МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ"

на здобуття освітнього ступеня магістра
за спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

________ Наум МАРЧЕНКО
(Підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Наум МАРЧЕНКО

Керівник:
к.т.н. Юрій ЩАВІНСЬКИЙ

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ

Завідувач кафедрою УІКБ

_________ Світлана ЛЕГОМІНОВА

“____”____________2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Марченку Науму Івановичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Технічні аспекти захисту інформації в автоматизованих системах управління”

керівник кваліфікаційної роботи Юрій ЩАВІНСЬКИЙ, к.т.н.

(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи “18” грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека автоматизованих систем, техннічні аспекти захисту інформації, криптографічний захист інформації.*

4. Перелік питань, які потрібно розробити:
   1. Зробити аналіз вітчизняної та зарубіжної наукової літератури та аналіз поточного стану інформаційної безпеки.
   2. Розкрити застосування технічних засобів захисту інформації в АСУ.
   3. Розробити план заходів забезпечення інформаційної безпеки в АСУ та пропозиції до політики безпеки.
   4. Провести тестування та оцінку результатів.
   5. Оцінити ефективність заходів та виявити можливі недоліки.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р..

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури та аналіз поточного стану інформаційної безпеки	15.10.2023	
3.	Аналіз технічних та криптографічних засобів захисту інформації	25.10.2023	
4.	Аналіз захисту мережевої інфраструктури	11.11.2023	
5.	Розробка плану заходів забезпечення інформаційної безпеки	15.11.2023	
6.	Тестування та оцінка результатів, формулювання висновків	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	16.01.2024	

Здобувач вищої освіти ______________ Наум МАРЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи ______________ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Марченко Н.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: “Технічні аспекти захисту інформації в автоматизованих системах управління”
Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _______________ Віталій САВЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

МАРЧЕНКО Наум у своїй кваліфікаційній роботі проаналізував сучасний стан та проблеми захисту в автоматизованих системах управління та встановив недосатнє приділення уваги фахівцями автоматизованих систем питанням захисту інформації, яка циркулюється в автоматизованих системах управління. Виявлені ключові виклики в цій області спонукали до розроблення в роботі конкретних заходів для покращення технічних і криптографічних методів забезпечення безпеки в автоматизованих системах управління. **МАРЧЕНКО Наум** продемонстрував глибоке розуміння тематики дослідження та бачення основних теоретичних та практичних напрямів її вирішення, здатність до самостійного наукового аналізу та організаційні навички, проявив себе як організований, відповідальний виконавець.. Його дослідження було представлено і високо оцінено на науково-практичній конференції.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **МАРЧЕНКА Наума** на оцінку “відмінно” та присвоїти йому кваліфікацію “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Керівник кваліфікаційної роботи ________ Юрій ЩАВІНСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“___________2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Марченко Н.І,. допускається до захисту роботи в екзаменаційній комісії

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _______________ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА

на кваліфікаційну магістерську роботу

здобувача вищої освіти Марченка Наума Івановича
на тему "ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ "

Актуальність Актуальність темидослідження полягає в недостатній увазі фахівців автоматизованих систем захисту інформації, що в них циркулює. Сучасний розвиток інформаційних технологій потребує відпрацювання додаткових досліджень у застосуванні організаційних та технічних засобів інормаційної безпеки в автоматизованих системах, що було здійснено у даній роботі.

Позитивні сторони

Проведений аналіз ефективності технічних аспектів захисту інформації в автоматизованих системах, розглянуті основні поняття і принципи, а також оціненений сучасний стан цієї проблематики в Україні, застосовані сучасні методи наукових досліджень дозволили здобувачу правильно визначити ключові фактори і виклики, що впливають на ефективність захисту інформації у автоматизованих системах управління.

Запропоновані конкретні рекомендації для покращення управління інформаційною безпекою та розроблена методика технічного захисту інформації можуть бути застосовані на початковому етапі створення автоматизованих систем управління інформаційною безпекою в компаніях середнього та малого бізнесу. Ці методи та підходи також можуть бути корисними для покращення існуючих систем і оптимізації роботи відділу безпеки.

Недоліки

Було б також доцільно у роботі запропонувати шляхи застосування штучного інтелекту в перспективній автоматизованій системі управління. Однак, зазначене зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно» а її автор Марченко Наум Іванович - присвоєння кваліфікації «Магістр кібербезпеки» за освітньо-професійною програмою «Управління інформаційною безпекою».

Рецензент: завідувач кафедри Інформаційної та кібернетичної безпеки, д.т.н, професор		Галина ГАЙДУР
	підпис	*(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 100 стор., 14 рис., 11 табл., 57 джерел.

Метою роботи є аназіз сучасного стану інформаційної безпеки в автоматизованих системах управління та визначення пропозицій підвищення ефективності захисту інформації і їх оцінка.

Об'єктом дослідження – захист інформації в автоматизованих системах управління.

Предмет дослідження – ефективність впровадження технічних засобів захисту інформації в автоматизованих системах управління.

Методи дослідження. У даній науковій роботі для вирішення поставленої задачі були використані такі методи: системний аналіз, теорія інформаційної безпеки, порівняння, теоретичне узагальнення, кейс-стаді, а також аналіз та синтез.

Короткий зміст роботи. У цій роботі було здійснено аналіз ефективності технічних аспектів захисту інформації в автоматизованих системах, розглянуто основні поняття і принципи, а також оцінено сучасний стан цієї проблематики в Україні. Визначено ключові фактори і виклики, що впливають на ефективність захисту інформації. В кінцевому розділі розглянуто основні тенденції і проблеми, вказано на важливі аспекти, що слід враховувати при розробці та впровадженні захисних технологій в банківських системах. Також були запропоновані конкретні рекомендації для покращення управління інформаційною безпекою.

Галузь застосування. Розроблені основні пункти та методики технічного захисту інформації, можуть бути застосовані на початковому етапі створення систем управління інформаційною безпекою в компаніях середнього та малого бізнесу. Ці методи та підходи також можуть бути корисними для покращення існуючих систем і оптимізації роботи відділу безпеки.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ, АВТОМАТИЗОВАНІ СИСТЕМИ .

ABSTRACT

The text part of the qualification work for the degree of Master's Degree: 100 pages, 14 figures, 11 tables, 57 sources.

The purpose of the work is the analysis of the current state of information security in automated management systems and the determination of proposals for improving the effectiveness of information protection and their evaluation.

Object of research is the information protection in automated management systems..

Subject of research is the effectiveness of implemented technical means of information protection in automated management systems

Research methods In this scientific work, the following methods were used to solve the problem: system analysis, information security theory, case stage, comparison, theoretical generalization, as well as analysis and synthesis.

Brief content of research. The studied standards and legislative norms, as well as the developed basic points and methods of technical information security, can be applied at the initial stage of creating information security management systems in small and medium-sized businesses. These methods and approaches can also be useful for improving existing systems and optimizing the work of the security department.

Field of research. The studied standards and legislative norms, as well as the developed basic points and methods of technical information security, can be applied at the initial stage of creating information security management systems in small and medium-sized businesses. These methods and approaches can also be useful for improving existing systems and optimizing the work of the security department.

KEYWORDS: INFORMATION SECURITY OF AN ENTERPRISE, THREAT TO INFORMATION SECURITY, TECHNICAL MEANS OF PROTECTION, AUTOMATED SYSTEMS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CIA (Confidential Integrity Availability) - Конфіденційність, цілісність та доступність.

DoS/ DDoS – Відмова в обслуговувані/ Розподілена атака на відмову в обслуговуванні.

ISO/IEC (International Organization for Standardization /International Electrotechnical Commission) – Міжнародна організація із стандартизації/ Міжнародна електротехнічна комісія.

ІБ – інформаційна безпека

NIST (National Institute of Standards and Technology) – Національний інститут стандартів і технології.

GDPR (General Data Protection Regulation) – Загальний регламент захисту даних.

PCI DSS (Payment Card Industry Data Security Standard) - стандарт безпеки даних індустрії платіжних карток.

HIPAA (Health Insurance Portability and Accountability Act) - є актом про мобільність та підзвітність медичного страхування.

СУІБ - системи управління інформаційною безпекою

FISMA (Federal Information Security Management Act) - Федеральний закон про безпеку інформаційних систем.

BYOD (Bring your own device) – Принесіть свій власний пристрій (Мається на увазі використання в роботі власних ноутбуків або смартфонів).

AI (Artificial intelligence) – штучний інтелект.

SOC (Security operation center) – Операційний центр безпеки.

LAN (Local Area Network) – Локальна комп’ютерна мережа

NGFW (Next generation firewall) – файрвол наступного покоління

EDR (end-point detection and response) – система реагування на кінцевих пристроях

SIEM (Security information and event management) Управління подіями та інформаційною безпекою.

ВСТУП

Актуальність теми. Технічні аспекти захисту інформації в автоматизованих системах є важливою темою, особливо в контексті України. Це складний процес, який впливає на всю роботу компаній та організацій, оскільки об'єднує різні процеси, методи, алгоритми, людей та законодавство. Кожна компанія має свій підхід до створення ефективної системи захисту, зважаючи на зростаючу кількість загроз. Результати дослідження допоможуть компаніям розробити або покращити свої системи управління інформаційною безпекою.

Крім цього кількість загроз та факторів що націлені на зловмисні дії з кожним днем лише збільшуються, через це досить актуальним стає питання як створити корпоративну СУІБ та відповідно покращення вже наявної.

З огляду на зазначене тема кваліфікаційної робити є актуальною, а її результати дозволять компаніям різних сегментів розробити свою робочу систему управління ІБ в той час як організаціям вже з наявною системою дозволить покращити та підняти її ще на вищий рівень.

Мета роботи полягає у аназізі сучасного стану інформаційної безпеки в автоматизованих системах управління та визначенні пропозицій підвищення ефективності захисту інформації і їх оцінці.

Об'єкт дослідження – захист інформацій в автоматизованих системах управління.

Предмет дослідження – ефективність впровадженння технічних засобів захисту інформації в автоматизовані система управління.

Для досягнення цієї мети в роботі виконані наступні *завдання:*

1. Зробленй аналіз вітчизняної та зарубіжної наукової літератури та сучасного стану інформаційної безпеки у автоматизованих системах управління і визначені основні проблеми.

2. Розроблений план заходів забезпечення інформаційної безпеки.

Методи дослідження. Для вирішення поставленого наукового завдання в роботі були застосовано метод системного аналізу, теорія інформаційної безпеки та метод порівняння та теоретичного узагальнення, кейс-стаді, аналізу та синтезу.

Наукова новизна одержаних результатів. У роботі представлено новий підхід до створення систем управління інформаційною безпекою (СУІБ), який базується на інтегрованому використанні кадрових ресурсів, технічних і програмних рішень, спрямованих на автоматизацію та оптимізацію процесів. Окрім цього, удосконалено критерії оцінки ефективності засобів захисту та алгоритми удосконалення технічного захисту інформації в автоматизованих системах управління банків.

Практичне значення одержаних результатів. Використання запропонованих рекомендацій дозволить створити модульну систему ефективних технічних засобів захисту інформації в автоматизованих банківських системах України. Це суттєво підвищить ефективність організаційного процесу в контексті інформаційної безпеки. Завдяки цим методам та матеріалам, компанія, яка раніше не займалася інформаційною безпекою, зможе досягнути первинного рівня захищеності з перспективою подальшого розвитку.

Апробація результатів кваліфікаційної роботи було оприлюднено на науково-практичній конференції:

Марченко Н.І. ТЕХНОЛОГІЧНІ ГОРИЗОНТИ: ДОСЛІДЖЕННЯ ТА ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ТЕХНОЛОГІЧНОГО ПРОГРЕСУ УКРАЇНИ І СВІТУ : ВСЕУКР. НАУКОВО-ПРАКТ. КОНФ., м. Київ, 28 лис. 2023 р. Київ, 2023. С. 98–101.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

1.1 Аналіз наукових досягнень захисту інформації в автоматизованих системах управління

Дослідження вітчизняної літератури дає унікальне розуміння місцевих особливостей та підходів у захисті інформації в автоматизованих системах управління (АСУ). Аналіз охоплює роботи, що розглядають як теоретичні основи, так і практичні аспекти захисту інформації, включаючи кейс-стаді, огляди імплементацій специфічних технологій та їх ефективність у місцевих умовах.

Поглиблене вивчення термінології допоможе уникнути непорозумінь та помилкових інтерпретацій. Особлива увага приділяється дефініціям ключових понять, таких як "кібербезпека", "захист даних", "криптографічний захист", "система управління інформаційною безпекою" тощо, їх історичному розвитку та контексту використання [1].

Детальний огляд історії розвитку включає аналіз зміни технологій, законодавчих рамок та стратегій управління інформаційною безпекою. Вивчаються періоди значних технологічних змін, вплив глобальних кіберзагроз, регіональні особливості розвитку сфери безпеки, та вплив міжнародних тенденцій на місцеві практики.

Аналіз сучасних принципів включає дослідження міжнародних та національних стандартів, використання передових практик і методологій, таких як ризик-орієнтоване управління, застосування штучного інтелекту в захисті інформації, та інтеграція захисту даних на етапі проектування систем.

Огляд ключових досліджень та розробок дозволить виявити передові технології та інноваційні рішення у сфері захисту інформації. Це може включати огляд новітніх алгоритмів шифрування, розробок у галузі штучного інтелекту для захисту інформації, та інших перспективних технологій [1].

Вивчення регуляторних вимог та стандартів є критично важливим для забезпечення відповідності діяльності в області захисту інформації законодавчим нормам. Це включає аналіз національного та міжнародного законодавства, нормативних документів, стандартів ISO/IEC у сфері інформаційної безпеки, та інших регулятивних актів [2,3].

Кожен з цих пунктів відкриває широкі можливості для детального дослідження та аналізу, допомагаючи створити всебічний та глибокий огляд захисту інформації в автоматизованих системах у контексті вітчизняних умов та глобальних тенденцій.

Важливим є вивчення та аналіз широкого спектру зарубіжних досліджень, що висвітлюють сучасний стан та розвиток у обраній галузі. Вона включає в себе вибір актуальних і впливових досліджень, оцінку їх якості та достовірності, а також аналіз методологій і отриманих результатів. Пошук відбувається через різноманітні бази даних та наукові ресурси.

Основна увага науковців приділяється виявленню глобальних трендів, які впливають на науку в цілому та на конкретну галузь зокрема. Огляд включає в себе вивчення розвитку технологій, наукових підходів та їх впливу на міжнародному рівні. Для цього слідкується за міжнародними конференціями, вебінарами та новими публікаціями [4,5].

Детальне вивчення і порівняння різноманітних методологій, підходів та технологій, які використовуються у зарубіжній науці, унікальність кожного підходу, його переваги та недоліки, зіставляючи різні методи та техніки, представлені у науковій праці [4], дозволяють зробити важливі висновки щодо ефективності технічних засобів, які застосовуються при управлінні інформаційною безпекою в автоматизованих системах управління.

Аналіз наукової літератури дозволив визначити, як у різних країнах підходять до питань захисту інформації, вивчаються відповідні законодавчі рамки та міжнародні стандарти. Цей аспект включає в себе огляд офіційних документів та рекомендацій відомих організацій, таких як ISO, і є ключовим для розуміння глобальних норм у сфері захисту даних. Здійснюється вивчення провідних наукових робіт, які мають значний вплив на розвиток галузі. Цей аналіз включає в себе оцінку новаторства, впливу та методів, які використовувалися в ключових дослідженнях. Особлива увага приділяється роботам, що отримали високе визнання у науковому співтоваристві [6].

При вивченні провідних наукових робіт, які мають значний вплив на розвиток галузі науковцями застосовується метод кейс-стаді, який включає в себе оцінку новаторства, впливу та методів, які використовувалися в ключових дослідженнях. Особлива увага приділяється роботам, що отримали високе визнання у науковому співтоваристві [6-8].

Основи теорії захисту інформації, принципи побудови систем захисту інформації в комп'ютерних системах та мережах, а також правові аспекти захисту інформації детально розглянуті в роботі [6]. Праця є навчальним посібником, що охоплює широкий спектр питань інформаційної безпеки, включаючи методи та засоби захисту інформації в автоматизованих системах. Особлива увага приділяється шифруванню транзакційних даних в АСУ, які містять конфіденційну інформацію про клієнтів та їхні фінансові операції. Важливим аспектом є також використання захищених каналів передачі даних, які гарантують, що інформація залишається недоступною для сторонніх під час її передачі.

Автор у своєму дослідженні [7] розкриває теоретичні основи кібербезпеки, включаючи аналіз ризиків, методи захисту інформації та стратегії протидії кіберзагрозам. Робота є дуже значущою та інформативною у сфері кібербезпеки та захисту інформації. Вона становить важливий внесок в розуміння сучасних технічних аспектів захисту інформації та кібербезпеки. Перш за все, вона представляє докладний огляд основних концепцій та принципів кібербезпеки. Автор ретельно розглядає теоретичні аспекти цієї проблеми, надаючи глибоке розуміння сутності кібербезпеки. Він пояснює, чому ця тема є настільки важливою в сучасному світі, де інформація стала однією з найцінніших активів.

Далі, автор розглядає практичні аспекти кібербезпеки. Він детально описує різні методи та техніки захисту від кібератак, включаючи технічні засоби захисту, мережеву безпеку та інші аспекти. Визначена інформація про те, як впроваджувати заходи з кібербезпеки в практичних умовах та як забезпечити безпеку інформації у сучасних АСУ.

Особливо важливою є розділ про аналіз сучасних загроз та трендів у сфері кібербезпеки [8]. Автор надає огляд сучасних кіберзагроз та вказує на їх потенційні наслідки для організацій та суспільства в цілому. Він також розглядає нові технологічні та соціальні тренди, які впливають на кібербезпеку. Праця є цінним ресурсом для фахівців у сфері інформаційної безпеки, студентів та всіх, хто цікавиться цією важливою темою. Вона об'єднує теоретичний підхід із практичними порадами, надаючи читачам різні інструменти та стратегії для забезпечення безпеки інформації. Праця також актуальна через свій підхід до аналізу сучасних загроз та трендів, що робить її важливим джерелом інформації для всіх, хто цікавиться кібербезпекою.

У дослідженні [9] автори аналізують сучасні методи криптографічного захисту інформації, їх переваги та недоліки, а також практичне застосування в різних сферах. Важливу роль у роботі відіграє аналіз реальних кейс-стаді та прикладів використання криптографії у захисті даних в різних сферах, включаючи фінансовий сектор, державні установи та приватний бізнес. Це дозволяє краще зрозуміти практичне застосування теоретичних знань у реальних ситуаціях.

Інше дослідження [10] присвячене аналізу питань забезпечення безпеки в автоматизованих системах обробки інформації. Автор розглядає ключові аспекти інформаційної безпеки, такі як захист даних, управління доступом, виявлення та запобігання несанкціонованому доступу. Можна сказати, що це дуже важлива та актуальна праця в сфері кібербезпеки та захисту інформації в автоматизованих системах. Автор звертається до різних аспектів цієї проблеми та розглядає їх з точки зору технічних аспектів. Перш за все, автор розглядає основні загрози та виклики, з якими стикаються автоматизовані системи в сучасному світі. Він надає читачам глибоке розуміння різних видів кібератак та вказує на їх наслідки для організацій та користувачів. Особливу увагу приділяється аналізу загрози для інформації та даних, які зберігаються та обробляються в автоматизованих системах.

Далі, автор представляє технічні засоби захисту інформації. Він описує різні методи шифрування, аутентифікації та виявлення загроз, які використовуються для забезпечення безпеки інформації в автоматизованих системах. Важливою частиною аналізу є розгляд технічних характеристик та ефективності цих засобів захисту в АСУ.

Крім того, автор докладно розглядає вітчизняний контекст захисту інформації в автоматизованих системах. Він вказує на особливості та виклики, які виникають українським організаціям та органам влади в цій сфері. Такий підхід допомагає читачам краще розуміти специфіку захисту інформації в українському контексті.

Особливу цінність становить те, що робота поєднує теоретичний підхід із практичними рекомендаціями. Автор надає практичні поради щодо вдосконалення безпеки їх автоматизованих систем та захисту інформації.

Зарубіжні автори у своїх наукових дослідженнях [11-14] обговорюють різні аспекти криптографії, включаючи шифрування, яке використовується в банківських системах, проводиться комплексний огляд концепцій та практик захисту мереж, в тому числі в контексті банківських систем? історичний контекст шифрування і його застосування, що може бути важливим для розуміння його розвитку в автоматизованих системах управління, банківській сфері.

Дослідження [11] є однією з ключових праць у сфері криптографії. Ця робота відіграє значну роль у формуванні розуміння криптографії, оскільки охоплює великий діапазон тем, від основних принципів до більш складних аспектів. Вона детально розглядає різноманітні алгоритми та протоколи, які використовуються у криптографії. Автор надає глибоке розуміння як традиційних, так і сучасних криптографічних технік. Він висвітлює не тільки теоретичні аспекти, але й практичну реалізацію цих технік у програмуванні, особливо у мові C, що робить цю книгу цінним ресурсом для розробників та дослідників у сфері захисту інформації в САУ.

Автор використовує зрозумілу та доступну мову, що робить придатним не тільки для експертів, але й для тих, хто тільки починає знайомство з криптографією. Він детально розкриває кожен алгоритм і протокол, надаючи приклади та пояснення, які допомагають краще зрозуміти складні концепції.

Однією з визначальних рис роботи є велика кількість прикладів джерельного коду, що дозволяє читачам не тільки теоретично вивчити алгоритми, але й побачити, як вони можуть бути реалізовані на практиці. Це робить роботу надзвичайно корисною для практикуючих програмістів та розробників систем безпеки.

Деякі технології та методи, описані у роботі, можуть бути застарілими через швидкий розвиток технологій, основні принципи та підходи, викладені Schneier, залишаються актуальними. Книга надає міцну основу для розуміння ключових концепцій та розвитку навичок у сфері криптографії та кібербезпеки.

Наукова праця [15] є комплексним посібником, який охоплює широкий спектр тем, пов'язаних з комп'ютерною та інформаційною безпекою. У ній розглядаються різні аспекти безпеки IT-систем, включаючи захист мереж, шифрування даних, управління ризиками, політики безпеки та методи протидії кіберзлочинам, створення систем управління інформаційною безпекою

Дослідження [15-16] визначають різні техніки та стратегії, які використовуються хакерами для виявлення вразливостей у комп'ютерних системах та програмному забезпеченні АСУ. Книга надає читачам глибоке розуміння принципів та методів хакінгу, включаючи програмування, використання мереж та аналіз безпеки.

Ці ресурси будуть особливо корисними для розуміння конкретних технічних та правових аспектів, що регулюють захист інформації в Україні, і вони допоможуть отримати глибинні знання про національні стандарти та вимоги.

На міжнародному рівні більша увага приділяється використанню передових алгоритмів шифрування, таких як AES (Advanced Encryption Standard) та RSA, для захисту банківської інформації. Зарубіжні дослідження також зосереджуються на використанні протоколів безпеки, таких як TLS (Transport Layer Security), для забезпечення безпечної передачі даних між банківськими системами та клієнтами.

Важливим є аналіз загроз та вразливостей АСУ банківських систем, зокрема, шляхом проведення пентестів (Penetration Testing) для виявлення потенційних слабких місць у системах захисту інформації.

Результати дослідження [17] забезпечують глибоке розуміння основних принципів інформаційної безпеки. У цьому навчальному посібнику ретельно розглядаються різноманітні аспекти захисту даних, що охоплюють широкий спектр тем від основних концепцій до складних технічних рішень.

Автори детально описують концепції, які лежать в основі інформаційної безпеки, включаючи ідентифікацію та автентифікацію, керування доступом, шифрування, а також політики безпеки. Важливу увагу приділяється також розгляду загроз інформаційній безпеці та способам їх виявлення та нейтралізації, включаючи кібератаки та внутрішні загрози.

Посібник також зосереджується на практичних аспектах інформаційної безпеки, надаючи читачам знання про реалізацію ефективних систем безпеки, аналіз ризиків та розробку політик безпеки. Особливу увагу автори приділяють розгляду сучасних технологічних рішень у сфері захисту даних, таких як хмарні технології, мобільна безпека та шифрування даних.

В цілому, посібник представляє собою комплексне джерело знань, яке охоплює як теоретичні, так і практичні аспекти інформаційної безпеки. Він відіграє ключову роль у підготовці спеціалістів у галузі кібербезпеки та є важливим ресурсом для студентів, які прагнуть зрозуміти складність та актуальність захисту інформації у сучасному цифровому світі.

Цей аналіз охоплює широкий спектр джерел, включаючи наукові статті, монографії, навчальні посібники, а також сучасні дослідження та розробки у галузі кібербезпеки. Основна мета полягає у виявленні основних тенденцій, методологій та технологій, що використовуються у світовій практиці для захисту інформації, а також у порівняльному аналізі з вітчизняними підходами та розробками.

Значущим внеском у сферу інформаційної безпеки є ключові аспекти захисту інформації в комп'ютерних системах, включаючи як технічні, так і програмні засоби. Автори, аналізують різні методики і стратегії захисту даних, від розгляду фізичних засобів безпеки до впровадження складних криптографічних рішень. Важливим є огляд сучасних тенденцій у цій галузі, таких як захист інформації в хмарних сервісах та застосування штучного інтелекту для виявлення та протидії кіберзагрозам. Автори включили в роботу детальний аналіз ризиків, пов'язаних з різними типами комп'ютерних систем, та методи їх мінімізації, включаючи огляд потенційних вразливостей та способів їх усунення.

Також важливим є розгляд міжнародних та національних стандартів захисту інформації, що включає в себе детальне вивчення законодавчих вимог та нормативних документів. Це дозволяє не лише зрозуміти загальноприйняті методики та практики захисту інформації, але й оцінити їхню ефективність та актуальність у сучасному контексті.

У сукупності, дослідження науковців та їх висновки надають цілісний погляд на проблематику захисту інформації, поєднуючи теоретичні засади з практичними рішеннями. Це робить її важливим ресурсом для фахівців у сфері кібербезпеки та інформаційних технологій, а також для студентів, які прагнуть зрозуміти складність та важливість цієї галузі.

Порівняльний аналіз наукових досліджень дозволяє виявити особливості та напрямки кожної наукової праці з метою застосування в управлінській діяльності при створенні система інформаційної безпеки в автоматизованих системах управління різного призначення [18-19]. Аналіз зведений в таблиці 1.1-1.2.

Таблиця 1.1

Порівняльний аналіз досліджень вітчизняних і зарубіжних науковців

Назва	Автор(и)	Основний Фокус	Ключові Особливості
"Захист інформації в комп'ютерних системах"	А.І. Пилипенко, В.В. Шестаков	Комплексний погляд на захист інформації в комп'ютерних системах	Поглиблений аналіз ризиків, обговорення сучасних технологій і стандартів, практичні рекомендації
"Інформаційна безпека: Навчальний посібник"	О.О. Рижов, О.В. Горбенко	Освітній підхід до інформаційної безпеки	Широкий огляд теорій та практик, акцент на практичному застосуванні знань
"Методи та засоби криптографічного захисту інформації"	В.К. Омельченко, О.І. Чернишенко	Фокус на криптографічних методах захисту	Детальний розгляд криптографічних алгоритмів, сучасні тенденції в криптографії
"Інформаційна безпека автоматизованих систем"	О. Клименко	Забезпечення безпеки в автоматизованих системах	Розгляд автоматизованих систем з точки зору технічних аспектів.
"Кібербезпека: теорія і практика"	В. Горбунов	Практична та теоретична складова кібербезпеки	Розуміння сучасних технічних аспектів захисту інформації та кібербезпеки.
"Applied Cryptography"	Bruce Schneier	Практичне застосування криптографії	Поглиблений аналіз алгоритмів, їхнє програмування, високий рівень технічних деталей
"Cryptography and Network Security"	William Stallings	Комбінація криптографії та мережевої безпеки	Поєднання теоретичних основ та практичних аспектів, сучасні технологічні рішення
"The Code Book"	Simon Singh	Історія та розвиток криптографії	Легкий для розуміння, охоплює широкий історичний контекст, зосередження на майбутніх тенденціях
"Computer and Information Security Handbook"	J.R. Vacca & T.J. Mullen	Захист інформації в автоматизованих системах	Обширність і докладність в розгляді технічних аспектів кібербезпеки.
"Hacking: The Art of Exploitation"	J. Erickson	Хакінг та комп’ютерна безпека	Техніки та методи, які використовуються хакерами для вторгнень та експлуатації вразливостей.

Таблиця 1.2

Спільні та відмінні особливості кожної роботи

Назва	Спільне	Відмінне
"Захист інформації в комп'ютерних системах"	Комплексний погляд на захист інформації	- Поглиблений аналіз ризиків - Обговорення сучасних технологій
"Інформаційна безпека: Навчальний посібник"	Освітній підхід до інформаційної безпеки	- Широкий огляд теорій та практик - Акцент на практичному застосуванні
"Методи та засоби криптографічного захисту інформації"	Фокус на криптографічних методах захисту	- Детальний розгляд алгоритмів - Сучасні тенденції в криптографії
"Інформаційна безпека автоматизованих систем"	Всесторонній підхід до інформаційної безпеки	- Широкий огляд теорій та практик - Обговорення сучасних технологій
"Кібербезпека: теорія і практика"	Історія та розвиток кібербезпеки, розбір теорій та практик	- Детальний огляд та розбір кібербезпеки як напрямку
"Applied Cryptography"	Практичне застосування криптографії	- Поглиблений аналіз алгоритмів - Програмування алгоритмів - Високий рівень технічних деталей
"Cryptography and Network Security"	Поєднання криптографії та мережевої безпеки	- Теоретичні основи і практичні аспекти - Сучасні технологічні рішення
"The Code Book"	Історія та розвиток криптографії	- Легкість розуміння - Широкий історичний контекст
"Computer and Information Security Handbook"	Фокус на криптографічних методах захисту	- Зосередження на майбутніх тенденціях - Більш загальна інформація
"Hacking: The Art of Exploitation"	Практичне застосування хакінгу	- Теоретичні основи і практичні аспекти - Легкість сприйняття

1.2 Аналіз поточного стану інформаційної безпеки в автоматизованих системах управління

На сьогоднішній день в Україні інформаційна безпека стала однією з найбільш важливих складових національної безпеки. Після збройного конфлікту та агресії російської федерації проти України в 2014 році, що призвело до незаконної анексії Криму та початку окупації ОРДЛО, питання інформаційної безпеки стали надзвичайно актуальними та складними. Ці виклики для України стали ще більш актуальними 24 лютого 2022 року, коли російська армія широкомасштабно вторглася на її територію.[10]

Було вирішено провести аналіз стану та технічних аспектів захисту інформації в автоматизованих банківських системах. Ця тема є актуальною для сьогодення оскільки кількість загроз та атак на банківську систему постійно зростає і є неабиякий попит у захисті банківської інформації.

Аналіз поточного стану інформаційної безпеки в автоматизованих банківських системах можна розбити на кілька ключових етапів (рис. 1.1)

Рис. 1.1. Аналіз поточного стану інформаційної безпеки в автоматизованих банківських системах

- Технологічна інфраструктура: важливо оцінити використовувані технології, включаючи апаратне і програмне забезпечення. Це включає сервери, мережеві пристрої, бази даних та інші компоненти.

- Політики та процедури: аналізується наявність та ефективність політик і процедур безпеки. Важливо перевірити, чи вони відповідають стандартам галузі, таким як ISO 27001, PCI DSS тощо.
- Шифрування даних: особлива увага до механізмів шифрування, що використовуються для захисту даних під час їх передачі та зберігання.
- Керування доступом: аналіз систем управління доступом, включаючи автентифікацію та авторизацію користувачів.
- Запобігання витоку даних: оцінка механізмів, спрямованих на запобігання несанкціонованому доступу або розголошенню конфіденційної інформації.
- Інцидентне реагування: аналіз процедур реагування на інциденти безпеки, включаючи плани відновлення після аварій.

На етапі проектування комплексних систем захисту інформації (КСЗІ), в АСУ важливо використовувати різні моделі безпеки (рис. 1.2).

Ці моделі дозволяють нам уявити, як елементи цієї системи будуть взаємодіяти та як можна забезпечити безпеку інформації. Використання цих моделей дозволяє провести дослідження і оцінити, наскільки ефективно КСЗІ буде захищати від сучасних загроз, таких як інформаційна безпека, кібербезпека, та змоделювати можливі деструктивні події та їх потенційні економічні наслідки у разі втрати банківської інформації. Це дозволяє ефективно планувати та забезпечувати безпеку активів банківської інформації в автоматизованих банківських системах [21] .

Аналіз показав, що при розробці комплексних систем захисту інформації (КСЗІ) часто використовується модель ЦКД (цілісність-конфіденційність-доступність) або її варіації. Перший підхід до створення та оцінки КСЗІ полягає в тому, щоб виконувати вимоги, які встановлені регуляторами або стандартами безпеки. Основним критерієм ефективності в такому випадку може бути мінімізація витрат на виконання цих вимог. Однак недоліком цього підходу є його статичність та відсутність можливості адаптуватися до мінливих загроз [22-23] .

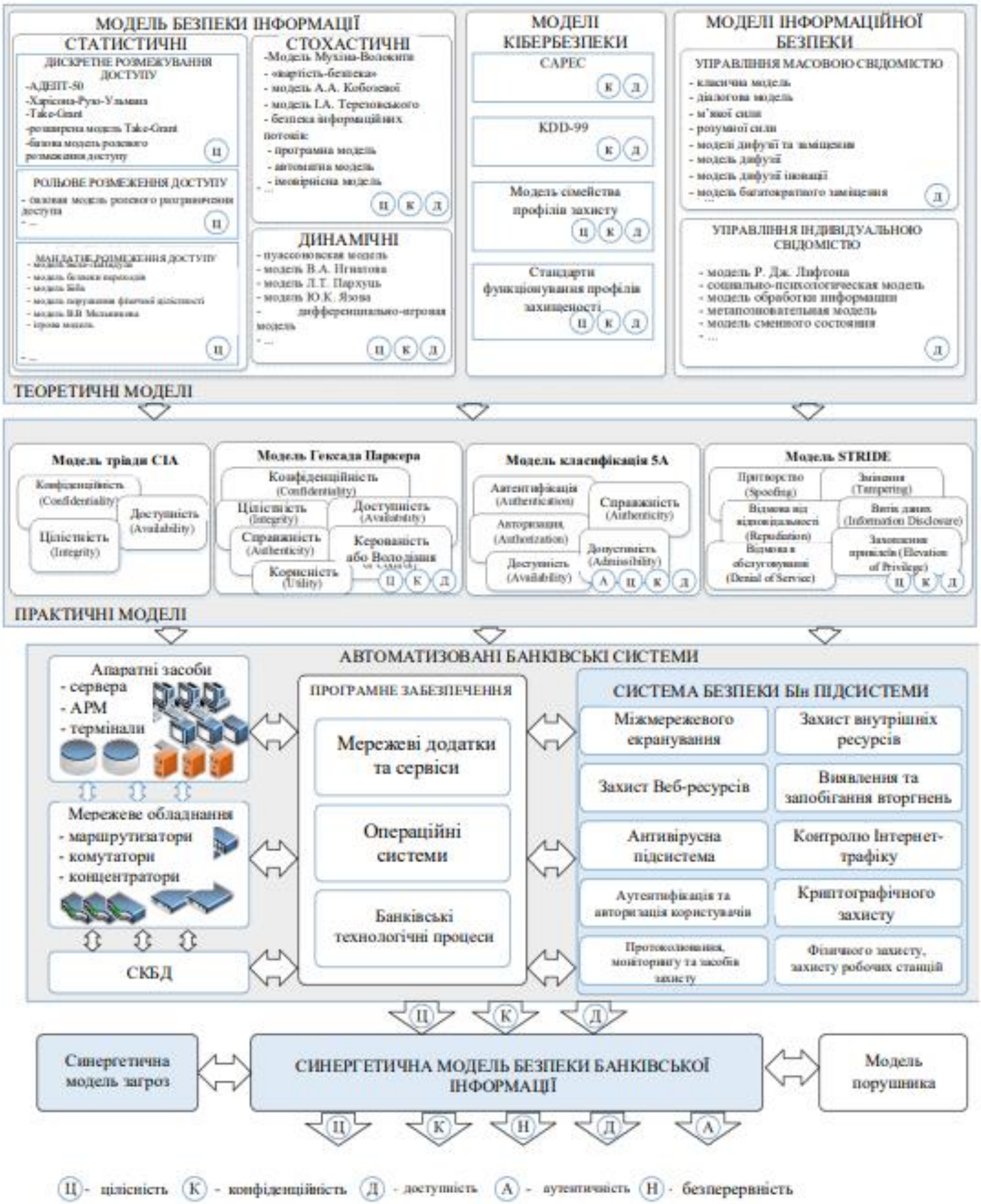

Рис. 1.2. Моделі безпеки

Другий підхід до створення та оцінки КСЗІ базується на принципі "розумної достатності", але це може не завжди передбачати потенційно деструктивні заходи загроз та приймати ризики. Цей підхід часто вимагає експертної оцінки та грошових витрат і може бути суб'єктивним. Такий підхід також вимагає постійного моніторингу та оновлення заходів безпеки банку в залежності від змін у стані інформаційної безпеки.

У обох випадках важливо забезпечити адекватний рівень захисту інформації банку в умовах постійної зміни загроз і технологічного середовища.

Для оцінки поточного стану інформаційної безпеки банку і відповідно оцінки ефективності функціонування КСЗІ в роботі пропонується використовувати синтез чотирьох моделей. (рис. 1.3)

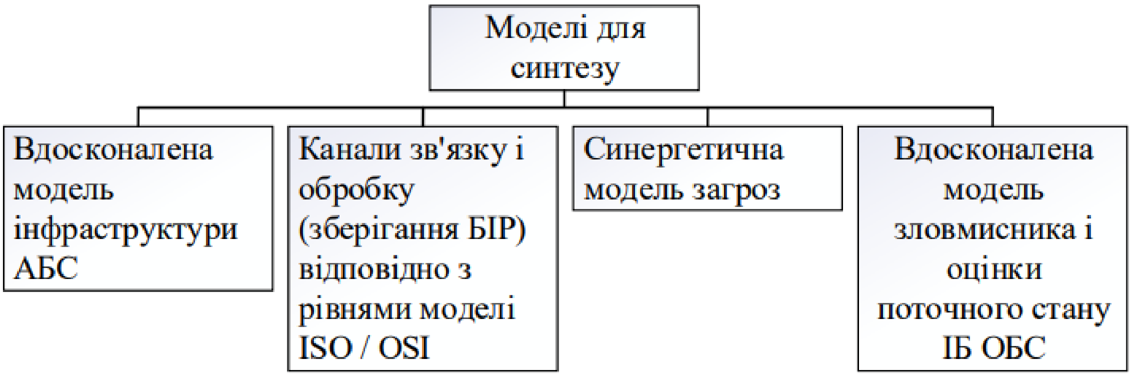

Рис. 1.3 – Моделі для синтезу

Даний підхід дозволяє забезпечити оцінку сучасних загроз з урахуванням їх вдосконалення (синергізму і гібридності) на всі складові безпеки (рис. 1.4): ІБ, КБ, БІ БІР АБС, визначити критичні точки уразливості в КСЗІ, можливість захисту БІР від загроз наявними криптографічними засобами КСЗІ, відповідність регуляторам з ІБ , і отримати якісну оцінку поточного стану безпеки інфраструктури АБС, і комплексування, оцінити вплив сучасних гібридних загроз на функціонування АБС, можливість проникнення і несанкціонованого доступу до активів БІР, а також функціональну ефективність засобів КСЗІ в АБС [20] .

Банк використовує сучасні сервери та мережеве обладнання, зокрема, фаєрволи та системи виявлення та запобігання вторгненням (IDS/IPS).

Необхідно регулярно оновлювати ці системи для забезпечення захисту від новітніх загроз. Крім того, важливо здійснювати періодичні стрес-тести мережі на предмет виявлення потенційних слабких місць [24-25] .

Рис. 1.4 – Складові безпеки банківської інформації

Використовуються різноманітні програмні рішення, включаючи CRM-системи, фінансові аналітичні інструменти, а також спеціалізоване банківське ПЗ.

Важливо забезпечити регулярне оновлення всього програмного забезпечення, особливо щодо патчів безпеки. Також рекомендується проведення аудиту використовуваного ПЗ на предмет вразливостей.

Банк активно використовує хмарні рішення для деяких своїх сервісів, включаючи зберігання даних та обчислення.

Потрібно забезпечити, що всі хмарні рішення відповідають високим стандартам безпеки. Важливо також контролювати доступ до хмарних ресурсів та впровадити шифрування для даних, що передаються та зберігаються в хмарі [26] .

Банк слідує міжнародним стандартам безпеки, таким як ISO 27001, але деякі аспекти, зокрема управління ризиками та бізнес-неперервність, потребують додаткового розвитку.

Рекомендується розробити більш комплексні політики управління ризиками та плани відновлення після аварій.

Проводяться періодичні внутрішні та зовнішні аудити, але існує потреба у збільшенні їх частоти та глибини.

Важливо використовувати передові методи аудиту для ідентифікації та мінімізації ризиків, особливо у контексті нових технологій та кіберзагроз.

Співробітники проходять базове навчання з питань кібербезпеки, але воно не завжди охоплює всі актуальні загрози.

Потрібно розробити більш комплексні та регулярні програми навчання, зокрема з фокусом на новітні кіберзагрози, фішинг, соціальну інженерію та безпечні практики онлайн-банкінгу [27-28] .

Банк використовує SSL/TLS для захисту мережевих транзакцій, але в деяких випадках шифрування даних в базах даних не повністю відповідає сучасним стандартам.

Необхідно реалізувати сучасні методи шифрування на рівні поля для чутливих даних у базах даних, а також переконатися, що всі мережеві транзакції захищені найсучаснішими протоколами шифрування.

Політики управління ключами шифрування існують, але вони не завжди строго дотримуються, особливо у відділеннях банку.

Потрібно зміцнити політики управління ключами шифрування, включаючи їх ротацію та безпечне зберігання, щоб забезпечити вищий рівень захисту даних [29].

В банку використовуються традиційні паролі для доступу до систем, багатофакторна автентифікація застосовується не повсюдно.

Рекомендується впровадження багатофакторної автентифікації для всіх внутрішніх та зовнішніх систем, особливо для систем, що обробляють чутливі фінансові дані.

Хоча моніторинг доступу до систем здійснюється, не всі спроби несанкціонованого доступу виявляються ефективно.

Необхідно покращити системи моніторингу та журналювання доступу, використовуючи передові технології для раннього виявлення та реагування на несанкціонований доступ [30].

Існуючі DLP-системи фокусуються на традиційних каналах передачі даних, але не повністю покривають хмарні сервіси та мобільні додатки.

Важливо розширити функціонал DLP-систем, щоб вони охоплювали всі канали передачі даних, включаючи хмарні та мобільні платформи, забезпечуючи комплексний захист від витоку даних.

Захист кінцевих точок, таких як робочі станції та мобільні пристрої, не завжди на належному рівні.

Потрібно зміцнити заходи ендпойнт безпеки, включаючи регулярні оновлення антивірусного програмного забезпечення, використання сучасних засобів шифрування та впровадження строгих політик управління мобільними пристроями [31] .

Існують загальні плани реагування на інциденти, але вони не завжди включають процедури для специфічних типів кібератак.

Рекомендується оновити плани реагування на інциденти, включаючи специфічні дії для різноманітних типів кібератак та впровадження ефективних процедур відновлення після аварій [32] .

Тренування з реагування на інциденти проводяться, але не регулярно та не завжди охоплюють всіх співробітників.

Важливо забезпечити регулярні та комплексні тренування для всіх співробітників, включаючи симуляції різних типів кібератак, для підвищення готовності та ефективності реагування на інциденти.

Цей аналіз показує, що банк має міцну основу для інформаційної безпеки, але існують ключові області для покращення, особливо в контексті внутрішнього навчання персоналу, управління доступом до даних, та посилення планів реагування на інциденти. Оновлення та адаптація цих стратегій є критично важливою для захисту від постійно змінних загроз у сфері кібербезпеки.

1.3 Потенційні загрози та ризики інформаційної безпеки в АСУ

Банківська система, будучи критично важливою для фінансової стабільності кожної країни, стикається з численними загрозами та ризиками. Ці ризики варіюються від традиційних фінансових викликів до сучасних кіберзагроз, кожен з яких може мати серйозні наслідки для цілісності та ефективності банківської системи. Розуміння та оцінка цих ризиків є ключовими для забезпечення стабільності та надійності банківських операцій. [33]

Розробка детального плану потенційних загроз та ризиків для банківської системи передбачає ідентифікацію, аналіз та розробку стратегій реагування на різноманітні види загроз. Перелік заходів планування наведено в таблиці 1.3 .

Таблиця 1.3

Перелік інцидентів, загроз ризиків та заходів реагування на них

Інцидент	Загрози	Ризики	Заходи реагування
Кібератаки	Віруси та шкідливе програмне забезпечення, Ransomware атаки, фішинг та соціальна інженерія, DDoS атаки	Втрата даних та порушення конфіденційності, переривання операційних процесів, фінансові втрати	Встановлення антивірусного програмного забезпечення, регулярне оновлення систем і програм, резервне копіювання даних
Внутрішні Загрози	Ненавмисний або навмисний витік даних співробітниками	Витік конфіденційної інформації, порушення внутрішніх політик безпеки	Впровадження політик управління доступом, проведення регулярних аудитів доступу
Технологічні Недоліки	Застаріле ПЗ, вразливості у нових технологіях	Виявлення та використання вразливостей хакерами	Регулярне оновлення та модернізація обладнання
Фізичний Доступ	Несанкціонований фізичний доступ до обладнання, крадіжка або пошкодження обладнання	Втрата або пошкодження критичного обладнання	Встановлення систем безпеки та контролю доступу, організація охорони та моніторингу
Природні Катастрофи	Землетруси, повені, пожежі	Втрата даних та обладнання, переривання роботи банку	Розробка планів відновлення після аварій та встановлення аварійних генераторів

Більш детально розберемо кожен пункт плану, розглянемо потенційні загрози, ризики та наведемо приклади.

Кібератаки становлять одну з найсерйозніших загроз сучасному фінансовому сектору, особливо для банківської системи, що зазнає постійного впливу різноманітних кібернетичних ризиків. Ці атаки не тільки призводять до безпосередніх фінансових втрат, але й загрожують конфіденційності клієнтських даних, що може мати довгострокові наслідки для репутації та довіри до банку.

Серед різних форм кібератак, найпоширенішими є фішингові атаки, розповсюдження шкідливого ПЗ, DDoS-атаки, а також викрадення та витік даних. Фішингові атаки часто ціляться на співробітників банків, спонукаючи їх ненароком розкрити конфіденційну інформацію, таку як логіни та паролі. Шкідливе ПЗ може бути використане для отримання несанкціонованого доступу до банківських систем, тоді як DDoS-атаки можуть паралізувати онлайн-сервіси банку, перешкоджаючи нормальній роботі та обслуговуванню клієнтів.

Одним з найбільш резонансних прикладів кібератаки на банківську систему була атака на Бангладешський Центральний Банк у 2016 році. Зловмисники використали шкідливе ПЗ для взлому системи банку та надіслали фальшиві запити на переказ коштів через систему SWIFT. В результаті з банку було нелегально виведено мільйони доларів. Цей інцидент підкреслив важливість посилення кібербезпеки в банківській системі [34] .

Для протидії таким загрозам банки активно впроваджують різноманітні заходи безпеки. Це включає в себе розробку та виконання комплексних політик кібербезпеки, впровадження багаторівневих систем захисту, таких як файрволи, антивірусне програмне забезпечення та системи виявлення вторгнень. Особливу увагу приділяють навчанню персоналу, адже людський фактор часто є слабкою ланкою в системі безпеки. Важливою складовою є також розробка та впровадження планів реагування на інциденти, щоб швидко і ефективно відновити роботу банківських систем у разі кібератак.

Внутрішні загрози банківській системі часто є менш помітними, але не менш небезпечними, ніж зовнішні кібератаки. Вони можуть включати в себе фактори, такі як внутрішні помилки співробітників, недбалість, або навіть умисні дії зі шкоди, які можуть призвести до втрати або компрометації конфіденційних даних, фінансових збитків або навіть юридичних наслідків для банку.

Одним з найбільш поширених ризиків є помилки співробітників, які можуть включати неправильне управління даними, помилки в обробці транзакцій або недостатньо обачне поводження з конфіденційною інформацією. Такі помилки часто виникають через недостатнє навчання персоналу або недостатній контроль за виконанням внутрішніх процедур. Крім того, існує ризик умисних дій зі шкоди, які можуть включати крадіжку даних або фінансових коштів, а також усвідомлене недотримання внутрішніх політик та процедур безпеки [35].

Один із прикладів внутрішньої загрози стався в одному з європейських банків, де співробітник ненавмисно відправив конфіденційну інформацію про клієнтів на зовнішню адресу електронної пошти. Цей інцидент призвів до великого витоку даних та вимагав серйозних заходів для вирішення виниклої кризи та відновлення довіри клієнтів.

Щоб протидіяти внутрішнім загрозам, банки впроваджують цілу низку заходів. Найважливішим кроком є ретельне навчання персоналу, що включає інформування про внутрішні політики та процедури безпеки, а також регулярні тренінги з кібербезпеки. Крім того, важливим є впровадження ефективних систем контролю та аудиту для виявлення та запобігання можливим порушенням або помилкам.

Іншим ключовим елементом є впровадження багаторівневих систем безпеки, які включають моніторинг та аналіз поведінки користувачів, що дозволяє своєчасно ідентифікувати будь-які відхилення від норми. Також банки активно використовують системи шифрування даних та впроваджують різні рівні доступу до інформації, щоб мінімізувати ризики пов'язані з управлінням даними.

Завершуючи, можна сказати, що внутрішні загрози банківській системі потребують комплексного підходу до управління ризиками, який поєднує в собі як технічні засоби захисту, так і стратегії управління людськими ресурсами. Це включає постійне навчання, моніторинг, а також розробку ефективних планів реагування на інциденти, щоб забезпечити захист банківської системи від потенційних внутрішніх загроз.

Технологічні недоліки в АСУ банківських систем становлять серйозну проблему, оскільки вони можуть стати причиною ряду ризиків і загроз, які варіюються від витоків даних до втрати фінансових активів та пошкодження репутації. Найбільш поширеними проблемами є застаріле програмне забезпечення, вразливості в системах безпеки, недостатня інтеграція технологій та обмежена масштабованість систем.

Застаріле програмне забезпечення часто використовується в банківських системах через високі витрати та складнощі, пов'язані з оновленням. Це може призвести до збоїв у роботі, а також збільшити вразливість до кібератак, оскільки старі системи не завжди здатні ефективно протистояти сучасним загрозам. Крім того, недоліки в системах безпеки, такі як відсутність достатнього шифрування або слабкі аутентифікаційні процеси, можуть сприяти несанкціонованому доступу до конфіденційних даних [34] .

Прикладом технологічної вразливості в банківській системі може слугувати інцидент, що стався з одним із європейських банків, де хакери змогли використовувати вразливість у системі обробки платежів для проведення несанкціонованих транзакцій. Відсутність своєчасних оновлень та ефективного моніторингу призвела до значних фінансових втрат та підриву довіри клієнтів.

Відповідь на технологічні недоліки в банківських системах вимагає комплексного підходу, який включає оновлення та модернізацію існуючих систем, впровадження розширених заходів безпеки та регулярний аудит технологій. Оновлення програмного забезпечення та інфраструктури повинні проводитися регулярно, щоб забезпечити відповідність сучасним стандартам безпеки та ефективності. Інтеграція сучасних технологій, таких як блокчейн або штучний інтелект, може допомогти в автоматизації процесів, підвищенні безпеки та покращенні загальної ефективності системи.

Також важливим є розвиток внутрішньої культури безпеки, яка охоплює регулярне навчання персоналу та впровадження чітких процедур для виявлення та реагування на інциденти. Банки повинні розробити ефективні стратегії реагування на інциденти, щоб швидко виявляти та усувати будь-які проблеми, мінімізуючи потенційні збитки [34].

У підсумку, технологічні недоліки в банківських системах вимагають уважного моніторингу, постійного оновлення та адаптації до змінних умов кіберпростору. Через їх потенційні наслідки, важливо підтримувати стратегічний фокус на інноваціях та безпеці, щоб гарантувати надійність та стійкість банківської системи.

Загрози фізичного доступу до банківських систем часто можуть бути недооцінені в епоху, де фокус переважно зосереджений на кіберзагрозах. Проте, незахищений фізичний доступ до банківських відділень, серверних приміщень, або інших критично важливих об'єктів може призвести до серйозних наслідків, включно з крадіжкою даних, фінансовими втратами, або навіть фізичними пошкодженнями інфраструктури.

Однією з найбільших загроз є несанкціонований доступ до приміщень, де зберігаються конфіденційні дані або важливе обладнання. Такий доступ може бути отриманий через проникнення зловмисників до будівлі або через внутрішніх співробітників, які використовують свій статус для отримання доступу до чутливих областей. Інша проблема – це фізичні атаки на банкомати або інші самообслуговувані термінали, які можуть бути спрямовані на викрадення готівки або встановлення шкідливих пристроїв.

Прикладом фізичної загрози банківській системі може бути ситуація, коли зловмисники встановили скімінгові пристрої на банкоматах. Ці пристрої були використані для нелегального зчитування інформації з банківських карт користувачів, що призвело до несанкціонованих транзакцій та фінансових втрат для клієнтів.

Для протидії фізичним загрозам банківським системам необхідно впровадження комплексних заходів безпеки. Це включає установку охоронних систем, таких як камери спостереження, системи контролю доступу, та тривожні системи. Важливим є також фізичне забезпечення серверних приміщень та інших критично важливих областей за допомогою замків, сейфів, та інших засобів забезпечення фізичної безпеки [35] .

Також важливою складовою є розробка та впровадження політик внутрішнього контролю для співробітників, що включають регулярне навчання з фізичної безпеки, а також процедури реагування на інциденти. Співробітникам потрібно надавати доступ лише до тих областей, які необхідні для виконання їх роботи, а також важливо впроваджувати процедури ретельної перевірки та моніторингу.

У підсумку, захист банківських систем від фізичних загроз вимагає поєднання технологічних, організаційних та фізичних заходів безпеки. Важливо не лише захищати від потенційних зовнішніх загроз, але й забезпечувати внутрішній контроль та обізнаність співробітників, щоб знизити ризики втрати даних, фінансових збитків та інших негативних наслідків.

Природні катастрофи, такі як землетруси, повені, урагани, та інші екстремальні погодні явища, становлять значний ризик для стабільності та безперервності роботи банківських систем. Незважаючи на те, що вони є непередбачуваними та часто неконтрольованими, наслідки природних катастроф можуть мати далекосяжні фінансові, технічні та операційні впливи на банки.

Основні ризики від природних катастроф включають фізичне пошкодження банківських відділень, серверних центрів та іншої критично важливої інфраструктури. Такі події можуть призвести до збоїв у банківських операціях, утрати даних та порушення зв'язків із клієнтами. Крім того, природні катастрофи можуть спричинити проблеми з електропостачанням, зв'язком, та доступом до фізичних об'єктів, що ускладнює відновлення послуг та виконання фінансових операцій [36] .

Прикладом впливу природної катастрофи на банківську систему може бути ураган "Катріна", який у 2005 році завдав серйозної шкоди банкам у Новому Орлеані та інших частинах Південної Луїзіани та Міссісіпі. Банки стикалися з великими викликами, включаючи відновлення фізичних відділень та відновлення даних та систем, що були пошкоджені або знищені.

Для мінімізації ризиків та наслідків природних катастроф, банки повинні впроваджувати всебічні плани готовності та відновлення після катастроф. Це включає розробку та регулярне оновлення планів реагування на надзвичайні ситуації, що охоплюють не тільки фізичну інфраструктуру, але й інформаційні системи, комунікації, та людські ресурси.

Важливим елементом планування є створення резервних центрів обробки даних та віддалених робочих місць, щоб забезпечити неперервність бізнесу навіть у випадку втрати основного фізичного місцезнаходження. Також важливо інвестувати в резервні системи електропостачання та засоби зв'язку, щоб підтримувати критичні операції в умовах перебоїв.

Крім того, банки повинні забезпечити належне навчання своїх співробітників для ефективного реагування на природні катастрофи, включаючи евакуаційні процедури, забезпечення безпеки та підтримання важливих банківських операцій під час кризових ситуацій.

У підсумку, протидія загрозам від природних катастроф вимагає комплексного підходу, що включає планування, технологічну підготовку та навчання персоналу. Підготовка до природних катастроф є ключовою складовою забезпечення стійкості та надійності банківських систем у сучасному світі.

Висновок до першого розділу. Порівняння вітчизняної та зарубіжної літератури виокремлює суттєві відмінності у підходах до технічних аспектів захисту інформації, особливо з огляду на правові та регуляторні рамки, а також на актуальність і практичне впровадження захисних технологій у реальних умовах.

Інформаційна безпека в банківському секторі залишається важливим та складним аспектом. Аналіз поточного стану виявив, що хоча банки і приділяють значну увагу захисту своїх систем, існує ряд потенційних загроз та ризиків, які потребують постійного моніторингу та удосконалення заходів безпеки.

Огляд показав, що головні виклики полягають у забезпеченні захисту від кібератак, управлінні внутрішніми ризиками, включаючи помилки співробітників та умисні дії зі шкоди, а також у захисті від фізичних загроз і загроз, пов'язаних з природними катастрофами. Ці виклики вимагають комплексного підходу, що включає технічні, організаційні та фізичні заходи безпеки.

Банки активно використовують сучасні технології для забезпечення безпеки своїх систем, але водночас стикаються з викликами, пов'язаними зі швидким розвитком кіберзагроз та постійною потребою в оновленні своїх захисних систем.

Враховуючи виявлені загрози та ризики, рекомендується продовжувати інвестування у розвиток інформаційної безпеки АСУ, зосереджуючись на оновленні захисного програмного забезпечення, розвитку навичок персоналу в області кібербезпеки та впровадженні ефективних стратегій реагування на інциденти. Також важливо підкреслити необхідність регулярного аудиту та оцінки ризиків, щоб вчасно виявляти нові загрози та адаптувати заходи безпеки до змінних умов.

Таким чином, дані отримані в результаті аналізу підкреслюють важливість комплексного підходу до забезпечення інформаційної безпеки в банківських автоматизованих системах і підтверджують потребу в постійному вдосконаленні та адаптації систем безпеки для ефективного протистояння існуючим та потенційним загрозам.

РОЗДІЛ 2

АНАЛІЗ ТЕХНІЧНИХ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ

2.1. Організаційно-технічні заходи забезпечення захисту інформації в АСУ

Технічний захист інформації – діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (або) витоку інформації технічними каналами.

Технічний захист інформації спрямований на запобігання можливим порушенням цілісності, блокуванню, або витоку інформації за допомогою технічних засобів і каналів/

Сучасний світ характеризується зростанням важливості інформації у суспільних відносинах. Суспільні інформаційні відносини постійно еволюціонують, особливо з удосконаленням технологій збирання, обробки, зберігання і передавання інформації. Ці процеси формують суть інформаційного суспільства. З цим розвитком також пов'язані соціальні проблеми, зокрема, ті, які стосуються кримінальних діянь і потребують ефективних заходів для їх вирішення.

Забезпечення інформаційної безпеки є важливою задачею, яка стала ще актуальнішою в епоху цифрових технологій та зростаючих кіберзагроз. Існують три основних підходи до цього завдання:

1. Приватний підхід: Цей підхід вирішує індивідуальні завдання щодо інформаційної безпеки. Хоча це менш ефективний підхід, його використовують, оскільки він не потребує значних витрат.

2. Комплексний підхід: В цьому підході розв'язуються багато завдань як одна єдина програма. Він є основним методом на сучасному етапі.

3. Інтегральний підхід: Цей підхід передбачає інтеграцію різних підсистем зв'язку та забезпечення безпеки в єдину систему з загальними технічними засобами та програмним забезпеченням.

Захист інформації в банківських системах стає особливо важливим у зв'язку з обробкою величезних обсягів конфіденційної інформації та фінансових операцій. Використання сучасних технічних засобів, таких як антивіруси, файрволи, системи виявлення та попередження вторгнень і методи шифрування, стає ключовим аспектом забезпечення інформаційної безпеки банків. Важливо постійно оновлювати та модернізувати ці засоби, оскільки кіберзагрози постійно змінюються. Захист інформації стає неперервним процесом, який вимагає уважності і адаптації до нових викликів кіберпростору.

В Україні існує перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. Або іншими словами засоби технічного захисту інформації, які є в переліку мають експертний висновок.

Цей Перелік формується відповідно з переліком нормативних документів [37-41], призначених для використання суб'єктами системи технічного захисту інформації (ТЗІ) під час розроблення, модернізації та впровадження комплексів ТЗІ на об'єктах інформаційної діяльності (ОІД) та комплексних систем захисту інформації (КСЗІ) в автоматизованих системах (АС).

Перелік містить номенклатуру засобів ТЗІ (технічних засобів, основним функціональним призначенням яких є захист інформації від загроз витоку, порушення цілісності та блокування; технічних засобів, в яких додатково до основного призначення передбачено функції захисту інформації; засобів, які призначені, спеціально розроблені або пристосовані для пошуку закладних пристроїв і які створюють загрозу для інформації; засобів, які спеціально розроблені або пристосовані для оцінювання захищеності інформації), відповідність яких вимогам нормативних документів з питань ТЗІ засвідчено сертифікатом відповідності або позитивним експертним висновком, одержаними у порядку, який встановлено нормативно-правовими актами:

Правилами проведення робіт із сертифікації засобів захисту інформації, затвердженими спільним наказом Адміністрації Держспецзв'язку та

Держспоживстандарту України від 25.04.2007 р. № 75/91 і зареєстрованими в Міністерстві юстиції України 14.05.2007 р. за № 498/13765, та Положенням про державну експертизу в сфері технічного захисту інформації, затвердженим наказом Адміністрації Держспецзв'язку України від 16.05.2007 р. № 93 і зареєстрованим в Міністерстві юстиції України 16.07.2007 р. за № 820/14087.[42]

Використання засобів цього Переліку під час створення, модернізації та впровадження комплексів ТЗІ на ОІД та КСЗІ в АС не увільняє від необхідності оцінювання відповідності досягнутого рівня захисту інформації встановленому вимогами нормативних документів з ТЗІ, яке здійснюється шляхом атестації комплексів ТЗІ на ОІД або експертизи КСЗІ в АС.

Порядок використання засобів ТЗІ, які не ввійшли до цього Переліку, в комплексах ТЗІ на ОІД та КСЗІ в АС визначається нормативними документами у сфері ТЗІ.

Оновлення інформації, яка міститься в Переліку, здійснюється шляхом періодичного внесення змін до попередньої редакції. Перелік та його доповнення розміщуються на WEB-сайті www.dsszzi.gov.ua.

За додатковими відомостями про засоби з цього Переліку, стан їх виробництва та порядок постачання необхідно звертатися до виробника (постачальника).

Захист інформації – це сукупність організаційних, технічних та правових заходів, спрямованих на запобігання нанесенню збитків інтересам власника інформації.

Основними об'єктами захисту інформації є:

1. Інформація з обмеженим доступом (ІзОД) - це інформаційні ресурси, включаючи таємну та конфіденційну інформацію.

2. Технічні засоби приймання, обробки, зберігання і передачі інформації (ТЗПІ) - це системи та засоби інформатизації, обчислювальна техніка, мережі і системи.

3. Програмні засоби - включаючи операційні системи, системи

керування базами даних та інше програмне забезпечення.

4. Автоматизовані системи керування, системи зв'язку, технічні засоби отримання, передачі та обробки ІзОД, включаючи апаратуру для звукозапису, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої, а також технічні засоби обробки графічної, алфавітно-цифрової та текстової інформації, інформативні фізичні поля.

5. Допоміжні технічні засоби і системи (ДТЗС) - це технічні засоби і системи, які не входять до ТЗПІ, але розташовані в приміщеннях, де оброблюється ІзОД. Сюди входять системи відкритого телефонного або гучномовного зв'язку, системи пожежної та охоронної сигналізації, системи енергопостачання, радіотрансляційна мережа, система часофікації, енергопобутові прилади і таке інше, а також самі приміщення, де циркулює ІзОД.

Результати аналізу показують можливі шляхи витоку і несанкціонованого доступу до інформації в типовому одноповерховому офісі банку.[43]

Схема каналу витоку і несанкціонованого доступу до інформації в типовому одноповерховому офісі банку (рис. 2.1) [43] :

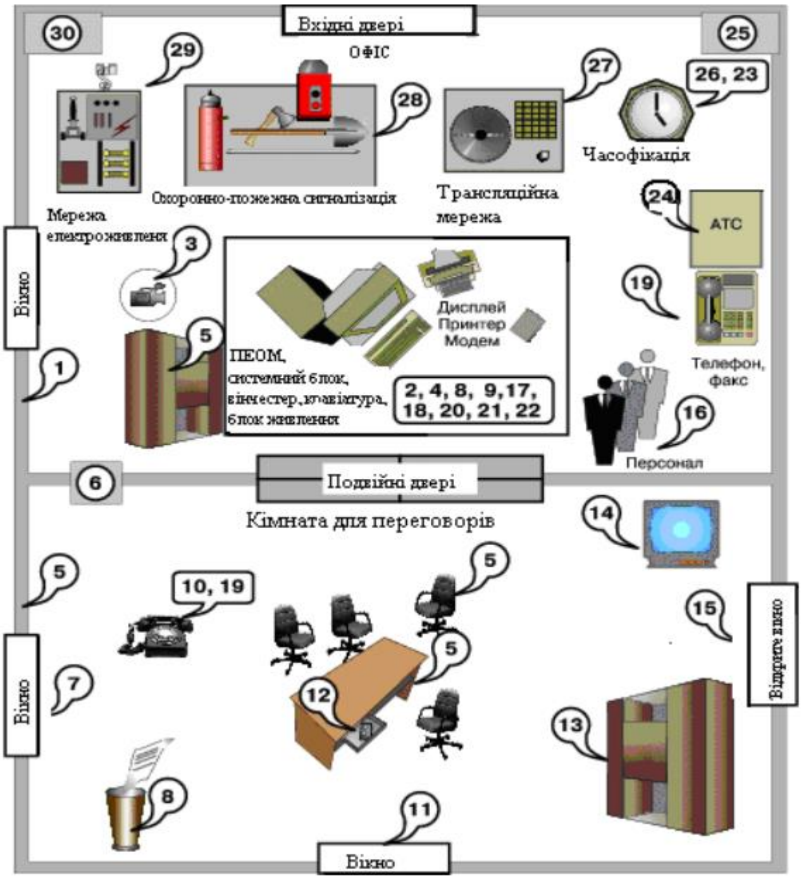

Рис. 2.1. Схема каналу витоку і несанкціонованого доступу до інформації

1. витік за рахунок структурного звуку в стінах і перекриттях
2. знімання інформації зі стрічки принтера, погано стертих дискет і т. п.
3. знімання інформації з використанням відеозакладок
4. програмно-апаратні закладки в ПЕОМ
5. радіо-закладки в стінах і меблях
6. знімання інформації з системи вентиляції
7. лазерне знімання акустичної інформації з вікон
8. виробничі й технологічні відходи
9. комп'ютерні віруси, логічні бомби й т. п.
10. знімання інформації за рахунок наведень і "нав'язування"
11. дистанційне знімання відео інформації (оптика)
12. знімання акустичної інформації з використанням диктофонів
13. розкрадання носіїв інформації
14. високочастотний канал витоку в побутовій техніці

15. знімання інформації спрямованим мікрофоном
16. внутрішні канали витоку інформації (через обслуговуючий персонал)
17. несанкціоноване копіювання
18. витік за рахунок побічного випромінювання термінала
19. знімання інформації за рахунок використання "телефонного вуха"
20. знімання з клавіатури й принтера акустичним каналом
21. знімання з дисплея по електромагнітному каналу
22. візуальне знімання з дисплея й принтера
23. наведення на лінії комунікацій і сторонні провідники
24. витік через лінії зв'язку
25. витік мережею заземлення
26. витік мережею часофікації
27. витік трансляційною мережею й гучномовним зв'язком
28. витік охоронно-пожежною сигналізацією
29. витік мережею електроживлення
30. витік мережею опалення, газо- і водопостачання

Захист інформації від витоку через технічні канали забезпечується за допомогою проектно-архітектурних рішень, організаційних та технічних заходів, а також виявленням портативних приладів для шпигунства.

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.[44]

До них входять такі заходи:

1. Залучення до робіт зі збереження інформації організацій, які мають відповідні ліцензії для діяльності в галузі технічного захисту інформації.
2. Класифікація та атестація об'єктів і приміщень для забезпечення відповідності вимогам щодо захисту інформації під час проведення секретних робіт.
3. Використання сертифікованих технічних засобів для забезпечення

безпеки інформації.

4. Встановлення контролю та обмежень доступу на об'єкти технічного захисту і в виділені приміщення.

5. Введення різноманітних обмежень, таких як територіальні, частотні, енергетичні, просторові і часові, для забезпечення безпеки технічних засобів.

6. Відключення технічних засобів, які мають елементи, які можуть використовуватися для шпигунства, від ліній зв'язку під час проведення секретних робіт.

Технічні заходи - це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи слугують для закриття каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів або зменшення відношення сигнал /завада у місцях можливого розміщення ТЗР або їх датчиків до рівнів, що унеможливлюють виділення інформаційних сигналів засобами розвідки. Під час проведення таких заходів використовують активні та пасивні методи.[44]

До пасивних технічних заходів для захисту інформації відносяться такі дії:

1. Контроль та обмеження доступу до об'єктів і приміщень, де знаходяться технічні засоби захисту інформації. Це включає встановлення спеціальних засобів і систем для обмеження та контролю доступу.

2. Локалізація випромінювання, що включає в себе:

- Екранування технічних засобів захисту і з'єднувальних ліній, щоб уникнути несанкціонованого перехоплення сигналів.

- Заземлення технічних засобів захисту і екранів їх з'єднувальних ліній для зменшення електромагнітного випромінювання.

- Звукоізоляція виділених приміщень, щоб уникнути прослуховування звукових сигналів.

3. Розв'язування інформаційних сигналів, що включає в себе:

- Встановлення спеціальних захисних засобів, таких як Граніт або Рікас, в допоміжних технічних засобах і системах для уникнення перехоплення інформації з мікрофонним ефектом.
- Використання діелектричних вставок в кабелях електроживлення, трубах систем опалення, водопостачання і каналізації, що виходять за межі контрольної зони, для запобігання витоку інформації.
- Встановлення автономних або стабілізованих пристроїв живлення для технічних засобів захисту інформації.
- Використання завадоподавляючих фільтрів, таких як ФП, ФСП, ФС-2, в мережах живлення технічних засобів захисту і в лініях освітлення і розеткових мережах виділених приміщень.

До активних технічних заходів для захисту інформації від витоку включають такі дії:

1. Просторове зашумлення, яке включає в себе:

- Електромагнітне зашумлення з використанням генераторів шуму або створення завад відповідними засобами, якщо відома частота випромінювання закладного пристрою або ТЗПІ.
- Акустичне та вібраційне зашумлення за допомогою генераторів шуму, відомих як шумотрони.
- Подавлення роботи записуючих пристроїв, таких як диктофони, за допомогою спеціальних приладів.

2. Лінійне зашумлення включає в себе вплив на мережі електроживлення та заземлення, а також на зовнішні дроти і з'єднувальні лінії ДТЗС, які виходять за межі контрольної зони.

3. Знешкодження закладних пристроїв за допомогою спеціальних генераторів імпульсів, які випалюють їх (такі прилади іноді називають "жучками").

Для виявлення закладних пристроїв використовують два основних підходи: пасивні і активні методи.[45]

Пасивні методи включають такі дії:

1. Встановлення засобів і систем виявлення лазерного випромінювання, наприклад, підсвічування скла на вікнах, щоб виявити можливі оптичні закладні пристрої.

2. Встановлення стаціонарних детекторів для виявлення диктофонів.

3. Розшук закладних пристроїв за допомогою індикаторів поля, інтерсепторів, частотомірів, сканувальних приймачів та програмно-апаратних комплексів контролю.

4. Організація радіоконтролю для виявлення побічних електромагнітних випромінювань, що можуть свідчити про наявність закладних пристроїв ТЗПІ.

Активні методи включають такі заходи:

1. Спеціальна перевірка виділених приміщень з використанням нелінійних локаторів, які можуть виявляти закладні пристрої, які не видно звичайними методами.

2. Спеціальна перевірка виділених приміщень, ТЗПІ та ДТЗІ за допомогою рентгенівських комплексів для виявлення можливих прихованих закладних пристроїв.

Ці методи допомагають виявити та нейтралізувати закладні пристрої для забезпечення безпеки інформації. (табл. 2.1)

Таблиця 2.1

Методи та засоби одержання інформації

Дії людини (типова ситуація)	Канали витоку інформації	Методи та засоби одержання інформації	Методи та засоби захисту інформації
Розмова в приміщенні або на вулиці	Акустика Віброакустика Гідроакустика Електроакустика	Підслуховування, диктофон, мікрофон, спрямований мікрофон, напівактивна система, стетоскоп, вібродатчик, гідроакустичний датчик, радіотехнічні спецприймачі	Шумові генератори, пошук закладок, захисні фільтри, обмеження доступу
Розмова по провідному телефону	Акустика Електросигнал у лінії наведення	Аналогічно п. 1 паралельний телефон, пряме підключення, електромагнітний датчик, диктофон, телефонна закладка	Аналогічно п. 1 Маскування, скремблювання, шифрування Спецтехніка
Розмова по	Акустика,	Аналогічно п. 1	Аналогічно п. 1

радіотелефону	електромагнітні хвилі Аналогічно п. 1 р	радіоприймальні пристрої	Аналогічно п.2
Документ на паперовому носії	Наявність	Крадіжка, візуально, копіювання, фотографування	Обмеження доступу, спецтехніка
Виготовлення документа на паперовому носії	Наявність Паразитні сигнали, наведення	Аналогічно п. 4 спеціальні радіотехнічні пристрої	Аналогічно п. 1 екранування
Документ на не паперовому носії	Носій	Розкрадання, копіювання, зчитування	Контроль доступу, фізичний захист, криптозахист
Передача документа каналами зв'язку	Електричні і оптичні сигнали	Несанкціоноване підключення, імітація зареєстрованого користувача	Криптозахист

2.2 Технічні засоби захисту інформації на рівні комп’ютерного ПЗ

Антивірусні програми є фундаментальним елементом захисту інформаційних систем будь-якої банківської установи. Вони забезпечують базовий рівень безпеки, виявляючи, блокуючи та видаляючи шкідливе програмне забезпечення та віруси, які можуть пошкодити або вкрасти важливі фінансові дані [46] .

Основні Функції

- Антивіруси сканують системи на предмет виявлення зловмисного програмного забезпечення та вірусів та їх подальшого видалення або карантину.
- Антивіруси виявляють фішингові спроби та шпигунські програми, що можуть викрасти конфіденційні дані.
- Оновлення бази даних вірусних підписів забезпечують захист від новітніх загроз.
- Постійний моніторинг системи допомагає виявляти та блокувати зловмисні дії у реальному часі.

Приклади популярних антивірусів що використовуються в автоматизованих банківських системах найчастіше:

1. Symantec Endpoint Protection - використовується у багатьох банках для захисту від складного шкідливого програмного забезпечення та мережевих загроз.

2. McAfee Endpoint Security - пропонує інтегровані захисні функції та ефективне виявлення загроз.

3. Bitdefender GravityZone - забезпечує комплексний захист для великих і малих банківських установ, включаючи захист від шифрувальників.

Антивірусні програми регулярно перевіряють всі комп'ютери та сервери в банківській мережі на наявність вірусів та інших шкідливих програм. Забезпечують безпеку онлайн-транзакцій клієнтів, запобігаючи спробам шахрайства.

Також антивіруси допомагають захистити конфіденційні дані клієнтів та банку від несанкціонованого доступу, захищають важливі фінансові записи та інформацію від пошкодження або втрати внаслідок вірусних атак.

Антивірусні програми грають критично важливу роль у забезпеченні безпеки банківських систем, захищаючи їх від низки цифрових загроз. Ефективний антивірусний захист повинен бути частиною комплексної стратегії безпеки кожного банку, яка включає різні рівні захисних заходів.

Файрволи є ключовим компонентом інформаційної безпеки в банківських системах, виконуючи роль мережевого бар'єра, який захищає внутрішні мережеві ресурси від зовнішніх загроз. Вони ефективно управляють та контролюють вхідний та вихідний мережевий трафік на основі заданих правил безпеки.[44]

Файрволи стежать за всім мережевим трафіком і блокують потенційно шкідливі пакети даних, запобігають доступу неавторизованих користувачів до мережі банку та створюють безпечну VPN-з'єднання для безпечного віддаленого доступу співробітників та клієнтів.

Приклади популярних файрволів що використовуються в автоматизованих банківських системах:

1. Cisco ASA with FirePOWER - ця інтегрована платформа забезпечує високий рівень захисту та гнучкість у налаштуваннях безпеки.

2. Palo Alto Networks Next-Generation Firewalls - пропонують передові можливості захисту, включаючи поведінковий аналіз та автоматичне запобігання загрозам.

3. Fortinet FortiGate - відомий своєю високою продуктивністю та інтегрованими функціями безпеки.

4. Check Point Next Generation Firewalls - передові файрволи, які пропонують глибоку інтеграцію з іншими заходами безпеки.

Файрволи захищають мережу банку від зовнішніх кібератак, таких як DDoS-атаки, шпигунські програми та інші загрози.

Вони дозволяють контролювати доступ до різних внутрішніх банківських сервісів, забезпечуючи, що лише авторизовані користувачі мають доступ та забезпечують безпеку онлайн-транзакцій, запобігаючи можливості перехоплення та маніпуляції даними транзакцій.

За допомогою файрволу проводиться реєстрація спроб вторгнення до системи та незвичайної мережевої активності для подальшого аналізу та удосконалення заходів безпеки.[44]

Файрволи відіграють незамінну роль у захисті банківських систем, виступаючи як перший рубіж оборони від зовнішніх кіберзагроз. Їх здатність моніторити, контролювати та захищати мережевий трафік є ключовою для забезпечення цілісності та безпеки банківських даних та сервісів. Вибір та налаштування ефективного файрволу вимагають глибокого розуміння специфіки банківської мережі та потенційних загроз.

Системи виявлення та попередження вторгнень (IDS/IPS) є важливими інструментами для захисту банківських інформаційних систем. Вони здійснюють постійний моніторинг мережі на наявність ознак аномалій або спроб вторгнення, тим самим забезпечуючи раннє виявлення потенційних загроз.

IDS/IPS аналізують мережевий трафік для виявлення незвичайної активності або відомих патернів атак, збирають інформацію про підозрілі події для подальшого аналізу та вдосконалюють захисні стратегії.

В разі виявлення підозрілої діяльності, IPS можуть автоматично блокувати трафік або вживати інших запобіжних заходів.[45]

Приклади Популярних Систем IDS/IPS

1. Cisco Firepower - забезпечує глибокий аналіз трафіку та ефективне виявлення загроз.

2. Palo Alto Networks Threat Prevention - пропонує передові функції виявлення та попередження вторгнень, інтегровані з файрволом.

3. Snort - відкрите програмне забезпечення, яке дозволяє виявляти вторгнення та вести детальний аналіз мережевого трафіку.

4. Fortinet FortiGate IPS - частина інтегрованої системи безпеки FortiGate, пропонує високопродуктивне виявлення загроз.

IDS/IPS використовуються у системах для виявлення складних загроз, які можуть уникати традиційних методів безпеки, неперервного моніторингу мережі, що дозволяє швидко реагувати на потенційні вторгнення або загрози, та виявлення певних типів внутрішніх загроз.

Також банки можуть використовувати дані з IDS/IPS для демонстрації відповідності регуляторним вимогам у сфері кібербезпеки.

Системи виявлення та попередження вторгнення є необхідними для забезпечення всебічного захисту банківських інформаційних систем. Вони допомагають ідентифікувати та запобігати потенційним загрозам, перш ніж вони завдадуть шкоди, і є важливою частиною комплексної стратегії інформаційної безпеки в банківському секторі.

Шифрування даних є критично важливим елементом захисту в банківських системах. Воно дозволяє перетворити конфіденційні дані в зашифрований формат, що робить їх недоступними для несанкціонованого доступу. Цей процес забезпечує конфіденційність та цілісність інформації, яка передається або зберігається.

Основні Способи Шифрування

- Шифрування на Рівні Транспорту (TLS/SSL) - забезпечує безпечне з'єднання між банком та його клієнтами під час онлайн-транзакцій.
- Шифрування Даних на Сервері (Database Encryption) - захищає дані, які зберігаються на серверах банку, включаючи особисті дані клієнтів та історію транзакцій.
- Шифрування Кінцевих Точок (Endpoint Encryption) - забезпечує захист даних на пристроях користувачів, наприклад, на банкоматах або терміналах обслуговування клієнтів.
- Асиметричне Шифрування (Public/Private Key Encryption) - використовується для безпечної передачі конфіденційних даних між банками або іншими фінансовими установами.

Приклади Технологій Шифрування

1. AES (Advanced Encryption Standard) - стандарт шифрування, який використовується для захисту величезних обсягів даних у всьому світі.
2. RSA (Rivest–Shamir–Adleman) - один з найбільш поширених методів асиметричного шифрування, використовуваний для захисту віддалених транзакцій.
3. SSL/TLS Протоколи - забезпечують безпечне з'єднання між веб-серверами та браузерами.
4. PGP (Pretty Good Privacy) - використовується для захисту електронних повідомлень та інших форм даних.

Шифрування TLS/SSL забезпечує безпечне проведення онлайн-транзакцій, захищаючи дані користувачів під час передачі, шифрування баз даних гарантує, що навіть у разі фізичного вторгнення, дані залишаються недоступними для зловмисників.[45]

Асиметричне шифрування використовується для захисту конфіденційних комунікацій між різними фінансовими установами, використання різних методів шифрування дозволяє створити багаторівневу систему захисту, що забезпечує цілісний захист інформаційних активів банку.

Тож ефективне шифрування даних є невід'ємною частиною стратегії захисту інформації в банківських системах. Використання передових технологій шифрування дозволяє банкам забезпечити конфіденційність і цілісність клієнтських та корпоративних даних, що є ключовим фактором для збереження довіри клієнтів та відповідності регуляторним стандартам.

Хмарні технології стрімко входять у сферу банківських послуг, пропонуючи гнучкість, масштабованість та підвищену ефективність управління даними. Використання хмарних рішень дозволяє банкам оптимізувати свої IT-операції, поліпшити обслуговування клієнтів та забезпечити більш високий рівень безпеки даних.

Хмарні сервіси, такі як Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) та Software-as-a-Service (SaaS), надають банкам можливість переносити різноманітні аспекти своєї діяльності у віртуальне середовище. Це включає все від розгортання баз даних та серверів до використання спеціалізованих фінансових програм і аналітичних інструментів.

Хмарні технології дозволяють банкам більш ефективно обробляти великі обсяги даних, включаючи транзакції клієнтів, кредитні аналізи, а також проводити ризик-менеджмент. З використанням хмарних рішень, банки можуть швидко масштабувати свої IT-ресурси відповідно до зростаючих потреб, без необхідності вкладення в дороге фізичне обладнання.[47]

Одним із ключових аспектів використання хмарних технологій у банківській сфері є підвищення безпеки. Хмарні провайдери пропонують розширені функції безпеки, які включають шифрування даних, регулярні оновлення безпеки та резервне копіювання даних. Це забезпечує захист від втрати даних та кіберзагроз, що є важливим для банківських установ, які зберігають конфіденційну інформацію клієнтів.

Хмарні технології також сприяють покращенню обслуговування клієнтів у банках. Завдяки їм, банки можуть надавати своїм клієнтам широкий спектр онлайн-сервісів, включаючи мобільний банкінг, онлайн-консультації та автоматизоване кредитування. Це не тільки підвищує задоволеність клієнтів, але й розширює можливості банку з приваблення нових клієнтів.

Впровадження хмарних технологій у банківських системах відкриває нові горизонти для інновацій та ефективності. Використання хмарних рішень дозволяє банкам підвищувати рівень обслуговування клієнтів, знижувати витрати на IT-інфраструктуру та підвищувати безпеку обробки та зберігання даних. Однак, важливо враховувати потреби у ретельному виборі провайдерів хмарних послуг та розробці стратегій, що забезпечують високий рівень конфіденційності та відповідність регуляторним вимогам.

2.3 Криптографічний захист інформації в АСУ

Криптографія - наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.
Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри та теорії ймовірностей [44] .

Історія криптографії сягає далеко в минуле. Вона почалася з простих шифрів, які використовувалися ще в античні часи, наприклад, шифр Цезаря - один з найвідоміших методів заміни букв у тексті. З розвитком технологій, особливо після створення комп'ютерів, криптографія перетворилася на складну і різнопланову науку. Сучасні криптографічні системи використовують складні математичні алгоритми та комп'ютерні технології для забезпечення безпеки даних.

В криптографії існують два основних типи шифрування: симетричне та асиметричне. Симетричне шифрування використовує один і той же ключ для шифрування та розшифрування даних. Найвідомішим прикладом симетричного шифрування є Алгоритм DES (Data Encryption Standard) та його наступник AES (Advanced Encryption Standard). Натомість, асиметричне шифрування використовує пару ключів - публічний для шифрування та приватний для розшифрування. Найвідомішим прикладом асиметричного шифрування є RSA.[40]

Застосування криптографії в сучасному світі є дуже широким, від захисту персональних та корпоративних даних до забезпечення безпеки електронних комунікацій. Цифрові підписи, які використовуються для перевірки автентичності та цілісності електронних документів, та криптографічні протоколи, такі як SSL/TLS, які забезпечують безпечний обмін інформацією в Інтернеті, є лише деякими прикладами її застосування.

Однак, з розвитком квантових комп'ютерів з'являються нові виклики для криптографії, оскільки вони здатні ефективно розбивати сучасні криптографічні системи. Це спонукає вчених та інженерів розвивати нові, більш стійкі до квантових атак криптографічні алгоритми, відкриваючи нові горизонти в цій області.[40]

Принципи криптографії відіграють вирішальну роль у захисті інформації в цифровому світі. Основу криптографії складають два фундаментальні процеси: шифрування та розшифрування. Шифрування - це процес перетворення зрозумілої інформації (відкритого тексту) у форму, що є незрозумілою без відповідного ключа (шифротекст). Розшифрування, в свою чергу, є оберненим процесом, який перетворює шифротекст назад у відкритий текст за допомогою ключа.

Основні типи шифрування поділяються на симетричні та асиметричні шифри. У симетричному шифруванні використовується один і той самий ключ для шифрування та розшифрування. Цей метод є швидким та ефективним, але він стикається з проблемою безпечної передачі ключа між відправником та одержувачем.

Найбільш поширені симетричні шифри включають AES (Advanced Encryption Standard) та DES (Data Encryption Standard). AES є одним із найбільш використовуваних стандартів і пропонує довжину ключа 128, 192 або 256 бітів, що робить його дуже стійким до спроб зламу. DES, старіший стандарт, зараз вважається менш безпечним через свою коротшу довжину ключа (56 бітів) [46].

Асиметричне шифрування, з іншого боку, використовує два ключі - публічний для шифрування та приватний для розшифрування. Цей метод вирішує проблему безпечної передачі ключів, оскільки публічний ключ може бути відкритим, а приватний - зберігається в таємниці. RSA (Rivest–Shamir–Adleman) є одним із найвідоміших асиметричних шифрів. Він використовує два великі прості числа для генерації пари ключів, що робить процес шифрування дуже стійким до криптографічних атак. Порівняння симетричних та асиметричних шифрів представлені в таблиці 2.2

Таблиця 2.2

Порівняння симетричних та асиметричних шифрів

Особливість	Симетричне Шифрування	Асиметричне Шифрування
Тип ключа	Один спільний ключ	Дві ключі (публічний та приватний)
Швидкість	Висока	Нижча в порівнянні з симетричним
Безпека передачі ключа	Потребує безпечного каналу	Публічний ключ можна передавати відкрито
Приклади	AES, DES	RSA

Ці два типи шифрування часто використовуються разом для забезпечення більшої безпеки. Наприклад, у протоколах безпечної передачі даних, таких як SSL/TLS, використовується асиметричне шифрування для безпечної передачі симетричного ключа, який потім використовується для шифрування даних.

Розуміння цих принципів криптографії є ключовим для розробки ефективних систем захисту інформації в сучасних технологічних середовищах, особливо в автоматизованих системах, де безпека даних є важливою [46] .

Сучасні криптографічні методи значно відрізняються від традиційних підходів, які використовувалися в минулому. На сьогоднішній день, ці методи включають різноманітні техніки, які розроблені для захисту інформації в цифровому світі. Основними серед них є блокові шифри, потокові шифри, хеш-функції та протоколи захисту.

Блокові шифри працюють шляхом перетворення фіксованого розміру блоку відкритого тексту у шифротекст, використовуючи симетричний ключ. Найвідомішим прикладом блокового шифру є AES (Advanced Encryption Standard), який широко використовується у багатьох застосуваннях. Іншим популярним блоковим шифром є DES (Data Encryption Standard), хоча він і вважається застарілим через свою відносно невелику довжину ключа.

Потокові шифри, у свою чергу, шифрують дані по одному біту або байту, замість обробки цілих блоків даних одночасно. Це робить їх підходящими для застосувань, де дані приходять у потоці, і потрібна швидка обробка. Прикладами потокових шифрів є RC4, який був популярний в протоколах безпечної передачі даних, та Salsa20.[48-49]

Хеш-функції використовуються для створення короткого, фіксованого розміру відбитку від довільного обсягу даних. Ці функції є односторонніми, що означає, що відтворити оригінальні дані з відбитку майже неможливо. Хеш-функції, такі як MD5, SHA-1 та SHA-2, використовуються для перевірки цілісності даних та у цифрових підписах.

Протоколи захисту, такі як SSL/TLS, забезпечують безпечне обмін інформацією між системами. Вони використовують комбінацію симетричних та асиметричних шифрів, а також хеш-функцій для забезпечення конфіденційності, аутентичності та цілісності даних [40] .

Огляд сучасних криптографічних методів представлений у таблиці 2.3.

Таблиця 2.3

Криптографічні методи

Тип Методу	Опис	Приклади
Блокові Шифри	Шифрують дані фіксованого розміру блоками	AES, DES
Потокові Шифри	Шифрують дані поодинокими бітами або байтами	RC4, Salsa20
Хеш-Функції	Створюють короткий відбиток даних для перевірки цілісності	MD5, SHA-1, SHA-2
Протоколи Захисту	Забезпечують безпечне обмін даними	SSL/TLS

Розуміння цих методів є необхідним для розробки ефективних систем криптографічного захисту в автоматизованих системах. Кожен з цих методів має свої переваги та області застосування, в залежності від потреб безпеки та характеристик системи.

Застосування криптографії в банківських автоматизованих системах є критично важливим для забезпечення безпеки фінансових транзакцій та конфіденційності клієнтської інформації. У світі, де фінансові операції стають все більш цифровими, криптографічні технології надають необхідні засоби для захисту від кіберзлочинності, шахрайства та несанкціонованого доступу.

Криптографія забезпечує захист персональних даних клієнтів, таких як деталі банківських рахунків, номери кредитних карток та історії транзакцій. Це досягається за допомогою сильного шифрування, яке перешкоджає доступу до цих даних несанкціонованими особами.[48]

Криптографічні протоколи, такі як SSL/TLS, використовуються для забезпечення безпечного обміну інформацією між банками та їх клієнтами. Ці протоколи захищають дані, що передаються через Інтернет, від перехоплення або модифікації третіми сторонами.

Цифрові підписи та сертифікати, що використовують асиметричне шифрування, надають засоби для аутентифікації користувачів та гарантії їх ідентифікації, підвищуючи рівень безпеки онлайн-сервісів.

Системи електронного банкінгу використовують криптографію для захисту фінансових операцій та забезпечення конфіденційності комунікацій між клієнтами та банками.[49]

Ключові криптографічні технології у банківських системах представлені у таблиці 2.4.

Таблиця 2.4

Ключові криптографічні технології

Криптографічна Технологія	Функція	Застосування
Шифрування Даних	Захист інформації від несанкціонованого доступу	Захист клієнтських даних, фінансових записів

SSL/TLS протоколи	Забезпечення безпечної передачі даних	Онлайн-транзакції, електронний банкінг
Цифрові Підписи	Аутентифікація та цілісність даних	Автентифікація користувачів, підтвердження транзакцій
Апаратні Безпекові Модулі (HSM)	Захист програмного та апаратного забезпечення	Захист ПЗ та апаратних систем банку

З ростом популярності мобільного банкінгу, криптографічні технології стають важливими для захисту додатків та транзакцій, що здійснюються через мобільні пристрої.

Нарешті, криптографія відіграє важливу роль у створенні та забезпеченні безпеки мобільних банківських додатків. Ці додатки надають користувачам можливість здійснювати фінансові операції через мобільні пристрої, і безпека цих операцій повністю залежить від ефективного використання криптографічних технологій.[50]

Загалом, криптографія є фундаментальною складовою сучасних банківських систем, що гарантує безпеку фінансових операцій та захист конфіденційності клієнтів у цифровому віці.

Повна назва комплексу - "Комплекс захисту SAP-системи "ІІТ Захист SAP"".

Головна мета цього комплексу - забезпечити криптографічний захист інформації у SAP-системі. Це включає в себе наступні завдання:

1. Аутентифікація користувачів SAP-системи, що дозволяє впізнавати користувачів і забезпечувати безпечний обмін даними між ними та сервером SAP. Ця аутентифікація використовує криптографічні методи для збереження конфіденційності та цілісності переданих даних.

2. Забезпечення цілісності та недоступності для змін даних та документів, що обробляються в системі. Це досягається за допомогою електронного цифрового підпису, який дозволяє перевірити автентичність та незмінність цих даних.

Для керування ключами і забезпечення їхньої безпеки використовується центр сертифікації ключів, який є складовою частиною комплексу.[46]

Структура та склад комплексу

Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах наведена на рисунку. (рис. 2.2)

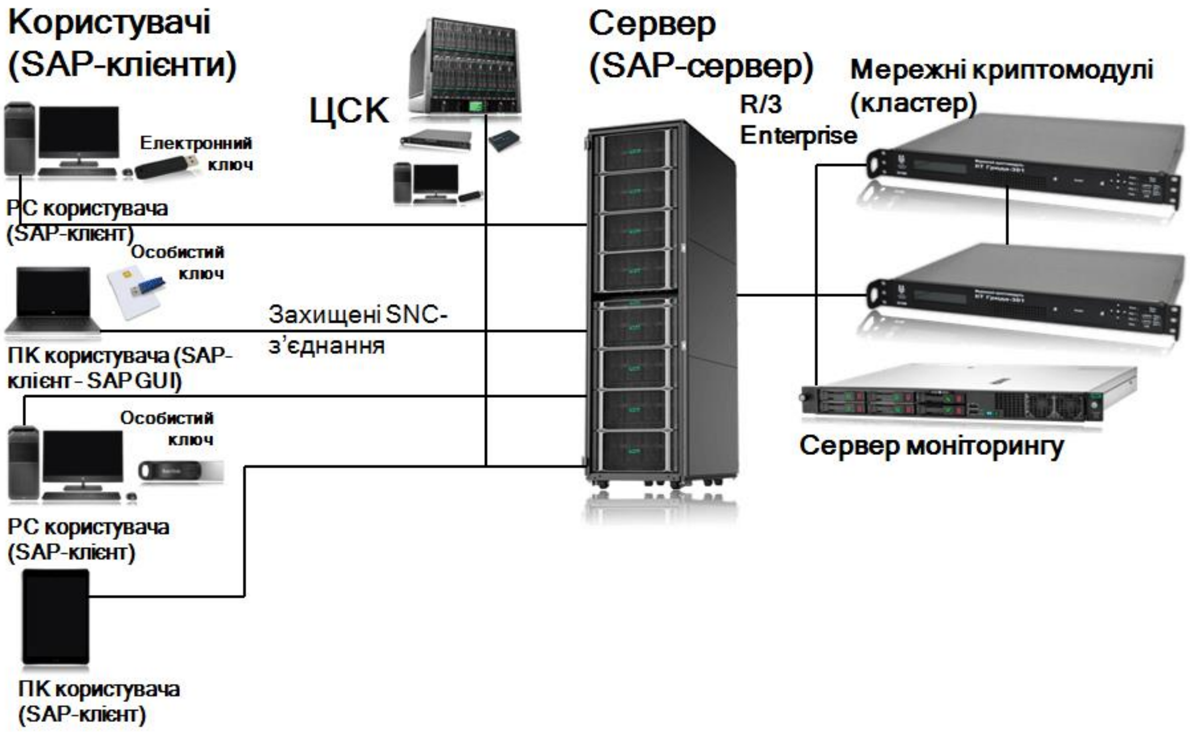

Рис. 2.2 . Структурна схема комплексу за розміщенням його складових частин на окремих технічних засобах

До складу комплексу входять:

1. Програмний комплекс захисту SAP-клієнта "ІІТ Захист SAP. Клієнт" у складі:

- SNC-бібліотеки (бібліотеки захисту з'єднань) для SAP-клієнта;
- SSF-бібліотеки (бібліотеки захищеного зберігання та пересилання) для SAP-клієнта;
- бібліотеки користувача ЦСК зі складу програмного комплексу користувача ЦСК "ІІТ Користувач ЦСК-1";
- засобів управління та моніторингу стану захисту клієнта;

2. Програмний комплекс захисту SAP-сервера "ІІТ Захист SAP. Сервер" у складі:

- SNC-бібліотеки для SAP-сервера;
- SSF-бібліотеки для SAP-сервера;
- бібліотек користувача ЦСК;
- засобів управління захистом сервера;
- агента моніторингу захисту SAP-сервера;

3. Програмний комплекс віддаленого моніторингу захисту SAP-сервера "ІІТ Захист SAP. Віддалений монітор сервера".

Основні компоненти комплексу включають:

1. Програмні засоби КЗІ (Криптографічного Захисту Інформації), які вбудовані безпосередньо в клієнтську та серверну частини SAP-системи. Ці програмні засоби взаємодіють з механізмами та інтерфейсами криптографічного захисту інформації в SAP-системі. Вони можуть використовувати зовнішні апаратні засоби КЗІ, такі як електронні ключі та мережні криптомодулі.

2. SNC-бібліотеки (бібліотеки захисту з’єднань) у складі SAP-клієнта та SAP-сервера, які відповідають за автентифікацію користувачів та забезпечення конфіденційності та цілісності даних, що передаються між користувачами та сервером SAP-системи. Вони використовують криптографічні методи для шифрування та перевірки цілісності інформації під час її передачі.

3. SSF-бібліотека (бібліотека захищеного зберігання та пересилання) у складі SAP-клієнта та SAP-сервера, яка використовується для забезпечення цілісності та недоступності для змін електронних даних та документів, що обробляються в SAP-системі. Вона створює та перевіряє електронний цифровий підпис для даних та документів, що обмінюються між користувачами та сервером SAP-системи.[46]

Компоненти системи включають:

1. Засоби управління та моніторингу клієнта: Вони використовуються для налаштування параметрів SNC- та SSF-бібліотек, а також для відслідковування їх роботи.

2. Засоби управління захистом сервера: Вони призначені для налаштування параметрів SNC- та SSF-бібліотек на стороні сервера.

3. Агент моніторингу захисту SAP-сервера: Цей агент відстежує стан програмних засобів захисту сервера і веде журнали подій. Він також зберігає інформацію про активні захищені з’єднання та надає доступ до цієї інформації для віддаленого моніторингу.

4. Програмний комплекс віддаленого моніторингу захисту SAP-сервера: Цей комплекс отримує інформацію від агента моніторингу сервера і відображає її, включаючи стан і статистику функціонування програмних засобів захисту та події з журналів реєстрації.

5. SNC-бібліотеки (бібліотеки захисту з'єднань): Вони використовуються для автентифікації користувачів та забезпечення конфіденційності і цілісності даних між користувачами та сервером SAP-системи. Вони реалізовані з використанням механізмів GSS-API v2 та SNC-адаптера.

6. SSF-бібліотеки (бібліотеки захищеного зберігання та пересилання): Вони використовуються для забезпечення цілісності та невідмовності авторства електронних даних та документів у SAP-системі. SSF-бібліотеки використовуються для формування та перевірки електронного цифрового підпису для даних та документів, що обмінюються між користувачами та сервером.

7. Електронний ключ і Мережний криптомодуль: Ці апаратні пристрої використовуються для забезпечення апаратної реалізації криптографічних операцій. Електронний ключ використовується для користувачів SAP-системи, а Мережний криптомодуль для серверів SAP-системи. Вони зберігають та захищають особисті ключі та забезпечують безпеку операцій з криптографією.[46]

Ці компоненти взаємодіють між собою для забезпечення криптографічного захисту інформації в SAP-системі.

Висновки до розділу 2. Виклики та перспективи в сфері криптографії відображають швидкий розвиток технологій та зміну кіберзагроз. Сучасна криптографія стикається з рядом викликів, які охоплюють технічні, теоретичні та практичні аспекти захисту інформації.

Одним з головних викликів є розвиток квантових комп'ютерів. Квантові комп'ютери мають потенціал ламати сучасні криптографічні алгоритми, зокрема асиметричні шифри, такі як RSA та ECC (еліптичні криві). Це створює потребу у розвитку квантово-стійких алгоритмів, які можуть витримати атаки з використанням квантових технологій.

Іншим значним викликом є потреба у балансуванні між безпекою та швидкістю. Як технології розвиваються, зростає потреба у швидших криптографічних алгоритмах, які можуть забезпечити необхідний рівень безпеки без зниження продуктивності систем.

Крім того, зростає необхідність у стандартизації криптографічних алгоритмів та протоколів. Забезпечення сумісності різних систем та пристроїв, які використовують криптографію, є важливим для гарантування безперебійної та безпечної роботи глобальних мережевих інфраструктур.

Серед перспектив криптографії – розвиток нових алгоритмів та методів шифрування, які можуть адаптуватися до мінливих вимог безпеки та ефективно протистояти зростаючим кіберзагрозам. Це охоплює також розробку алгоритмів машинного навчання та штучного інтелекту для автоматизації процесів виявлення та відповіді на кібератаки.

Однією з головних перспектив є також розвиток квантово-стійкої криптографії. Оскільки загроза від квантових комп'ютерів стає дедалі більш реальною, необхідність у розробці нових криптографічних систем, які можуть витримати квантові атаки, стає нагальною.

В цілому, сектор криптографії знаходиться на передньому краї технологічного прогресу, намагаючись відповісти на постійно змінювані виклики та загрози в цифровому світі. Це вимагає неперервних досліджень та інновацій для забезпечення безпеки інформації та захисту цифрових систем у майбутньому.

РОЗДІЛ 3

ФОРМУВАННЯ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ З АСУ

3.1 Аналіз загроз мережевим ресурсам АСУ

Проблематика дослідження критичних обставин та елементів, які можуть створювати ризики для інформаційної безпеки, а також знаходження та обґрунтування способів їх усунення чи мінімізації, характеризується декількома ключовими аспектами:

- Наявність великої кількості факторів, що можуть призводити до небезпечних ситуацій, та необхідність ідентифікації їхніх джерел та причин;
- Важливість визначення та дослідження всього спектру можливих стратегій та методів протидії цим ризикованим елементам для забезпечення захисту інформації.

З іншого боку, існує також загроза захищеній інформації. У наукових працях ця загроза описана як "сукупність обставин, факторів та умов, що становлять ризик порушення статусу інформації". Це означає, що загрози інформації визначаються конкретними елементами та умовами, які можуть виникати у певних ситуаціях. (рис. 3.1)[50]

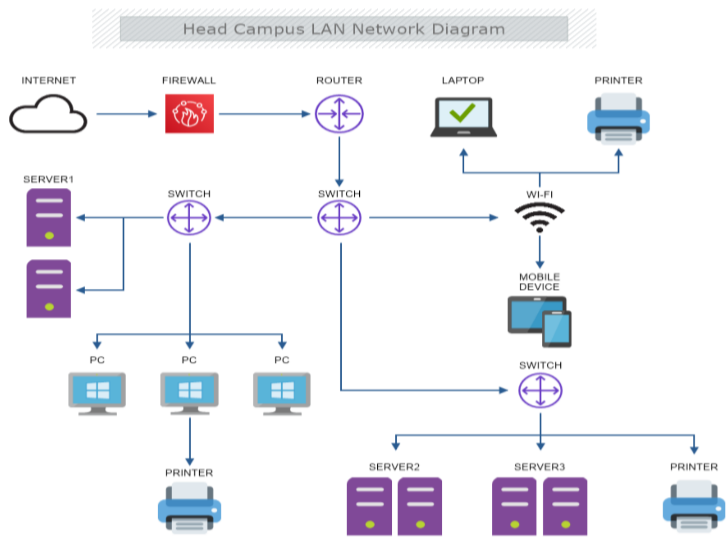

Рис. 3.1 - Мережева інфраструктура

Щодо інформаційних систем, усі потенційні ризики можна класифікувати на дві основні категорії: зовнішні та внутрішні. Кожна з цих категорій поділяється на навмисні та ненавмисні загрози, які можуть бути як очевидними, так і прихованими [51] .

Розпізнавання та аналіз цих загроз є критично важливими елементами при створенні ефективної системи захисту інформації. Часто використовуваний термін у цій сфері - «загрози інформаційної безпеки». Проте, важливо розуміти, що інформаційна безпека означає забезпечення стану, в якому інформація захищена від будь-яких небажаних втручань, що можуть порушити її цілісність або доступність.

Основу мережевої інфраструктури формують сервери, які зберігають бази даних, прикладні програми та інші важливі системи. Ці сервери зазвичай розташовуються в кількох дата-центрах для забезпечення надійності та відмовостійкості. Маршрутизатори та комутатори забезпечують зв'язок між серверами та різними частинами мережі, включно з відділеннями банку, банкоматами та іншими точками доступу.

Брандмауери та інші системи безпеки відіграють ключову роль у захисті мережі. Вони не тільки контролюють вхідний та вихідний трафік, але й захищають від несанкціонованого доступу та інших кіберзагроз. Застосування сучасних методів фільтрації та ідентифікації аномалій у мережевому трафіку є невід'ємною частиною стратегії безпеки [52] .

Інфраструктура також включає бездротові мережі та мобільний доступ, що дозволяє співробітникам банку та його клієнтам здійснювати транзакції з будь-якої точки світу. Це ставить додаткові вимоги до безпеки, оскільки мобільні пристрої та бездротові мережі можуть бути вразливими до специфічних видів атак.

Завдяки використанню віртуальних мереж (VPN) та інших технологій шифрування, дані, що передаються через цю мережу, захищені від перехоплення та зловмисного використання. VPN забезпечують зашифроване з'єднання між віддаленими користувачами та центральними системами банку, що є критично важливим для забезпечення конфіденційності та цілісності фінансових транзакцій.

В цілому, мережева інфраструктура автоматизованих банківських систем є складною та багатогранною, забезпечуючи не лише необхідну продуктивність та надійність, але й високий рівень захисту від різноманітних кіберзагроз. Вивчення та постійне вдосконалення цієї інфраструктури є ключовими для забезпечення безпеки інформації в сучасному банківському секторі.

Існують два фундаментально відмінних підходи до управління користувачами та мережевими ресурсами:

- Модель управління, заснована на робочих групах;

Модель доменного управління.

Робоча група представляє собою логічне угруповання мережевих комп'ютерів, які надають спільний доступ до таких ресурсів, як файли та принтери (рис. 3.2) .

Модель робочої групи

Рис. 3.2 - Модель робочої групи (модель розподіленого управління)

Така група є характерною для однорангових мереж, де кожен комп'ютер надає однаковий доступ до ресурсів без необхідності використання окремого сервера. Всі комп'ютери в робочій групі управляють власними локальними базами даних безпеки, що містять інформацію про облікові записи користувачів і захист ресурсів. Така організація призводить до децентралізованого (розподіленого) управління обліковими записами і безпекою ресурсів.[49]

Недоліки робочої групи включають:

- Необхідність у створенні облікових записів користувачів на кожному комп'ютері, до якого потрібен доступ.
- Вимога виконання всіх змін в облікових записах, таких як зміни паролів або створення нових облікових записів, на кожному комп'ютері в робочій групі.
- Доступ до файлів та пристроїв обмежений користувачами, які мають облікові записи на кожному конкретному комп'ютері.

Переваги робочої групи:

- Немає необхідності в сервері для зберігання централізованої інформації безпеки.
- Простота в проектуванні та управлінні, в порівнянні з доменними системами, з меншими вимогами до планування та адміністрування.
- Підходить для невеликих мереж, де комп'ютери знаходяться поруч, але стає непрактичним у мережах, що містять більше 10 комп'ютерів.

Домен є логічною структурою, що об'єднує мережеві комп'ютери, доступ до ресурсів яких регулюється через централізовану базу даних. Ця база, відома як База даних каталогу або просто каталог, містить всі облікові записи користувачів та параметри безпеки домена. Вона є частиною більшої служби каталогу, яка обробляє запити користувачів на доступ до ресурсів. Ці ресурси включають не тільки файлові системи та мережеві принтери, а й інші мережеві служби та інформаційні ресурси.

Каталоги домена розміщуються на контролерах домена - спеціалізованих комп'ютерах, на яких встановлені операційні системи, що підтримують ці функції (наприклад, Windows 2000/2003 Server). Ці контролери забезпечують централізоване управління безпекою та адмініструванням домена. Важливо, що домен не обмежується фізичним розташуванням або конкретною конфігурацією мережі [50].

Комп'ютери в домені можуть бути фізично розташовані поряд, у межах маленької локальної мережі, або розосереджені по різних країнах. Вони можуть з'єднуватися через різноманітні фізичні засоби, такі як модеми, ISDN (Integrated Services Digital Network), оптоволоконні лінії, Ethernet, з'єднання з ретрансляцією кадрів, супутникові та орендовані лінії. (рис. 3.3)

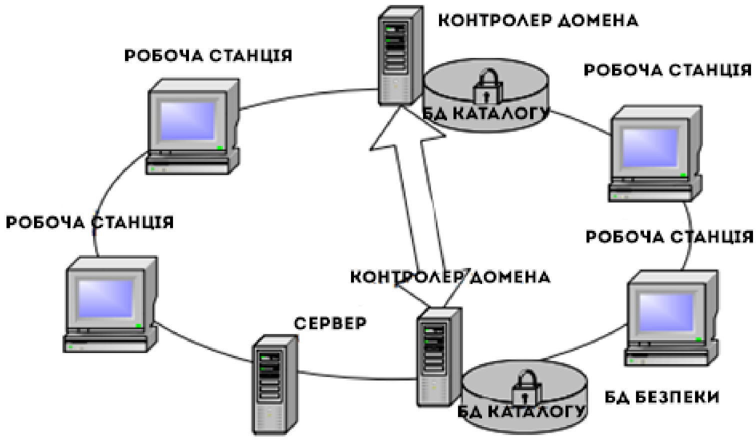

Рис. 3.3. Модель домена (модель централізованого управління)

Переваги використання доменної моделі управління включають наступне:

- Централізоване управління користувачами: Всі дані про користувачів зосереджуються в одному місці, що спрощує адміністрацію. Зміни, такі як оновлення паролів користувачів, автоматично поширюються по всьому домену.
- Єдиний вхід для доступу до мережевих ресурсів: Користувачі мають можливість входити в систему на одному комп'ютері і доступатися до ресурсів інших комп'ютерів в межах дозволених прав доступу.
- Масштабованість: Домени дозволяють адміністраторам ефективно управляти великими мережами.[52]

Структура типового домену містить:

- Контролери домену: Кожен з них містить копію каталогу із обліковими записами користувачів. Під час входу користувача в домен, контролер домену перевіряє його дані в каталозі. У випадку наявності декількох контролерів, вони синхронізують дані між собою.

- Рядові сервери: Це сервери, що не налаштовані як контролери домену. Вони не зберігають дані каталогу і не здійснюють перевірку користувачів домену, а лише надають доступ до ресурсів, як-от файли та принтери, використовуючи дані каталогу для перевірки прав доступу.
- Клієнтські комп'ютери: Це комп'ютери, які використовують користувачі і які дозволяють їм доступатися до ресурсів домену.

Загрози та вразливості в мережевій інфраструктурі автоматизованих банківських систем є різноманітними та складними, враховуючи постійно зростаючий обсяг цифрових операцій та їхню складність. Вони включають як зовнішні, так і внутрішні загрози, кожна з яких вимагає уваги та відповідних заходів безпеки.

Серед зовнішніх загроз особливо важливими є кібератаки, такі як атаки "man-in-the-middle", при яких зловмисник може перехоплювати та змінювати дані, що передаються між двома сторонами. Це особливо небезпечно у випадку транзакцій, де конфіденційність та цілісність даних є критично важливими. DDoS-атаки (Distributed Denial of Service) також є значною загрозою, оскільки вони можуть зупинити роботу банківських систем, переповнюючи їх надмірним трафіком та виводячи з ладу важливі компоненти мережі.

Віруси та шпигунське програмне забезпечення є іншими формами зовнішніх загроз, які можуть інфікувати системи, викрадати конфіденційні дані, або навіть здійснювати несанкціоновані фінансові транзакції. Фішинг та інші види соціальної інженерії також є значною проблемою, оскільки вони спрямовані на викрадення облікових даних та іншої конфіденційної інформації шляхом обману співробітників або клієнтів.

Внутрішні загрози, такі як несанкціонований доступ або зловмисні дії власних співробітників, є не менш важливими. Це може включати зловживання доступом до систем, ненавмисне використання слабких паролів або ігнорування політик безпеки, що може призвести до витоку або компрометації конфіденційної інформації.

Безпека фізичних компонентів мережі також є важливою. Недостатній фізичний захист серверних приміщень, маршрутизаторів, комутаторів та інших критичних компонентів може призвести до несанкціонованого доступу та пошкоджень.

Таблиця 3.1 допомагає систематизувати розуміння різних загроз, їх наслідків і конкретних сценаріїв, з якими може зіткнутися банківська мережева інфраструктура.

Таблиця 3.1

Види загроз і їх наслідки

Основні Види Загроз	**Потенційні Наслідки**	**Приклади**
Атаки 'man-in-the-middle'	Перехоплення та зміна даних	Перехоплення фінансових транзакцій
DDoS-атаки	Перевантаження мережевих ресурсів, зупинка роботи систем	Атака на сервери банку, що викликає їх недоступність
Віруси та шпигунське програмне забезпечення	Крадіжка конфіденційних даних, шкода системам	Інфекція робочих станцій вірусами, викрадення даних клієнтів
Фішинг та соціальна інженерія	Викрадення облікових даних, шахрайство	Використання фальшивих електронних листів для отримання доступу до рахунків

3.2 Застосування технічних засобів захисту інформації в АСУ

Захист через віртуальні приватні мережі (VPN) відіграє ключову роль у забезпеченні безпеки мережевої інфраструктури автоматизованих банківських систем. VPN створюють зашифрований канал між користувачем та мережею, що забезпечує безпечне і приватне підключення через інтернет. Це особливо важливо для банківських установ, де конфіденційність інформації та її захист від несанкціонованого доступу є пріоритетом.

Використання VPN дозволяє забезпечити безпеку даних при їх передачі між центральним офісом банку, філіями, банкоматами та іншими віддаленими локаціями, а також для мобільних співробітників. Шифрування даних, що проходять через VPN, ускладнює можливість їх перехоплення та дешифрування зловмисниками.

Ключовими аспектами захисту через VPN є використання сучасних методів шифрування, таких як AES (Advanced Encryption Standard), які забезпечують високий рівень безпеки. Крім того, використання надійних механізмів аутентифікації, таких як багаторівнева аутентифікація або цифрові сертифікати, допомагає переконатися, що доступ до мережі мають тільки уповноважені користувачі.

VPN також допомагають вирішити проблеми з сумісністю різних мережевих протоколів та забезпечити безперервність бізнес-процесів, оскільки вони дозволяють віддаленим співробітникам ефективно та безпечно працювати за межами традиційного офісного середовища.

Втім, потрібно зазначити, що, хоча VPN забезпечують значний рівень безпеки, вони не є панацеєю. Необхідно також забезпечувати безпеку на кінцевих точках, регулярно оновлювати програмне забезпечення та виконувати аудити безпеки, щоб ідентифікувати та усунути потенційні вразливості.

Таблиця 3.2, яка демонструє різні типи VPN, використані методи шифрування, типи аутентифікації, а також приклади їх застосування:

Таблиця 3.2

Типи VPN

Типи VPN	Методи Шифрування	Типи Аутентифікації	Приклади Застосування
Site-to-Site	IPsec, SSL/TLS	Цифрові сертифікати, PSK	З'єднання між різними філіями банку
Remote Access	SSL/TLS, OpenVPN	Цифрові сертифікати, Багаторівнева аутентифікація	Безпечний доступу для віддалених співробітників

Ця таблиця допомагає візуально представити ключові характеристики та застосування різних типів VPN, які є важливими для забезпечення безпеки мережевої інфраструктури в автоматизованих банківських системах.

Мережеві фільтри та брандмауери є невід'ємною частиною захисту мережевої інфраструктури автоматизованих банківських систем. Вони функціонують як бар'єр між внутрішньою мережею банку та зовнішнім світом, контролюючи вхідний та вихідний мережевий трафік на основі встановлених правил безпеки.

Брандмауери можуть бути апаратними, програмними або комбінованими, і їх основна функція полягає у перешкоджанні несанкціонованого доступу до мережі, а також у запобіганні витоку конфіденційної інформації. Вони аналізують пакети даних, які проходять через мережу, та визначають, чи відповідають вони встановленим критеріям безпеки.

Мережеві фільтри діють як частина брандмауера, використовуючи різні методи для перевірки та управління мережевим трафіком. Вони можуть включати фільтрацію за IP-адресами, портами, протоколами або навіть за конкретним вмістом пакетів. Це дозволяє ефективно блокувати шкідливі або підозрілі запити, а також забезпечувати, що лише легітимний трафік потрапляє в мережу банку.

Існують різні типи брандмауерів, включаючи станові та безстатеві. Станові брандмауери відрізняються тим, що вони відстежують стан активних з'єднань та приймають рішення на основі контексту трафіку. Безстатеві брандмауери ж працюють на більш простому рівні, фільтруючи пакети на основі встановлених правил без врахування стану з'єднання.

Управління брандмауерами та мережевими фільтрами вимагає ретельного планування та налаштування. Неправильно сконфігуровані правила можуть призвести до ненавмисного блокування легітимного трафіку або, навпаки, дозволити проходження шкідливих пакетів.

Цей пункт охоплює широкий спектр рішень і практик, які використовуються для зміцнення безпеки мережевої інфраструктури. Ці технології включають, але не обмежуються, інтрузивними системами виявлення та запобігання (IDS/IPS), системами управління ідентифікацією та доступом (IAM), а також рішеннями з шифрування даних.

Інтрузивні системи виявлення (IDS) та системи запобігання вторгненням

(IPS) є критично важливими для виявлення потенційних загроз та негайного реагування на них. IDS моніторить мережевий трафік, виявляючи підозрілу активність та потенційні атаки, тоді як IPS активно блокує таку активність, запобігаючи потенційній шкоді.

Системи управління ідентифікацією та доступом (IAM) відіграють ключову роль у забезпеченні того, що тільки авторизовані особи мають доступ до відповідних ресурсів. Вони забезпечують централізоване управління ідентифікацією користувачів, їхніми правами доступу, а також здійснюють моніторинг та записують дії користувачів у системі.

Шифрування даних є ще однією важливою складовою цілісної стратегії безпеки. Використання сучасних алгоритмів шифрування для захисту даних, збережених на серверах або переданих через мережу, є необхідним для запобігання їх перехопленню та несанкціонованому використанню.

Всі ці технології повинні інтегруватися в єдину, багаторівневу систему безпеки, яка охоплює як технічні, так і організаційні аспекти. Важливо також регулярно проводити аудити безпеки та оновлювати системи для захисту від нових загроз і вразливостей.

Важливим і новим у дослідженнях є застосування методу кейс-стаді.

Кейс 1: Оптимізація мережевої інфраструктури інформаційної безпеки

У сучасних системах інформаційної безпеки акцент робиться на надійність та економічну ефективність рішень, які забезпечують більш широкий огляд сегментів мережі з вже встановленими засобами безпеки. Нові засоби безпеки, що впроваджуються, мають бути інтегровані з існуючими точками збору мережевого трафіку (рис. 3.4) .

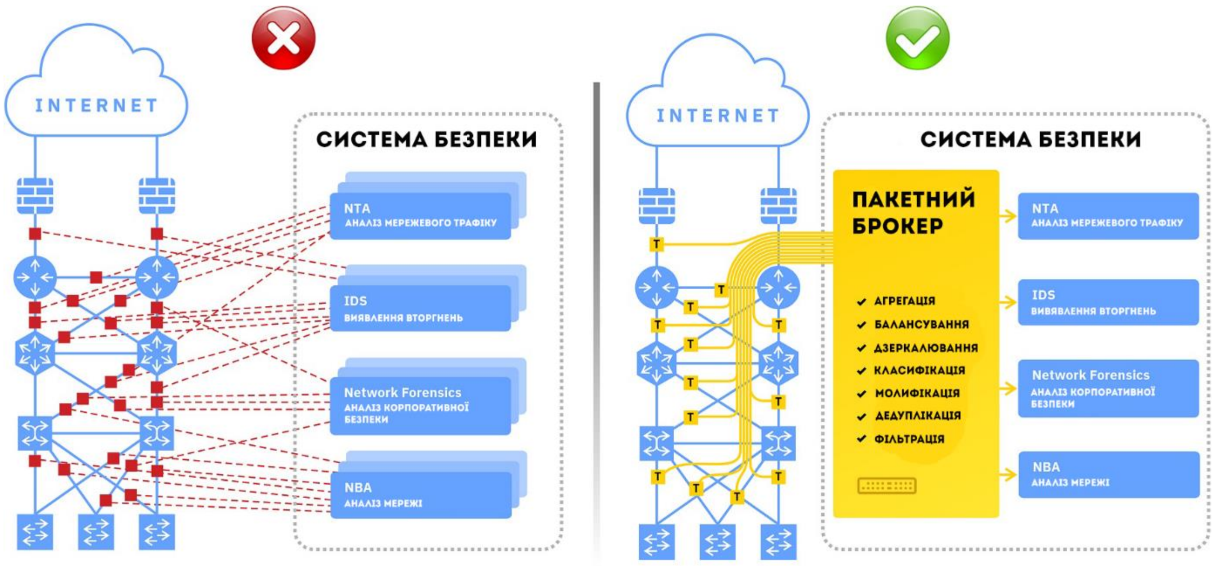

Рис. 3.4. Мережева інфраструктура підприємства

Однак, існуючі методи моніторингу трафіку, такі як використання SPAN-портів та мережевих відгалужень (TAP), мають свої обмеження. Трафік через SPAN-порти має низький пріоритет і може втрачатися при високому навантаженні на комутатор, в той час як високий пріоритет може призводити до втрати основного трафіку, що створює ризики. З іншого боку, використання TAP забезпечує точне віддзеркалення трафіку, але має обмеження щодо кількості точок, де можна встановити TAP.

По мірі зростання кількості засобів інформаційної безпеки, які потребують доступу до одних і тих же мережевих сегментів, виникає важливе питання їх інтеграції в існуючу інфраструктуру.

Задача: У компанії використовуються системи для виявлення вторгнень (IDS) і аналізу поведінки мережі (NBA), а також ведеться впровадження систем Network Forensics і NTA. Для забезпечення повної видимості мережевого трафіку, використовуються TAP, а не SPAN-порти. Потрібно забезпечити передачу трафіку від TAP з відповідних мережевих сегментів до чотирьох різних систем безпеки.

Рішення: Ця задача ефективно вирішується за допомогою брокера мережевих пакетів. Використання брокера дозволяє агрегувати мережевий трафік, отриманий через TAP з різних сегментів мережі. Це дозволяє оптимізувати трафік, застосовуючи різні функції, такі як фільтрація, класифікація, дедуплікація, та модифікація, а також рівномірно розподіляти його між всіма системами інформаційної безпеки.

Кейс 2: Використання інструментів безпеки 1G в сучасних мережах

Стандарт 10-гігабітного Ethernet (10GbE або 10G) був вперше представлений у 2002 році і набрав популярності до 2007 року. Відтоді 10G став фундаментом для розгортання великих мережевих інфраструктур і магістральних з'єднань. Наразі стають все більш поширеними стандарти 40G та 100G, а в майбутньому очікується впровадження стандартів 200G та 400G. (рис. 3.5)

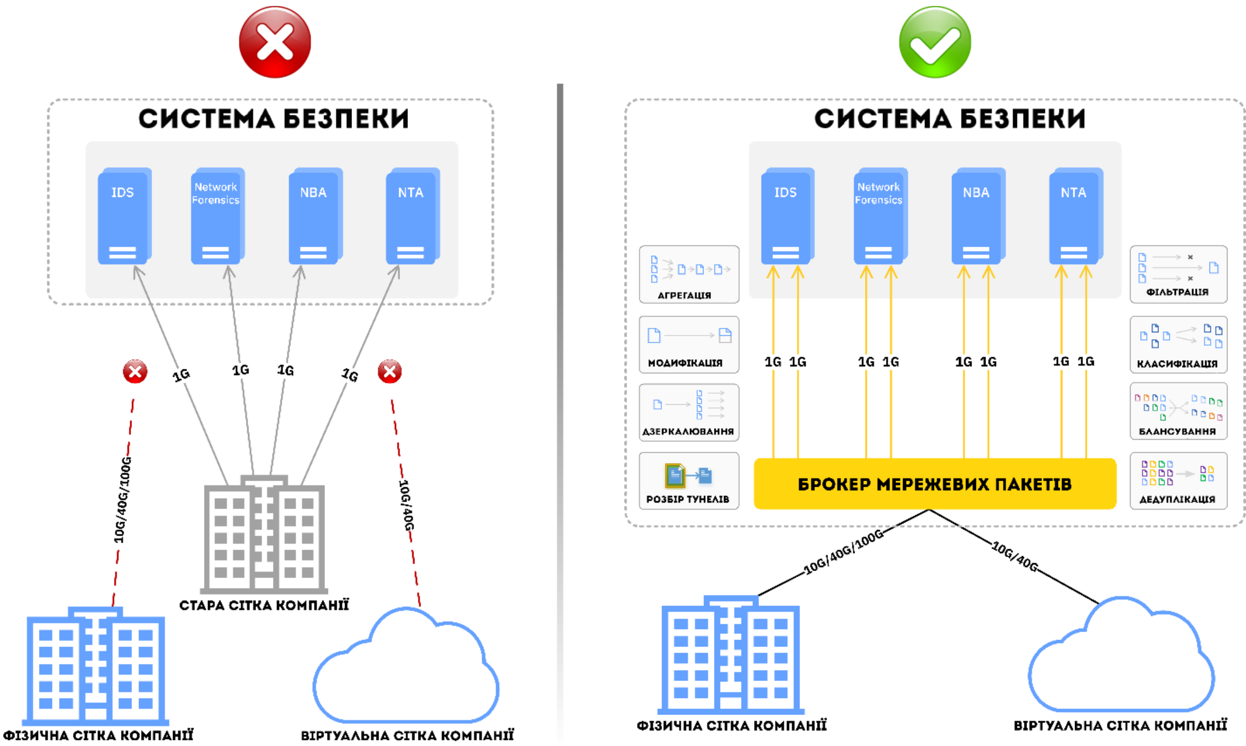

Рис. 3.5 - Використання інструментів безпеки 1G в сучасних мережах

У більшості великих комп'ютерних мереж є численні пристрої для моніторингу безпеки 1-гігабітних волоконно-оптичних мереж (1G). Ці системи залежно від моделі здатні обробляти більше 1 Гбіт/с трафіку. Однак обладнання з 1G інтерфейсами фізично не може підключатися до мереж із вищими стандартами, такими як 10G, 40G або 100G.

Завдання: У зв'язку з модернізацією мережевої інфраструктури компанії, яка передбачає заміну 1G інтерфейсів на більш швидкісні 10G, 40G, і 100G інтерфейси, виникає потреба адаптувати існуючу систему інформаційної безпеки, що працює на 1G, до нових умов.

Рішення: Ефективним рішенням є використання брокерів мережевих пакетів. Ці пристрої дозволяють агрегувати та оптимізувати трафік із швидкісних мереж (10G/40G/100G), адаптуючи його для систем безпеки з 1G інтерфейсами. Вони забезпечують не тільки подовження терміну експлуатації існуючих засобів, але і підвищують їх продуктивність та надійність.

Використання брокерів мережевих пакетів вирішує наступні завдання:

- Розширює можливості моніторингу і контролю мережі;
- Дозволяє підключати більшу кількість засобів моніторингу та контролю трафіку;
- Оптимізує використання систем інформаційної безпеки;
- Не впливає на надійність мережі;
- Забезпечує сумісність різних інтерфейсів в системі безпеки;
- Підвищує рівень видимості мережі для систем безпеки.

Це підкреслює, наскільки просто можна вирішити типові проблеми, що виникають при розбудові систем інформаційної безпеки, використовуючи брокери мережевих пакетів для підвищення ефективності та надійності всієї системи. У наступній частині обговоримо активні методи забезпечення мережевої безпеки та розглянемо типові сценарії їх інтеграції в мережеву інфраструктуру компанії.

3.3 Формулювання політики інформаційної безпеки в АСУ

Забезпечення власної інформаційної безпеки на підприємствах, як правило, є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань та має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо. В лекції перераховуються основні напрями управлінської (організаційної) роботи у сфері інформаційної безпеки на рівні окремого підприємства. Розкривається загальна структура політики інформаційної безпеки підприємства як основного організуючого документа в цій галузі.

Забезпечення інформаційної безпеки також, як правило, має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямків діяльності та бізнес-процесів, таких як комерційні переговори і умови контрактів, цінова політика, тощо. Крім того, значимість забезпечення інформаційної безпеки в деяких випадках може визначатися наявністю в загальній системі інформаційних потоків підприємства відомостей, що становлять не тільки комерційну, а й державну таємницю, а також інші види конфіденційної інформації (відомості, що становлять банківську таємницю, лікарську таємницю, інтелектуальну власність компаній-партнерів тощо). [52]

Так само як і на державному рівні, управління інформаційною безпекою на рівні підприємств націлене на нейтралізацію різних видів загроз:

- зовнішніх, таких як неправомірні дії державних органів (у тому числі і закордонних), протиправна діяльність злочинців і злочинних угруповань, незаконні дії компаній-конкурентів та інших господарюючих суб'єктів, недобросовісні дії компаній-партнерів, невідповідність чинної нормативно-правової бази фактичному розвитку технологій і суспільних відносин, збої і порушення в роботі глобальних інформаційних та телекомунікаційних систем та інформаційних систем компаній-партнерів (контрагентів) та ін.;
- внутрішніх, таких як помилки і халатність персоналу підприємства, а також навмисно допускаються порушення, збої і порушення в роботі власних інформаційних систем та ін.

Таким чином, управління інформаційною безпекою на кожному окремому підприємстві має здійснюватися в контексті його загальної господарської діяльності: з урахуванням характеру діяльності компанії (технології виробництва, специфіки ринків збуту тощо), а також як фактично складається ситуація у ринковій конкурентній боротьбі, державній політиці, розвитку правової та правоохоронної системи, рівня розвитку окремих використовуваних інформаційних і телекомунікаційних технологій та інших факторів, що формують загальні умови поточної діяльності [48].

Формальною підставою (передумовою) для здійснення цілеспрямованої діяльності у сфері захисту інформації, крім загальнодержавних вимог до захисту інформації, що становить державну, військову, лікарську та банківську таємницю, також є перелік відомостей, що становлять комерційну таємницю підприємства, який визначається підприємством самостійно з урахуванням вимог чинного законодавства.

Крім того, необхідність розробки і впровадження політики інформаційної безпеки може бути обумовлена такими обставинами як:

- необхідність зменшення вартості страхування інформаційних ризиків або певних бізнес-ризиків;
- необхідність впровадження міжнародних стандартів, таких як ISO/IEC 27002.

На рисунку 3.6 представлено передумови розробки політики безпеки підприємства.

Рис. 3.6. Передумови розробки політики безпеки підприємства

Для нейтралізації існуючих загроз і забезпечення інформаційної безпеки підприємства створюють систему менеджменту у сфері інформаційної безпеки, в рамках якої (системи) проводять роботу за кількома напрямками (рис. 3.7) :

- формування та практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;
- організація департаменту (служби, відділу) інформаційної безпеки;
- розробка системи заходів і дій на випадок виникнення непередбачених ситуацій («Управління інцидентами»);
- проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен аспект організаційної діяльності має свої унікальні характеристики і вимагає застосування спеціалізованих управлінських методів та дотримання відповідних правил. Політика і правила в області інформаційної безпеки служать організаційними директивами, що керують діяльністю як всієї організації, так і окремих її підрозділів (або груп співробітників) у взаємодії з інформаційними системами та потоками. Відділ інформаційної безпеки, як вузькоспеціалізований сегмент, вирішує конкретні завдання з охорони інформації. Система заходів для реагування на інциденти гарантує, що уся організація (включно з відділом інформаційної безпеки) буде готова до свідомих та цілеспрямованих дій у разі будь-яких проблем, пов'язаних з інформаційною безпекою. Проведення регулярних або подієвих внутрішніх аудитів інформаційної безпеки необхідне для забезпечення контролю над поточним станом захисних заходів і для незалежної перевірки відповідності фактичного стану справ офіційним правилам та вимогам.

Кожна сфера діяльності в організації повинна неперервно розвиватися і адаптуватися, з урахуванням змін в організаційній структурі, виробничих процедурах, а також у зовнішніх умовах. Це передбачає регулярне уточнення та адаптацію конкретних завдань, щоб забезпечити їх актуальність і ефективність у динамічному бізнес-середовищі.

Рис. 3.7. Структура організаційної діяльності у сфері інформаційної безпеки на підприємстві

Структура політики інформаційної безпеки та її розробка об'єднують комплекс документів, які відображають ключові вимоги до захисту інформації та стратегію підприємства в цій області. Політика інформаційної безпеки може бути розділена на три основні рівні: вищий, середній і нижчий.

На вищому рівні політика інформаційної безпеки виконує такі функції:

- Вона виражає позицію і підхід керівництва компанії до питань інформаційної безпеки, відображаючи загальні цілі компанії в цій сфері.
- Цей рівень служить основою для створення специфічних політик безпеки, правил і процедур на більш низьких рівнях.
- Він також виступає інструментом для інформування співробітників компанії про основні завдання та пріоритети в області інформаційної безпеки.

Політики інформаційної безпеки середнього рівня визначають ставлення підприємства (керівництва підприємства) до певних аспектів його діяльності та функціонування інформаційних систем:

- ставлення і вимоги (більш детально в порівнянні з політикою верхнього рівня) підприємства до окремих інформаційних потоків та інформаційних систем, обслуговуючим різні сфери діяльності, ступінь їх важливості та конфіденційності, а також вимоги до надійності (наприклад, відносно фінансової інформації, а також інформаційних систем і персоналу, які відносяться до неї);

- відношення і вимоги до певних інформаційних та телекомунікаційних технологій, методів і підходів до обробки інформації і побудови інформаційних систем;
- відношення і вимоги до співробітників підприємства як до учасників процесів обробки інформації, від яких безпосередньо залежить ефективність багатьох процесів і захищеність інформаційних ресурсів, а також основні напрями і методи впливу на персонал з метою підвищення інформаційної безпеки.

Політики безпеки на найнижчому рівні відносяться до окремих елементів інформаційних систем і ділянок обробки та зберігання інформації і описують конкретні процедури і документи, пов'язані із забезпеченням інформаційної безпеки.[49]

Розробка політики безпеки передбачає здійснення низки попередніх кроків:

- оцінку особистих (суб'єктивних) відносин до ризиків підприємства його власників і менеджерів, відповідальних за функціонування і результативність роботи підприємства в цілому або окремі напрями його діяльності;
- аналіз потенційно вразливих інформаційних об'єктів;
- виявлення загроз для значущих інформаційних об'єктів (відомостей, інформаційних систем, процесів обробки інформації) і оцінку відповідних ризиків.

Виконання попереднього аналізу дозволяє оцінити значимість інформаційної безпеки для стабільної діяльності і економічної стійкості компанії. Цей аналіз, враховуючи оцінки менеджменту та власників, допомагає визначити конкретні напрямки заходів з інформаційної безпеки. У деяких випадках, індивідуальні погляди окремих керівників можуть не мати вирішального впливу.

Отже, політика інформаційної безпеки, майже на всіх рівнях, буде ґрунтуватися на чітко визначених, формалізованих правилах та процедурах. Це може включати застосування сертифікованого обладнання та програмного забезпечення, дотримання процедур доступу, організацію спеціальних приміщень для зберігання даних та інші подібні заходи.При розробці політик безпеки всіх рівнів необхідно дотримуватися наступних основних правил.

1) Політики безпеки на більш низьких рівнях повинні повністю підкорятися відповідній політиці верхнього рівня, а також чинному законодавству і вимогам державних органів.

2) Текст політики безпеки повинен містити тільки чіткі і однозначні формулювання, що не допускають подвійного тлумачення.

3) Текст політики безпеки повинен бути доступний для розуміння тих співробітників, яким він адресований.

Загалом політика інформаційної безпеки повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців при впровадженні та використанні інформаційних систем і засобів захисту інформації, а також при здійсненні інформаційного обміну та виконанні операцій з обробки інформації. Крім того, з політики безпеки, якщо вона відноситься до певної технології та/або методології захисту інформації, повинні бути зрозумілі основні принципи роботи цієї технології. Важливою функцією політики безпеки є чітке розмежування відповідальностей в процедурах інформаційного обміну: всі зацікавлені особи повинні ясно усвідомлювати межу як своєї відповідальності, так і відповідальності інших учасників відповідних процедур і процесів. Також одним із завдань політики безпеки є захист не тільки інформації та інформаційних систем, а й захист самих користувачів (співробітників підприємства і його клієнтів і контрагентів).

Загальний життєвий цикл політики інформаційної безпеки включає в себе ряд основних кроків.

1) Проведення попереднього дослідження стану інформаційної безпеки.

2) Власне розробку політики безпеки.

3) Впровадження розроблених політик безпеки.

4) Аналіз дотримання вимог впровадженої політики безпеки та формулювання вимог щодо її подальшого вдосконалення (повернення до першого етапу, на новий цикл вдосконалення).

Цей цикл (рис. 3.8) може повторюватися кілька разів з метою вдосконалення організаційних заходів у сфері захисту інформації та усунення виявлених недоробок.

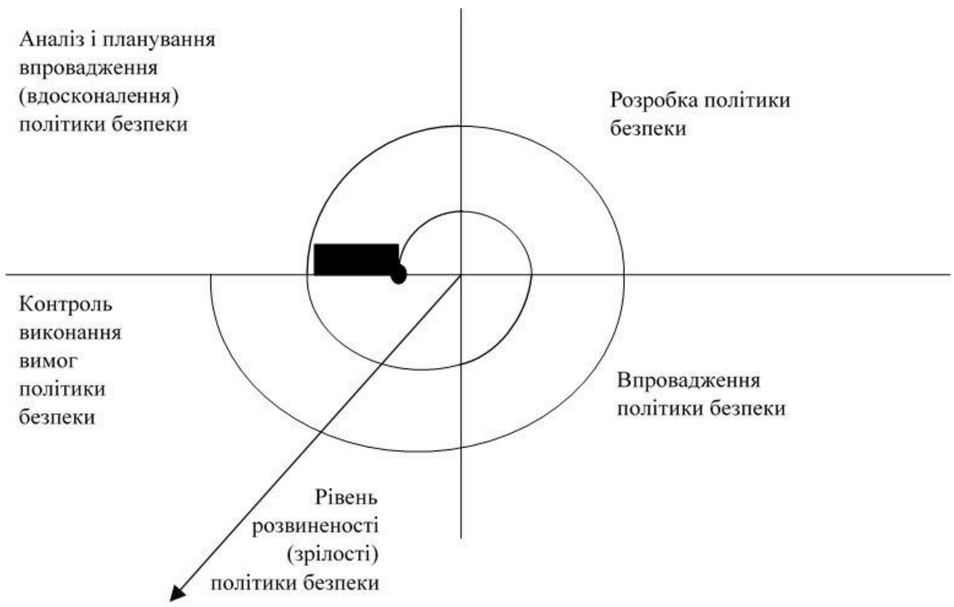

Рис. 3.8. Цикли розвитку і вдосконалення політики інформаційної безпеки підприємства

Політика інформаційної безпеки підприємства: верхній рівень.

Верхній рівень політики інформаційної безпеки, по суті, є декларацією з боку керівництва та/або власників компанії про важливість цілеспрямованої роботи з захисту інформаційних активів. Ця декларація служить основою для підвищення ефективності діяльності компанії у своєму основному напрямку. Крім того, вона спрямована на усунення різноманітних ризиків, які можуть призвести до фінансових збитків, негативно вплинути на репутацію компанії, а також викликати адміністративне чи кримінальне переслідування керівників та інші негативні наслідки.

Політика інформаційної безпеки на цьому рівні може визначати й описувати:

- власне рішення про здійснення цілеспрямованої систематичної діяльності щодо забезпечення інформаційної безпеки підприємства;
- перелік основних інформаційних ресурсів, таких як інформаційні системи, масиви даних, інформація про окремі факти та явища (конструкторських розробках, комерційних угодах, результатах НДДКР тощо), захист яких має найбільший пріоритет для всього підприємства;
- загальний підхід до розподілу відповідальності за забезпечення інформаційної безпеки всередині організації;
- необхідність для всього персоналу дотримуватися певних запобіжних заходів при роботі з інформацією та інформаційними системами, підвищувати свою кваліфікацію в даній області і усвідомлювати міру відповідальності за можливі порушення;
- відношення керівництва підприємства до фактів порушення вимог щодо забезпечення інформаційної безпеки та осіб, що чинять такі порушення, а також загальний підхід до їх переслідування в разі виявлення таких фактів.

Однією з основних задач політики інформаційної безпеки на верхньому рівні є визначення та демонстрація значущості захисту інформації як ключового фактора, що впливає на конкурентоздатність підприємства. Це включає здатність компанії досягати своїх цілей, а також, в деяких випадках, забезпечувати власне виживання та здатність продовжувати свою діяльність. Важливим елементом цього процесу є визначення пріоритетних напрямків бізнесу, відповідних інформаційних систем та потоків інформації, а також аналіз причинно-наслідкових зв'язків між можливими порушеннями конфіденційності або стабільності роботи інформаційних систем і негативним впливом на поточні бізнес-операції. Від цього залежить визначення ключових напрямків діяльності у сфері інформаційної безпеки. Особливо ця залежність є важливою для компаній, які:

- займаються т.зв. електронною комерцією або працюють у суміжних сферах (електронні платежі, Інтернет-реклама тощо);

- безпосередньо пов'язані з обігом (створенням, купівлею-продажем, охороною, оцінкою) об'єктів інтелектуальної власності і, зокрема, наукомістких технологій;
- безпосередньо пов'язані із обігом великих обсягів інформації, що становить таємницю інших осіб (банки, медичні установи, аудиторські компанії тощо).

При цьому робота над політикою інформаційної безпеки повинна включати в себе не тільки її початкову розробку, але й постійний моніторинг загроз, змін у зовнішньому середовищі для подальшого уточнення (або навіть повної переробки) політики відповідно до змінення умов роботи.

Політика інформаційної безпеки підприємства: середній рівень.

Політики інформаційної безпеки середнього рівня безпосередньо деталізують вимоги, завдання та правила, позначені в політиці верхнього рівня, і окремо описують основні сфери, в яких необхідне системне здійснення тих чи інших організаційних і/або технічних заходів.

Політика інформаційної безпеки середнього рівня повинна містити наступні основні розділи.

- Загальний опис тієї сфери діяльності (інформаційної технології, аспекту інформаційної системи, бізнес-процесів підприємства), на яку вона поширюється.
- Область застосування політики безпеки - перелік всіх осіб, організацій, інформаційних систем, до яких вона застосовується або які виключаються зі сфери її застосування.
- Безпосереднє відношення підприємства до даного аспекту інформаційних технологій та інформаційної безпеки - основна частина політики безпеки, що визначає конкретні правила, критерії та вимоги до процедур обігу інформації, елементів інформаційної інфраструктури, програмних і апаратних засобів тощо
- Розподіл ролей і функцій, необхідних для вирішення конкретних питань – закріплення за певними співробітниками (фахівцями, керівниками)

обов'язків з виконання необхідної роботи з метою вирішення завдань в рамках даної політики безпеки.

- Порядок вирішення питань , що виникають, – під час основних процедур вирішення з'являються труднощі у поточній роботі і прийняття рішень про можливі винятки з загальних правил, а також перелік осіб (підрозділів), відповідальних за безпосередню роботу з персоналом підприємства з питань, що належать до даної політики безпеки.

Одним із ключових етапів в розробці політики інформаційної безпеки та впровадженні відповідних заходів є групування інформаційних ресурсів, що містяться в компанії, відповідно до їх значимості та рівня конфіденційності. Цей процес передбачає класифікацію всіх інформаційних об'єктів (і пов'язаних з ними елементів інформаційної інфраструктури) компанії в п'ять або шість основних категорій, ґрунтуючись на їх важливості та рівні конфіденційності.

1. Критично важлива (абсолютно секретна) інформація – інформація, що вимагає особливих гарантій безпеки.
2. Важлива інформація (інформація, що становить комерційну таємницю) – інформація, яка використовується тільки всередині підприємства, порушення конфіденційності якої може завдати серйозної шкоди самому підприємству або його партнерам.
3. Значна (конфіденційна) інформація – інформація, призначена для використання обмеженим колом співробітників і керівників підприємства.
4. Персональна інформація – інформація про співробітників, що не підлягає розголошенню.
5. Інформація для внутрішнього використання – інформація для використання всередині підприємства, порушення конфіденційності якої не може завдати шкоди.
6. Інша інформація – відкрита інформація, конфіденційність якої не має особливого значення для діяльності підприємства.

Політика інформаційної безпеки підприємства: нижній рівень.

Цей рівень політики інформаційної безпеки включає документи, які служать як безпосередні інструкції та методики для щоденної роботи співробітників компанії. Ці документи стосуються конкретних сервісів, процедур і інформаційних систем. Основна мета створення такої організаційної документації полягає в забезпеченні детального та формалізованого опису всіх процедур і вимог, пов'язаних з захистом окремих елементів інформаційних систем, інформаційних потоків та баз даних. Важливим аспектом в розробці політики інформаційної безпеки є створення якомога більш комплексного набору організаційної документації, який включає:

- бланки типових заявок на надання доступу окремих співробітників до певних інформаційних ресурсів та інформаційних систем, а також регламенти надання такого доступу;
- регламенти (процедури) роботи з певними інформаційними і телекомунікаційними системами, програмним забезпеченням і базами даних;
- посадові обов'язки окремих категорій співробітників щодо забезпечення інформаційної безпеки, а також вимоги, що пред'являються до персоналу;
- типові договори з зовнішніми контрагентами, пов'язані з передачею або отриманням інформації, або основні вимоги, що пред'являються до таких договорів.

Процедурні документи, які стосуються надання доступу до ресурсів (таких як мережа Інтернет, корпоративне інформаційні системи і бази даних, апаратні засоби, засоби передачі інформації тощо) можуть включати як типові бланки заявок на надання доступу, так і опис основних процедур (регламенту) прийняття рішень про надання такого доступу та надання конкретних прав при роботі з інформаційними ресурсами, а також переліки критеріїв, необхідних для надання тих чи інших прав в інформаційних системах.

Процедури роботи з окремими інформаційними системами і/або модулями інформаційних систем (базами даних, модулями корпоративної ERP-системи, системами електронного документообігу тощо) можуть перераховувати всі основні вимоги, правила і обмеження, наприклад, заборона використовувати дискети для копіювання та перенесення інформації або обмеження, що накладаються на можливість віддаленого доступу до тих чи інших інформаційних сервісів. Вимоги і правила, пов'язані із забезпеченням інформаційної безпеки, можуть бути включені як в загальні інструкції по використанню інформаційних систем або регламенти здійснення бізнес-процесів, так і в оформлені у вигляді спеціальних інструкцій і пам'яток, що містять виключно вимоги і правила інформаційної безпеки.

Посадові обов'язки співробітників, що стосуються інформаційної безпеки, мають бути включені до їхніх посадових інструкцій. Крім того, в рамках політики безпеки може бути передбачено підписання додаткових договорів чи зобов'язань про нерозголошення інформації окремими категоріями працівників, як при прийомі на роботу, так і при звільненні. Також можуть бути введені додаткові вимоги до персоналу, що має доступ до особливої інформації чи систем, наприклад, відсутність судимості, наявність певних навичок чи сертифікації, проходження психологічної перевірки.

Політика безпеки стосовно зовнішніх контрагентів може включати стандартні форми та інструкції для укладення комерційних договорів з різними типами контрагентів і обміну інформацією з постачальниками, клієнтами, консультантами та іншими бізнес-партнерами. В цих політиках може бути визначено конкретні процедури обміну інформацією, умови забезпечення конфіденційності та заходи відповідальності за порушення умов договору будь-якою зі сторін.

У тих випадках, коли певна політика безпеки описує складну інформаційну систему і систему захисту інформації, призначену для виконання найбільш відповідальних операцій (таких як, наприклад, електронні грошові перекази), вона може бути розділена на дві складові:

- внутрішній регламент роботи підрозділів (груп, адміністраторів), що відповідають за виконання найбільш важливих адміністративних функцій (наприклад, видача та обслуговування електронних сертифікатів Інфраструктури публічних ключів);

- політику, яка безпосередньо відображає вимоги до користувачів і процесів, а також опису процедур роботи та взаємодії всіх учасників інформаційного обміну.

Основні Компоненти Плану Заходів:

1. Оцінка Ризиків

Аналіз поточного стану безпеки: Визначення слабких місць у системі.

Оцінка загроз: Ідентифікація потенційних зовнішніх та внутрішніх загроз.

2. Розробка Політики Безпеки

Створення документа політики безпеки: Включає принципи та стандарти, яких мають дотримуватися співробітники.

Правила доступу до даних: Встановлення рівнів доступу в залежності від ролей і обов'язків співробітників.

3. Технічні Заходи Захисту

Конфігурація мережевого обладнання: Налаштування файрволів, маршрутизаторів та комутаторів.

Шифрування даних: Використання стандартів шифрування для захисту даних, що передаються та зберігаються.

Захист серверів і баз даних: Застосування механізмів аутентифікації та шифрування на рівні серверів і баз даних.

Моніторинг та аудит системи: Встановлення систем моніторингу для виявлення несанкціонованого доступу.

4. Заходи Фізичного Захисту

Захист центрів обробки даних: Фізичні бар'єри, контроль доступу, системи відеонагляду.

5. Розвиток Компетенцій Персоналу

Тренінги з безпеки: Регулярні навчальні курси для персоналу щодо засад інформаційної безпеки.

Свідомість безпеки: Формування культури безпеки серед працівників.

6. Розробка Плану Відновлення після Інцидентів

Розробка процедур реагування на інциденти: План дій у випадку виявлення безпекових порушень.

Відновлення системи: Процедури швидкого відновлення роботи системи після інцидентів.

У сучасному світі, де інформація стала однією з найцінніших активів, забезпечення інформаційної безпеки стає критичним завданням для будь-якої організації, особливо для банківських установ. Банківські автоматизовані системи містять у собі обширний обсяг конфіденційних даних, від фінансових транзакцій до особистих інформаційних активів клієнтів. Збереження цих даних в цілісності та захист їх від ризиків та загроз - це завдання, на виконання якого впливає не тільки фінансовий успіх банку, але й довіра клієнтів.

Цей розділ призначений для розгляду та розробки основних принципів та стратегій, що допоможуть забезпечити інформаційну безпеку нашої банківської автоматизованої системи. Він включає в себе аналіз поточного стану безпеки, визначення цілей та принципів безпеки, розробку конкретних політик та процедур, план дій при інцидентах та моніторинг виконання.

Політика Безпеки є фундаментальним документом, який визначає наше зобов'язання перед клієнтами, партнерами та регуляторами щодо забезпечення конфіденційності, цілісності та доступності даних. Ця політика розробляється з урахуванням технічних аспектів захисту та враховує сучасні тенденції та загрози інформаційної безпеки.

Докладніше кроки та заходи, які включаються в процес розробки Політики Безпеки, а також важливі аспекти забезпечення інформаційної безпеки нашої банківської автоматизованої системи в додатку Б. Безпека - це не статичний процес, і вона вимагає постійної уваги та оновлення відповідно до змінюючихся загроз та вимог.

Технічні заходи захисту в інформаційній безпеці є критично важливими для гарантування цілісності, конфіденційності та доступності даних у будь-якій організації. Цей аспект охоплює широкий спектр дій, від налаштування мережевого обладнання до моніторингу та аудиту системи.

Починаючи з конфігурації мережевого обладнання, основною задачею є створення міцного першого ряду захисту. Файрволи, маршрутизатори та комутатори повинні бути налаштовані таким чином, щоб вони могли ефективно фільтрувати небажаний трафік, блокувати підозрілі запити та забезпечувати захист від відомих загроз. Наприклад, файрвол може бути налаштований так, щоб блокувати доступ до певних IP-адрес або портів, які відомі як часто використовувані для кібератак.

Шифрування даних є ще однією важливою частиною технічних заходів безпеки. Використання стандартів шифрування, таких як AES (Advanced Encryption Standard), дозволяє захистити дані під час їх передачі через мережу, а також під час зберігання. Це гарантує, що навіть у випадку витоку або несанкціонованого доступу, конфіденційні дані залишаються незрозумілими та захищеними.

Захист серверів і баз даних також є ключовим. Це включає в себе використання міцних паролів, механізмів аутентифікації на основі двофакторної перевірки, а також шифрування баз даних. Наприклад, застосування TLS (Transport Layer Security) для захисту з'єднань між клієнтами та серверами баз даних може значно знизити ризик перехоплення або маніпулювання даними.

Моніторинг та аудит системи є невід'ємною частиною забезпечення безпеки. Системи моніторингу, такі як IDS (системи виявлення вторгнень) та IPS (системи запобігання вторгнень), допомагають виявляти та реагувати на аномалії у поведінці мережі, які можуть вказувати на кібератаки. Журнали аудиту важливі для підтримки обліку дій користувачів та забезпечення можливості відстеження та аналізу подій після виявлення інцидентів безпеки.

Загалом, технічні заходи захисту є фундаментом для захисту інформаційних активів організації. Вони допомагають забезпечити, що дані залишаються безпечними від широкого спектра загроз, від хакерських атак до внутрішніх загроз, і відіграють важливу роль у загальній стратегії інформаційної безпеки.

Організація режиму секретності в установах і на підприємствах

Організація режиму секретності в установах і на підприємствах ґрунтується на вимогах законодавства, що стосується питань державної таємниці, і відповідних підзаконних актів. Відповідно до діючих норм до державної таємниці може бути віднесена інформація, що стосується обороноздатності країни, її економіки, міжнародних відносин, державної безпеки та охорони правопорядку (в тому числі відомості про методи та засоби захисту секретної інформації, а також про державні програми і заходи в області захисту державної таємниці); в законодавстві також спеціально уточнюються області діяльності, інформація про які не може бути віднесена до державної таємниці. Віднесення конкретної інформації до державної таємниці здійснюється рішенням спеціально призначених посадових осіб, а загальний Перелік відомостей, віднесених до державної таємниці, затверджується Президентом і підлягає обов'язковому опублікуванню. Для відомостей, що становлять державну таємницю, встановлюються три ступені секретності: "особливої важливості", "цілком таємно" та "таємно", а носії таких відомостей (документи) повинні мати відповідні реквізити.

Основним елементом організації режиму секретності є допуск посадових осіб і громадян до відомостей, що становлять державну таємницю. Він передбачає виконання керівництвом підприємства і підрозділів із захисту державної таємниці (у взаємодії з уповноваженими правоохоронними органами) наступних основних заходів [50].

- Ознайомлення посадових осіб і громадян з нормами законодавства, які передбачають відповідальність за порушення вимог.
- Отримання згоди на тимчасові обмеження їх прав відповідно до законодавства.
- Отримання згоди на проведення щодо них перевірочних заходів.
- Прийняття рішення про допуск до відомостей, що становлять державну таємницю.
- Висновок щодо осіб, які отримали допуск, що відображає взаємні

зобов'язання таких осіб і адміністрації підприємства (в т.ч. зобов'язання таких осіб перед державою з нерозповсюдження довірених їм відомостей, що становлять державну таємницю).

Крім віднесення відомостей до державної таємниці та допуску посадових осіб і громадян до засекречених відомостей, важливим елементом системи забезпечення режиму секретності є організація інформаційного обміну між підприємствами при спільному виконанні робіт. Зокрема, передача засекречених відомостей від одного підприємства до іншого повинна проводитися з дозволу уповноваженого державного органу, договір на виконання робіт повинен передбачати зобов'язання сторін щодо забезпечення схоронності відомостей, а замовник робіт повинен контролювати виконання нормативних вимог контрагентами за такими договорами (наявність ліцензій, оформлення допуску співробітників і т.п.) і вживати необхідних заходів у разі виявлення порушень. Також важливим елементом забезпечення режиму секретності є організація передачі відомостей, що становлять державну таємницю, іншим державам (в тому числі ознайомлення з такими відомостями і надання можливості доступу до них).

Політика використання комунікаційних засобів може визначати межі використання технологій, що дозволяють підключити комп'ютери та інформаційні системи підприємства до інформаційних систем і комунікаційних каналів за його межами.

Зокрема, така політика може вводити певні обмеження на використання модемів для телефонних ліній, пристроїв, що використовують сучасні бездротові технології, такі, як GSM (GPRS), Wi-Fi, передача даних в мережах стандарту CDMA і т.п.

Політика використання мобільних апаратних засобів може ставитися до різних пристроїв, таким як мобільні ПК, КПК (PDA), переносні пристрої зберігання інформації (дискети, USB-flash, карти пам'яті, що підключаються жорсткі диски і т.п.). Вона може відображати загальне ставлення підприємства до використання співробітниками таких пристроїв, визначати вимоги і встановлювати конкретні області, в яких їх використання допустимо. Також можуть встановлюватися додаткові загальні вимоги до стаціонарного обладнання з метою обмеження підключення до них мобільних комп'ютерів і засобів передачі даних [50].

3.4 Оцінювання ефективності запропонованих рекомендацій

У цій роботі я зосереджую увагу на критичній темі інформаційної безпеки в банківських автоматизованих системах. Важливість інформаційної безпеки у сучасному цифровому світі не може бути переоцінена, особливо в контексті фінансової індустрії, де захист даних та транзакцій має вирішальне значення. Зі зростанням кіберзагроз та зломів даних, банки та інші фінансові інститути постійно шукають способи зміцнення своїх систем інформаційної безпеки.

Ми розглянуи комплексний підхід до інформаційної безпеки, який охоплює розробку, впровадження, тестування, оцінку та удосконалення заходів безпеки. Робота включає детальний аналіз існуючих загроз, вразливостей та методів їх запобігання, а також практичні аспекти впровадження цих заходів у банківських системах.

Ключовою частиною роботи є вивчення ефективності існуючих заходів безпеки та виявлення потенційних слабких місць. Це включає розробку стратегій тестування, оцінки та удосконалення заходів безпеки, які спрямовані на підвищення їхньої ефективності та адаптивності до змінюючихся умов та загроз.

Робота надає цінні висновки та рекомендації, які можуть бути використані банками та іншими фінансовими установами для зміцнення їх систем інформаційної безпеки. Вона спрямована на забезпечення глибокого розуміння важливості інформаційної безпеки та надає практичний інструментарій для її підтримки та розвитку.

В рамках нашого комплексного підходу до забезпечення інформаційної безпеки, ми провели всебічне тестування реалізованих заходів у банківській автоматизованій системі. Тестування охоплювало як технічні, так і фізичні аспекти безпеки, що дозволило нам отримати цілісне уявлення про стан наших захисних механізмів.

Почали ми з технічного тестування, де основним інструментом стало пенетраційне тестування. Цей метод виявився особливо корисним для визначення потенційних слабких місць в наших мережевих протоколах та системах захисту від несанкціонованого доступу. Результати показали, що наші файрволи та системи виявлення вторгнень діють ефективно, але були виявлені певні недоліки в конфігурації шифрування даних, що потребує додаткового перегляду.

Далі ми зосередились на фізичному тестуванні, провівши ряд контрольних інспекцій та симуляцій несанкціонованого доступу. Фізичні заходи безпеки, такі як системи контролю доступу та відеонагляд, продемонстрували високу ефективність, забезпечуючи надійний захист від фізичного вторгнення. Однак, було виявлено, що деякі зони не піддаються достатньому відеонагляду, що вимагає розширення системи камер спостереження.

Загалом, проведене тестування виявило, що більшість реалізованих заходів інформаційної безпеки є ефективними та забезпечують міцний захист наших систем. Водночас, отримані результати вказують на необхідність удосконалення деяких аспектів, зокрема, шифрування даних та охоплення відеонаглядом, що буде нашим пріоритетом у подальших діях із підвищення рівня безпеки.

Оцінка базувалася на аналізі результатів тестувань, звітів про інциденти, а також відгуків персоналу.

Результати пенетраційного тестування та інших форм технічного аналізу підтвердили, що більшість наших систем захисту працюють ефективно. Особливо добре себе зарекомендували системи контролю доступу та файрволи. Однак, аналіз показав, що шифрування даних вимагає додаткових покращень, щоб відповідати сучасним стандартам безпеки.

Що стосується фізичних заходів безпеки, то вони в цілому виявилися досить надійними. Проте, було виявлено, що деякі зони не мають достатнього відеонагляду, що може створювати потенційні ризики.

Зібрані звіти про інциденти та відгуки персоналу також надали важливу інформацію. Вони підтвердили, що співробітники задоволені рівнем захисту, який надають реалізовані заходи, хоча й висловили деякі побажання щодо зручності використання систем.

На основі цих даних я розробив таблицю 3.3 для оцінки ефективності заходів безпеки:

Таблиця 3.3

Оцінка ефективності заходів безпеки

Заходи Безпеки	**Рівень Ефективності**	**Зауваження**
Файрволи	Високий	-
Контроль доступу	Високий	-
Шифрування даних	Середній	Вимагає покращень
Відеонагляд	Задовільний	Недостатнє охоплення зон

У цілому, наша оцінка показує, що більшість заходів є ефективними, проте виокремлені напрямки потребують додаткових вдосконалень. Це допоможе нам в подальшому зосередитись на поліпшенні тих аспектів нашої системи безпеки, які потребують підвищення ефективності.

У третьому розділі нашого плану (Додаток А) зосереджено на виявленні та аналізі недоліків в реалізованих заходах інформаційної безпеки. Цей процес включав детальний аналіз результатів тестування, оцінку відповідності до встановлених стандартів безпеки, а також залучення зовнішніх експертів для незалежного аудиту.

В ході аналізу я виявив декілька ключових недоліків. Перш за все, система шифрування даних виявилася недостатньо сучасною та ефективною, особливо в контексті захисту від розширених кіберзагроз. Другий важливий аспект стосується системи відеонагляду - деякі критичні зони в наших фізичних просторах залишалися без належного моніторингу.

Залучення зовнішніх експертів допомогло виявити додаткові слабкі місця у нашій системі, зокрема в області аутентифікації користувачів та моніторингу мережевих транзакцій. Це вказувало на потребу в більш глибокому перегляді та удосконаленні цих аспектів.

Нижче представлена таблиця 3.4 з виявленими недоліками та їх оцінкою:

Таблиця 3.4

Оцінка недоліків

Недоліки	**Оцінка Серйозності**	**Коментарі**
Шифрування даних	Висока	Потребує оновлення до сучасних стандартів
Відеонагляд	Середня	Недостатнє покриття деяких критичних зон
Аутентифікація користувачів	Середня	Необхідність удосконалення системи
Моніторинг мережевих транзакцій	Середня	Вимагає покращення аналітичних можливостей

Цей розділ плану допоміг нам виявити важливі області для покращення і створити основу для розробки плану удосконалення. Результати аналізу будуть використані для наступних кроків, спрямованих на підвищення загального рівня інформаційної безпеки в нашій організації.

Перш за все, я розробив стратегію оновлення системи шифрування даних. Це означає впровадження сучасних криптографічних рішень, які відповідають найвищим стандартам безпеки. Це не тільки зміцнить захист наших даних, але й забезпечить кращу відповідність до міжнародних регулятивних вимог.

Другим важливим елементом плану є покращення системи відеонагляду. Це включає в себе розширення охоплення камерами важливих зон, а також впровадження більш розвинених систем аналізу відеоданих.

Ще однією критичною областю для удосконалення є система аутентифікації користувачів. Ми плануємо впровадити більш складні механізми аутентифікації, такі як двофакторна аутентифікація та біометричні технології, що значно підвищить безпеку користувацьких акаунтів.

Останнім аспектом нашого плану є покращення моніторингу мережевих транзакцій. Це включає в себе впровадження більш складних систем моніторингу та аналізу трафіку, які дозволять нам краще виявляти та запобігати кібератакам.

Ці кроки будуть реалізовані відповідно до затвердженого графіка та бюджету, забезпечуючи таким чином поступове, але впевнене підвищення рівня інформаційної безпеки в нашій організації. Ми також встановимо чіткі критерії для вимірювання успіху цих ініціатив.

Висновок до розділу 3. Сучасні банківські системи залежать від складної мережевої інфраструктури, яка вимагає ретельного підходу до безпеки. Це включає захист від зовнішніх та внутрішніх загроз, використання передових технологій та постійне оновлення безпекових практик. Загрози мережевій безпеці постійно еволюціонують, включаючи такі вектори атак як DDoS, фішинг, віруси, шпигунське програмне забезпечення, а також внутрішні загрози. Розуміння цих загроз та їх потенційних наслідків є важливим для ефективного управління ризиками.

У цьому розділі ми розглянули комплексний підхід до забезпечення інформаційної безпеки в організації, охоплюючи від оцінки ризиків до розробки плану відновлення після інцидентів. Важливість проведення глибокого аналізу поточного стану безпеки та ідентифікації потенційних загроз не може бути переоцінена, адже саме це формує основу для всіх подальших заходів. Розробка політики безпеки, яка включає чіткі принципи та стандарти поведінки співробітників, є критичною для створення безпечного робочого середовища.

Технічні заходи захисту, такі як конфігурація мережевого обладнання та шифрування даних, грають вирішальну роль у захисті інформаційних активів від зовнішніх та внутрішніх загроз. Разом із цим, заходи фізичного захисту, включаючи захист центрів обробки даних та систем відеонагляду, забезпечують необхідний рівень безпеки для фізичних активів організації.

Розвиток компетенцій персоналу через тренінги та освітні кампанії важливий для формування культури безпеки, де кожен співробітник усвідомлює свою роль у захисті інформації. Нарешті, розробка ефективного плану відновлення після інцидентів гарантує, що організація зможе швидко відновити свою діяльність після можливих порушень безпеки, мінімізуючи втрати та наслідки.

Загалом, розробка комплексного плану заходів забезпечення інформаційної безпеки вимагає інтегрованого підходу, який враховує як технічні, так і людські аспекти, а також потребу в постійному оновленні та адаптації до змінюваних умов та загроз. Тільки за цих умов можливо досягнути високого рівня захисту інформаційних активів організації.

Використання VPN, мережевих фільтрів, брандмауерів та інших технологій є критично важливим для забезпечення конфіденційності та цілісності даних. Це також включає реалізацію сильних механізмів аутентифікації та шифрування. Людський фактор часто є найслабшою ланкою в системі безпеки. Регулярне навчання персоналу та підвищення обізнаності щодо кібербезпеки є невід'ємною частиною захисту інформації.

Аналіз реальних випадків допомагає зрозуміти практичне застосування теорій безпеки, оцінити ефективність існуючих заходів та розробити стратегії для покращення. Сектор банківської безпеки вимагає постійного оновлення та адаптації до змін у технологіях та методах кібератак. Це вимагає гнучкості, передбачливості та використання передових практик.

ВИСНОВКИ

Проведено дослідження, в якому було проаналізовано основні основні дослідження у підвищенні ефективності інформаційної безпеки в АСУ.

Огляд показав, що головні виклики полягають у забезпеченні захисту від кібератак, управлінні внутрішніми ризиками, включаючи помилки співробітників та умисні дії зі шкоди, а також у захисті від фізичних загроз і загроз, пов'язаних з природними катастрофами. Ці виклики вимагають комплексного підходу, що включає технічні, організаційні та фізичні заходи безпеки. Одним із самих важливих викликів у звязку з розвитком інформаційних технологій є технічні заходи зазисту інформації в АСУ.

Встановлено, що сьогодні державвами, організаціями та підприємствами активно використовуються сучасні технології для забезпечення безпеки своїх систем, але водночас стикаються з викликами, пов'язаними зі швидким розвитком кіберзагроз та постійною потребою в оновленні своїх захисних систем.

Враховуючи виявлені загрози та ризики, рекомендується продовжувати інвестування у розвиток інформаційної безпеки АСУ, зосереджуючись на оновленні захисного програмного забезпечення, розвитку навичок персоналу в області кібербезпеки та впровадженні ефективних стратегій реагування на інциденти. Також важливо підкреслити необхідність регулярного аудиту та оцінки ризиків, щоб вчасно виявляти нові загрози та адаптувати заходи безпеки до змінних умов.

Визначено, що одним з головних викликів є розвиток квантових комп'ютерів. Квантові комп'ютери мають потенціал ламати сучасні криптографічні алгоритми АСУ, зокрема асиметричні шифри, такі як RSA та ECC (еліптичні криві). Це створює потребу у розвитку квантово-стійких алгоритмів, які можуть витримати атаки з використанням квантових технологій.

Крім того, зростає необхідність у стандартизації криптографічних алгоритмів та протоколів. Забезпечення сумісності різних систем та пристроїв, які використовують криптографію, є важливим для гарантування безперебійної та безпечної роботи глобальних мережевих інфраструктур.

Однією з головних перспектив є також розвиток квантово-стійкої криптографії. Оскільки загроза від квантових комп'ютерів стає дедалі більш реальною, необхідність у розробці нових криптографічних систем, які можуть витримати квантові атаки, стає нагальною.

Розроблено та детально описано комплексний план удосконалення інформаційної безпеки для банківських автоматизованих систем. Через проведене глибоке дослідження, аналіз та тестування, вдалося ідентифікувати ключові аспекти, які потребують удосконалення – оновлення системи шифрування даних, покращення системи відеонагляду, вдосконалення системи аутентифікації користувачів, та покращення моніторингу мережевих транзакцій.

Розроблений план удосконалення відображає сучасні вимоги до інформаційної безпеки та орієнтується на використання передових технологій та методів для забезпечення надійного захисту даних та систем. Особлива увага була приділена не тільки технічним аспектам безпеки, але й залученню персоналу до процесу постійного поліпшення заходів безпеки.

Реалізація цього плану не тільки зміцнить захист банківських систем, але й забезпечить більшу довіру та безпеку для клієнтів та співробітників. Важливо підкреслити, що інформаційна безпека є неперервним процесом, який вимагає регулярного перегляду та оновлення, щоб відповідати зростаючим загрозам у цифровому світі. Таким чином, розроблений план удосконалення стане фундаментом для тривалого процесу захисту та управління ризиками в сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Євсєєв С. Оцінка забезпечення безперервності бізнес-процесів в організаціях банківського сектора на основі синергетичного підходу, ч. 2 / С. Євсєєв, Ю. Хохлачова, О. Король. // Сучасна спеціальна техніка. Науковопрактичний журнал. – 2017. – №2. – С. 10–17.
2. Грищук Р. В. Основи кібернетичної безпеки: Монографія / Р. В. Грищук, Ю. Г. Даник. – Житомир: ЖНАЕУ, 2016.
3. А.І. Пилипенко, В.В. Шестаков "Захист інформації в комп'ютерних системах" – 2012р.
4. J.R. Vacca & T.J. Mullen "Computer and Information Security Handbook" – 2018р.
5. Євсєєв С. П. Аналіз захисту в національній системі масових електронних платежів / С. П. Євсєєв. // Інформаційна безпека. – 2014. – №3. – С. 15.
6. Юдін О. К. Інформаційна безпека. Нормативно-правове забезпечення / О. К. Юдін. – Київ: НАУ, 2011. – 639 с.
7. W. Ten, G. Manimaran, and C.-C. Liu,. Cybersecurity for criticalinfrastructures : Attack and defense modeling. IEEETrans. Syst., Man Cybern. A, vol. 40, no. 4, pp.853 – 865, 2010.
8. В. Горбунов "Кібербезпека: теорія і практика.навчальний посібник. Км– 2008р. 128 с.
9. Равенков П. В. Защита информации в банке: основные угрозы и борьба с ними [Електронний ресурс] / П. В. Равенков. – 2011. – Режим доступу до ресурсу: http://www.crmdaily.ru/novosti-rynka-crm/568-zashhita-informacii-vbanke-osnovnye-ugrozy-i-borba-s-nimi.html.
10. В.К. Омельченко, О.І. Чернишенко "Методи та засоби криптографічного захисту інформації" – 2011р.
11. Security of Internet Banking – A Comparative Study of Security Risks and Legal Protection in Internet Banking in Thailand and Germany [Online].Available:

http://www.thailawforum.com/articles/internet-banking-thailand.html. Acessed on: Des. 09, 2017.

12. Milov O.V. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / Milov O., Voitko A., Husarova I., 88 Domaskin O., Ivanchenko E., Ivanchenko I., Korol O., Kots H, Opirskyy I., FrazeFrazenko O.// Eastern-European Journal of Enterprise Technologies, 2019, v.9, N 2, pp. 56-68.

13. Simon Singh. Code book - the science of secrecy from ancient egypt to quantam cryptography. ark:/13960/t0sr45g2b. 2013 . 300 p.

14. William Stallings. Cryptography and Network Security. ark:/17942/t0sr56g7c – 2007p. 276 p.

15. Домарев В. В. Безпека інформаційних технологій. Методологія створення систем захисту / В. В. Домарев, Р. В. Климчук., 2013. – 688 с.

16. John Baichtal (March 3, 2008). "GeekDad Review: Hacking: The Art of Exploitation". Wired. Retrieved March 27, 2009.

17. Рижов О.О., Горбенко О.В. Інформаційна безпека: навчальний посібник – 2010р. 132 с.

18. Яковлєв В. В. Інформаційна безпека та захист інформації в корпоративних мережах: підручник. / В. В. Яковлєв, А. А. Корнієнко., 2002. – 328 с.

19. А. В. Барабанов, А. И. Лавров, А. С. Марков, И. А. Полотнянщиков. Дослідження атак типу «Міжсайтовий підробка запитів». Питання кібербезпеки. – 2016. – №5. – С. 43–50.

20. Erickson, Jon. Hacking: The Art of Exploitation. No Starch Press, 2003. https://www.amazon.com/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441

21. Hryshchuk R. Yevseiev S., Shmatko A. Construction methodology of information security system of banking information in automated banking systems : monograph . Vienna.: Premier Publishing s. r. o., 2018. – 284 p.

22. Романець Ю. В. Захист інформації в комп’ютерних системах і мережах / Ю. В. Романець, П. А. Тимофєєв, В. Ф. Шаньгина. – 2001: Радіо та зв'язок, 2001. – 376 с.

23. Венбо М. Сучасна криптографія: теорія і практика. Київ: Видавничий дім «Вільямс», 2005. – 768 с.

24. Бучик С. С. Методика експертного оцінювання функціональніх профілів загроза державних інформаційних ресурсів. Відкриті інформаційні технології. – 2015. – №70. – С. 271–280.

25. Домарєв Д., Прокопенко С. Методика оцінювання захищеності інформаційних систем за допомогою СУІБ “Матриця”. Захист інформації. – 2013. – №1. – С. 80–86. URL: https://doi.org/10.18372/2410-7840.15.4223

26. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень / Р. В. Грищук. – Житомир: Рута, 2010.

27. Бучик С. С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів/ Захист інформації. – 2016. – №1. – С. 81–89.

28. Яковлєв В. В. Інформаційна безпека та захист інформації в корпоративних мережах / В. В. Яковлєв, А. А. Корнієнко., 2002. – 328 с.

29. Bank of Thailand, BOT (2011): Law and regulation: online: http://www.bot.or.th/ENGLISH/LAWSANDREGULATIONS/Pages/default2.aspx, access date: 24.01.2011.

30. Bundesamt für Sicherheit in der Informationstechnik (BSI)(2011), Internet Banking, online: https://www.bsi-fuer-buerger.de/cln_030/BSIFB/DE/SicherheitImNetz/OnlineBanking/onlinebanking_node.html, acess date 1.02.2011.

31. Bundesamt für Sicherheit in der Informationstechnik (BSI)(2011), Danger and risks from online banking, online: https://www.bsi-fuer-buerger.de/cln_030/BSIFB/DE/SicherheitImNetz/OnlineBanking/GefahrenUndSicher

heitsrisiken/gefahren_sicherheitsrisiken_node.html, access date: 25.01.201. URL: http://www.thailawforum.com/articles/internet-banking-thailand.html

32. Larpsiri, R., Rotchanakitumnaui, S., Chairakeo, S. and Speece, M. (2002), The impact of Internet banking on Thai consumer perception, paper presented at the Conference of Marketing Communication Strategies in a Changing Global Environment, Hong Kong.

33. Lee, M.K. & Turban, E. (2001): A trust model for consumer Internet shopping, in International Journal of Electronic Commerce, Vol. 6, No. 1, pp. 75-91.

34. Rotchanakitumnuai, S., Chairakeo, S., Larpsiri, R. and Speece, M. (2003): Retail Banking consumer perception toward Thai Internet Banking, paper presented in Bangkok at 8th International Conferrence on marketing and development, Bangkok, 4-7 January 2003.

35. Chitak V.V., Usmanov Yu.I. International and national legal analysis of the state of information security of Ukraine in conditions of armed conflict. Науковий вісник Ужгородського Національного Університету, 2023. Pp. 271-278. https://doi.org/10.24144/2307-3322.2022.76.2.43

36. Архипов О. Є, Луценко В. М., Худяков В. О. Захист інформації в телекомунікаційних мережах та системах зв’язку: навч. посіб. - К.: Політехніка, 2003 – 38 с.

37. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

38. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення». URL: https://tzi.com.ua/downloads/1.1-005-07.pdf

39. НД ТЗІ 3.1-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи». URL: https://tzi.com.ua/downloads/3.1-001-07.pdf

40. НД ТЗІ 3.3-001-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок

розроблення та впровадження заходів із захисту інформації». URL: https://tzi.com.ua/downloads/3.3-001-07.pdf

41. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення». URL: https://tzi.com.ua/downloads/2.1-002-07.pdf

42. Наказ Адміністрації Держспецзв'язку та Держспоживстандарту України від 25.04.2007 р. № 75/91. [Електронний ресурс] – Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/z0498-07#Text

43. Sira, O., & Katkova, T. (2017). Formation of securities portfolio under conditions of uncertainty. Eastern-European Journal of Enterprise Technologies, 1(4 (85), 49–55. URL: https://doi.org/10.15587/1729-4061.2017.92283

44. Connor, G., Goldberg, L. R., Korajczyk, R. A. Portfolio Risk Analysis. Princeton University Press, 354. 2010. URL: https://doi.org/10.1515/9781400835294

45. Read, C. The Portfolio Theorists: von Neumann, Savage, Arrow and Markowitz. Springer, 240. 2012. URL: https://doi.org/10.1057/9780230362307

46. Raskin, L., Sira, O. Method of solving fuzzy problems of mathematical programming. Eastern-European Journal of Enterprise Technologies, 5 (4 (83)), 23–28. 2016. URL: https://doi.org/10.15587/1729-4061.2016.81292

47. Raskin, L., Sira, O. Method of solving fuzzy problems of mathematical programming. Eastern-European Journal of Enterprise Technologies, 5 (4 (83)), 23–28. 2016. URL: https://doi.org/10.15587/1729-4061.2016.81292

48. Read, C. The Early Years of John von Neumann and Oskar Morgenstern. In: The Portfolio Theorists. Great Minds in Finance. Palgrave Macmillan, London. 2012 URL: https://doi.org/10.1057/9780230362307_3

49. R. E. Bellman, L. A. Zadeh. Decision-Making in a Fuzzy Environment. Published Online. Vol. 17, No. 4. URL: https://doi.org/10.1287/mnsc.17.4.B141

50. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с

51. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.

52. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с

ДОДАТКИ

Додаток А

План Удосконалення Інформаційної Безпеки

1. Оновлення Системи Шифрування Даних

- **Мета:** Впровадження сучасних криптографічних рішень для забезпечення відповідності до міжнародних стандартів безпеки.
- **Кроки:**
  - Вибір нових криптографічних алгоритмів та протоколів.
  - Інтеграція вибраних рішень в існуючу систему.
  - Тестування та валідація нової системи шифрування.
- **Терміни:** Запуск – 1 квартал 2024 року; Завершення – 3 квартал 2024 року.

2. Покращення Системи Відеонагляду

- **Мета:** Розширення охоплення камерами важливих зон та впровадження систем аналізу відеоданих.
- **Кроки**
  - Ідентифікація зон з недостатнім відеонаглядом.
  - Встановлення додаткових камер.
  - Інтеграція системи аналізу відеоданих.
- **Терміни:** Запуск – 2 квартал 2024 року; Завершення – 4 квартал 2024 року.

3. Вдосконалення Системи Аутентифікації Користувачів

- **Мета:** Впровадження більш складних механізмів аутентифікації для забезпечення безпеки користувацьких акаунтів.
- **Кроки**
  - Розробка та впровадження двофакторної аутентифікації.

- Інтеграція біометричних технологій.

- **Терміни:** Запуск – 3 квартал 2024 року; Завершення – 1 квартал 2025 року.

4. Покращення Моніторингу Мережевих Транзакцій

- **Мета:** Впровадження більш складних систем моніторингу для кращого виявлення та запобігання кібератакам.

- **Кроки**

  - Вибір та встановлення розширених систем моніторингу трафіку.

  - Інтеграція аналітичних інструментів для аналізу даних транзакцій.

- **Терміни:** Запуск – 4 квартал 2024 року; Завершення – 2 квартал 2025 року.

Цей план удосконалення передбачає поетапне впровадження нових технологій та покращень у сфері інформаційної безпеки. Він буде регулярно переглядатися та оновлюватися для забезпечення актуальності та ефективності впроваджених заходів.

Додаток Б

Політика Безпеки для Банківської Автоматизованої Системи

Крок 1: Аналіз поточного стану безпеки

1.1 Огляд Безпеки

На цьому етапі проводиться всебічний аналіз поточного стану безпеки банківської автоматизованої системи. Включає в себе перевірку фізичних та логічних заходів безпеки, політик доступу, процедур реагування на інциденти та рівень обізнаності персоналу.

1.2 Виявлення слабких місць

Під час аналізу визначаються слабкі місця та потенційні вразливості в системі, що можуть стати воротами для витоку даних або інших безпекових інцидентів.

Крок 2: Визначення цілей та принципів безпеки

2.1 Основні цілі безпеки

Основними цілями безпеки є забезпечення конфіденційності, цілісності та доступності даних та інформаційних активів. Це визначається як найважливіші аспекти безпеки для нашої банківської системи.

2.2 Принципи безпеки

Ми керуємося принципами безпеки, які включають в себе принцип мінімізації прав доступу, що передбачає обмеження прав доступу до системи та даних відповідно до ролей та потреб користувачів. Також, ми використовуємо принцип обміну ключами та шифрування даних для забезпечення їх конфіденційності та цілісності.

Крок 3: Розробка політик та процедур

3.1 Політика доступу

Ми встановлюємо політику доступу, яка чітко визначає права доступу користувачів до системи та даних відповідно до їхніх ролей та потреб. Політика включає в себе процедури аутентифікації та авторизації.

3.2 Процедури аутентифікації

Ми розробляємо процедури аутентифікації, які забезпечують перевірку легітимності користувачів під час входу в систему. Це включає в себе використання паролів, біометричних даних та інших методів ідентифікації.

3.3 Ведення журналів подій

Ми встановлюємо процедури ведення журналів подій для моніторингу та відстеження активності користувачів та подій в системі. Це допомагає виявляти та реагувати на потенційні інциденти безпеки.

Крок 4: План дій при інцидентах

4.1 Виявлення інцидентів

Ми розробляємо процедури для виявлення інцидентів безпеки, включаючи моніторинг мережевої активності та поведінки користувачів.

4.2 Реагування на інциденти

Ми встановлюємо план дій для реагування на інциденти безпеки, включаючи ізоляцію та виправлення вразливостей. Важливо швидко та ефективно реагувати на будь-які потенційні загрози.

Крок 5: Аудит та перевірка виконання

5.1 Аудит безпеки

Ми проводимо регулярний аудит системи та безпеки для виявлення вразливостей та дотримання політик безпеки. Аудит включає в себе перевірку конфігурацій системи, доступ до даних та відповідність політикам.

Ми підтримуємо постійне оновлення Політики Безпеки відповідно до змінюючихся загроз та технічних вимог. Регулярне оновлення дозволяє нам залишатися впереду в галузі інформаційної безпеки.

Ця політика безпеки є невід'ємною частиною стратегії забезпечення інформаційної безпеки та відображає зобов'язання перед клієнтами та партнерами щодо збереження конфіденційності, цілісності та доступності їх даних.