Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: «Дослідження методів конфіденційності та цілісності даних в банківській сфері»

Виконав(ла): студент(ка) IV курсу, групи СБс-41
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

		Шиндеровьский С.В.
	(підпис)	(прізвище та ініціали)
Керівник		Стадник М.А.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Лобур Т.Б.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Загородна Н.В.
	(підпис)	(прізвище та ініціали)
Рецензент		
	(підпис)	(прізвище та ініціали)

м. Тернопіль - 2023

Завдання на кваліфікаційну роботу бакалавра

АНОТАЦІЯ

Дослідження методів конфіденційності та цілісності даних в банківській сфері// Кваліфікаційна робота «Бакалавр» // Шиндеровський Сергій Вікторович // Тернопільський національний технічний університет імені Івана Пулюя, Факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-41 // Тернопіль, 2023 // С. 61, рис. - 4, табл. - 3, кресл. - 0, додат. – 0.

Ключові слова: ІНФОРМАЦІЙНА БАНКІВСЬКА СИСТЕМА, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ КІБЕРАТАКАМ.

Кваліфікаційна робота по дослідженню методів конфіденційності та цілісності даних в банківській сфері. В роботі проаналізовано інформаційну банківську систему як об'єкт захисту, проаналізовано дані, які потребують захисту, загрози в банківській сфері з якими активно стикаються банки.

Метою даної роботи є дослідження методів конфіденційності та цілісності даних в банківській сфері для протидії кібератакам, що застосовуються для забезпечення безпеки, конфіденційності та цілісності даних у банківських установах.

В першому розділі описано інформаційну банківську систему, типи даних та загрози в банківській сфері з якими активно стикаються банки. В другому розділі описано зберігання та обробку персональних даних, методи конфіденційності і дистанційне банківське обслуговування банків. В третьому розділі розглядаються популярні загрози для банківських систем, та дослідження методів конфіденційності та цілісності даних для уникнення цих загроз. В четвертому розділі висвітлено окремі питання охорони праці та безпеки життєдіяльності.

ANNOTATION

Research on methods of data confidentiality and integrity in the banking sector // Thesis of educational level “Bachelor” // Shinderovskii Serhii Victorovich // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Departament of Cybersecurity, СБС-41 group // Ternipol, 2023 // P. 61, fig. - 4, table. - 3, chair. - 0, added. - 0.

Keywords: BANKING INFORMATION SYSTEM, COMPREHENSIVE INFORMATION SECURITY SYSTEM, SOFTWARE, RESEARCH ON METHODS TO COUNTER CYBER ATTACKS.

Qualification work on the research of methods for data confidentiality and integrity in the banking sector. The work analyzes the information banking system as the object of protection, examines the data requiring protection, and explores the threats faced by banks in the banking sector. The "Remote Banking Services" are also analyzed as modern opportunities for banks to provide remote customer service.

The purpose of this work is to investigate methods of data confidentiality and integrity in the banking sector to counter cyber attacks, focusing on the study, analysis, and risk assessment of approaches used to ensure the security, confidentiality, and integrity of data in banking institutions.

The first chapter describes the information banking system, data types, and threats encountered by banks in the banking sector. The second chapter discusses the storage and processing of personal data, confidentiality methods, and remote banking services provided by banks. The third chapter discusses popular threats to banking systems and explores methods of data confidentiality and integrity to mitigate these threats. The fourth chapter highlights occupational safety and security considerations in the banking sector.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АБС – Автоматизована банківська система

СУІБ – Система управління інформаційною безпекою

ДБО – Дистанційне банківське обслуговування

ЕОМ – Електронні обчислювальні машини

ІБС – Інформаційна банківська система

ПЗ – Програмне забезпечення

ОС – Операційна система

КСЗІ – Комплексна система захисту інформації

CSP – Content Security Policy

OTP – One-Time Password

VPN – Virtual Private Network

ЗМІСТ

ВСТУП

У сучасному світі, де інформаційні технології займають все більш вагому роль у різних сферах життя, захист даних стає дедалі більш актуальним питанням. Банківська сфера не є виключенням з цього правила, оскільки банки зберігають величезні обсяги конфіденційної інформації своїх клієнтів, які є вкрай важливими для їх ділової та повсякденної діяльності. Зростаюча кількість та складність кібератак, зловживання даними та порушення безпеки вимагають постійного розроблення та вдосконалення методів та стратегій, спрямованих на захист конфіденційної інформації та забезпечення цілісності даних в банківській сфері.

Метою даної роботи є дослідження методів конфіденційності та цілісності даних в банківській сфері має на меті вивчення, аналіз та оцінку ризику підходів, що застосовуються для забезпечення безпеки, конфіденційності та цілісності даних у банківських установах.

Цілісність і конфіденційність даних є ключовими аспектами захисту інформації в банківській сфері. Цілісність даних означає, що дані залишаються непошкодженими та не зміненими, під час зберігання і обробки. В той час як конфіденційність означає, що інформація не доступна для незаконного використання, перегляду, копіювання або розголошення третім особам. В рамках дослідження будуть проаналізовані сучасні методи шифрування, аутентифікації та контролю доступу, які використовуються в банківській сфері для захисту конфіденційності даних.

Одним з основних завдань банків є збір, зберігання та обробка конфіденційної інформації своїх клієнтів, такої як персональні дані, фінансова інформація та інші.

Банк здійснює обробку і зберігання персональних даних у своїх дата-центрах, які відповідають вимогам законодавства України. При зверненні до Банку для отримання кредиту або інших послуг може здійснюватися передача персональних даних до бюро кредиторних історій і операторів, провайдерів стосовно

телекомунікацій, які представляють певні послуги зв'язку, з метою перевірки параметрів клієнта як користувача відносно рухомого зв'язку та для надання Банку відповідних відомостей про клієнта. Ця обробка здійснюється лише за наявності згоди суб'єкта персональних даних.

Важливою частиною роботи буде вивчення законодавства та нормативних актів, які регулюють зберігання та обробку конфіденційної інформації в банківській сфері, а також стандартів безпеки, таких як PCI DSS (Payment Card Industry Data Security Standard), які вимагають від банків виконання конкретних вимог щодо захисту даних.

Для банків, які працюють з великою кількістю клієнтської інформації, втрата персональних даних або несанкціонований доступ до них може призвести до серйозних наслідків, включаючи втрату довіри клієнтів, штрафи за порушення законодавства про захист даних та інші фінансові втрати.

Висновки цієї роботи мають на меті зрозуміти складність проблеми безпеки даних в банківській сфері, ідентифікувати вразливості та загрози, а також запропонувати ефективні методи і стратегії для забезпечення конфіденційності та цілісності даних. Це сприятиме зміцненню безпеки і підвищенню довіри до банківської сфери в цілому.

1 УПРАВЛІНСЬКА СИСТЕМА БАНКУ

1.1 Інформаційна банківська система

Інформаційна банківська система (ІБС) представляє собою набір програмних засобів, що автоматизують облік та опрацювання фінансових операцій у банку.

У склад ІБС входять різноманітні компоненти, такі як системи управління клієнтськими рахунками, кредитування, операцій з цінними паперами, звітності й аналізу, електронної комерції. Для забезпечення функціонування ІБС використовуються спеціалізовані комп'ютери, сервери, мережі зв'язку, технічні засоби зберігання даних та інші компоненти інфраструктури [2].

Завдяки ІБС банки значно зменшують час і витрати на опрацювання фінансових операцій, покращують якість обслуговування клієнтів та гарантують високий рівень безпеки й конфіденційності даних. Застосування ІБС дозволяє банкам швидко відстежувати фінансові потоки, аналізувати результативність своєї діяльності, приймати управлінські рішення й розробляти нові продукти та послуги.

Складові та функції інформаційної банківської системи:

- система управління клієнтськими рахунками є частиною ІБС і відповідає за ефективний облік та керування рахунками клієнтів у банку. Її завдання включають збереження інформації про клієнтів, їх рахунки, транзакції, баланси та інші фінансові дані. Крім цього, ця система також може містити інструменти для ризик-менеджменту, виявлення шахрайства та моніторингу фінансової активності клієнтів;
- система кредитування є складовою ІБС і забезпечує автоматизовану обробку кредитних операцій, включаючи подання заявок, оцінку кредитного ризику, управління кредитним портфелем та контроль погашення кредитів. Вона сприяє прийняттю рішень банком щодо надання кредитів, встановленню кредитних лімітів та управлінню процесом кредитного адміністрування;

- система операцій з цінними паперами є однією з складових ІБС, яка використовується для ефективного обліку та обробки операцій з цінними паперами, такими як акції, облігації, деривативи та інші фінансові інструменти. Вона дозволяє банку вести реєстри власників цінних паперів, здійснювати операції купівлі-продажу, розраховувати дивіденди та відсотки, а також надає інформацію про ринкові ціни та торгові умови;
- система звітності та аналізу в межах ІБС охоплює різноманітні фінансові звіти, статистичну звітність, звіти про ризики, аналітичні звіти та інші форми звітності, які допомагають банкам контролювати та аналізувати їхню фінансову діяльність. Ці системи можуть автоматично генерувати звіти відповідно до регуляторних вимог, стандартів фінансової звітності та внутрішніх потреб банку.
- система електронної комерції, що входить до складу ІБС, дозволяє банкам надавати своїм клієнтам електронні фінансові послуги, такі як інтернет-банкінг, мобільний банкінг, онлайн-платежі та електронні гроші. Вона забезпечує зручність та доступність банківських послуг через різні електронні платформи та пристрої;
- система безпеки та контролю, що входить до складу ІБС, відповідає за захист інформації банку, запобігання шахрайству, контроль доступу та виявлення вторгнень. Вона включає механізми шифрування, аутентифікації користувачів, моніторингу системи та аналізу поведінки для виявлення незвичайних або підозрілих дій.

Інтеграція та обмін даними є однією з компонент ІБС, яка відповідає за передачу інформації між банківськими системами, платіжними системами, регуляторами та іншими сторонніми організаціями. Цей компонент забезпечує взаємодію різних систем та стандартів даних, щоб забезпечити безперебійний обмін фінансовою інформацією між різними учасниками фінансового ринку. Це включає передачу платіжних інструкцій, обмін даними про клієнтів, обробку електронних транзакцій та інші фінансові операції.

Автоматизація бізнес-процесів є ще одним аспектом ІБС, який включає рішення для автоматизації різних банківських процесів та операцій, з метою підвищення ефективності та зниження ризиків. Це можуть бути системи управління відносинами з клієнтами (CRM), системи управління ризиками, системи планування ресурсів підприємства (ERP) та інші інструменти, які сприяють оптимізації робочих процесів банку [1].

Мобільні додатки є ще одним функціоналом ІБС, оскільки мобільні пристрої стали невід'ємною частиною нашого повсякденного життя. Ці додатки дозволяють клієнтам здійснювати операції, переглядати баланси, отримувати сповіщення та виконувати інші банківські дії безпосередньо зі своїх смартфонів або планшетів, забезпечуючи зручний та мобільний доступ до банківських послуг.

Інформаційно-банківська система (ІБС) відіграє невід'ємну роль у банківській галузі, сприяючи покращенню ефективності, забезпеченню високого рівня обслуговування клієнтів, зниженню ризиків та збільшенню прибутковості для банків. Ця система допомагає банкам стати більш конкурентоспроможними на ринку.

Важливо відзначити, що конфігурація та функціональність ІБС можуть варіюватись залежно від потреб конкретного банку. Кожен банк має можливість розробляти та налаштовувати власну ІБС відповідно до своїх вимог та стратегії, що дозволяє забезпечити індивідуальний підхід до використання системи.

1.2 Типи даних в банківській сфері

Сьогодні дані є надзвичайно важливим елементом у секторі BFSI, який багатий на дані. Вони впливають на основні рішення, пов'язані з розробкою політики, аналізом фінансової звітності, банківськими правилами та положеннями, допомагаючи їм приймати обґрунтовані рішення на основі даних.

У банківській галузі використовуються різноманітні типи даних для обробки, зберігання та аналізу фінансової інформації. До основних типів даних, що використовуються в банківській галузі, належать: клієнтські дані, фінансові дані, дані про кредити, дані про ризики, дані про валютні курси, дані про транзакцію, регуляторна звітність [3].

Клієнтські дані. Це інформація про клієнтів банку, яка включає особисті дані (ім'я, адреса, контактна інформація), реквізити рахунків, історію транзакцій, кредитну історію та інші дані, що стосуються клієнтів. Ці дані використовуються для ведення обліку клієнтів, надання фінансових послуг, оцінки кредитного ризику та аналізу поведінки клієнтів.

Фінансові дані включають інформацію про різноманітні фінансові операції, такі як платежі, перекази, кредитні транзакції, інвестиції, процентні ставки, валютні курси та інші фінансові параметри. Ці дані мають значення для внутрішнього обліку, звітності, аналізу ризиків та прийняття рішень в банку.

Дані про кредити охоплюють інформацію про кредитну історію клієнтів, кредитні заявки, умови та деталі кредитних угод, розрахунки погашення кредитів, заборгованість та інші фінансові показники, пов'язані з кредитуванням.

Дані про ризики включають інформацію, яка стосується оцінки та управління ризиками, такі як кредитований ризик, також ринковий, і операційний, та ліквідності. Ці дані допомагають банкам виявляти, оцінювати та керувати ризиками з метою забезпечення стабільності та безпеки своєї діяльності.

Дані про валютні курси та ринки охоплюють інформацію про валютні курси, ринкові ціни на цінні папери, товари, процентні ставки та інші фінансові

інструменти. Ці дані використовуються для розрахунків, аналізу ринкових умов, управління ризиками та прийняття рішень щодо інвестицій.

Дані про взаємодію та транзакції включають інформацію про комунікацію та взаємодію між банком та клієнтами, такі як журнали обміну повідомленнями, історії транзакцій, логи входу та виходу, дані про виконання доручень та інші дані, пов'язані з банківськими операціями.

Регуляторна звітність охоплює дані, необхідні для відповідності банківським регуляторним вимогам і стандартам. Ці дані використовуються для формування звітів про фінансовий стан, дотримання правил та інших регуляторних вимог.

Дані для аналізу отримуються з різних джерел, деякі з них згадуються нижче:

- персональні дані клієнта;
- реквізити облікового запису;
- транзакції клієнтів;
- скарги клієнтів і запити на обслуговування;
- стрічки соціальних мереж;
- ринкові настрої;
- продуктивність продукту.

Банки вирішують значні бізнес-проблеми, такі як прибутковість, продуктивність і доступність ризиків, шляхом використання аналітики великих даних (Big Data Analytics). Це також допомагає банкам знизити витрати на привертання клієнтів, передбачаючи ризик непогашення іпотечних кредитів і, що ще важливіше, ідентифікувати справжніх клієнтів [3].

1.3 Загрози в банківській сфері

Кібербезпека включає в себе організацію технологій, процедур і методів, що мають на меті запобігання атакам, пошкодженням, зловмисному програмному забезпеченню, вірусам, злому, крадіжці даних або несанкціонованому доступу до мереж, пристроїв, програм і даних.

У банківській сфері основна мета кібербезпеки полягає в захисті активів користувачів, оскільки все більше фізичних осіб здійснюють безготівкові операції та проводять транзакції онлайн. Особи використовують свої цифрові кошти, такі як дебетові та кредитні картки, для транзакцій, які потребують надійного кіберзахисту.

Кібербезпека не є виключно важливою для IT-організацій, вона має велике значення для кожного бізнесу, зокрема для банків. Банки проводять щодня мільйони операцій, тому вони дуже усвідомлюють необхідність застосування захисних процедур із кібербезпеки для захисту своїх даних від кібератак.

У фінансовому секторі за останні кілька років кіберзлочини значно поширилися, ставши однією з найбільших загроз у цій галузі. Хакери просунулися в своїх технологіях та навичках, що ускладнює боротьбу з цією загрозою для будь-якого банку. Наприклад, серед загроз, з якими зіштовхуються банки, можна виокремити фішинг, шкідливе програмне забезпечення, незашифровані дані, спуфінг та маніпулювання даними.

Фішинг означає отримання конфіденційних даних, таких як інформація про кредитні або дебетові картки, з метою зловживання, приховуючи свою справжню ідентичність під час електронного спілкування. Фішингові шахраї в онлайн-банкінгу постійно вдосконалюють свої методи, видаваючись за довірену сторону, але насправді спрямовуючи вас на розкриття своїх відкритих даних.

Клієнтські пристрої, такі як комп'ютери та мобільні пристрої, є основними засобами здійснення цифрових транзакцій, тому вони потребують належного захисту. Якщо ці пристрої були заражені шкідливим програмним забезпеченням,

це може створити серйозні кібернезпечні ризики кожного разу, коли вони підключаються до банківської мережі. Цінні конфіденційні дані проходять через цю мережу, і якщо на пристрої користувача є шкідливе програмне забезпечення, це може становити значну загрозу безпеці мережі банку.

Це є однією з найпоширеніших загроз, з якими стикаються банки, коли дані залишаються незашифрованими, а кіберзлочинці або хакери негайно маніпулюють цими даними, створюючи серйозні проблеми для банків. Всю інформацію, яка зберігається на комп'ютерах у банках або в Інтернеті, необхідно повністю зашифрувати. Це забезпечує, що навіть у випадку крадіжки даних, хакери не зможуть їх використати.

Це є одним із останніх видів кіберзагроз, з якими зіштовхуються фінансові установи. Хакери створюють URL-адресу веб-сайту банку, яка виглядає і працює так само, як оригінальний, і коли клієнт вводить свої вхідні дані, хакери викрадають ці дані для входу та використовують їх пізніше.

Поширене непорозуміння стосовно кібератак полягає у тому, що людей турбує лише крадіжка даних. Однак, це не завжди вірно, оскільки атаки на маніпулювання даними поступово стають все більш поширеними серед хакерів. Атаки маніпулювання даними відбуваються, коли зловмисник проникає в систему та непомітно змінює дані для своєї користі [2]. Наприклад, працівник може змінити дані клієнта, і це може залишитися непоміченим, оскільки транзакції виглядатимуть правдоподібними, що може спричинити помилки у збереженні майбутніх даних. Чим довше таке маніпулювання залишається непоміченим, тим більше шкоди воно може заподіяти.

1.4 Закони України для банківської сфери

Банки в Україні підпорядковуються низці законів та нормативно-правовим актам, які регулюють їх діяльність у банківській сфері. Основними законами, які стосуються банківської діяльності в Україні є: ЗУ" Про Національний банк України", ЗУ "Про банки і банківську діяльність", ЗУ "Про захист персональних даних", ЗУ "Про аудит фінансової звітності та аудиторську діяльність", ЗУ "Про бухгалтерський облік та фінансову звітність в Україні" та інші.

Закон України "Про Національний банк України" (№ 679-14). Цей закон визначає статус, завдання та функції Національного банку України (НБУ), який є головним регулятором банківської системи країни. Він також встановлює основні принципи банківського нагляду, забезпечення стабільності фінансової системи та захисту прав клієнтів банків.

Закон України "Про банки і банківську діяльність" (№ 2121-III). Цей закон встановлює загальні правила, принципи та умови здійснення банківської діяльності в Україні. Він визначає вимоги до створення, реєстрації, функціонування та ліцензування банків, а також встановлює правила ведення банківської діяльності та захисту інтересів клієнтів.

Український закон "Про захист персональних даних" (№ 2494-IX) встановлює правила, які регулюють обробку та захист персональних даних клієнтів банків. Цей закон визначає обов'язки банків щодо збору, зберігання, використання та передачі персональних даних, а також захищає права клієнтів на приватність.

Закон України "Про аудит фінансової звітності та аудиторську діяльність" (№ 2597-IX) застосовується до аудиторів, суб'єктів господарювання незалежно від їх форми власності та виду діяльності, а також до органів державної влади та органів місцевого самоврядування. Проте цей закон не охоплює діяльність органів державної влади, їх підрозділів та посадових осіб, що мають повноваження здійснювати державний фінансовий контроль, а також діяльність з внутрішнього

аудиту юридичних осіб, органів державної влади та органів місцевого самоврядування.

Закон України "Про бухгалтерський облік та фінансову звітність в Україні" (№ 2435-IX) поширюється на всіх юридичних осіб, створених згідно з українським законодавством, незалежно від їх організаційно-правових форм і форм власності. Цей закон також застосовується до представництв іноземних суб'єктів господарської діяльності (підприємств), які зобов'язані вести бухгалтерський облік та подавати фінансову звітність. Більш того, цей закон охоплює операції щодо виконання державного та місцевих бюджетів та складання фінансової звітності про виконання бюджетів відповідно до бюджетного законодавства.

Закон України "Про валюту і валютні операції" (№ 2888-IX). Валютне регулювання в Україні ґрунтується на таких принципах:

- свобода здійснення валютних операцій;
- ризикоорієнтованість, прозорість, достатність та ефективність валютного регулювання;
- самостійність та ринковість валютного регулювання.

Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" (№ 3050-IX) є чинним для громадян України, іноземців та осіб без громадянства, фізичних осіб - підприємців, юридичних осіб, їх філій, представництв та інших відокремлених підрозділів, які здійснюють фінансові операції на території України та за її межами згідно з міжнародними договорами України, на які надана згода Верховною Радою України, а також для органів місцевого самоврядування, правоохоронних та розвідувальних органів та інших державних органів України.

Закон України "Про платіжні системи та перекази коштів в Україні" (№ 1971-IX) встановлює загальні принципи функціонування платіжних систем в Україні та регулює відносини у сфері переказу коштів. Ці відносини підпорядковуються Конституції України, законам України "Про Національний банк України", "Про банки і банківську діяльність", "Про поштовий зв'язок", самому Закону, іншим

актам законодавства України, нормативно-правовим актам Національного банку України, а також міжнародним правилам та звичаям для документарних акредитивів Міжнародної торгової палати, правилам з інкасо Міжнародної торгової палати та правилам по договірних гарантіях Міжнародної торгової палати.

Закон України "Про захист прав споживачів" (№ 2529-IX) регулює взаємовідносини між споживачами товарів (за винятком харчових продуктів, якщо інше не передбачено цим Законом), робіт і послуг та виробниками і продавцями товарів, виконавцями робіт і надавачами послуг.

Закон України "Про запобігання корупції" (№ 2849-IX) регулює відносини у сфері запобігання корупції згідно з Конституцією України, міжнародними договорами, на які надана згода Верховною Радою України, цим Законом та іншими законами, а також відповідними нормативно-правовими актами, що прийняті для їх виконання.

Закон України "Про інформацію" (№ 2849-IX) встановлює норми, що регулюють відносини, пов'язані зі створенням, збиранням, одержанням, зберіганням, використанням, поширенням, охороною та захистом інформації.

Закон України "Про захист інформації в інформаційно-комунікаційних системах" (№ 2130-IX) визначає норми, що регулюють відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Закон України "Про доступ до публічної інформації" (№ 2849-IX) встановлює порядок реалізації та забезпечення права кожного на доступ до інформації, що перебуває у володінні суб'єктів владних повноважень та інших розпорядників публічної інформації, визначених цим Законом, а також інформації, що становить суспільний інтерес.

Закон України "Про державну таємницю" (№ 2849-IX) встановлює правила, що регулюють громадські відносини, пов'язані з класифікацією інформації як державної таємниці, її засекречуванням, розсекречуванням матеріальних носіїв і захистом державної таємниці з метою забезпечення національної безпеки України.

Дотримання законів стосовно банківської сфери має важливе значення з кількох причин:

- захист інтересів клієнтів. Закони банківської сфери встановлюють правила та стандарти, які сприяють захисту інтересів клієнтів. Вони гарантують конфіденційність та безпеку особистої інформації клієнтів, встановлюють вимоги щодо якості обслуговування та розкриття інформації про фінансові продукти. Дотримання цих законів забезпечує довіру клієнтів до банків та сприяє стійкому розвитку банківської системи;
- фінансова стабільність. Законодавство банківської сфери має на меті забезпечення стабільності фінансової системи. Воно встановлює принципи та правила, які регулюють діяльність банків, контролюють ризики та здатні надати ефективний функціонал ринку фінансистських послуг. Дотримання цих законів допомагає запобігати фінансовим кризам, зберігати стабільність та забезпечувати доступність фінансових ресурсів для розвитку економіки;
- боротьба зі злочинністю. Банківська сфера може бути предметом злочинної діяльності, такої як легалізація доходів злочинного походження, фінансування тероризму, шахрайство та інші злочини. Закони стосовно банківської сфери встановлюють механізми для запобігання та виявлення такої діяльності, а також визначають відповідальність за її порушення. Дотримання цих законів сприяє зниженню ризику злочинної діяльності та забезпечує безпеку для клієнтів, банків та суспільства в цілому;
- забезпечення довіри та репутації. Дотримання законів є важливим елементом забезпечення довіри до банків та підтримання їхньої репутації. Коли банк дотримується встановлених правил і норм, це відображається на його надійності та професіоналізмі.

Таким чином, дотримання законів у банківській сфері є важливим для захисту інтересів клієнтів, забезпечення фінансової стабільності, боротьби зі злочинністю та збереження довіри та репутації банків. Відповідне виконання законодавчих вимог сприяє ефективному та етичному функціонуванню банківської системи.

2 СПОСОБИ ЗАХИСТУ ДАНИХ

2.1 Зберігання і обробка персональних даних

Підстави для обробки особистих даних визначаються згідно зі статтею 11, пунктом 3 Закону України "Про захист персональних даних". Банк має право обробляти особисті дані з метою укладання та виконання правочинів, в яких суб'єктом персональних даних є сам суб'єкт або на користь якого такі правочини укладено, або для здійснення передумов, що передують укладанню таких правочинів за вимогою суб'єкта персональних даних.

У межах Банку доступ до особистих даних надається підрозділам та/або окремим співробітникам з метою виконання їх службових (трудових) обов'язків, які пов'язані з виконанням договірних, юридичних та/або регуляторних зобов'язань Банку і захисту законних інтересів Банку. Кожен співробітник Банку зобов'язаний підписати зобов'язання про нерозголошення інформації, до якої він має доступ.

Банк надає приватним особам та організаціям (включаючи розпорядників персональних даних) доступ до особистих даних кожної фізичної особи з метою забезпечення виконання їх функцій або надання послуг Банку (включаючи IT та бек-офіси) [5]. Цей доступ надається на основі укладених між Банком і цими особами (організаціями, компаніями) договорів, наскільки це необхідно для надання відповідних послуг. Всі розпорядники персональних даних, яким Банк дозволяє обробляти такі дані власним іменем, зобов'язані конфіденційно обробляти ці дані та використовувати їх виключно для надання послуг Банку.

Банк передає персональні дані фізичних осіб - клієнтів Банку або надає доступ до цих даних за запитом державних органів та осіб, зазначених у статті 62 Закону України "Про банки і банківську діяльність", якщо існують законні підстави для розкриття банківської таємниці третім особам згідно з вимогами українського законодавства. Крім того, такі дані можуть передаватись іншим особам на підставі належним чином оформленої письмової згоди відповідних суб'єктів персональних

даних або умов, передбачених договорами та іншими правочинами, укладеними з Банком.

Також абсолютно всі банки мають власні веб сайти в інтернеті. І в основному цими сайтами користуються користувачі для дій над платежами для власних потреб.

Банк є власником особистих даних користувачів Сайту. При використанні сервісів Сайту користувачем, Банк здійснює обробку його персональних даних, включаючи, але не обмежуючись:

- персональні дані, які користувач надає під час заповнення реєстраційних форм і тоді користування потрібними сервісами. Це є ПіП, номер реєстрації, (ідентифікаційний номер), фактичне місце проживання, місце роботи, особисті відомості про вік, сімейний стан та інше;
- копії документів, виданих на ім'я користувача;
- фінансова інформація, включаючи стан рахунків, доходи, нарахування та утримання;
- електронна пошта, номери телефонів та інші електронні ідентифікаційні дані;
- записи голосу, зображення (фото та відео);
- кредитна історія та інформація про виконання зобов'язань за договорами з Банком та іншими документами;
- інша інформація, що стала відома Банку в процесі правовідносин з користувачем, відповідно до вимог законодавства України та внутрішніх документів Банку;
- файли cookie;
- IP-адреси;
- параметри та налаштування інтернет-браузерів (User-agent).

Банк збирає тільки ті персональні дані, які користувач свідомо і добровільно надає як суб'єкт персональних даних. Ці дані можуть включати ім'я, прізвище, логін, пароль, електронну адресу, номер телефону, дату народження, стать та інші

дані. Надання цих даних відповідає вимогам законодавства і розглядається як згода суб'єкта персональних даних на їх обробку Банком для цілей надання послуг та сервісів Сайту.

Банк обробляє персональні дані протягом всієї тривалості ділових відносин з суб'єктами персональних даних. Цей період включає укладення договору або замовлення послуги, їх виконання та закінчення дії відповідного договору, а також дотримання строків зберігання інформації, встановлених умовами укладених договорів або законодавством України. Такі строкові обмеження можуть бути визначені Законом України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення", Правилами застосування переліку документів Національного банку України та внутрішніми документами Банку, затвердженими Постановою Правління Національного банку України від 27 листопада 2018 року під номером 130.

2.2 Методи конфіденційності

Захист конфіденційної інформації про клієнтів є надзвичайно важливою та серйозною проблемою для банків, тому вони вживають різних заходів для забезпечення її безпеки та захисту від несанкціонованого доступу.

Основними засобами захисту інформації є фізичні, апаратні, програмні, апаратно-програмні, криптографічні та адміністративні методи.

2.2.1 Фізичний захист

Фізичні засоби захисту використовуються для зовнішнього та точного захисту ЕОМ, територій та об’єктів, пов'язаних з обчислювальною технікою. Вони створюють фізичні перешкоди для потенційних порушників, що намагаються проникнути і отримати доступ до частин систем інформації та ЗІ. Сучасний величезний вибір приладів захисту є великим. Це включає різноманітні замки, які облаштовані на входах до приміщень та на блоках системи, на додачу системи пожежної сигналізації. До засобів захисту на додачу належать різні засоби екранування кімнат та шляхів передачі даних.

Фізичний захист, що використовують банки для захисту серверних приміщень та інших областей, де зберігаються цінні дані, також може містити в собі такі елементи: фізичну охорону, системи відеоспостереження, захищені двері та замки [5].

Фізичну охорону. Банки наймають професійних охоронців, які контролюють доступ до серверних приміщень та інших областей, де зберігаються дані клієнтів та інші цінні документи. Охоронці мають великий досвід у виявленні та запобіганні незаконним діям з боку працівників банку або ж сторонніх осіб.

Системи відеоспостереження. Банки встановлюють системи відеоспостереження для моніторингу приміщень та контролю доступу до них. Камери можуть бути розташовані в різних місцях, щоб охопити всі області огляду, які потребують захисту. Деякі камери можуть мати можливість розпізнавання

обличь та інших розпізнавальних функцій, що полегшує ідентифікацію осіб, що знаходяться у приміщенні.

Захищені двері та замки. Банки встановлюють захищені двері та замки, щоб запобігти незаконному доступу до серверних приміщень та інших областей, де зберігаються цінні дані. Двері можуть мати вбудовані датчики, що можуть виявляти будь-які намагання їх зламати або пробити.

2.2.2 Апаратні засоби захисту

Апаратні засоби захисту включають різноманітні електронні, електронно-механічні та інші пристрої, які вбудовуються в серійні блоки електронних систем обробки і також щоб передати дані для локального захисту обчислювальної техніки, таких як термінали, пристрої вводу та виходу даних, процесори, лінії зв'язку.

До основ функцій техніки основи засобів захисту включають:

- заборону несанкціонованого зовнішнього доступу віддалених користувачів;
- заборону несанкціонованого локального пропуску до баз даних через спеціальні дії персоналу;
- захист цілісності програм.

Ці функції виконуються шляхом:

- підтвердження суб'єктів (користувачів) та об'єктів (ресурсів) коректної системи;
- аутентифікації суб'єкта на основі наданого ним ідентифікатора.
- перевірки повноважень, що включає перевірку дозволу на виконання певних дій;
- збереження (протоколювання) при доступі до небезпечних ресурсів;
- реєстрації спроб невірного доступу.

2.2.3 Програмні засоби захисту

Програмні засоби захисту виконують логічні і інтелектуальні функції захисту, які вбудовані в програмне забезпечення системи.

З їх допомогою реалізуються такі задачі забезпечення безпеки:

- контроль процесу завантаження та входу в систему з використанням системи паролів;
- створення меж і контроль прав доступу до системних ресурсів, терміналів, зовнішніх ресурсів, постійних та тимчасових наборів даних;
- захист потрібних даних від вірусів;
- автоматичний контроль роботи користувачів способом протоколювання їхніх дій.

2.2.4 Апаратно-програмні засоби захисту

Апаратно-програмні засоби для захисту представляють собою комбінацію програмних та апаратних рішень. Ці засоби широко використовуються для аутентифікації користувачів в АБС, що означає перевірку їх ідентифікаторів перед наданням доступу до системних ресурсів.

Також, технічні прилади захисту використовуються для створення ЕЦП відповідальних користувачів. У багатьох АБС сильно поширене використання смарт-карт, які містять засекречені паролі та ключі.

2.2.5 Криптографічне шифрування

Криптографічні методи захисту засновані на застосуванні криптографічних перетворень до даних, що передбачає їх шифрування. Основні методи криптографічного захисту включають: метод шифрування з датчиком псевдовипадковими числами, криптографічними стандартами, з використанням пари ключів.

Метод шифрування з використанням псевдовипадкових чисел. Цей спосіб включає генерацію гамма-шифру за допомогою випадкових чисел, який потім застосовується до відкритих даних з урахуванням зворотності процесу.

Метод шифрування з використанням криптографічних стандартів (з симетричним шифруванням). Цей метод використовує перевірені алгоритми шифрування з високим рівнем криптостійкості. Наприклад, американський стандарт такого шифру DES (Data Encryption Standard).

Метод шифрування з використанням пари ключів (з асиметричною системою шифрування). Цей метод використовує два ключі - відкритий ключ для шифрування інформації та закритий ключ для розшифрування інформації.

Наприклад цим методом може бути RSA (Rivest-Shamir-Adleman).

Таким чином, криптографічні методи захисту забезпечують захист даних шляхом застосування шифрування з використанням датчиків псевдовипадкових чисел, криптографічних стандартів та пари ключів.

Усі ці методи криптографічного захисту мають за мету забезпечити конфіденційність та цілісність даних під час їх передачі та зберігання.

Криптографічне шифрування, яке використовують банки для захисту персональних даних своїх клієнтів, зазвичай базується на потужних алгоритмах шифрування, таких як AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman) та SHA (Secure Hash Algorithm).

AES є одним з найпопулярніших алгоритмів блочного шифрування, який використовується для захисту конфіденційної інформації. Він є стандартом у багатьох промислових та урядових секторах для захисту даних.

AES має фіксовану довжину 128 біт, а розмір ключа може бути 128, 192 або 256 біт. Через фіксований розмір блоку 4 × 4 байта, AES операціює з масивом, що називається станом (у випадку алгоритмів з більшим розміром блоку також є додаткові стовпці).

Для ключа довжиною 128 біт, алгоритм складається з 10 раундів, під час яких виконуються наступні операції в послідовному порядку:

- subBytes();
- shiftRows();
- mixcolumns() (у 10-му раунді пропускається);
- xorRoundKey().

RSA є одним з найпопулярніших алгоритмів шифрування з відкритим ключем, який використовується для безпечного обміну ключами та підпису даних.

Алгоритм RSA складається з 4 етапів: генерація ключів, шифрування, розшифрування та розповсюдження ключів.

Безпека алгоритму RSA базується на складності факторизації цілих чисел. Алгоритм використовує два ключі: відкритий (public) і секретний (private). Ці ключі утворюють пару ключів (keypair), причому відкритий ключ не потребує особливої конфіденційності і використовується для шифрування даних. Розшифрування можливе лише за допомогою відповідного секретного ключа, якщо повідомлення було зашифровано відкритим ключем.

SHA є алгоритмом хешування, який використовується для забезпечення конфіденційності і цілісності даних.

Банки також можуть застосовувати комбінації цих та інших алгоритмів для захисту даних своїх клієнтів. Важливо зазначити, що банки повинні постійно вдосконалювати свої методи шифрування та захисту даних, оскільки кібератаки стають все складнішими і здатними обійти або зламати існуючі захисні механізми.

В АБС широко використовуються криптографічні методи захисту інформації, які реалізуються через використання апаратних, програмних або програмно-апаратних засобів захисту.

На рисунку 2.1 наведено орієнтовні характеристики алгоритмів криптографічного захисту.

Характеристика	DES	RSA
Вид алгоритму	Одноключовий	Двоключовий
Швидкість роботи	Швидко	Повільно
Функція, що використовується	Перестановка і підстановка	Піднесення до степеня
Довжина ключа	56 біт	300-600 біт
Найменш затратний криптоаналіз	Перебір по всьому ключовому простору	Розкладання модуля
Стійкість	Теоретична	Практична
Часові витрати на розкриття	Століття	Залежать від довжини ключа
Час генерації ключів	Мілі-секунди	Десятки секунд
Тип ключа	Симетричний	Асиметричний

Рисунок 2.1 – Характеристики і порівняння алгоритмів DES та RSA

2.2.6 Адміністративні засоби захисту

Адміністративні засоби захисту включають організаційні заходи, що регулюють процеси функціонування АБС, використання її ресурсів та діяльність персоналу з метою максимальної перешкоди та усунення загроз безпеці. Існує багато адміністративно-організаційних заходів, серед яких можна виділити наступні:

- розробка чіткої технології обробки інформації в АБС та контроль її дотримання;
- організація захисту приміщень інформаційних служб від встановлення прослуховуючої апаратури;
- уважний підбір персоналу, включаючи перевірку нових співробітників, ознайомлення їх з правилами роботи з конфіденційною інформацією та встановлення відповідальності за порушення суворості обробки.

2.3 Дистанційне банківське обслуговування

ДБО є загальним терміном, що описує технологію, яка дозволяє надавати банківські послуги клієнтам відносно основі їх розпоряджень, переданих на відстані без необхідності відвідувати фізичний банк. Це здійснюється за допомогою різних можливостей самообслуговування, в основному комп'ютерних і особливо телефонних мереж. Всі операції, які можна виконати дистанційно, без прямого відвідування банку, повинна забезпечувати саме ДБО.

Базове і головне завдання використання ДБО в банківській сфері полягає в забезпеченні рівних можливостей для використання фінансових приладів у будь-якому регіоні, включаючи міжнародні операції.

Функціонування дистанційного банківського обслуговування великої кількості людей ґрунтується на наступних принципах:

- неперервність роботи системи. Клієнт може керувати своїми фінансами незалежно від свого місцезнаходження та часу;
- загальнодоступність. Засоби доступу до системи повинні бути широко поширеними та доступними за прийнятною ціною;
- множинність працюючих каналів доступу. Клієнту надається можливість використовувати різні канали доступу в будь-якій їх комбінації;
- різноманітність обслуговування. Система робить можливість проведення завдань в режимі самообслуговування. Клієнт повинен та хоче отримати вибір між інтерактивним режимом та обслуговуванням через оператора;
- здатність проведення операцій стосовно режиму реального часу (за можливості);
- максимальне зменшення ручної обробки операцій. Технологія дистанційного банківського обслуговування максимально уникатиме або зменшуватиме етапи, які вимагають обов’язкової ручної обробки.

Дистанційне банківське обслуговування включає в себе не лише роботу з клієнтами банку, але також взаємодію з банками-кореспондентами та різними

підрозділами банку, такими як філії, відділення, віддалені каси, обмінні пункти. Шляхом використання системи дистанційного банківського обслуговування (ДБО) забезпечується широкий спектр послуг, що охоплює як найпростіші інформаційні сервіси (наприклад, перегляд залишку на рахунку), так і складніші, наприклад, можливість отримання кредиту дистанційно, розміщення брокерських заявок на фондових чи валютних ринках. Банк, за допомогою технологій ДБО, може проводити платежі та здійснювати різні операції з коштами клієнтів на основі їх дистанційних розпоряджень, які передаються до банку за допомогою різних каналів та засобів доступу, таких як телефонні або Інтернет.

Система дистанційного банківського обслуговування (ДБО) базується на використанні автоматизованої системи, що складається з наступних компонентів:

- сервер каналу зв'язку, який контролює інтерфейс між системою та клієнтами, реєструє дистанційні розпорядження клієнтів і створює відповідні електронні документи у базі даних і також системи ДБО. В залежності від типу каналу, сервери можуть включати обладнання комп'ютерної телефонії та програмне забезпечення для телефонних каналів або програму на Інтернет-сервері для каналу Інтернету;
- сервер обробки дистанційних розпоряджень, який відповідає за обробку зареєстрованих розпоряджень клієнтів та створення на їх основі документів (квитанцій, повідомлень, платіжних доручень) і реалізацію внутрішніх операцій у системі ДБО;
- операційний день системи ДБО, який включає програмний комплекс або складову частину автоматизованої системи банківських операцій. Він призначений для зберігання інформації про клієнтів, рахунки та проведені операції.

Впровадження технології ДБО має безсумнівні переваги як для банків, так і для клієнтів. Основні переваги для банку включають:

- конкурентні переваги по відношенню до банків, що не збираються надавати послуги ДБО;

- збільшення масштабів бізнесу шляхом примноження клієнтської бази без обмежень кількістю філій або персоналу;
- екстериторіальність банківського обслуговування, що дозволяє обслуговувати клієнтів з інших міст або країн без потрібності в додаткових відділень;
- можливість надавати цілодобовий сервіс для залучення віддалених клієнтів;
- спрощення процесу розширення бізнесу і впровадження нових продуктів без суттєвих витрат і організаційних процедур;
- спрощення процесу реалізації комплексних фінансових продуктів, таких як банківські та страхові продукти;
- зниження організаційних витрат через зменшення кількості персоналу та зменшення коштів на функціонування відділень.

Однак використання системи ДБО також має деякі недоліки:

- високі витрати на придбання або розробку системи ДБО, її впровадження та навчання співробітників;
- необхідність тривалої підготовки співробітників до роботи з електронними документами;
- постійні витрати на обслуговування, включаючи витрати на канали зв'язку з хорошою пропускною здатністю для обслуговування гігантської кількості клієнтів.

Основні переваги використання дистанційного банківського обслуговування (ДБО) клієнтами банку включають:

- можливість здійснювати операції в будь-який час і з будь-якого місця без необхідності відвідування банку особисто;
- легкий доступ до актуальної інформації про стан рахунків та надходження коштів;
- прискорення обігу коштів на внутрішньому ринку завдяки швидкому виконанню операцій;

- зниження вартості банківських операцій.

Недоліки системи ДБО для клієнтів включають наступне:

- потребу в необхідному обладнанні та вищій кваліфікації користувачів для використання основних каналів доступу до ДБО;
- зазвичай банки хочуть плату за користування цією системою.

Отже, ДБО дає клієнтам можливість самостійно користуватися банківськими послугами, незалежно від працівників банку. Сучасні банки активно впроваджують системи ДБО з метою покращення ефективності обслуговування своїх клієнтів, дивитися рисунок 2.2.

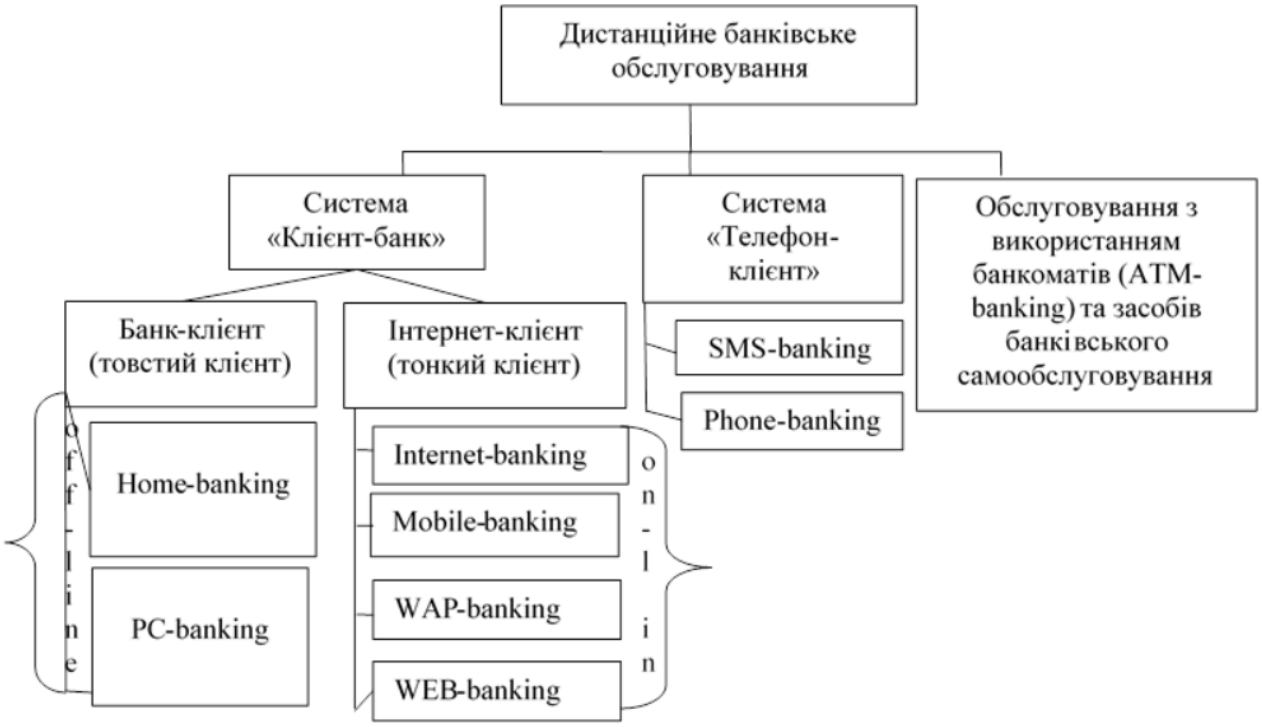

Рисунок 2.2 – Сучасні технології дистанційного банківського обслуговування

Завдяки різноманітним каналам дистанційного доступу клієнта до банку, сьогодні стали поширеними такі концепції:

- пряме банківське обслуговування (direct-banking);
- дистанційні операції за допомогою телефону (phone-banking, telebanking);
- операції через мобільний телефон (handy ipocket-banking);

- операції факсом (fax-banking).

Однією з перших технологій дистанційного банківського обслуговування стала «Home-banking» (домашнє обслуговування). Ця технологія дозволяє клієнтам отримувати будь-які банківські послуги та здійснювати операції без необхідності відвідування банку, передаючи інформацію мобільними або ж через двосторонню систему кабельного сигналу.

На теперішній час «Home-banking» описує узагальнену модель банківської діяльності, котра використовує різні канали віддаленого доступу з метою покращення ефективності банківської установи та проникнення на нові сегменти ринку фінансових послуг [5].

Виокремлюють певний ряд ризиків, які виникають при використанні дистанційного банківського обслуговування (рисунок 2.3).

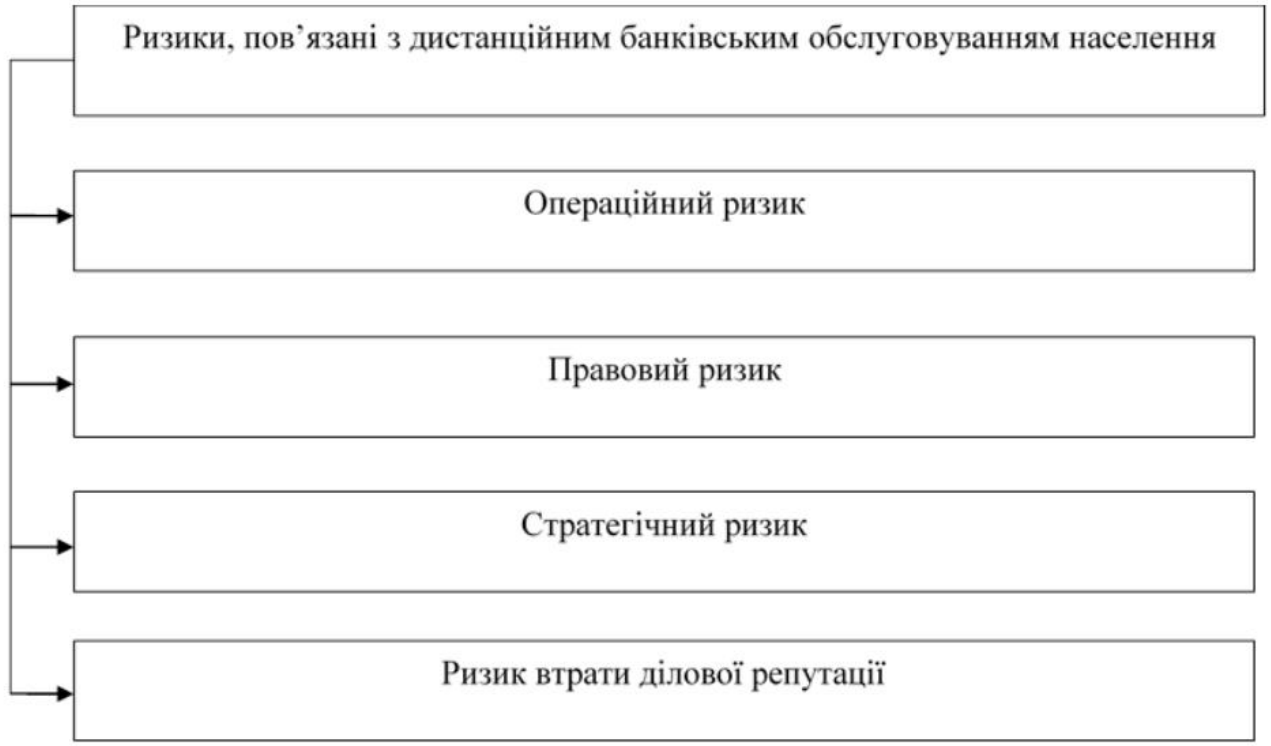

Рисунок 2.3 – Небезпеки, які пов'язані з дистанційним банківським обслуговуванням

Операційний ризик при використанні системи дистанційного банківського обслуговування (ДБО) може виникнути з наступних причин:

- неналежна організація інформаційних потоків, внутрішньобанківських процесів і процедур, а також недостатня інформаційна безпека, як у кредитній організації, так і у провайдерах;
- недотримання режимів функціонування інформаційних систем банку, які використовуються для Інтернет-банкінгу, може виникати внаслідок аварій, відмов, або збоїв у роботі обладнання та програмного забезпечення, які належать банку або надаються його провайдерами;
- помилки в роботі техніки забезпечення системи ДБО призведуть до шкоди цілісності даних у його інформаційному контурі;
- неправомірний доступ до інформації банку з користуванням системи ДБО;
- замала потужність і захист ІС та ІКС мереж, як у банку, так і у провайдерів, які використовуються в інформаційному секторі ДБО, включаючи можливість неправомірного доступу за допомогою Інтернет-технологій;
- помилки співробітників банку, людей або провайдерів ДБО, а особливо поганий рівень контролю, включаючи програмний контроль, щодо можливості вчинення помилок;
- невиконання договірних зобов'язань тими хто надають послуги (виконавцями робіт) стосовно кредитної організації;
- недотримання кредиторами обов’язків перед клієнтами через недоліки в апаратно-програмному забезпеченні систем ДБО.

Основні причини правового ризику, пов'язаного з застосуванням системи ДБО, включають:

- порушення банком вимог законодавства України, включаючи нормативні акти НБУ, через недоліки апаратно-програмного забезпечення системи ДБО;
- наявність недоліків у правовій системі, яка не вирішує певні питання, пов'язані з дистанційним банківським обслуговуванням та

відповідальністю сторін, зокрема в контексті надання банківських послуг через кордон;

- незаконний доступ до даних під час її обробки, передачі або зберігання, як у банку, так і у провайдерах, з якими кредитна фірма склала договори на взаємодію;
- погана увага банку до правових питань при укладанні договорів з давцями послуг, які роблять обробку, передачу та зберігання банківських даних, особливо визначення відповідальності провайдерів за невиконання своїх обов'язків у межах ДБО.

3 ДОСЛІДЖЕННЯ МЕТОДІВ КОНФІДЕНЦІЙНОСТІ ТА ЦІЛІСНОСТІ ДАНИХ

3.1 Типи кібератак на банківські системи

В сучасному світі, де банківські системи стають все більш цифровими та потребують постійного підключення до Інтернету, кібербезпека стає невід'ємною частиною їхнього функціонування. Однак, разом із модернізацією технологій та зручностей, з’являються нові загрози, спрямовані на вразливості цих систем. На рисунку 3.1 представлено топ банківських кіберзагроз.

Рисунок 3.1 – Типи банківських кіберзагроз

Серед найпоширеніших та найнебезпечніших кібератак на банківські системи можна виділити такі, як malware, MITM атаки, XSS атаки, DDoS атаки, phishing та вразливості нульового дня. Кожна з цих атак має свої унікальності та методи, якими зловмисники намагаються отримати доступ до конфіденційної інформації, завдати шкоди банківським системам.

Один з найпоширеніших типів кібератак - це шкідливе програмне забезпечення (Malware). Воно може інфікувати комп'ютери або мобільні пристрої користувачів і здійснювати крадіжку конфіденційних даних, виконувати шкідливі дії та поширюватись через мережу.

Інша поширена атака - це "людина в середині" (MITM attack). Зловмисник розміщується між комунікуючими сторонами і перехоплює або змінює передачу даних. Це дає зловмиснику можливість отримати доступ до конфіденційної інформації або навіть виконувати дії від імені користувача.

Атака XSS (Cross-Site Scripting) використовує вразливості веб-додатка, щоб вставити і виконати шкідливий скрипт на веб-сторінці, що може призвести до перехоплення даних користувачів або виконання шкідливих дій.

DDoS атаки (Distributed Denial of Service) мають на меті перевантажити мережу або систему банку, щоб знизити їх доступність для легітимних користувачів. За допомогою ботнетів та розподілених ресурсів зловмисники можуть запустити масштабну атаку, яка може спричинити серйозні перебої у роботі системи.

Фішинг - це атака, коли зловмисники виманюють конфіденційну інформацію шляхом імітації легітимних комунікацій від банків або організацій. Це призводить до розкриття паролів, фінансових даних та доступу до особистої інформації.

Останнім, але не менш важливим, є вразливості нульового дня (Zero-day vulnerabilities). Це вразливості, про які розробники ще не знають і не виправити. Зловмисники можуть використовувати ці вразливості, щоб отримати доступ до банківських систем перед тим, як вони будуть виявлені й усунені. В таблиці 3.1 зображено короткий опис атак та інструментів які використовують хакери.

Таблиця 3.1 – Опис атак та інструментів хакерів

Кібератака	Опис	Інструменти хакерів
Malware	Шкідливе програмне забезпечення, призначене для злому комп'ютерних систем або крадіжки інформації.	Троянські програми, віруси, черв'яки, шпигунські програми.
MITM атака	Атака "людина посередині", в якій зловмисник перехоплює комунікацію між двома сторонами з метою злому або перехоплення даних.	ARP spoofing, DNS spoofing, SSL strip.
XSS атака	Атака на вразливості у веб-додатках, яка дозволяє зловмиснику впроваджувати та виконувати власний скрипт на стороні користувача.	Впровадження скриптів JavaScript або HTML в веб-сторінках.
DDoS атака	Атака на мережу або сервер, в якій зловмисники намагаються перевантажити систему шляхом відправки великого обсягу запитів.	Ботнети, бот-сіті, мережа збирачів ("зомбі").
Phishing	Атака, в якій зловмисники підроблюють легітимні веб-сторінки або електронні повідомлення з метою шахрайства, крадіжки конфіденційних даних або фінансових втрат.	Фішингові сторінки, соціальна інженерія, масштабні розсилки електронної пошти.
Zero-day вразливість	Використання вразливостей в програмному забезпеченні, які ще не були виявлені або виправлені розробниками.	Використання нових інструментів та експлойтів, які не були розкриті широкій публіці.

Більш детальний опис тих типів кібератак, їх характеристик та інструментів, які використовують хакери для здійснення цих атак, що зображені в таблиці 3.1.

3.1.1 Короткий опис Malware

Malware (malicious software) - це широкий термін, що охоплює різноманітні типи погане ПЗ, призначеного для злому комп'ютерних систем або крадіжки конфіденційної інформації. Це можуть бути троянські програми, віруси, черв'яки та шпигунське програмне забезпечення, кожен з яких має свою специфіку та методи дії.

Хакери використовують різні інструменти для розробки та поширення небезпечне ПЗ. Наприклад, вони можуть створювати зловмисний код в програмних мовах, таких як C++ або Python, а потім використовувати компілятори або інші інструменти для створення виконуваних файлів або скриптів, вони також використовують закриті спільноти для обміну знаннями та отримання нових інструментів для здійснення атак.

3.1.2 Короткий опис MITM attack

MITM атака (Man-in-the-Middle) - це тип кібератаки, в якій зловмисник вступає між двома комунікуючими сторонами і перехоплює їхню взаємодію. Зловмисник маскується під легітимну сторону та отримує несанкціонований доступ до передаваної інформації. Ця атака може відбуватися як у фізичних мережах, так і у бездротових мережах.

Механізм MITM атаки полягає в тому, що зловмисник встановлює контроль над комунікаційним каналом між двома легітимними сторонами. Це може бути досягнуто шляхом використання шпигунського програмного забезпечення, фізичних пристроїв або зловмисних мережевих налаштувань. Після успішного встановлення проміжного зв'язку зловмисник може контролювати, перехоплювати та навіть змінювати передавану інформацію між двома сторонами без їхнього відома.

Ця кібератака може мати серйозні наслідки. Зловмисник може перехоплювати чутливу інформацію, таку як логіни, паролі, фінансові дані або конфіденційні документи. Він також може змінювати дані, що передаються між сторонами, створюючи можливість для впровадження шкідливого коду або змінюючи передану інформацію в свою користь.

Хакери використовують різні методи та інструменти для здійснення MITM атак. Наприклад, вони можуть використовувати програмне забезпечення, яке дозволяє перехоплювати мережевий трафік, таке як Cain & Abel, Wireshark або Ettercap. Вони також можуть використовувати фізичні пристрої, такі як акустико-магнітні перехоплювачі або мережеві адаптери для безпроводового перехоплення сигналу.

3.1.3 Короткий опис XSS attack

XSS атака (Cross-Site Scripting) - це тип кібератаки, в якій зловмисник впроваджує зловісний скрипт на веб-сторінку, яку відвідує користувач. Цей скрипт виконується в браузері жертви і може мати потенційно шкідливі наслідки, такі як викрадання інформації або злам системи.

Механізм XSS атаки полягає в тому, що зловмисник впроваджує вразливість на веб-сторінку, яка дозволяє вставляти в неї зловісний код. Це може бути досягнуто через некоректну обробку введення користувача, відсутність або недостатню фільтрацію введених даних. Коли користувач відкриває таку веб-сторінку, браузер виконує вбудований зловісний скрипт, що дає зловмиснику можливість зламувати сеанси користувачів, викрадати інформацію або впроваджувати інші шкідливі дії.

Зловмисники використовують різні методи та інструменти для здійснення XSS атак. Вони можуть вставляти зловісний код безпосередньо в HTML-код веб-сторінки, включати його у параметри URL або введення форм, також зловмисник впроваджує зловісний код на веб-сторінку, який зберігається на постійній основі і виконується при кожному відкритті цієї сторінки користувачем, або зловмисник впроваджує зловісний код у веб-сторінку, який відображається

тільки під час певної дії користувача, наприклад, при переході за посиланням або введенні певних параметрів, або використовувати соціальну інженерію для переконання користувачів у виконанні зловісних дій.

3.1.4 Короткий опис DDoS-attack

DDoS-атака (Distributed Denial of Service) - це тип кібератаки, в якій зловмисники намагаються перевантажити цільову систему, сервіс або мережу штучним збільшенням трафіку. Метою такої атаки є призупинення нормального функціонування цільової системи або зниження її продуктивності, недоступність для законних користувачів та виклик хаосу.

DDoS-атаки використовують багато комп'ютерів, які становлять ботнет - мережу компрометованих комп'ютерів, керованих зловмисниками. Ці комп'ютери, які можуть бути заражені шкідливим програмним забезпеченням, таким як троянські коні або боти, виконують команди зловмисників, щоб одночасно надсилати велику кількість запитів до цільової системи або сервера. Це призводить до перевантаження ресурсів цільової системи, викликаючи відмову в обслуговуванні для законних користувачів.

Хакери використовують різні методи та інструменти для здійснення DDoS-атак. Вони можуть використовувати ботнети для масштабних атак з використанням великої кількості комп'ютерів. Зловмисники також можуть використовувати техніки, такі як IP-саморозподіл та IP-підробка, для уникнення виявлення та блокування їхніх IP-адрес.

3.1.5 Короткий опис Phishing

Phishing - це тип кібератаки, в якій зловмисники намагаються використати соціальну інженерію та маніпуляцію, аби взяти таємну інформацію, таку як паролі, номери карток або особисті дані, шляхом підробки та імітації довірливих комунікаційних каналів.

Зловмисники, які здійснюють phishing атаки, створюють вигляд або використовують існуючі веб-сторінки, електронні листи, повідомлення в

соціальних мережах або миттєві повідомлення, які імітують відомі організації, бренди або особи. Вони намагаються переконати потенційну жертву надати свої особисті дані, виконати фінансову транзакцію або перейти за посиланням, що призводить до зловмисних дій.

Phishing атаки можуть мати різні форми, включаючи електронну пошту з проханням оновити акаунт або пароль, підроблені веб-сторінки для введення особистих даних, фішингові спам-повідомлення через соціальні мережі або миттєві повідомлення з проханням здійснити фінансову операцію. Ці атаки покладаються на психологічний тиск та недостатню обізнаність користувачів, щоб отримати доступ до їх конфіденційних даних або виконати шахрайські дії.

3.1.6 Короткий опис A zero-day exploit

A zero-day exploit (вразливість нульового дня) - це тип кібератаки, яка використовує вразливості або слабкі місця в програмному забезпеченні, які ще не відомі розробникам або постачальникам програмного забезпечення. Це означає, що вразливість використовується зловмисниками до того моменту, поки розробники не знайдуть і не виправлять її (надалі ця вразливість стає відомою як "нульовий день"). Це дозволяє зловмисникам отримувати несанкціонований доступ до системи або виконувати шкідливі дії без відома адміністраторів системи або користувачів.

Zero-day атаки можуть включати в себе розповсюдження шкідливих програм або використання дефектів у програмному забезпеченні, таких як веб-браузери, операційні системи або додатки. Зловмисники можуть створювати спеціально сформовані віруси, троянські програми, які використовують вразливості, щоб отримати доступ до системи або збирати конфіденційну інформацію.

Zero-day атаки є складними для виявлення і протидії, оскільки вони використовують невідомі раніше вразливості. Тому попередження, швидка реакція та вживання відповідних заходів безпеки є важливими елементами в боротьбі з цим типом кібератак.

3.2 Дослідження методів конфіденційності та цілісності даних для протидії кібератакам в банківській сфері

У сучасному світі, банки стають все частішою мішенню для кібератак. Зловмисники використовують різноманітні методи, щоб отримати доступ до конфіденційної інформації, зламати фінансові системи та спричинити серйозні фінансові втрати. Однак, відповідний захист даних та захист від кібератак можуть зменшити ризики та запобігти потенційним проблемам.

Нижче наведена таблиця, яка містить популярні види кібератак на банки та методи, які активно використовуються та модернізуються для їх запобігання. Ці методи захисту включають навчання персоналу, використання спеціалізованих програмних засобів та фізичних заходів безпеки.

Безпека даних є невід'ємною частиною успішної функціонування банківської сфери. Розуміння ризиків і впровадження адекватних методів захисту можуть допомогти забезпечити конфіденційність та цілісність даних, а також зберегти довіру клієнтів та добре функціонуючі фінансові системи.

У таблиці 3.2 надано інформацію про популярні кібератаки на банки та відповідні методи захисту, які можуть бути використані для запобігання цим загрозам.

Банки та банківські системи використовують різні методи конфіденційності та цілісності даних, щоб захистити себе від кібератак. До цих методів відносяться шифрування даних, щоб забезпечити конфіденційність. Автентифікація, така як от паролі, біометричні дані чи двохфакторна автентифікація. Системи моніторингу які аналізують активність в мережі з метою виявлення підозрілих дій. Резервне копіювання важливих даних в разі їх втрати чи пошкодження.

3.2.1 Методи протидії фішингу

Для протидії фішингу банки проводять систематичне навчання своїх співробітників з питань кібербезпеки, зокрема стосовно виявлення фішингових

атак. Це включає навчання про основні ознаки фішингових електронних листів, підозрілі посилання та вимоги розкриття конфіденційної інформації. Регулярні нагадування та оновлення навичок допомагають співробітникам бути більш обережними і уникати потенційних фішингових схем.

Банки впроваджують мультифакторну автентифікацію для забезпечення додаткового рівня захисту. Крім звичайного введення пароля, цей метод вимагає додаткових перевірок, таких як використання одноразових кодів, біометричних даних або підтвердження засобів доступу (наприклад, мобільних пристроїв). Це робить процес автентифікації складнішим для зловмисників, які намагаються отримати нелегітимний доступ до банківських систем.

Банки використовують спеціалізовані системи виявлення фішингових атак, які аналізують електронні повідомлення, посилання та інші елементи для виявлення ознак фішингу. Ці системи використовують алгоритми машинного навчання та бази даних зі зразками фішингових атак для розпізнавання та блокування підозрілих повідомлень. Це допомагає банкам вчасно виявляти фішингові спроби та запобігати шкоді.

Банки використовують системи перевірки та блокування фішингових веб-сайтів. Вони використовують бази даних зі списками відомих фішингових сайтів та аналізують посилання, які надходять у вхідних повідомленнях або на веб-сторінках, щоб виявити підозрілі або шкідливі посилання. Такі заходи допомагають уникнути небезпеки перенаправлення на фішингові сайти та ненавмисного розкриття особистої інформації.

Банки постійно оновлюють та вдосконалюють свої безпекові заходи для внеможливлення нових методів фішингу. Це включає оновлення програмного забезпечення, встановлення патчів та використання останніх технологій шифрування даних. Регулярні аудити та тестування на проникнення також допомагають виявляти потенційні вразливості та вживати відповідних заходів для їх усунення.

3.2.2 Методи протидії DDoS-атакам

Банки використовують розподілені системи захисту, що дозволяють розподілити навантаження та відбивати атаки на кілька серверів. Це забезпечує високу доступність банківських систем навіть під час масштабних DDoS-атак.

Банки використовують спеціальні пристрої та програмне забезпечення для фільтрації трафіку та виявлення шкідливого або небажаного трафіку, пов'язаного з DDoS-атаками. Ці системи виявляють та блокують небезпечний трафік, що дозволяє забезпечити нормальну роботу банківських сервісів.

Банки використовують технологію кешування контенту, що дозволяє зберігати копії важливих сторінок та даних на різних серверах або в CDN (Content Delivery Network). Це дозволяє зменшити навантаження на сервери та витрати ресурсів під час DDoS-атак.

Банки встановлюють обмеження швидкості для вхідного трафіку з метою запобігання перевантаження серверів під час DDoS-атак. Це може включати обмеження кількості запитів від одної IP-адреси або встановлення лімітів на швидкість передачі даних.

Банки використовують системи моніторингу трафіку, які аналізують і виявляють незвичайну активність або збільшення обсягу запитів. Це дозволяє швидко реагувати на DDoS-атаки та приймати заходи для їх відбиття.

Банки регулярно створюють резервні копії даних та забезпечують їх безпечне зберігання в ізольованих системах або на віддалених серверах. Це дозволяє відновлювати дані після DDoS-атак та запобігає втратам важливої інформації.

Деякі банки використовують хмарні-послуги для розміщення своїх систем. Це дозволяє розподілити навантаження та використовувати інфраструктуру з високою мірою захищеності від DDoS-атак.

3.2.3 Методи протидії Malware

Банки встановлюють та підтримують потужне антивірусне програмне забезпечення на всіх комп'ютерах та серверах. Це допомагає виявляти, блокувати та усувати шкідливі програми, віруси та інші загрози, що можуть спричинити пошкодження або незаконний доступ до банківських даних.

Банки використовують фаєрволи для контролю доступу до мережі та обмеження небажаних підключень. Вони перевіряють трафік на наявність шкідливого програмного забезпечення та блокують небезпечні з'єднання, що допомагає запобігти поширенню Malware та інших загроз.

Банки використовують практику пониження привілеїв, отже користувачі та програми не мають повних адміністративних прав доступу. Це допомагає уникнути неправомірних дій та обмежує можливості поширення Malware, оскільки шкідливі програми не зможуть отримати доступ до важливих системних ресурсів.

Банки пильно стежать за випусками оновлень безпеки для використовуваного програмного забезпечення та оперативно їх встановлюють. Це включає оновлення операційних систем, браузерів, плагінів та інших компонентів, що знижує ризик використання вразливостей зловмисниками.

Банки встановлюють системи перевірки на вторгнення, що допомагають виявити незвичайну або підозрілу активність в мережі та системах. Вони аналізують трафік, журнали подій та інші дані для виявлення можливих атак Malware та негайного реагування на них.

Банки використовують системи моніторингу та аналізу активності для виявлення незвичайної або підозрілої активності на своїх системах. Вони аналізують журнали подій, мережеві з'єднання та інші дані для виявлення можливих атак Malware та реагують на них.

3.2.4 Методи протидії MITM attack

Банки використовують криптографічні протоколи та алгоритми шифрування для захисту конфіденційності даних під час передачі між клієнтами та банківськими серверами. Такі протоколи, як TLS (Transport Layer Security) або SSL (Secure Sockets Layer), забезпечують захищене з'єднання та шифрування даних, унеможливлюючи їх перехоплення та зміну.

Банки вимагають використання валідних сертифікатів SSL/TLS для аутентифікації серверів та перевірки їх справжності. Це допомагає уникнути MITM-атак, оскільки клієнтські програми перевіряють правильність сертифікатів сервера перед встановленням з'єднання.

Банки можуть використовувати тунелювання, таке як VPN (Virtual Private Network), для створення захищених каналів зв'язку між клієнтами та банківськими серверами. Це дозволяє запобігти MITM-атакам, оскільки всі дані, що передаються через такий тунель, шифруються та захищаються від перехоплення.

Банки використовують двофакторну аутентифікацію, де клієнти повинні підтвердити свою ідентичність не тільки за допомогою паролів, але й іншими факторами, такими як OTP (One-Time Password), біометричні дані, апаратні токени або мобільні додатки. Це ускладнює завдання зловмисників, які намагаються перехопити аутентифікаційні дані на шляху спілкування.

Банки встановлюють системи моніторингу мережі та виявлення аномалій, які допомагають виявляти підозрілу активність, включаючи можливі MITM-атаки. Системи аналізують трафік, патерни з'єднань та інші характеристики, щоб виявити потенційні загрози та негайно реагувати на них.

3.2.5 Методи протидії XSS attack

Банки використовують спеціальні механізми фільтрації та екранування для очищення введеного користувачем контенту, що вбудовується на сторінки. Це допомагає уникнути виконання шкідливого JavaScript коду, який може бути впроваджений зловмисниками через вразливості XSS.

Банки встановлюють правила валідації та обмеження для введених даних, щоб запобігти впровадженню шкідливого коду. Наприклад, вони перевіряють, щоб користувач не міг вставляти HTML-теги або JavaScript-код, якщо вони не є допустимими в контексті.

Банки старанно відбирають та використовують безпечні бібліотеки та фреймворки для розробки веб-додатків. Ці інструменти мають вбудовані механізми захисту від XSS, такі як автоматичне екранування введення або захищені методи відображення даних.

Банки встановлюють HTTP заголовки безпеки, такі як Content Security Policy (CSP), що дозволяють встановлювати правила для джерел вмісту, що можуть бути завантажені на сторінки. Це допомагає унеможливити виконання шкідливого коду, якщо зловмисник спробує впровадити його зовнішніми джерелами.

Банки постійно оновлюють свої веб-додатки та системи, виправляючи виявлені вразливості XSS. Вони встановлюють офіційні патчі від розробників програмного забезпечення та системно оновлюються, щоб уникнути використання вразливостей зловмисниками.

Банки встановлюють системи моніторингу, які стежать за активністю на своїх веб-сайтах та додатках. Якщо виявляється спроба XSS-атаки, системи сповіщають адміністраторів та спрацьовують механізми автоматичного реагування, які можуть блокувати атаку та вживати заходів для відновлення безпеки.

3.2.6 Методи протидії A zero-day exploit

Банки постійно та регулярно оновлюють операційні системи, бази даних, серверне програмного забезпечення та інші компоненти, які допомагають уникнути атак, які використовують вразливості "A zero-day exploit".

Банки встановлюють спеціальні системи, які моніторять мережу та виявляють незвичайну або підозрілу активність. Ці системи базуються на підписах відомих атак, поведінковому аналізі та інших алгоритмах, які допомагають виявляти атаки "A zero-day exploit" або їх наслідки.

Банки використовують фаєрволи, які контролюють вхідний та вихідний трафік мережі. Ці системи встановлюють правила фільтрації та блокування, які дозволяють виявляти та блокувати шкідливий трафік, який може бути пов'язаний з атаками "A zero-day exploit".

Банки використовують стратегію сегментації мережі, що дозволяє розділити мережу на окремі зони або сегменти. Це допомагає обмежити поширення атаки у разі її виникнення та зменшує вплив зловмисників на весь банківський сервіс.

Банки використовують сильні методи контролю доступу та автентифікації для запобігання несанкціонованому доступу до систем і даних. Це може включати використання комплексних паролів, біометричних ідентифікаторів, двофакторної аутентифікації та інших методів, що забезпечують високий рівень захисту від атак "A zero-day exploit".

Таблиця 3.2 – Дослідження методів конфіденційності даних для протидії кібератакам в банківській сфері

Кібератака	Методи захисту конфіденційності
Фішинг	Навчання співробітників розпізнавати та уникати небезпек соціального інжинірингу. Встановлення політик безпеки, які забороняють розкриття конфіденційної інформації. Застосування механізмів двофакторної аутентифікації та ідентифікації користувачів.
DDoS-атаки	Використання систем захисту від DDoS-атак. Резервування мережевої інфраструктури для забезпечення відновлення послуг. Впровадження технологій масштабування та обмеження впливу атак.
Malware	Використання антивірусного ПЗ для виявлення та блокування шкідливих програм. Регулярне оновлення ПЗ та ОС для заповнення вразливостей. Обмеження прав доступу та встановлення політик безпеки.
MITM-атаки	Використання шифрування даних за допомогою протоколів SSL/TLS для захисту конфіденційності. Використання сегментованих мереж та фаєрволів для обмеження доступу до систем.
XSS-атаки	Валідація введених даних, що запобігає виконанню шкідливого JavaScript коду на стороні клієнта. Застосування спеціальних заголовків безпеки (Content Security Policy). Регулярне оновлення веб-додатків.
A zero-day exploit	Використання систем виявлення вторгнень (IDS/IPS) для виявлення незвичайної активності. Впровадження технологій вимикання коду та аналізу поведінки для виявлення невідомих загроз.

Таблиця 3.3 – Дослідження методів цілісності даних для протидії кібератакам в банківській сфері

Кібератака	Методи захисту цілісності
Фішинг	Використання механізмів перевірки ідентичності та автентифікації клієнтів перед здійсненням фінансових операцій. Впровадження механізмів моніторингу. Використання алгоритмів визначення аномалій для виявлення спроб шахрайства.
DDoS-атаки	Використання систем захисту від DDoS-атак. Резервне копіювання та відновлення даних для запобігання втраті чи пошкодженню. Використання механізмів розподіленої обробки трафіку.
Malware	Використання антивірусного програмного забезпечення для виявлення та блокування шкідливих програм. Регулярне оновлення ПЗ. Встановлення політик безпеки, що обмежують виконання небезпечного коду.
MITM-атаки	Використання шифрування даних за допомогою протоколів SSL/TLS для запобігання перехопленню та зміні інформації. Використання сертифікатів та цифрових підписів для перевірки автентичності та цілісності комунікації.
XSS-атаки	Валідація введених даних на веб-сайтах для запобігання впровадженню шкідливого коду. Використання механізмів фільтрації, та обмеження JavaScript.
A zero-day exploit	Використання систем виявлення вторгнень (IDS/IPS) для виявлення незвичайної активності. Впровадження технологій вимикання коду та аналізу поведінки для виявлення невідомих загроз. Регулярне оновлення ПЗ.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Стихійні лиха та їх характеристики

Стихійні лиха – це природні явища, які мають негативні наслідки для людей, тварин і навколишнього середовища. Ці явища є непередбачуваними та можуть спричинити значні руйнування та збитки.

Відповідно до видів природних явищ, що спричиняють пов'язані з ними катастрофи, існує багато причин для природних катаклізмів. Загалом стихійне лихо є спричинені кліматичними явищами, геоморфологічними процесами, біологічними факторами чи просторовими явищами. Ці явища вважаються катастрофами, коли вони досягають крайності. Кліматичні стихійні лиха включають тропічні циклони, повені, посуху, лісові пожежі, смерчі, хвилі спеки та хвилі холоду. З іншого боку, маємо космічні катастрофи, які трапляються набагато рідше, ніж вплив метеоритів та астероїдів.

Серед причин, що спричиняють ці катастрофи, маємо наступне:

- кліматичні причини: вони трапляються з коливаннями атмосферної погоди з точки зору температури, опадів, вітрів, атмосферного тиску. Зазвичай саме ця різка зміна атмосферних змінних спричиняє такі явища, як урагани, електричні бурі, торнадо, хвилі холоду чи тепла;
- геоморфологічні причини: вони зазвичай трапляються тоді, коли переміщення тектонічних плит та динаміка земної кори та мантії спричиняють землетруси, цунамі та виверження вулканів;
- біологічні причини: дисбаланс в екосистемах може призвести до зростання патогенних організмів та їх переносників. Таким чином, зростання бактерій та вірусів може створити епідемії або пандемії;
- зовнішній простір: Метеорити та астероїди, що потрапляють в атмосферу Землі, можуть завдати серйозної шкоди;

До найпоширеніших стихійних лих та їх можливостей, що трапляються в різних частинах світу, включають наступні:

- лавина: це падіння великої маси снігу зі стрімкою місцевістю через вплив сили тяжіння. Якщо це відбувається в районах зайнятих людьми чи подорожуючими, то це може призвести до серйозних наслідків;
- тропічний циклон: вони обертаються штормами великої величини. Ці циклони супроводжуються сильними опадами та швидкісними вітрами. Вітри здатні спричиняти дискомфорт у морі, повені, руйнувати інфраструктуру та спричиняти смерті людей;
- наземні гірки: це рух, схожий на лавину, але з похилими наземними масивами він досить крутий. Зазвичай це відбувається внаслідок інтенсивних і тривалих опадів, які насичують ґрунт водою і спричиняють зсув. Вони також можуть відбуватися внаслідок існування землетрусів;
- вплив метеоритів і комет: вони рідкість, але можуть завдати серйозної шкоди;
- град: сильні шторми з опадами крижаного каменю 5-50 мм можуть вплинути і завдати значної шкоди;
- землетрус: підземні коливання, руйнування будівель та інфраструктури
- повінь: Вони утворюються внаслідок розливу великих річок та озер, коли є велика кількість опадів. Довгий покрив може руйнувати інфраструктуру, тягнути тварин і людей, викорчовувати дерева;
- стихійна пожежа: знищення лісів, полів, міст, швидке поширення пожежі;
- торнадо: це продовження хмари, яка утворює конус повітря в обороті. Вони можуть зруйнувати інфраструктуру, пошкодити шляхи сполучення та загрожувати життю тварин та людей;
- цунамі: їх ще називають припливними хвилями. Вони спричинені існуванням підводних землетрусів, які спричиняють великі хвилі, що

рухаються з великою швидкістю. Внаслідок удару на узбережжі вони можуть спричинити великі катастрофи внаслідок удару та повені;

- виверження вулканів: це масові вигнання магми, попелу та газів, що надходять із мантії Землі. Магма дрейфує в потік, який повзе поверхнею Землі і спалює все на своєму шляху;
- електричні бурі: Вони виникають внаслідок накопичення викидів гарячого і вологого повітря, яке потрапляє в досить нестійку атмосферу. Як результат, блискавки та блискавки генеруються у супроводі сильного дощу, вітру та навіть граду;
- піщана буря: штормовий вітер, що розносить пісок та пил, зниження видимості, може спричинити ушкодження очей та дихальних шляхів;
- пожежа: знищення лісів, полів, будівель, небезпечне поширення вогню, яке спричинене сильним вітром, спричинення жертв також, як матеріальні так і екологічні збитки;
- смерч: сильні вітри та дощ, що обертаються навколо центру, руйнування будівель та дерев, спричинення жертв;
- снігопад: сильний снігопад, що може призвести до затруднення руху, пошкодження ліній електропередач, руйнування будівель, може створити небезпеку для життя людей;
- засуха: Це відсутність дощу протягом тривалого часу і, як наслідок, висока температура, через це можливе виникнення пожеж. Врожай втрачається, тварини гинуть, а люди голодом і спрагою змушені покидати територію.

Хоча стихійні лиха мають різні характеристики, вони всі мають серйозні наслідки для людей, тварин та навколишнього середовища.

4.2 Інженерно-технічні рішення з охорони праці

Інженерно-технічні рішення з охорони праці є важливою складовою системи безпеки та здоров'я праці в організації. Вони включають в себе застосування інженерних та технічних засобів, методів та процедур з метою запобігання травмам, професійним захворюванням та іншим ризикам, пов'язаним з працею. Основна мета інженерно-технічних рішень полягає в створенні безпечних та здорових умов праці для працівників.

В банківській сфері інженерно-технічні рішення з охорони праці відіграють важливу роль у забезпеченні безпеки та здоров'я працівників, а також захисту клієнтів і відвідувачів. У банківських установах існують певні особливості і ризики, які потребують уваги при розробці та впровадженні інженерно-технічних рішень з охорони праці. Основні аспекти цих рішень в банківській сфері включають:

- безпека працівників у банківських приміщеннях: Банківські приміщення можуть мати особливості, пов'язані з ергономікою робочих місць, безпекою використання обладнання та іншими факторами. Інженерно-технічні рішення можуть включати раціоналізацію розташування обладнання, використання адаптивних робочих столів та стільців, підвищення освітленості приміщень, встановлення систем вентиляції для забезпечення чистого повітря, а також попередження пожеж та інших небезпек;
- безпека праці під час обслуговування банківського обладнання: Банки використовують різноманітне обладнання, таке як банкомати, касові апарати, комп'ютери, системи безпеки. Інженерно-технічні рішення повинні забезпечувати безпечне використання цього обладнання, включаючи правильне розташування, захист від електричних і механічних ризиків, забезпечення належного охолодження і вентиляції приміщень, а також раціональні системи кабельного управління;

- безпека клієнтів і відвідувачів: У банківській сфері важливо враховувати безпеку не лише працівників, але й клієнтів та відвідувачів. Інженерно-технічні рішення можуть включати встановлення систем відеоспостереження, контроль доступу до обмежених зон, автоматичні системи попередження про надзвичайні ситуації (пожежу, напад), а також правильне розташування вихідних шляхів та евакуаційних виходів;
- організаційні заходи: Окрім інженерно-технічних рішень, важливо враховувати організаційні аспекти охорони праці в банківській сфері. Це може включати надання навчання працівникам щодо безпеки та правил ведення роботи, проведення планових перевірок обладнання, організацію системи звітності про випадки порушення безпеки, контроль за дотриманням нормативних вимог, а також розробку ефективної системи управління охороною праці.

Усі ці заходи спрямовані на забезпечення безпеки працівників та клієнтів банківських установ, запобігання аваріям та непередбаченим ситуаціям, а також зменшення ризиків для здоров'я працівників у банківській сфері.

Загальною метою інженерно-технічних рішень з охорони праці є створення безпечних умов праці, зменшення ризиків і покращення здоров'я та безпеки працівників. Організації повинні ретельно аналізувати свої процеси та робочі середовища, щоб виявити можливі небезпеки та впровадити відповідні інженерно-технічні рішення для їх усунення або зменшення.

ВИСНОВКИ

У процесі дослідження різних аспектів банківської сфери, зокрема кібератак, захисту даних, операцій з даними та інших важливих питань, можна зробити кілька висновків.

Спочатку слід відзначити, що банківська система є привабливою мішенню для кіберзлочинців, оскільки вона містить велику кількість фінансової інформації та особистих даних клієнтів. Кібератаки на банківські системи можуть призвести до витоку даних, фінансових втрат та поглиблення довіри громадськості до банківської сфери.

Для захисту від кібератак банки використовують комплексний підхід, який включає технічні, організаційні та правові заходи. Важливими аспектами є використання сучасних технологій шифрування, механізмів аутентифікації, систем виявлення вторгнень та моніторингу. Також важливо забезпечити фізичну безпеку і контроль доступу до інфраструктури та обладнання.

Операції з даними в банку вимагають високої точності та безпеки. Резервне копіювання та відновлення даних є важливими процесами, щоб забезпечити відновлення інформації у разі втрати або пошкодження. Також варто зазначити значення дотримання нормативних вимог, які включають в себе вимоги до захисту даних, зберігання, обробки особистої інформації та забезпечення приватності клієнтів.

Збір та зберігання даних клієнтів вимагають від банків дотримання високих стандартів безпеки та конфіденційності. Банки повинні використовувати захищені системи для збору, передачі та зберігання даних клієнтів, враховуючи вимоги законодавства про захист персональних даних. Важливо також забезпечити контроль доступу до цих даних та використання ефективних механізмів аутентифікації.

Обробка фінансових транзакцій є однією з найважливіших функцій банку. Забезпечення безпеки та надійності цих операцій є критично важливим

завданням. Банки використовують різні заходи для попередження шахрайства, зловживання та несанкціонованого доступу до фінансових систем. Це включає валідацію та перевірку транзакцій, моніторинг підозрілих активностей, використання систем виявлення фроду та сильну аутентифікацію.

Загалом, захист даних в банківській сфері вимагає комплексного підходу та поєднання технічних, організаційних та правових заходів. Банки повинні постійно оновлювати свої системи, регулярно аудитувати та перевіряти на вразливості, навчати свій персонал та співпрацювати зі спеціалізованими організаціями для забезпечення ефективного захисту від кібератак та збереження конфіденційності та безпеки даних. Лише такий підхід дозволить банкам залишатися впевненими в надійності своїх систем та забезпечувати високий рівень обслуговування своїх клієнтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Big Data in Banking – Leapfrogging into Digital Banking Era https://techvidvan.com/tutorials/big-data-banking/ (10.04.2023)

2. The Importance of Cyber Security in Banking Sector https://intellipaat.com/blog/cyber-security-in-banking/?US#:~:text=The%20main%20objective%20of%20Cyber,be%20safeguarded%20under%20Cyber%20security/ (18.04.2023)

3. Умови обробки персональних даних в Райфайзен банк аваль https://raiffeisen.ua/storage/files/umovy-obrobky-personalnyh-danyh-1-1-1.pdf (23.04.2023)

4. How to Protect Banks from Cyberattacks https://any.run/cybersecurity-blog/how-to-protect-banks-from-cyberattacks (29.04.2023)

5. Загрози безпеки а автоматизованій банківській системі https://studfile.net/preview/9708356/ (25.04.2023)

6. Техніка безпеки під час експлуатації обладнання https://oppb.com.ua/news/tehnika-bezpeky-pid-chas-ekspluataciyi-obladnannya-v-remontnyh-maysternyah (10.05.2023)

7. Стихійні лиха https://www.meteorologiaenred.com/uk/desastres-naturales.html (16.05.2023)