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 бакалавра

студента *Полякова Івана Ігоровича*

академічної групи ***125-20-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплексна система захисту інформації інформаційно-комунікаційної системи ТОВ БДО***

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Корченко А.О.			
розділів:				
спеціальний	Ассистент БІТ Мілінчук Ю. А.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:

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

«_____»_____2024року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Полякова Івана Ігоровича* **академічної групи** ***125-20-1***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему Комплексна система захисту інформації інформаційно-комунікаційної системи ТОВ БДО

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ	15.03.2024
Розділ 2	ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ТОВ "БДО"	10.05.2024
Розділ 3	ЕКОНОМІЧНА ЧАСТИНА	11.06.2024

Завдання видано _____ _____
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ _____
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 71 с., 3 рис., 12 табл., 3 додатка, 17 джерел.

Об'єкт розробки: інформаційно-комунікаційна система міжнародної аудиторської компанії ТОВ «БДО».

Предмет розробки: комплексна система захисту інформації інформаційно-комунікаційної системи ТОВ «БДО».

Мета роботи: підвищення рівню безпеки ІТС підприємства ТОВ «БДО»

У першому розділі було проведено ретельний аналіз підприємства, розглянуто стан безпеки ІТС, виявлено основні ризики та загрози.

У другому розділі було виконано розробку КЗСІ, приведені відомості про стан ІТС в компанії, сформовані моделі порушника та моделі загроз. Запропоновано етапи підвищення захисту КЗСІ та введення заходів для покращення безпеки. Проведено роботу з аналізу коефіцієнтів загроз та порівняння цих загроз після запропонованих заходів безпеки.

У третьому розділі було розраховано доцільність впроваджених методів для підвищення захисту підприємства, ефективність відносно економічних затрат та впровадження в систему на об'єкті інформаційної діяльності.

Практична цінність розробки полягає у ретельному аналізі моделі загроз та порушника, виявлення вразливостей та введення комплексних заходів підвищення захисту інформації інформаційно-комунікаційної системи «ТОВ БДО».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ЗЛОМИСНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ABSTRACT

Explanatory note: _72__ pp., _3__ pic., _12__ table, _3__ app, _17__ sources.

The diploma thesis is dedicated to the development and implementation of a comprehensive information security system for the information and communication system of BDO LLC. The primary objective is to ensure the confidentiality, integrity, and availability of the company's sensitive data. This involves assessing potential risks, defining security policies, and deploying appropriate technological and administrative measures to safeguard against cyber threats.

The study begins with an analysis of the current state of the information and communication infrastructure at BDO LLC, identifying key vulnerabilities and threats. It then proceeds to outline a multi-layered security framework, incorporating elements such as network security, access control, data encryption, and security monitoring.

Furthermore, the thesis examines the economic aspects of the information security system, evaluating the return on security investment (ROSI) and demonstrating the cost-effectiveness of the proposed measures. By implementing this comprehensive security system, BDO LLC aims to mitigate risks, comply with regulatory requirements, and protect its critical information assets from unauthorized access and cyberattacks.

This work provides a detailed roadmap for BDO LLC to enhance its information security posture, ensuring robust protection for its information and communication systems in the face of evolving cyber threats.

SECURITY POLICY, THREAT MODEL, INTRUDER MODEL, INFORMATION SYSTEM, CYBERSECURITY, INFORMATION SECURITY MANAGEMENT.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД - інформація з обмеженим доступом;

ІС - інформаційна система;

ІТС - інформаційно-телекомунікаційна система;

КЗСІ - комплексна система захисту інформації

ПЗ - програмне забезпечення;

СУІБ - система управління інформаційною безпекою.

ЗМІСТ

с.

ВСТУП

Актуальність дослідження: В умовах сучасного світу інформація стає одним із найцінніших ресурсів, а її захист - однією з ключових задач для будь-якої організації. Постійне зростання обсягу даних, активне використання інформаційно-комунікаційних технологій, а також циркуляції в ТОВ "БДО" конфіденційної інформації, інформації про фінанси клієнтів та багато іншої, робить питання захисту інформації надзвичайно актуальним.

З кожним роком кількість кіберзагроз та атак зростає, а методи зловмисників стають все більш витонченими. Компанії, що не приділяють достатньої уваги захисту своїх інформаційних систем, стають вразливими до різноманітних загроз, включаючи крадіжку конфіденційних даних, фінансові втрати, порушення нормального функціонування бізнес-процесів та втрату довіри з боку клієнтів і партнерів.

Для ТОВ "БДО", як і для багатьох інших компаній, інформація є основним активом, який потребує надійного захисту. Впровадження комплексної системи захисту інформації дозволяє мінімізувати ризики, пов'язані з несанкціонованим доступом, витоком даних, а також забезпечити відповідність нормативним вимогам у сфері інформаційної безпеки.

Таким чином, розробка та впровадження ефективної системи захисту інформації є надзвичайно актуальною задачею, яка дозволяє забезпечити стабільну роботу компанії, збереження її конкурентних переваг та репутації на ринку.

Мета дослідження: покращення та впровадження комплексної системи захисту інформації інформаційно-комунікаційної системи ТОВ БДО. Важливість роботи полягає у контексті зростаючих загроз інформаційної безпеки та необхідності захисту конфіденційних даних, які обробляються і зберігаються в інформаційній системі підприємства.

Об’єкт розробки: інформаційно-комунікаційна система міжнародної аудиторської компанії ТОВ «БДО».

Предмет розробки: механізми та засоби забезпечення захисту інформаційно-комунікаційної системи ТОВ «БДО» від сучасних кіберзагроз, включаючи заходи щодо захисту конфіденційних даних, запобігання несанкціонованому доступу та мінімізації ризиків витоку інформації.

Робота спрямована на забезпечення високого рівня захисту інформаційно-комунікаційної системи ТОВ БДО від сучасних кіберзагроз, що є критично важливим для безпеки та стабільності роботи підприємства.

Практичне значення полягає в покращенні функціонування інформаційно-комунікаційної системи підприємства. Запропоновані рішення сприяють забезпеченню високого рівня захищеності інформації, зменшенню ризиків витоку та несанкціонованого доступу до даних, а також покращенню загальної безпеки й ефективності діяльності підприємства.

Структура роботи: робота містить вступ, три розділи, висновки, список використаних джерел.

1. СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ.

1.1 Стан питання

До основних загроз, з якими стикалась міжнародна аудиторська компанія ТОВ «БДО», спеціалісти з кібербезпеки ТОВ «БДО» приділяють фішинг з смішингом, зловмисне ПЗ, програми-вимагачі, компрометація електронної пошти, надійні внутрішні загрози, ненавмисне розголошення, розвідка сховища, атаки нульового дня, соціальна інженерія та витік даних.

Під визначення загрози підпадає потенційна можливість порушити інформаційну безпеку. Найчастішими загрозами є саме ненавмисні помилки користувачів, системних адміністраторів та іншого персоналу, який пов'язаний з ІС підприємства. Прикладами є помилкове налаштування систем, необережне поводження з конфіденційною інформацією або випадкове видалення важливих файлів, помилки при введені даних та витік даних через користувачів системи. Найголовнішим засобом захисту є максимальна автоматизація, контроль та аудит даних, проведення постійних навчальних заходів з питань безпеки з користувачами ІС.

Загрози можуть бути людського або природного джерела та поділяються на випадкові або навмисні. Джерела випадкових та навмисних загроз обов'язково підлягають повній ідентифікації. Виникнення загрози може бути як з середини, так і ззовні організації. Ідентифікація загроз відбувається за родовим класом і типом. Під це може підпадати фізичне пошкодження, технічні аварії, неавторизовані дії та інше.

Зловмисне програмне забезпечення існує в багатьох формах та є дуже розповсюдженим типом атак, котре також нанесло і організації ТОВ «БДО» велику шкоду у 2017 році після масової атаки російськими хакерами на українські підприємства з використанням вірусного ПЗ під назвою «Petya». Була видалена та пошкоджена велика кількість даних та пристроїв, після чого був проведений самий великий аудит безпеки за історію компанії ТОВ «БДО», та були введені нові методології протидії загрозам.

Існує кілька основних методологій захисту інформаційних систем, кожна з яких має свої унікальні підходи та інструменти для забезпечення безпеки. Один із найпоширеніших підходів - захист на основі ризиків. Ця методологія включає в себе аналіз потенційних загроз, вразливостей та наслідків можливих інцидентів. Вона дозволяє визначити найкритичніші ризики та розробити пріоритетні заходи для їх зменшення. Управління ризиками є невід'ємною частиною цієї методології, спрямованою на зниження ризиків до прийнятного рівня шляхом впровадження відповідних контролів та процедур [2].

Іншим ключовим підходом є захист на основі шарів, або багатошаровий захист. Цей підхід передбачає використання кількох рівнів захисту для забезпечення безпеки. Він включає мультифакторний захист, який охоплює мережеві екрани, антивірусне програмне забезпечення, системи виявлення та запобігання вторгнень, а також інші засоби безпеки. Захист застосовується на всіх рівнях - від мережі до операційних систем, додатків та фізичного захисту, що забезпечує комплексний підхід до безпеки.

Безперервний моніторинг та аудит також є важливим аспектом захисту інформаційних систем. Постійний моніторинг безпеки включає використання SIEM-систем для збору та аналізу даних про події безпеки. Регулярні аудити допомагають перевірити відповідність політикам безпеки, виявити та усунути вразливості, забезпечуючи тим самим постійне підвищення рівня безпеки.

Керування доступом є ще однією ключовою методологією. Вона включає ідентифікацію та автентифікацію користувачів за допомогою багатофакторної автентифікації та управління доступом. Обмеження привілеїв для користувачів та надання доступу тільки тим, хто має відповідні повноваження, допомагає мінімізувати ризики несанкціонованого доступу до інформаційних ресурсів.

Криптографічний захист також відіграє важливу роль у забезпеченні інформаційної безпеки. Використання шифрування для захисту даних під час

зберігання та передачі, а також надійне управління криптографічними ключами є основними аспектами цієї методології.

Метою ідентифікації ризиків є визначення ймовірності подій, які можуть призвести до потенційних втрат, та ретельний аналіз причин виникнення цих витрат. Це є важливою складовою процесу управління ризиками, яка дозволяє компаніям розробляти ефективні стратегії для мінімізації негативного впливу ризиків на діяльність організації.

Необхідною частиною оцінки ризиків є ідентифікація наявних та запланованих заходів безпеки компанії для усунення зайвих затрат ресурсів та уникнення дублювання заходів безпеки. Дуже важлива перевірка, наскільки ефективно ці заходи спрацювали, які результати були отримані. При виявлені не працюючих або не релевантних заходів безпеки є ризик створення вразливості. В таких випадках потрібен повний розгляд ситуації, в якій обрані стратегії відмовляють під час функціонування, що потребує додаткових заходів безпеки для ефективного врахування ідентифікованого ризику [3].

До основної ідентифікації вразливостей компанія включає такі сфери:

- процеси та процедури;
- організація;
- персонал;
- залежність від зовнішніх сторін;
- фізичне оточення;
- порядок управління;
- ПЗ, обладнання чи комунікаційне обладнання.

Наслідками ризиків може бути втрата ефективності, особистих даних, втрата паролів та доступів, втрата бізнесу, репутації та інше. Ці події ідентифікують нанесення шкоди чи наслідки для організації, які могли бути спричинені описаними загрозами, що використовують вразливості або набір вразливостей в інциденті інформаційної безпеки. Сценарій інциденту має вплив на певну кількість ресурсів СУІБ, отже до них може бути прописано їх фінансову цінність, якщо ресурси буде пошкоджено або скомпрометовано.

По завершенню ідентифікації усіх сценаріїв, уповноваженими особами проводиться оцінка ймовірностей подій. Важливими критеріями для оцінки ймовірності подій є частота виникнення загроз, наслідки та наскільки легко використовуються вразливості. Для побудування цих критеріїв враховується досвід и доступна статистика імовірності загроз та мотивація і можливості зловмисників.

Оброблення та запобігання ризиків в контексті управління інформаційною безпекою є критично важливими аспектами для будь-якої організації. Компанії часто використовують чотири основні стратегії для управління ризиками: прийняття ризику, коли вони свідомо приймають можливий негативний вплив; модифікація ризику шляхом впровадження заходів для зменшення його впливу; усунення ризику, коли вони використовують заходи для повного усунення його наслідків; та розподілення ризику, коли вони делегують частину ризику іншим сторонам або використовують страхування.

Блок-схема управління ризиками інформаційної безпеки відображає ключові етапи цього процесу, включаючи ідентифікацію потенційних загроз, аналіз їх впливу, визначення відповідних стратегій оброблення ризиків, впровадження контрольних заходів та моніторингу ефективності вжитих заходів.

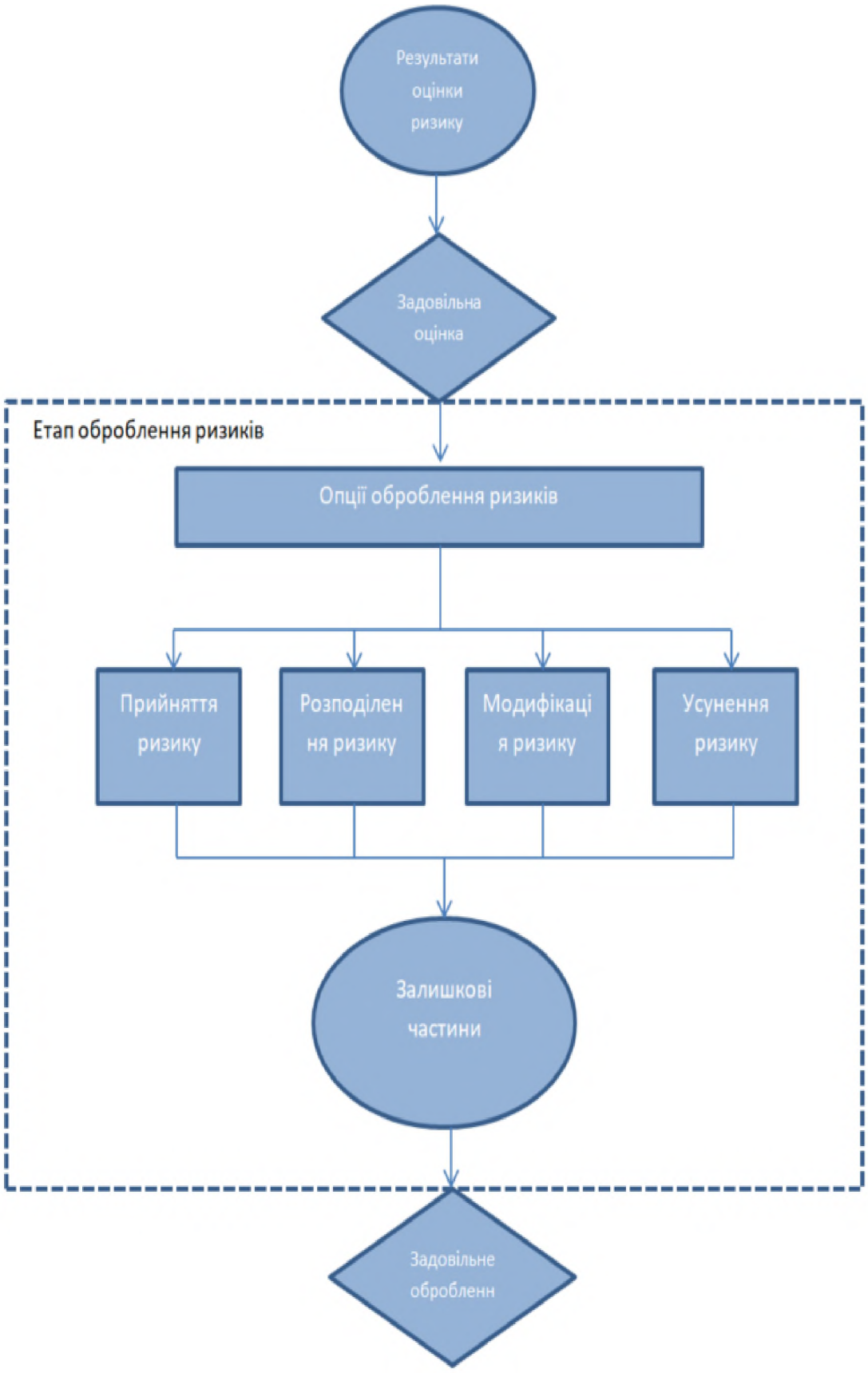


Рисунок 1.1 – Блок-схема етапів управління ризиками.

Важливо розглядати, що ризики не є статичними та вразливості, загрози або наслідки можуть змінюватись без будь-якої ідентифікації, через що проводиться постійний моніторинг для виявлення змін. В організації постійно проводиться моніторинг:

- необхідних модифікацій цінностей ресурсів СУІБ;

- нових загроз, що можуть виникати зсередини, ззовні та недооцінені загрози;

- нові ресурси СУІБ, ідентифіковані вразливості, які використовуються загрозами, що повторно виникли;

- інциденти інформаційної безпеки;

- посилений вплив чи наслідки оцінених загроз чи вразливостей.

У сучасному бізнес-середовищі, де інформаційна безпека є критично важливою, застосування програмного забезпечення для моніторингу ризиків стає невід'ємною частиною управління інформаційними системами. Компанія ТОВ «БДО» обрала один із найефективніших рішень у цій сфері, платформу RSA Archer, який дозволяє інтегрувати дані з різних джерел, що забезпечує повну картину ризиків і відповідності в організації. Це особливо важливо для великих компаній, де інформаційні потоки можуть бути складними та різноманітними.

1.2 Опис діяльності компанії

Міжнародна аудиторська компанія ТОВ «БДО» знаходиться за адресою вулиця Андрія Фабра, 4, м. Дніпро. Компанія має колективну форму власності та розподілений тип організації. Вид діяльності підприємства: діяльність у сфері бухгалтерського обліку та аудиту. Контрольованою зоною підприємства є поверх споруди.

До персоналу підприємства, який використовує ІС: Президент / старший партнер, директор виконавчий, керівник напрямку advisory, фінансовий директор, партнер з питань оцінки, партнер з аудиту - 5 осіб, директор з розвитку міжнародних відносин, маркетолог, керівник відділу бухгалтерського консультування та супроводу транзакцій, керівник відділу продажів, керівник

відділу з надання бухгалтерських послуг, керівник напряму «консалтинг в галузі охорони праці», старший юрист - 3 особи, проєктний менеджер, партнер з консалтингу, начальник відділу інформаційних технологій, аудитор інформаційний технологій, аудитор - 10 осіб, бухгалтер - 10 осіб, системний адміністратор - 4 особи [1].

Персонал, відповідальний за роботу та безпеку ІС: Начальник відділу інформаційних технологій, аудитор інформаційних технологій, 4 системний адміністратор.

В компанії ТОВ "БДО" циркулюють наступні типи інформації:

- фінансова інформація про клієнтів;
- бухгалтерська звітність;
- аудиторські звіти;
- конфіденційні дані клієнтів;
- внутрішня адміністративна інформація.

1.3 Основні та вторинні інформаційні потоки підприємства

У ході аналізу діяльності та інформаційних потоків ТОВ "БДО" було виявлено, що компанія має великий обсяг діяльності в сфері бухгалтерського обліку та аудиту. За визначенням основних та вторинних інформаційних потоків стало очевидним, що основними процесами в компанії є обробка аудитів та укладення та адміністрування договорів. До аудиту входить перелік кількості програмного забезпечення та закріплених пристроїв за персоналом.

Обробка аудитів:

1. Збір та обробка даних:

- компанія ТОВ "БДО" збирає фінансові дані від клієнтів для проведення аудитів;
- дані включають фінансові звіти, рахунки, контракти, податкові декларації та іншу релевантну документацію;
- дані обробляються за допомогою спеціалізованих програмних засобів для аналізу фінансової інформації та виявлення можливих порушень або невідповідностей.

2. Аналіз та підготовка висновків:

- отримані дані використовуються аналітиками та аудиторами компанії для проведення всебічного аналізу фінансового стану клієнтів.

- на основі аналізу готуються аудиторські висновки та звіти, які містять рекомендації щодо покращення фінансової звітності та управління.

3. Розповсюдження результатів аудиту:

- підготовлені звіти передаються клієнтам, керівництву компанії та регулюючим органам.

- результати можуть бути розповсюджені у вигляді електронних документів або в паперовій формі.

Договори:

1. Укладення договорів:

- компанія ТОВ "БДО" укладає договори з клієнтами на надання аудиторських послуг;

- договори містять інформацію про обсяги робіт, терміни виконання, вартість послуг та інші умови співпраці.

2. Адміністрування договорів:

- всі укладені договори реєструються в системі документообігу компанії;

- відстежується виконання умов договорів, своєчасність оплати послуг та дотримання термінів виконання робіт.

3. Зберігання та захист договорів:

- договори зберігаються в захищених електронних архівах та, при необхідності, в паперових архівах компанії;

- забезпечується конфіденційність та доступність договорів для співробітників, що мають відповідні повноваження.

Проведений аналіз інформаційних потоків ТОВ "БДО" дозволив виокремити не тільки основні, але й вторинні інформаційні потоки, які грають важливу роль у функціонуванні компанії. До вторинних інформаційних потоків відносяться такі аспекти, як кількість апаратних засобів та закріплення техніки за співробітниками.

Кількість апаратних засобів:

1. Інвентаризація апаратних засобів:

- облік усіх апаратних засобів, що знаходяться на балансі компанії;

- перелік кількості та моделей комп'ютерів, серверів, принтерів, мережевих обладнань та інших технічних засобів.

2. Моніторинг стану та оновлення:

- регулярний моніторинг технічного стану обладнання;

- проведення планових та позапланових оновлення та ремонтів апаратних засобів.

Закріплення техніки за співробітниками:

1. Розподіл обладнання:

- розподілення техніки між співробітниками компанії згідно з їхніми функціональними обов'язками.

- ведення обліку працівників з закріпленими до них пристроями для забезпечення відповідальності за його збереження та належне використання.

2. Управління доступом:

- отримання співробітниками доступу до техніки та систем на основі їхніх посадових обов'язків та рівня доступу.

- забезпечення контролю за доступом до конфіденційної інформації та критичних систем компанії.

1.3 Облік та управління апаратними засобами.

Перелік апаратних засобів:

Для забезпечення ефективної роботи компанії ТОВ "БДО" використовується широкий спектр апаратних засобів. Нижче наведено перелік

основних пристроїв, що використовуються співробітниками, з зазначенням моделей та кількості.

Вищий керівний склад (Президент, Директор виконавчий, Керівники напрямків):

- ноутбук: Dell Latitude 7420 (15 шт);

- смартфон: iPhone 14 (15 шт).

Партнери з аудиту та фінансові директори:

- ноутбук: HP EliteBook 850 G8 (10 шт);

- смартфон: Samsung Galaxy S23 (10 шт).

Керівники відділів (маркетинг, бухгалтерське консультування, продажі, бухгалтерські послуги, консалтинг в охороні праці):

- ноутбук: Lenovo ThinkPad X1 Carbon (5 шт);

- смартфон: Samsung Galaxy S23 (5 шт).

Старші юристи, HR Partner, Проєктний менеджер, Аудитор інформаційних технологій, Партнер з консалтингу:

- ноутбук: Dell XPS 13 (7 шт);

- смартфон: iPhone 14 (7 шт).

Аудитори:

- ноутбук: HP EliteBook 850 G8 (10 шт);

- смартфон: Samsung Galaxy S23 (10 шт).

Бухгалтери:

- ноутбук: Dell Latitude 7420 (10 шт);

- смартфон: iPhone 14 (10 шт).

Системні адміністратори:

- робочі станції: Dell Precision 3640 (4 шт) ;

- смартфон: Samsung Galaxy S23 (4 шт).

Додаткове обладнання

Для забезпечення безперебійної роботи ІКС також використовується додаткове серверне та мережеве обладнання, а також периферійні пристрої:

Серверне обладнання:

- сервери: Dell PowerEdge R740 (2 шт).

Мережеве обладнання:

- роутери: Cisco ISR 4331 (2 шт);
- комутатори: Cisco Catalyst 9300 (4 шт)
- принтери та сканери:
- принтери: HP LaserJet Enterprise MFP M528f (4 шт)
- сканери: Fujitsu fi-7160 (3 шт)
- Wi-Fi точки доступу: Cisco Aironet 3800 Series, Aruba AP-535
- сервери: Dell PowerEdge R740, HPE ProLiant DL380 Gen10

Таблиця 1.1 - Програмне забезпечення

Назва версії програмного забезпечення	Тип ліцензії
Windows 11	Комерційна, закрита, Windows 11 Enterprise
Windows Server 2022 Standard	Комерційна, закрита
Microsoft Office 2021 Professional Plus	Комерційна, закрита, одноразове придбання
Acronis Cyber Protect	Комерційна, закрита, річна підписка
Cisco AnyConnect Secure Mobility Client	Комерційна, закрита
Microsoft System Center 2022	Комерційна, закрита
Adobe Acrobat Pro DC	Комерційна, закрита, річна підписка

Продовження таблиці 1.1

Назва версії програмного забезпечення	Тип ліцензії
VMware Workstation Pro	Комерційна, закрита, одноразове придбання
M.E.Doc	Комерційна, закрита, одноразове придбання

Таблиця 1.2 - Класифікація інформаційної системи та її елементів

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення	Вимоги до захисту		
1	Інформація про діяльність підприємства	Відкрита	Відкрита	Електронний та паперовий	К	Ц	Д
2	Договори аудиту	З обмеженим доступом	Конфіденційна	Електронний та паперовий	К	Ц	Д
3	Фінансовий облік компаній-клієнтів	З обмеженим доступом	Конфіденційна	Електронний та паперовий	К	Ц	Д
4	Фінансовий облік компанії	З обмеженим доступом	Конфіденційна	Електронний та паперовий	К	Ц	Д
5	Юридична інформація	З обмеженим доступом	Конфіденційна	Електронний та паперовий	К	Ц	Д

Продовження таблиці 1.2

№	Вид інформації	Режим доступу	Правовий режим	Вид представлення	Вимоги до захисту		
6	Данні про доходи компанії	З обмеженим доступом	Конфіденційна	Електронний	К	Ц	Д
7	Технічні завдання відділу безпеки	З обмеженим доступом	Комерційна таємниця	Електронний та паперовий	К	Ц	Д
8	Інформація про діяльність відділів компанії	Комерційна таємниця	Комерційна таємниця	Електронний та паперовий	-	Ц	-

Матриця доступу є ключовим інструментом управління доступом до інформаційних ресурсів. Вона визначає, які користувачі мають доступ до яких об'єктів із системи, регулюючи права і обмеження доступу з метою забезпечення безпеки та конфіденційності даних. Це таблиця, в якій рядки відповідають користувачам або групам користувачів, а стовпці відповідають ресурсам або об'єктам у системі. Кожна комірка матриці містить права доступу, які визначають, що конкретний користувач може робити з конкретним об'єктом. Основними принципами роботи матриці доступу є ідентифікація та аутентифікація користувачів, авторизація прав доступу на основі матриці, а також аудит та логування спроб доступу. Це забезпечує гнучкий, чіткий контроль і високий рівень безпеки, знижуючи ризики несанкціонованого доступу до конфіденційної інформації, що є необхідною частиною будування комплексної системи захисту інформації.

Таблиця 1.3 - Матриця доступу до інформації.

Інформація	Посада					
	Фінансові директора	Аудитор	Бухгалтер	Юрист	Системний адміністратор	Начальник та аудитор відділу інформаційних технологій
1	CRWDP	RP	RP	RP	RP	RP
2	CRWDP	CRWDP	CRWDP	CRWDP	RP	RP
3	CRWDP	CRWDP	CRWDP	RP	RP	RP
4	CRWDP	CRWDP	CRWDP	RP	RP	RP
5	CRWDP	RWP	RWP	CRWDP	RP	CRWDP
6	CRWDP	CRWDP	CRWDP	RP	RP	RP
7	CRWDP	RP	RP	RP	CRWDP	CRWDP
8	CRWDP	RP	RP	RP	RP	CRWDP

1.4 Постановка задачі.

Так як в організації циркулює інформація з обмеженим доступом, а саме конфіденційна інформація, то ця інформація потребує захисту і на підприємстві виникає необхідність створення комплексної системи захисту інформації. Необхідно виконати обстеження інформаційної системи, персоналу, програмного забезпечення, розробити модель загроз та модель порушника та розробити заходи з забезпечення безпеки інформації.

Висновки до першого розділу.

У ході аналізу діяльності та інформаційних потоків ТОВ "БДО" було виявлено, що компанія має великий обсяг діяльності в сфері бухгалтерського обліку та аудиту, та в підприємстві циркулює інформація з обмеженим доступом. За визначенням основних та вторинних інформаційних потоків

визначили, що основними процесами в компанії є обробка аудитів, збір та обробка фінансових даних, укладення та адміністрування договорів, а також облік та управління апаратними засобами. Проведений аналіз також дозволив виявити загрози та потенційні ризики для інформаційної безпеки компанії.

2. ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ТОВ "БДО"

2.1 Поточний стан інформаційної безпеки в ТОВ "БДО"

Об'єктом досліджень було обрано інформаційно-телекомунікаційну систему підприємства ТОВ "БДО". У процесі дослідження основна увага була приділена аналізу існуючої ІТС компанії з метою визначення її поточного стану захисту інформації та виявлення потенційних загроз і вразливостей. ІТС ТОВ "БДО" включає в себе апаратне та програмне забезпечення, мережеву інфраструктуру, а також організаційні процеси, що забезпечують функціонування інформаційних систем компанії. З метою збереження конфіденційності та захисту секретної інформації, що циркулює в межах ІТС ТОВ "БДО", під час дослідження було здійснено анонімізацію та модифікацію даних.

Таблиця 2.1 - Структура організації.

Посада	Хто підпорядковується
Президент / Старший партнер	Директор виконавчий, фінансовий директор, директор з розвитку міжнародних відносин.
Директор виконавчий	Керівник напрямку advisory, маркетолог, старший юрист, проєктний менеджер.
Фінансовий директор	Партнер з питань оцінки, партнер з аудиту, керівник відділу з надання бухгалтерських послуг, аудитор, бухгалтер.

Продовження таблиці 2.1

Посада	Хто підпорядковується
Керівник відділу з надання бухгалтерських послуг	Аудитор, бухгалтер
Аудитор інформаційний технологій	Системний адміністратор

Кількість співробітників в компанії становить 47 чоловік. 16-23 співробітника працюють в офісі, інші дистанційно.

Таблиця 2.2 - Місця роботи працівників.

Посада	Робота віддалено / в офісі
Президент / Старший партнер	віддалено
Директор виконавчий	в офісі
Керівник напрямку Advisory	віддалено
Фінансовий директор	віддалено
Партнер з питань оцінки	віддалено
Партнер з аудиту - 5 осіб	віддалено
Маркетолог	віддалено
Керівник відділу з надання бухгалтерських послуг	віддалено
Старший юрист - 3 особи	1 особа - віддалено, 2 особи - в офісі
Проєктний менеджер	в офісі
Аудитори - 10 осіб	5 осіб - віддалено, 5 осіб - в офісі
Бухгалтери - 10 осіб	5 осіб - віддалено, 5 осіб - в офісі
Системний адміністратор - 4 особи	2 особи - віддалено, 2 особи - в офісі
Аудитор інформаційний технологій	в офісі

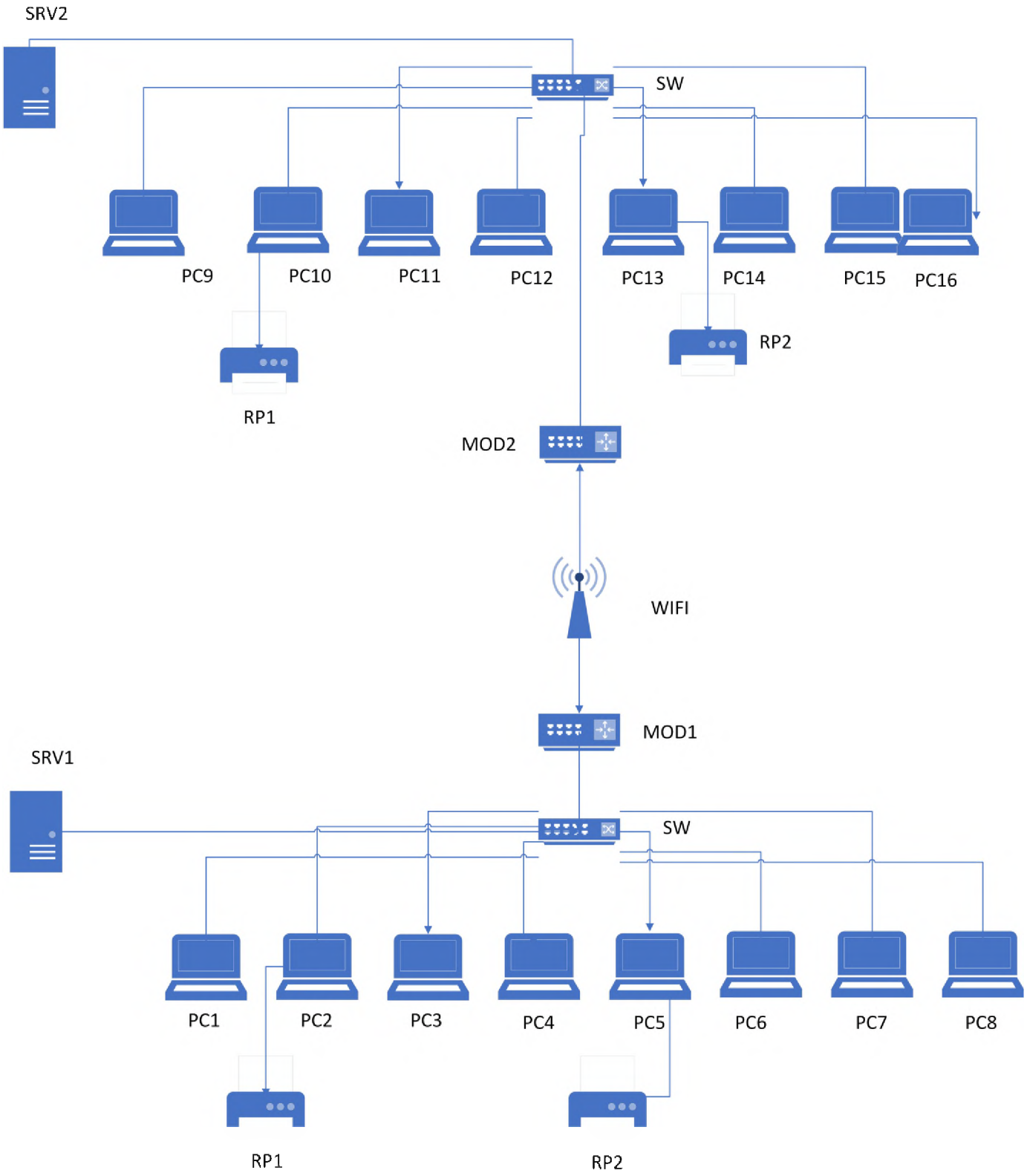


Рисунок 2.1 Схема мережі

Проведення детального вивчення об'єкта є критичним етапом у створенні комплексної системи захисту інформації. На цьому етапі здійснюється глибокий аналіз всіх аспектів об'єкта, включаючи його фізичну інфраструктуру, інформаційно-комунікаційні системи, програмне забезпечення та організаційні процеси. Уточнення моделі загроз включає виявлення потенційних загроз інформаційній безпеці, таких як несанкціонований доступ, витік даних, зловмисне програмне забезпечення, внутрішні загрози від співробітників тощо. Важливо також ідентифікувати потенційного порушника, який може здійснити атаки на інформаційні системи компанії. Це можуть бути як зовнішні зловмисники (хакери, конкуренти), так і внутрішні (незадоволені працівники, випадкові порушники). Аналіз можливості керування ризиками передбачає оцінку ймовірності реалізації кожної загрози та потенційних наслідків для компанії. Цей аналіз допомагає визначити пріоритети у впровадженні заходів безпеки та розробити стратегії для мінімізації ризиків. В результаті, компанія отримує чітке уявлення про свої слабкі місця та необхідні заходи для їх захисту[9].

Найбільш оптимальним варіантом, відповідно до п. 32 ДСТУ 3396.1, було обрано досягнення максимального рівня захисту ІзОД за необхідними затратами та допустимого рівня обмежень видів ІД. Згідно з пунктом 32 ДСТУ 3396.1, найкращим підходом до забезпечення інформаційної безпеки є баланс між максимальним рівнем захисту інформації з обмеженим доступом та раціональними витратами на реалізацію захисних заходів. Це означає, що для досягнення високого рівня захисту інформації необхідно не тільки впроваджувати технічні засоби захисту, але й враховувати економічну доцільність таких заходів. Досягнення максимального рівня захисту включає використання сучасних технологій, таких як шифрування даних, багатофакторна автентифікація, моніторинг та виявлення загроз у реальному часі, а також регулярні аудити та тестування систем безпеки. Рівень обмежень доступу до інформації має бути допустимим та не впливати негативно на ефективність бізнес-процесів. Впроваджені заходи безпеки повинні бути

зручними для користувачів та не створювати зайвих перешкод у роботі співробітників, що може призвести до зниження продуктивності або навіть до спроб обійти системи захисту [15].

Технічне завдання на створення комплексної системи захисту інформації (КЗСІ) в інформаційно-телекомунікаційній системі (ІТС) є основоположним організаційно-технічним документом. Цей документ визначає всі вимоги щодо захисту інформації, яка оновлюється в ІТС, а також регламентує порядок створення КЗСІ, проведення всіх видів випробувань та введення її в експлуатацію в складі ІТС. Технічне завдання є ключовим документом під час аналізу автоматизованих систем (АС) на відповідність вимогам інформаційної безпеки. Розробка технічного завдання відбувається на відповідній стадії створення ІТС, враховуючи комплексний підхід до побудови КЗСІ. Цей підхід передбачає об'єднання всіх необхідних заходів та засобів захисту від різноманітних загроз безпеці інформації на всіх етапах життєвого циклу ІТС. Комплексний підхід означає, що технічне завдання охоплює не лише технічні аспекти, такі як налаштування програмного та апаратного забезпечення, але й організаційні заходи, включаючи навчання співробітників, розробку політик безпеки та процедури реагування на інциденти.

Технічне завдання для КЗСІ може створюватись для вперше створених ІТС, а також під час модернізації вже існуючих ІТС.

При створенні та оформлені ТЗ використовуються такі варіанти:

- у вигляді окремого (часткового) ТЗ;
- у вигляді доповнення до ТЗ;
- у вигляді окремого розділу ТЗ на створення ІТС.

Під час виконання обстеження ІТС розглядається як організаційно-технічна система, яка поєднує:

- фізичне середовище;
- обчислювальну систему;
- середовище користувачів.

Оброблювану інформацію і технологію її обробки.

Метою обстеження є підготовка базових даних для формування вимог до комплексної системи захисту інформації. Цей процес включає детальний опис кожного середовища функціонування інформаційно-телекомунікаційної системи (ІТС) та виявлення елементів, які можуть безпосередньо або опосередковано впливати на безпеку інформації. Обстеження спрямоване на виявлення всіх факторів, що можуть становити загрозу для інформаційної безпеки, а також на аналіз взаємодії та впливу цих елементів одне на одного.

Основні завдання обстеження включають:

1.Опис середовищ функціонування ІТС: детальне вивчення і документування всіх середовищ, у яких функціонує ІТС, включаючи апаратне та програмне забезпечення, мережеву інфраструктуру, фізичне середовище (офісні приміщення) та організаційні процеси.

2.Виявлення елементів, що впливають на безпеку інформації: ідентифікація всіх компонентів системи, які можуть впливати на безпеку інформації, таких як сервери, робочі станції, мережеві пристрої, системи зберігання даних, програми та користувачі.

3.Аналіз взаємного впливу елементів різних середовищ: дослідження взаємодії між різними елементами системи та середовищами, в яких вони функціонують, з метою виявлення потенційних точок вразливості та взаємозв'язаних загроз.

4.Документування результатів обстеження: створення детальної документації, яка містить результати обстеження, включаючи опис виявлених елементів, їх взаємодії та впливу на безпеку інформації. Ця документація буде використовуватися на наступних етапах робіт для розробки вимог до КСЗІ та подальшого проєктування системи захисту.

Обстеження є критично важливим етапом у процесі створення комплексних систем захисту інформації (КСЗІ). Цей етап дозволяє отримати детальні дані про поточний стан інформаційних ресурсів організації, ідентифікувати потенційні загрози та ризики, що можуть вплинути на безпеку інформації. На основі отриманих даних розробляються конкретні вимоги до

системи захисту інформації, визначаються необхідні заходи зі зміцнення безпеки і розробляються стратегії захисту, що відповідають унікальним потребам організації.

Відповідно до документу НД ТЗІ 2.5-004-99 зі змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» побудуємо профіль захищеності, вказавши опис послуг та необхідні умови: 3.КЦ.1={КД-2, КВ-3, ЦД-3, ЦО-2, НИ-2, НО-2, НА-2} [16] [17].

Таблиця 2.3 - Профіль захищеності.

№	Послуга	Назва послуги	Опис послуги	Необхідні умови
1	КД-2	Базова довірча конфіденційність	Ця послуга дозволяє користувачу керувати інформаційними потоками від захищених об'єктів його домену до інших користувачів. Рівні послуги визначаються рівнем захисту і керування.	НИ-1
2	КВ-3	Повна конфіденційність при обміні	Політика конфіденційності при обміні, що реалізується КЗЗ, охоплює всі об'єкти і інтерфейсні процеси. Вона визначає рівень захищеності, забезпечуваний використовуваними механізмами, і дозволяє користувачам і/або процесам керувати цим рівнем. КЗЗ забезпечує захист від несанкціонованого ознайомлення з інформацією, що передається об'єктом.	НО-1 НВ-1

Продовження таблиці 2.3

№	Послуга	Назва послуги	Опис послуги	Необхідні умови
3	ЦД-3	Повна довірча цілісність	Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів його домену. Рівні захисту і керування визначаються відповідно до повноти захисту та вибірковості управління. Політика довірчої цілісності, реалізована КЗЗ, визначає множину об'єктів КС, до яких вона стосується.	КО-1 НИ-1
4	ЦО-2	Повний відкат	Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.	НИ-1
5	НИ-2	Одиночна ідентифікація і автентифікація	Ідентифікація і автентифікація дозволяють КЗЗ визначати і перевіряти особистість користувача, який намагається отримати доступ до КС. Рівні цієї послуги визначаються кількістю задіяних механізмів автентифікації. Політика ідентифікації і автентифікації, реалізована КЗЗ, встановлює атрибути, що характеризують користувача, і послуги, які вимагають цих атрибутів. Кожен користувач повинен однозначно ідентифікуватися перед КЗЗ.	НК-1

Продовження таблиці 2.3

№	Послуга	Назва послуги	Опис послуги	Необхідні умови
6	НО-3	Розподіл обов'язків на підставі привілеїв	Ця послуга дозволяє знижувати потенційні збитки від навмисних або помилкових дій користувача і обмежувати авторитарність управління. Політика розподілу обов'язків, реалізована КЗЗ, визначає ролі адміністратора і звичайного користувача, а також їхні функції. Мінімум дві адміністративні ролі мають бути обов'язково визначені: адміністратор безпеки та інший адміністратор. Функції кожної ролі повинні бути мінімізовані і включати лише необхідні для виконання цих ролей завдання. Користувач повинен мати можливість приймати певну роль лише після виконання певних дій, що підтверджують його призначення на цю роль.	НИ-1
7	НА-1	Базова автентифікація відправника	Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем.	НИ-1

2.2 Виявлення моделі порушника та аналіз загроз інформації

Для чіткого побудування КЗСІ важливий етап побудування моделі порушника, що поділяється на **осіб** з доступом в КЗ та осіб без доступу. Потенційних порушників можна поділити на зовнішніх та внутрішніх, що здійснюють атаки за межами або в межах КЗ. В таблиці розписано більш детально про порушників, їх мотиви, рівень обізнаності, можливості для подолання системи захисту, можливості за часом та місцем та сума загроз.

Таблиця 2.4 - Модель порушника.

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Президент / Старший партнер	М1	К4	З1	Ч1	Д2	17
Директор виконавчий	М1	К4	З1	Ч1	Д2	17
Директор виконавчий	М1	К4	З1	Ч1	Д2	17
Фінансовий директор	М1	К3	З1	Ч1	Д2	16
Партнер з питань оцінки	М1	К3	З1	Ч1	Д2	16
Партнер з аудиту	М1	К3	З1	Ч1	Д2	16

Продовження таблиці 2.3

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор з розвитку міжнародних відносин	М1	К3	З1	Ч1	Д2	16
Керівник відділу маркетингу	М1	К3	З1	Ч1	Д2	16
Керівник відділу бухгалтерського консультування та супроводу транзакцій	М1	К3	З1	Ч1	Д2	16
Керівник відділу з надання бухгалтерських послуг	М1	К3	З1	Ч1	Д2	16
Керівник напряму «Консалтинг в галузі охорони праці»	М1	К3	З1	Ч1	Д2	16
Старший юрист	М1	К2	З1	Ч2	Д2	17

Продовження таблиці 2.3

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Проєктний менеджер	М1	К2	З2	Ч2	Д2	18
Партнер з консалтингу	М1	К2	З2	Ч2	Д2	18
Начальник відділу інформаційних технологій	М1	К4	З3	Ч2	Д2	21
Аудитор інформаційний технологій	М1	К4	З3	Ч2	Д2	21
Аудитор	М1	К2	З2	Ч2	Д2	18
Бухгалтер	М1	К2	З2	Ч2	Д2	18
Системний адміністратор	М1	К4	З3	Ч3	Д2	18
Прибиральниця	М1	К1	З1	Ч3	Д1	11
Охоронець	М1	К1	З1	Ч3	Д1	11
Зловмисник	М2	К4	З3	Ч2	Д3	21

М1 - Безвідповідальність (недбалість, ненавмисне порушення) - 3

М2 - Корислива цілеспрямованість (зловмисне порушення) - 5

К1 - Не має знань та інформації про порядок функціонування інформаційної системи, а також не володіє навичками користування штатними засобами обробки та захисту інформації. - 1

К2 - Має навички щодо користування ПК на рівні користувача - 3

К3 - Має базові знання про функціонування програмного забезпечення та операційних систем, а також володіє практичними навичками роботи із засобами обробки інформації. - 4

К4 - Володіє знаннями щодо: функціонування засобів та механізмів обробки інформації та її захисту, що використовуються на ІС та їх недоліків. - 5

З1 - Має фізичний доступ до компонентів ІС, але не є авторизованим користувачем ІС - 2

З2 - Має можливість запуску програм, що реалізують функції обробки інформації - 3

З3 - Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації. - 4

Ч1 - Під час бездіяльності компонентів системи - 3

Ч2 - Під час функціонування ІС - 5

Ч3 - Під час перерв у роботі для обслуговування та ремонту - 2

Д1 - Усередині приміщення, без доступу до технічних засобів ІС - 3

Д2 - З робочих місць користувачів та персоналу ІС, місць розміщення обладнання ІС, де обробляється інформація, яка підлягає захисту - 4

Д3 - Без доступу до приміщень, також враховуючи з зовнішніх каналів зв'язку, з можливістю застосування технічних засобів здобуття інформації оптичними, акустичними каналами. - 2

Ще одним важливим фактором є визначення моделі загроз. Правильно розрахована модель з включенням усіх необхідних факторів, дозволяє визначити існуючи загрози, створити контрзаходи, при цьому підвищити рівень безпеки ІТС та оптимізувати витрати. Протягом життєвого циклу системи необхідно мати повну модель загроз, для використання її при

експлуатації, проєктуванні, модернізації та проведені регламентних та ремонтних робіт.

Модель загроз має використовуватись для вирішення задач з аналізу захищеності від загроз в ході проведення робіт з питань інформаційної безпеки, контролю над забезпеченням вимог та проведення профілактичних засобів з запобігання НДС.

Таблиця 2.5 - модель загроз.

Вид загрози	Джерело загрози	Вразливості	Наслідки
Навмисні загрози			
Копіювання ІзОД	Зловмисник	Відсутність політики безпеки, яка регламентує використання дозволеного програмного забезпечення.	К, Д
Несанкціонований доступ	Зловмисник	Ненадійна система охорони, недотримання правил використання комп'ютерних систем, відсутність системи розмежування доступу.	К, Ц, Д
Крадіжка	Зловмисник	Недосконала система фізичної охорони або охоронних заходів.	Д

Продовження таблиці 2.5

Вид загрози	Джерело загрози	Вразливості	Наслідки
Навмисні загрози			
Порушенні цілісності інформації	Зловмисник, користувач	Відсутність шифрування даних та резервного копіювання.	К, Ц, Д
Копіювання ІзОД	Зловмисник	Відсутність політики безпеки регулювання використання дозволених ПЗ.	К, Д
Соціальна інженерія	Зловмисник	Наявність тренінгів та навчальних програм для персоналу.	К, Ц, Д
Ddos атаки	Зловмисник	Недостатній захист мережної інфраструктури.	Д
Ненавмисні загрози			
Помилки	Користувач	Порушення правил, передбачених політикою інформаційної безпеки.	К, Ц
Вірусне зараження	Користувач, зловмисник	Відсутність антивірусних програмних засобів, використання піратського ПЗ	К, Ц

Продовження таблиці 2.5

Вид загрози	Джерело загрози	Вразливості	Наслідки
Навмисні загрози			
Технічні несправності	Користувач	Ігнорування правил використання пристроїв чи ПЗ.	Д
Ненавмисні дії користувачів	Користувач	Низький рівень кваліфікації користувачів	К, Ц
Розголошення таємної або конфіденційної інформації	Користувач	Низький рівень кваліфікації користувачів	К, Ц

Після формування моделі порушника та моделі загроз, важливо зазначити ймовірність ризиків та коефіцієнт наслідку події.

Таблиця 2.6 - Коефіцент ризиків наслідку подій.

Тип загрози	Конкретна загроза	Коефіцієнт ймовірності	Коефіцієнт впливу	Коефіцієнт ризику
Кіберзлочинці	Несанкціонований доступ до даних	Високий (0.8)	Високий (0.9)	0.72
	Викрадення конфіденційної інформації	Високий (0.8)	Високий (0.9)	0.72
	Встановлення шкідливого ПЗ	Високий (0.7)	Середній (0.7)	0.49

Продовження таблиці 2.6

Тип загрози	Конкретна загроза	Коефіцієнт ймовірності	Коефіцієнт впливу	Коефіцієнт ризику
Внутрішні загрози	Зловмисні дії співробітників	Середній (0.5)	Високий (0.8)	0.40
	Випадкові дії співробітників	Високий (0.6)	Середній (0.6)	0.36
	Зловживання правами доступу	Середній (0.5)	Високий (0.7)	0.35
Фізичні загрози	Крадіжка обладнання	Низький (0.3)	Високий (0.9)	0.27
	Несанкціонований фізичний доступ до серверів	Низький (0.3)	Високий (0.8)	0.24
Програмні загрози	Віруси	Високий (0.7)	Середній (0.6)	0.42
	Трояни	Високий (0.6)	Середній (0.7)	0.42
	Ransomware (вимагальне ПЗ)	Середній (0.5)	Високий (0.8)	0.40
Атаки типу "відмова в обслуговуванні" (DoS/DDoS)	Атаки на веб-сервери	Середній (0.5)	Високий (0.8)	0.40
	Атаки на мережеву інфраструктуру	Середній (0.5)	Високий (0.7)	0.35
Людські помилки	Неправильне налаштування систем	Високий (0.7)	Середній (0.6)	0.42

Продовження таблиці 2.6

Тип загрози	Конкретна загроза	Коефіцієнт ймовірності	Коефіцієнт впливу	Коефіцієнт ризику
Людські помилки	Випадкове видалення або зміна даних	Високий (0.8)	Середній (0.6)	0.48
	Неправильна обробка конфіденційної інформації	Високий (0.7)	Середній (0.7)	0.49

2.3 Впровадження технічних заходів захисту

Першим етапом впровадження заходів захисту для підприємства є розробка комплексної політики безпеки. Основною метою цієї політики є встановлення чітких вимог щодо використання доступів та паролів для користувачів автоматизованої системи. Політика безпеки розробляє правила та процедури, яких зобов'язані дотримуватись всі співробітники, забезпечуючи тим самим дотримання стандартів інформаційної безпеки.

Основні правила для створених паролів:

- заборонено використання персональних даних, а саме: ПІБ співробітника, родичів, назву компанії, дати народження та інше);
- пароль має бути мінімум 12 символів та містити літери малого та великого реєстру, містити числа та спеціальні символи;
- заборонено використовувати послідовні паролі, типу “qwerty”, “abcd”, “1234567890”;
- паролі мають змінюватись кожного місяця;
- паролі не мають містити існуючи слова.

Політика використання електронної пошти та запобігання фішинговим загрозам.

Мета та основні положення політики:

Політика використання електронної пошти та запобігання фішинговим атакам має на меті встановити чіткі вимоги для користування корпоративною електронною поштою, а також запобігти атакам соціальної інженерії. Одержання зловмисником доступу до корпоративної електронної пошти може мати серйозні наслідки, включаючи викрадення конфіденційної інформації, отримання доступу до фінансових ресурсів, документів, паролів та інших критично важливих даних.

Вимоги до використання корпоративної електронної пошти

1. Захист електронних листів:

- уся інформація, що передається через корпоративну електронну пошту, повинна містити електронний цифровий підпис для підтвердження автентичності відправника та забезпечення цілісності повідомлення.

2. Безпечне зберігання документів:

- документи, які зберігаються в хмарних сховищах, повинні відкриватися виключно з корпоративних облікових записів електронної пошти. Забороняється відкривання файлів за допомогою особистих або сторонніх облікових записів електронної пошти, не пов'язаних з компанією.

Запобігання фішинговим атакам

1. Заборона переходу за підозрілими посиланнями:

- забороняється перехід за будь-якими посиланнями, які містяться у електронних листах, якщо їхня достовірність не підтверджена;

- Забороняється взаємодія з підозрілими електронними листами, які можуть містити фішингові посилання або вкладення.

2. Підвищення обізнаності співробітників:

- впровадження регулярних тренінгів для підвищення обізнаності співробітників з питань фішингу та інших кіберзагроз.

- проведення тестових фішингових кампаній для оцінки готовності співробітників протидіяти фішинговим атакам. Співробітники, які не пройшли перевірку, мають пройти повторні тренінги.

Проведення на підприємству постійного моніторингу та аудиту є невід'ємною частиною безпеки, допомагає виявити існуючи проблеми та впровадити нові рішення за допомогою отриманої інформації. Метою системи моніторингу є забезпечення постійного контролю за дотриманням політики безпеки, що дозволяє своєчасно виявляти підозрілі дії та можливі порушення. За допомогою цієї системи забезпечується оперативна реакція на потенційні загрози безпеці.

Регулярні аудити є необхідним елементом ефективного контролю за безпекою корпоративної електронної пошти. Під час аудитів оцінюється ефективність впроваджених заходів безпеки, виявляються потенційні вразливості та ризики, а також розробляються рекомендації щодо удосконалення політики безпеки. Аудити також включають перевірку дотримання працівниками встановлених стандартів безпеки при використанні корпоративної електронної пошти. Це включає в себе перевірку слабких місць, неправильних практик та можливих порушень безпеки.

У разі порушення встановлених правил безпеки, співробітники можуть бути піддані різноманітним дисциплінарним заходам згідно з внутрішніми регламентами компанії. Ці заходи можуть включати усні або письмові попередження, тимчасове або постійне обмеження доступу до корпоративної електронної пошти, а також звільнення у випадку серйозних порушень.

Впровадження механізму для анонімного повідомлення про порушення політики безпеки, що дозволяє співробітникам безпечно інформувати про підозрілі дії або недотримання правил. Прийняття своєчасних заходів для розслідування та усунення виявлених порушень, а також запобігання їх повторенню у майбутньому.

Система моніторингу є важливим етапом впровадження заходів захисту для підприємства. Її мета полягає в постійному контролі за дотриманням

політики безпеки, виявленні підозрілих дій та можливих порушень. Встановлення постійної системи моніторингу дозволяє забезпечити своєчасну реакцію на потенційні загрози. Поділяється на два етапи:

1. Встановлення постійної системи моніторингу: Цей етап передбачає створення та постійне функціонування системи моніторингу для контролю за дотриманням політики безпеки. Ця система дозволяє своєчасно виявляти підозрілі дії та можливі порушення.

2. Використання спеціалізованого програмного забезпечення: Застосування спеціалізованого програмного забезпечення для автоматичного виявлення підозрілих активностей у корпоративній електронній пошті. Ці інструменти надійно захищають корпоративну електронну пошту від потенційних загроз і допомагають оперативно реагувати на них.

Недотримання встановлених вимог може призвести до серйозних наслідків, таких як викрадення конфіденційної інформації, отримання зловмисниками доступу до фінансових ресурсів, документів та паролів, що може спричинити значні фінансові втрати та пошкодження репутації компанії. Співробітники, які порушують правила безпеки, можуть бути піддані дисциплінарним заходам відповідно до внутрішніх регламентів компанії.

Запровадження та дотримання цієї політики сприятиме підвищенню рівня інформаційної безпеки в компанії та забезпеченню захисту корпоративних даних від кіберзагроз.

Ефективним та безпечним способом зберігання інформації є впровадження зберігання даних у хмарних середовищах. Компанія використовує рішення від Google та Microsoft. Такий метод забезпечує швидкий та безпечний доступ до інформації в середині компанії, запобігання втрати, змінення або викрадання інформації. Основними перевагами є доступність, зменшення витрат, забезпечення безпеки даних, автоматичне резервне копіювання. Хмарні сховища надають можливість звертатися до інформації з будь-якого місця, де є інтернет-з'єднання. Це компактне рішення для компаній з розподіленими командами або для роботи віддалено.

Використання хмарних сховищ дозволяє уникнути значних витрат на обладнання та його підтримку, оскільки інфраструктура для зберігання даних розміщується на серверах постачальника хмарних послуг. Відповідно до сучасних вимог безпеки, провайдери хмарних сховищ мають високий рівень захисту. Вони застосовують шифрування, механізми автентифікації та авторизації, а також інші заходи безпеки для захисту конфіденційної інформації. Хмарні сховища часто автоматично створюють резервні копії даних, що дозволяє уникнути втрати інформації у разі виникнення проблем зі зберіганням або знищенням оригінальних даних. Інфраструктура хмарних сховищ може легко масштабуватися з ростом потреб користувача. Це означає, що компанія може легко збільшувати або зменшувати обсяг зберігання даних, відповідаючи поточним потребам. Хмарні сховища дозволяють легко обмінюватися даними між співробітниками та спільно працювати над документами та проєктами.

Для захисту від шкідливого ПЗ, вірусів, програм-шахраїв та інших необхідно встановлення на усі пристрої ліцензійного антивіруса, який комплексно перевіряє систему та браузер на наявність загрози, постійно та автоматизовано робить перевірку, не впливаючи та не загальмовуючи роботу пристроя. Політикою безпеки заборонено відвідування підозрілих та незахищених сайтів, що не мають протоколу безпеки HTTPS. Усі програми, які використовуються для роботи мають бути ліцензійними та перевіреними. Рекомендовано ввести додаткові засоби безпеки від завантаження шкідливого ПЗ, а саме:

- видання працівникам робочих пристроїв, ноутбуків, комп'ютерів та інше, які не будуть використовуватись в персональних цілях, а тільки робочих;

- встановлення на пристрої заборону на завантаження файлів без дозволу адміністратора ІС;

- обмеження на пристроях доступу до шкідливого трафіку та підозрілих сайтів.

Важливим фрагментом захисту є використання фізичних ключів доступу та біометричних методів авторизації.

Для поліпшення системи захисту було запропоновано наступні дії:

1. Використання двофакторної аутентифікації.

Двофакторна аутентифікація (2FA) є важливою складовою захисту інформаційних систем, яка значно підвищує рівень безпеки доступу до облікових записів і даних. Вона полягає у використанні двох різних методів перевірки особи користувача, що забезпечує додатковий рівень захисту. Зазвичай використовується авторизація за допомогою пошти, телефону або додатку “Google Authenticator”, з отриманням тимчасового коду для входу [4].

2. Розмежування по підмережам.

Розмежування по підмережам є одним із ключових методів забезпечення інформаційної безпеки та ефективного управління мережевими ресурсами в корпоративному середовищі. Цей підхід дозволяє розділити загальну мережу на кілька підмереж, кожна з яких має свої правила доступу, що забезпечує додатковий рівень захисту від несанкціонованого доступу та інших загроз. Використання VLAN дозволяє розділити мережу на кілька сегментів на основі портів комутаторів, незалежно від фізичного розташування пристроїв. Це один із найбільш популярних методів розмежування в сучасних мережах. Також виділяють методи: Міжмережеві екрани (Firewall), розділення на основі IP-адрес, мережеві сегменти на основі функцій. Це сприяє ізоляції трафіку, спрощує управління та полегшує виявлення та регулювання на інциденти.

3. Розмежування доступів користувача і адміністратора.

Розмежування доступів між користувачами та адміністраторами є критично важливим аспектом управління інформаційною безпекою в будь-якій організації. Це дозволяє зменшити ризик несанкціонованого доступу до важливих систем та даних, а також запобігти потенційним помилкам та зловживанням, що можуть виникнути в результаті надмірних прав доступу. Кожному користувачу надаються лише ті права доступу, які необхідні для виконання його обов'язків. Це обмежує можливості користувачів виконувати

дії, що виходять за межі їхніх посадових обов'язків. Функції та обов'язки розділяються таким чином, щоб один користувач не мав можливості виконувати всі критично важливі операції самостійно. Це допомагає запобігти шахрайству та помилкам.

4. Політика управління ризиками для мобільних пристроїв.

Для ефективного управління ризиками для мобільних пристроїв необхідно впроваджувати політику, що включає використання системи управління мобільними пристроями (Mobile Device Management). На всі мобільні пристрої, що використовуються співробітниками для доступу до корпоративних ресурсів, повинна бути встановлена MDM-система. Це дозволяє централізовано керувати пристроями та забезпечувати захист даних. При встановленні MDM-системи створюється зашифрований робочий обліковий запис для зберігання корпоративних даних. Це забезпечує захист інформації навіть у випадку фізичного доступу до пристрою сторонніх осіб. Всі дані, що зберігаються на робочому обліковому записі, повинні бути зашифровані. Це забезпечує додатковий рівень захисту у випадку втрати або компрометації пристрою. У разі втрати або крадіжки пристрою, MDM-система повинна мати можливість дистанційно видалити робочий обліковий запис. Це дозволяє захистити корпоративні дані від несанкціонованого доступу.

5. Встановлення на усі робочі пристрої VPN.

Встановлення VPN на всі робочі пристрої забезпечує захист корпоративних даних, особливо при доступі до інформаційних систем компанії через незахищені мережі, такі як громадський Wi-Fi. Враховуючи, що більшість співробітників працюють дистанційно, важливо підключати їх через VPN (Virtual Private Network), який створює зашифрований тунель для передачі даних між пристроєм користувача і корпоративною мережею, що дозволяє забезпечити конфіденційність та цілісність інформації, та запобігає перехаченню даних.

6. Шифрування жорсткого диску.

Шифрування жорсткого диску є важливим компонентом комплексної системи захисту інформації. Воно забезпечує захист даних на пристроях у разі їх втрати або крадіжки, що особливо актуально для ноутбуків та мобільних пристроїв, які часто використовуються для роботи в офісах та поза їх межами. Використовуються сучасні алгоритми шифрування, такі як AES з довжиною ключа не менше 256 біт, для забезпечення високого рівня безпеки.

Враховуючи існуючи методи захисту, а також запропоновані, можемо знов провести аналіз коефіцентів ризиків, та порівняти результати виконаної роботи.

7. Закупівля обладнання та ліцензійних ПО для підвищення рівня безпеки.

Сервер HPE ProLiant DL380 Gen10 має перевагу в забезпеченні високої продуктивності і масштабованість, мають високий рівень безпеки завдяки вбудованим функціям шифрування та безпечного завантаження, а також підтримують широкий спектр процесорів і пам'яті.

Комутатор Cisco C9200L-24T-4G-E забезпечує надійний захист мережі від несанкціонованого доступу, атак з мережі та інших кіберзагроз. Він дозволяє фільтрувати вхідний та вихідний трафік, запобігаючи доступу до мережі зловмисників. Серед його основних функцій - розширені списки контролю доступу (ACLs), які дозволяють створювати правила для контролю доступу до мережевих ресурсів на основі IP-адрес, портів і протоколів. Він також підтримує аутентифікацію пристроїв за допомогою стандарту 802.1X Network Access Control, що запобігає несанкціонованому доступу. Dynamic ARP Inspection (DAI) захищає від ARP-атак, перевіряючи відповідність ARP-повідомлень дійсним IP-адресам.

Acronis Backup дозволяє регулярно створювати резервні копії важливих даних та системних налаштувань, що захищає від втрати даних у разі збоїв або кібератак. Це програмне забезпечення забезпечує автоматичне резервне копіювання та зручне відновлення даних, допомагаючи зберігати бізнес-процеси та мінімізувати час простою.

Таблиця 1.7 Повторний аналіз коефіценту ризиків наслідку подій.

Тип загрози	Конкретна загроза	Коефіцієнт ймовірності	Коефіцієнт впливу	Коефіцієнт ризику
Кіберзлочинці	Несанкціонований доступ до даних	Низький(0.3)	Середній (0.5)	0.15
	Викрадення конфіденційної інформації	Середній (0.5)	Високий (0.9)	0.45
	Встановлення шкідливого ПЗ	Низький(0.3)	Середній (0.6)	0.18
Внутрішні загрози	Зловмисні дії співробітників	Середній (0.5)	Високий (0.8)	0.40
	Випадкові дії співробітників	Низький (0.2)	Низький (0.3)	0.06
	Зловживання правами доступу	Низький (0.2)	Середній (0.5)	0.10
Фізичні загрози	Крадіжка обладнання	Низький (0.2)	Низький (0.2)	0.04
	Несанкціонований фізичний доступ до серверів	Низький (0.2)	Високий (0.7)	0.14
Програмні загрози	Віруси	Середній (0.4)	Середній (0.5)	0.20
	Трояни	Середній (0.4)	Середній (0.4)	0.16
	Ransomware (вимагальне ПЗ)	Середній (0.4)	Середній (0.6)	0.24

Продовження таблиці 1.7

Тип загрози	Конкретна загроза	Коефіцієнт ймовірності	Коефіцієнт впливу	Коефіцієнт ризику
Атаки типу "відмова в обслуговуванні" (DoS/DDoS)	Атаки на веб-сервери	Середній (0.5)	Високий (0.8)	0.40
	Атаки на мережеву інфраструктуру	Низький (0.3)	Середній (0.4)	0.12
Людські помилки	Неправильне налаштування систем	Середній (0.5)	Середній (0.5)	0.25
	Випадкове видалення або зміна даних	Високий (0.8)	Низький (0.2)	0.16
	Неправильна обробка конфіденційної інформації	Середній (0.7)	Середній (0.7)	0.49

Висновки до спеціальної частини.

В ході виконання спеціальної частини роботи було проведено створення та впровадження системи захисту інформації в інформаційно-комунікаційній системі ТОВ "БДО". Було визначено основні загрози та ризики, які можуть вплинути на безпеку інформації, а також розроблено рекомендації щодо їхньої мінімізації та запобігання. Проведене обстеження дозволило отримати детальні дані про поточний стан інформаційних ресурсів компанії, виявити потенційні

вразливості та сформувати конкретні вимоги до системи захисту інформації. На основі цих вимог було розроблено комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

Особлива увага була приділена розробці політики безпеки, яка регулює розподіл обов'язків між адміністраторами та користувачами, а також визначає процедури ідентифікації та автентифікації. Це дозволило створити ефективну систему контролю доступу до інформаційних ресурсів, що мінімізує ризики несанкціонованого доступу та модифікації даних.

Також у роботі було враховано коефіцієнт ризиків наслідків подій, модель загроз та модель порушника, а також профіль захищеності. Це дозволило забезпечити комплексний підхід до оцінки та управління ризиками, що підвищує надійність запропонованої системи захисту інформації.

Загалом, реалізація запропонованих заходів забезпечить підвищення рівня інформаційної безпеки ТОВ "БДО", що сприятиме захисту критично важливих даних та стабільній роботі компанії в умовах сучасних кіберзагроз.

3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Економічне обґрунтування доцільності впровадження політики безпеки інформації.

Метою економічної частини дипломної роботи є проведення комплексного аналізу фінансових аспектів впровадження комплексної системи захисту інформації (КЗСІ) в інформаційно-комунікаційній системі (ІКС) підприємства ТОВ "БДО". В умовах зростаючої кількості кіберзагроз та постійного розвитку інформаційних технологій забезпечення належного рівня інформаційної безпеки стає критичним фактором успішного функціонування будь-якої організації.

Можна визначити економічну доцільність за такими критеріями:

- експлуатаційні витрати;
- капітальні затрати;
- річний економічний ефект після впровадження засобів інформаційної безпеки.

Першим етапом є розрахунок капітальних витрат на придбання і налагодження складових системи інформаційних безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення. Відповідно до законодавства України для машинного обладнання мінімальний строк використання 5 років.

Таблиця 3.1 - придбане обладнання та затрачені кошти.

Придбання приладів та ПЗ	Кількість	Вартість за шт, грн	Загальна вартість, грн
СЕРВЕР HEWLETT PACKARD ENTERPRISE DL380 GEN10 8SFF (P50751-B21 / V1-2-1)	1 шт	120 092	120 092

Продовження таблиці 3.1

Придбання приладів та ПЗ	Кількість	Вартість за шт, грн	Загальна вартість, грн
Коммутатор Cisco C9200L-24T-4G-E	2 шт.	59 581	59581
Acronis Cyber Backup Standard Server (річна підписка)	5 шт.	19 348	193 480

Загальна вартість за пристрої 120 092 + 119 162 + 193 480 = 432 734 грн.

Придбане обладнання значно підвищить захист від кібератак та інших загроз.

Оцінка складності та обсягу робіт з розробки політики інформаційної безпеки визначається затратою по часу робочої операції, затрачених на складання технічного завдання, визначення ризиків та оформлення наказів та технічних документацій.

Формула 3.1 - Оцінка складності та обсягу робіт з розробки політики інформаційної безпеки.

$$t = t_{m3} + t_b + t_a + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_d, \text{ годин}$$

t_{m3} - тривалість складання ТЗ на розробку ПБІ = 90 години;

t_b - тривалість розробки концепції безпеки інформації у організації = 25 години;

t_a- тривалість процесу аналізу ризиків = 70 години;

t_{b3} - тривалість визначення вимог заходів, методів та засобів захисту = 35 години

$t_{озб}$- тривалість виробу основних рішень з забезпечення БІ = 110 години;

$t_{овр}$- тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 180 години;

t_d - тривалість документального оформлення ПБ = 45 години;

$$90 + 25 + 70 + 35 + 110 + 180 + 45 = 555 \text{ годин}$$

Розрахування витрат на створення КЗСІ

Витрати на розробку політики безпеки інформації (Крп) складаються з оплати праці спеціаліста з інформаційної безпеки (Ззп) та вартості машинного часу, необхідного для цієї розробки (Змч).

Формула 3.2 - Витрати на розробку політики безпеки інформації.

$$К_{рп}: К_{рп} = З_{зп} + З_{мч}.$$

$$К_{рп} = 75\ 000 + 2\ 092{,}08 = 87\ 100{,}08 \text{ грн.}$$

$$З_{мч} = t * З_{пр} = 555*200 = 111{,}000 \text{ грн.}$$

t - загальна тривалість розробки політики безпеки, годин

Вартість використання часу на ПК для розробки політики безпеки інформації обчислюється за наступною формулою:

$$З_{мч} = t* С_{мч} =555*3{,}53 = 1959{,}15 \text{ грн.}$$

$С_{мч}$ - вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}6 * 4 * 0{,}9 + ((6000*0{,}4)/1920) + ((2300*0{,}1)/1920) =$$
$$2{,}16+1{,}25+0{,}1197=3{,}53 \text{ грн}$$

Вартість пристрою = 20000 грн, термін корисної служби = 42 місяці.

Накопичена амортизація = (20000 *42)/(5*12) = 14000 грн

Залишкова вартість = 20000 - 14000 = 6000 грн.

Капітальні витрати на створення політики безпеки інформації становлять:

$$К=К_{рп}+К_{зпз}+К_{аз}+К_{навч}+К_{н}=25300+74898+5000+15000 +7000=127198 \text{ грн.}$$

Компоненти витрат

$К_{рп}$ - вартість розробки політики інформаційної безпеки та залучення зовнішніх консультантів, 25 300 грн.

$К_{зпз}$ - вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 74898грн.

$К_{аз}$ - вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 5 000 грн.

$К_{навч}$ - витрати на навчання технічних фахівців і обслуговуючого персоналу, 15000 грн.

$К_{н}$ - витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 7 000 грн.

Таблиця 3.2 - Вартість програмних засобів.

Програмний засіб	Вартість, грн.
ESET Endpoint Security	346
Microsoft Office 2021 Pro Plus	450
Google Workspace	518
Кількість ПК	57
Всього	(346+450+518)*57=74898

3.2 Розрахунок поточних витрат.

Обслуговування об’єкта протягом визначеного періода є важливим критерієм та називається експлуатаційними витратами. Сюди відносять витрати на покращення й модернізацію ІС. Витрати на навчання персоналу визначається за даними організації з проведення тренінгів. ($С_{н}$).

Річний фонд амортизованих відрахувань ($С_{п}$) визначають за відсотками від суми інвестицій.

Річний фонд заробітної плати інженерно-технічного персоналу складає з:

Формула 3.3 - Річний фонд заробітної плати інженерно-технічного персоналу

$$С_з=З_{осн}+З_{дод}, \text{ грн.}$$

Основна заробітна плата розраховується на основі місячного посадового окладу, а додаткова заробітна плата становить 8-10% від основної заробітної плати. Основна заробітна плата одного спеціаліста з інформаційної безпеки складає 38000 грн на місяць. Додаткова заробітна плата дорівнює 10% від основної заробітної плати. Для виконання налаштувань інфраструктури безпечних підключень мобільних користувачів до внутрішньої мережі підприємства необхідно залучити спеціаліста з інформаційної безпеки на 0,25 ставки. Отже:

$$Сз = (20000 *12 + 20000 *12*0,1)*0,25= 66\ 000 \text{ грн.}$$

На момент 01.01.2024 р. ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 66\ 000*0,22 = 14\ 520 \text{грн}$$

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

$$С_{ел} = Р * F_р * Ц_е, \text{ грн.},$$

де:

Р - встановлена потужність апаратури інформаційної безпеки, (Р=0,6 кВт);

$F_р$ - річний фонд робочого часу системи інформаційної безпеки (Fр = 1920 год.);

$Ц_е$ - тариф на електроенергію, (Це = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$Сел = 0,6 * 1920 * 1,68 = 1935,36 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1%.

$$Стос = 50\ 314 * 0,01 = 503,14 \text{ грн.}$$

Річний фонд амортизаційних відрахувань:

$$Са = (120092+59581)/ 5 = 35\ 934{,}6 \text{ грн.}$$

$$Са = 19348/2 = 9674 \text{ грн.}$$

Витрати на керування системою інформаційної безпеки визначаються за формулою:

$$Ск = 45\ 608+ 66\ 000 + 14\ 520 + 1935{,}36 + 503{,}14 = 128\ 566.5 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 128 566.5 грн.

Оцінка величини збитку:

Для розрахунку вартості збитків можна застосувати спрощену модель оцінки для умовного підприємства. Необхідні вихідні дані для розрахунку:

$t_п$ - час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_{ви}$ - час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 години;

$t_{ви}$ - час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі;

$З_о$ - заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 9000 грн./міс.;

$З_с$ - заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 12 500 грн./міс.;

$Ч_о$ - чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

$П_{зч}$ - чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 10 осіб;

О - обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 7500 грн. у рік;

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн;

I - число атакованих сегментів корпоративної мережі, 1;

N - середнє число атак на рік, 12.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

Формула 3.4 - Упущена вигода від простою атакованого сегмента корпоративної мережі

$$U=П_п+П_в+V$$

де:

$П_п$ - оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ - вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V - втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п= ((12500*12)/ 176) * 4=3409,09 \text{ грн}$$

де:

F - місячний фонд робочого часу (при 40-годинному робочому тижні становить 176 годин).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

Формула 3.5 - Витрати на відновлення працездатності вузла або сегмента корпоративної мережі.

$$П_в=П_{ви}+П_{пв}+П_{зч}$$

де:

$П_{ви}$ - витрати на повторне введення інформації, грн;

$П_{пв}$ - витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ - вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви}= ((57407*12)/ 176) * 3=11742,42грн.$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{вп} = ((11750*1)/176)×3=200,28 грн.$$

Витрати на заміну устаткування або запасних частин можуть скласти 2320,50 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в=1948,86+200,28+2320,50=4469,64 грн.$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо годинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V=(2300000/2080)*(3+4+3)=8807,69 грн.$$

де:

$F_г$ - річний фонд часу роботи філії (52 робочих тижні, 5-денний робочий тиждень, 8-годинний робочий день) становить близько 2080 годин.

Отже, загальні втрати:

$$U=11742,42+4469,64+8807,69=25019,75грн.$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$В=1*12*25019,75=300237,04 грн.$$

Загальний ефект від впровадження системи інформаційної безпеки:

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E=B×R−C$$

де:

В - загальний збиток від атаки у разі перехоплення інформації, тис. грн;

R - ймовірність успішної реалізації атаки на сегмент мережі, частки одиниці, що дорівнює 57%;

C - щорічні витрати на експлуатацію системи інформаційної безпеки.

Вихідні дані:

Загальний збиток від атаки B=200237,04

Ймовірність успішної реалізації атаки R=0,57

Щорічні витрати на експлуатацію системи інформаційної безпеки C=128 566,5

Отже, загальний ефект від впровадження системи інформаційної безпеки:

$$E=300237,04\times0,57-128\ 566,5$$

Обчислимо:

$$E=171\ 135,1-128\ 566,5=42\ 568,6 \text{ грн}$$

Таким чином, загальний ефект від впровадження системи інформаційної безпеки складає 42 568,6 грн.

3.3 Визначення та оцінка економічної ефективності системи інформаційної безпеки

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

Формула 3.6 - Коефіцієнт повернення інвестицій (ROSI).

$$ROSI = \frac{E}{K}$$

де:

E - загальний ефект від впровадження системи інформаційної безпеки, грн;

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

ROSI = 42 568,6 /50314 = 0,85

Проєкт визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100$$

де:

$N_{деп}$ - річна депозитна ставка, (23%);

$N_{інф}$ - річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,85 > (23-14)/100 \Rightarrow 0,85 > 0,09$$

Термін окупності капітальних інвестицій (Т) показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T = 1/ROSI = 1/0,85 \approx 15 \text{ місяців.}$$

Висновок до економічної частини.

В ході виконання економічної частини роботи було проведено ретельний аналіз економічної ефективності впровадження системи захисту інформації в інформаційно-комунікаційній системі ТОВ "БДО". Дослідження показало, що інвестиції у заходи інформаційної безпеки є не лише необхідними для захисту критично важливих даних, але й економічно доцільними.

Було розраховано коефіцієнт повернення інвестицій (ROSI). Даний показник перевищує величину річної депозитної ставки з урахуванням інфляції, що підтверджує економічну доцільність проєкту.

Загалом, економічний аналіз підтвердив, що впровадження системи захисту інформації є фінансово виправданим і вигідним кроком для ТОВ "БДО". Це дозволить компанії знизити потенційні збитки від інформаційних інцидентів, підвищити конкурентоспроможність та забезпечити стабільний розвиток в умовах зростаючих кіберзагроз.

ВИСНОВКИ

В першому розділі було проведено детальний опис діяльності компанії, її основні та вторинні інформаційні потоки, облік та управління апаратними засобами. Обозначено види загроз та їх вплив на діяльність компанії та проведено ретельна оцінка ризиків. Також було розглянуто теоретичні аспекти інформаційної безпеки, визначено ключові терміни та поняття, зсилаючись на основні джерела та міжнародні стандарти безпеки. Ефективна система захисту інформації є невід'ємною складовою стратегії управління сучасними підприємствами. Також було підкреслено важливість інтеграції інформаційної безпеки в загальну корпоративну політику компанії. Було вивчено найпоширеніші загрози інформаційній безпеці та методи їх попередження.

В другому розділі було представлено процес розробки комплексної системи захисту інформації для інформаційно-комунікаційної системи ТОВ "БДО". На основі проведеного обстеження було визначено конкретні вимоги до системи захисту інформації. Розробка системи включала врахування коефіцієнта ризиків наслідків подій, моделі загроз та моделі порушника, а також профілю захищеності. Особлива увага була приділена забезпеченню конфіденційності, цілісності та доступності інформації, що є критично важливими аспектами для ефективного функціонування підприємства. Було проведено аналіз різних методів і технологій захисту, що дозволило створити оптимальну та надійну систему та запроваджено основні заходи підвищення рівня безпеки підприємства.

В економічному розділі було здійснено аналіз впровадження системи захисту інформації в ТОВ "БДО". На основі розрахунків було визначено коефіцієнт повернення інвестицій (ROSI), який свідчить про економічну доцільність проєкту. Аналіз показав, що впровадження системи захисту інформації дозволить компанії знизити потенційні збитки від інформаційних інцидентів та забезпечити стабільний розвиток в умовах зростаючих кіберзагроз. У роботі було враховано ключові показники ризиків, що забезпечило комплексний підхід до оцінки та управління ризиками.

Таким чином, результати роботи підтверджують важливість і доцільність впровадження комплексної системи захисту інформації в ТОВ "БДО" як з технічної, так і з економічної точки зору.

ПЕРЕЛІК ПОСИЛАНЬ

1. Офіси БДО в Україні - BDO. URL: https://www.bdo.ua/uk-ua/offices-of-bdo-in-ukraine-2/dnipro

2. ДСТУ ISO-IEC 27001:2022 [Електронний ресурс] // ДСТУ. - 2022. - URL: https://www.iso.org/standard/27001

3. ДСТУ ISO/IEC 27005:2015 [Електронний ресурс] // ДСТУ. - 2015. - URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

4. Cybersecurity & Infrastructure Security Agency (CISA) - Two-Factor Authentication (2FA) [Електронний ресурс] URL: https://www.cisa.gov/MFA

5. Cisco Systems. "Virtual LANs: Configuring VLANs." Cisco. [Електронний ресурс] URL: https://slideplayer.com/slide/7531082/

6. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994. - No 80. [Електронний ресурс]. - URL: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

7.Закон України “Про захист інформації в автоматизованих системах” від 05.07.1994 No80-VI // Відомості Верховної Ради України. - 1994 р., N 31. [Електронний ресурс]. - URL: https://zakon.rada.gov.ua/laws/show/2594-15

8. Гребенніков В. В. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ: проєктування, впровадження, супровід [Електронний ресурс] / Вадим Вікторович Гребенніков. - 2013.

9. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

10. Закон України “Про основні засади забезпечення кібербезпеки України” від 05.10.2017 No 2163-VIII. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/2163-19

11. Служба Безпеки України - Основні напрямки діяльності у сфері кібербезпеки. [Електронний ресурс]. URL: https://ssu.gov.ua/ua/pages/5/category/23

12. Коваль В. В. "Аналіз ризиків інформаційної безпеки на основі методології OCTAVE" / В. В. Коваль. // Науковий журнал "Сучасні інформаційні системи". - 2020. [Електронний ресурс].

13. NIST Special Publication 800-37 Rev. 2 - Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. [Електронний ресурс]

14. .НД ТЗІ 2.5-004 - Критерії оцінки захищеності інформації в комп'ютерних

системах від несанкціонованого доступу. - [Чинний від 28.04.1999] - К. : ДСТСЗІ СБУ, 1999. - No22

15. Державний стандарт України. ДСТУ 3396.1-96. Інформаційні технології. Методи та засоби забезпечення безпеки. Загальні вимоги до захисту інформації. Київ: Державний комітет України з питань технічного регулювання та споживчої політики, 1996.

16. Національний документ України. НД ТЗІ 2.5-004-99. Захист інформації. Загальні вимоги до захисту інформації в інформаційних системах. Київ: Міністерство оборони України, 1999.

17. Адміністрація Держспецзв'язку. Наказ від 28.12.2012 № 806 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». [Електронний ресурс]. Київ: Держспецзв'язок України, 2012.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	2	
5	А4	1 Розділ	14	
6	А4	2 Розділ	29	
7	А4	3 Розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Комплексна система захисту інформації інформаційно-комунікаційної системи ТОВ БДО.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:

студента групи 125-20-1

Полякова Івана Ігоровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунка, __ таблиці, __ джерел та __ додатка.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

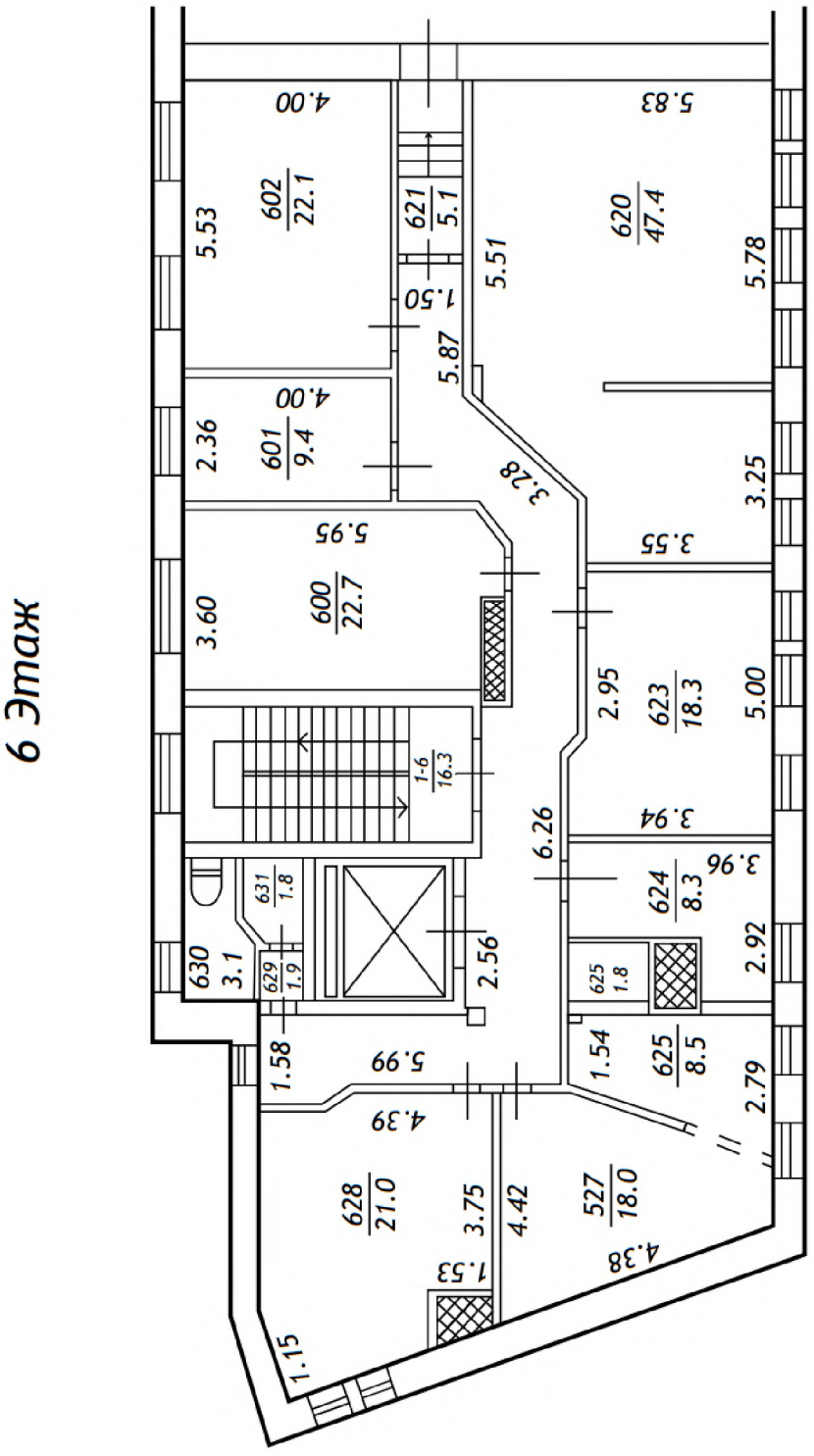
Робота оформлена та написана грамотною мовою, відповідає вимогам положення про систему запобігання та виявлення плагіату у Національному технічному університеті «Дніпровська політехніка». Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник

ДОДАТОК Ґ. План приміщення.

Рисунок 1 План приміщення



ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-20-1

Полякова Івана Ігоровича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «БДО»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 72 сторінках.

Метою кваліфікаційної роботи є підвищити рівень захисту інформації в інформаціно-комунікаціній системі ТОВ «БДО».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека».

В кваліфікаційній роботі було проаналізовано стан інформаційної захищеності в ІКС, виявлено основні ризики та загрози.

В рамках другого розділу було проведено обстеження ТОВ «БДО», розроблено модель порушника, модель загроз та проведено оцінку ризиків інформації, що можуть призвести до завдання збитків ТОВ «БДО». Згідно з проведеним аналізом, запропоновані до впровадження методи та засоби захисту інформації для покращення безпеки інформаційно-комунікаційної системи підприємства.

У третьому розділі було розраховано доцільність впроваджених методів для підвищення захисту підприємства, ефективність відносно економічних затрат та впровадження в ІКС ТОВ «БДО».

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності властивостей інформації з обмеженим доступом в інформаційно-комунікаційній системі «БДО».

До недоліків кваліфікаційної роботи потрібно віднести відсутність достатньо аргументованих висновків в підрозділах та розділах роботи та незначні відхилення від стандартів оформлення.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату». у Національному технічному університеті «Дніпровська політехніка».

Кваліфікаційна робота заслуговує оцінки « 70 / задовільно».

Керівник спец. частини асист. Мілінчук Ю.А.

Керівник кваліфікаційної роботи: проф. Корченко А.О.

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («добре»).

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