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 *Філіпенко Максима Валерійовича*

академічної групи *125-20-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформаційно-комунікаційної системи ТОВ Справедливість*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Гусєв О.Ю.			
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.			
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.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Філіпенко Максиму Валерійовичу*** **академічної групи** ***125-20-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформаційно-комунікаційної системи ТОВ Справедливість***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Дослідити стан питання, проаналізувати нормативно-правову базу, виконати постановку задачі.	15.03.2024
Розділ 2	Провести обстеження підприємства та ІКС компанії, проаналізувати та класифікувати інформацію яка циркулює в підприємстві, створити моделі порушника та загроз, обрати профіль захищеності, розробити політики безпеки.	10.05.2024
Розділ 3	Розрахувати економічну доцільність витрат на розробку, та впровадження політики безпеки.	11.06.2024

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

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2023р.

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

РЕФЕРАТ

Пояснювальна записка: 69 с., 6 рис., 9 табл., 6 додатка, 18 джерел.

Об’єкт розробки: інформаційно-комунікаційна система ТОВ Справедливість.

Предмет розробки: політика безпеки інформації ІКС підприємства ТОВ Справедливість.

Мета роботи: підвищення рівня захищеності інформації в ІКС приватного підприємства ТОВ Справедливість.

У першому розділі описано стан питання та основні актуальні проблеми забезпечення кібербезпеки та захисту інформації на типовому підприємстві, визначено нормативно-правову базу згідно якої буде відбуватися побудова КСЗІ, також вказані підстави та етапи створення КСЗІ та ПБ.

У другому розділі проаналізовано загрози для ІКС підприємства, виконано класифікацію інформації та розроблено модель порушника. Після проведення аналізу отриманих даних обрано профіль захищеності спираючись на нормативно-правові документи, зазначені в розділі. Розроблено елементи політики безпеки підприємства.

У третьому розділі проаналізовано економічну сторону підприємства, на основі результатів аналізу зроблені оцінки щодо економічної доцільності розробки та інтеграції розробленої системи захисту. Ґрунтуючись на всіх отриманих результатах інтеграція вважається доцільною.

Практична цінність розробки полягає у підвищенні рівня інформаційної безпеки ІКС ТОВ Справедливість.

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, ВРАЗЛИВОСТІ, ФУНКЦОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕННОСТІ.

ABSTRACT

Explanatory note: 69 pp., 6 pic., 9 table, 6 app, 18 sources.

Object of development: the information and communication system of Spravedlyvist LLC.

The subject of the development: information security policy of the information and communication system of the Spravedlyvist LLC enterprise.

The purpose of the work: increasing the level of information security in the information and communication system of the private enterprise Spravedlyvist LLC.

The first chapter describes the state of the issue and the main current problems of ensuring cyber security and information protection at a typical enterprise, defines the regulatory and legal framework according to which the construction of the comprehensive information protection system will take place, as well as the grounds and stages of the creation of the comprehensive information protection system and security policy.

In the second section, threats to the company's information and communication system were analyzed, information was classified, and a model of the offender was developed. After analyzing the received data, a security profile was selected based on the normative and legal documents specified in the section. The elements of the company's security policy have been developed.

In the third section, the economic side of the enterprise is analyzed, based on the results of the analysis, assessments are made regarding the economic feasibility of the development and integration of the developed protection system. Based on all the obtained results, the integration is considered appropriate.

The practical value of the development lies in increasing the level of information security of ICS LLC Spravedlyvist.

SECURITY POLICY, THREAT MODEL, VIOLATOR MODEL, INFORMATION SYSTEM, VULNERABILITIES, FUNCTIONAL SECURITY PROFILE.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

DDoS – Distributed Denial of Service;

MitM – Man-in-the-middle;

ROSI - Return on Investment for Security;АС – автоматизована система;

SQL – Structured Query Language;

БЦ – бізнес центр;

Держспецзв'язок – державна служба спеціального зв'язку та захисту інформації України;

ІзОД - інформація з обмеженим доступом, що не становить державної таємниці;

ІКС – інформаційно-комунікаційна система;

КЗЗ — комплекс засобів захисту;

КПП – контрольно пропускний пункт;

КСЗІ – комплексна система захисту інформації;

МінФін – міністерство фінансів;

НБУ – національний банк України;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ - політика безпеки;

ПЗ – програмне забезпечення;

ПК - персональний комп'ютер;

ПКП – пристрій контролю проникнення;

РФ – Російська Федерація;

США – Сполучені Штати Америки;

ТОВ – товариство з обмеженою відповідальністю;

ЗМІСТ

с.

ВСТУП

Актуальність цієї кваліфікаційної роботи повязана з підвищеною необхідністю забезпечення безпеки інформаційних ресурсів. За даних умов зростає загроза кібератак, а це в свою чергу підвищує потреби до захисту конфіденційної та іншої інформації.

Об'єктом розробки є політика безпеки інформаційно-комунікаційної системи ТОВ Справедливість, підприємство займається юридичною діяльністю.

Предметом розробки в кваліфікаційній роботі є політика безпеки інформації ІКС підприємства ТОВ Справедливість.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІКС приватного підприємства ТОВ Справедливість

Тема є актуальною, основуючись на зовнішніх факторах які впливають на безпеку організації (крадіжка, пограбування) та не фізичні небезпеки (взлом, ураження ПО компанії). На даний момент існує дуже велика проблема витоку або розголошення інформації. На фоні постійно зростаючої сфери послуг дуже сильно зростає кількість конкурентів, зважаючи що не кожен конкурент є добропорядним з'являється проблема цілісності даних. При таких умовах кожен керівник або власник стає зацікавленим в максимальному збереженні даних своєї компанії та даних своїх клієнтів. Також для кожного підприємства дуже великою проблемою стали кібератаки, посилаючись на інформацію що надає Мінфін кількість кібератак на українські підприємства є критичною. Зважаючи що основною метою даних атак є нанесення якомога більшої шкоди малому та середньому бізнесу.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

На сьогоднішній день існує велика проблема кіберзлочинності. Через поширення глобальної мережі інтернет збільшилась швидкість передачі інформації і зручність. Але це несе дуже велику проблему ураження, витику, пошкодження даної інформації будь то фізична крадіжка диску з конфіденційною інформацією чи проникнення в мережу підприємства. З цифровізацією компаній фізичні крадіжки даних відійшли на другий план тепер найбільшою проблемою стали кіберзлочинці. Будь то конкуренти, хакери одинаки чи цілі групи хакерів. Дуже великою проблемою сьогодення стали кібератаки. Кібератаки вражають бізнес та фізичних осіб щодня. Кіберзлочинність зростає з кожним роком, оскільки люди намагаються отримати якусь вигоду будь то вимагання чи нагорода від іншої особи чи компанії яка зацікавлена в чомусь. Існує багато видів кібератак ось декілька [3]:

1. Шкідливе програмне забезпечення:

Цей термін використовується для опису багатьох видів шкідливого програмного забезпечення, такого як:

- шпигунське;
- програми-вимагачі;
- віруси;
- черв'яки;

2. Фішинг:

Фішинг — це практика надсилання шахрайських повідомлень, які нібито надходять із надійного джерела, зазвичай електронною поштою. Мета — викрасти конфіденційні дані, як-от дані кредитної картки та дані для входу, або встановити шкідливе програмне забезпечення на машину жертви. Фішинг стає все більш поширеною кіберзагрозою.

Атака типу "людина посередині":

Атаки типу Man-in-the-middle (MitM), також відомі як атаки підслуховування, виникають, коли зловмисники входять у двосторонню транзакцію. Як тільки зловмисники переривають трафік, вони можуть фільтрувати та викрадати дані.

3. DDoS атаки:

Атака типу DDoS або "відмова в обслуговуванні" заповнює системи, сервери або мережі трафіком, щоб вичерпати ресурси та пропускну здатність. У результаті система не може виконувати законні запити. Зловмисники також можуть використовувати кілька скомпрометованих пристроїв для здійснення цієї атаки.

4. SQL ін'єкція:

Ін'єкція мови структурованих запитів (SQL) відбувається, коли зловмисник вставляє зловмисний код на сервер, який використовує SQL, і змушує сервер розкривати інформацію, яку він зазвичай не відкрив би. Зловмисник може здійснити SQL-ін'єкцію, просто ввівши зловмисний код у вікно пошуку вразливого сайту.

На сьогоднішній день відбуваються перегони між фахівцями кібербезпеки, та хакерами. Через те що кожне впровадження нової технології для компанії означає що ймовірність того що вона може стати головної ціллю для небайдужих хакерів збільшується.

Гарним прикладом масованих кібератак є початок повномасштабного вторгнення Росії. Як запевняє директор IT-компанії UNITY-BARS, що розробляє ПЗ для фінансових установ, Олег Музика, Україна майже весь 2022 рік займала друге місце в світі після США серед найбільш атакованих країн світу [5]. В порівнянні з 2021 роком кількість кібератак збільшилась у 3,5 рази на фінансовий сектор України прийшлось 5% усіх атак, на IT-галузь – 10%, констатують UNITY-BARS. Найчастіше кібершахраї отримують доступ до організацій-жертв завдяки таргетованому фішингу. Хакери втручаються у системи, розповсюджують шкідливе програмне забезпечення, щоб шпигувати, збирати дані чи використовувати вразливості сервісів, розповідають у державній

службі спеціального зв'язку та захисту інформації України. У 2023 році з інформації НБУ, крім банків хакери атакують страхові компанії, юридичні компанії та розробників ПЗ для банків [2]. Також високоактивними є кібератаки, спрямовані на викрадення коштів. Найчастіше кібершахраї отримують доступ до організацій-жертв завдяки таргетованому фішингу. Хакери втручаються у системи, розповсюджують шкідливе програмне забезпечення, щоб шпигувати, збирати дані чи використовувати вразливості сервісів. У Держспецзв'язку припускають, що збільшення фішингових атак та компрометації акаунтів, спрямованих на банківську систему України, можуть свідчити про те, що росіяни планують зламати ресурси комерційних організацій та атакувати їх, щоб викрасти гроші.

Гарним підтвердженням тези про те що кібератаки є дуже серйозним методом нанесення шкоди є єдина координація атак РФ як і кібератак так і ракетних по енергетиці України. Mandiant (дочірня структура Google, що займається кібербезпекою) дослідила дві атаки 10 і 12 жовтня 2022 року, коли російське хакерське угруповання Sandworm скористалося вразливостями системи управління підстанціями в Україні [4].

До повномасштабного вторгнення РФ Україну атакували окремі хакерські угрупування. Натомість з початком повномасштабної війн хакерів координує єдиний центр. Кібератаки самі по собі є дуже коштовними і Росія витрачає на кожну серйозну кібератаку мільйони доларів.

За інформацією Держспецзв'язку змінилась і мета кібератак РФ. До повномасштабного вторгнення російських хакерів цікавила фінансова вигода, така як:

- викуп за повернення системи до ладу;
- крадіжка даних з метою продажу;

РФ постійно атакує енергетику України. Щомісячна кількість кібератак становить від 100 до 300, найбільша частина припадає на енергетику та критичну інфраструктуру країни. Данні атаки призводять до проблем в роботі малого та середнього бізнесу, держустанов.

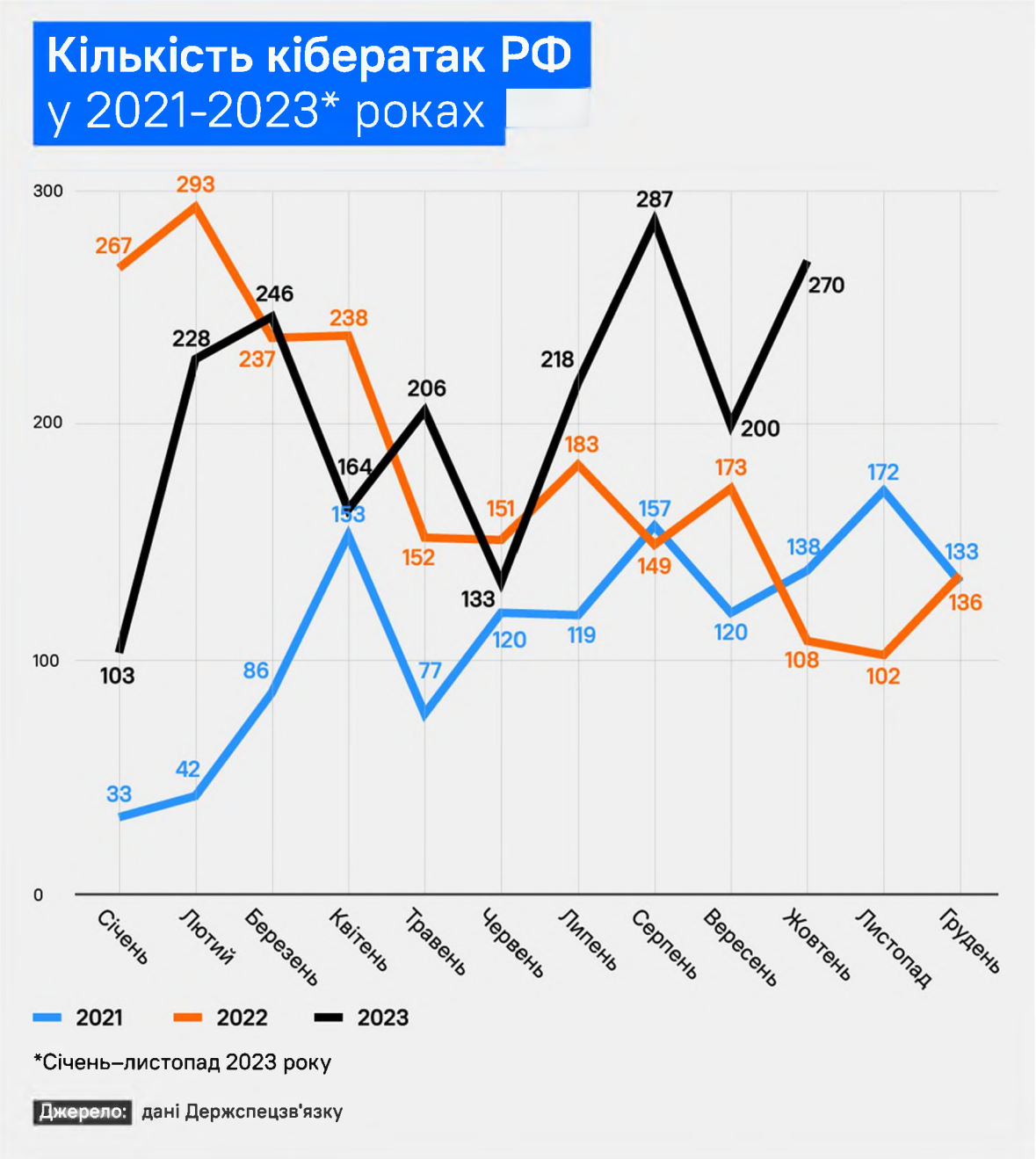

Рисунок 1.1 Кількість кібератак РФ (2021-2023) [4]

У 2022 році [4] росіяни вдавалися до DDoS-атак удесятеро частіше, ніж у 2021 році. Але РФ майже відмовилася від цього інструменту як неефективного.

У січні–лютому 2023 року урядова команда реагування на комп'ютерні надзвичайні події, опрацювала понад 300 кіберінцидентів та кібератак.

Це майже вдвічі менше, ніж у відповідний термін 2022 року, коли Росія готувалася до повномасштабного вторгнення і активність хакерів була аномально високою. У січні 2023 року активність кіберзловмисників була дещо знижена.

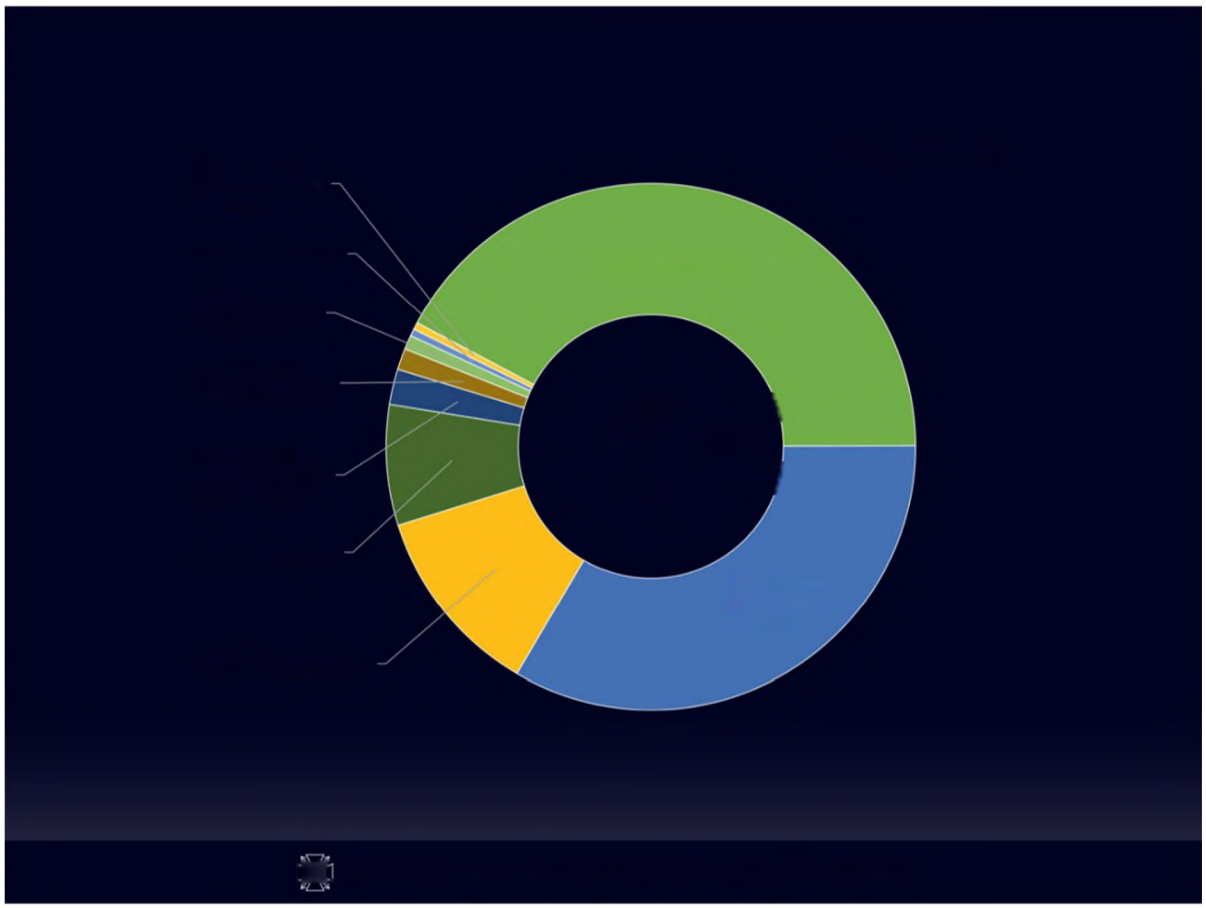

Рисунок 1.2 – Категорії кіберінцидентів [5]

Від початку цього року урядова команда реагування фіксує зростання кількості атак з метою шпигунства з акцентом на утриманні постійного доступу до організації [5]. І навіть серед шкідливого програмного забезпечення, яке поширюють російські хакери, переважають програми для збору даних та віддаленого доступу до пристроїв користувачів. За допомогою хакерів вона намагається отримати будь-яку інформацію, яка може дати перевагу в війні проти нашої країни: дані щодо мобілізації, розкриття секретів логістики, західна зброя, розміщення активних військових об’єктів.

Також дуже великою проблемою є необізнаність або навмисне порушення основних правил кібербезпеки. У зв’язку з тим що як демонструє практика найслабше місце в захисті будь чого це завжди людина. Гарним прикладом цієї тези є кібератака на “Київстар”.

Кібератака на компанію “Київстар” (найбільший в Україні оператор зв’язку) сталась 12 грудня 2023 року [6]. Дана атака визвала катастрофічні руйнування в середині системи. Ця атака знищила тисячі віртуальних серверів і

ПК, голова департаменту СБУ Ілля Вітюк описав це як ,ймовірно, перший приклад деструктивної кібератаки, що “повністю знищила ядро телекомунікаційного оператора”. За цією атакою стоїть російське хакерське угрупування Sandworm, яке являє собою штатний підрозділ російської військової розвідки. Sandworm і раніше неодноразово здійснювало кібератаки на українські об’єкти, зокрема і на операторів зв’язку та інтернет-провайдерів. Кібератака була настільки сильною, що на кілька днів вивела з ладу всі системи компанії “Київстар” та зробила неоцінні фінансові так репутаційні збитки для компанії так впевненості в захисті даних кожного Українця. А зробили хакери це через скомпрометований обліковий запис одного з працівників самої компанії. Як було зазначено головою департаменту кібербезпеки СБУ, хакерське угрупування мало доступ до даних системи ще з травня 2023 року. Даний випадок дає змогу поміркувати над принципами захисту від соціальної інженерії яка і є фундаментом для фішингових атак, або промислового шпіонажу.

Найбільше від хакерських атак страждає середній та малий бізнес бо частіше за все він за нестачу коштів на захист не переймається через конфіденційність інформації якою володіє, вважаючи що хакери будуть атакувати великі компанії. Але як демонструє практика сьогодні зловмисники у переважній кількості випадків беруть не якістю жертв, а кількістю [15]. Їм байдуже, чи це великий концерн, чи домашній комп’ютер фрилансера – будь-яка інформація має свою цінність та ціну. З даних причин малий і середній бізнес може потрапити під кібератаку навіть випадково – й втратити приватні дані, інтелектуальні активи. Як показує практика після такого роду атак більшість компаній банкрутують через відсутність коштів на відшкодування та відновлення внутрішньої системи компанії. Також державні установи та юридичні компанії зіштовхнулись з проблемою шпіонажу. Даного роду атаки націлені не стільки на пошкодження мережі чи виведення з ладу самої системи скільки на ураження системи та збір особистих даних клієнтів з метою маніпулювання, викрадені аналітичні даних компаній, ці дані використовують для шантажу даної компанії

або компрометації дій компанії на ринку через що компанія несе репутаційні збитки.

1.2 Аналіз нормативно-правової бази забезпечення інформаційної та кібербезпеки

В даному розділі розглядаються правові норми, що визначають порядок створення, правовий статус і функціонування захищених інформаційно-комунікаційних систем і мереж, регламентують порядок одержання, перетворення та використання інформації і інформаційних ресурсів.

Закон України “Про Адвокатську діяльність” [16]

Основним з видів таємниць до якого можна віднести підприємство юридичного характеру є адвокатська таємниця. Її суть полягає в наступних пунктах:

- будь яка інформація, що стала відома адвокату про клієнта а також питання з яким клієнт звертається до адвоката;
- зміст порад, консультації та роз’яснення адвоката;
- документи які складені адвокатом, відомості та будь які інші документи які причетні до справи;
- вся інформація що зберігається на електронних носіях;
- ім’я, по батькові клієнта та його контактні дані;
- факт звернення клієнта;

Всі ці дані під час адвокатської діяльності підпадають під адвокатську таємницю.

Адвокатська таємниця є правом та обов'язком адвоката [16]. Право та обов'язок зберігати адвокатську таємницю розповсюджується на всі відомості, що стали відомі адвокату при виконанні доручення клієнта, і продовжують зберігатися після виконання такого доручення. Адвокатська таємниця не обмежена в часі. Обов'язок зберігати адвокатську таємницю поширюється на адвоката, його помічника, стажиста та осіб, які перебувають у трудових відносинах з адвокатом, адвокатським бюро, адвокатським об'єднанням, а також на особу, стосовно якої припинено або зупинено право на зайняття адвокатською діяльністю.

Втрата, пошкодження чи розголошення є порушенням адвокатської таємниці.

Закон України “Про персональні дані” [17]

Для початку слід визначити, що таке персональні данні. Персональними даними являються ті особисті дані які дозволяють за допомогою їх ідентифікувати особу.

Компанія якій було надано дозвіл на обробку персональних даних повинна забезпечити повну конфіденційність цих даних, виключенням є дозвіл на передачу даних третім особам за згоди власника.

Закон України “Про інформацію”:

Даний закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в всіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

Кожна КСЗІ базується на вимогах чинного законодавства України та на нормативно правових документах. З яких можна виділити наступні:

- НД ТЗІ 1.1-002-99 [9]: Загальні положення з захисту інформації в комп'ютерних системах від НСД;

У цьому документі наведена інформація щодо заходів та засобів захисту інформації та їх впровадження. Також наведена інформація щодо керування доступом та концепції забезпечення захисту інформації.

- НД ТЗІ 1.1-003-99 [10]: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

У цьому документі містить перелік термінів та понять у сфері захисту

інформації в ІТС від несанкціонованого доступу.

– НД ТЗІ 2.5-004-99 [11]: Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

Цей документ встановлює критерії, за якими оцінюються стан захищеності інформації, яка обробляється в АС від несанкціонованого доступу.

– ДСТУ ISO/IEC 27001:2015 [7];

У цьому документі наведені методи захисту інформації та системи управління інформаційною безпекою.

– ДСТУ ISO/IEC 27005:2015 [8];

У цьому документі наведена інформація щодо управління ризиками інформаційної безпеки.

– НД ТЗІ 1.6-005-2013 [1]: Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

У цьому документі наведені положення про захист інформації на ОІД та інформацію про категоріювання об'єктів, де циркулює ІзОД, що не становить державної таємниці.

1.3 Постановка задачі

Задача базується на описі проблеми в пункті 1.1, де було зазначено про збільшення кількості кіберзлочинів та збільшення кібератак на бізнес зі сторони РФ. В описаній ситуації підприємство було змушено придати більше уваги захисту даних клієнтів та своїх для уникнення пагубних наслідків. Відповідно до виконаного аналізу та вимог нормативних документів у спеціальній частині необхідно виконати наступні задачі:

– Виконати обстеження об'єкту інформаційної діяльності;

– Проаналізувати фізичні характеристики об'єкту;

– Проаналізувати логічну характеристику об'єкту;

- Проаналізувати види інформації та особливості взаємодії інформації на об’єкті;
- Обрати профіль захищеності;
- Розробити основні елементи політики безпеки.

1.4 Висновок до першого розділу

У першому розділі кваліфікаційної роботи описано стан кібербезпеки в Україні, основні загрози які стосуються інформаційної безпеки малого та середнього бізнесу та наслідки цих загроз. Також позначаються основні цілі та мета здійснення хакерами кібератак, даними цілями є державні установи та юридичні компанії. Таким чином розкрита потреба в збільшенні захищеності підприємства для уникнення збитків для нього самого. Також був проаналізовано список нормативно-правових документів в сфері захисту інформації на основі як будується захист. Та було поставлена задача з чіткими вимогами для побудування надійного захисту.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Загальні відомості про вид діяльності ТОВ Справедливість

Основним видом діяльності ТОВ Справедливість є надання широкого спектру юридичних послуг, в даний спектр входять такі послуги як:

Корпоративне право

- реєстрація, реорганізація та ліквідація компаній;
- підготовка та аналіз корпоративних документів;
- консультації щодо корпоративного управління;
- супровід угод злиття та поглинання;

Контрактне право:

- підготовка, аналіз та супровід договорів;
- консультації з питань виконання та розірвання договорів;
- вирішення спорів, пов'язаних з контрактними зобов'язаннями;

Трудове право:

- консультації з питань працевлаштування та звільнення;
- підготовка трудових контрактів та внутрішніх положень;
- вирішення трудових спорів;

Податкове право:

- консультації з питань оподаткування;
- податкове планування та оптимізація;
- захист інтересів клієнтів у податкових спорах;
- підготовка та подача податкової звітності;

Земельне право та нерухомість:

- юридичний супровід угод з нерухомістю;
- оформлення прав на земельні ділянки;
- консультації з питань використання та оренди землі;
- вирішення спорів щодо нерухомого майна;

Судова практика:

- представництво інтересів клієнтів у судах;
- виконання судових рішень;

- консультації з питань судової практики;

Банківське та фінансове право:

- консультації з питань банківської діяльності та фінансових операцій;
- юридичний супровід кредитних та інших фінансових угод;
- регулювання діяльності фінансових установ;

Конкурентне право та антимонопольне регулювання:

- консультації з питань конкурентного законодавства;
- представництво інтересів у антимонопольних органах;
- захист від недобросовісної конкуренції;

Міжнародне право та міжнародний бізнес:

- юридичний супровід зовнішньоекономічної діяльності;
- консультації з питань міжнародного права;
- представництво інтересів у міжнародних судах;
- вирішення міжнародних комерційних спорів;

Діяльність компанії пов'язана з взаємодією з юридичними та з фізичними особами, різниця тільки в допустимому спектрі послуг які компанія може надати.

Через юридичний профіль підприємства в ньому циркулює різного роду інформація, яка може собою становити:

- комерційна таємниця;
- банківська таємниця;
- адвокатська таємниця;
- конфіденційні данні;

Також в стінах компанії знаходиться і циркулює конфіденційна інформація самої компанії, такі дані як:

- дані про заробітну плату;
- особисті дані працівників компанії (дипломи про освіту, виписки про несудимість, тощо);
- бухгалтерські дані компанії;
- різноманітні договори про співпрацю компаній з партнерами;
- договори про партнерство між компаніями;

- непублічні договори;
- договори з клієнтами;
- особисті дані клієнтів які допомагають в розвитку справи клієнта, але являють собою конфіденційні дані клієнта;
- інше;

Підприємство працює 5 днів на тиждень (з понеділка по п'ятницю) з 10:00 до 17:00, з перервою з 13:30 до 14:00

2.2 Обґрунтування необхідності створення КСЗІ

Виходячи з положення чинного законодавства України щодо захисту інформації, необхідно обмежити доступ до деяких видів інформації. Директором підприємства ініційовано та видано акт про категоріювання об'єкта (див. ДОДАТОК В). Для цього, за розпорядженням власника інформації (див ДОДАТОК Г), створюється КСЗІ, в якій визначено рішення щодо забезпечення цілісності і доступності інформації, в тому числі і порядок доступу до інформації, перелік користувачів і їх права доступу до даної інформації. Рішення щодо створення та впровадження КСЗІ покладається на власника системи, оскільки він несе повну відповідальність за її цілісність та збереження.

2.3 Організаційна структура підприємства

На підприємстві ТОВ Справедливість кількість співробітників складає 8 чоловік:

- директор;
- секретар директора;
- 2 юристи;
- 2 працівника відділу аналітики;
- адвокат;
- секретар;

Директор - обов'язки директора виконує власник компанії, в обов'язки якого входить:

- основні організаційні питання;
- підписання договорів з кожним важливим клієнтом;
- підписання договорів з партнерами;
- основні рішення котрі можуть фундаментально впливати на компанію;

Секретар директора – виступає в ролі заступника директора, бухгалтера, помічника директора в обов'язки входить:

- бухгалтерська діяльність;
- розробка договорів;
- організаційні питання;
- первинна робота з важливими клієнтами;
- менеджмент часу директора;

Юрист – в ролі юристів виступають 2 працівника кожен з яких займається свого роду юридичними питаннями в своєму спектрі права, в обов'язки юристів входять:

Робота з клієнтом

- робота з договорами;
- судові справи;
- розробка договорів разом за клієнтами;
- підтримка клієнтів під час судового процесу;

Адвокат – адвокат виконує майже туж саму роль що і юрист але в сфері кримінального кодексу в обов'язки адвоката входять

- робота з клієнтом;
- підтримка клієнтів під час судового процесу;
- здійснення правового захисту;
- супровід справи у суді;

Аналітик – компанія має відділ аналітики в якому налічується 2 працівника, в їх обов'язки входить:

- збір та обробка аналітичних даних;
- пропозиції по оптимізації виробництва;

- розробка бізнес моделей;
- розробка бізнес планів для клієнтів;
- розробка моделей масштабування клієнтського бізнесу;

Секретар – людина займаючи дану посаду бере на себе роль помічника для юристів та адвокатів, в обов'язки входить:

- менеджмент часу юристів та адвоката;
- робота з клієнтами;
- складання шаблонів договорів;
- визначення потреб клієнта та передача його на правильного спеціаліста;

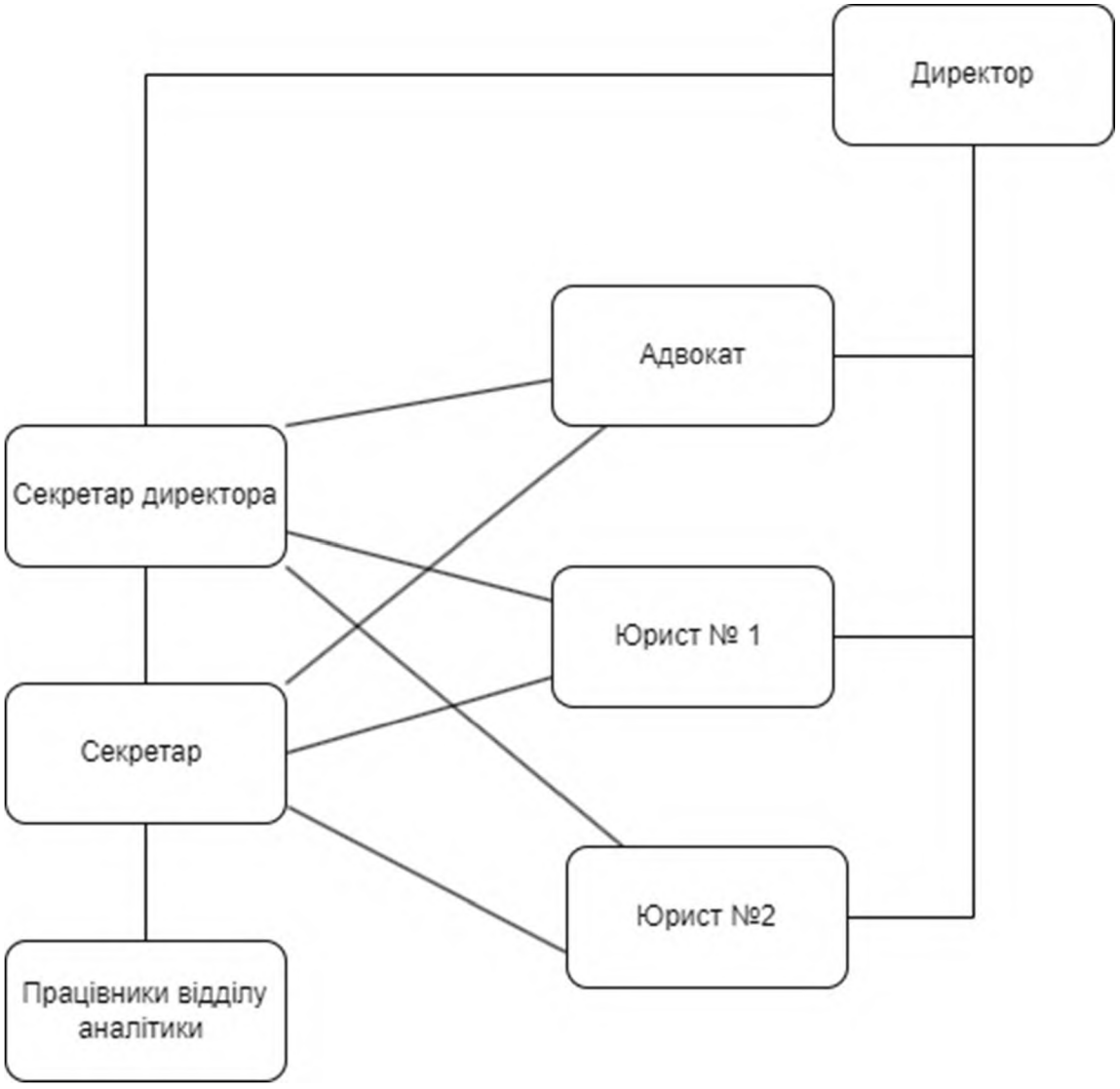

Рисунок 2.1 – Схема організаційної структури ТОВ Справедливість

Також окрім працівників ТОВ Справедливість задіяний обслуговуючий персонал компанії власника бізнес центру “Arena Tower” в якому знаходиться приміщення компанії, а саме:

- 2 прибиральники;
- 2 різнороби;
- 3 охоронці з групи реагування;
- 2 охоронці на КПП на першому поверсі БЦ;

За необхідністю їм може бути наданий доступ до ОІД.

2.4 Аналіз інформації підприємства

На підприємстві співробітниками обробляється інформація з обмеженим доступом:

- судові рішення;
- договори купівлі-продажу;
- бухгалтерські дані клієнтів;
- бухгалтерські дані компанії:
- банківські виписки;
- внутрішні договори компанії з партнерами;
- договори компанії з клієнтами;
- трудові договори;
- списки документів;
- інші;

Вся документація існує в фізичному та електронному вигляді, вся електронна інформація знаходиться у хмарному сховищі. Всі документи в фізичній формі видає працівникам при запиті секретар директора. Запит має буду сформований в кінці попереднього робочого дня з вказання часу на який вони беруться, або раніше з вказанням дати потреби, також є позачергова процедура отримання документів. Після втрати чинності документи підлягають ретельному знищенню. Компанія не використовує зовнішні носії інформації. Перелік

інформації, правовий режим, вид зберігання та вимоги до захисту в таблиці 2.1 Для розуміння таблиці наведено умовні позначення:

- К - вимога конфіденційності;
- Ц – вимога цілісності;
- Д – вимога доступності;

Також дані вимоги мають рівні:

- низька вимога (1);
- середня вимога (2);
- підвищена вимога (3);

Таблиця 2.1 - Інформація яка обробляється в ОІД

№	Інформація	Режим доступу	Правовий режим	Вимоги до властив. Інформації		
				К	Ц	Д
1	Персональні дані робітників	Обмежений доступ	Конфіденційна	3	1	1
2	Запити працівників на документи	Обмежений доступ	Конфіденційна	1	1	2
3	Договори з клієнтами	Обмежений доступ	Комерційна таємниця	3	2	1
4	Договори з партнерами	Обмежений доступ	Комерційна таємниця	3	2	1
5	Інформація про бухгалтерські справи компанії	Обмежений доступ	Комерційна таємниця	2	2	1
6	Список клієнтів	Обмежений доступ	Комерційна таємниця	2	1	2
7	Судові рішення	Обмежений доступ	Судова таємниця	3	3	1
8	Звіти аналітичного відділу з справ компанії	Обмежений доступ	Комерційна таємниця	2	1	1

Продовження таблиці 2.1

9	Інформація про заробітну плату працівників	Обмежений доступ	Комерційна таємниця	2	1	1
10	Конфіденційні данні клієнтів, які фігурують в судовій справі	Обмежений доступ	Судова таємниця	3	2	1

2.5 Обстеження зовнішнього фізичного середовища ОІД

Підприємство розташовано на одинадцятому поверсі бізнес центру “Arena Tower” за адресою вулиця Костомарівська, 4, Дніпро.

Фундаментом БЦ є бетон, стіни будівлі виконані з залізо-бетону, фасад БЦ складається з панорамних металопластикових вікон. До будівлі підведено електроне та водопостачання під землею.

Бізнес центр поділено на поверхи. В свою чергу кожен з поверхів поділено на офісні приміщення з системою коридорів та переходів в середині.

Території навколо БЦ немає як токової. БЦ має підземну паркову з КПП.

Перший поверх виступає в ролі КПП. Перший поверх виглядає як велика зала з кількома диванами для очікування, та КПП біля ліфтів та сход. В всіх ліфтах та дверях які надають доступ на сходи та поверхи стоять зчитувачі магнітних карт. Тимчасові співробітники мають записатися в список для отримання тимчасової карти доступу до поверх.

У неробочий час безпека забезпечується охороною БЦ, сигналізацією самого підприємства (сигналізація на відкриття дверей та вікон, та на об’єм). Охорона БЦ має доступ до системи охорони самого підприємства. У разі спрацювання сигналізації охорона БЦ повинна вжити дії, та вона ж несе відповідальність.

Біля БЦ є будинки які перелічені в таблиці 2.2 та на рисунку 2.1.

Таблиця 2.2 - Характеристика сусідніх споруд

№	Найменування	Адреса	Відстань до ОІД, м
1	Стадіон “Дніпро Арена”	вулиця Херсонська 7	30
2	Гуртожиток	вулиця Костомарівська 1	30
3	Перукарня	вулиця Воскресенська 46	50
4	Салон краси	вулиця Воскресенська 41	30
5	Туристичне агентство	вулиця Воскресенська 41	40
6	Магазин хоз. товари	вулиця Воскресенська 46	50

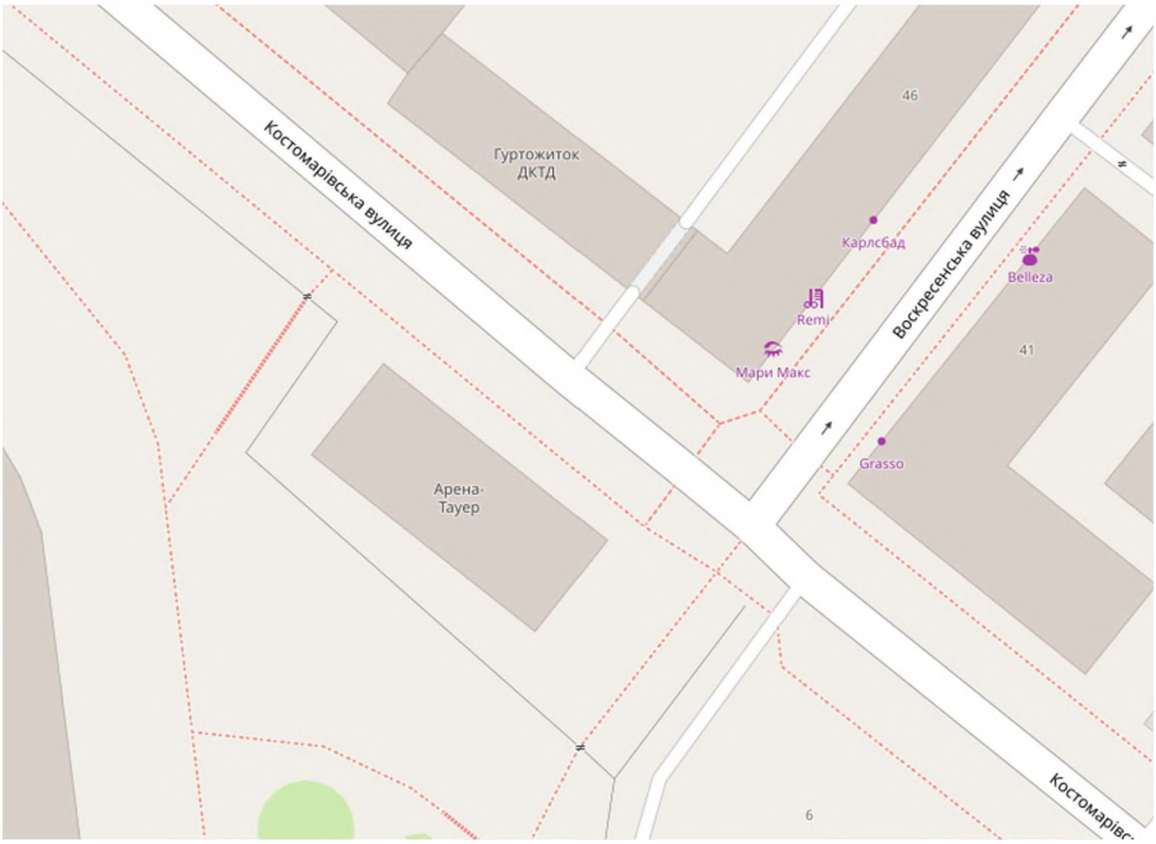

Рисунок 2.1 План будівлі та сусідніх споруд

До БЦ підключенні комунікації такого виду:

– електропостачання

Йде від найближчої трансформаторної підстанції через підземне комунікації розподільної системи, яка знаходиться з зовні БЦ. Також мається промисловий аварійний генератор з зовні біля БЦ.

– каналізація та водопостачання;

Підключено до міської системи каналізації, знаходиться в підвальному приміщенні БЦ.

– система опалення;

Система опалення є автономною для даного БЦ. Котельня знаходиться в підвалі БЦ, та опалює всю будівлю

– інтернет;

Інтернет підключено до лінії провайдера та протягнено по всій будівлі.

2.6 План приміщення підприємства

Рисунок 2.2 План підприємства

Опис приміщення:

- площа ОІД: 216,76 м^2;
- висота стін: 280 см;
- поверх – 11;
- підлога:
    1. Матеріал: бетон
    2. Товщина 1м
    3. Покриття: ламінат
- стіни:
    1. Товщина: стін 10 см.
    2. Матеріал: цегла.
    3. Кожна стіна обшита звукоізоляцією.
- вікна:
    1. Матеріал: пластик.
    2. Кількість: 10 шт.
    3. Всі вікна панорамні.
- сигналізація підключена до ПКП на КПП охорони БЦ на першому поверсі;
- інтернет: оптоволоконний кабель, підключено до мережевого обладнання провайдеру (компанія “Київстар”)

2.7 Захист приміщення підприємства

Захистом приміщення займається охорона компанія яку найняв власник БЦ “Arena Tower”. На цю фірму падає вся відповідальність за охорону приміщення компанії. Фізична охорона відбувається таким чином:

У робочий час. Чергові знаходяться на КПП на першому поверсі та займаються перевіренням особистостей. Також Команда реагування стежить за приміщеннями завдяки встановленим по всій будівлі камерам стеження.

У неробочий час. Група охорони стежить по камерах та патрулює територію БЦ не заходячи в приміщення підприємств орендуючих. Окрім камер та патрулів на території підприємства стоять датчики диму, об’єму, руху,

відкриття дверей та вікон, магнітні замки на дверях. У разі спрацювання системи сигналізації, охорона БЦ повинна знайти причинну спрацювання, занести факт спарювання системи в звіт охорони за ніч та повідомити директора компанії на території якої було спрацьовування.

2.8 Опис обчислювальної системи

В системі використовуються однакові вісім стаціонарних комп'ютери. Специфікація комп'ютерів вказана в таблиці 2.3, також налічується 5 принтерів для друку копій документів але вони до системи не підключені, вони підключені до комп'ютерів на робочих місцях за допомогою проводу. Всі комп'ютери підключені до єдиної мережі.

Таблиця 2.3 - Опис обчислювальної системи

№	Назва в системі	Специфікація
1	Директор	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
2	Секретар директора	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
3	Адвокат	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
4	Юрист №1	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
5	Юрист №2	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
6	Аналітик №1	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
7	Аналітик №2	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660
8	Секретар	Процесор: Ryzen 5 2600, ОЗУ: 16 Gb 2400Mhz DDR 4, Пам'ять: 1TB SSD, Відеокарта: RTX 1660

Принцип підключення кожного з комп’ютерів співробітників до мережевої системи зображено на рисунку 2.4

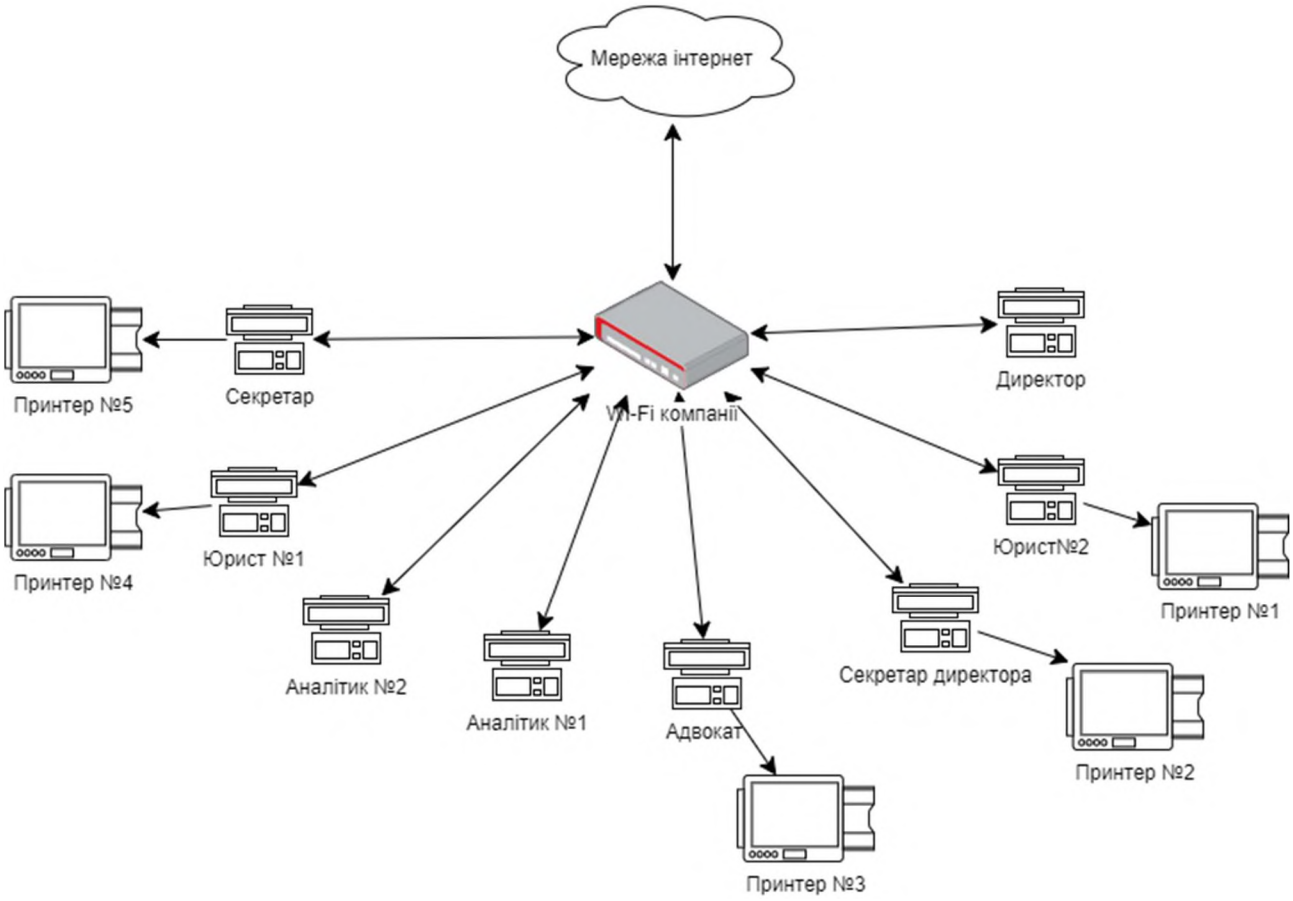

Рисунок 2.4 Схема ІКС

Після обробки в системі дані відправляються в хмарне сховище. Після відправки документа або його копії дані видаляються з комп’ютера для забезпечення безпеки конфіденційності даних клієнтів та самої компанії. Даний протокол допомагає запобігти витику інформації при можливому фізичному вкрадені самого комп’ютера співробітника або випадковому витику при відправці комп’ютера на технічне обслуговування, модифікацію чи ремонт.

2.9 Аналіз загроз

В даному розділі буде зроблено аналіз ризиків, а саме загроз та вразливостей підприємства. Даний аналіз буде зроблено основуючись на основі нормативного документу ДСТУ ISO/IEC 27005:2015 [8].

Аналіз загроз вразливостей включає в себе:

- розробка моделі порушника;
- розробка моделі загроз:
- оцінка ризиків та вірогідність реалізації;
- ідентифікація наслідків;

Згідно до НД ТЗІ 1.4-001-2000 [13] буде розроблено класифікації та модель порушника. Для початку пояснюється хто є порушником. Порушник – це особа що намагається отримати несанкціонований доступ до інформації порушуючи конфіденційність, з мотивами:

- ознайомлення;
- зміни;
- знищення;
- копіювання;
- тощо;

Порушника можна поділити на дві групи

Перша група це зовнішні порушники. До даного типу порушників відносяться особи, які знаходяться за межами системи. Даний тип порушників можуть становити крадії, недобросовісні клієнти, конкуренти. Також під даний тип порушника підходять особи які обслуговують приміщення такі як сантехніки, прибиральники, та інші. Даним особам не передбачено доступ до ІзОД, але вони можуть мати доступ до приміщень в яких розміщено компоненти ІКС, а маючи доступ до компонентів ІКС вони можуть отримати доступ до ІзОД.

Другою групою є внутрішні порушники. До даного типу порушників відносяться особи, які безпосередньо мають доступ до фізичного підключення до каналів зв'язку, обігу інформації та інших частин мережі передачі інформації. Даними особами можуть бути користувачі системи або персонал який

безпосередньо обслуговує саму систему та забезпечує її працездатність та функціонування.

Модель порушника створюється беручи до уваги різну специфікацію з різними показниками:

- за мотивами;
- за рівнем обізнаності до ІКС;
- за часом та містом доступу до ІКС;
- за рівнем можливостей використання елементів ІКС для реалізації загрози;

Профіль порушника в свою чергу визначає сукупність цих характеристик.

Також кожен з порушників має свій рівень загрози для системи. Рівні поділяються наступним чином:

- 0 – не становить загрози;
- 1 – незначна;
- 2 – низька;
- 3 – середня;
- 4 – висока;
- 5 – критична;

Роблячи висновок з результатів характеристик оброблюємої інформації, категорії порушників. Робиться висновок, що найбільш небезпечними вважаються порушення конфіденційності та цілісності інформації, а спостережності найменшим.

Таблиця 2.4 - Категорії порушників за мотивами здійснення порушень

Позначення	Мотиви порушень	Рівень загрози
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисний інтерес	3

Таблиця 2.5 - Категорії порушників за рівнем кваліфікації та обізнаності щодо ІКС

Позначення	Рівень кваліфікації	Рівень загрози
К1	Низький рівень знань та вміння працювати з ІКС	1
К2	Високий рівень знань, має практичний досвід роботи з ІКС	2

Таблиця 2.6 - Категорії порушників за показником можливостей використання методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загрози
ПС1	Не має навичок	0
ПС2	Підглядав за роботою	0
ПС3	Взлом	3

Таблиця 2.7 - Класифікація порушника за місцем дії

Позначення	Місце дії	Рівень загрози
МД1	У приміщенні з елементами ІКС	1
МД2	У будь-якому місці, маючи доступ до інформації у хмарному сховищі	5

Після створення класифікацій порушників згідно до НД ТЗІ 1.4-001-2000 потребується створити модель порушника та визначити суму загроз які вони можуть становити для підприємства

Таблиця 2.8 - Модель порушника

Особа	Мотив	Подолання захисту	Кваліфікація	Місце	Сума загроз
Директор	М1	ПС3	К2	МД2	11
Секретар директора	М1	ПС3	К2	МД2	11
Адвокат	М1	ПС3	К2	МД2	11
Юрист №1	М1	ПС3	К2	МД2	11
Юрист №2	М1	ПС3	К2	МД2	11
Аналітик №1	М1	ПС3	К2	МД2	11
Аналітик №2	М1	ПС3	К2	МД2	11
Секретар	М1	ПС3	К2	МД2	11
Клієнти	М3	ПС3	К1	МД1	5
Прибиральниця	М3	ПС2	К1	МД1	5
Різнороби	М3	ПС2	К1	МД1	5
Охорона БЦ	М1	ПС3	К1	МД1	6

Аналізуючи більш детально модель порушника можливо зробити висновок що найбільшу загрозу для підприємства становлять співробітники даного підприємства. Оскільки вони мають доступ до всіх документів компанії напряму.

Серед зовнішніх порушників найбільшу загрозу становить охорона БЦ, яка в неробочий час має доступ до ІКС і маючи спеціалізоване обладнання для взлому має змогу отримати доступ до інформації.

2.10 Модель загроз

Після аналізу підприємства розглянуто згідно до НД ТЗІ 2.5-004-99 [11] перелік можливих загроз для К,Ц.Д.

- К – конфіденційність;
- Ц – цілісність;

– Д – доступність інформації;

Таблиця 2.9 - Перелік можливих загроз

Можливі загрози для інформації	Ризики для		
	К	Ц	Д
Відсутність доступу до інтернету			+
Несанкціоноване читання даних компанії	+		
Несанкціоноване підключення до мережі компанії	+	+	
Несанкціоноване прослуховування	+		
Розголошення паролів	+	+	+
Пошкодження пристроїв		+	+
Модифікація ПЗ з цілю шпіонажу	+		
Вхід до системи сторонніх осіб	+	+	
Розголошення інформації персоналом	+		
Ураження шкідливим ПЗ	+	+	+

2.12 Можливі вразливості компанії

У разі зникнення доступу до інтернеті, підприємство не зможе деякий час отримати потрібні для роботи документи це зупинить роботу на деякий час, це призводить до втрати доступності.

У разі недобросовісного співробітника він може надавати стороннім особам конфіденційні дані, це призводить до втрати конфіденційності.

У разі несанкціонованого доступу до мережі компанії, компанія може понести великі збитки через копіювання або знищення важливих документів чи розголошення конфіденційних даних, це призводить до втрати конфіденційності, цілісності та доступності.

У разі пошкодження пристроїв є вірогідність втрат даних копії яких ще не були зроблені, це в свою чергу призводить до втрати цілісності та доступності.

У разі ушкодження шкідливим ПЗ є вірогідність пошкодження системи та всіх даних в ній, це призводить до втрати конфіденційності, цілісності та доступності.

2.13 Профіль захищеності

Проаналізувавши характеристики ІКС об’єкту кваліфікаційної роботи, та вимог відповідно до НД ТЗІ 2.5-005-99 [14] підприємству видано 3 клас захисту як розподілений багатомашинний багатокористувацький комплекс який обробляє інформацію різних ступенів обмеження доступу.

Проаналізувавши підприємство та якій йому придатні загрози обрано наступний профіль захищеності:

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

КД-2. Базова довірча конфіденційність

Базова довірча конфіденційність. В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Необхідною умовою є НИ-1.

КА-2. Базова адміністративна конфіденційність

Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і

захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту. Необхідними умовами є НО–1, НИ–1.

КО-1. Повторне використання об'єктів

Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною

КВ-2. Базова конфіденційність при обміні

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ

повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Необхідною умовою є НО-1.

ЦД-1. Мінімальна довірча цілісність

Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта. Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту. Необхідною умовою є НИ-1.

ЦА-2. Базова адміністративна цілісність

Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів,

процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт. КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес. Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту. Необхідними умовами є НО-1, НИ-1.

ЦО-1. Обмежений 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 певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу. Необхідною умовою є НИ-1.

ЦВ-2. Базова цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання. Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження. Необхідною умовою є НО-1.

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження. Необхідною умовою є НО-1.

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. Необхідною умовою є НО-1.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ має бути здатним передавати журнал реєстрації в інші системи з використанням певних механізмів захисту. Необхідною умовою є НИ-1.

НИ-2. Одиночна ідентифікація і автентифікація

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі. Необхідною умовою є НИ-1.

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Необхідною умовою є НО-1.

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.14 Розробка політики безпеки

Основуючись на аналізі підприємства, загрозах, моделі порушника і беручи до уваги показники профілю захищеності, розроблено базові елементи політики безпеки інформації для підприємства [18].

До загроз підприємству належать:

- модифікація стандартного ПЗ з метою шпіонажу;
- ураження шкідливим ПЗ;
- розголошення паролів;
- вхід до системи сторонніх осіб;

2.14.1 Антивірус

Мета:

Метою даної політики є допомога в запобіганні зараженню комп'ютерів, мережі, та інших систем компанії шкідливим ПЗ та пошкодження конфіденційних даних компанії.

Додаткове навчання:

Не потребується.

Додаткове забезпечення:

Потребується додаткове ПЗ, а саме підписка на ліцензійний антивірус

Дії:

Співробітник має дочекатися та не відключати комп'ютер до завершення обстеження, та у разі виявлення шкідливого ПЗ вжити дій запропонованих антивірусом та повідомити секретаря директора.

Відповідальність у разі порушення:

Компанія має проаналізувати яких саме втрат вона зазнала. В залежності від втрат обрати міру покарання, починаючи з дисциплінарної відповідальності закінчуючи звільненням та вимогою відшкодування частини витрат.

2.14.2 Політика інтернету

Метою політики є впровадження правил використання глобальної мережі інтернет.

Додаткове навчання:

Тренінг по розпізнаванню ненадійних сайтів та підозрілих посилань

Додаткове забезпечення:

Не потребується.

Дії:

Співробітникам забороняється скачувати та встановлювати стороннє ПЗ. Також забороняється переходити за посиланнями від незнайомих осіб та переходити на підозрілі сайти.

Відповідальність у разі порушення:

Фінансове стягнення, у разу якщо через це компанія понесла великі збитки мірою покарання може бути звільнення.

2.14.3 Політика контролю фізичного доступу

Метою політики є запобігання ознайомлення сторонніх осіб з системою.

Додаткове навчання:

Не потребується.

Додаткове забезпечення:

Не потребується.

Дії:

Співробітник повинен стежити щоб ніхто не міг підглядати за його роботою з системою. Для цього він повинен тримати монітор завжди розгорнутим до себе. Також він має бути впевненим що його ніхто не знімає під час роботи з системою.

Відповідальність у разі порушення:

Через неможливість контролювання та людський фактор, відповідальності за порушення немає. Окрім випадків виявлення навмисного порушення. В такому разі мірою покарання дисциплінарна відповідальність бо більше.

2.14.4 Політика керування журналами

Метою даної політики є стеження за фізичними копіями документів та обігом їх в компанії

Додаткове навчання:

Не потребується.

Додаткове забезпечення:

Не потребується.

Дії:

Співробітник повинен при потребі фізичної копії документу записати у журнал який саме документ був взято, дату та час. У разі створення копії даного документу співробітник повинен внести в журнал факт створення та кількість копій.

Відповідальність у разі порушення:

У разі одноразового порушення слід надати дисциплінарну відповідальність, у разі постійного порушення мірою покарання може бути звільнення співробітника.

2.14.5 Політика електронної пошти

Мета політики полягає в створені прави ведення корпоративної пошти.

Додаткове навчання:

Тренінг по розпізнаванню ненадійних сайтів та підозрілих посилань

Додаткове забезпечення:

Не потребується.

Дії:

Заборона на реєстрацію на не офіційних ресурсах за допомогою корпоративної пошти. Заборона відчинення листів від не надійних осіб для запобігання ураження комп'ютера та системи в цілому, та перехід за посилання триманим отриманим від не надійних осіб.

Відповідальність у разі порушення:

Співробітник який порушив має бути притягнутий до дисциплінарної відповідальності, але у разі якщо через це компанія понесла збитки мірою покарання обирається фінансове стягнення.

2.14.6 політика паролів

Мета цієї політики є створення надійних паролів для співробітників компанії за для забезпечення більшої безпеки компанії.

Додаткове навчання:

Не потребується.

Додаткове забезпечення:

Не потребується.

Дії:

Кожен працівник компанії має встановити в системі та на офіційних сайтах де потребується реєстрація встановлення надійного пароля. Надійним паролем є пароль який налічує від 10 або більше символів. Він має налічувати в собі цифри, великі та малі літери особливі знаки. В системі та на кожному сайті має бути пароль який не повторює інші.

Відповідальність у разі порушення:

Співробітник який порушив має бути притягнутий до дисциплінарної відповідальності.

2.15 Висновок до другого розділу

У другому розділі кваліфікаційної роботи розроблені та наведені відомості що до роботи підприємства ТОВ Справедливість. Базуючись на проведеному

аналізі підприємства був створений акт обстеження підприємства. Після цього проведено аналіз загроз та вразливостей підприємства. Данії дії показали що підприємство потребує більшої захищеності і спираючись на це були розроблені елементи політики безпеки інформації на підприємстві.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування доцільності витрат на реалізацію ПБ

Метою розрахунків є економічне обґрунтування доцільності витрат на впровадження політики безпеки інформації. Для цього треба розрахувати доцільність та економічну ефективність ведення розробки заходів безпеки, їх ведення та експлуатації. Основною для визначення витрат на розробку політики безпеки є концепція сукупної вартості володіння. У даній моделі враховується наступні витрати:

Економічна доцільність визначається за допомогою розрахунків:

капітальних витрат, витрати що потребує розроблення політики безпеки;

поточних витрат, витрати на експлуатацію та обслуговування об'єкта;

економічної ефективності від впровадження;

3.2 Розрахунок капітальних витрат

Капітальні інвестиції – дані кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.2.1. Визначення трудомісткості на розробку політики безпеки

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

Трудомісткість створення політики безпеки розраховується за формулою:

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

- $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, склало 5 години
- $t_{\text{в}}$ – тривалість розробки концепції безпеки інформації у організації, склало 14 години
- $t_{\text{а}}$ – тривалість процесу аналізу ризиків, склало 6 години

- $t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту, склало 6 годин
- $t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, склало 4 годин
- $t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, склало 12 годин;
- $t_{д}$ – тривалість документального оформлення політики безпеки, склало 6 години

$$t = 5 + 14 + 6 + 6 + 4 + 12 + 6 = 53$$

Трудомісткість створення ПБ складає: t = 53 години.

3.2.2 Розрахунок витрат на створення ПБ.

Витрати на розробку ПБ інформації являють собою суму витрат на заробітну плату спеціаліста з інформаційної безпеки та вартості витрат машинного часу, необхідного для розробки ПБ. Розраховуються за формулою:

$$К_{рп} = З_{зп} + З_{мч} \text{ (3.2)}$$

- $К_{рп}$ - витрати на розробку ПБ
- $З_{зп}$ - заробітна плата спеціаліста з інформаційної безпеки
- $З_{мч}$ - вартість витрат машинного часу

Заробітна плата виконавця враховує основну і додаткову заробітну плату та соціальні відрахування (пенсійне страхування, соціальне страхування тощо) та розраховується за формулою:

$$З_{зп} = t \cdot З_{іб}, \text{грн (3.3)}$$

- t – загальна тривалість створення ПЗ, годин
- $З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину

$$З_{зп} = 53 \cdot 220 = 11600 \text{ грн}$$

Заробітна плата спеціаліста з інформаційної безпеки складає $З_{зп}$ = 11600 грн.

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

$$З_{мч} = t \cdot С_{мч}, \text{грн} \quad (3.4)$$

- t – трудомісткість розробки політики безпеки інформації на ПК,годин
- $С_{мч}$ – вартість 1 години машинного часу ПК, грн./годин

Вартість 1 години машинного часу ноутбуків визначається за формулою:

$$С_{мч} = P \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р} \quad (3.5)$$

- P – встановлена потужність ПК, кВт (0,6 кВт)
- $С_е$ – тариф на електричну енергію, грн/кВт·година (2,64 грн/кВт·година)
- $Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн ($Ф_{зал}$ = 14000 грн).;
- $Н_а$ – річна норма амортизації на ПК, частки одиниці (1/4 на рік);
- $Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення,частки одиниці (1);
- $К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн (25000 грн);
- $F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920.)

$$С_{мч} = 0{,}6 \cdot 2{,}64 + \frac{14000 \cdot \frac{1}{4}}{1920} + \frac{25000 \cdot 1}{1920}, \text{грн}$$

Вартість 1 години машини складає: $С_{мч}$ = 16,42 грн.

$$З_{мч} = 53 \cdot 16{,}42$$

Вартість витрати машинного часу складає: $З_{мч}$ = 870,26 грн.

$$К_{рп} = 11600 + 870{,}26$$

Витрати на розробку ПБ складають: $К_{рп}$ = 12470,26 грн

Таким чином капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} \quad (3.6)$$

- $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн. (11600), до розробки залучено спеціаліста за кібербезпеки.
- $К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, тис. грн. (25000), такого як Windows 11 pro, MS Office 2021, Avast Ultimate Business Security.
- $К_{рп}$ – вартість розробки політики безпеки інформації, тис. грн. (12470)
- $К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн. (5000)
- $К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Не враховується у зв'язку з тим що підприємство не закуповує додаткового обладнання.

$$К = 11600 + 25000 + 12470 + 5000 = 54070 \text{ грн}$$

Сума фіксованих витрат становить: К = 54070 грн.

3.3. Розрахунок поточних витрат.

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \text{тис. грн.} \quad (3.7)$$

- $С_{в}$ – витрати на Upgrade-відновлення й модернізації системи
- $С_{к}$ - витрати на керування системою інформаційної безпеки в цілому
- $С_{ак}$ - витрати, викликані активністю користувачі системи інформаційної безпеки.

Витрати на керування системою в цілому ($С_{к}$) вираховується за формулою:

$$С_к = С_н + С_а + С_з + С_{єв} + С_с + С_{ел} + С_о + С_{тос}, грн \quad (3.8)$$

- $С_н$ - витрати на навчання адміністративного персоналу й кінцевих користувачів (0).

$С_а$ - річний фонд амортизаційних відрахувань вираховуються заформулою:

$$С_а = К_{зпз} \cdot А, грн (3.9)$$

Беручи до уваги що компанія не закуповує ніякого додаткового обчислювального обладнання, єдине на що треба робити амортизаційні відрахування, це придбання ліцензійного програмного забезпечення, через це отримаємо, щорічний відсоток амортизації на 2 роки використання буде:

$$А = \frac{100}{2}\% = 50\%$$

Далі використовується формула 3.9 та отримуємо:

$$С_а = 25000 \cdot 0.5 = 12500 грн.$$

Отже річні амортизаційні витрати становлять: $С_а$ = 12500 грн.

$С_з$ - Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки складає:

$$С_з = З_{осн} + З_{дод}, грн. \quad (3.10)$$

$З_{осн}$, $З_{дод}$ - основна і додаткова заробітна плата відповідно, грн на рік.

$З_{осн}$= 35200 грн на місяць

$З_{дод}$ вираховується в розмірі 8-10% від основної заробітної плати.

$$С_з = 35200 \cdot 12 + (35200 \cdot 12 \cdot 0{,}1) = 464\,640 грн$$

Річний фонд заробітної плати становить: $С_з$ = 464 640 грн на рік

Для платників податків на спрощений системі ставка ЄСВ становить 22%, отже:

$$С_{єв} = 464640 \cdot 0{,}22 = 102\,220 грн$$

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування становить: $С_{єв}$ = 102 220 грн

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, грн \quad (3.11)$$

- Р – встановлена потужність апаратури інформаційної безпеки, кВт (2);
- $F_р$ – річний фонд робочого часу системи інформаційної безпеки($F_р$ = 1920);
- $Ц_е$ – тариф на електроенергію, грн/кВт·годин (2,64 грн/кВт·год)

$$С_{ел} = 2 \cdot 1920 \cdot 2{,}64 = 10137 \text{ грн}$$

Вартість електроенергії становить: $С_{ел}$ = 10137 грн.

$С_о$ – витрати на залучення сторонніх організацій, не залучено.

$С_{тос}$ – витрати на технічне та організаційне адміністрування й сервіс системи інформаційної безпеки що визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає 3% від суми капітальних інвестицій що = 1622 грн.

$$С_к = 0 + 12500 + 464\,640 + 102\,220 + 10137 + 0 + 1622 = 595\,119 \text{ грн}$$

Витрати на керування системою в цілому становлять: $С_к$ = 595 119 грн.

3.4. Оцінка величини збитків.

- $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідокатаки, годин (16 годин)
- $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин (7 годин)
- $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин (10 годин)
- $З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів таін.), грн на місяць (35200 грн)

- $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць (23000 грн)
- $Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.),осіб. (3 особа)
- $Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб. (8 осіб)
- О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік, в даному підприємстві немає продажу, але налічується надання послуг за допомогою системи (8 000 000 грн)
- $П_{зч}$ – вартість заміни встаткування або запасних частин, грн (12000)
- I – число атакованих вузлів або сегментів корпоративної мережі (8)
- N – середнє число атак на рік (3 разів).

Розміри заробітної плати працівників компанії становить:

- Директор = 52000 грн;
- Секретар директора = 35000;
- Адвокат = 48000 грн;
- Юрист №1 = 37000 грн:
- Юрист №2 = 37000 грн;
- Аналітик №1 = 30000 грн;
- Аналітик №2 = 30000 грн;
- Секретар = 24000 грн;

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V \qquad (3.12)$$

- $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;
- $П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі, 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:

$$П_{П} = \frac{\sum З_{С}}{F} \cdot t_{П} \qquad (3.13)$$

F- місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч)

$$П_{П} = \frac{52000+35000+48000+37000 \cdot 2+30000 \cdot 2+240}{176} \cdot 16 = 26636 \text{ грн.}$$

Оплачувані втрати робочого часу та простої співробітників становить:

$П_{П} = 26636$ грн.

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

$$П_{В} = П_{ВИ} + П_{ПВ} + П_{ЗЧ}, \qquad (3.14)$$

- $П_{ВИ}$ – витрати на повторне уведення інформації, грн.
- $П_{ПВ}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн.
- $П_{ЗЧ}$ – вартість заміни устаткування або запасних частин, 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:

$$П_{ВИ} = \frac{\sum З_{С}}{F} \cdot t_{ВИ} \qquad (3.15)$$

$$П_{ВИ} = \frac{52000+35000+48000+37000 \cdot 2+30000 \cdot 2+24}{176} \cdot 10 = 16648 \text{ грн}$$

Витрати на повторне уведення інформації становить: $П_{ВИ} = 16648$ грн.

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються часом відновлення після атаки і розміром середньо годинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum З_{О}}{F} \cdot t_{В} \qquad (3.16)$$

$$П_{пв} = \frac{35200 \cdot 3}{176} \cdot 7 = 4200 \text{ грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі становлять: $П_{пв}$ = 4200 грн.

Далі за формулою (3.14):

$$П_{в} = 16648 + 4200 + 12000 = 32848 \text{ грн.}$$

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі $П_{в}$ = 32848 грн.

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

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \qquad (3.17)$$

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

$$V = \frac{8\,000\,000}{2080} \cdot (16 + 7 + 10) = 126\,923 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі становить: V = 126 923 грн.

Далі за формулою (3.12):

$$U = 26\,636 + 32\,848 + 126\,923 = 186\,407 \text{ грн.}$$

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить: U = 186 407 грн.

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

$$= \Sigma_i \Sigma_n U \qquad (3.18)$$

$$B = 8 \cdot 3 \cdot 186\,407 = 4\,473\,768 \text{ грн.}$$

Загальний збиток становить: 4 473 768 грн.

3.5. Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \quad (3.19)$$

- 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 (0.3);
- C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$\text{E} = 4\,473\,768 \cdot 0{,}3 - 595\,119 = 747\,011 \text{ грн.}$$

Загальний ефект від впровадження системи становить: E = 747 011 грн.

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

$$\text{ROSI} = \frac{E}{K} \quad (3.20)$$

$$\text{ROSI} = \frac{747\,011}{54070} = 13.8$$

$$\text{ROSI} = 13.8$$

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100) \quad (3.21)$$

- $\text{N}_{\text{кр}}$ – банківська кредитна ставка, %;
- $\text{N}_{\text{інф}}$ – річний рівень інфляції, %.

$$13.8 > ((35 - 4)/100)$$

$$13.8 > 0{,}31$$

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

$$T_0 = \frac{K}{E} = \frac{1}{ROSI}, \text{років (3.22)}$$

$$T_0 = \frac{1}{13.8}$$

Термін окупності капітальних інвестицій становить: T_0 = 0.07 роки

3.5 Висновок до третього розділу

У третьому розділі проведено детальний аналіз доцільності введення в експлуатацію захисних систем на основі витрат як капітальних так і експлуатаційних. За допомогою детального економічного аналізу визначено витрати, прибутки, та втрати.. Витрати на впровадження становлять - 54070 грн, витрати на експлуатацію - 595 119 грн, загальні збитки - 4 473 768 грн, загальний ефект від впровадження системи – 747 011 грн, коефіцієнт ROSI – 13.8. Основуючись на результатах аналізу зроблено висновок що впровадження системи є доцільним. Термін окупності становить менше місяця.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи описано стан кібербезпеки в Україні, основні загрози які стосуються інформаційної безпеки малого та середнього бізнесу та наслідки цих загроз. Також позначаються основні цілі та мета здійснення хакерами кібератак, даними цілями є державні установи та юридичні компанії. Таким чином розкрита потреба в збільшенні захищеності підприємства для уникнення збитків для нього самого. Також був проаналізовано список нормативно-правових документів в сфері захисту інформації на основі як будується захист. Та було поставлена задача з чіткими вимогами для побудування надійного захисту.

У другому розділі кваліфікаційної роботи розроблені та наведені відомості що до роботи підприємства ТОВ Справедливість. Базуючись на проведеному аналізі підприємства був створений акт обстеження підприємства. Після цього проведено аналіз загроз та вразливостей підприємства. Данії дії показали що підприємство потребує більшої захищеності і спираючись на це були розроблені елементи політики безпеки інформації на підприємстві.

У третьому розділі проведено детальний аналіз доцільності введення в експлуатацію захисних систем на основі витрат як капітальних так і експлуатаційних. За допомогою детального економічного аналізу визначено витрати, прибутки, та втрати.. Витрати на впровадження становлять - 54070 грн, витрати на експлуатацію - 595 119 грн, загальні збитки - 4 473 768 грн, загальний ефект від впровадження системи – 747 011 грн, коефіцієнт ROSI – 13.8. Основуючись на результатах аналізу зроблено висновок що впровадження системи є доцільним. Термін окупності становить менше місяця.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 1.6-005 – Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (Нормативний документ системи технічного захисту інформації)

2. Кількість кібератак у 2022 (Електронний ресурс) – 2023 – Режим доступу до ресурсу: https://forbes.ua/news/v-2022-rotsi-kilkist-kiberatak-na-ukrainu-zrosla-mayzhe-vtrichi-90-khakerskikh-grup-z-rf-kontrolyuyut-siloviki-04052023-13454

3. Пояснення шо таке кібератаки (Електронний ресурс) – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html?dtid=osscdc000283

4. Координація російських хакерів (Електронний ресурс) – 2023 – Режим доступу до ресурсу: https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosistemu-08112023-17242

5. Кібератаки на Україну (Електронний ресурс) – 2023 - Режим доступу до ресурсу: https://cip.gov.ua/ua/news/kiberataki-na-ukrayinu-za-dopomogoyu-khakeriv-rosiya-namagayetsya-otrimati-bud-yaku-informaciyu-yaka-mozhe-dati-yii-perevagu-v-konvenciinii-viini

6. Кібератака на компанію “Київстар” (Електронне ресурс) – 2023 - https://forbes.ua/news/khakeri-perebuvali-v-sistemi-kiivstar-z-travnya-2023-roku-sbu-04012024-18307

7. ДСТУ ISO/IEC 27001:2015 (Електронний ресурс) – 2015 - https://www.assistem.kiev.ua/doc/dstu_ISO-IEC_27001_2015.pdf

8. ДСТУ ISO/IEC 27005:2015 - Управління ризиками інформаційної безпеки

9. НД ТЗІ 1.1-002-99 - Загальні положення з захисту інформації в комп'ютерних системах від НСД (Нормативний документ системи технічного захисту інформації)

10. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в

комп'ютерних системах від несанкціонованого доступу (Нормативний документ системи технічного захисту інформації)

11. НД ТЗІ 2.5-004-99 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (Нормативний документ системи технічного захисту інформації)

12. НД ТЗІ 1.6-005-2013 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (Нормативний документ системи технічного захисту інформації)

13. НД ТЗІ 1.4 001 2000 - Типове положення про службу захисту інформації в автоматизованій системі (Нормативний документ системи технічного захисту інформації)

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

15. Ризики малого й середніх бізнесів (Електронний ресурс) – 2024 https://forbes.ua/brandvoice/kiberzakhist-dlya-malogo-ta-serednogo-biznesu-masshtab-zagroz-i-shcho-robiti-yakshcho-nemae-byudzhetu-rozpovidae-seo-digvel-oleksandr-babko-30062024-21931

16. Закон про адвокатську таємницю (Електронний ресурс) – 2013 - https://ips.ligazakon.net/document/JH1DU1AA?an=180

17. Закон про захист персональних даних (Електронний ресурс) – 2010 - https://zakon.rada.gov.ua/laws/show/2297-17#Text

18. Політики безпеки (Електронний ресурс) - https://purplesec.us/resources/cyber-security-policy-templates/#Wireless

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	10	
6	А4	2 Розділ	26	
7	А4	3 Розділ	10	
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	1	
14	А4	Додаток Д	1	
14	А4	Додаток Е	1	

ДОДАТОК Б. Перелік документів на оптичному носії

ФіліпенкоМ.В._125-20-2_ПЗ.docx

ФіліпенкоМ.В._125-20-2_ПЗ.pdf

Презентація.pptx

ДОДАТОК В. Акт категоріювання

Гриф обмеження доступу

Прим. № ___

ЗАТВЕРДЖУЮ
Керівник установи-власника (розпорядника, користувача) об'єкта
директор_Архіпов__А.В.
(посада, підпис, ініціали, прізвище)
18. 06. 2024
М.П.

АКТ
категоріювання ***ТОВ Справедливість***
(найменування об'єкта категоріювання)

1. Підстава для категоріювання ***Наказ про створення КСЗІ***
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об'єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

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

3.На ОІД здійснюється ***обробка технічними засобами та озвучування інформації***

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

5. Встановлена категорія ***IV категорія, бо четвертою категорією характеризуються об'єкти на яких обробляється технічними засобами***

та/або озвучується ІзОД, вимога щодо захисту якої встановлюється законом_

Голова комісії _____ А.С.Болов
(підпис) (ініціали, прізвище)

Члени комісії: _____ В.А.Дудков
(підпис) (ініціали, прізвище)

15.06.2024

ДОДАТОК Г. Наказ про створення КСЗІ

НАКАЗ

м. Дніпро

19.06.2024 №1

Про створення комплексної системи
захисту інформації в автоматизованій
системі класу “3” ІКС ТОВ Справедливість

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

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в автоматизованій системі класу “3” для обробки інформації з обмеженим доступом.
2. Відповідальному за службу захисту інформації в автоматизованих системах Донцову І.В., забезпечити супроводження робіт зі створення комплексної системи захисту інформації.
3. Контроль за виконанням наказу покласти на Мірного А.В.

Директор Архіпов А.В.

ДОДАТОК Д. Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 85 б. («добре»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-2

Філіпенко Максима Валерійовича

на тему: «Розробка політики безпеки інформаційно-комунікаційної системи ТОВ Справедливість»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 52 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІКС приватного підприємства ТОВ Справедливість.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». В кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз загроз для ІКС підприємства; аналіз ОІД та визначення типів інформації циркулюючої в системі підприємства; створення моделі порушника; обрання профіля захищеності; розробка політик безпеки інформації підприємства.

Практична цінність розробки полягає у підвищенні рівня інформаційної безпеки ІКС ТОВ Справедливість шляхом впровадження організаційних заходів захисту інформації.

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

За час дипломування Філіпенко М.В. проявив себе фахівцем, здатним самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» . Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки 74 (добре).

Керівник кваліфікаційної роботи проф. Гусєв О.Ю.

Керівник спец. розділу ст. викл. Тимофєєв Д.С.