. Ефективність такої системи оцінюється через здатність виявляти та блокувати зловмисні листи, а також через швидкість реагування на нові види електронних загроз. Регулярне тестування за допомогою контрольних фішингових атак та аналіз відповідей системи на такі інциденти можуть допомогти оцінити рівень її підготовки.

Використання комплексної політики BYOD в іноземних банках сприяє не тільки підвищенню продуктивності та зручності для співробітників, але й забезпечує необхідний рівень безпеки для захисту від внутрішніх та зовнішніх загроз, підтримуючи цілісність та конфіденційність корпоративних даних.

Network Operations Center (NOC) виділяється тим, що відіграє важливу роль у забезпеченні стабільності та безперебійності мережевих послуг. Оцінка ефективності NOC включає аналіз часу реагування на інциденти, ефективність виявлення та виправлення помилок, а також здатність системи прогнозувати потенційні проблеми перш, ніж вони вплинуть на операційну діяльність.

Моніторинг та аналіз логів мережі, використання систем виявлення і запобігання вторгненням допомагають визначити надійність цієї системи.

Іноземні банки також часто впроваджують інноваційні підходи до кібербезпеки, які можуть значно покращити безпеку банківської установи:

1. Використання штучного інтелекту та машинного навчання: Іноземні банки активно використовують штучний інтелект для виявлення аномалій і загроз у реальному часі. Машинне навчання допомагає прогнозувати можливі атаки і вчасно на них реагувати.

2. Розширене шифрування даних: Крім стандартних методів шифрування, деякі банки впроваджують технології квантового шифрування, які забезпечують вищий рівень безпеки і стійкість до сучасних методів злому.

3. Проведення кібервійськових навчань: Регулярні тренування та симуляції кібератак допомагають банкам підвищити готовність до можливих загроз та перевірити ефективність своїх систем безпеки в умовах, близьких до реальних інцидентів.

4. Інтеграція багатофакторної автентифікації (MFA): Використання додаткових факторів автентифікації, таких як біометричні дані або апаратні токени, значно підвищує рівень безпеки доступу до систем і даних.

5. Побудова розподілених систем безпеки: Деякі банки створюють розподілені системи безпеки, що дозволяє забезпечити захист даних навіть у випадку компрометації окремих компонентів системи.

Варто виділити залучення працівників до процесу забезпечення кібербезпеки, що це є важливим фактором оцінки ефективності заходів безпеки. Інформаційні сесії, тренінги, семінари з кібербезпеки та регулярне тестування готовності персоналу до дій в умовах можливих кібератак є важливими для підвищення загального рівня обізнаності та підготовки кожного працівника. Дотримання такої політики сприяє створенню культури безпеки в організації, яка є невід’ємною складовою захисту від внутрішніх загроз і людських помилок [15].

Насправді оцінити ефективність проваджених заходів без доступу до них дуже важко, але основним заходом для поліпшення безпеки будь-якої установи є

постійне оновлення систем безпеки для того, щоб банківська система завжди була готова до нових викликів та кібератак. Тому вкрай важливо впроваджувати систематичний процес аудиту та аналізу, який не лише виявляє потенційні слабкі місця в системі безпеки, але й планує необхідні оновлення та вдосконалення. Постійний перегляд політики безпеки та технологій, що використовуються банком, дозволяє адаптуватися до нових загроз і змін у сфері кіберзлочинності. Особливо важливо звернути увагу на криптографічний захист, системи виявлення та запобігання вторгненням і захист від шкідливого програмного забезпечення, оскільки вони є фундаментальними елементами оборонного периметра банку від зовнішніх атак.

У час постійного розвитку кіберзагроз банкам необхідно не лише регулярно оновлювати та модернізувати свої системи безпеки, але й оцінювати ефективність цих заходів на основі реальних інцидентів та поточних загроз. Такий підхід забезпечує більшу гнучкість та адаптивність системи безпеки банку, дозволяючи йому своєчасно реагувати на загрози, а також передбачати потенційні майбутні загрози та відповідно коригувати стратегії захисту.

3.3 Розробка та впровадження системи інформаційної безпеки в банку

Провівши аналіз та порівняння систем, які використовують найсучасніші іноземні банки та банки, що знаходяться в Україні, я можу запевнити, що наші банки не є достатньо захищеними від витоку інформації.

З метою удосконалення вимог до захисту інформації в інформаційних системах банківських установ з урахуванням актуальних кіберзагроз, установлення вимог щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту банків, було затверджене Постанову «Про організацію заходів із забезпечення інформаційної безпеки в банківській системі» від 28.09.2017 № 95 [17].

Також, задля поліпшення безпеки за допомогою криптографічного захисту було затверджено Постанову «Про затвердження Положення про використання

засобів криптографічного захисту інформації Національного банку України» від 14.04.2023 № 49 [21].

Ці два документи, встановлюють обов’язкові мінімальні вимоги щодо організації заходів із забезпечення інформаційної безпеки та кіберзахисту, принципи управління інформаційною безпекою, та вимоги до інформаційних систем банку [17]. А також, визначає порядок використання засобів криптографічного захисту інформації Національного банку України банками України та здійснення контролю за їх використанням [21].

Вони значно полегшують розробку системи управління інформаційною безпекою в банківський сфері, але, на мій погляд, не є досконалими. Ці документи лише визначають порядок забезпечення мінімальної інформаційної безпеки, але не дуже надійної, тому що кожного дня зростає кількість кібератак саме на банківський сектор за допомогою найновітніших методів зламу.

Система управління інформаційною безпекою (СУІБ) – це системний підхід до розробки, впровадження, функціонування, моніторингу, підтримки та вдосконалення інформаційної безпеки банку для досягнення його бізнес-цілей [18].

Ціллю інформаційної банківської безпеки є збереження конфіденційності, цілісності, доступності та захист інформації від внутрішніх та зовнішніх загроз [20].

Як ми визначили, існує багато рішень, які рекомендуються для провадження в інфраструктуру банківських систем для виконання вимог Постанови НБУ. Проаналізувавши методи та системи, які використовують іноземні банки, та провівши порівняння з методами, що використовуються нашими банками, можна зробити наступні висновки:

Банківські установи, що знаходяться в нашій країні, є достатньо захищеними, але кожного дня з’являються нові методи зламу, які використовують кіберзлочинці для зламу та отримання конфіденційних даних з банків.

Також, можу запевнити, що іноземні банки технічно більш захищені він потенційного зламу, тому мною були створені пропозиції щодо впровадження нових технічних систем захисту інформації в українські банки, які вони, наразі, не

використовую, та які значно зміцняють безпеку в їхньому інформаційному середовищі. Серед них я виділю наступні:

– Додаткові фактори аутентифікації, серед яких потрібно впровадити апаратні токени та авторизацію через біометричні дані. Інтегрування саме цих факторів значно покращує безпеку серед персоналу та перешкоджає несанкціонованому доступу.

– Захист від шкідливого коду – це комплекс заходів і методів з метою запобігання, виявлення, аналізу та видалення шкідливого програмного забезпечення, яке може завдати шкоди інформаційним системам або викрасти дані.

– Система запобігання атакам (IPS) по всьому периметру мережі банку є критично важливою складовою інформаційної безпеки банку, оскільки вона активно моніторить мережевий трафік і вживає заходів для запобігання потенційних атак ще до того, як вони завдадуть шкоди мережі або даним. Розгортання IPS по всьому периметру мережі банку забезпечує безперервний захист від широкого спектру загроз, включаючи хакерські атаки, шкідливе програмне забезпечення, віруси, спроби фішингу та інші форми кібератак.

– Система захисту електронної пошти (Webmail Security) є важливим елементом безпеки, тому що велика кількість кібератак здійснюється за допомогою фішингу або шкідливих електронних листів. Ефективна система безпеки електронної пошти забезпечує захист від широкого спектру загроз, включаючи шкідливе програмне забезпечення, спам і фішинг, а також допомагає зберегти конфіденційність і цілісність надісланої інформації.

– Контроль використання змінних носіїв – елемент політики кібербезпеки будь-якої організації фінансового сектору. Ці засоби контролю включають низку заходів і технологій для управління та моніторингу використання портативних пристроїв зберігання даних, таких як флешки, зовнішні жорсткі диски, оптичні диски та інші знімні носії інформації, які можуть становити загрозу для безпеки корпоративної інформації.

– Контроль мобільних пристроїв BYOD (Bring Your Own Device) є фундаментальним аспектом корпоративної безпеки, особливо у банківській сфері,

де доступ до конфіденційної інформації через особисті пристрої може збільшити ризики витоку даних та кібератак. Політика BYOD дозволяє співробітникам використовувати особисті пристрої для виконання робочих завдань, але вимагає ретельного контролю та управління цими пристроями для забезпечення безпеки корпоративних ресурсів.

Впровадження цих систем, може надати українським банківським установам більшої безпеки та зможе гарантувати кращу захищеність від витоку інформації. Але для того, щоб вдосконалити безпеку від подальших загроз, які будуть створені у найближчому майбутньому за допомогою штучного інтелекту, потрібно створити оболонку і для таких загроз.

На мою думку, для загроз з якими, у майбутньому, може зіткнутися банківський сектор, потрібно заздалегідь розробити спеціальну оболонку, яка буде допомагати в боротьбі з потенційними загрозами, створеними штучним інтелектом та машинного навчання. Для таких загроз, я вважаю що потрібно використовувати такі методи:

– Використання штучного інтелекту та машинного навчання, які здатні аналізувати великі масиви даних, виявляти аномалії та швидко реагувати на потенційні загрози. Основними перевагами є підвищення роботи персоналу, автоматичне виявлення та реагування на загрози, прогнозування цих загроз, та аналіз великих обсягів даних.

– Розширене шифрування даних, де використовується квантове шифрування, що забезпечує високий рівень безпеки та стійкість до сучасних методів злому.

– Проведення кібервійськових навчань, яке дозволить банкам не лише перевірити готовність своїх систем і персоналу до відбиття атак, але й відпрацювати ефективні стратегії реагування на інциденти.

– Децентралізація систем безпеки, що передбачає розподіл функцій захисту між різними компонентами та локаціями, що знижує залежність від єдиного центрального вузла. Це забезпечить вищу стійкість до атак, оскільки компрометація одного вузла не призводить до компрометації всієї системи.

Переваги децентралізації включають підвищену надійність та доступність, масштабованість, краще управління ризиками, а також підвищену безпеку завдяки розподіленому зберіганню та обробці даних, що ускладнює доступ зловмисників до всієї інформації.

На мою думку, за допомогою впровадження всіх вищезазначених механізмів, можна досягти надійної безпеки даних, що знаходяться на серверах або в системі банківської структури. Використання цих систем не дасть змоги кіберзлочинцям миттєво отримати потрібну інформацію, а персоналу – набагато більше часу на реагування та нейтралізацію цієї загрози.

Дуже важливо, щоб система управління інформаційною безпекою включала передові технології та практики, які застосовуються в усіх аспектах банківської діяльності. Інтеграція з автоматизованими системами реагування на інциденти дозволяє банку оперативно реагувати на загрози, тим самим мінімізуючи потенційні збитки.

Окрім технічних засобів, важливим аспектом захисту банку є розробка та впровадження суворої політики безпеки, яка регулює доступ до інформації та ресурсів банку. Це передбачає встановлення політики мінімальних привілеїв для доступу до систем і даних, багатофакторну автентифікацію для доступу до критично важливих систем, а також регулярне навчання співробітників з питань кібербезпеки.

Саме для того, щоб отримати дані результати дослідження, було проведено аналіз та порівняння систем інформаційної безпеки, які використовуються у світових банках. Тепер завдяки цьому ми можемо бути впевнені, що системи, які використовують наші банки, є актуальними від нинішніх загроз. Але, щоб створити надійний захист від майбутніх загроз, потрібно провести велику роботу та впровадити нові системи для поліпшення безпеки.

ВИСНОВКИ

У час стрімкого розвитку кіберзагроз діяння кіберзлочинців стало частіше припадати на фінансові сектор країни. Кожного дня, банки стають віч-на-віч з новими випадками хакінгу та загрозами, які перешкоджають нормальній роботі банку. Але основною проблемою сучасних кібератак є виток конфіденційної інформації, що зберігається у банківських установах.

З початку повномасштабної війни, банківські установи почали активніше розвиватись та все більше використовуватись населення задля допомоги армії. Але злочинці не стоять на місці, та постійно намагаються атакувати цей сектор аби отримати нову інформації про державу, армію та користувачів, яку згодом використовують вкрадені дані для того, щоб дезорієнтувати населення країни, а ще гірше – завдати матеріальної шкоди банку та його користувачам.

Саме для того був проведений великий аналіз потенційних загроз та методів за допомогою яких, банківський сектор може боротися з кіберзлочинністю у нелегкий для нас час.

Під час виконання кваліфікаційної роботи було проведено дослідження та аналіз різноманітної інформації щодо сучасних підходів та методів захисту інформації, що є одним із завдань та метою даної роботи.

Під час виконання роботи було проаналізовано нормативно-правове забезпечення у сфері захисту інформації та визначено основні загрози, які порушують основні властивості інформації (цілісність, конфіденційність, доступність).

Провівши аналіз усіх можливих систем захисту інформації, які ми можемо інтегрувати у банківський сектор, було визначено, що основними та найефективнішими методами є навчання персоналу, використання штучного інтелекту та машинного навчання. Зараз, ці три методі, активно використовують та впроваджують іноземні банки для покращення безпеки установи, та позитивно відгукуються про них.

Таким чином, можна стверджувати, що банківський сектор потребує постійного оновлення систем безпеки і моніторингу нових загроз для того, щоб бути готовими до нових викликів, які можуть статися у будь-який момент. А також, потрібно завжди впроваджувати найновітніші методи для запобігання та блокування майбутніх загроз. Але потрібно розуміти, що ніхто не може гарантувати стовідсоткову безпеку, тому що наразі основним ворогом будь-якої системи є технології, які стрімко зростають, поновлюються та розвиваються.

Тільки за допомогою людей, що розуміються на своїй роботі та мають нестандартне мислення, можливо подолати загрози, які приносять великі втрати для кожного з нас.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про інформацію : Закон України від 02.10.1992р. № 2657-XII. Дата оновлення 27.07.2023р. № 3005-IX. URL: https://zakon.rada.gov.ua/laws/show/2657-12
2. Банківська система України та її роль у розвитку реального сектору економіки. 2021. 32 с. URL: http://bit.ly/3ywpZJa
3. Теслюк С.А., Матвійчук Н.М., Левчук А.О. Фінансова безпека банківських установ в умовах цифровізації. [Електронний ресурс]: електронний журнал. Волинський нац. ун-т. Луцьк, 2024. 9 с. Режим доступу: https://doi.org/10.32782/2524-0072/2024-60-117
4. Ситник Н.С., Стасишин А.В., Блащук-Девяткіна Н.З., Петик Л. О. Банківська система. [Електронний ресурс]: навчальний посібник. Львів, 2020. – 291 с. Режим доступу: https://bit.ly/4bxvxSF
5. Нашинець-Наумова А.Ю. Інформаційне право Питання правового регулювання. [Електронний ресурс]: навчальний посібник. Київ, 2020. – 136 с. Режим доступу: https://bit.ly/4dYh83u
6. Луценко В. М., Прогонов Д. О. Методи та засоби технічного захисту інформації. [Електронний ресурс]: опорний конспект лекцій. КПІ ім. Ігоря Сікорського, Київ, 2021. – 289 с. Режим доступу: https://ela.kpi.ua/handle/123456789/42397
7. Піперков Д.А., Несторенко Т.П. Роль інформаційно-телекомунікаційних технологій у розвитку банківських систем України та Польщі/ під ред. Калініченко К.К., Устіловська А.С., Бредіхін В.М., Тодріна І.В.: Харківський нац. ун-т буд. та арх., 2021. С.94–96.
8. Азізова К.М. Інформаційні системи та технології в банківській сфері. [Електронний ресурс]: методичні рекомендації. Харківський нац. економ. ун-т. ім. С. Кузнеця, Харків, 2021. 42 с. Режим доступу: https://bit.ly/4bpIIVz
9. Ткачук Л.М., Леонтьєв І.В. Методи захисту українських банків від кібератак. URL: https://bit.ly/3VeGlzh

10. Чобаль О.І., Трикур І.І., Самохвалов М.П., Різак В.М. Методи і засоби захисту інформації. [Електронний ресурс]: лабораторний практикум. Ужгород, 2023. – 80 с. Режим доступу: https://bit.ly/4bvU22z
11. Ситайло Р. В. Блокування каналів витоку інформації. URL: https://prezi.com/p/i1cjl4jpqqar/presentation
12. Канали витоку інформації. *Матеріал з вікіпедії – вільної енциклопедії.* URL: https://uk.wikipedia.org/wiki/Канали_витоку_інформації
13. Порядок захисту персональних даних та приватності. URL: https://newpromos.privatbank.ua/zakhyst_personalnykh_danykh
14. Стратегія інформаційної безпеки банку. URL: https://my-itspecialist.com/banks-information-security-strategy
15. Усік П.С., Буравченко К.О. Безпека банківських систем. [Електронний ресурс]: навчальний посібник. Кропивницький, 2022. – 195 с. Режим доступу: https://bit.ly/3wTSdxb
16. Типовий опис системи захисту інформації в правилах платіжної системи, платіжною організацією якої є резидент. URL: https://bank.gov.ua/admin_uploads/article/Tipovij_opis_PS_rezident.pdf
17. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України : Постанова від 28.09.2017р. № 95. URL: https://zakon.rada.gov.ua/laws/show/v0095500-17
18. Політика інформаційної безпеки акціонерного товариства «БАНК 3/4». URL: https://bank34.ua/bezpeka-obslugovuvannya/politika-informacijnoi-bezpeki.html
19. Про затвердження Правил організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України : Постанова від 02.04.2007р. № 112. URL: https://zakon.rada.gov.ua/laws/show/z0419-07
20. Про затвердження нормативно-правових актів з питань інформаційної безпеки : Постанова від 26.11.2015р. № 829. URL: https://zakon.rada.gov.ua/laws/show/v0829500-15

21. Про затвердження Положення про використання засобів криптографічного захисту інформації Національного банку України : Постанова від 14.04.2023р. № 49. URL: https://zakon.rada.gov.ua/laws/show/v0049500-23