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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Рички Владислава Сергійовича*

академічної групи *125м-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Засоби забезпечення інформаційної безпеки на об'єкті банківської діяльності*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Ковальова Ю.В.			
розділів:				
спеціальний	к.т.н., доц. Ковальова Ю.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Ричка Владиславу Сергійовичу* **академічної групи** *125м-20-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Засоби забезпечення інформаційної безпеки на об'єкті банківської діяльності***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз нормативно-правової бази у сфері ІБ. Види інформації, які підлягають технічному захисту.	14.11.2021
Розділ 2	Обстеження обчислювальної техніки. Обстеження складу офісного обладнання. Квалифікаційні відомості про персонал та заходи забезпечення інформаційної безпеки.	20.12.2021
Розділ 3	Техніко-економічне обґрунтування доцільності політики безпеки.Оцінка збитків від реалізації загроз	09.01.2022

Завдання видано _____ Ковальова Ю.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 13.10.2021р.

Дата подання до екзаменаційної комісії: 14.01.2022р.

Прийнято до виконання _____ Ричка В.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 стор. , рис 5., табл. 17, додатків 10, джерел 17.

Об'єкт обстеження**:** Об'єкт банківської діяльності на прикладі комерційного банку.

Предмет дослідження: процес управління та встановлення політики безпеки на об'єкті банківської діяльності.

Мета кваліфікаційної роботи**:** Провести дослідження ОБД. Виявити основні загрози та запропонувати ефективні засоби зниження ризику нанесення збитків активам компанії.

У першому розділі було досліджено теоретичну базу у сфері банківскої діяльності. Розглянули види інформації, які підлягають технічному захисту.

У другому розділі було проведено обстеження ОБД, та виявлено основні загрози активам. На основі даних отриманих під час дослідження була створено модель загроз, на основі якої розроблено політику безпеки, що описує контрдії нанесення збитків активам.

В третьому розділі визначено економічну доцільність розробки та введення у роботу політики безпеки. Проведено розрахунки капітальних витрат, поточних витрат. Економічне обґрунтування показало, що введені дії економічно вигідними для компанії так як капітал, що буде витрачено на введення та реалізацію заходів безпеки описаних у політиці безпеки, повертаються менше ніж за рік.

Наукова новизна роботи полягає у заходах на те, щоб знизити для банків ризик отримання небажаних збитків, притому витратив на заходи захисту менші кошти, ніж могли втратити у наслідок реалізації вище перерахованих загроз.

БАНКІВСЬКА ДІЯЛЬНІСТЬ, КОМЕРЦІЙНИЙ БАНК,ПОЛІТИКА БЕЗПЕКИ, РИЗИКИ, ЗБИТКИМОДЕЛЬ ЗАГРОЗ.

ABSTRACT

Qualifying work: 79 pages., pictures 5., tables 17, addition 10, sources 17.

Object of research: The object of banking activity on the example of the commercial bank.

Subject of study: the management process and the establishment of a security policy at the banking facility.

The purpose of the qualification work: To conduct a study of OBD. Identify the main threats and propose effective means to reduce the risk of damage to the company's assets.

The first chapter explored the theoretical framework in the field of banking. Considered the types of information subject to technical protection.

In the second section, a survey of the HBS was conducted and the main threats to the assets were identified. Based on the data obtained during the study, a threat model was created, on the basis of which a security policy was developed that describes counter-actions to damage assets.

The third section defines the economic feasibility of developing and implementing a security policy. Calculations of capital costs, current expenses are made. The business case showed that the introduced actions are economically beneficial for the company, since the capital that will be spent on the introduction and implementation of the security measures described in the security policy is returned in less than a year.

The scientific novelty of the work lies in the measures to reduce the risk of unwanted losses for banks, while spending less money on protection measures than they could lose as a result of the implementation of the above threats.

BANKING, COMMERCIAL BANK, SECURITY POLICY, RISKS, LOSS, THREATS MODEL.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ - державний стандарт України;

ДТЗ - допоміжні технічні засоби;

ЕСКД – єдина система конструкторської документації;

ЕСПД - єдина система програмної документації;

ІБ – інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КЗЗ - комплекс засобів захисту від несанкціонованого доступу;

КС - комп'ютерна система;

КСЗІ - комплексна система захисту інформації;

НД - нормативний документ;

НД ТЗІ - нормативний документ системи технічного захисту інформації;

НСД - несанкціонований доступ;

ОБД - об'єкт банківської діяльності;

ОІД - об'єкт інформаційної діяльності;

ЗМІСТ

ВСТУП

На сьогоднішній день питання кібербезпеки у банківській сфері є одним з найважливіших для функціонування банку. Адже, банк існує у більшій степені за рахунок коштів вкладників, яких в першу чергу цікавить безпека своїх коштів та особистих даних, що вкладник залишає для свого обслуговування.

У незалежній Україні банківська справа завжди була під пильним контролем з боку Національного Банку України та держави загалом. Але після масової вірусної атаки у 2017-му році вірусом «Petya», яка уразила більшість інформаційних систем не тільки банків, а і служб електроенергетики, Харківського аеропорту, Чорнобильської АЕС тощо, в Україні почався стрімкий ріст попиту на спеціалістів з кібербезпеки. У тому числі і банки України, ще більше посилили контроль з цього питання.

Також у зміцненні тренду на посилення стану інформаційної безпеки в банківській сфері відіграли нові, більш жорсткі вимоги до стану банківської ІБ, які були описані у постанові НБУ №95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», у якій було зібрано 150 пунктів, які описують принципи, підходи та вимоги до інформаційної безпеки.

Саме ці події послугували стрімкому розвитку кібербезпеки в Україні та у її банківській сфері зокрема. Також це і призвело до спонукання розробки та вдосконалення КСЗІ на даному об’єкті інформаційної діяльності. Матеріали що будуть наведені нижче і будуть спрямовані на виявлення та усунення недоліків безпеки інформаційних активів підприємства на даному об’єкті.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.

1.1 Стан питання

На сьогоднішній день розробка політики безпеки є важливою частиною створення КСЗІ на ОІД. Цей документ та/або комплекс документів регламентує правила, обв'язки та нові способи обробки інформації.

У цій частині дипломної роботи будуть представленні основні принципи зазначені законами України та нормативними документами, що пов'язані із захистом інформації.

Головною митою усієї дипломної роботи буде знайдення вразливостей в інформаційній системі ОІД. Та буде складена Політика безпеки, у якій будуть визначатися рішення щодо мінімізації ризику нанесення збитків інформаційним активам банку.

1.2 Аналіз нормативно-правової бази у сфері ІБ

У зв'язку із стрімкими розвитком ІТ та рівня кіберзлочинності, законодавство в Україні не може не розвиватися. Далі будуть наведені основні терміни та поняття що стосуються інформаційної безпеки згідно із нормами та законами України щодо цього питання.

1.2.1 Терміни

Інформація з обмеженим доступом - конфіденційна, таємна та службова інформація. [1]

Конфеденційна інформація – це 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.[1] Банківська таємниця – інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Відповідно до Закону України "Про банки і банківську діяльність" до б. т. відносять відомості та інформацію:

- про банківські рахунки клієнтів, у тому числі кореспондентські рахунки банків у Національному банку України;
- про операції, проведені на користь чи за дорученням клієнта, та здійснені ним угоди;
- про фінансово-економічний стан клієнтів;
- про системи охорони банку та клієнтів;
- про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності;
- стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- щодо звітності банку, за винятком тієї, що підлягає опублікуванню;
- про коди банків для захисту інформації. [2]

Службова інформація – це інформація що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень. [3]

Комплекс ТЗІ – сукупність організаційних, інженерних і технічних заходів та засобів, призначених для захисту від витоку інформації з обмеженим доступом технічними каналами на об’єктах інформаційної діяльності. [4]

Об’єкт інформаційної діяльності – будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди, функціональне призначення яких передбачає обіг інформації з обмеженим доступом. [4]

Технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації; [5]

Інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку. [6]

Комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті. [7]

АС Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, що обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. [8]

Цілісність. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності. Якщо існують вимоги щодо обмеження можливості модифікації інформації, то відповідні послуги треба шукати в розділі ―Критерії цілісності‖. В цьому розділі описані такі послуги: довірча цілісність, адміністративна цілісність, відкат і цілісність при обміні.

Доступність. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності. Якщо існують вимоги щодо захисту від відмови в доступі або захисту від збоїв, то відповідні послуги треба шукати в розділі ―Критерії доступності‖. В цьому розділі описані такі послуги: використання ресурсів, стійкість до відмов, горяча заміна, відновлення після збоїв.

Спостереженість. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості. Якщо існують вимоги щодо контролю за діями користувачів або легальністю доступу і за спроможністю комплексу засобів захисту виконувати свої функції, то відповідні послуги треба шукати у розділі ―Критерії спостереженості. В цьому розділі описані такі послуги: реєстрація, ідентифікація і автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікація при обміні,

автентифікація відправника (невідмова від авторства), автентифікація одержувача.

Реєстрація — це процес розпізнавання, фіксування і аналізу дій і подій, що пов'язані з дотриманням політики безпеки інформації. Використання засобів перегляду і аналізу журналів, а особливо засобів налагодження механізмів фіксування подій, має бути прерогативою спеціально авторизованих користувачів. [9]

1.2.2 Основні поняття.

Так як створення політики безпеки є один із пунктів створення КСЗІ, нижче буде розглянуто усі пункти її створення

1.2.2.1 Процеси створення КСЗІ

Створення комплексу ТЗІ передбачає проведення організаційних, інженерних і технічних заходів на ОІД, а саме:

- озвучення ІзОД (при проведенні нарад, під час показів зі звуковим супроводженням кіно- і відеофільмів тощо);
- здійснення обробки ІзОД технічними засобами (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація, приймання, отримання, передавання ІзОД тощо);
- обіг іншої ІзОД при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

У створенні комплексу ТЗІ беруть участь:

- установа, яка є замовником створення комплексу ТЗІ (далі – замовник або установа-замовник);
- виконавець робіт зі створення комплексу ТЗІ (далі – виконавець робіт з ТЗІ); виконавець проведення випробувань щодо створення комплексу ТЗІ (далі – виконавець випробувань);

- виконавець проведення атестації комплексу ТЗІ (далі – виконавець атестації).

Установа-замовник може бути виконавцем робіт з ТЗІ і виконавцем випробувань або може залучати до виконання таких робіт і випробувань суб'єктів господарської діяльності, що мають ліцензії на провадження діяльності у сфері ТЗІ.

Атестацію комплексу ТЗІ здійснює виконавець, що має відповідну ліцензію або дозвіл на провадження діяльності у сфері ТЗІ.

У створенні комплексу ТЗІ (залежно від характеру, складності та обсягу робіт) можуть брати участь один або декілька виконавців. У цьому разі замовник визначає головного виконавця.

Установа-замовник для створення комплексу ТЗІ також залучає:

- свої структурні підрозділи, діяльність яких пов’язана з ІзОД та які обґрунтовують необхідність і заявляють про створення комплексу ТЗІ (підрозділизаявники створення комплексу ТЗІ);
- призначену за необхідністю посадову особу з відповідною фаховою підготовкою для організації та координації робіт на всіх етапах створення комплексу ТЗІ, а також для організації експлуатації цього комплексу;
- підрозділ або посадові особи з відповідною фаховою підготовкою, яким доручено супроводження робіт з ТЗІ в установі (далі – підрозділ ТЗІ), службу захисту інформації в ІТС;
- інші підрозділи установи, які залучаються для формування положень щодо використання в інформаційній діяльності ІзОД, проведення обстеження, категорування об'єктів тощо.

Рішення щодо необхідності створення (модернізації) комплексу ТЗІ готує замовник на стадіях проектування, нового будівництва, розширення, реконструкції (далі – будівництво) ОІД, а також у разі змін умов функціонування ОІД.

Будівництво ОІД може виконуватися за відповідною проектнокошторисною документацією. При цьому повинні бути враховані вимоги ДБН А.2.2-2 і ДБН А.2.2-3.

Засоби забезпечення захисту інформації застосовують у складі комплексу ТЗІ за наявності сертифіката відповідності Системи УкрСЕПРО вимогам НД з питань ТЗІ або позитивного висновку державної експертизи у сфері ТЗІ.

Застосування імпортних засобів забезпечення захисту інформації можливе лише за умови відсутності вітчизняних аналогів при наявності відповідних техніко-економічних обґрунтувань і проведення їх сертифікації або одержання позитивного експертного висновку.

Джерела фінансування робіт зі створення комплексу ТЗІ визначає замовник.

Витрати на проектування, будівельно-монтажні роботи, проведення випробувань щодо ТЗІ, атестації комплексу ТЗІ вносяться до кошторису на будівництво та експлуатацію (утримання) ОІД. [4]

1.2.2.2 Види інформації, які підлягають технічному захисту

- інформація Відомості про об'єкти, процеси та явища (ДСТУ 2226)
- інформація з обмеженим доступом Інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами
- таємна інформація Інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю
- конфіденційна інформація Інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними

1.2.2.3 Класифікація загрози для інформації

- витік інформації - неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання

- порушення цілісності інформації Спотворення інформації, її руйнування або знищення

- блокування інформації Унеможливлення санкціононованого доступу до інформації

- загроза для інформації Витік, можливість блокування чи порушення цілісності інформації. Примітка. Загрози для інформації можуть виникати під час використання технічних засобів чи технологій, недосконалих щодо захисту інформації

- модель загроз для інформації Формалізований опис методів та засобів здійснення загроз для інформації

- доступ до інформації (ТЗІ) Можливість одержаання, оброблення інформації, її блокування та (чи) порушення цілісності

- доступ до інформації (ТЗІ) Можливість одержаання, оброблення інформації, її блокування та (чи) порушення цілісності

- закладний пристрій (ТЗІ); Потай встановлюваний технічний засіб, який створює загрозу для інформації

- комп'ютерний вірус Програма, що розмножується та поширюється самочинно Примітка. Комп'ютерний вірус може порушувати цілісність інформації, програмне забезпечення та (чи) режим роботи обчислювальної техніки

- спеціальний вплив (ТЗІ) Вплив на технічні засоби, що призводить до здійснення загрози для інформації

- спеціальний вплив (ТЗІ) Вплив на технічні засоби, що призводить до здійснення загрози для інформації

- спеціальний вплив (ТЗІ) Вплив на технічні засоби, що призводить до здійснення загрози для інформації

1.2.2.4 Технічні канали витоку інформації

- носій інформації (ТЗІ) Матеріальний об'єкт, що містить інформацію з обмеженим доступом
- інформативний сигнал (ТЗІ) Фізичне поле та(чи) хімічна речовина, що містять інформацію з обмеженим доступом
- інформативний сигнал (ТЗІ) Фізичне поле та(чи) хімічна речовина, що містять інформацію з обмеженим доступом
- самочинний (технічний) канал витоку інформації; ненавмисний канал витоку інформаціїТехнічний канал витоку інформації, в якому носії інформації та (чи) середовище їх поширення формуються самочинно
- 2 штучний (технічний) канал витоку інформації; навмисний канал витоку інформації
- побічне електромагнітне випромінення і навід;

ПЕМВН Електромагнітне випромінення та навід, що є побічним результатом функціонування технічного засобу і може бути носієм інформації

1.2.2.5 Технічний захист інформації

- (технічний) засіб із захистом; захищений (технічний) засіб; захищена техніка Технічний засіб, у якому додатково до основного призначення передбачено функцію захисту інформації від загроз
- засіб технічного захисту інформації Пристрій та (чи) програмний засіб, основне призначення яких - захист інформації від загроз
- засіб технічного захисту інформації Пристрій та (чи) програмний засіб, основне призначення яких - захист інформації від загроз
- пасивне приховування інформації Приховування інформації ослабленням енергетичних характеристик фізичних полів або зниженням концентрації речовин

- активне приховування інформації Приховування інформації створенням таких фізичних полів та речовин, які утруднюють здобування інформації або спричиняють невизначеність її змісту

- активне приховування інформаціїПриховування інформації створенням таких фізичних полів та речовин, які утруднюють здобування інформації або спричиняють невизначеність її змісту [10] Витяги з Законів України:

- Правову основу технічного захисту інформації в Україні становлять Конституція України (254к/96-ВР), закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою

України, з питань технічного захисту інформації, а також це Положення. { Пункт

3 із змінами, внесеними згідно з Указом Президента N 333/2008 (333/2008) від 11.04.2008 }

- Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку України) у взаємодії з органами, щодо яких здійснюється ТЗІ. {Пункт 4 із змінами, внесеними згідно з Указом Президента N 333/2008 (333/2008) від 11.04.2008}

- Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників. Організаційно-технічні принципи, порядок здійснення заходів з технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

- Нормативно-правові акти технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

- Розроблення, видання нормативно-правових актів з питань технічного захисту інформації, а також роботи, пов'язані з розробленням і виконанням загальнодержавних програм розвитку системи технічного захисту інформації, здійснюються за рахунок коштів державного бюджету та інших джерел фінансування, не заборонених законодавством. [11]

Вимоги до комплексної системи захисту інформації в АС в частині захисту від витоку інформації технічними каналами Мають бути сформульовані загальні вимоги до об'єктів (компонентів АС), що захищаються, визначені засоби захисту і засоби їх використання (наприклад, реалізація вимог до захищеності повинна досягатись без застосування екранування приміщень, активні засоби мають застосовуватись тільки для захисту інформації головного сервера АС і т. ін.).

Наводиться перелік нормативних і методичних документів, відповідно до яких повинні проводитись роботи щодо захисту інформації від витоку технічними каналами. Мають бути вказані вимоги до розмірів зони безпеки інформації. Мають бути вказані необхідні величини показників захищеності, що враховують реальну завадову обстановку на об'єкті електронної обчислювальної техніки. Основними показниками є: відношення величин електричної і магнітної складових напруженості поля побічних електромагнітних випромінювань до рівня завад на об'єкті ЕОТ; відношення величини напруженості інформативного сигналу в провідних комунікаціях на межі зони безпеки інформації до рівня завад на об'єкті ЕОТ; величина нерівномірності струму, який споживається по мережі електроживлення; коефіцієнт екранування засобів обчислювальної техніки, в тому числі від впливу зовнішніх ЕМВ.

Гранично допустимі значення основних показників є нормованими величинами і визначаються за відповідними методиками. Відношення розрахованих (виміряних) значень основних показників до гранично допустимих (нормованих) значень визначають необхідні умови захисту інформації. Мають

бути вказані вимоги щодо застосування способів, методів і засобів досягнення необхідних показників захищеності.

Рекомендується застосування таких способів, методів і засобів:

- системо- і схемотехнічних методів: обмеження використання інтерфейсів з передачею сигналів у вигляді послідовного коду і в режимі багатократних повторень; використання мультиплексних режимів обробки інформації, а також ЗОТ і системного забезпечення, що базуються на багаторозрядних платформах, інтерфейсів з передачею сигналів у вигляді багаторозрядного паралельного коду; використання раціональних способів монтажу, за яких забезпечується мінімальна довжина електричних зв'язків і комунікацій; використання ЗОТ і технічних засобів, до складу яких входять стійкі до самозбудження схеми, розв'язувальні і фільтрувальні елементи, комплектуючі з низькими рівнями ЕМВ; використання мережевих фільтрів для блокування витоку ІзОД мережами електроживлення, а також лінійних (високочастотних) фільтрів для блокування витоку ІзОД лініями зв'язку; використання ЗОТ і технічних засобів у захисному виконанні;
- засобів просторового і лінійного "зашумлення";
- засобів локального або загального екранування;
- засобів оптимального розміщення ЗОТ і технічних засобів з метою мінімізації зони, в межах якої граничне відношення сигнал/шум не перевищує встановлених норм.

Мають бути вказані вимоги до проведення спецдосліджень ЗОТ і технічних засобів, мета яких — пряме вимірювання показників ЕМВ. Мають бути вказані вимоги до проведення спецперевірки ЗОТ, мета якої — виявлення та вилучення (блокування) спеціальних електронних (закладних) 12 пристроїв. [12]

1.2.2.6 Документальне оформлення політики безпеки інформації.

Політика безпеки може розроблятись для ІТС в цілому або, якщо мають місце особливості функціонування окремих компонентів КСЗІ, для окремої

компоненти, для окремої функціональної задачі, для окремої технології обробки інформації тощо.

Політика безпеки розробляється згідно з положеннями НД ТЗІ 1.1-002 та рекомендаціями НД ТЗІ 1.4-001. Політику безпеки рекомендується оформляти у вигляді окремого документу Плану захисту.

Примітка**:**

1. Положення політики безпеки, які пов'язані з рішеннями, що приймаються на наступних етапах робіт (стосовно проектних рішень, організації робіт, встановлення відповідальності, порядку впровадження і експлуатації КСЗІ та ін.), вносяться до документу після прийняття цих рішень на відповідних етапах. [12] Автоматизована система являє собою організаційно-технічну систему, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію (малюнок). Прийнято розрізняти два основних напрями ТЗІ в АС — це захист АС і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наводів). Цей документ і комплект НД, що базується на ньому, присвячений питанням організації захисту від НСД і побудови засобів захисту від НСД, що функціонують у складі обчислювальної системи АС. Організаційні і фізичні заходи захисту, включаючи захист від фізичного НСД до компонентів ОС, як і захист від витоку технічними каналами не є предметом розгляду1. Незважаючи на це, при викладі увага приділяється також і деяким нетехнічним аспектам, але тільки там, де це впливає на оцінку технічної захищеності.

Основні загрози інформації Інформація в КС існує у вигляді даних, тобто представляється в формалізованому вигляді, придатному для обробки. Тут і далі під обробкою слід розуміти як власне обробку, так і введення, виведення, зберігання, передачу і т. ін. (ДСТУ 2226-93). Далі терміни «інформація» і «дані» використовуються як синоніми. Інформація для свого існування завжди вимагає наявності носія. Як носій інформації може виступати поле або речовина.

В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія. При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. Спроба реалізації загрози називається атакою.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу. Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації. Загрози можуть впливати на інформацію не безпосередньо, а опосередковано. Наприклад, втрата КС керованості може призвести до нездатності КС забезпечувати захист інформації і, як результат, до втрати певних властивостей оброблюваної інформації.

Політика безпеки інформації Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників.

Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз.

Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси 11 КС можуть істотно відрізнятись.

Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах. Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступ.

Комп'ютерна система, як правило, складається з безлічі компонентів. Деякі з компонентів можуть бути спеціально призначені для реалізації політики безпеки (наприклад, засоби ізоляції процесів або керування потоками інформації). Інші можуть впливати на безпеку опосередковано, наприклад, забезпечувати функціонування компонентів першого типу. І, нарешті, треті можуть взагалі не бути задіяні під час вирішення завдань забезпечення безпеки.

Множина всіх компонентів перших двох типів називається комплексом засобів захисту. Іншими словами, КЗЗ — це сукупність всіх програмно-апаратних засобів, в тому числі програм ПЗП, задіяних під час реалізації політики безпеки. Частина КС, що складає КЗЗ, визначається розробником.

Будь-який компонент КС, який внаслідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатись як частина КЗЗ. Комплекс засобів захисту розглядає ресурси КС як об'єкти і керує взаємодією цих об'єктів відповідно до політики безпеки інформації, що реалізується.

Як об'єкти ресурси характеризуються двома аспектами: логічне подання (зміст, семантика, значення) і фізичне (форма, синтаксис).

Об'єкт характеризується своїм станом, що в свою чергу характеризується атрибутами і поводженням, яке визначає способи зміни стану. Для різних КС об'єкти можуть бути різні. Наприклад, для СУБД в якості об'єктів можна розглядати записи БД, а для операційної системи — процеси, файли, кластери, сектори дисків, сегменти пам'яті і т. ін. Все, що підлягає захисту відповідно до політики безпеки, має бути визначено як об'єкт.

При розгляді взаємодії двох об'єктів КС, що виступають як приймальники або джерела інформації, слід виділити пасивний об'єкт, над яким виконується операція, і активний об'єкт, який виконує або ініціює цю операцію. Далі розглядаються такі типи об'єктів КС: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Прийнятий у деяких зарубіжних документах термін "суб'єкт" є суперпозицією об'єкта-користувача і об'єкта-процеса.

Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену — ізольованої логічної області, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини. В інших доменах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим об'єктом-процесом або навіть об'єктомкористувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Іншими словами, об'єкти можуть знаходитись в одному з трьох різних станів: об'єкт-користувач, об'єкт-процес і пасивний об'єкт. Перехід між станами означає, що об'єкт просто розглядається в іншому контексті. Пасивний об'єкт переходить в стан об'єкта-користувача, коли індивід (фізична особа-користувач) «входить» в систему.

Цей об'єкт-користувач виступає для КЗЗ як образ фізичного користувача. Звичайно, за цим процесом іде активізація об'єкта-процесу за ініціативою користувача. Цей об'єкт-процес є керуючим для пасивних об'єктів всередині домену користувача. Об'єктикористувачі, об'єкти-процеси і пасивні об'єкти далі позначаються просто як користувачі, процеси і об'єкти, відповідно. Взаємодія двох об'єктів КС (звернення активного об'єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об'єктами і/або зміни стану системи.

1.3 Модель порушника та постановка задач

Як порушник розглядається особа, яка може одержати доступ до роботи з включеними до складу КС засобами. Порушники класифікуються за рівнем 13 можливостей, що надаються їм штатними засобами КС. Виділяються чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний

рівень включає в себе функціональні можливості попереднього: - перший рівень визначає найнижчий рівень можливостей проведення діалогу з КС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації; - другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації; - третій рівень визначається можливістю управління функціонуванням КС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування; - четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів КС, аж до включення до складу КС власних засобів з новими функціями обробки інформації.

Припускається, що в своєму рівні порушник — це фахівець вищої кваліфікації, який має повну інформацію про КС і КЗЗ. Така класифікація порушників є корисною для використання в процесі оцінки ризиків, аналізу вразливості системи, ефективності існуючих і планових заходів захисту.

Основними завданнями засобів захисту є ізоляція об'єктів КС всередині сфери керування, перевірка всіх запитів доступу до об'єктів і реєстрація запитів і результатів їх перевірки і/або виконання. З одного боку, будь-яка елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути 18 віднесена до функцій ізоляції, перевірки або реєстрації.

З іншого боку, будь-яка з функцій, що реалізуються засобами захисту, може бути віднесена до функцій забезпечення конфіденційності, цілісності і доступності інформації або керованості КС і спостереженості дій користувачів. Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної КС.

Водночас одні й ті ж самі механізми можуть використовуватись для реалізації кількох послуг. Наприклад, для розробника слушно реалізувати і адміністративне і довірче керування доступом єдиним набором механізмів. Реалізація механізмів може бути абсолютно різною. Для реалізації функцій захисту можуть використовуватись програмні або апаратні засоби,

криптографічні перетворення, різні методи перевірки повноважень і т. ін. Вибір методів і механізмів практично завжди залишається за розробником.

Єдиною вимогою залишається те, щоб функції захисту були реалізовані відповідно до декларованої політики безпеки і вимог гарантій. Для реалізації певних послуг можуть використовуватись засоби криптографічного захисту.

Згідно із законодавством створення переліку вимог, сертифікація і атестація систем шифрування покладається на відповідний уповноважений орган виконавчої влади. Ця діяльність регламентується ―Положенням про порядок здійснення криптографічного захисту інформації в Україні‖. [13]

Виходячи із інформації зазначеної вище, можна визначити що у процессі розробки політики безпеки, потрібно виконати обстеження ОІД, виявити можливі загрози інформаційним активам, які мають своє місце на об’єкті та визначити заходи для усунення можливих ризиків при складанні політики безпеки.

Висновок до розділу 1

Під час постановок завдачі та аналізу нормативно правової бази здійснення забезпечення інформаційної безпеки на ОІД, було визначено необхідність здійснення обстеження об'єкту та виявлення основних вразливостей та ризиків, реалізуючи які порушники можуть завдати шкоди інформаційним активам підприємства. У наступній частині будуть виконані задачі поставленні вході першої частини дипломної роботи та створена політика безпеки, яка буде визначати заходи запобігання збітків, які може понести підприємство у разі реалізації ризику експлуатації загроз інформаційній безпеці.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про об'єкт

Ситуаційний план знаходиться на додатку В.

- Фізична адреса ОІД – м Дніпро, проспект Героїв Майдану 3а;
- Об'єкт є будівлею підрозділу ІТ;
- Штат робітників складає 9 осіб (1- керівник відділу ІТ-безпеки, 2-спеціаліст з інформаційної безпеки, 1 – спеціаліст з технічного захисту інформації, 2 – системні адміністратори, 3 – розробники баз даних);
- Будівля ОІД одноповерхове;
- 100 м на захід від ОІД двоповерхова будівля контактного центру «Абанку»;
- 105 м у західно-південному напрямку двоповерхова будівля кафе «Мальвіна»;
- 105 м у південно-західному напрямку двоповерховий жилий дім;
- 85 м на південь двоповерховий жилий дім;
- 85 м в південно-східному напрямку двоповерховий жилий дім;
- В 40 м на схід триповерхова будівля планетарію;
- В 32 м в південно-західному напрямку головний офіс банку;
- 60 метрів на південь знаходиться проїжджа частина;
- Контрольована зона ОІД обмежується стінами будівлі де він знаходиться.

2.1.2 Розташування комунікацій

План на якому зображено ці системи зображено у додатку Д. План коммунікацій охоронної системи зображена у додатку В.

Таблиця 2.1 Підключення комунікаційних систем

Назва системи	Спосіб підключення
Система електропостачання	До об’єкта надходить з підстанції, що знаходиться на території банку. Прокладено під землею, та підключається до розподільно щитка. Заземлено на 10 метрів.
Паливна система	Є автономною, забезпечується котлом зігрівання води, до якого вода для нагріву потрапляє з труб водопостачання
Охоронно сигналізаційна система	Електропостачання йде до камер, датчиків, замків та панелі управління з розподільного щитка. Кожен прилад передає інформацію на панель управління, яка передає сигнал про стан сигналізації на пульт охорони, який знаходиться в головному офісі банку.
Водопостачання та каналізаційна система	Надходить централізовано, з центральних труб міського водопостачання та каналізації. Під’єднано до об’єкта двома трубами.

2.2 Обстеження об’єкту

2.2.1. Генеральний план

Генеральний план зображено у додатку Г.

- електро-проводка проходить по стінам з розподільчого щитка;
- заземлення розташовано на глибині 10 м під землею;
- на дверях, при вході до будівлі встановлено кодовий замок (код від якого знають лише співробітники працюючі у цій будівлі) та співробітники охорони;
- у кімнаті А – знаходяться робочі місця відділу ІТ-безпеки, розташована у північній частині будівлі;

- у кімнаті Б – знаходяться робочі місця відділу розробників баз даних розташована у центрально-східній частині будівлі;
- у кімнаті В – знаходяться робочі місця системних адміністраторів, розташована у південній частині будівлі;
- сервер знаходиться у серверні, на дверях якої знаходиться кодовий замок, до який знають лише системні адміністратори та керівник відділу ІТбезпеки, також у серверній виконані усі вимоги постанови НБУ № 243 «Про затвердження Правил з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи;
- кімната номер 5 – це кімната для переговорів, на вікнах встановленні штори;
- на об’єкті ведеться відеоспостереження;
- енергосистема розгалужена на систему охоронного електроживлення та електроживлення іншого технічного обладнання;
- датчики диму встановлені у кімнатах: А, Б, В, Серверній та у коридорі;
- на об’єкті встановлено автономну систему опалення, опалення

здійснюється котлом для зігрівання води, яка поступає до батарей опалення;

- вода поступає до об’єкту з труби водопостачання в західній частині будівлі.

2.2.2 Обстеження обчислювальної техніки. Обстеження складу офісного обладнання.

На об’єкті інформаційної діяльності ведеться інвентарний облік обчислювальних пристроїв, дані з обліку апаратного забезпечення наведено у таблиці 2.2.

Таблиця 2.2 - Інвентарні відомості апартного забезпечення ОІД

Назва	Кількість	Характеристики	Серійні номера
Робочий комп'ютер ((Patriot S i37100/120))	4	Intel Core i3-7100 (3.9 ГГц)/RAM 8 ГБ/SSD 120 ГБ/Intel HD Graphics 630/без ОД/LAN/без ОС	10011 10012 10013 10014
Мережевий принтер (HP LaserJet Pro M227fdw)	1	Лазерний друк (ч/б), максимальнороздільна здатність друку 1200x1200 dpi, мережеві інтерфейси - Wi-Fi, Ethernet	10034
Сервер (Сервер Dell PowerEdge T330)	4	Чотириядерний Intel Xeon Quad-Core E3-1230 v6 (3.5 - 3.9 ГГц), ОЗУ 8ГБ, чипсет - Intel C236, мережевий інтерфейс - Gigabit Ethernet, операційна система - Операційна система Microsoft Windows Server 2016 Essentials x64	10035 10036 10037 10038
Оперативна пам'ять для серверів (Оперативна пам'ять Kingston DDR4-2666)	3	Обсяг пам'яті 32 ГБ, тип пам'яті DDR4 SDRAM, частота пам'яті - 2666 МГц, пропускна здатність - 21300 МБ/сек	10039 10040 10041

Продовження таблиці 2.2.

Назва	Кількість	характеристики	Серійні номера
Жорсткий диск для серверів(Жорсткий диск Western Digital Ultrastar DC)	4	обсягпам'яті-8ТБ, технологія–HDD,форм фактор-3.5",швидкість обертання шпинделя-7200 об/хв, Обсяг буфера -256 МБ	10042 10043 10044 10045
Коммутатор Cisco Catalyst 2960 Plus	1	управляемый коммутатор с 48 портами Fast Ethernet и 2 портами Combo Gigabit SFP. Cisco Catalyst 2960-Plus. Коммутатор 2 уровня для офисов филиалов. 48 портов Fast Ethernet Uplink порты SFP и Gigabit Ethernet Поддержка PoE стандарта IEEE 802.3af Программное обеспечение LAN Base или LAN Lite Инструменты SmartOperations позволяют упростить разворачивание и снизить стоимость обслуживания сети Технология Cisco EnergyWise	10046
Маршрутизатор Ethernet Cisco ISR 4221 - WAN-порт	1	Ethernet, Интерфейсы: 3 x LAN 10/100/1000 Мбит/с, Поддержка протоколов: PPPoE, IPsec, L2TP, PPTP, Защита информации: WPA, WPA2, WEP, Без антенны	10047

Таблиця 2.3 - Апаратне забезпечення персонала працюючого на ОІД

Відділ ІТ-безпеки	Системне адміністрування	Розробники баз данних
10011,10012,10013, 10014	10047,10046,10042,10043, 10044,10045,10039,10040, 10041,10035,10036,10037, 10038,10031,10032	10021,10023,10024

Технічне обладнання охоронного призначення:

На об'єкті встановлено системи пожежної сигналізації та охоронні датчики. Крім того на двох дверях встановлено кодові замки.

Таблиця 2.4 - Інвентарні відомості пристроїв охоронного призначення

Назва приладу	Кількість	Інвентарний номер
turbo HD камера Hikvision DS-2CC12D8T-AMM	9	10101,10102,10103, 10104,10105,10106,10107, 10108, 10109
датчик DT-107	4	10110,10111,10112,10113
панель управління АПК	1	10114
Датчик диму СПД 3.10 з базою Б4	5	10115,10116,10117,10118, 10119
Опис Геркон МС-11S	2	10120, 10121
БезконтактнийRFID замок з магнітними ключами	2	10122, 10123
Флеш накопичувачі пам'яті	9	10123, 10124, 10125, 10126, 10127, 10128, 10129, 10130, 10131

Назва та характеристики охоронного обладнання:

Turbo HD камера Hikvision DS-2CC12D8T-AMM- внутрішня установка охоронної камери зйомки під об'єктив з ультра-низьким освітленням. Технологія Ultra-Low Light забезпечує для камери вивчення світлочутливості, випромінює її сліповувати до рівня 0,005 Люкс / F1.2. Матрица розсчитана на зйомці в широкій двох мегапіксельному форматі при частоті всіх 25 кадрів в секунду. Для камери сумісний будь-який об'єкт з автодиафрагмой і різьбленням C / CS. Широкий функціонал камери включає AGC, белас белого, BLC, 3D DNR, режим День / Ніч, WDR 120 дБ, 4 зони детекції за рухом, 4 зони приватності, зеркало.

Ключові технічні властивості:

- відеокамера Ultra-Low Light;
- матриця: High-performance CMOS;
- роздільна здатність запису: 2 Мп (1920 х 1 080);
- швидкість запису: 25 кадрів в секунду;
- мінімальний рівень освітленості: 0.005 Люкс (денна зйомка).

Внутрішня синхронізація;

Функції обробки зображення: WDR (120 дБ), AWB, BLC, AGC, 3D DNR, дзеркальне відображення;

- екранне меню налаштувань;
- детектор руху (4 області);
- маска конфіденційності (4 області);
- роз'єм для підключення: 1 х CVBS вихід (75 Ом / BNC);
- вимоги до живлення: DC 24 В;
- матеріал корпусу: метал;
- працює в межах діапазону температур -30 ° C ... + 60 ° C;
- габарити: 69,29 х 54 х 56 мм.

Такі камери встановлено у всіх приміщеннях де ведеться відеоспостереження.

Датчик DT-107 -датчик руху цифровий інфрачервоний пасивний з функцією імунітету до тварин середнього розміру. У датчиках використовується спеціально розроблена унікальна оптична лінза з технологією двоелементною відображення (Dual PIR), а також електроніка, заснована на базі спеціалізованої IMC. Цей комплекс технологій дозволяє знизити до мінімуму помилкові спрацьовування, і не реагувати на домашніх тварин до 25 кілограм. Відстань виявлення зловмисника становить до 15 метрів. На платі спеціальний тамперний контакт і є можливість регулювати чутливість інфрачервоного детектора. Сучасна лінза Френеля забезпечує прилад широким кутом до 90 градусів, що значно скоротило «сліпу зону» безпосередньо під детектором. Датчик укомплектований кріпильних набором, а саме з двома дюбелями і саморізами.

Для управління сигналізацією використовується Адресна панель управління АПК.

Опис панелі управління - Адресна панель управління АПК призначена для управління системою безпеки об'єкту, що охороняється (складській території, виробничого комплексу, офісного центру і т.д.). За допомогою пристрою можна не тільки управляти системою, але і отримувати повідомлення від зовнішніх пристроїв оптичної сигналізації та інших сповіщувачів. Пристрій виконаний в міцному металевому корпусі. Воно підключається до системи приймальноконтрольних приладів за допомогою двох ліній зв'язку. Панель управління двомовна (українська та російська).

Пристрій автоматично шукає і визначає компоненти системи безпеки. Для зручності на великому графічному дисплеї роздільною здатністю 320 * 480 точок відображаються найменування зон і приладів, підключених до системи. Робочий діапазон харчування напруги 10,0В-15,0В. Загальна маса приладу трохи більше 1,5 кілограм.

Характеристики:

- діапазон напруг живлення 10,0В-15,0В;
- струм у всіх режимах, не більше 0,23А;

- струм в черговому режимі, не більше 0,16А;
- габаритні розміри 270мм * 200мм * 55мм;
- маса 1,65 кг.

Датчик диму СПД 3.10 з базою Б4 - Сповіщувач СПД-3.10 призначений для виявлення загорянь в закритих приміщеннях будівель і споруд і реагує на появу диму малої концентрації, індикації цього стану і передачі сигналу «ПОЖЕЖА» на приймально-контрольний прилад. Даний оптичний пожежний димовий сповіщувач серії СПД-3.10 відрізняється від популярних датчиків СПД-3 і СПД-3.2 уменьшіна габаритами і великим вибором настановних баз зі зручними клемами для підключення кабелю передачі сигналу. Кнопка "Тест" дозволять легко перевірити працездатність димового детектора СПД-3.10

Датчик СПД-3.10 розрахований на безперервну, цілодобову роботу спільно з ППК з двопровідним або чотирьох провідних ШС.Підключення датчика СПД-3.10 до ППК з двопровідним ШС здійснюється за допомогою баз Б01, Б1. Підключення до ППК з чотирьох провідних ШС здійснюється за допомогою баз Б2, Б3, Б4, Б5. Бази Б6, Б7, Б8, Б9 є кінцевими, встановлюються по одній в кінці кожного шлейфу і використовуються в чотирьох провідних ШС для контролю наявності напруги живлення і цілісності ланцюга.Сповіщувач має функції індикації чергового режиму роботи і перевірки працездатності. База Б4 призначена для підключення сповіщувача СПД-3.10, ВПС-3.10 до ВУОС і чьотирьох ШС. База Б4 формує вихідний сигнал за допомогою контактів реле і управляє ВУОС.

При побудові шлейфу пожежної сигналізації на базах Б4, необхідно в кінці кожного ШС встановлювати базу Б6 або Б8 (база Б8 з ВУОС). В такому ШС відсутність напруги живлення через обрив або зніманні будь-якого блоку електронного з бази призводить до формування на ППК сповіщення «Несправність» з цього ШС.

Технічні характеристики:

- Чутливість, дБ / м 0,05-0,2;
- Інерційність, с, не більше 10;
- Напруга електроживлення, В 10-30;
- Струм споживання в черговому режимі, мА, не більше 0,1;
- Внутрішній опір в режимі «ПОЖЕЖА» при струмі 20 мА, Ом, не більше 500;
- Струм споживання в режимі «ПОЖЕЖА», мА 8-30;
- Час скидання режиму «ПОЖЕЖА», с, не менше 5;
- Час технічної готовності, с, не більше 30;
- Габаритні розміри, мм Ø85 × 37;
- Маса, кг 0,15.

Також на дверях встановлення датчики відкриття Геркон МС-11S

Опис Геркон МС-11S - "MS-11S" Магнітно-контактний накладної сповіщувач. Призначений для блокування будівельних конструкцій на відкривання. Зручний для установки на дерев'яні (пластикові) двері або скла / рами вікон. Кріплення сповіщувача здійснюється за допомогою самоклеющейся основи або з використанням шурупів. Максимальный ток и напряжение контактов: 0,5А / 200 В постоянный / 10 Ватт.

Безконтактний RFID замок з магнітними ключами- безконтактний RFID замок для будинку, офісу з магнітними ключами Робоча напруга 12 В постійного струму Розблокувати ток 1000mA Статичний струм 60 мА Пам'ять 250 стандартних користувачів Підтримка Карт stall.com.ua плюс пароль і пароль плюс карти. Функції Можна додати номер карти і видалити номер карти. Відстань читання до 10 см Тип РФ ЕМ. карти Варіанти відкриття дверей (адміністратор вибирається користувачем) Card (Key Tag) і Пароль / Card

(брелок) тільки / пароль. Робоча температура -10 ~ 70 С Діапазон Вологість від 10 до 90%.

2.2.3 Обстеження програмного забезпечення ІТС

2.2.3.1 Склад програмнного забезпечення

- для роботи з документами на цьому об'єкті інформаційної діяльності використовують пакет программ Microsoft office 365 для підприємств, до складу якої входять такі програми для роботи з документами: Word, Excel, PowerPoint, OneDrive;
- для комунікації використовуються такі програми: TeamViewer Business, Skype for business, окрім того компанія використовує свій власний поштовий домен для комунікації поштою;
- база даних створена на основі СУБД Oracle Enterprise;
- для розгалуження доступу використовується Active Directory;
- на сервері встановленна операційна система Windows Server 2016;
- на робочих станціях встановленно операційну систему Windows 10 Корпоративна;
- на кожному комп'ютері встановлено антивірус Zillya для бізнесу.

Усе програмне забезпечення, яке встановлено на усіх робочих машинах організації – є ліцензованим. Згідно з вимогами НБУ до банків України, у тому числі з вимогами які описані в постанові НБУ №95.

2.2.3.2. Обробка інформації

На ІТС ОІД, знаходиться тестовий сервер на якому зберігається програмний код, програмних продуктів банку, які знаходяться на стадії тестування. На самих серверах він зберігається у зашифрованому вигляді, а саме симетричним алгоритмом шифрування із довжиною ключа 256 біт. Між іншим розробники ПО (у випадку із досліджуваним ОІД – це розробник баз даних), мають копії програмного коду на своїх робочих станціях.

Доменна система, база даних клієнтів, база даних робітників та інша інформація, яка тим чи іншим чином циркулює, отримується з сервері, які знаходяться у центрі обслуговування сервері, який належить самому банку. З'єднання із об'єктом інформаційної діяльності відбувається за допомогою віртуальної приватної мережі(VPN).

Також, робітники мають право використовувати переносні носії пам'яти, але ці носії обов'язково повинні буди зареєстрованими. Крім того строго забороняється використання робітниками своїх власних носіїв пам'яті. Успішно протестований програмний код, передається на встановлення до робочого сервера по VPN з'єднанню. Також для аналізу безпеки всієї банківської інформаційної системи, через VPN з'єднання на об'єкт потрапляє інша інформація, стосовно банківського обігу інформації, а саме:

- логи з журналів подій;
- логи журналу інтернет трафіку;
- банківські документи службового призначення;
- загальна клієнтська база клієнтів банку (Де зберігається особиста інформація клієнта, яка стала відома банку у процесі обслуговування).

Також на об'єкті зберігаються посадові інструкції, у паперовому вигляді.

При з'єднанні мережевих пристроїв на об'єкті використовуються кабелі типу «вита пара» категорії 5E та оптично-волоконні кабелі для організації структурованої кабельної системи.

2.2.3.3 Топологія мережі на об'єкті

У банку використовується змішана архітектура мережевої топології. У Додатку Г показана схема побудови топології мережі на даному ОІД. У мережі, яка діє на території об'єкта було створено 3 локальні комп'ютерні мережі (vlan). Їх найменування: 1. IT-security, 2. Admins, Data base Developers.

При передачі інформації через інтернет використовується захищений протокол IPs за основу яркого взято протокол IPv6, згідно з вимогами

Національного Банку України, які описано у постанові НБУ 95. На території Об'єкту нема бездротового зв'язку типу Wi-Fi.

2.2.3.4 Комунікація через банківську мережу

Банк здійснює мережевий зв'язок використовуючи стек протоколів TCP/IP, та використовує останні версії протоколів захисту даних на транспортному рівні.

У внутрішньо-банківському з'язку використовується IP-телефонія. Розподіл унікальних ідентифікаторів мережевого рівня у мережі банку здійснюється відповідно до вимог описаних у стандарті стандарту RFC 1918 ―Розподіл адрес у приватних IP-мережах‖

Зв'язок із поштовим сервером при користуванні корпоративною електронною поштою відбувається шифрованим каналом, який використовує POP3S – захищений протокол для передачі повідомлень.

2.2.4 Квалифікаційні відомості про персонал та заходи забезпечення інформаційної безпеки

2.2.4.1. Таблиця 2.5 - Склад персоналу

Посада	Кількість
Системний адміністратор	2
Керівник IT-безпеки	1
Спеціаліст IT-безпеки	2
Спеціаліст з технічного захисту інформації	1
Розробник баз даних	3

2.2.4.2. Обов`язки робітників

Системний адміністратор:

- підтримка пк користувачів на базі Windows 10;

- підтримка серверів на базі Windows server 2016;
- підключення, налаштування, забезпечення якісної роботи оргтехніки; налагодження та забезпечення працездатності локальної мережі, телефонної, робочих місць користувачів;
- ведення бюджету підрозділу і інвентаризація;
- діагностика роботи каналів зв'язку і передачі даних;
- налаштування правдоступу для користувачів;
- забезпечення організації нових робочих місць;

Керівник ІТ-безпеки:

- розробка внутрішніх нормативних документів в області ІБ;
- контроль виконання політик ІБ;
- проведення оцінки ризиків ІБ;
- управління інцидентами ІБ;
- розробка планів реагування на критичні інциденти ІБ;
- управління та активну участь у впровадженні сучасних іт технологій;
- оптимізація бізнес-процесів підрозділу ІБ;
- здійснення контролю за станом захисту інформаційних ресурсів в іт системі банку;
- складання і виконання бюджету підрозділу ІБ;
- розробка технічних завдань і технологічної документації;
- консультування співробітників з питань ІБ;
- виконання функцій щодо забезпечення безперервності діяльності банку відповідно до чинного законодавства україни.

Спеціалісти ІТ-безпеки:

- організація безпеки комп'ютерної інформаційної мережі Банку;
- забезпечення захисту електронних банківських документів;
- адміністрування Центру сертифікації ключів для забезпечення застосування електронного цифрового підпису та шифрування документів, що проходять через електронну пошту, систему документообігу та зберігаються на внутрішніх файлових ресурсах;
- адміністрування процесу використання SSL-сертифікатів;
- адміністрування системи антивірусного захисту на базі рішення ESMC 7 (ESET);
- адміністрування Proxy SQUID;
- контроль за наданням віддаленого доступу до інформаційних систем Банку за технологією двофакторної аутентифікації на базі обладнання і ПЗ компанії;
- контроль за порядком і обсягом надання прав доступу користувачів до інформаційних ресурсів Банку;
- аналіз рівня інформаційної безпеки при впровадженні нових програмних комплексів і банківських продуктів;
- щорічна оцінка ризиків інформаційної безпеки та ефективності СУІБ;

Спеціаліст з технічного захисту інформації:

- виявлення технічних каналів витоку інформації на об’єкті;
- складання технічної документації щодо захисту інформації;
- слідкування за дотриманням норм технічного захисту інформації на об’єкті та відповідності до Законів України та вимог НБУ;
- проведення оцінки стану технічних засобів захисту інформації;
- проведення обслуговування засобів захисту інформації згідно із рекомендацій виробника;

2.2.4.3. Заходи захисту інформації

- забороняється приклеювати папірці паролями на видному місці; забороняється використовувати на робочому незареєстровані носії пам'яті;
- забороняється користуватися соціальними мережами з робочого місця;
- суворо забороняється виносити з території банку цифрові або паперові копії документів службового призначення;
- забороняється копіювати, передавати третім особам та розміщати у соціальних мережах конференційну інформацію та інформацію що складає банківську таємницю;
- при залишені робочого місця забороняється залишати робочий комп'ютер у розблокованому стані;
- до трудових контрактів/договорів працівника включені посадові інструкції та обов'язки працівника щодо виконання вимог із забезпечення інформаційної безпеки;
- при вході до робочої електронної пошти використовується двофакторна авторизація. Треба ввести свій логін, пароль та код, який приходить на особистий телефон робітника у вигляді смс-повідомлення;
- усі з'єднання з зовнішніми серверами відбуваються через VPN-канали;
- при використанні мережі інтернет використовуються захищенні протоколи такі як: IPsec, HTTPs, SSl та інші;
- ключі шифрування та дешифрування даних знаходяться у керівника IT-безпеки та у голови правління банку та особи що його заміняє;
- один раз на пів року ключі шифрування резервно копіюються та архівуються за необхідністю;
- у разі компрометування ключів шифрування їх негайно знищують та генерують нові;

- інформація що зберігається на сервері об’єктузнаходиться у зашифрованому вигляді, при шифруванні використовується алгоритм симетричного шифрування RSA із 256 бітним ключем;

- на об’єкті використовується виключно актуальні версії ПО, у тому числі і антивірусне програмне забезпечення та програмні продукти робота яких націлена на забезпечення інформаційної безпекиРаз на місяць відділ ІТ-безпеки проводить перевірку:

- вхідних та вихідних повідомлень корпоративної електронної пошти, уключаючи вкладання до них;

- усього вхідного інтернет трафіку;

- усіх змінних носіїв інформації, що підключається до робочих станцій або іншого обладнання інформаційних систем, що знаходяться на території ОІД.

- один раз на неділю проводиться резервне копіювання інформації, що зберігається на сервері, для цього використовується 1 з чотирьох серверів;

- раз на неділю проводиться оновлення та створення нових бекапів;

- зберігання електронного журналу роботи засобі захисту від зловмисного коду зберігається 3 місяці

- у локальній мережі є розмежування користувачів по правам та доступу до інформації в системі. (додаток Е табл. 7)

- кожна дія користувача у системі реєструється у журналі подій.

- паролі облікових записів співробітників змінюються кожні 30 діб;

- у разі трьох невдалих спроб вести пароль, обліковий записспівробітника блокується, розблокувати його може лише системний адміністратор;

- централізоване розповсюдження налаштувань параметрів безпеки та інших параметрів конфігурації операційних систем здійснюється за допомогою

використання групових політик контролю домену «Active Directory»; на об'єкті створено та підтримується у актуальному стані перелік ПО, що використовується на об'єкті.

- самостійне встановлення ПО на робочі станції блоковано усім співробітникам, які не мають прав адміністратора у системі.
- на комп'ютерах об'єкту встановлено DLP систему Zecurion.
- на робочих станціях відбувається контроль працівника на робочому місці за допомогою програми DeskTime, контроль відбувається скріншотам екрану раз на 3 хвилини, моніторингу інтернет трафіку та активності дій робітника за комп'ютером.
- персоналу раз на місяць проводиться інструктаж з інформаційної безпеки;
- із практикантами також проходить інструктаж з інформаційної безпеки.

2.2.4.4 Встановлення охоронного режиму на об'єкті

У робочий час доступ у будівлю відкривається о 9:30. Співробітник який перший входить до Об'єкту повинен ввести код доступу, після цього двері відкриються, та співробітнику протягом 60-ти секунд потрібно буде ввести код для вимкнення сигналізації на панелі управління, яка знаходиться по ліву руку від співробітника.

Таким чином співробітник вимикає датчики руху, які встановлені на ОІД.У разі невчасного введення коду, двері на вихід з приміщення блокуються, тривожний сигнал передається на пульт охорони в головному офісі. Магнітні ключі від дверей у існують лише у двох екземплярах: один у чергового охоронця, другий у керівника IT - безпеки.

Коли останній робітник виходить з будівлі де знаходиться ОІД, він повинен ввести код включення сигналізації, тим самим увімкняться датчики

руху. Відеоспостереження ведеться постійно та передається охоронцям на екран спостереження, які знаходяться у головному офісі.

Пожежна сигналізація представлена датчиками диму встановленими на стелях у кімнатах, які були перераховані вище.

2.3 Створення моделы загроз

Виходячи з «Акту обстеження» для даної ІТС визначені антропогенні загрози та меншим ступенем загрози пов'язані із природними умовами на місцевості де знаходиться ОІД, джерелами яких є кримінальні елементи, персонал та особливості природних умов.

2.3.1. Модель порушника

Таблиця 2.6 - Модель порушника

Джерело	Загроза	Вразливість
Кримінальні елементи	Викрадення інформації	Можливість проникнення третіх осіб на об'єкт через недостатню стійкість кодового замку на температурні умови місцевості (В особливості у зимній сезон)
	Знищення інформації	Відсутність датчиків цілісності скла на вікнах об'єкту (можливість проникнення на об'єкт через вікно)
	Викрадення або пошкодження обчислювальної техніки	
Персонал	Несанкціонований друк (копіювання інформації)	Відсутність в політиці безпеки контролю за інформацією,яка надходить до принтера немережевим шляхом

2.3.2 Аналіз загроз

Таблиця 2.7 Аналіз загроз

Загроза	Джерело
Крадіжка інформації	Кримінальні елементи
Знищення інформації	
Викрадення, або пошкодження обчислювальної техніки	
Несанкціонований друк та копіювання інформації	Персонал

Для розрахунку коефіцієнта небезпеки (далі – К небезпеки), використаємо формулу

$$\frac{K1*K2*K3}{125} = K_{\text{небезпеки}} \quad (2.1)$$

для визначення найкритичнішої загрози.

Маючи перелік актуальних вразливостей, маємо можливість розрахувати $K_{\text{небезпеки}}$ для кожної з загроз за формулою.

Де К1 – фатальність;

К2 – можливість/зручність реалізації;

К3 – кількість елементів, котрим притаманна вразливість) і визначити, яка з загроз найкритичніша.

Ця формула використовується для аналізу ризику та аналізу вразливостей. Число 125 у формулі задається, як максимально можливе значення коєфіцієнту небезпеки.

2.3.3. Аналіз вразливостей

Таблиц. 2.8 Аналіз вразливостей

Вразливість	К1	К2	К3	$К_{небезпеки}$
Можливість проникнення третіх осіб на об'єкт через недостатню стійкість кодового замку на температурні умови місцевості (В особливості у зимний сезон)	4	2	1	0,064
Відсутність датчиків цілісності скла на вікнах об'єкту (що дає змогу проникнення на об'єкт через вікно)	3	5	1	0,12
Відсутність в політиці безпеки контролю за інформацією, яка надходить до принтера немережевим шляхом	3	5	1	0,12

Рівні К1:

- 1 – наслідки, якими можна знехтувати;
- 2 – незначні наслідки;
- 3 – відчутні наслідки;
- 4 – значні наслідки; 5 – крах компанії.

Рівні К2*:*

- 1 – вразливість дуже складно або неможливо використати;
- 2 – для використання вразливості потрібні спеціальні умови, обладнання і/або висококваліфікований порушник;
- 3 – вразливість може використати лише кваліфікований порушник з мінімальним набором обладнання;
- 4 – вразливість може використати лише кваліфікований порушник;
- 5 – вразливість може використати будь хто; Рівні К3*:*
- 1 – 0-1 елемент;
- 2 – 2-9 елементів;
- 3 – 10-14 елементів;
- 4 – 15-19 елементів;
- 5 – 20+ елементів.

Для розрахунку коефіцієнта небезпеки (далі – К небезпеки), використаємо формулу (2.1) для визначення найкритичнішої загрози

2.3.4.Аналіз ризиків

Таблиця 2.9 Аналіз ризиків

Назва	Загроза	К небезпеки
Кримінальні єлементи	Викрадення або пошкодження обчислювальної техніки	0,128
	Знищення інформації	0,48
	Крадіжка інформації	0,48
Персонал	Несанкціонована модифікація інформації	0,512
	Несанкціонований друк та копіювання інформації	0,512

К1 – визначає ступінь доступності до об’єкта Рівні К1*:*

- 1 – Без доступу до об’єкта;
- 2 – З контрольованої території без доступу у будинки та споруди.
- 3 – Усередині приміщень, але без доступу до технічних засобів АС.
- 4 – З робочих місць користувачів АС або використовуючи віддалений доступ.
- 5 – З доступом у зони даних (баз даних, архівів й т.ін.) і/або у зону керування засобами забезпечення безпеки АС. К2 – визначає ступінь кваліфікації та мотив Рівні К2*:*
- 1 – виконавець не зацікавлений в реалізації загрози, він не володіє методами, що реалізують загрозу;
- 2 – виконавець зацікавлений в реалізації загрози, але він не володіє методами, що реалізують загрозу;
- 3 – виконавець не зацікавлений в реалізації загрози, він володіє методами, що реалізують загрозу;
- 4 – виконавцю вигідна реалізація загрози, він володіє методами, що реалізують загрози;
- 5 – виконавцю вигідна реалізація загрози, він досконало володіє методами, що реалізують загрозу (наприклад, він працює у відповідній сфері). К3 – визначає рівень серйозності наслідків Рівні К3*:*
- 1 – наслідки, якими можна знехтувати;
- 2 – незначні наслідки;
- 3 – відчутні наслідки;
- 4 – значні наслідки;
- 5 – крах компанії.

За підрахунками, усі загрози окрім «Ненавмисне розголошення конференційної інформації» мають достатньо високий коефіцієнт небезпеки.

Висновок**:** на основі отриманих даних, можна зробити висновок, найбільш актуальними є загрози:

- Крадіжка інформації;
- Знищення інформації;
- Викрадення або пошкодження обчислювальної техніки;
- Несанкціонована модифікація інформації;
- Несанкціонований друк та копіювання інформаці;

2.4. Політика безпеки

Політику безпеки затверджує керівник відділу ІТ-безпеки банку.

2.4.1 Політика підбору кодових замків для вхідних дверей у будівлю з оід

1. Опис

Може слугувати, як пам’ятка новим спеціалістам з технічного захисту інформації стосовно вимог, які повинні виконуватися при підборі кодових замків до вхідних дверей до ОІД у місцевості знаходження об’єкта.

2. Мета

Встановлення мінімальних вимог до встановлювальних кодових замків, для підтримки високого рівня захищенності будівлі від несанкціонованного проникнення, виходячи з погодних умов регіону.

3. Галузь використання

Ця політика застосовується до всіх співробітників, які відповідальні за підбір кодових замків.

4. Політика

Співробітники зобов'язані, які займаються підбором пристроїв для запобігання несанкціонованому проникненню на об’єкт, повинні мати на увазі такі мінімальні вимоги до пристроїв: температура встановлювального пристрою повинна витримувати максимально низьку температуру не вище -25 ℃ та максимально високою температурою не нижче +60 ℃. Пристрій

обов’язково повинен підтримувати функцію преавторізації (код від замка, біометричну систему або систему відкриття дверей після піднесення до нього смарт-карти)

5. Працівник

Працівник, який порушив дану політику, може понести дисциплінарне стягнення, включаючи звільнення, відповідно до діючого законодавства.

6. Лист реєстрації змін

Червень 2019 – Політика введена в дію керівником відділу IT безпеки банку.

2.4.2 Політика чистого столу

1. Опис

Може бути важливим інструментом для гарантії того, що всі критичні/конфіденційні матеріали вилучені з робочого місця працівників відділу освіти виконавчого комітету Апостолівської міської ради і заблоковані, коли вони не використовуються або співробітник покидає свою робочу станцію. Така політика може підвищити обізнаність працівників з питань захисту конфіденційної інформації.

2. Мета

Встановлення мінімальних вимог для підтримки "чистого столу", де конфіденційна/критична інформація про співробітників, навчальні заклади, працівників навчальних закладів та постачальників знаходиться в безпеці. Політика чистого столу не тільки сумісна зі стандартом ISO 27001, але вона також є частиною стандартного базового контролю конфіденційності.

3. Галузь використання

Ця політика застосовується до всіх співробітників будівлі IT-відділу банку.

4. Політика

Співробітники зобов'язані забезпечувати збереження всієї конфіденційної інформації у друкованому або електронному вигляді на своєму робочому місці в кінці робочого дня і протягом тривалого періоду часу.

Робочі комп'ютери повинні бути заблоковані, коли робоче місце не зайняте.

Робочі комп'ютери повинні бути повністю вимкнені в кінці робочого дня.

Будь-яка інформація з обмеженим доступом повинна бути вилучена зі столу і зберігатись в ящику, коли працівник не знаходиться на робочому місці і в кінці робочого дня.

Ключі, що використовуються для доступу до інформації з обмеженим доступом, не можна залишати на столі без нагляду.

Паролі не можуть бути залишені в робочих записах персоналу, розміщених на комп'ютері або під комп'ютером, і не можуть бути записані в доступному місці.

Документи, що містять інформацію з обмеженим доступом, повинні бути видалені з принтера відразу після друку.

Потрібно пам`ятати, що зйомці носії інформації є вразливими, отже, їх треба зберігати у захищеному місці.

Всі принтери повинні бути очищені від документів, як тільки завершиться друк; це допомагає гарантувати, що конфіденційні документи не будуть залишені у лотках принтера.

5. Відповідальність

Працівник, який порушив дану політику, може понести дисциплінарне стягнення, включаючи звільнення, відповідно до діючого законодавства.

6. Лист реєстрації змін

Червень 2019 – Політика введена в дію керівником відділу IT – безпеки банку.

2.4.3 Політика заборони копіювання службових документів з будь-яких переносних носіїв пам’яті

1. Опис

Може бути важливим інструментом для гарантії того, робітники не будуть використовувати переносні носії пам’яті для копіювання з них

інформації за допомогою мережевого прінтера. Через те, що копіювання в такий спосіб робить неможливим індетифікацію копіюючого у журналі подій.

2. Мета

Полегшити процес рослідування інциденту несанкціонованого копіювання інформації. Копіювання буде можливе лише відправкою документа для копіювання на прінтер по корпоративній мережі до якої він підключен.

3. Галузь використання

Ця політика застосовується до всіх співробітників будівлі IT-відділу банку.

4. Політика

Заборонено використовувати для копіювання переносних носіїв пам'яті, тепер дозволено копіювання відправкою файлу з робочої станції до мережевого прінтера підключеного до корпоративної мережі.

Суворо забороняється використовувати чужі робочі станції для відправки документу на печать.

Робітник несе особисту відповідальність за скопійований їм документ.

Потрібно пам`ятати, що зйомці носії інформації є вразливими, отже, їх треба зберігати у захищеному місці. Всі принтери повинні бути очищені від документів, як тільки завершиться друк; це допомагає гарантувати, що конфіденційні документи не будуть залишені у лотках принтера.

5. Відповідальність

Працівник, який порушив дану політику, може понести дисциплінарне стягнення, включаючи звільнення, відповідно до діючого законодавства.

6. Лист реєстрації змін

Червень 2019 – Політика введена в дію керівником відділу IT – безпеки банку.

2.4.4 Ранжування ризиків

Таблиця 2.4.4 - Ранжування ризиків.

Загроза	Ризик до введенння політики безпеки	Ранжований ризик
Викрадення або пошкодження обчислювальної техніки.	0,128	0,05
Знищення інформації	0,48	0,1
Несанкціонована модифікація інформації	0,512	0,15
Несанкціонований друк та копіювання інформації	0,512	0,15

Висновок до розділу 2

У ході виконання спеціальної частини, проведено обстеження ОІД. У ході обстеження було виявлено ряд основних вразливостей. У ході створення моделі загроз було виявлено джерела загроз та ризики реалізації загроз інформаційним активам через вразливості системи безпеки. На основі моделі угроз було створено політику безпеки, де були описані засоби зниження ризику завдання збитків активам.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Техніко-економічне обґрунтування доцільності політики безпеки.

Так як головною метою підприємства є отримання прибутко, актуальним питанням стає економічне обґрунтування витрат, що може тягнути за собою введення нової політики безпеки та засобів запобігання збитків активам. Це означає, що введення контрмір проти реалізації ризиків повинно коштувати компанії менше ніж можуть складати збитки у разі реалізації загроз.

3.1.1 Стислий опис і значення проблеми.

Політикою безпеки, яка вводиться у цій кваліфікаційній роботі зазначені протидії реалізації таких загроз:

- Несанкціоноване проникнення на об’єкт.
- Викрадення інформації.
- Несанкціоноване знищення інформації.
- Несанкціоноване копіювання інформації.

3.1.2 Обґрунтування необхідності та актуальності вирішення проблеми.

В політиці безпеки наведеної вище, були наведені необхідні мінімальні заходи для зниження ризику реалізації загроз.

3.1.3 Сутність запропонованого в кваліфікаційній роботі методу зниження ризику.

Заходи, що запропоновано у цій кваліфікаційній роботі на те що знизити для компані ризик отримання небажаних збитків, притому витратив на заходи захисту менші кошти, ніж могли втратити у наслідок реалізації вище перерахованих загроз.

3.1.4 Розрахунок капітальних витрат.

3.1.4.1 Трудоміскість розробки політики безпеки

Вартість розробки проекту інформаційної безпеки:

Основна формула:

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин} \quad (3.1)$$

$t_{тз}$ – 16 год - тривалість складання технічного завдання на розробку політики безпеки інформації.

$t_{в}$ – 8 год - тривалість розробки концепції безпеки інформації у організації.

$t_{а}$ – 16 год - тривалість процесу аналізу ризиків.

$t_{вз}$ – 24 год - тривалість визначення вимог до заходів, методів та засобів захисту.

$t_{озб}$ – 16 год - тривалість вибору основних рішень з забезпечення безпеки інформації.

$t_{овр}$ – 32 год - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації.

$t_{д}$ – 4 год – тривалість документального оформлення політики безпеки.

1. Піставляємо числа у формулу:

$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д} = 100$ год.

2. Розрахунок витрат на створення політики безпеки інформації:

Основна формула:

$$Крп = Ззп + Змч \quad (3.2)$$

Ззп - 12500 грн

Формула заробітної плати працівника:

$$З_{зп} = t \cdot З_{іб} \quad (3.3)$$

Середня заробітна плата працівників на ОІД становить – 20000 грн/міс, робочий день складає 8 годин, працівник працює приблизно 20 робочих днів.

З цього слідує, що $З_{іб} = 100 * 125 = 12500$ грн

Щоб розрахувати вартість 1 годинного часу, скористаюсь формулою:

$$С_{мч} = Р \cdot t_{пал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн} \quad (3.4)$$

де P – встановлена потужність ПК, кВт;

C_e – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920).

Де Р = 0,4 кВт, $С_е$=1,94 грн/кВт, $Ф_{зал}$= 8888 – 2962 = 5926, $Н_а$ = 1/3 на рік, $К_{ЛПЗ}$ = 331 + 400 + 1500 = 1231 грн, $Н_{апз}$= 100% на рік, $F_р$ = 1920.

$С_{мч}$ = 78,25 грн.

З цього слідує що, $З_{мч}$ = 78,25 * 100 = 7825.

З підрахувань вище слідує, що *Крп = 12500 + 7825 = 20325 грн* – витрати на розробку політики безпеки.

Визначення суми фіксованних капітальних витрат:

Основна формула:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.5)$$

Де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн; $К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Виходячи з описаних уполітиці безпеки заходах, встановлення нового програмного забезпечення, навчання персоналу не э необхідним тому ми можемо змінити формулу фіксованих капітальних витрат, тобто:

$$К = Кпр + Крп + Каз + Кн \quad (3.6)$$

Де було виключено змінну $К_{зпз}$- вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ).

Користуючись попередніми розрахунками робимо висновок, що $К_{рп}$ = 20 тис. грн.

Вартість закупівлі апаратного забезпечення та допоміжних матеріалів разрахуємо з цін на необхідні матеріали, а тоб-то: датчиків биття скла та купівлі нового замку на вхідні двері.

В якості рішення для проблеми проникнення на об’єкт шляхом робиття скла, використаємо: датчик розбиття VIDICON STAR - Датчики, які реагують на удар и розбіття скла необхідні для надійного захисту вікон або других засклення конструкцій. При віявленні розбіття скла зараз пристрій передает сигнал тривоги на приймально-контрольний прилад. Такі датчики могут встановлюватіся на стелю, стіну або віконні та дверні прорізи. Його ціна складає 378 грн за один датчик, значить для закупівлі трьох таких датчиків буде витрачено 1,134 грн.

Для заміни кодового замку на вхідних дверях у будівлю підійде розумний кодовий замок Smart Mortise Lock, він підходить, за робочою температурою та за надійністю. Його ціна складає 10456 грн. Закупівля пломб для

USB-входу для мережевого принтера коштує 200 грн за 10 одиниць. Допоміжні матеріали для підключення датчиків входять у ціну монтажу.

Користуючись перерахованим вище, робимо висновок, що $К_{аз}$ = 1134 + 10456 + 200 = 11790 грн.

Розрахунок вартість розробки проекту інформаційної безпеки.

Розробкою проекту інформаційної безпеки займатимуться спеціалісти відділу ІТ-безпеки, і буде займати 12 години

З чого слідує, що формула Кпр = Ззп + Змч = 2(125*12 + 78,25*12) = 3000 + 1878 = 4878 грн.

Вирати на встановлення та налагодження системи інформаційної безпеки.

У середньому монтаж та налагодження датчиків биття скла разом из закупівлею та прокладкою дротів буде коштувати 1500 грн. З чого робимо висновок, що $К_{н}$ = 1500 грн.

Із підрахунків що наведені вище можна резюмувати, що К = 4878 + 20000 + 11790 + 1500 = 38168 грн.

3.1.5 Розрахунок поточних (експлуатаційних) витрат.

Для розрахунків поточних витрат на рік буде використовуватись $С_{ел}$(ціна електроенергії, що будет витрачена на роботу встановлених датчиків та замку) $С_{тс}$- ціна роботи спеціаліста з технічного захисту інформації та $С_{ауд}$ – витрати пов’язані із внутрішнім аудитом системи інформаційної безпеки, який буде проводити чотири рази на рік керівник відділу ІТ-безпеки.

Основна формула:

$$С = С_{о} + 4С_{тс} + 4С_{ауд} \quad (3.7)$$

Де $С_{о}$ – складається з суми робочого року приладів, встановлення, яких було запроваджено політикою безпеки.

$$С_{о} = С_{рд} + С_{ед} \quad (3.8)$$

Сума безперервної роботи за рік, буде розрахововатись за формулою:

$$C_р = P * t_{нал} * Ce \quad (3.9)$$

Де $C_р$ – це ціна рокової роботи кВт. $t_{нал}$ – час що працює прилад, на рік кількість годин становить 8760 год.

Се – це тариф за кіловат.

Виходячи з потужності роботи датчика в 0,004 кВт маємо ціну робочого року:

$$C_{рд} = 0,004 * 8760 * 1,94 = 67,97 \text{ грн.}$$

Потужність електронного замку складає 0,125 кВт, сума безперервної роботи за рік:

$$C_{ед} = 0,125 * 8760 * 1,94 = 2124 \text{ грн.}$$

$C_о = 67,97 * 3 + 2124 = 2327$ грн. – безперервної роботи на рік, приладів встановлення, яких було запроваджено політикою безпеки.

Ціна обслуговуванн та діагностики спеціалістом з технічного захисту інформації. Обчислюється за формалою:

$$C_{тс} = C_{рч} * t, \quad (3.10)$$

Де $C_{рч}$ – Ціна робочого часу спеціаліста грн/год. t- час роботи.

На діагностику датчиків та електронного замку та перепломбування мережевого принтеру спеціаліст витратить 8 годин.

$$C_{тс} = 125 * 8 = 1000 \text{ грн.}$$

Ціна аудиту розраховується за формулою:

$$C_{ауд} = C_{квб} * t, \quad (3.11)$$

Де $C_{квб}$ – зарплата працівника на годину. t – час що потрібен на проведення аудиту.

На проведення аудиту політик безпеки, що були введені у кваліфікаційній роботі спеціалісту потрібно 12 годин.

$$С_{ауд} = 125 * 12 = 1500 \text{ грн}$$

Так як, політиками безпеки нових обов'язків робітникам не було назначено, то і заробітну платню додатково вони не отримують.

Виходячи з розрахунків приведених вище можна розрахувати суму поточних витрат:

С = 2327+ 4000 + 6000 = 12327 грн – поточні витрати на рік.

3.2 Оцінка збитків від реалізації загроз.

3.2.1 Аналіз збитків від реалізації загроз пов'язаних із можливістю несанкціонованного проникнення на об'єкт

До загроз, що пов'язані із цією вразливістю можна віднести: пошкодження або викрадення обчислювальнох техніки та викрадення інформації. На об'єкті не захищеної техніки дверями із кодовим замком знаходиться приблизно на суму 107 991 грн. Тому збитки у разі пошкодження або викрадення обчислювальної техніки можуть сягати від 8888 грн до 107991 грн. У середньому збитки від реалізації цієї загрози будуть складати 58439 грн.

Так як на об'єкті резервне копіювання відбувається раз на неділю збитки з викрадення чи знищення інформації будуть складати від 2000 грн до 10000 грн відповідно часу, який розробники баз даних будуть відновлювати програмний код, збитки також залежать від того скількі днів пройшло після останього резервного копіювання. У середньому збитки будуть сягати 5000 грн.

Висновок: при реалізації загроз пов'язаних із цією вразливістю збитки всередньому будють становити 63439 грн.

3.2.2 Аналіз збитків від реалізації загроз пов'язаних із можливістю несанкціонованого копіювання інформації на мережевому принтері.

У разі витоку інформації таким способом та передачі цих даних третім особам, на банк може бути складено коллективний позов за статтями ст.1076 Цивільного Кодексу і ст. 60 закону "Про банки і банківську діяльність" щодо банківської таємниці, ст. 32 Конституції України про заборону на збір,

зберігання, використання та поширення конфіденційної інформації про особу без її згоди, ст. 24 закону "Про захист персональних даних". Розмір компенсації клієнтам встановлюється у судовому порядку. Наприклад через виток інформації на Приват банк було складено

позов за раніше перерахованими статтями. Позов вимагав від банку заплатити по 11 тис гривень заплатите кожному з ісців.

Якщо умовно узяти інформацію 100 клієнтів чия інформація була скопійована та передана третім особам, то у разі ухвалення судом цього позову, то збитки банку

будуть складати 1100000 грн.

3.2.3 Сума збитків на рік.

Загальний ефект від впровадження системи інформаційної безпеки:

$$E = B \cdot R - C \qquad (3.12)$$

Загальний ефект від впровадження системи інформаційної безпеки де B – загальний збиток від атаки на вузол або сегмент корпоративної

мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$R = (R_1 + R_2 + R_3 + R_4) / 4 = (0.128 + 0.48 + 0.512 + 0.512) / 4 = 0.408$$

У разі реалізації кожної з загроз в продовж року, збитки будуть складати у середньому 1163439 грн.

$E = 1163439 \cdot 0.408 - 12327 = 462.356$

ROSI = Е/К = 462,356 / 38168 = 12.11 - коефіцієнт повернення інвестицій.

$T_o = 1/12,11 = 0,08$ років - термін окупності капітальних інвестицій

Висновок до розділу 3

Політика безпеки, що була запроваджена у цій кваліфікаційній роботі є економічно обгрунтованною, бо витрати на її розробку, реалізацію та підтримання складають 50495 грн, а збитки при реалізації усіх описаних загроз у продовж року сягають 1163439 грн, що на багато перевищує витрати на впровадження засобів зниження ризику експлуатації загроз.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи проекту було проведено аналіз нормативноправової бази. На підставі розглянутих нормативних документів та законів України було визначено необхідність здійснення обстеження об'єкту та виявлення основних вразливостей та ризиків, реалізуючи які порушники можуть завдати шкоди інформаційним активам підприємства. У ході обстеження були визначенні основні вразливості та загрози у системі безпеки ОІД.

Було розроблено та запроваджено заходи зниження ризику реалізації загроз інформаційним активам підприємства. Крім того була сформована вимога до контрдій. Які обов'язково потрібно запровадити для зниження ризику несанкційованого проникнення на об'єкт інформаційної діяльності.

У економічній частині було підраховано фіксовані витрати та поточні витрати на підтримку мір, що були запроваджені для зниження ризиків експлуатації загроз.

Також у ході економічного обґрунтування було виявлено, що розробка та реалізація політики безпеки є економічно обґрунтованою.

Витрати на підтримку та встановлення заходів забезпечення безпеки інформаційних активів. У декілька разів менше ніж збитки, які компанія понесе у разі реалізації загроз. Під час виконання роботи деякі дані було модифіковано з метою запобігання витоку конфеденційної інформації банку. Усі імена та відомості спеціалістів були змінені.

ПЕРЕЛІК ПОСИЛАНЬ

1. Стаття 21. Інформація з обмеженим доступом

2. Про банки і банківську діяльність Закон України від 07.12.2000 р. № 2121-III.

3. Закон України від 13.01.2011 № 2939-VI «Про доступ до публічної інформації

4. НД ТЗІ 1.1-005-07 нормативний документ (НД) системи технічного захисту інформації (ТЗІ) визначає основи організації та етапи виконання робіт щодо створення комплексу на об’єкті інформаційної діяльності (ОІД) органу державної влади, місцевого самоврядування, військового формування, підприємства, установи та організації

5. Указ Президента Украины от 27.09.1999 № 1229/99 «Про Положення про технічний захист інформації в Україні»

6. Про затвердження Інструкції про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів технічного захисту інформації, а також з наданням послуг із технічного захисту інформації, та контроль за їх дотриманням. Ліцензійна палата України,

Департам.спецтелекомсистем СБУ, Служба безпеки України; Приказ, Инструкция от 13.10.1998 № 92/80

7. Про затвердження Ліцензійних умов провадження господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації Держкомпідприємництво, Департам.спецтелекомсистем СБУ, Служба безпеки України; Наказ, Умови від 29.12.2000 № 89/67

8. 2.5-005-99 документ встановлює принципи класифікації автоматизованих систем та освіти стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

9. НД ТЗІ 2.5-004-99 нормативний документ — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

10. ДСТУ 3396.2-97 Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації.

11. https://zakon.rada.gov.ua/laws/show/1229/99

12. НД ТЗІ 1.4-001-2000 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Типове положення про службу захисту інформації в АС;

13. НД ТЗІ 1.6-005-2013 - Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці

14. НД ТЗІ 2.5-005-99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

15. НД ТЗІ 3.1-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи;

16. НД ТЗІ 3.3-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;

17. Проект Концепції інформаційної безпеки України [Електронний ресурс]. – 2015. – Режим доступу: http://mip.gov.ua/ru/documents/30.html

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	3	
4	А4	Вступ	1	
5	А4	1 Розділ	18	
6	А4	2 Розділ	28	
7	А4	3 Розділ	8	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	2	
13	А4	Додаток Г	2	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	1	
16	А4	Додаток Е	1	
17	А4	Додаток Є	2	
18	А4	Додаток Ж	1	
19	А4	Додаток З	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Кваліфікаційна робота
2. Додаток В
3. Додаток Г
4. Додаток Ґ
5. Додаток Д
6. Додаток Е
7. Додаток Є

Презентація.pptx

ДОДАТОК В. Ситуаційний план

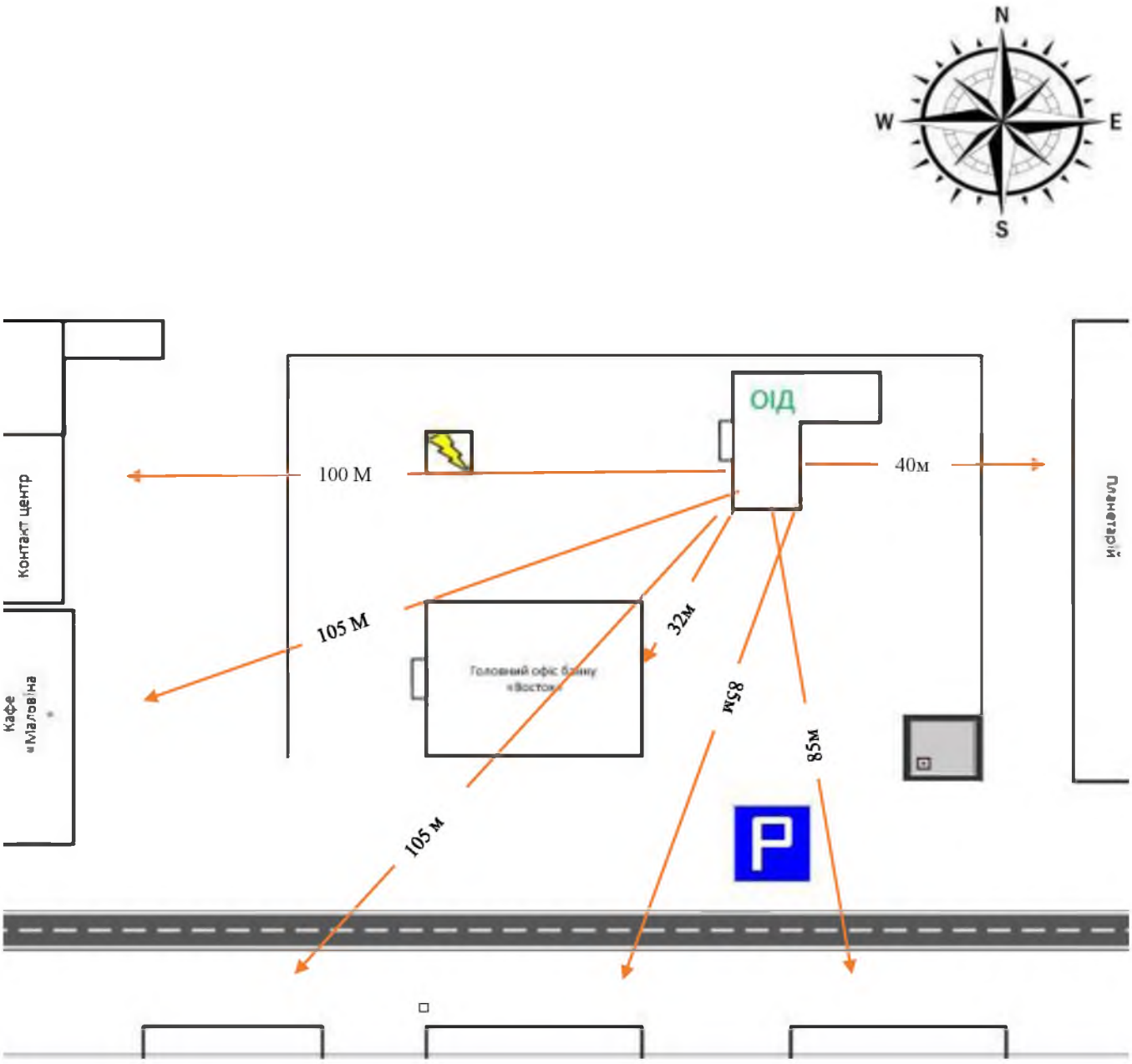

Рис. 1. Ситуаційни план

Легенда мапи

Назва елементу	Вигляд елементу
Паркан	
Проїзджа частина	
Автостоянка	
Електроживлення	
Труба центрального водопостачання та каналізації	
Електро-підстанція	
Контур будівлі	
Охоронний пункт	
Електро-щит	
Труби водопостачання та каналізації	

ДОДАТОК Г. Генеральний план

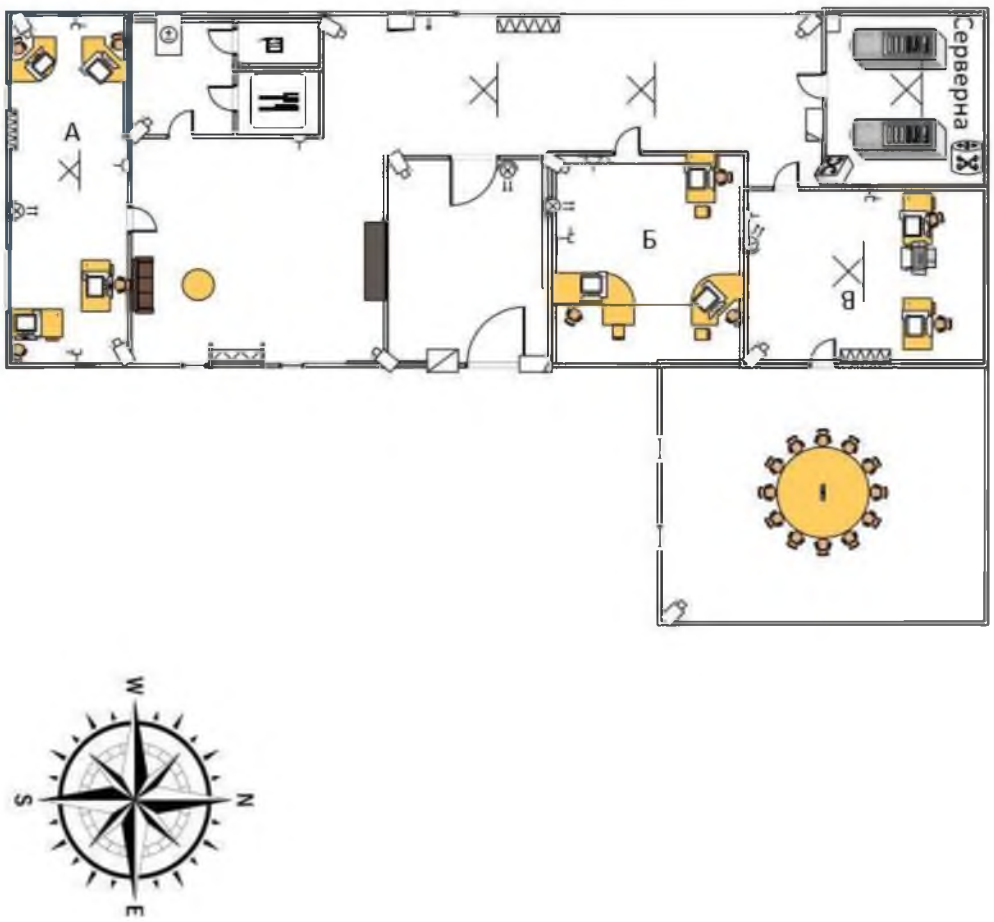

Рис. 2. Генаральний план

Легенда мапи

Таблиця 2

Назва елементу	Іконка елементу
Робоча станція	
Датчик пожежної сигналізації	

Продовження таблиці 2

Розетка	
Панель управління сигналізацією	
Кодовий замок двері із датчиком на розмикання	
Котел для опалення	
Вимикач світла	
Труби каналізації та водопостачання	
Безперебійник	
Комутатор	
Маршрутизатор	
Камера відео-спостереження	
Батарея опалення	
Датчик руху	

ДОДАТОК Ґ. План сигналізаційної системі

Рис. 3. План сиганлізаційної системи.

Легенда мапи

Таблиця 3

Назва елементу	Іконка елементу
Дроти системи пожежної сигналізації	
Дроти системи відеоспостереження	
Дроти датчиків руху	
Дріт передачі зображення на пульт охорони	
Дріт датчиків розмикання	

ДОДАТОК Д. План комунікацій

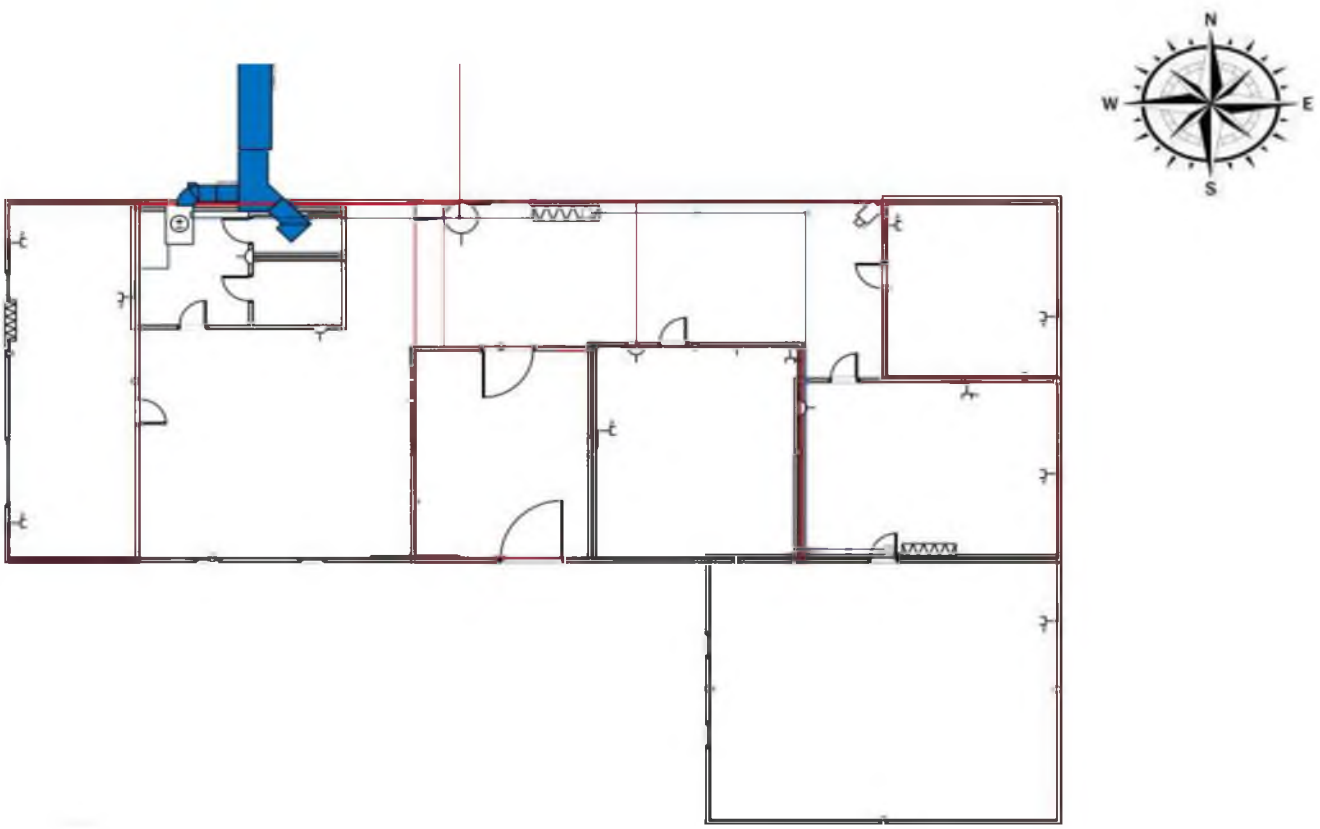

Рис. 4. План комунікацій.

Таблиця 4

Назва елементу	Позначення елементу
Електрична проводка	
Труби опалення	
Розетка	
Батарея опалення	
Труби водопостачання	
Вимикач світла	

ДОДАТОК Е. Мережева топологія

Схема мережевої топології:

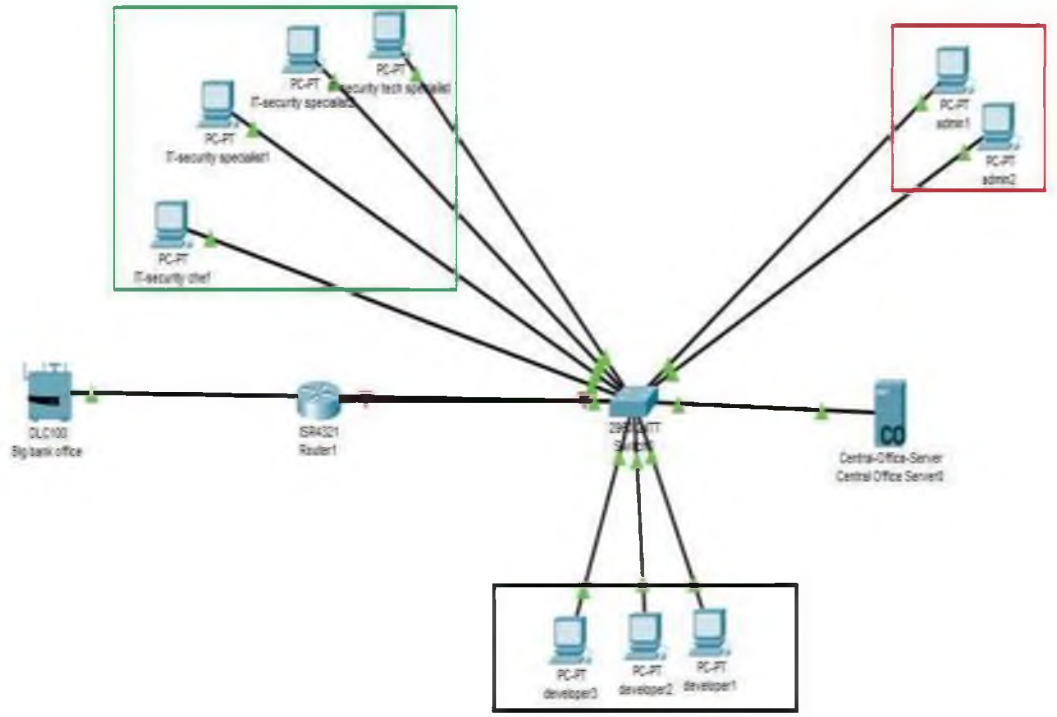

Рис. 5. Мережева топологія

Таблиця 5

Назва елементу	Іконка елементу
Робоча станція	
Сервер	
Мережева система банку	
Маршрутізатор	
Коммутатор	

ДОДАТОК Є

Класифікація інформації, що циркулює на Об’єкті інформаційної діяльності та сітка розгалуження доступу

Таблиця 6 Класифікації інформації, що циркулює на об’єкті.

Найменування	Доступність інформації
Програмний код	Конфіденційна інформація
Логи журналу подій	Конфіденційна інформація
Логи журналу інтернет трафіку	Конфіденційна інформація
Банківські документи службового призначення	Банківська таємниця
Загальна клієнтська база клієнтів банку	Банківська таємниця
Документи що формують собою технічне завдання для розробників	Конфіденційна інформація
Ключі шифрування	Банківська таємниця
Посадові інструкції	Відкрита інформація

Таблиця 7 Розгалуження доступу до інформації

	Спеціаліст з IT-безпеки	Керівник відділу ITбезпеки	Технічний спеціаліст із захисту інформації	Розробник баз даних	Системний адміністратор
Программний код	Немає доступу	Немає доступу	Немає доступу	Читання/модифікація	Немає доступу
Банківська база даних клієнтів	Читання	Читання	Немає доступу	Немає доступу	Немає доступу

Продовження таблиці 7

	Спеціаліст з IT-безпеки	Керівник відділу ITбезпеки	Технічний спеціаліст із захисту інформації	Розробник баз даних	Системний адміністратор
Логи робітників на ОІД	Читання	Читання	Немає доступу	Немає доступу	читання
Логи робітників всього банку	Читання	Читання	Немає доступу	Немає доступу	Немає доступу
Журнал інтернет трафіку	Читання	Читання	Немає доступу	Немає доступу	Читання (лише ОІД)
Банківські документи службового призначення	Читання	читання/ модифікаці я (якщо документ стосується безпеки інформації)	Читання/модифікація (якщо документ стосується технічних питань безпеки інформації)	Немає доступу	Читання
Паролі від облікових записів користувачів	Модифікація (може лише зробити запит на зміну пароля)	Модифікація (може лише зробити запит на зміну пароля)	Немає доступу	Немає доступу/модиф ікація(лише зміна пароля на своєму обліковому записі)	Модифікація (може лише зробити запит на зміну пароля)

ДОДАТОК Ж. Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК З

Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу магістра студента групи 125м-20-2

Рички Владислава Сергійовича

На тему: «Засоби забезпечення інформаційної безпеки на об’єкті банківської діяльності".

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 66 сторінках.

Метою кваліфікаційної роботи є підвищення рівня забезпечення інформації на об’єкті банківської діяльності.

Тема кваліфікаційної роботи безпосередньо пов’язана з об’єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі:
обстеження банківської діяльності, проведення аналізу захисту інформації; створення документів з політики безпеки.

Практичне значення результатів кваліфікаційної роботи полягає у підвищені та забезпеченні рівня захисту інформації в банківської діяльності за рахунок розробки політики безпеки інформації.

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

За час дипломування Ричка В.С. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістр 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 «_____».

Керівник кваліфікаційної роботи **Ковальова Ю.В.**

Керівник спец. розділу **Ковальова Ю.В.**