Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студентки *Агашкової Катерини Олегівни*

академічної групи *гр. 125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи АТ КБ «Dniprobank*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н проф. Кагадій Т.С.	90	відмінно	
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.	90	відмінно	
економічний	к. е. н., доц. Пілова Д.П.	92	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.	95	відмінно	

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студентці *Агашковій К.О.* **академічної групи** *125*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи АТ КБ «Dniprobank*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с

Розділ	Зміст	Термін виконання
1	Проаналізувати нормативно-правову базу та підстави для створення КСЗІ та розробки політики безпеки.	06.05.2022
2	Виконати обстеження середовищ функціонування об'єкта інформаційної діяльності. Розробити моделі загроз та порушника безпеки інформації, проаналізувати ризики та сформувати основні положення політики безпеки інформації.	19.05.2022
3	Розрахувати економічну доцільність впровадження політики безпеки.	02.06.2022

Завдання видано _____ Кагадій Т.С
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 10.01.2022

Дата подання до екзаменаційної комісії: 09.06.2022

Прийнято до виконання _____ Агашкова К.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 8 схем., 27 табл., 11 додатків, 16 джерел.

Об'єкт дослідження: ІТС АТ КБ «Dniprobank».

Предмет дослідження: політика безпеки інформації інформаційно-телекомунікаційної системи АТ КБ «Dniprobank».

Мета проєкту: забезпечення достатнього рівня захищеності інформації в інформаційно-телекомунікаційній системі АТ КБ «Dniprobank».

Методи розробки: спостереження, аналіз, порівняння, опис.

У першому розділі кваліфікаційної роботи проведено аналіз нормативно-правової бази та підстав для створення КСЗІ та розробки політики безпеки.

У другому розділі виконано обстеження на ОІД, розглянуто загальні відомості про відділення комерційного банку, його організаційну структуру, аналіз середовища функціонування ОІД, класифікована інформація, що обробляється у інформаційно-телекомунікаційній системі та наведено характеристику компонентів системи. Також розроблено моделі загроз та порушника безпеки інформації, проаналізовані ризики для інформації і сформовані основні положення політики безпеки інформації.

У третьому розділі визначено економічну доцільність впровадження політики безпеки. Були проведені розрахунки поточних витрат на розробку політики безпеки, капітальних витрат, експлуатаційних витрат та оцінка можливого збитку від атаки.

Практичне значення роботи полягає у забезпеченні достатнього рівня захисту інформації об’єкта інформаційної діяльності за рахунок аналізу вразливостей та розробки політики безпеки.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, АКТ ОБСТЕЖЕННЯ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, АНАЛІЗ РИЗИКІВ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ, ПОКАЗНИК ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ.

ABSTRACT

An Explanatory note: 81 p., 8 pic. 27 tables, 11 applications, 16 sources.

The object of research is information security policy of information and telecommunication system of JSC CB "Dniprobank"

The purpose of the project is to ensure a sufficient level of information security in the information and telecommunication system of JSC CB "Dniprobank". The subject of research is information security policy of information and telecommunication system of JSC CB "Dniprobank".

The first chapter of the qualification work provides a general review and analysis of the regulatory framework and the grounds for the creation of comprehensive information security system and security policy.

The second chapter contains an inspection report on the object of information activity, general information about the branch of a commercial bank, its organizational structure, analysis of the environment of the object of information activity, classified information processed in the information and telecommunications system and characteristics of system components. Models of threats and violators of information security are also developed, risks for information are analyzed and the main provisions of information security policy are formed.

The third chapter identifies the economic feasibility of implementing a security policy. Calculations of current security policy development costs, capital expenditures, operating costs, and an estimate of possible damage from the attack were made.

The practical significance of the work is to ensure a sufficient level of protection of information of the object of information activities through the analysis of vulnerabilities and the development of security policies.

INFORMATION SECURITY POLICY, INFORMATION SECURITY POLICY, THREAT ANALYSIS, RISK ASSESSMENT, ECONOMIC FEASIBILITY, ECONOMIC EFFICIENCY INDICATORS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

БД – база даних;

ЗУ – Закон України;

ІБ - інформаційна безпека;

ІзОД- інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

КЗЗ – комплекс засобів захисту;

НСД – несанкціонований доступ;

НД ТЗІ – нормативні документи технічного захисту інформації;

ОІД - об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ПБ – політика безпеки.

ЗМІСТ

ВСТУП

Об'єктом дослідження є ІТС АТ КБ «Dniprobank».

Предметом дослідження є політика безпеки інформації (далі – політика безпеки) інформаційно-телекомунікаційної системи АТ КБ «Dniprobank».

Метою проєкту є забезпечення достатнього рівня захищеності інформації в інформаційно-телекомунікаційній системі АТ КБ «Dniprobank»

На даний час інформатизація відіграє важливу роль у розвитку української економіки та суспільного життя.

Майже кожна інформаційна система має таку інформацію, розголошення якої третім особам може завдати шкоди її власнику або особі, якої стосується інформація. Це робить питання інформаційної безпеки (ІБ) особливо актуальним у компаніях та організаціях, у яких обробляється інформація з обмеженим доступом.

В Україні процес інформатизації здійснюється згідно з Національною програмою інформатизації, що визначає стратегію вирішення проблеми інформаційного забезпечення соціально-економічної, екологічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у сферах національного значення.

Одним з етапів побудови КСЗІ є розробка політики безпеки. Чим точніше буде створена політика безпеки, тим простіше буде адміністратору безпеки розробити КЗЗ для того, щоб запобігти успішним атакам. Важливу роль в розробці політики безпеки має визначення організаційних методів захисту інформації, що є базисом комплексної системи захисту інформації в системі. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему. Конкретні організаційні методи захисту інформації приводяться при розгляді протидії загрозам безпеки інформації.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Стан інформаційної безпеки критичної інфраструктури є важливим питанням для інформаційного простору України та світу, враховуючи постійне збільшення спектру загроз.

Поняття інформаційної безпеки є не лише безпекою технічних інформаційних систем чи безпекою інформації в чисельному або електронному вигляді, адже потрібно охопити усі аспекти захисту даних чи інформації, незалежно від їхньої форми. [5] Проблему ІБ розглядають у таких основних аспектах: захист інформації, достатнє інформаційне забезпечення державних органів, громадських, приватних організацій. У захисті інформації вбачається система заходів з недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності тощо.

Становлення України як правової держави, економічні та оборонні реформи, інтеграція її в Європейський простір – це чинники, що посприяли створенню нових систем захисту інформації та законодавчого підґрунтя для врегулювання інформаційних комунікацій. Конституція України враховує міжнародні тенденції глобалізації та інформатизації суспільства, тому деякі її статті визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави та стають основою для розвитку відповідного законодавства.

За опублікованими данними ESET - міжнародного розробника антивірусного програмного забезпечення, у банківській сфері в 2021 році була зафіксована найвища середня вартість витоку даних за 17 років [14].

Найбільш поширеною причиною витоку даних була крадіжка облікових даних користувачів. На цей вектор атак припадало 20% порушень. Крім того, атаки за допомогою методів соціальної інженерії стали серйозною загрозою для установ державного управління, зокрема, на них припало 69% усіх порушень для цього сектора.

У 2021 році кількість виявлення банківських шкідливих програм для Android різко зросла, зокрема за січень-лютий майже на 160%, а в наступні чотири місяці на близько 50%. Така тенденція викликає занепокоєння, оскільки банківські трояни можуть мати доступ до фінансів жертв атак.

Шахрайство з інвестиціями в криптовалюту залишається популярним серед зловмисників.

За останні роки зловмисники перейшли від простого зараження систем програмами-здирниками до подвійного здирництва, яке передбачає викрадення даних та їх публікацію чи продаж. Загрози витоку вкрадених даних різко зросли з 8,7% у 2020 році до колосальних 81% у другому кварталі 2021 року.

Найбільше від кіберзлочинності постраждало старше покоління, зокрема близько 28% загальної кількості збитків від шахрайства припало на жертв старше 60 років.

Що стосується України, то за даними Держспецзв'язку, з початку 2021 року в Україні зафіксовано 41 мільйон підозрілих подій інформаційної безпеки, опрацьовано 160 тисяч критичних подій, зареєстровано 147 кіберінцидентів [14].

Відповідно до статистики зібраних та опрацьованих даних, представленої Оперативним центром реагування на кіберінциденти Державного центру кіберзахисту [15], протягом 2021 року були зафіксовані такі типи та категорії подій інформаційної безпеки, які представлені на рис. 1.1 та рис. 1.2.

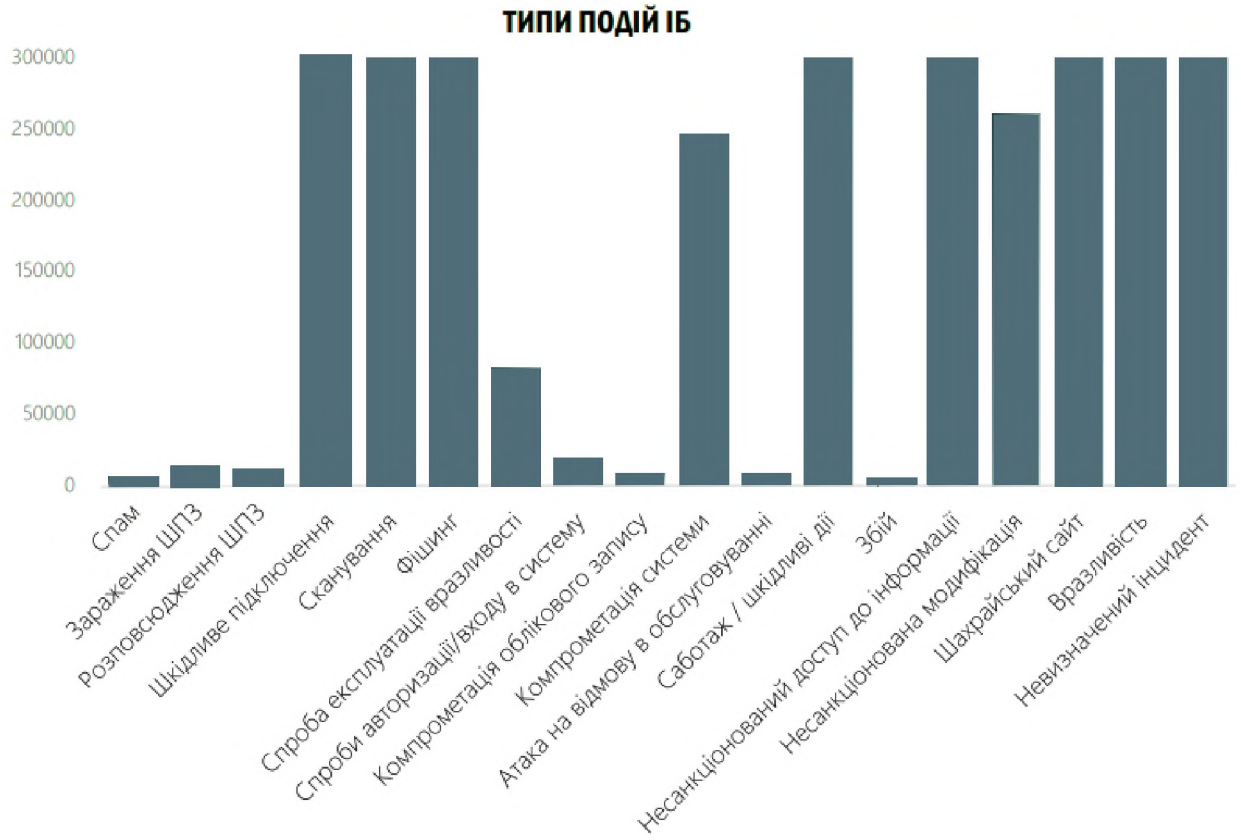

Рис. 1.1 – Типи подій ІБ в Україні за 2021 рік

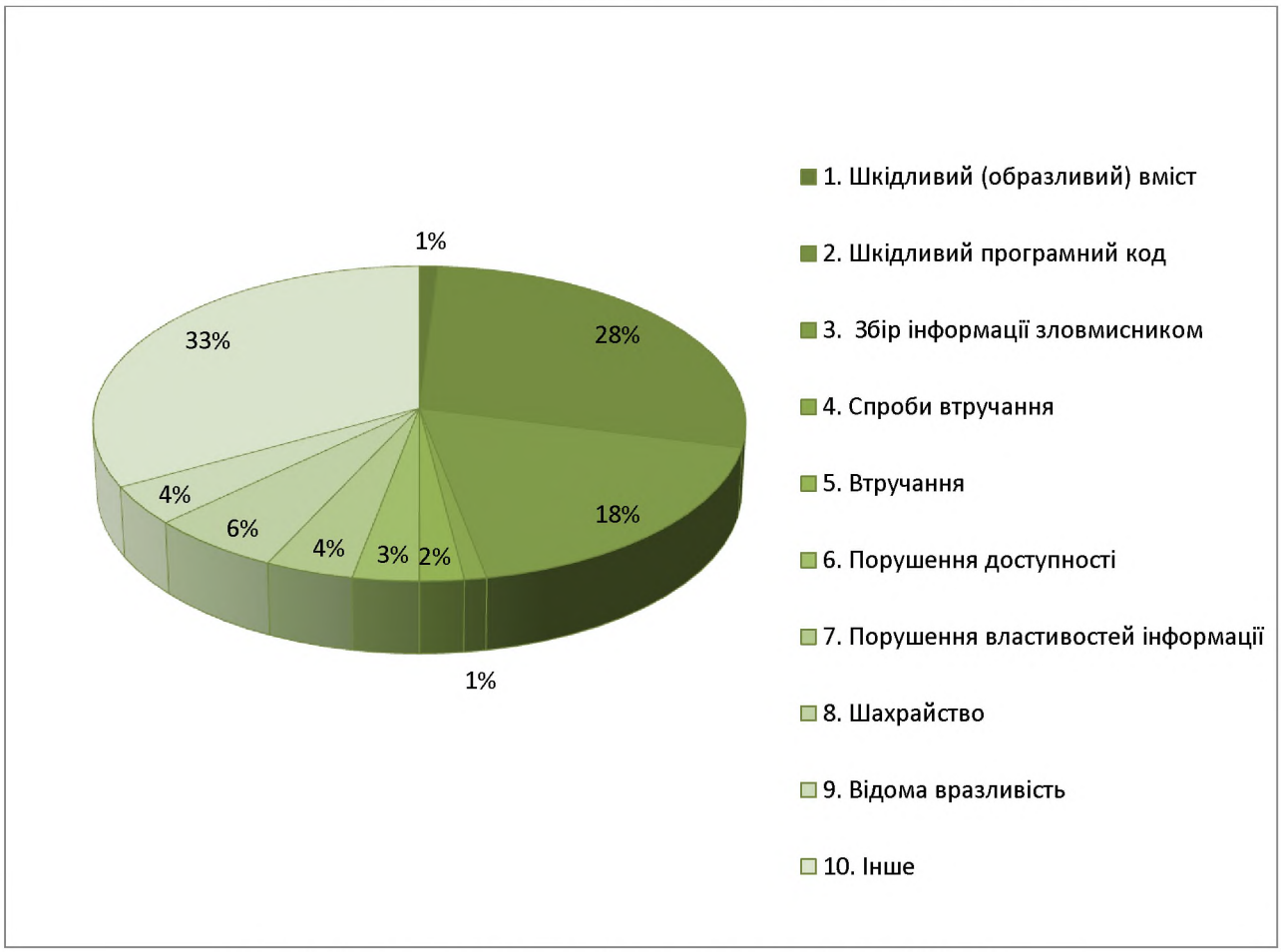

Рис 1.2 – Категорії подій ІБ в Україні за 2021 рік.

Звертаючи увагу на наведені статистичні дані та динаміку розвитку відповідних процесів, можна зробити висновок, що проблеми захисту інформації в комерційних та банківських системах України стають все більш важливими.

1.2 Аналіз нормативно-правової бази у сфері захисту інформації

Останнім часом суспільство стикається з дедалі більшою кількістю різних типів кібератак: фішинг, кіберзлочинність, порушення цілісності, конфіденційності та доступності інформації, відмова сервісів у наданні електронних послуг, блокування роботи державних органів, інформаційний тиск на громадськість, кібертероризм, блокування роботи стратегічно важливих для економіки та безпеки держави підприємств чи установ.

У зв’язку з цим Україна запровадила комплекс заходів для вирішення стратегічних, правових, нормативних та технічних питань, пов'язаних із забезпеченням безпечного інформаційного простору.

Слід зазначити, що законодавство стосовно кібербезпеки в Україні зазнало суттєвих змін з 2014 року. Станом на 2022 рік створено нормативно-правову базу у сфері державної кібербезпеки, прийнято Доктрину інформаційної безпеки України (набрала чинності 25 лютого 2017 року), закони України «Про основні засади забезпечення кібербезпеки України» 2163-VIII (набрав чинності 09.05.2018 р.), «Про національну безпеку України» 2469-VIII (набрав чинності 08.07.2018 р.), «Про інформацію» 2657-XII (редакція від 01.01.2017 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» 80/94-ВР (редакція від 19.04.2014 р.), «Про захист персональних даних» 2297-VI (редакція від 30.01.2018 р.), «Про електронні довірчі послуги» 2155-VIII (набрав чинності 07.11.2018 р.) тощо. [2]

Згідно з Законом України «Про інформацію» [3], за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Будь-яка інформація є відкритою, крім тієї, що віднесена законом

до інформації з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Саме цей закон врегульовує відносини щодо створення, отримання, зберігання, використання, поширення та захисту інформації.

Згідно з ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» [4], умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Тобто, вищезгаданий закон врегульовує відносини в галузі захисту інформації в інформаційно-телекомунікаційних системах.

Також в указі президента приведено низку відповідних положень щодо кібербезпеки, зокрема: «Про Концепцію розвитку сектора безпеки і оборони України» (№ 92/2016 від 14.03.2016 р.); «Про Національний координаційний центр кібербезпеки» (№ 242/2016 від 07.06.2016 р.), «Про стратегічний оборонний бюлетень України» (№ 240/2016 від 06.06.2016 р.) тощо.

Саме у Законі «Про основні принципи кібербезпеки України» визначено основні об’єкти кіберзахисту, які складають критичну національну інфраструктуру, нормативно концептуалізовано сферу кібербезпеки, визначено та регламентовано принципи забезпечення кібербезпеки та встановлено відповідальність за порушення законодавства у цій галузі.

Крім вищеозначеного, було розглянуто нормативно-правове забезпечення, що розроблено регулятором у сфері діяльності підприємства, а саме Національним банком України.

1.3 Постановка задачі

Відповідно до означення та за результатами аналізу нормативно-правової бази та вимог до захисту інформації в ІТС необхідно виконати обстеження, проаналізувати можливі загрози та порушників і розробити заходи захисту інформації на ІТС.

Згідно з НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», комплексна система захисту інформації – це сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС. [7]

Відповідно до НД ТЗІ 3.7-003-05 «Порядку проведення робіт із створення комплексних системи захисту інформації в інформаційно-телекомунікаційній системі» , підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов'язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд. [8]

Нормативні документи визначають необхідність впровадження систем захисту інформації на ОІД, де циркулює відкрита інформація та ІзОД.

Власник (розпорядник) організації відповідає за забезпечення захисту інформації в системі та своєчасне розроблення необхідних для цього заходів.

Розробка КСЗІ починається з обстеження на об'єкті інформаційної діяльності. Під час обстеження ІТС розглядається як організаційно-технічна система, яка поєднує фізичне середовище, обчислювальну систему, середовище користувачів, оброблювану інформацію і технологію її обробки.

При обстеженні фізичного середовища треба проаналізувати загальні характеристики ОІД, умови функціонування ОІД, особливості його розташування на місцевості тощо.

Під час обстеження обчислювальної системи повинен бути виконаний аналіз та опис:

- загальної структурної схеми і складу обладнання, технічних і програмних засобів, їхніх зв'язків, особливостей конфігурації, програмно-апаратних засобів захисту інформації, взаємного розміщення засобів тощо;
- видів та характеристик каналів зв’язку;
- особливостей взаємодії окремих компонентів та їх вплив на один одного.

Мета такого аналізу – надання загального уявлення про наявність потенційних можливостей забезпечення захисту інформації, виявлення компонентів системи, які мають підвищені вимоги до захисту інформації і впровадження додаткових заходів щодо захисту інформації.

Під час обстеження інформаційного середовища аналізується вся інформація, яка обробляється та зберігається в ІТС. В процесі дослідження інформація класифікується за режимом доступу і правовим режимом, описуються її види.

При обстеженні середовища користувачів аналізується функціональний та кількісний склад користувачів, визначаються їх посадові обов’язки, повноваження, кваліфікація та рівень можливостей, наданий їм засобами ІТС.

За результатами проведення обстеження на ОІД формуються завдання захисту інформації в ІТС, здійснюється аналіз ризиків (аналізується модель загроз і модель порушника, визначаються можливі наслідки від реалізації потенційних загроз). Згідно з виконаним обстеженням і аналізом ризиків постає питання щодо розробки політики безпеки інформації задля мінімізації ймовірності реалізації ризиків через наявні вразливості системи. Слід

зазначити, що в АС може бути реалізовано декілька різних політик безпеки, які можуть істотно відрізнятися.

Висновки до розділу 1

Було розглянуто стан злочинів в сфері інформаційної безпеки та статистика реалізованих атак за 2021-2022 роки в Україні. Виявлено значна кількість інцидентів порушення інформаційної безпеки на території України. Зазначена необхідність розвитку кібербезпеки.

В цьому розділі приведено перелік нормативно-правових документів в сфері захисту інформації, зазначено їх основні положення. Серед документів, що є правовою основою забезпечення безпеки інформації розглянуті НД ТЗІ та галузі їх використання, Закони України, положення та накази.

Було обґрунтовано потребу у створенні КСЗІ у відділенні банку для запобігання НСД до важливих ресурсів системи. Відповідно до нормативної документації, до етапів створення КСЗІ, які використані в роботі, віднесені: обґрунтування необхідності створення КСЗІ, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує загрози усіх рівнів.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про АТ КБ «Dniprobank»

Об’єктом інформаційної діяльності є приміщення відділення комерційного банку " Dniprobank".

Рисунок 2.1 – Організаційна структура банку

Відділення банку надає такі послуги:

- прийом депозитів від юридичних та фізичних осіб;
- відкриття та ведення поточних рахунків клієнтів;
- валютні операції;
- надання гарантій та інших зобов'язань від третіх осіб, які передбачають їхнє виконання у грошовій формі;
- послуги з відповідального зберігання та надання в оренду сейфів для зберігання цінностей та документів;
- випуск банківських платіжних карток та здійснення операцій із використанням цих карток;
- надання консультаційних та інформаційних послуг щодо банківських операцій та інших фінансових операцій.

Структурні підрозділи відділення комерційного банку виконують такі основні функції:

Відділ кредитування здійснює кредитування юридичних і фізичних осіб, які перебувають на території, що обслуговується, аналізує структуру кредитного портфеля відділення та розробляє пропозиції щодо вибору напрямків кредитування, контролює формування резерву на можливі втрати по позиках.

Операційний відділ забезпечує універсальне обслуговування фізичних і юридичних осіб на основі надання всього комплексу банківських послуг.

Відділ бухгалтерського обліку та звітності організовує бухгалтерський облік і звітність в відділенні, контролює раціональне використання фінансових ресурсів, формує зведену і достовірну інформацію про фінансові результати діяльності відділення.

Економічний відділ аналізує фінансову діяльність відділення, складає зведені фінансові плани, кошториси витрат та витрат відділення, контролює їх виконання, готує пропозиції щодо вдосконалення процентної політики відділення з урахуванням регіональних особливостей, здійснює планування і прогнозування діяльності відділення, збирає і аналізує статистичну інформацію про діяльність відділення.

Юридичний відділ забезпечує дотримання законності в діяльності відділення, здійснює захист прав і законних інтересів відділення, забезпечує правовими методами майнові інтереси відділення.

Відділ автоматизації здійснює введення і експлуатацію в відділенні систем і засобів автоматизації банківських операцій, забезпечує впровадження та експлуатацію систем міжбанківських телекомунікацій, організовує технічне обслуговування засобів обчислювальної та банківської техніки, що експлуатуються в відділенні, забезпечує супровід і адміністрування програмних комплексів.

Служба внутрішнього контролю проводить ревізії і цільові перевірки діяльності установ відділення, попереджає і своєчасно виявляє негативні явища в діяльності відділення.

Штат працівників відділення складається з 20 людей: керівник відділенням, заступник керівника відділенням, операціоніст – 4 люд., головний економіст, економіст, юрисконсульт, менеджер по роботі з клієнтами – 2 люд., адміністратор безпеки, головний бухгалтер, бухгалтер, системний адміністратор, охоронник – 3 люд., прибиральниця – 2 люд.

2.2 Обстеження на об’єкті інформаційної діяльності

Обстеження на об’єкті інформаційної діяльності проведено відповідно до Методичних вказівок щодо структури та змісту Плану захисту інформації в автоматизованій системі - НД ТЗІ 1.4-001-2000 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Типове положення про службу захисту інформації в АС [13], здійснено обстеження середовищ функціонування. Акт оформлено відповідно до Додатку А. «Форма та зміст акта обстеження на об'єкті інформаційної діяльності стосовно створення комплексу ТЗІ, НД ТЗІ 3.1- 001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи».

Порядок проведення обстеження відповідає ДСТУ 3396.1. Під час обстеження розглянуто середовище функціонування ІТС: фізичне середовище, обчислювана система, середовище користувачів та оброблювана інформація. Приводиться опис кожного середовища функціонування ІТС.

2.3 Обстеження фізичного середовища

Відділення розташоване на 1 поверсі п’ятиповерхової будівлі, має площу 115 м^2, знаходиться за адресою: м. Дніпро, пр. Дмитра Яворницького 23.

Контрольована зона обмежена по периметру стінами будівлі, зверху – стелею, знизу - підлогою.

Режим контрольованої зони цілодобово забезпечується найманими співробітниками приватної охоронної агенції «Леон» згідно з договором №865/00382 від 01.05.2015 року та з використанням централізованої системи охоронної сигналізації.

Будівлю введено в експлуатацію у 1998 році. Фундамент будинку – бутовий, стіни – цегляні. Перекриття між поверхами – залізобетонні плити.

Підлога – залізобетонна. Покрівля будівлі – залізобетонна, горизонтальна, покриття - руберойд.

Територія навколо будівлі з відділенням має асфальтове покриття.

Зі сходу ділянка обмежена парканом. Навколо розташовані багатоповерхові будівлі, в тому числі і житлові. Є місце для паркування автомобілів. По ступеню надійності електрозабезпечення будівля відділення відноситься до споживачів II категорії, тобто допустимі перерви в електропостачанні на час, необхідний для включення резервного живлення черговим персоналом.

Схема розташування ОІД та об’єктів навколо нього наведена на ситуаційному плані (рис. 2.2). Об’єкти, що оточують будинок, в якому знаходиться ОІД наведено в таблиці 2.1.

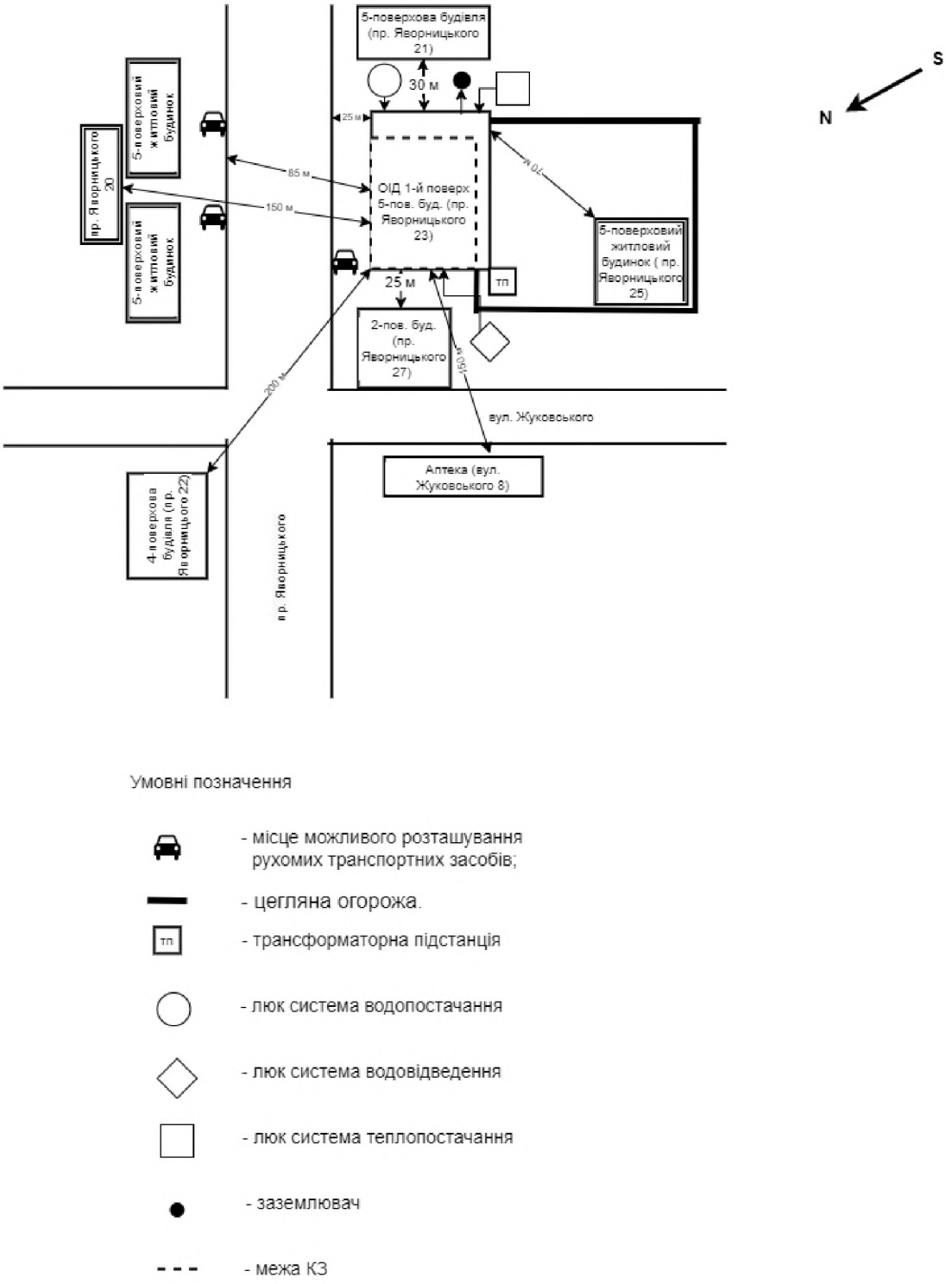

Рисунок 2.2 – Ситуаційний план ОІД

Таблиця 2.1 - Об’єкти, що знаходяться навколо ОІД.

№ п\п	Розташування відносно ОІД	Кількість поверхів	Адреса	Характер діяльності	Відстань від ОІД, (м)
1	Північний захід	4	вул. Жуковського 8	Аптека	150

Продовження таблиці 2.1

№ п\п	Розташування відносно ОІД	Кількість поверхів	Адреса	Характер діяльності	Відстань від ОІД, (м)
2	Північ	4	Пр. Яворницького 22	Адміністративна будівля	200
3	Північний схід	5	Пр. Яворницького 20	Житловий будинок	150
4	Захід	5	Пр. Яворницького 25	Житловий будинок	70
5	Схід	5	пр. Яворницького 21	Будівля з комерційними приміщеннями для оренди	50
6	Південний схід	2	пр. Яворницького 27	Салон краси	25

На генеральному плані зазначені схеми систем опалення, електроживлення, пожежної та охоронної сигналізацій (рис. 2.3).

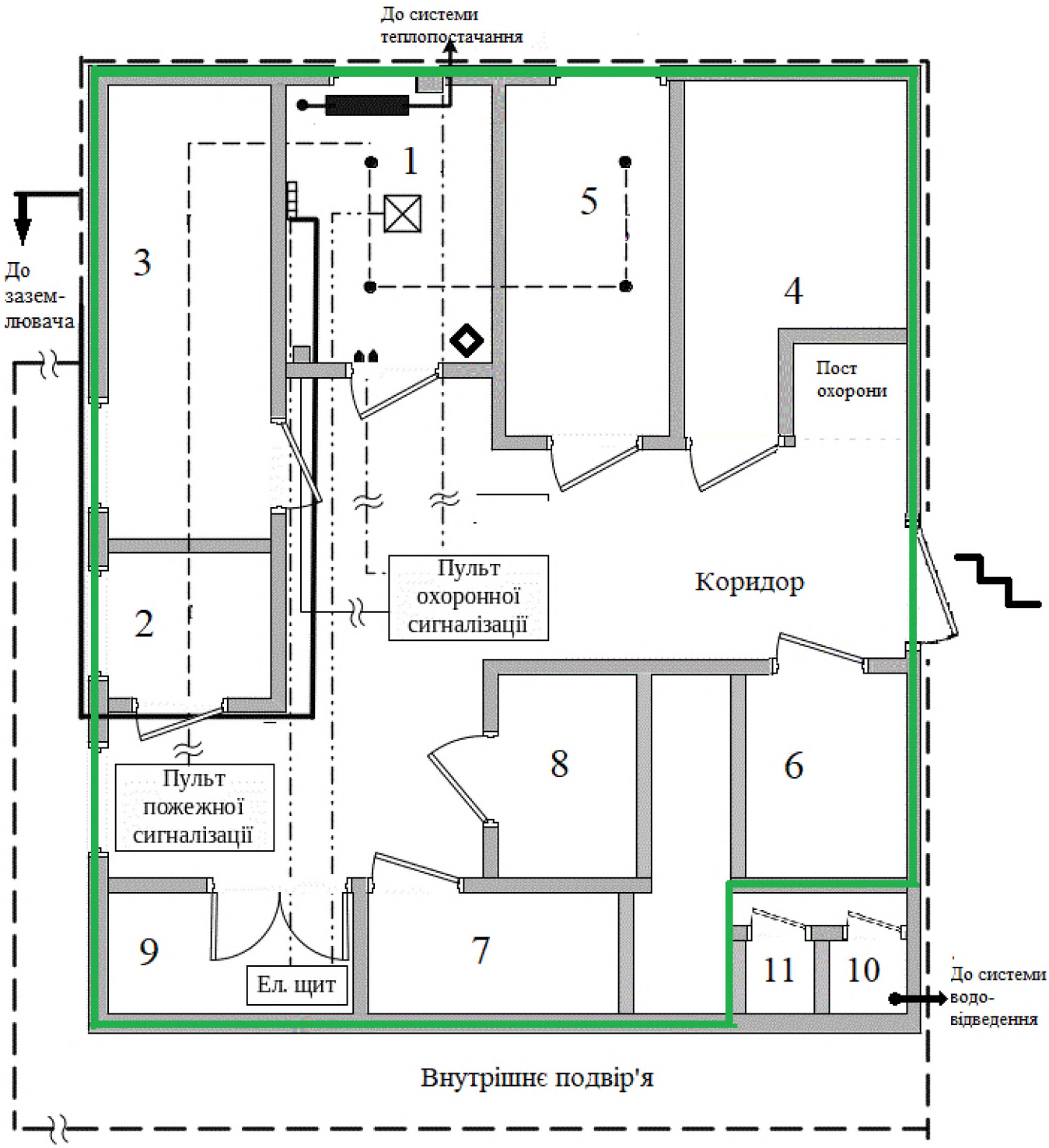

Рисунок 2.3 – Схема генерального плану ОІД

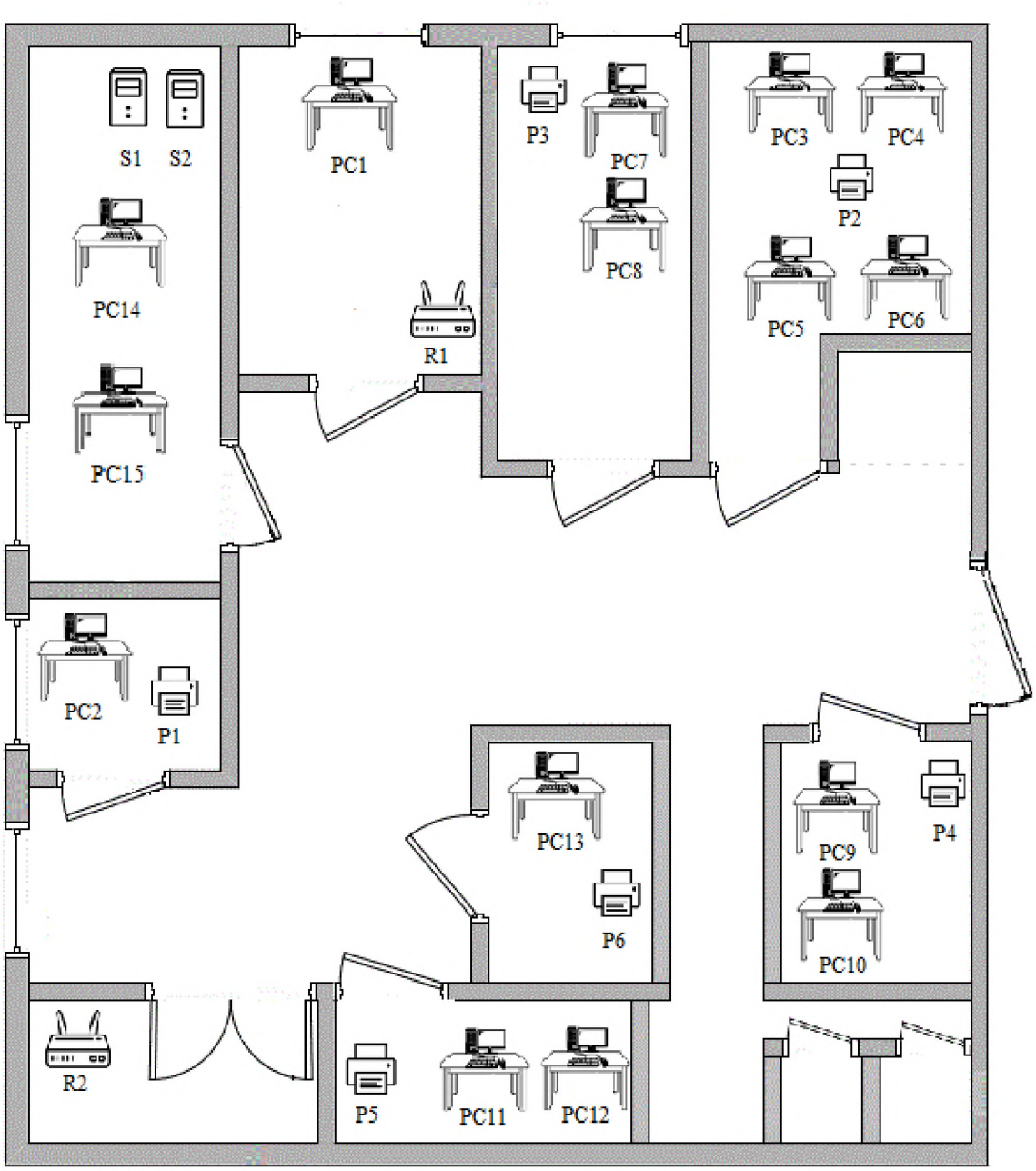

Рисунок 2.4 - План розміщення засобів обчислювальної техніки

Умовні позначення елементів та допоміжні засоби обробки інформації:

- датчик на відкриття дверей	- кабель охоронної сигналізації
- датчик пожежної сигналізації	- кабель пожежної сигналізації
- батарея опалення	- сходи
- світильник	- межа контрольованої зони
- датчик на відкриття вікон	- кабель електроживлення
- пасивний інфрачервоний датчик	- шина заземлення

- ел. розетка	- система заземлення
- камера система відеоспостереження	- межа ОІД

Умовні позначення приміщень:

1	кабінет керівника
2	кабінет заступника керівника
3	серверна
4	операційний відділ
5	відділ кредитування
6	відділ бухгалтерського обліку
7	економічний відділ
8	юридичний відділ
9	служба внутрішнього контролю
10	вбиральня
11	технічне приміщення

Характеристика складових ОІД:

- Висота стель – 3 м; стінні перегородки з гіпсокартону – 150 мм; стіни зовнішні з цегли - 500 мм.
- В приміщенні 5 металопластикових одностворчатих вікон розміром 1300 мм х 1500 мм, захищені металевими решітками та жалюзі.
- Вхідні двері металеві двостворчаті з розміром отвору 2000 мм х 1000 мм. Двері захищені циліндровим замком. Ключі знаходяться на посту охорони.
- У приміщенні є 11 міжкімнатних одностворчатих дверей з розміром отвору 2000 мм х 800 мм, що захищені циліндровими замками. Ключі від замків знаходяться на посту охорони.
- Система електроживлення в будівлі здійснюється від трансформаторної підстанції №76. Підземними лініями комунікацій та

кабелем ТП підключена до щитової, яка розташована в приміщенні служби внутрішнього контролю, яке розташоване на першому поверсі будівлі у кімнаті 9.

- Система електроживлення (освітлення): мережа 220В; генератор електроживлення Hertz HG 13 RC; світильники з LED лампами. Кабельне підключення до мережі Інтернет – оптоволоконний кабель.
- Системи сигналізації:

- пожежна – димовий сповіщувач Артон СПД 3.4, ручний пожежний сповіщувач, шлейфи по стелі, сигнальні пристрої.

- охоронна – магнітно-контактні датчики на відкриття дверей та вікон Ajax DoorProtect, оптичні датчики руху F&F накладний (20м 360), централь.

- Система пожежної сигналізації підключена на центральний пульт через GSM.
- Живлення систем освітлення, електропостачання та опалення здійснюється через підключення до міських комунальних мереж.
- Система заземлення в будівлі присутня. Зовнішні підключення до заземлювача відсутні.
- На вході до будівлі розташована відомча охорона, що забезпечує пропускний режим до приміщень та здійснює цілодобову охорону.
- На фасаді приміщення встановлена система відеоспостереження з візуальним контролем охороною приміщення на вході в будівлю.

Таблиця 2.2 – Технічні системи ОІД

№ п/п	**Вид системи комунікацій**	**Характеристика**
1	Електропостачання	Підключена від трансформаторної підстанції підземними шляхами, яка має сторонніх споживачів і знаходиться за межами КЗ, до щитової, яка знаходиться у кімнаті 9 (служба внутрішнього контролю). Розетки та світильники підключені до щитової.

Продовження таблиці 2.2

№ п/п	Вид системи комунікацій	Характеристика
2	Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
3	Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ підземним з'єднанням.
4	Система водопостачання	Підключена до міського водоканалу, який знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
5	Заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
6	Система вентиляції	Приточно-витяжна

Основні та допоміжні технічні засоби обробки інформації наведені в табл. 2. 3 і табл. 2. 4

Таблиця 2.3 – Основні технічні засоби

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Фізичне розташування
1	Системний блок	PC1	HP Z440 (T4K25EA)	KF55343286	Під столом
2	Сервер	S1-S2	Dell PowerEdge T20	OC91808F87	На столі
3	Маршрутизатор	R1-R2	Xiaomi Mi AIoT Router ax3600	KTY15UT82D, GHK846LOJ9	На стіні
4	Системний блок	PC2	HP Z440 (T4K25EA)	KTY16UT83D	Під столом
5	Системний блок	PC3- PC6	HP Z440 (T4K25EA)	DG827177V5, KTY14UT81D, UHJGF7457P, LKDC47632N	Під столом
6	Системний блок	PC7 – PC8	HP Z440 (T4K25EA)	KB3212O5E4,OJZX1036LM	Під столом
7	Системний блок	PC9 - PC10	HP Z440 (T4K25EA)	XD74OK93D0, IH847HK6215	Під столом
8	Системний блок	PC11 - PC12	HP Z440 (T4K25EA)	UV861B5298, LI496ZSM461	Під столом
9	Системний блок	PC13-PC14	HP Z440 (T4K25EA)	KTY18UT85D, DF093498LN	Під столом
10	Системний блок	PC15	HP Z440 (T4K25EA)	KTY17UT84D	Під столом
11	БФП, підключений до PC2	P1	Brother HL -L2365DWR	PL3286M86	На столі

Продовження таблиці 2.3

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Фізичне розташування
12	БФП, підключений до PC3, PC4, PC5, PC6	P2	Brother HL -L2365DWR	TG84IS1O5L	На столі
13	БФП, підключений до PC7, PC8	P3	Brother HL -L2365DWR	CCF4758SVG	На столі
14	БФП, підключений до PC9, PC10 Brother HL -L2365DWR	P4	Brother HL -L2365DWR	PS85G145LM	На столі
15	БФП, підключений до PC11, PC12 Brother HL -L2365DWR	P5	Brother HL -L2365DWR	CFW36415L1	На столі
16	БФП, підключений до PC13, PC14 Brother HL -L2365DWR	P6	Brother HL -L2365DWR	ER85IT56VD	На столі
17	Комп'ютерна миша, підключена до PC1-PC15	-	Logitech Wireless Mouse M185 (910-002238) Black	AJ8436M156	На столі
18	Монітор, підключений до PC1	-	Philips V-line 203V5LSB26/10/62	XL546921FB	На столі
19	Монітор, підключений до PC2	-	Philips V-line 203V5LSB26/10/62	DYG4589S1K	На столі
20	Монітор, підключений до PC3-PC6	-	Philips V-line 203V5LSB26/10/62	5D84EHF369, 7BHL84AG96, O4FGT5FGH1,234FR56GHY	На столі

Продовження таблиці 2.3

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Фізичне розташування
21	Монітор, підключений до PC7-PC8	-	Philips V-line 203V5LSB26/10/62	EF48B26U79, VDC34RS5XN	На столі
22	Монітор, підключений до PC9-PC10	-	Philips V-line 203V5LSB26/10/62	PPDF49722S, MJ23749FGH	На столі
23	Монітор, підключений до PC11-PC12	-	Philips V-line 203V5LSB26/10/62	HDC458919P, KD638F5GS6H	На столі
24	Монітор, підключений до PC13-PC14	-	Philips V-line 203V5LSB26/10/62	NDS564SKJ, XG92GHYT30	На столі
25	Монітор, підключений до PC15	-	Philips V-line 203V5LSB26/10/62	XCM4589MK	На столі
26	Клавіатура, підключена до PC1	-	Logitech K120 USB Black	RS84579613	На столі
27	Клавіатура, підключена до PC2	-	Logitech K120 USB Black	SDJH856LB	На столі
28	Клавіатура, підключена до PC3	-	Logitech K120 USB Black	LCM145Z6C	На столі

Продовження таблиці 2.3

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Фізичне розташування
29	Клавіатура, підключена до PC3-PC6	-	Logitech K120 USB Black	ADV548DFM, HSK728BSGH, 89SHBUD302, LKXSYG8936	На столі
30	Клавіатура, підключена до PC7-PC8	-	Logitech K120 USB Black	SDD5615CDS, ZKO37DGZC	На столі
31	Клавіатура, підключена до PC9-PC10	-	Logitech K120 USB Black	UYK1420XZ, 3F43N RSF56	На столі
32	Клавіатура, підключена до PC11-PC12	-	Logitech K120 USB Black	PSA415MN5, 45Z6C VDC34	На столі
33	Клавіатура, підключена до PC13-PC14	-	Logitech K120 USB Black	EFW463F43N, D5FGH186SH	На столі
34	Клавіатура, підключена до PC15	-	Logitech K120 USB Black	RSF5621NB	На столі

Таблиця 2.4 – Допоміжні технічні засоби (фрагмент)

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Фізичне розташування
1	Світильник		Expert XH-C15-255-SS	VX58L	На стелі
2	Датчик на відкриття вікон		Ajax DoorProtect white	GW96M	На стіні
3	Пасивний інфрачервоний Датчик		F&F DR-05B	SD18E	На стіні

2.4 Обстеження обчислювальної системи ІТС

Схема ІТС наведена на рис. 2.5 За класифікацією АС відноситься до 3 класу: розподілений багатомашинний багато користувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

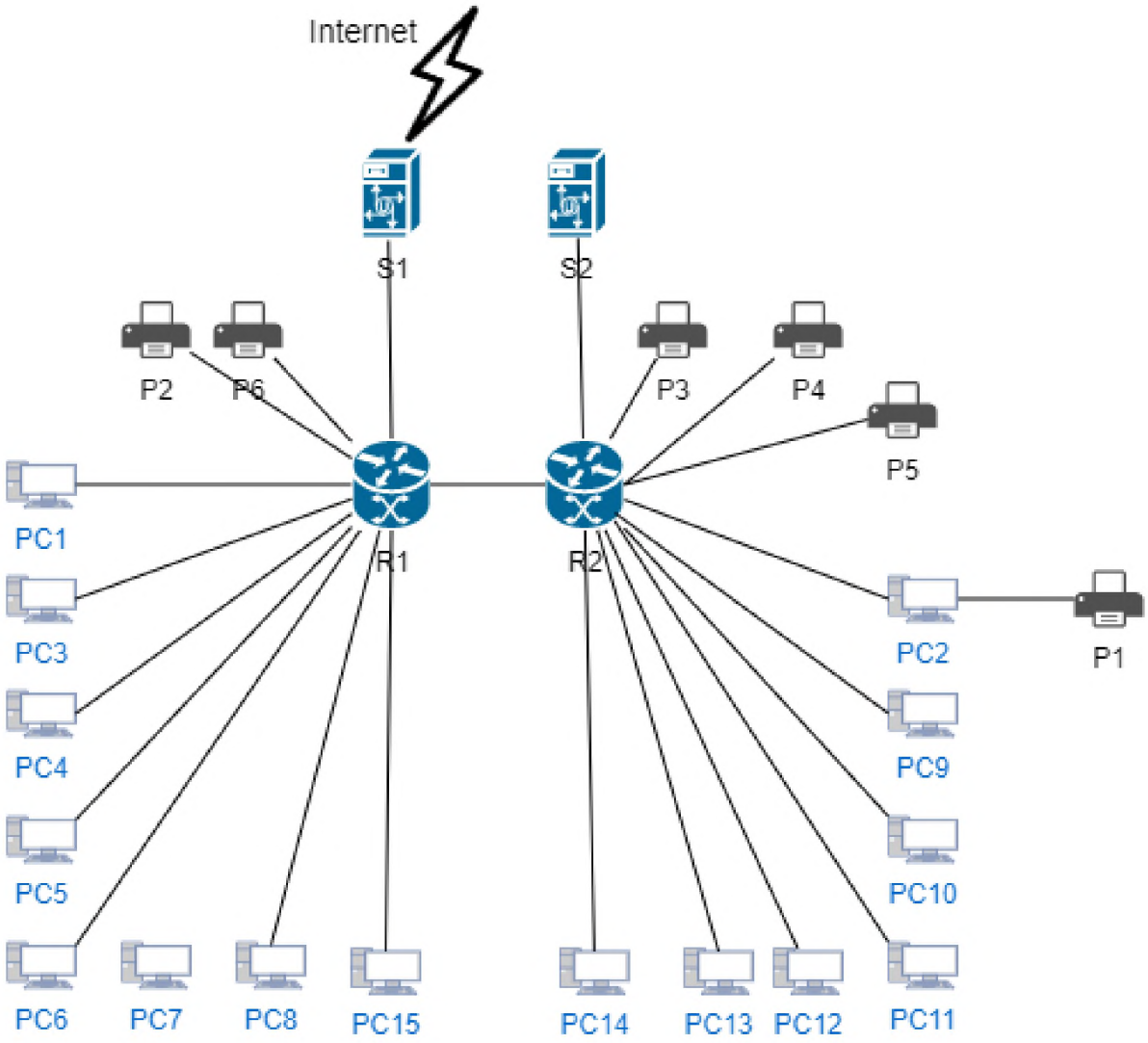

Рисунок 2.5– Схема ІТС

В обчислювальній системі з'єднуються пристрої, що розташовані в межах ОІД, тому вона є локальною. Підключена до глобальної мережі Internet для забезпечення взаємодії з генеральним офісом, іншими відділеннями та організаціями-партнерами. Канал зв'язку в межах корпоративної мережі та підключення до мережі Internet забезпечує провайдер «Київстар», який надає послуги з побудови, надання та підтримки відомчої телекомунікаційної мережі у відповідності до Договорів між «Dniprobank» та «Київстар».

Таблиця 2.5 - Засоби обробки інформації (апаратне забезпечення)

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Характеристика
1	Системний блок	PC1	HP Z440 (T4K25EA)	KF55343286	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (GFC3F7VEKD95) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
2	Сервер	S1-S2	Dell PowerEdge T20	OC91808F87	I7/64 Gb/SSD 1 Tb (SA2000BM8/8459-BK) /2NA 1 Gb/s Тип підключення для S1 – оптоволоконний кабель, для S2 – кручена пара.
3	Маршрутизатор	R1-R2	Xiaomi Mi AIoT Router ax3600	KTY15UT82D GHK846LOJ9	802.11ax інтерфейс підключення: 3x10 / 100 / 1000M швидкість з'єднання: 2402 + 574 Мбіт / с Тип підключення - кручена пара.
4	Системний блок	PC2	HP Z440 (T4K25EA)	KTY16UT83D	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (HSL6S1XLSN42) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
5	Системний блок	PC3	HP Z440 (T4K25EA)	DG827177V5	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (YGH4S9TGHR65) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
6	Системний блок	PC4 – PC6	HP Z440 (T4K25EA)	KTY14UT81D UHJGF7457P LKDC47632N	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (AFR4V6RDE15) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
7	Системний блок	PC7 - PC9	HP Z440 (T4K25EA)	KB3212O5E4 OJZX1036LM IH847HK6215	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (DHC6T4AUD47) / AMD Radeon RX 470, 4 ГБ ***Тип підключення - кручена пара.***

Продовження Таблиці 2.5

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Характеристика
8	Системний блок	PC10 - PC11	HP Z440 (T4K25EA)	XD74OK93D0 LI496ZSM461	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (KDF2E5LKV91) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
9	Системний блок	PC12 - PC13	HP Z440 (T4K25EA)	UV861B5298 DF093498LN	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (OHJ9S5LDN13) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
10	Системний блок	PC14	HP Z440 (T4K25EA)	KTY18UT85D	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (PFV4S3WKM86) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
11	Системний блок	PC15	HP Z440 (T4K25EA)	KTY17UT84D	Intel Pentium G4560 (3.5 ГГц) / RAM 8 ГБ / HDD 1 ТБ (TFB7S3BDG15) / AMD Radeon RX 470, 4 ГБ Тип підключення - кручена пара.
12	БФП, підключений до PC2	P1	Brother HL - L2365DWR	PL3286M86	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення – USB 2.0
13	БФП, підключений до PC3, PC4, PC5, PC6	P2	Brother HL - L2365DWR	TG84IS1O5L	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.
14	БФП, підключений до PC7, PC8	P3	Brother HL - L2365DWR	CCF4758SVG	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.
15	БФП, підключений до PC9, PC10	P4	Brother HL - L2365DWR	PS85G145LM	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.

Продовження Таблиці 2.5

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Характеристика
16	БФП, підключений до РС11, РС12	Р5	Brother HL - L2365DWR	CFW36415L1	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.
17	БФП, підключений до РС13	Р6	Brother HL - L2365DWR	ER85IT56VD	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.
18	БФП, підключений до РС15	Р7	Brother HL - L2365DWR	LN8SD413L6	Макс. розд. здатність друку 600x2400 dpi. Техн. друку Лазерний (ч/б). Станд. лоток: A4, Letter, A5, A6, Executive. Шв. друку: до 30 стр/хв; Тип підключення - кручена пара.
19	Комп'ютерна миша, підключена до РС1-РС15	-	Logitech Mouse M185 (910-002238) Black	AJ8436M156	Тип датчика Оптичний. Кількість кнопок 2. Тип підключення – USB 2.0
20	Монітор, підключений до РС1	-	Philips V-line 203V5LSB26/10/62	XL546921FB	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
21	Монітор, підключений до РС2	-	Philips V-line 203V5LSB26/10/62	DYG4589S1K	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
22	Монітор, підключений до РС3-РС6	-	Philips V-line 203V5LSB26/10/62	USFGE3645F	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.

Продовження Таблиці 2.5

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Характеристика
23	Монітор, підключений до PC7-PC8	-	Philips V-line 203V5LSB26/10/62	EF48B26U79	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
24	Монітор, підключений до PC9-PC10	-	Philips V-line 203V5LSB26/10/62	PPDF49722S	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
25	Монітор, підключений до PC11-PC12	-	Philips V-line 203V5LSB26/10/62	HDC458919P	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
26	Монітор, підключений до PC13-PC14	-	Philips V-line 203V5LSB26/10/62	NDS564SKJ	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
27	Монітор, підключений до PC15	-	Philips V-line 203V5LSB26/10/62	XCM4589MK	Діагональ дисплея 19.5". Тип матриці TN+film. Максимальна роздільна здатність дисплея 1600 x 900. Тип підключення – кабель HDMI.
28	Клавіатура, підключена до PC1	-	Logitech K120 USB Black	RS84579613	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
29	Клавіатура, підключена до PC2	-	Logitech K120 USB Black	SDJH856LB	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна

Продовження таблиці 2.5

№ п/п	Найменування	Позначення на схемі	Модель	Серійний номер	Характеристика
30	Клавіатура, підключена до PC3	-	Logitech K120 USB Black	LCM145Z6C	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
31	Клавіатура, підключена до PC4-PC6	-	Logitech K120 USB Black	ADV548DFM	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
32	Клавіатура, підключена до PC7-PC9	-	Logitech K120 USB Black	SDD5615CDS	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
33	Клавіатура, підключена до PC10-PC11	-	Logitech K120 USB Black	UYK1420XZ	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
34	Клавіатура, підключена до PC12-PC13	-	Logitech K120 USB Black	PSA415MN5	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
35	Клавіатура, підключена до PC14	-	Logitech K120 USB Black	EFW463F43N	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна
36	Клавіатура, підключена до PC15	-	Logitech K120 USB Black	RSF5621NB	Інтерфейс USB. Кількість кнопок 104. Тип: мембранна

Таблиця 2.6 - Системне програмне забезпечення

№ п/п	Найменування	Версія	Де встановлено	Тип ліцензії
1	OS Windows 10 Pro	10.0.19042.1164	PC1 – PC15	ESD
2	Windows Server 2016	14393.0	S1 – S2	ESD
3	Драйвер відеоадаптеру	NVIDIA GeForce 920MX27.21.14.5167	PC1 – PC15	-
4	Драйвер жорсткого диску	Disk drive 10.0.19041.789	PC1 – PC15	-
5	Драйвер клавіатури	PC/AT Enhanced PS/2 Keyboard (101/102-Key) 10.0.19041.1	PC1 – PC15	-
6	Драйвер процесору	Intel Processor 10.0.19041.1620	PC1 – PC15	-

Таблиця 2.7 - Прикладне ПЗ

№ п/п	Найменування	Версія	Де встановлено	Тип ліцензії
1	MS Office 2016	16.0.14026.20270	PC1 – PC15	ESD
2	Diasoft FA# Beans	7.2	PC1 – PC15	ESD
3	Flextera BI	1.3	PC12 - PC13	ESD

Таблиця 2.8 - Спеціалізоване ПЗ

№ п/п	Найменування	Версія	Де встановлено	Тип ліцензії
1	Avast Antivirus Pro Plus	21.6.2474	PC14, PC10, S1 – S2	ESD

Таблиця 2.9 - Види і характеристики каналів зв'язку

№ п/п	Вид каналу зв'язку	Характеристика
1	Кабель кручена пара (Cat 5e)	Не екранований 4-парний UTP кабель категорії 5e призначений для застосування в локальних мережах передачі даних: PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Мбіт/с, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Мбіт/с, Gigabit Ethernet (1000BASE-T), Firewire 100 Мбіт/с. Для стаціонарного прокладання всередині будівель, станцій, споруд, апаратури. Експлуатується при частотах до 250 МГц. Використовується при підключенні всіх ПК, БФП та серверів до роутерів і роутерів між собою.
2	Оптоволоконний кабель	Одномодовий, швидкість 10 Гбіт/с. Використовується для підключення сервера S1 до мережі Інтернет.
4	Дротовий USB 2.0	Режим роботи - High-speed, швидкість 25—480 Мбіт/с. Використовується при підключенні БФП до ПК.

2.5 Обстеження інформаційного середовища ІТС

У табл. 2.10 наведена класифікація інформації, яка обробляється в інформаційній системі.

Таблиця 2.10 – Класифікація інформації в ІС

№ п/п	Вид інформації	За режимом доступу	За режимом секретності	За вид. предст. в ІС	Вимоги до захисту
1	Корпоративні дані про співробітників	Із обм. дост.	Конф.	Паперовий Електронний	К, Ц, Д

Продовження таблиці 2.10

№ п/п	Вид інформації	За режимом доступу	За режимом секретності	За вид. предст. в ІС	Вимоги до захисту
2	Персональні дані співробітників	Із обм. дост.	Конф.	Електронний	К, Ц, Д
3	Інформація про послуги, які надає відділення банку	Відкрита	Відкрита	Паперовий Електронний	Ц
4	Інформація про графік роботи відділення банку	Відкрита	Відкрита	Паперовий Електронний	Ц, Д
5	Статутні документи відділення	Відкрита	Відкрита	Паперовий Електронний	Ц, Д
6	Трудові договори	Із обм. дост.	Конф.	Паперовий Електронний	К, Ц, Д
7	Бухгалтерські звіти	Із обм. дост.	Конф.	Паперовий Електронний	К, Ц, Д
8	Інформація про фінансову діяльність відділення	Із обм. дост.	Конф.	Електронний	К, Ц, Д
9	Бази даних відділення	Із обм. дост.	Конф.	Електронний	К, Ц, Д
10	Договори з клієнтами	Із обм. дост.	Конф.	Паперовий Електронний	К, Ц, Д
11	Інформація про конфігурацію мережі та її компонентів	Із обм. дост.	Конф.	Паперовий Електронний	К, Ц, Д

Обстеження інформаційного середовища включає в себе інформацію, що планується до обробки за допомогою ІТС.

За результатами обстеження в ІТС наявні наступні види інформації: відкрита інформація і конфіденційна інформація.

За режимом доступу інформація, що оброблюється за допомогою ІТС поділяється на інформацію з обмеженим доступом (ІзОД) та відкриту, що потребує захисту.

ІзОД зображена в ІТС у вигляді електронних документів, створених за допомогою пакету прикладних програм Microsoft Office 2016, Adobe Acrobat або у друкованому паперовому вигляді. Паперові носії інформації зберігаються в сейфі. Правила доступу до інформації встановлені власником.

ІзОД, що циркулює в ІТС, зберігається на жорсткому магнітному диску та на комп'ютерах співробітників, що мають до неї доступ. Документи, що містяться ІзОД, друкуються за допомогою принтерів, які входять до складу ІТС. Перелік відомостей, що включають ІзОД, а також всі відомості за режимом доступу, за правовим режимом та за типом представлення в ІТС приведені та класифіковані у таблиці.

Вимоги захисту встановлено власником згідно з вимогами нормативно-правових актів. Для всіх видів інформації, представлених в таблиці, встановлюється адміністративне керування доступом. Атрибути доступу присвоюються в момент створення документа в системі. Інформація може зберігатися в системі у текстових та графічних форматах. Імпорт та експорт інформації в ІТС здійснюється за допомогою використання електронної пошти, сканування та друку документів.

При аналізі технології обробки інформації виявлено особливості обігу електронних документів. Процеси виникнення, рухи й обробки інформації, що циркулює в системі, створюють інформаційні потоки.

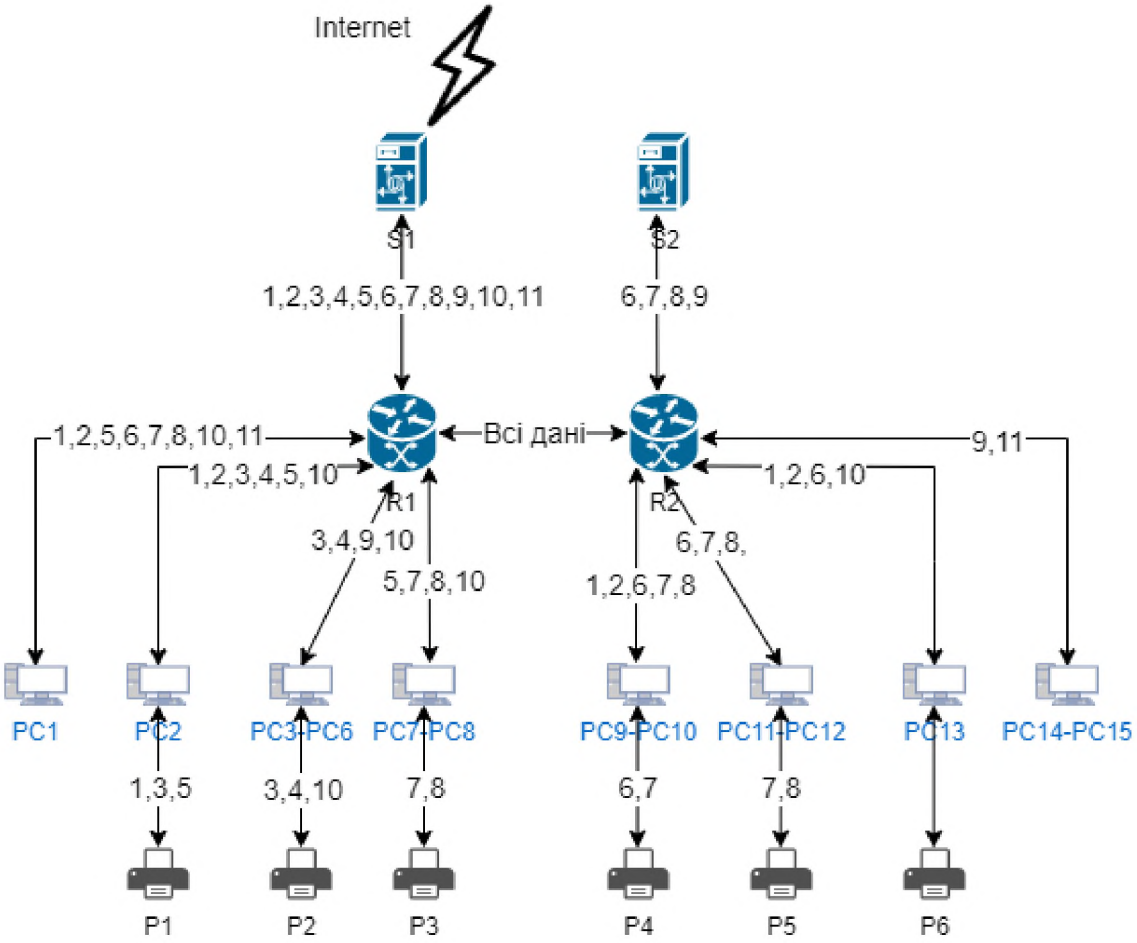

Рисунок 2.6 - Схема інформаційних потоків

До основних інформаційних потоків належать:

1. Обробка корпоративних даних про співробітників. Створюються на ПК керівника та заступника керівника. Можуть передаватися через Інтернет до центрального офісу. Можуть бути роздруковані.
2. Обробка персональних даних про співробітників. Створюються на ПК керівника. Можуть передаватися через Інтернет до центрального офісу.
3. Обробка інформації про послуги, які надає відділення банку. Може створюватися і передаватися між кожним учасником ІТС в залежності від необхідності взаємодії. Може бути роздрукована та передаватися до центрального офісу.
4. Обробка інформації про графік роботи відділення банку. Створюється заступником керівника. Може бути роздрукована та передана до центрального офісу.

5. Обробка статутних документів. Оброблюються на ПК керівника та заступника керівника. Можуть передаватися до центрального офісу. Можуть роздруковуватися.
6. Обробка кадрових документів: створюється та обробляється на ПК заступника керівника, бухгалтерії , за необхідністю передається між ними та на ПК керівника відділенням.
7. Обробка документації бухгалтерського обліку: створюється та обробляється на ПК бухгалтера, дані можуть передаватися через мережу Інтернет економісту, головному економісту та керівнику; може бути роздрукована.
8. Обробка інформації про фінансову діяльність відділення. Створюється та обробляється на ПК бухгалтера, дані можуть передаватися через мережу Інтеренет економісту, головному економісту та керівнику; може бути роздрукована.
9. Обробка баз даних відділення. Створюються на ПК заступника керівника. Можуть редагуватися працівниками в залежності від прав доступу.
10. Обробка договірної документації. Створюється на ПК заступника директора, бухгалтера або менеджера по роботі з клієнтами та циркулює між ними, передається на розгляд юрисконсульту через мережу Інтернет та друкується.
11. Обробка інформації про конфігурацію мережі та її компонентів. Створюється та обробляється на ПК системного адміністратора та адміністратора безпеки, за необхідності передається на ПК заступника керівника відділення та до центрального офісу через Інтернет.

2.6 Середовище користувачів

За рівнем повноважень щодо доступу до інформації, характером та складом робіт, які виконуються у процесі функціонування ІТС, користувачі поділяються на такі категорії:

- Група 1: користувачі, що мають розширений доступ до ІТС.
- Група 2: користувачі, що мають дозвіл на перегляд, створення та редагування інформації, пов'язаної з бухгалтерськими обліком.
- Група 3: користувачі, що мають дозвіл на перегляд, створення та редагування інформації, пов'язаної зі станом системи та її компонентів.
- Група 4: користувачі, які мають дозвіл на перегляд, створення та редагування інформації про банківські операції.
- Група 5: користувачі, які мають дозвіл на перегляд, створення та редагування інформації про договори.

Суб'єкти доступу до інформації представлені в таблиці.

Таблиця 2.11 - Суб'єкти доступу до інформації

№ п/п	**Посада**	**Роль в ІТС**	**Фізичне розташування**	**Група користувача**
1	Керівник відділенням	Користувач	Кабінет керівника відділенням	Група 1
2	Заступник керівника відділенням	Користувач	Кабінет заст. керівника відділенням	Група 1
3	Системний адміністратор	Адміністр.	Серверна	Група 3
4	Операціоніст	Користувач	Операційний відділ	Група 4
5	Операціоніст	Користувач	Операційний відділ	Група4
6	Операціоніст	Користувач	Операційний відділ	Група 4
7	Операціоніст	Користувач	Операційний відділ	Група 4
8	Головний бухгалтер	Користувач	Відділ бух. обліку	Група 2
9	Бухгалтер	Користувач	Відділ бух. обліку	Група 2
10	Головний економіст	Користувач	Економічний відділ	Група 2

Продовження таблиці 2.11

№ п/п	Посада	Роль в ІТС	Фізичне розташування	Група користувача
11	Економіст	Користувач	Економічний відділ	Група 2
12	Юрисконсульт	Користувач	Юридичний відділ	Група 5
13	Менеджер по роботі з клієнтами	Користувач	Відділ кредитування	Група 5
14	Менеджер по роботі з клієнтами	Користувач	Відділ кредитування	Група 5
15	Адміністратор безпеки	Адміністр.	Серверна	Група 1

У табл. 2.12 вказані дії, які користувачі можуть виконувати відносно інформації.

Таблиця 2.12 – Розмежування прав доступу

№ п/п	Вид інформації	Група 1	Група 2	Група 3	Група 4	Група 5
1	Корпоративні дані про співробітників	Читання, створення, модифікація, видалення	Читання	Читання	Читання	Читання
2	Персональні дані співробітників	Читання, створення, модифікація, видалення	Читання	Читання	Читання	Читання
3	Інформація про послуги, які надає відділення банку	Читання, створення, модифікація	Читання	Читання	Читання	Читання
4	Інформація про графік роботи відділення банку	Читання, створення, модифікація	Читання	Читання	Читання	Читання
5	Статутні документи відділення	Читання, створення, модифікація	Читання	Читання	Читання	Читання

Продовження таблиці 2.12

№ п/п	Вид інформації	Група 1	Група 2	Група 3	Група 4	Група 5
6	Трудові договори	Читання, створення, модифікація, видалення	Читання	Читання	Читання	Читання, створення, модифікація
7	Бухгалтерські звіти	Читання, модифікація	Читання, створення, модифікація, видалення	Читання	Читання	-
8	Інформація про фінансову діяльність відділення	Читання, модифікація	Читання, створення, модифікація, видалення	Читання	-	-
9	Бази даних підприємства	Читання	-	Читання, створення, модифікація	-	-
10	Інформація про конфігурацію мережі та її компонентів	Читання, модифікація	-	Читання, створення, модифікація	-	-
11	Договори з клієнтами	Читання, модифікація	Читання	Читання	Читання	Читання, створення, модифікація
12	Технологічна інформація	Читання, створення, модифікація, оновлення	-	Читання, створення, модифікація	-	-

2.7 Аналіз інформаційних ризиків

Відповідно до Постанови № 95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», банк зобов'язаний запровадити процес управління ризиками інформаційної безпеки в рамках системи управління ризиками банку. Банк має право самостійно визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки. [12]

Аналіз ризиків інформаційної безпеки виконано на основі документу ДСТУ ISO/IEC 27005:2015 - Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) з урахуванням особливостей діяльності організації. Представлений аналіз включає в себе модель порушника. модель загроз, ідентифікація наслідків реалізації загроз, оцінку ризиків та ймовірності їх появи.

2.8 Модель порушника

Порушником вважається особа, яка здійснює спробу несанкціонованого доступу до об'єктів захисту (ознайомлення, модифікація, знищення, тощо). Враховуючи умови функціонування ІТС, потенційними порушниками можуть бути персонал та користувачі АС, які безпосередньо пов'язані із забезпеченням функціонування ІТС, а також обробкою інформації, що підлягає захисту, а також наступні категорії користувачів, які не мають права обробки інформації в АС:

- особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено компоненти ІТС і можуть отримати доступ до ІзОД;
- особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних та можуть здійснити дії щодо порушення діючої в ІТС політики безпеки.

Категорії порушників, що використовуються при створенні моделі, наведено в табл. 2.13. У наступних таблицях наведено специфікації моделі порушника за мотивами здійснення порушень, за рівнем кваліфікації та обізнаності щодо ІТС, за показником можливостей використання засобів ІТС для реалізації загроз, за часом дії та містом дії. Сукупність цих характеристик визначає профіль порушника. У колонці «Рівень загрози» зазначених таблиць наведено рейтингову оцінку загроз порушника. Рівень загрози характеризується наступними категоріями:

1 – незначний;

2 – низький;

3 – середній;

4 – високий;

5 - неприпустимо високий.

Таблиця 2.13 - Категорії порушників, що визначені в моделі

Позначення	**Визначення категорії**	**Рівень загрози**
П1	Авторизовані користувачі ІТС, яким надано право доступу до ІзОД (директор, заступник директора, юрист, головний економіст, головний бухгалтер)	4
П2	Авторизовані користувачі, яким надано повноваження контролювати дії користувачів та персоналу та забезпечувати управління ІТС (адміністратор безпеки)	5
П3	Особи, які забезпечують працездатність технічних і програмних засобів ІТС (системний адміністратор)	4
П4	Особи, яким не передбачено доступ до ІзОД, але які мають доступ до приміщень, де розміщено ІТС і потенційно можуть отримати доступ до ІзОД (операціоністи, менеджери, прибиральниці, охоронці, відвідувачі відділення)	3
П5	Особи, які знаходяться за межами ІТС, мають можливість фізичного підключення до каналів зв'язку та можуть здійснити дії щодо порушення діючої в ІТС політики безпеки	3

Таблиця 2.14 - Специфікація моделі порушника за місцем дії

Позначення	**Характеристика місця дії порушника**	**Рівень загрози**
Д1	Усередині приміщення, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів та персоналу ІТС, а також місць розміщення обладнання ІТС, де обробляється інформація, яка підлягає захисту	5
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами	2

Таблиця 2.15 - Специфікація моделі порушника за рівнем кваліфікації та обізнаності

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
К1	Не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами обробки інформації системи та захисту інформації	1
К2	Має навички щодо користування ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо функціонування програмного забезпечення і операційних систем, а також практичними навичками роботи з засобами обробки інформації	4
К4	Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІТС та їх недоліків	5

Таблиця 2.16 - Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
З1	Має фізичний доступ до компонентів ІТС, але не є авторизованим користувачем ІТС	1
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керування функціонуванням ІТС, тобто конфігурує програмне забезпечення ІТС	5

Таблиця 2.17 - Специфікація моделі порушника за мотивами здійснення порушень

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
М1	Безвідповідальність (недбалість, ненавмисне порушення)	3
М2	Корислива цілеспрямованість (зловмисне порушення)	5

Таблиця 2.18 - Специфікація моделі порушника за часом дії

Позначення	**Основні кваліфікаційні ознаки порушника**	**Рівень загрози**
Ч1	Під час бездіяльності компонентів системи (під час планових перерв у роботі, неробочий час)	4
Ч2	Під час функціонування ІТС	5
Ч3	Під час перерв у роботі для обслуговування та ремонту	3

Профілі порушників всіх категорій наведено в табл. 3.7, у колонці «Рівень загроз» наведено рейтингову оцінку загроз порушника з відповідними характеристиками.

Таблиця 2.19 - Профілі можливостей порушників

Позначення	**Визначення категорії**	**Характер дій порушника**					**Сумарний рівень загроз**
		Мотив порушення	**Кваліфікація**	**Можливості**	**Час дії**	**Місце дії**	
П1	Авторизовані користувачі	М1, М2	К2	З2	Ч1, Ч2	Д2	20
		5	2	3	5	5	
П2	Адміністратор безпеки	М1, М2	К4	З3	Ч1, Ч2, Ч3	Д2	25
		5	5	5	5	5	

Продовження таблиці 2.19

Позначення	**Визначення категорії**	**Характер дій порушника**					**Сумарний рівень загроз**
		Мотив порушення	**Кваліфікація**	**Можливості**	**Час дії**	**Місце дії**	
П3	Персонал, який забезпечує працездатність технічних засобів, в т.ч. системний адміністратор	М2	К3	З1	Ч3	Д1, Д2	22
		5	4	5	3	5	
П4	Особи, які не повинні мати доступу до ІзОД, але мають доступ до приміщень, де розміщено обладнання ІТС і потенційно можуть отримати доступ до ІзОД	М2	К3	З1	Ч1, Ч2	Д1, Д2	20
		5	4	1	5	5	
П5	Особи, які знаходяться за межами ІТС	М2	К3	З1	Ч2	Д3	17
		5	4	1	5	2	

З результатів у табл. 2.19 можна зробити висновок, що найбільшу загрозу, що має відношення до проблеми захисту інформації, становить адміністратор безпеки та Персонал, який забезпечує працездатність технічних засобів. Тому організація роботи цих осіб повинна бути найбільш контрольованою, оскільки вона є основним потенційним порушником безпеки інформації.

2.9 Модель загроз для інформації в ІТС

Для оцінки ймовірності реалізації загроз використовуються наступна шкала:

Таблиця 2.20 - Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	**Характеристика**
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Виникнення інциденту ймовірне до 1 разу на 3 місяці
4	Виникнення інциденту ймовірне до 1 разу на тиждень
5	Виникнення інциденту ймовірне до 1 разу на добу

Значення в стовпчику «Загальна оцінка загрози» табл. 2.21 розраховувались шляхом находження середнього між значенням ймовірності та рівня загрози. В таблиці не розглядаються загрози, що використовують технічні канали витоку інформації (перехоплення побічних електромагнітних випромінювань і наведень, акусто-електричних перетворень інформаційних сигналів, оптичних каналів витоку інформації).

Загрози з загальним рівнем нижче 3 при аналізі ризиків не розглядаються та вважаються незначними.

Таблиця 2.21 - Результати аналізу загроз та вразливостей інформації в ІТС

№ п/п	**Вид загрози**	**Вразливості, що призведуть до реалізації загроз**	**Ймовірність появи**	**Що порушує**	**Рівень загрози**	**Джерело**	**Загальна оцінка загрози**
1. Навмисні загрози							
1.1	Несанкціонований доступ до ІзОД	-порушення правил використання системи -недостатній контроль за діями персоналу	3	К, Ц, Д	3	внутрішнє	3

№ п/п	Вид загрози	Вразливості, що призведуть до реалізації загроз	Ймовірність появи	Що порушує	Рівень загрози	Джерело	Загальна оцінка загрози
1.2	Несанкціоноване копіювання інформації	-відсутність контролю та протоколювання журналу подій -порушення правил політики безпеки	2	К	4	внутрішнє	3
1.3	Викрадення ІзОД шляхом використання електронної пошти	-порушення правил політики безпеки	2	К, Ц, Д	4	внутрішнє	3
1. Випадкові загрози							
2.1	Ненавмисне порушення працездатності КС	-недостатній контроль за цілісністю компонентів системи -недостатній контроль з боку служби охорони	2	Д	2	внутрішнє	2
2.2	Ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	-недостатній контроль за діяльністю працівника (системний адмін., адмін. безпеки)	2	К	3	внутрішнє	2,5
2. Стихійні лиха							
3.1	Повінь	-пошкодження фундаменту будівлі	1	Ц, Д	1	зовнішнє	1,5
3.2	Зсув ґрунту	-пошкодження фундаменту будівлі внаслідок землетрусу, рясних опадів чи діяльності людей	2	Ц, Д	2	зовнішнє	2

Найбільш актуальними загрозами для ОІД вважаються:

- несанкціонований доступ до ІзОД;
- несанкціоноване копіювання інформації;
- викрадення ІзОД шляхом використання електронної пошти;
- ненавмисне порушення працездатності КС;
- ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю.

Якщо ідентифіковані загрози будуть використовувати відповідні вразливості і призведуть до інциденту інформаційної безпеки, негативними наслідками для підприємства може стати повна або часткова втрата інформації, пошкодження або заміна інформації, компрометація інформації. Ці інциденти вплинуть на ресурси підприємства. Таким чином, ресурсам можуть бути приписані значення їх фінансової вартості.

Для оцінки ризиків використані такі шкали:

Таблиця 2.22 - Шкала оцінювання впливу реалізації загрози на конфіденційність

Оцінка рівня наслідків	**Характеристика**
1	Практично не призводить до розкриття конфіденційної інформації
2	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і не призводить до фінансових втрат
3	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до незначних фінансових втрат
4	Призводить до розкриття окремих документів, які відносяться до ІзОД та/або персональних даних і призводить до значних фінансових втрат, може призвести до зупинки роботи системи підприємства
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Таблиця 2.23 - Шкала оцінювання впливу реалізації загрози на цілісність

Оцінка рівня наслідків	**Характеристика**
1	Практично не призводить до наслідків з фінансовими втратами
2	Призводить до незначних фінансових втрат
3	Призводить до значних фінансових втрат
4	Призводить до великих фінансових втрат і може призвести до зупинки роботи системи підприємства
5	Призводить до зупинки роботи системи, порушення вимог нормативно-правової бази

Таблиця 2.24 - Шкала оцінювання впливу реалізації загрози на доступність

Оцінка рівня наслідків	**Характеристика**
1	Практично не впливає на доступність
2	Вплив на доступність незначний (не більше 1/10 від максимально допустимого часу простою)
3	Вплив на доступність середній (не більше 1/4 від максимально допустимого часу простою)
4	Вплив на доступність значний (до максимально допустимого часу простою)
5	Призводить до зупинки роботи системи на тривалий час, який перевищує максимально допустимий час простою)

Таблиця 2.25 - Шкала оцінювання впливу реалізації загрози на спостережність

Оцінка рівня наслідків	**Характеристика**
1	Практично не впливає
2	Вплив незначний

Продовження таблиці 2.25

Оцінка рівня наслідків	**Характеристика**
3	Призводить до неможливості відстежити частину дій користувачів в Системі
4	Призводить до неможливості відстежити дії користувачів і адміністраторів системи
5	Призводить до неможливості відстежити дії всіх кроситувачів і адміністратора системи, може призвести до зупинки роботи системи на тривалий час

Оцінка збитків, що можуть бути нанесені ІТС внаслідок реалізації загроз складається з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості системи внаслідок реалізації загрози. Величина можливих збитків визначається розміром фінансових втрат якісною шкалою, через визначення цього критерія кількісно.

Величина збитків:

1- відсутня,

2- низька,

3- середня,

4- висока,

5- неприпустимо висока.

Для оцінки ризиків використана комбінація кількісних та якісних методів, що дає змогу розрахувати доцільність впровадження політики безпеки, адже вартість заходів безпеки, не мають бути більшими, ніж фінансові втрати інциденту інформаційної безпеки.

Рівень ризику за окремою парою загроза/вразливість визначається перемноженням оцінки ймовірності реалізації на оцінку величини можливих збитків та на максимальну величину з окремих оцінок впливу на цілісність, конфіденційність, доступність, спостережність.

Для створення пари загроза/вразливість, необхідно виокремити найбільш критичну вразливість по загрозі. Рівень критичності вказує наскільки сильним є вплив загрози на ресурс з урахуванням ймовірності її реалізації.

Це виокремлення вразливостей проводяться експертним методом. До загроз, що мають більше однієї вразливості відносяться:

- несанкціонований доступ до ІзОД;
- несанкціоноване копіювання інформації;
- ненавмисне порушення працездатності КС.

Результати оцінки рівня ризику наведені у Таблиці 2.26.

Таблиця 2.26 – Рівень ризику

№	Загроза/ вразливість	Оцінка ймовірності реалізації загрози з використанням вказаної вразливості	Оцінка реалізації загрози на цілісність	Оцінка реалізації загрози на конфіденційність	Оцінка реалізації загрози на доступність	Оцінка реалізації загрози на спостережність	Оцінка величини можливих збитків	Рівень ризику за окремою парою загроза/ вразливість
1	несанкціонований доступ до ІзОД	1	2	2	2	2	3	48
2	несанкціоноване копіювання інформації	2	1	2	1	2	3	24
3	викрадення ІзОД шляхом використання електронної пошти	2	1	3	1	2	3	18
4	ненавмисне порушення працездатності КС	1	2	1	2	2	2	16
5	ненавмисне розголошення конфіденційної інформації або інформації, що становить комерційну таємницю	2	1	2	3	1	2	12

За отриманим максимальним рівнем ризику за окремою парою, складена шкала оцінки ризику для можливості класифікувати ризики за рівнем прийнятності. Шкала оцінки ризику:

- 0-21 малий рівень ризику;
- 22-43 припустимий рівень ризику;
- 44-64 критичний рівень ризику

Отже, найбільш критичними для системи є наступні загрози: несанкціонований доступ до ІзОД та несанкціоноване копіювання інформації. Це необхідно враховувати при створенні організаційних засобів протидії загрозам у контексті розробки політики безпеки.

2.10 Профіль захищеності

Згідно з НД ТЗІ 2.5-005-99. основні загрози для банківської інформації — це в першу чергу загрози шахрайства (підробка, відмова від авторства, відмова від одержання) і порушення технології роботи, а в другу — порушення доступності і конфіденційності. У зв'язку з цим до КЗЗ ОС, що входять до складу банківських АС, пред'являються вимоги щодо забезпечення захисту від зазначених загроз. [10]

Враховуючи характеристики існуючої ІТС та вимог до властивостей інформації, було обрано стандартний функціональний профіль захищеності для системи:

3.КЦД.3 = { КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2 }

Перелік послуг, що входять в обраний профіль захищеності приведено посилаючись на НД ТЗІ 2.5-004-99 [11] зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

КД-2 Базова довірча конфіденційність, відноситься до Критерії конфіденційності - Довірча конфіденційність.

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес).

КА-2 Базова адміністративна конфіденційність, відноситься до Критерії конфіденційності - Адміністративна конфіденційність

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління.

Згідно з політикою адміністративної конфіденційності об'єкту присвоюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі або процеси, які намагаються одержати інформацію. Найбільше розповсюдження отримав механізм, коли у вигляді атрибутів доступу використовуються мітки, що визначають рівень конфіденційності інформації (об'єкта) і рівень допуску користувача. Таким чином КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що здійснює запит на доступ до інформації, авторизованим користувачем.

КО-1 Повторне використання об'єктів, відноситься до Критерії конфіденційності - Повторне використання об'єктів.

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КК-1 Виявлення прихованих каналів, відноситься до Критерії конфіденційності - Аналіз прихованих каналів.

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів.

КВ-3 Повна конфіденційність при обміні, відноситься до Критерії конфіденційності - Конфіденційність при обміні.

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Реалізація даної послуги на рівні КВ-3 дозволяє забезпечити криптографічне розділення каналів обміну і є необхідною для забезпечення взаємодії КЗЗ, що підтримують обробку інформації рівня секретної або реалізують різні політики безпеки.

ЦД-1 Мінімальна довірча цілісність, відноситься до Критерії цілісності – Довірча цілісність.

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену.

На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів).

ЦА-3 Повна адміністративна цілісність, відноситься до Критерії цілісності – Адміністративна цілісність.

Ця послуга дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

ЦО-2 Повний відкат, відноситься до Критерії цілісності – Відкат .

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат.

ЦВ-2 Базова цілісність при обміні, відноситься до Критерії цілісності – Цілісність при обміні.

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування.

Реалізація даної послуги на рівні ЦВ-2 додатково дозволяє керувати засобами експорту і імпорту об'єктів і додатково забезпечує захист від помилок користувача та інших випадкових помилок, а також від модифікації інформації у разі підключенні несанкціонованих користувачів.

ДР-2 Недопущення захоплення ресурсів, відноситься до Критерії доступності - Використання ресурсів.

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Рівень послуги ДР-2 являє собою реалізацію досконалішої форми квот. Квоти використовуються таким чином, щоб гарантувати, що жоден користувач не зможе захопити решту певного ресурсу, дозволяючи виділяти менші обсяги ресурсів, ніж максимальна квота користувача, гарантуючи таким чином іншому користувачеві доступ до розділюваного ресурсу.

ДС-1 Стійкість при обмежених відмовах, відноситься до Критерії доступності - Стійкість до відмов.

Стійкість до відмов гарантує доступність КС (можливість використання інформації, окремих функцій чи КС в цілому) після відмови її компоненту. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість КС продовжувати функціонування залежно від кількості відмов і послуг, доступних після відмови.

ДЗ-1 Модернізація, відноситься до Критерії доступності - Гаряча заміна.

Ця послуга дозволяє гарантувати доступність КС (можливість використання інформації, окремих функцій або КС в цілому) в процесі заміни окремих компонентів. Рівні даної послуги ранжируються на підставі повноти реалізації.

Основна мета реалізації даної послуги полягає в тому, що встановлення нової версії системи, відмова або заміна захищеного компонента не повинні призводити до того, що система потрапить до стану, коли політика безпеки, що реалізується нею, стане скомпрометованою.

ДВ-2 Автоматизоване відновлення, відноситься до Критерії доступності - Відновлення після збоїв.

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

НР-3 Сигналізація про небезпеку, відноситься до Критерії Спостережності – Реєстрація.

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НИ-2 Одиночна ідентифікація і автентифікація, відноситься до Критерії Спостережності – Ідентифікація і автентифікація.

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ранжируються залежно від числа задіяних механізмів автентифікації.

НК-1 Однонаправлений достовірний канал, відноситься до Критерії Спостережності – Достовірний канал.

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ранжируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НО-2 Розподіл обов'язків адміністраторів, відноситься до Критерії Спостережності – Розподіл обов'язків.

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ран жируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

НЦ-3 КЗЗ з функціями диспетчера доступу, відноситься до Критерії Спостережності – Цілісність комплексу засобів захисту.

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Для рівня НЦ-3 необхідно, щоб КЗЗ забезпечував керування захищеними ресурсами таким чином, щоб не існувало можливості доступу до ресурсів, минаючи КЗЗ. Дана вимога є другою функціональною вимогою до реалізації диспетчера доступу.

НТ-2 Самотестування при старті, відноситься до Критерії Спостережності – Самотестування.

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

НВ-2 Автентифікація джерела даних, відноситься до Критерії Спостережності – Ідентифікація і автентифікація при обміні.

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

Реалізація рівня НВ-2 даної послуги дозволяє виключити можливість несанкціонованого використання встановленого авторизованого підключення.

2.11 Розробка основних елементів політики безпеки

За результатами створених моделі порушника та загроз, виконаної оцінки ризиків, обстеження фізичного, обчислювального і інформаційного середовища, було розроблено основні складові політики безпеки інформації.

Як складові частини загальної політики безпеки в АС мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації.

Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів АС), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів АС політика безпеки стосується, а яких – ні).

Загальні правила, яких слід дотримуватися при розробці ПБ:

- У системі необхідно ввести чіткі правила розмежування прав доступу.. Інформаційний ресурс, що підлягає захисту повинен мати свій атрибут доступу, на підставі якого здійснюється організація прав доступу користувача до інформаційного ресурсу.
- У системі повинна виконуватися однозначна ідентифікація та автентифікація користувачів. Автентифікація користувача повинна відбуватися за допомогою захищених механізмів, перш ніж дозволити користувачеві виконувати будь-які дії в системі.
- Для зменшення потенційних збитків від навмисних або випадкових дій адміністратора безпеки бажано обмежити авторитарність адміністратора.

Для цього необхідно визначити рівні доступу адміністратора безпеки та користувачів системи і встановити перелік функціональних можливостей та обов'язків користувачів та адміністратора.

- З метою зменшення рівня загроз, пов'язаних з людським фактором, необхідно організувати процес навчання, контролю та перепідготовки персоналу за напрямом забезпечення безпеки інформації.
- Для захисту інформації в системі від комп'ютерних вірусів необхідно використовувати антивірусне програмне забезпечення. Для коректної роботи програми необхідно регулярно проводити оновлення баз даних сигнатур з достовірного джерела.
- Необхідно відстежувати ризики інформаційної безпеки та вживати необхідні дії, коли чинники призводять до виникнення непередбачуваних ризиків.
- Інциденти інформаційної безпеки не повинні призводити до серйозних непередбачуваних втрат або до суттєвих перешкод діяльності відділення.

Розроблена політика безпеки складається з таких розділів:

1. Вступ: означено стурбованість керівництва відділення банку проблемами забезпечення інформаційної безпеки.
2. Терміни та поняття: надано пояснення щодо термінів та понять, які вжиті у ПБ.
3. Ціль політики: вказана ціль впровадження політики безпеки інформації.
4. Сфера застосування: вказано персонал банку та бізнес-процеси, на які розповсюджується ПБ; встановлено організаційні вимоги, спрямовані на забезпечення безпеки інформації.
5. Ролі та обов'язки: визначені основні ролі співробітників відділення банку та їх посадові обов'язки і повноваження стосовно забезпечення безпеки інформації.

6. Перегляд документу: вказано порядок перегляду політики інформаційної безпеки та змін/доповнень до ПБ.
7. Дотримання політики: визначено відповідальних за контроль та дотримання користувачами ПБ та відповідальність за несанкціоноване втручання в роботу ІТС банку.
8. Додаткові документи: визначено правила розмежування доступу та порядок використання змінних носіїв інформації (флеш-накопичувачів).

Розроблена політика безпеки наведена у Додатку 5. Створення ПБ затверджено наказом (Додаток 4).

Висновки до розділу 2

У другому розділі було описано об'єкт інформаційної діяльності, рід діяльності об’єкту, інформаційна система, інформаційні потоки, апаратне та програмне забезпечення. У технічному завданні виконаний аналіз структури ІТС, аналіз наявних вразливостей у системі та загальної моделі загроз, розроблена модель порушника, інформаційних потоків. Виконано вибір профілю захищеності відділення.

У результаті проведеного обстеження ОІД було побудовано модель загроз, що можуть бути реалізовані в ІТС, було класифіковано інформацію, що зберігається і циркулює на відділенні та виявлено активи, які потребують найбільшого рівня інформаційної безпеки. За отриманими результатами було розроблено політику безпеки у відділенні АТ КБ «Dniprobank».

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою виконання економічного розділу кваліфікаційної роботи є економічне обґрунтування доцільності впровадження політики безпеки відділенням комерційного банку.

Для цього визначено економічну ефективність використання основних результатів, що отримані в результаті виконання роботи.

Економічна доцільність визначається розрахунками:

- капітальних витрат, що потребує розроблена політика безпеки;
- експлуатаційних витрат;
- річного економічного ефекту від впровадження інформаційної політики безпеки.

Запропонована політика інформаційної безпеки передбачає необхідність витрат на її реалізацію. Заходами, що потребують витрат, є:

- оновлення ліцензій програмного забезпечення;
- навчання персоналу в питаннях інформаційної безпеки;

3.2 Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ год} \quad (3.2)$$

Де $t_{тз}$ = 4 год - тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ = 3 год - тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ = 3 год – тривалість процесу аналізу ризиків;

$t_{вз}$ = 4 год – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ = 3 год – тривалість вибору основних рішень з забезпечення безпеки інформації;

tовр = 2 год – тривалість організації виконання відновлювальних робіт забезпечення неперервного функціонування організації;

tд = 4 год.– тривалість документального оформлення політики безпеки.

t = 4 год + 3 год + 3 год + 4 год + 3 год + 2 год + 4 год = 23 год

3.3 Розрахунок витрат на створення політики безпеки

$$Крп = Ззп + Змч, \quad (3.3)$$

де Крп – витрати на створення політики безпеки;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для створення політики безпеки.

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$Ззп = t * Зіб = 23 * 125 = 2875 \text{ грн}$$

де t – загальна тривалість розробки політики безпеки, год;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 125 грн/год.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t * Смч, \text{грн}$$

де t – трудомісткість розробки політики безпеки інформації на ПК, год;

Смч – вартість 1 години машинного часу ПК, грн/год.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = Р * tнал * Се + \frac{Фзал * На}{Fр} + \frac{Клпз * Напз}{Fр} =$$

$$= 0,2 * 2 * 1,68 + \frac{(7000 * 0,2)}{1920} + \frac{5000 * 0,2}{1920} =$$

$$= 0,67 + 0,73 + 0,52 = 1,92 \text{ грн/год},$$

Де Р- встановлена потужність апаратури інформаційної безпеки, 0.3 кВт - середня потужність одного комп'ютера;

tнал – кількість машин на яких розроблюється політика безпеки;

Се – тариф на електричну енергію, 1,68 грн/кВт·год;

Фзал – залишкова вартість ПК на поточний рік, 7000 грн;

На – річна норма амортизації на ПК, 0.2 частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, 0,2 частки одиниці;

Клпз – вартість ліцензійного програмного забезпечення, 5000 грн;

Fр – річний фонд робочого часу (за 40-годинного робочого тижня Fр = 1920 год)

$$Змч = t * Смч = 23 * 1,92 = 44,16 \text{ грн}$$

$$Крп = Ззп + Змч = 2875 + 44,16 = 2919,16 \text{ грн}$$

3.4 Розрахунок (фіксованих) капітальних витрат:

Оновлення ліцензії системного, прикладного і спеціалізованого ПЗ: Avast Antivirus Pro Plus - 1700 грн (вартість ліцензії для одного ПК на рік), Windows 10 Pro — 2500 грн на рік, MS Office 2016 – 1200 грн на рік, Diasoft FA# Beans – 1500 грн на рік, Flextera BI – 1300 грн на рік. Необхідно оновлення ПЗ для 15 комп'ютерів.

Загальна вартість закупівель ліцензійного ПЗ:

$$Кзпз = 15 * 6500 \text{ грн} = 97500 \text{ грн} \quad (3.4)$$

Таким чином, капітальні (фіксовані) витрати на впровадження системи інформаційної безпеки складають:

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн,$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 105000 тис. грн;

Каз – вартість закупівель апаратного забезпечення та допоміжних матеріалів відсутня, оскільки за розробленими політики безпеки закупівля апаратного забезпечення не є необхідною.

Кнавч - витрати на навчання адміністратора безпеки, становлять 2000 грн.

Крп – вартість розробки політики безпеки інформації, 2919,16 тис. грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки відсутні, оскільки не закуповується апаратне забезпечення.

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн =$$
$$= 2919{,}16 + 97500 + 2000 = 102419{,}16 \text{ грн}$$

3.5 Розрахунок поточних (експлуатаційних) витрат:

- навчання персоналу в питаннях інформаційної безпеки;
- витрати на керування системою інформаційної безпеки.

1. Витрати на навчання персоналу в питаннях інформаційної безпеки включають в себе послуги сторонніх організацій, що створюють політику безпеки

інформації та відповідно до неї розробляють інструкції для персоналу, що є користувачами системи. Вартість навчання адміністративного персоналу й кінцевих користувачів розглянутої системи:

Со = 5000 грн – витрати на навчання персоналу.

2. Обов'язки з керування системою інформаційної безпеки виконує керівник та адміністратор безпеки (за відсутності керівника), тому річний фонд заробітної плати складає додаткову заробітну плату директора та системного адміністратора за рік:

$$Сз = Зк + Заб = 1500 + 1000 = 2500 \text{ грн (за 1 місяць)} \qquad (3.5)$$

$$Сз = 2500 * 12 = 30000 \text{ грн (за 1 рік)}$$

де Зк – додаткова заробітна плата керівника, 18000 грн на рік.

Заб – додаткова заробітна плата адміністратора безпеки, 12000 грн. на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року (Се), визначається за формулою:

$$Се = Р * Fp * Це$$

де Р – встановлена потужність апаратури інформаційної безпеки (0,3 кВт*15 комп'ютерів = 4,5 кВт)

Fр = 12 міс * 20 робочих діб/міс * 8 робочих годин * 15 комп'ютерів = 28800 год – річний фонд робочого часу системи інформаційної безпеки;

Це = 1,68 грн за 1 кВт/год – тариф на електроенергію на 01.01.2022 року.

$$Се = 4{,}5 * 28800 * 1{,}68 = 217728 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) визначаються у відсотках від вартості капітальних витрат (2%).

$$\text{Стос} = \text{К} * 0{,}02 = 102419{,}16 * 0{,}02 = 2048{,}4 \text{ грн}$$

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$\text{С} = \text{Со} + \text{Сз} + \text{Се} + \text{Стос} =$$
$$= 5000 + 30000 + 217728 + 2048{,}4 = 254776{,}4$$

Розрахунок оцінки величини збитку:

Втрати від зниження продуктивності співробітників атакованої системи мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки (Пп).

Таблиця 3.1 Заробітні плати працівників за місяць

Посада	**Розмір зар. плати**	**Кількість співробітників**	**Витрати на зар. плату на міс., грн**
Керівник відділенням	27000	1	27000
Заступник керівника відділенням	21000	1	21000
Адміністратор безпеки	20000	1	20000
Системний адміністратор	15000	1	15000
Головний бухгалтер	16000	1	16000
Бухгалтер	13000	1	13000
Головний економіст	16000	1	16000

Продовження таблиці 3.1

Посада	**Розмір зар. плати**	**Кількість співробітників**	**Витрати на зар. плату на міс., грн**
Економіст	13000	1	13000
Юрисконсульт	15000	1	14000
Операціоніст	13000	4	52000
Менеджер по роботі з клієнтами	13000	4	52000
		Сума	1546000

Місячний фонд робочого часу складає 160 годин. Річний – 1920 годин. Час простою внаслідок атаки tп = 4 год.

$$Пп = (Зс/Fр) * tв = (1546000/160) * 4 = 38650 \text{ грн}$$

Витрати на відновлення працездатності системи включають кілька складових:

Пви – витрати на повторне введення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частин системи, грн.

Витрати на повторне введення інформації розраховуються виходячи з розміру заробітної плати співробітників системи Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви = 8 год:

$$Пви = (1546000/160) * 8 = 77300 \text{ грн}$$

Витрати на відновлення системи визначаються часом відновлення після атаки tв = 4 год і розміром середньогодинної заробітної плати адміністратора безпеки:

$$Ппв = (20000/160) * 4 = 500$$

Витрати на відновлення працездатності системи:

$$Пв = Пви + Ппв + Пзч = 77300 + 500 + 5500 = 83300 \text{ грн}$$

Пзч = 5500 грн - вартість для витрат на заміну частин;

О = 6500000 грн - обсяг чистого прибутку за рік.

Втрати від зниження працездатності атакованої системи:

$$V = О/Fр * (tп + tв + tви) = 6500000/1920 * (3 + 4 + 8) = 50781{,}25 \text{ грн}$$

Fr – це річний фонд часу роботи відділення, 1920 годин;

tп – 4 годин простою після атаки;

tв – 4 годин відновлення після атаки;

tви – 8 годин повторного введення загубленої інформації під час атаки;

Таким чином, загальний збиток від атаки на ІТС відділення при реалізації загрози складе:

$$U = Пп + Пв + V = 38650 + 83300 + 50781{,}25 = 172731{,}25 \text{ грн}$$

Таким чином, загальний збиток від атак на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n * U = 3 * 4 * 172731{,}25 = 2072775 \text{ грн}$$

де: і- число атакованих вузлів, 3 комп'ютери;

n – середнє число атак на рік, 4 рази.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням B – загального збитку від атаки; R – очікуваної ймовірності атаки на систему; C – щорічних витрат на експлуатацію системи інформаційної безпеки.

Ймовірність R (0…1). Якщо реалізація загроз наймовірніша 1 раз на 3 місяці, тобто 4 рази на рік, то R=0,25.

Загальний ефект від впровадження політики безпеки:

$$E = B * R - C = 2072775 * 0{,}25 - 254776{,}4 = 263417{,}35 \text{ грн}$$

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки:

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій To.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі.

Коефіцієнт ROSI розраховують за допомогою показників:

E – загальний ефект від впровадження системи інформаційної безпеки тис. грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

$$ROSI = E/K = 263417,35/102419,16 = 2,57$$

Термін окупності капітальних інвестицій показує, за скільки років інвестиції окупляться за рахунок загального ефекту від впровадження ПБ.

$$To = K/E = 1/ ROSI = 1 / 2,57 = 0,38 \text{ років} = 4,5 \text{ місяців.}$$

Висновки до розділу 3

Розробка і впровадження політики інформаційної безпеки для відділення АТ КБ «Dniprobank» можна назвати економічно доцільними, так як витрати на її створення значно менші за суму збитків, завдяки невеликій вартості комплектуючих, необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників.

Тому в результаті:

- капітальні витрати на впровадження інформаційної політики безпеки становлять 102419,16 грн;
- експлуатаційні витрати на впровадження інформаційної політики безпеки становлять 254776,4 грн.;
- загальний збиток від атаки на вузол складає 2072775 грн;
- ефект від впровадження системи інформаційної безпеки становить 263417,35 грн;
- термін окупності капітальних інвестицій складатиме 4.5 місяців.

Отже, економічна доцільність обґрунтована і впровадження інформаційної політики безпеки може бути ефективною та успішною.

ВИСНОВКИ

Було розглянуто суттєві загрози та стан злочинів в сфері інформаційної безпеки та статистика реалізованих атак за 2021 рік в Україні. Виявлено значна кількість інцидентів порушення інформаційної безпеки на території України. Зазначена необхідність розвитку кібербезпеки. Було обґрунтовано потребу у створенні КСЗІ у відділенні банку для запобігання НСД до важливих ресурсів системи.

Відповідно до нормативної документації, до етапів створення КСЗІ, які використані в роботі, віднесені: обґрунтування необхідності створення КСЗІ, обстеження на ОІД, аналіз та оцінка інформаційних ризиків та розробка політики безпеки, що враховує загрози усіх рівнів.

У результаті проведеного обстеження ОІД було побудовано модель загроз, що можуть бути реалізовані в ІТС, було класифіковано інформацію, що зберігається і циркулює у відділенні. Проведено аналіз ризиків з урахуванням критичності бізнес-процесів.

У економічному розділі було проведено розрахунок капітальних та експлуатаційних витрат на розробку та впровадження ПБ.

Отримані результати були використані для розробки політики безпеки у відділенні АТ КБ «Dniprobank».

ПЕРЕЛІК ПОСИЛАНЬ

1. SWOT-аналіз стану інформаційної безпеки України / Вознюк Є.; [Електронний ресурс] – Режим доступу до ресурсу: https://sj.npu.edu.ua/index.php/pnspd/issue/view/51/19
2. Кібербезпека України: аналіз сучасного стану / Трофименко О., Прокоп Ю., Логінова Н., Задерейко О.; [Електронний ресурс] – Режим доступу до ресурсу:http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y
3. ЗУ "Про інформацію"; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12
4. ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах»; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80;
5. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125-18-1 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручинін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с. [Електронний ресурс] – Режим доступу до ресурсу: https://bit.nmu.org.ua/ua/student/diplom/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%9A%D0%A0%D0%91_125_2020.pdf
6. Постанова КМУ від 29 березня 2006 р. №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». [Електронний ресурс] – Режим доступу до ресурсу - Режим доступу https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text;
7. НД ТЗІ «Термінології в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99» [Електронний ресурс] – Режим доступу до ресурсу - https://tzi.ua/assets/files/1.1_003_99.pdf
8. НД ТЗІ «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003 -2005»

[Електронний ресурс] – Режим доступу до ресурсу - https://tzi.com.ua/downloads/3.7-003-2005.pdf

9. ДСТУ 3396.1-96 - Технічний захист інформації. Порядок проведення робіт; [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
10. НД ТЗІ «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу НД ТЗІ 2.5-005 -99» [Електронний ресурс] – Режим доступу до ресурсу - https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf
11. НД ТЗІ «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99» [Електронний ресурс] – Режим доступу до ресурсу - https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
12. Постанова № 95 від 28.09.2017 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України» [Електронний ресурс] – Режим доступу до ресурсу - https://zakon.rada.gov.ua/laws/show/v0095500-17#Text
13. Типове положення про службу захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу до ресурсу - https://tzi.com.ua/downloads/1.4-001-2000.pdf
14. Річний звіт Державного центру кіберзахисту - [Електронний ресурс] – Режим доступу до ресурсу - https://cip.gov.ua/ua/news/321f4bf8
15. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки - [Електронний ресурс] – Режим доступу до ресурсу - https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf
16. Методичні вказівки до виконання економічної частини дипломного проекту для студентів спеціальності 125 Кібербезпека / Упоряд.: Д.П. Пілова, доц., канд. екон. наук – Дніпро: НТУ «ДП», 2019 – 16 с.

Додаток 1. Акт категоріювання

Затверджую
Керівник АТ КБ «Dniprobank»
Петренко І.Д
__.__.20__
М.П.

АКТ
Категоріювання ___АТ КБ «Dniprobank»_____ (найменування об'єкта категоріювання)

1. Підстава для категоріювання - рішення про створення КСЗІ №17 від 26.09.2021р_____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання
_____первинне_____
(первинне, чергове, позачергове)
_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється
_____обробка інформації технічними засобами та озвучування_____
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
_____конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія ___4 категорія (до 4 категорії відносяться об’єкти, в яких циркулює службова та конфіденційна інформація, вимога щодо захисту якої встановлена законом)_____

Керівник Петренко І.Д

Додаток 2. Наказ про створення КСЗІ

Н А К А З

м. Дніпро

26.09.2021 № 17

Про створення комплексної системи захисту інформації в автоматизованій системі класу «3» ІТС АТ КБ «Dniprobank»

На виконання вимог статті 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами) та п.16 «Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджених Постановою Кабінету Міністрів України від 26.03.2006 року №373 (зі змінами)

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі класу «3» для обробки інформації з обмеженим доступом.
2. Відповідальному за службу захисту інформації в автоматизованих системах Орленко С.С., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.

Директор Петренко І.Д

Додаток 3. Наказ про встановлення КЗ

Н А К А З

м. Дніпро

20.11.2021 № 28

Про встановлення контрольованої зони

За результатами обстеження обчислювальної системи, фізичного середовища, середовища користувачів, оброблювальної інформації та технології її обробки

НАКАЗУЮ:

1. Встановити контрольовану зону в межах приміщення АТ КБ «Dniprobank», що знаходиться за адресою: м. Дніпро, пр. Дмитра Яворницького, буд. 23.

Директор Петренко І.Д

Додаток 4. Наказ про затвердження ПБ

Н А К А З

м. Дніпро

19.12.2021 № 46

Про затвердження політики безпеки інформації АТ КБ «Dniprobank»,

За результатами обстеження обчислювальної системи, фізичного середовища, середовища користувачів, оброблювальної інформації та технології її обробки

НАКАЗУЮ:

1. Затвердити «Політику безпеки інформації АТ КБ «Dniprobank», що знаходиться за адресою: м. Дніпро, пр. Дмитра Яворницького, буд. 23.

Директор Петренко І.Д

Додаток 5. Розроблена політика безпеки

ЗАТВЕРДЖЕНО

Наказом керівника АТ КБ «Dniprobank»
від 01.02.2022 р. №71

ПОЛІТИКА
безпеки інформації ІТС АТ КБ «Dniprobank»

Дніпро-2022

1. ВСТУП

Політика інформаційної безпеки ІТС АТ КБ «Dniprobank» (далі Політика) є внутрішнім нормативним документом, який містить звід законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на забезпечення захисту інформації від певного виду загроз. Політика містить мінімальні вимоги щодо організації заходів із забезпечення інформаційної безпеки ІТС АТ КБ «Dniprobank»

Політика є нормативною основою для захисту інформаційних активів Банку з метою забезпечення:

конфіденційності – забезпечення доступності інформації, активів тільки для авторизованих осіб, користувачів, процесів в мінімально необхідному обсязі;

цілісності – захисту точності, коректності та повноти активів і методів обробки інформації;

доступності – забезпечення безперервного доступу до інформаційних і супутніх активів і сервісів Банку, згідно з наданими користувачам повноваженням і правами у мінімально необхідному обсязі та мінімізації збитків в разі їх порушення.

2. ТЕРМІНИ ТА ПОНЯТТЯ

В цій Політиці терміни та поняття вживаються в таки значеннях:

Інформаційна безпека (ІБ) – сукупність процесів, засобів та заходів, які мають на меті забезпечення цілісності, конфіденційності, доступності інформації.

Заходи безпеки – засоби керування ризиком, включаючи політики, процедури, інструкції, практики та організаційну структуру, які можуть носити адміністративний, технічний, управлінський, методологічний чи юридичний характер.

Загроза - будь-які обставини чи події, що можуть спричинити порушення ІБ та нанесення збитку Банку.

Вразливість - нездатність протистояти реалізації певної загрози або ж сукупності загроз.

Ризик ІБ (ризик) – ймовірність того, що визначена загроза, впливаючи на вразливості системи або групи систем, може спричинити шкоду Банку.

Інші терміни, що вживаються в цій Політиці, використовуються в значеннях, визначених законами України, нормативно-правовими актами в сфері технічного захисту інформації в т.ч. НД ТЗІ 1.1-003-99.

3. ЦІЛЬ ПОЛІТИКИ

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційної безпекою, у тому числі визначення ролей та обов'язків у галузі ІБ, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями співробітників Банку, забезпечучення безперервної роботи Банку, сприяння мінімізації ризиків інформаційної безпеки Банку.

4. СФЕРА ЗАСТОСУВАННЯ

Дія Політики розповсюджується на весь персонал АТ КБ «Dniprobank» у цілому та використовується для всіх бізнес-процесів, які можуть негативно вплинути на результати діяльності АТ КБ «Dniprobank».

Ця Політика встановлює організаційні вимоги, спрямовані на забезпечення безпеки інформації в ІТС АТ КБ «Dniprobank».

Принцип забезпечення інформаційної безпеки АТ КБ «Dniprobank»:

1) підхід до забезпечення інформаційної безпеки має бути системним (комплексним);

2) процес удосконалення та розвитку інформаційної безпеки має бути безперервним і здійснюватися шляхом обгрунтування та реалізації раціональних засобів, методів, заходів;

3) заходи захисту від реальних та потенційних загроз інформаційній безпеці ІТС АТ КБ «Dniprobank» мають бути своєчасні й адекватні, в т.ч. у фінансовому плані.

5. РОЛІ ТА ОБОВ'ЯЗКИ

5.1 Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку та сприяє (організаційно та фінансово) впровадженню, контролю та підтримці вимог прийнятої Політики.

Документи системи управління інформаційною безпекою розробляються відділом інформаційної безпеки та іншими структурними підрозділами Банку за відповідними напрямками діяльності.

Документи системи управління інформаційною безпекою доступні співробітникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на відділ інформаційної безпеки Банку.

Кожний співробітник Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов'язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України та внутрішньобанківськими нормативними документами.

5.2 Керівник АТ КБ «Dniprobank» на підставі вимог чинного законодавства України в сфері захисту інформації, НД ТЗІ призначає на посаду адміністратора безпеки інформації та забезпечує:

1) стратегічне керівництво з питань інформаційної безпеки АТ КБ «Dniprobank»;
2) визначення напрямів розвитку інформаційної безпеки АТ КБ «Dniprobank» відповідно до вимог чинного законодавства України в сфері захисту інформації;
3) відповідність заходів безпеки інформації потребам бізнес-процесів;

4) контроль за впровадженням заходів безпеки інформації в АТ КБ «Dniprobank»;
5) організацію процесу навчання, контролю та перепідготовки персоналу за напрямом забезпечення безпеки інформації.

Забезпечення захисту інформації в АС здійснює призначений наказом керівника АТ КБ «Dniprobank» адміністратор безпеки, до функціональних обов'язків якого включено положення, які передбачають виконання вимог щодо забезпечення безпеки інформації.

Посадові обов'язки адміністратора безпеки включають в себе:

- розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій;
- вживаня заходів у разі виявлення спроб НСД до ресурсів АС, порушенні правил експлуатації засобів захисту інформації або інших дестабілізуючих факторів;
- забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід з ладу або порушення режимів функціонування;
- організацію керування доступом до ресурсів АС (розподілення між користувачами необхідних реквізитів захисту інформації – паролів, привілеїв, ключів та ін.);
- супроводження і актуалізація бази даних захисту інформації (матриці доступу, ідентифікатори користувачів тощо);
- спостереження (реєстрація і аудит подій в АС, моніторинг подій тощо) за функціонуванням ІТС та її компонентів;
- підготовку пропозицій щодо удосконалення порядку забезпечення захисту інформації в АС, впровадження нових технологій захисту і модернізації;
- організацію та проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій АС або КСЗІ;

- інформування власників інформації про технічні можливості захисту інформації в АС і типові правила, встановлені для персоналу і користувачів АС;
- негайне втручання в процес роботи АС у разі виявлення атаки на інформаційну систему, проведення у таких випадках робіт з викриття порушника;
- регулярне подання звітів керівництву про виконання користувачами АС вимог з захисту інформації;
- контроль за виконанням персоналом і користувачами АС вимог, норм, правил, інструкцій з захисту інформації відповідно до визначеної політики безпеки інформації;

5.3 Повноваження й обов'язки користувачів при експлуатації ресурсів комп'ютерної мережі АТ КБ «Dniprobank»:

1) користуватися ресурсами комп'ютерної мережі згідно наданих повноважень та у відповідності до посадових обов'язків;
2) виконувати вимоги адміністратора безпеки відповідно до цієї Політики й інших нормативних документів;
3) використовувати зареєстровані матеріальні носії інформації;
4) змінювати свої паролі доступу до ресурсів комп'ютерної мережі відповідно до парольної політики;
5) виконанувати вимоги нормативно-правових актів щодо інформаційної безпеки;
6) повинні вживати всіх можливих заходів безпеки з метою запобігання чи зменшення втрат чи збитків.

6. ПЕРЕГЛЯД ДОКУМЕНТУ

Перегляд даної Політики повинен проводитися не рідше, ніж 1 раз на 12 місяців.

Внесення змін/доповнень до Політики інформаційної безпеки здійснюється після узгодження з наступними керівниками:

- керівник відділенням;
- адміністратор інформаційної безпеки.

Внесення змін/доповнень до Політики інформаційної безпеки здійснюється відповідальною особою у наступних випадках:

- при змінах в документах, на підставі яких розроблено Політику;
- при впровадженні нових документів, що змінюють/впливають на процеси, описані в Політиці;
- при зміні ролей, відповідальності та процесів, що встановлює дана Політика;
- щорічно, за необхідності актуалізації найменувань документів, на які посилається ця Політика;

Цей документ набуває чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні керівництва, яким документ затверджується.

Зміни та доповнення до цього документу набувають чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні керівництва, яким документ затверджується. Усі зміни та доповнення до цього документу є його невід'ємною частиною.

Дана редакція цього документу втрачає свою чинність з дати набрання чинності наступної/нової редакції цього документу або на підставі рішення керівництва.

7. ДОТРИМАННЯ ПОЛІТИКИ

7.1 Керівник відділенням та адміністратор безпеки відповідальні за контроль та дотримання користувачами ІТС АТ КБ «Dniprobank» даної Політики.

7.2 Співробітники відділення під час прийому на роботи ознайомлюються з вимогами даної Політики під розпис.

7.3 Вимоги даної Політики є обов'язковими для виконання всіма користувачами системи.

7.4 Несанкціоноване втручання в роботу інформаційно-телекомунікаційної системи АТ КБ «Dniprobank» несе за собою адміністративну чи кримінальну відповідальність.

8. ДОДАТКОВІ ДОКУМЕНТИ

8.1 Політика розмежування доступу.

8.2 Політика використання змінних носіїв інформації (флеш-накопичувачів).

Додаток 6. Політика розмежування доступу

ПОЛІТИКА РОЗМЕЖУВАННЯ ДОСТУПУ

1. Опис

Політика розмежування прав доступу регламентує правила доступ користувачів і процесів до пасивних об'єктів.

2. Мета

Надання доступу до інформації користувачам, яким він необхідний згідно з посадовими інструкціями.

3. Галузь застосування

Відноситься до всіх користувачів системи.

4. Інструкція

Відповідно до НД ТЗІ 1.4-001-2000, мають виконуватися наступні дії:

- кожне робоче місце повинно мати свого користувача, який несе відповідальність за його працездатність та за дотримання всіх вимог і процедур, пов'язаних з обробкою інформації та її захистом. Користувач повинен бути забезпечений відповідними інструкціями і навчений всім вимогам і процедурам;
- для попередження неавторизованого доступу до даних, ПЗ, інших ресурсів, керування механізмами захисту здійснюється адміністратором безпеки;
- за всі зміни ПЗ, створення резервних і архівних копій несе відповідальність адміністратор безпеки. Такі роботи виконуються за його дозволом;
- кожний користувач має свій унікальний ідентифікатор і пароль.

Право видачі цих атрибутів надається системному адміністратору. Атрибути для системного адміністратора надає адміністратор безпеки.

Видача атрибутів дозволяється тільки після документальної реєстрації особи як користувача;

- користувачі проходять процедуру автентифікації для отримання доступу до ресурсів ІТС;
- атрибути користувачів змінюються двічі на рік , а невикористовуванні і скомпрометовані – видаляються.

Додаток 7. Політика використання змінних носіїв інформації

ПОЛІТИКА ВИКОРИСТАННЯ ЗМІННИХ НОСІЇВ ІНФОРМАЦІЇ (ФЛЕШ-НАКОПИЧУВАЧІВ)

1. Опис

Флеш-накопичувачі використовується практично в усіх галузях і часто є основним засобом зберігання, перенесення та резервного копіювання. У той же час, неправильне використання флеш-накопичувачів може спричинити багато ризиків, що стосуються інформаційної безпеки, тому для користувача необхідно розуміти важливість належного використання змінних носіїв інформації.

2. Мета

Метою даної політики є забезпечення правильного використання користувачами АТ КБ «Dniprobank» змінних носіїв інформації (флеш-накопичувачів), та інформувати їх про те, що саме АТ КБ «Dniprobank» вважає прийнятним і неприйнятним при використанні змінних носіїв інформації. Ця політика визначає мінімальні вимоги до використання флеш-накопичувачів у ІТС.

3. Галузь застосування

Ця політика охоплює належне використання змінних носіїв інформаціїі застосовується до всіх співробітників АТ КБ «Dniprobank»

3. Інструкція

Керівник АТ КБ Dniprobank» зобов'язаний здійснювати контроль за:

- використанням змінних носіїв інформації, включаючи процедури їх обліку та виведення з експлуатації;
- категоріями інформації, яка може оброблятися на змінних носіях інформації;
- ідентифікацією змінних носіїв інформації, які використовуються у відділенні;

- обмеженням використання змінних носіїв інформації;
- забезпеченням обов'язкової ідентифікації змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія.

Працівники АТ КБ Dniprobank» зобов'язані:

- здійснювати обов'язкову перевірку змінних матеріальних носіїв інформації на наявність вірусів перед використанням на ПК;
- обов'язково використовувати стандартний засіб шифрування диску BitLocker Drive Encryption, який входить до складу операційної системи Windows 10 Pro, для шифрування інформації, що міститься на змінних носіях інформації;
- змінювати пароль доступу до змінних матеріальних носіїв інформації раз на 6 (шість) місяців.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи.

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	49	
7	А4	Економічна частина	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток 1	1	
11	А4	Додаток 2	1	
12	А4	Додаток 3	1	
13	А4	Додаток 4	1	
14	А4	Додаток 5	8	
15	А4	Додаток 6	2	
16	А4	Додаток 7	2	
17	А4	Додаток А	1	
18	А4	Додаток Б	1	
19	А4	Додаток В	1	
20	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії.

1. Агашкова_КО_125_18_1_ПЗ.docx
2. Агашкова_КО_125_18_1_ПЗ.pdf
3. Агашкова_КО_125_18_1_ДМ.pptx
4. Агашкова_КО_125_18_1_ПЗ.pdf.p7s

ДОДАТОК В. Відгуки керівників розділів.

Відгук керівника економічного розділу

Економічний розділ виокнаний відповідно до вимог, які ставляться до кваліфакаційних робіт, та заслуговує на оцінку 92 б. («відмінно»)

Керівник розділу _____ доц. Пілова Д.П.
(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи.

ВІДГУК

на кваліфікаційну роботу студентки групи 125-18-1

Агашкової Катерини Олегівни

на тему: Політика безпеки інформації інформаційно-телекомунікаційної системи АТ КБ «Dniprobank.

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 101 сторінках.

Метою кваліфікаційної роботи є забезпечення достатнього рівня захищеності інформації в інформаційно-телекомунікаційній системі АТ КБ «Dniprobank».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки та обстеження на ОІД. У результаті проведеного обстеження було побудовано модель загроз, що можуть бути реалізовані в ІТС, було класифіковано інформацію, що зберігається і циркулює на відділенні та виявлено активи, які потребують найбільшого рівня інформаційної безпеки. За отриманими результатами було розроблено політику безпеки у відділенні АТ КБ «Dniprobank».

Практичне значення роботи полягає у забезпеченні достатнього рівня захисту інформації об'єкта інформаційної діяльності за рахунок аналізу вразливостей та розробки політики безпеки.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Агашкова К.О. проявила себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «90 (відмінно)».

Керівник кваліфікаційної роботи Кагадій Т.С.

Керівник спец. розділу Тимофєєв Д.С.