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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Лігачова Єгора Тимуровича*

академічної групи *125-18ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ІнТайм»*

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

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Лігачову Є.Т.* **академічної групи** *125-18ск-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «ІнТайм»*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021№ 317-с

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Дослідити стан питання, проаналізувати базу, постановку задачі	20.05.2021
Розділ 2	Провести обстеження фізичного середовища, обстежити обчислювальну систему, побудувати модель порушника, модель загроз, виявити вразливості на підприємстві, визначити профіль захищеності, розробити елементи політики безпеки	30.05.2021
Розділ 3	Об'грунтувати витрати на впровадження політики безпеки	14.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 12.01.2021

Дата подання до екзаменаційної комісії: 15.06.2021

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ____ ст., ____ рис., ____ табл., ____ додатків, ___джерел.

Предмет розробки: політика безпеки інформації інформаційно-телекомунікаційної системи приватного підприємства ТОВ «ІнТайм».

Об'єкт розробки: інформаційно-телекомунікаційна система ТОВ «ІнТайм» – підприємство, що займається оптово-роздрібною торгівлею.

Мета проекту: підвищення рівня захищеності інформації в ІТС приватного підприємства ТОВ «ІнТайм».

Перший розділ кваліфікаційної роботи описує стан питання, нормативно-правову базу, підстави та етапи створення КСЗІ та ПБ, види загроз для малих підприємств.

У другому розділі наведено основні відомості про підприємство. Виконано обстеження інформаційної системи, фізичного середовища, середовища користувачів. Описано технологію обробки інформації та функціональний профіль захисту. Виконано категоріювання інформації, що обробляється в ІТС та визначено основні загрози та вразливості, їх джерела та складено модель порушника. Розроблено основні положення політики безпеки.

В третьому розділі було розраховано витрати на впровадження політики безпеки інформації та щорічні експлуатаційні витрати на її підтримку. Також було доведено економічну доцільність введення в експлуатацію політики безпеки інформації, розробленої в другому розділі.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки приватного підприємства ТОВ «ІнТайм».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ, ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕНОСТІ.

РЕФЕРАТ

Пояснительная записка:____ст.,___рис., ___табл.,___приложений, ____источников.

Предмет разработки: политика безопасности информации информационно телекоммуникационной системы частного предприятия ООО «ИнТайм».

Объект разработки: информационно-телекоммуникационная система ООО «ИнТайм» - предприятия, занимающегося оптово-розничной торговлей.

Цель проекта: повышение уровня защищенности информации в ИТС приват ного предприятия ООО «ИнТайм».

Первый раздел квалификационной работы описывает состояние вопроса, нормативно-правовую базу, основания и этапы создания КСЗИ и ПБ, виды угроз для малых предприятий.

Во втором разделе приведены основные сведения о предприятии. Выполнено обследование информационной системы, физической среды, среды пользователей. Описана технология обработки информации и функциональный профиль защиты. Выполнен категорирование информации, обрабатываемой в ИТС и определены основные угрозы и уязвимости, их источники и составлен модель нарушителя. Разработаны основные положения политики безопасности.

В третьем разделе было рассчитано затраты на внедрение политики безопасности информации и ежегодные эксплуатационные затраты на ее поддержку. Также было доказано экономическую целесообразность введения в эксплуатацию политики безопасности информации, разработанной во второй главе.

Практическое значение проекта заключается в повышении уровня информационной безопасности частного предприятия ООО «ИнТайм».

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТРИ, ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ ЗАЩИЩЕННОСТИ.

ABSTRACT

Explanatory note: ____art., ____Fig., ____Table., ____Appendices, ____sources.

Subject of development: information security policy of the information and telecommunication system of the private enterprise LLC "InTime".

Object of development: information and telecommunication system of LLC "InTime" - an enterprise engaged in wholesale and retail trade.

The purpose of the project: to increase the level of information security in the ITS of the private enterprise LLC "InTime".

The first section of the qualification work describes the state of the issue, the regulatory framework, the grounds and stages of creation of KSZI and PB, types of threats to small businesses.

The second section provides basic information about the company. The survey of the information system, physical environment, user environment was performed. The information processing technology and the functional protection profile are described. The categorization of information processed in ITS is performed and the main threats and vulnerabilities, their sources are identified and the model of the violator is made. The main provisions of the security policy have been developed.

In the third section, the costs of implementing the information security policy and the annual operating costs of its support were calculated. The economic feasibility of implementing the information security policy developed in the second section was also demonstrated.

The practical significance of the project is to increase the level of information security of the private enterprise LLC "InTime".

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

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОМ – електронно-обчислювальна машина;

ЖМД – жорсткий магнітний диск;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

НД ТЗІ – нормативний документ в галузі технічний захист інформації.

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЕМВ – побічне електромагнітне випромінювання;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПЗП – постійний записуючий пристрій.

СКУД – система контролю та управління доступом;

СУБД – система управління базами даних;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

У кваліфікаційній роботі предметом дослідження є забезпечення інформаційної безпеки малих підприємств, оскільки у сучасному світі складно уявити організацію роботи людини та підприємства без впровадження автоматизованих систем і процесів. При цьому кожен розробник намагається зробити свою систему більш простою і зручною у використанні, так як конкуренція на цьому ринку досить велика. З кожним роком сфера інформаційних технологій розвивається все швидше. Все більше і більше піддаються автоматизації різні виробничі процеси. Так само зростає і кількість користувачів мережі Інтернет. В даний час рідкісна система функціонує без використання ресурсів мережі Інтернет.

Об’єктом в кваліфікаційній роботі виступає інформаційно-телекомунікаційна система ТОВ «ІнТайм» – підприємства, що займається оптово-роздрібною торгівлею.

Предметом роботи в кваліфікаційній роботі є політика безпеки інформації.

Метою кваліфікаційної роботи є розробка політики безпеки. Дана тема є актуальною, оскільки окрім зовнішніх впливів на безпеку (пограбування, злом) організації існує загроза витоку інформації з інформаційних каналах зв'язку. Зовнішнє забезпечення безпеки стає недостанім. З'являється все більше різних фірм, які виробляють однакові послуги, росте і конкуренція. В таких умовах, кожен керівник зацікавлений в забезпеченні цілісності, доступності та конфіденційності інформації, що стосується діяльності організації.

Актуальність роботи полягає у необхідності протидії широкому спектру загроз в корпоративних мережах малих комерційних підприємств.

1 СТАН ПИТАННЯ. ПОСТАВНОВКА ЗАДАЧІ

1.1 Стан питання

У першому півріччі 2020 року кількість кібератак зросла на 22% з порівнянням із другим півріччям 2019 року. За даними Gartner [1] до 2022 року ринок програмного забезпечення та послуг з захисту інформації від несанкціонованого доступу досягне за ціною 170,7 мільярдів доларів.

У середньому лише 5% від усіх папок компанії повністю захищено від кібератак.

Статистика Symantec [1]показує, що 37% усіх форматів шкідливих вкладень в електронній пошті мають формати .docx і .dot, приблизно 19,5% має формат .exe.

Сьогодні уникнути кібератак неможливо. Вони вже стали звичним явищем для бізнесу, адже кожна нова впроваджена технологія або онлайн-сервіс для компанії підвищує ймовірність стати їх головною мішенню. І чим більше розвивається ІТ-складова компанії, тим більше вдосконалюються хакери. Тому сьогодні головне завдання власників компаній – не уникнути кібератак, а захистити дані бізнесу.

Статистика компаній Symantec показує, що:

– на 1 з 36 мобільних пристроїв встановлено небезпечні додатки;

– 1 з 13 пошукових запитів приводять до шкідливих програм;

– 48% від усіх шкідливих повідомлень електронної пошти відносяться до офісних файлів.

За місяць IoT-пристрої фіксують у середньому 5200 кібератак.

Науковці проводять грань між порушеннями, що скоїли хакери, і порушеннями, що призвели до витоку інформації через помилки персоналу при обороті інформації. Зазвичай, кількість кібератак і випадкових витоків приблизно однакова, але не у 2020 році – кількість інцидентів витоку даних стабільна, а кількість кібератак зросла у 2 рази. Це пов’язано з підвищенням

навантаження на організації через пандемію і переводом співробітників на дистанційний режим роботи. Співробітники все більше і більше покладаються на телекомунікаційні технології при спілкуванні і обміні інформацією, при цьому роблячи все більше можливостей для реалізації загроз.

Найчастішим випадком стають інциденти з вірусами-вимагачами. Цей метод йде перед вразливостями системи, фішинговими атакими і шкідливими програмами.

Велика кількість кіберзлочинців запускають до системи організації програми-вимагачі за допомогою фішингових атак. В такому випадку, програма-вимагач – це лише перший крок, і з цього слідує, що організація в полі спостереження з боку злочинців, це лише складова інциденту безпеки.

При витоку інформації, внутрішні помилки організацій займають переважну більшість – 83%. Як правило, такі випадки трапляються, коли співробітники надсилають інформацію не тій людині, залишають важливі фізичні и цифрові файли в загальнодоступному місці і не інсталюють оновлення.

Внутрішні помилки досить часто призводять до ситуації, коли важко знайти стороннього, оскільки задачею начальства є інформування співробітників про ризики безпеки, причиною яких вони можуть стати, і демонструвати, як уникати помилок, котрі для компанії стають дуже коштовними.

Ще однією причиною витоку інформації є інсайдери, тобто зловмисники всередині організації (див. рис. 1.1) [2].

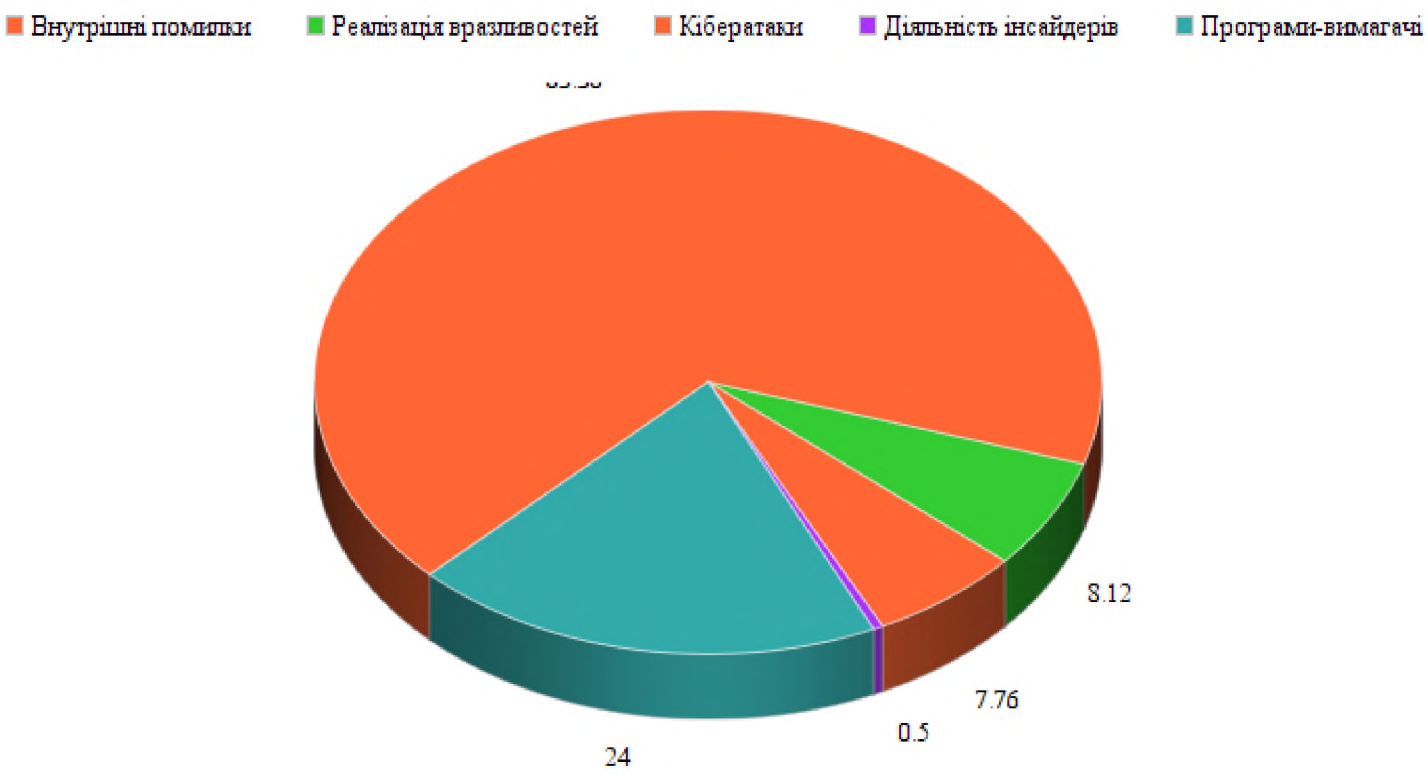


Рисунок 1.1 – Типи порушень

Компанія, що спеціалізується на розробці антивірусного ПЗ, щорічно проводить дослідження динаміки DDoS-атак на базі даних системи моніторингу DDoS Intelligence. За підсумками дослідження у 3 кварталі 2020 року кількість DDoS-атак у всьому світі зросла в 3 рази в порівнянні з результатами попереднього року (див.рис. 1.2).[3]

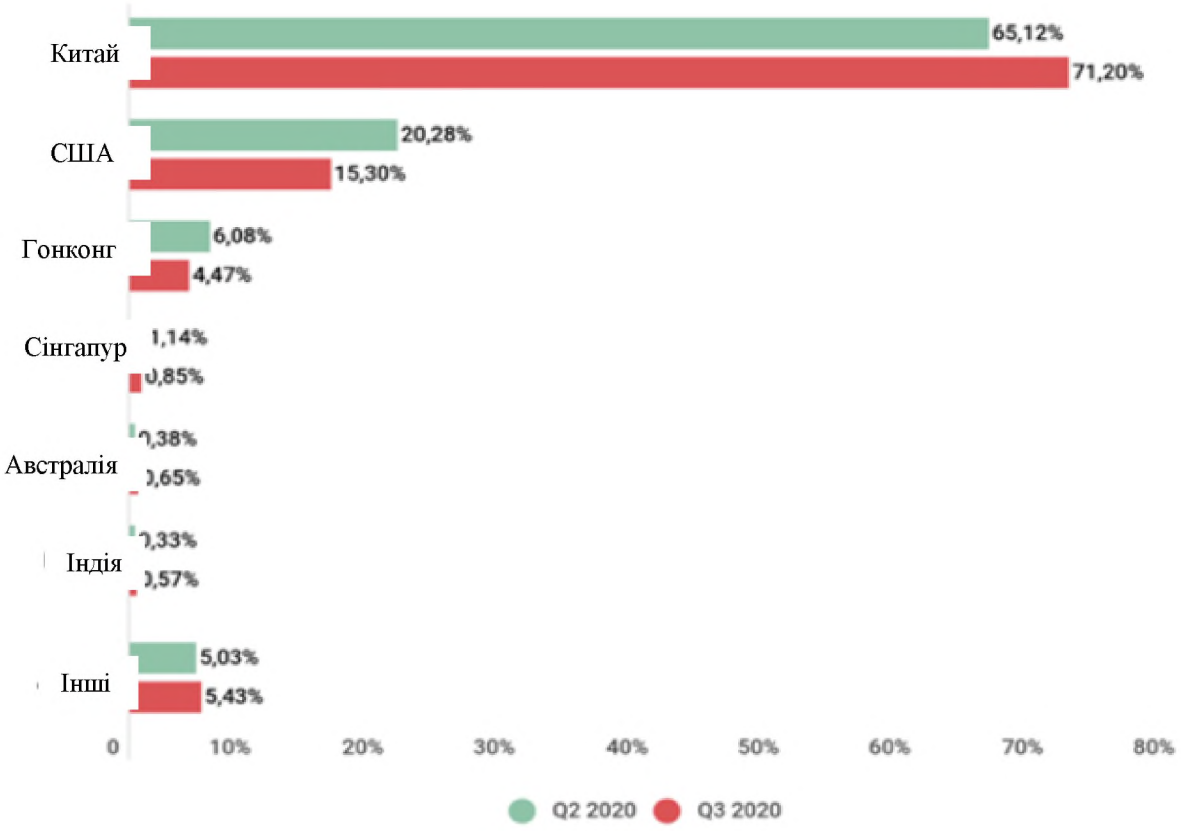


Рисунок 1.2 – Порівняння кількості атак у 2 та 3 кварталі 2020 року

У 91 відсотку кібератак фішинг є першою лінією атаки. У той час як при традиційних фішинг-атаках розсилають електронні листи сотням або тисячам адресатів, спрямовані фішинг-атаки (гарпунний фішинг, Spear Phishing) націлені на невеликі підгрупи людей, як правило, співробітників компаній.

Шахрай, який планує спрямовану фішинг-атаку, може створити фальшиву електронну адресу співробітника і з неї написати кільком легітимним співробітникам, запитуючи інформацію про компанію. Думаючи, що вони спілкуються з колегою, легітимні співробітники можуть надати цю інформацію без задньої думки.

У разі використання стратегії атаки типу «Watering Holes» хакери розміщують шкідливі програми в коді веб-сайтів, які з найбільшою ймовірністю відвідують співробітники компанії, що атакується. Якщо працівник заходить на такий сайт з комп'ютера компанії, вся мережа компанії може піддатися вірусу,

що викрадає дані [4].

Компанія ESET – лідер у галузі інформаційної безпеки – попереджала про високу активність вже відомої програми-вимагача WannaCryptor (також відома як WannaCry або WCrypt) в 1 кварталі 2020 року.

Наймасштабніша атака WannaCry відбулася у травні 2017 року і спричинила глобальний хаос в комп'ютерних системах у всьому світі. Загроза поширювалася через експлойт EternalBlue, який був спрямований на критичну уразливість в ОС Microsoft, а саме в реалізації застарілої версії протоколу Server Message Block (SMB). Під час такої атаки кіберзлочинці сканували мережу на наявність комп'ютерів з незахищеним портом SMB, після чого запускали код експлойта для будь-яких виявлених уразливих пристроїв, а після цього завантажували шкідливий компонент, наприклад програму-вимагач WannaCryptor.D.

Через три роки WannaCry як і раніше залишається найактивнішою загрозою серед програм-вимагачів (див.рис. 1.3). За результатами дослідження ESET, в 1 кварталі 2020 року 40,5% виявлень програм-вимагачів припадає на WannaCry. Такий високий показник насторожує, враховуючи, що пройшло майже три роки з моменту найбільшого спалаху. За даними ESET, на початку 2020 року WannaCry була спрямована на користувачів Туреччини, Таїланду та Індонезії через велику кількість уразливих пристроїв в цих регіонах [5].

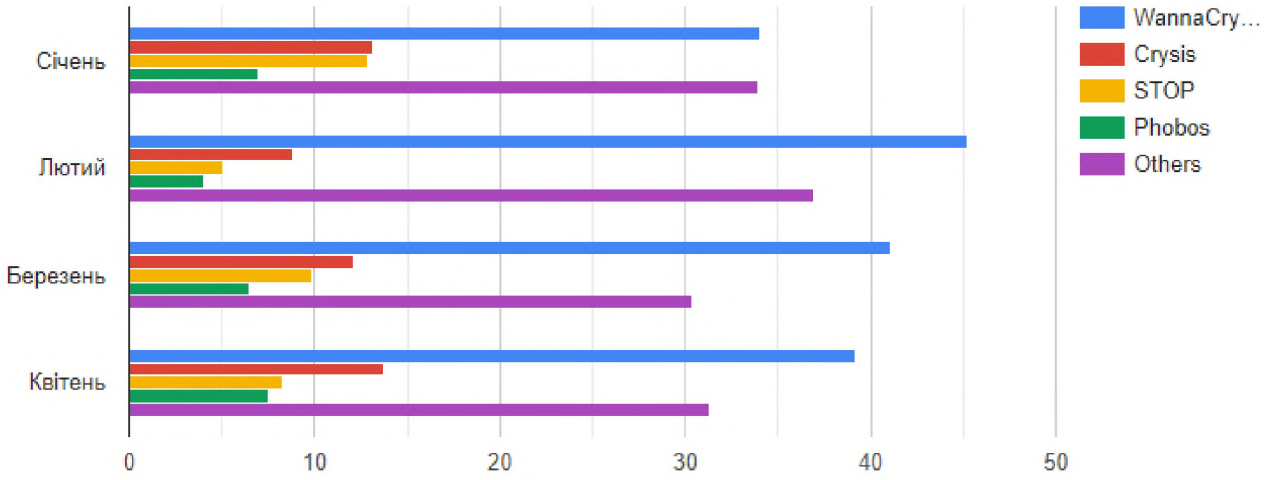


Рисунок 1.3 – Найактивніші програми-вимагачі

Будь-якому керівнику компанії доводиться стикатися з різними ризиками і загрозами бізнесу. Врахувати і перерахувати всі практично неможливо.

Внутрішні загрози бізнесу – це результат того, що відбувається всередині самої компанії. Розглянемо основні внутрішні ризики для компаній малого і середнього бізнесу. У корпораціях можуть бути свої можливості і загрози бізнесу.

До основних внутрішніх загроз бізнесу можна віднести:

– неблагонадійність персоналу. Співробітник може передавати важливу інформацію конкурентам. У разі звільнення менеджер найчастіше йде до конкурента і проводить дзвінки до власної клієнтської бази, пропонуючи співпрацю. Щоб звести до мінімуму подібний ризик, багато компаній впроваджують CRM-систему і зберігають дані не в Excel-таблицях, а в централізованій базі на сервері компанії;

– партнери. Наприклад, двоє друзів вирішили відкрити свою справу. Бізнес пішов в гору, почався розподіл прибутку. Друзі починають сваритися, кожен з них впевнений, що заслуговує більшого. В результаті може дійти до конфлікту і навіть до розвалу бізнесу. Тут можна порадити тільки одне – починати бізнес поодинці, без партнерів і співзасновників, а в міру необхідності

наймати фахівців. Звільнити працівника можна в будь-який момент, а співзасновник залишиться з вами назавжди;

– проблеми з менеджментом. Слідство недостатньої кваліфікації управлінського персоналу, помилок в плануванні, неправильних рішень. Низький рівень управління компанією може призвести до розвалу всього підприємства;

– фінансові загрози. Даний вид загроз бізнесу може бути в рівній мірі віднесений і до зовнішніх, і до внутрішнім. Він виникає як через невчасні оплати, стрибки валют або проблеми в економіці країни, так і з-за невірного фінансового планування. Рішенням може бути планування витрат, формування необхідних фінансових резервів, при необхідності - своєчасне отримання кредитів у банку.

Зовнішні загрози безпеки бізнесу – це ситуація, що склалася поза підприємства. Вона не пов'язана з діяльністю компанії, тому керівник може лише знизити наслідки. До основних загроз такого типу відносяться:

– макроекономічні кризи. Будь-яка проблема в світовій економіці неминуче впливає на діяльність окремих компаній. Під час криз знижується купівельна спроможність клієнтів, спостерігається зростання вартості кредитів та рівня інфляції;

– недобросовісні конкуренти. Одна з головних загроз - це дії компаній, що пропонують аналогічний товар;

– несанкціонований доступ сторонніх до комерційної інформації;

– різка зміна політичної ситуації в країні та світі;

– зміна регіонального та федерального законодавства і вплив цієї зміни на господарську діяльність підприємств. Держава повинна гарантувати безпеку громадянам і бізнесу. На практиці це відбувається не завжди: постійно змінюється податкова і кредитна політика, не завжди проводиться достатня боротьба з фінансовими злочинами щодо підприємців;

– надзвичайні ситуації природного характеру. Стихійні лиха, урагани, гради, пожежі;

– надзвичайні ситуації технічного характеру;

– недобросовісні клієнти. Вони можуть несвоєчасно сплачувати замовлений товар, відмовитися його забирати або повернути на наступний день;

– контрагенти. Є постачальники, які з якихось причин починають необгрунтовано завищувати ціни на товар, зривати терміни поставок, поставляти компанії сировину неналежної якості. Якщо постачальник у компанії один, загроза збільшується [6].

1.2 Аналіз нормативно-правової бази забезпечення інформаційної та кібербезпеки

Розглянемо основні нормативно-правові акти, що діють у сфері забезпечення інформаційної та кібербезпеки в Україні.

Наприклад, у НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу розглянуто поняття політики безпеки: «Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у

галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу» [7].

В НД ТЗІ 3.7-003-2005 наведено обгрунтування необхідності створення КСЗІ і основні етапи створення КСЗІ: «Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо

цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ.

Обстеження середовищ функціонування ІТС

Під час виконання цих робіт ІТС розглядається як організаційно-технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі - середовища функціонування ІТС).

Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт. Обстеження виконується, коли розроблена концепція ІТС (основні

принципи і підходи побудови), визначені основні завдання і характеристики ІТС, функціональних комплексів ІТС та існує варіант(и) їх реалізації.

При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

- можливі обмеження щодо використання засобів та ін. Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види (в термінах об’єктів КС) її представлення в ІТС. Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи КС (спостережність), яким вони повинні задовольняти. Аналіз технології обробки

інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС. Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об'єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об'єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв'язку, а також режим функціонування цих об'єктів. Порядок проведення обстеження повинен відповідати ДСТУ 3396.1, а в частині, що стосується захисту інформації від витоку технічними каналами, – НД ТЗІ 3.1-001. Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- наявність категорійованих приміщень, в яких мають розміщуватися компоненти ІТС;

- режим доступу до компонентів фізичного середовища ІТС;

- вплив чинників навколишнього середовища, захищеність від засобів технічної розвідки;

- наявність елементів комунікацій, систем життєзабезпечення і зв'язку, що мають вихід за межі контрольованої зони;

- наявність та технічні характеристики систем заземлення;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

- наявність проектної та експлуатаційної документації на компоненти фізичного середовища.

При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов'язків та рівня кваліфікації;

- повноважень користувачів щодо допуску до відомостей, які обробляються в ІТС, доступу до ІТС та її окремих компонентів;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС;

- наявності СЗІ в ІТС.

Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001. 6.1.2.9 За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001, НД ТЗІ 2.5-007, НД ТЗІ 2.5-008, НД ТЗІ 2.5-010 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002, НД ТЗІ 1.4-001 та НД ТЗІ 1.6-003. Модель загроз для інформації та модель порушника рекомендується 13оформляти у вигляді окремих документів (або поєднаних в один документ) Плану захисту.

Формування завдання на створення КСЗІ На цьому етапі:

- визначаються завдання захисту інформації в ІТС, мета створення КСЗІ, варіант вирішення задач захисту (відповідно до ДСТУ 3396.1), основні напрями забезпечення захисту (відповідно до п. 5.8);

- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту (наприклад, обмеження щодо використання засобів активного захисту від витоку інформації каналами ПЕМВН за рахунок використання засобів ЕОТ в захищеному виконанні тощо), інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

Здійснюється оформлення звіту про виконання робіт цієї стадії та оформлення заявки на розробку КСЗІ (тактико-технічного завдання на створення КСЗІ або іншого документу аналогічного змісту, що його замінює).»[8].

Законі України «Про інформацію» надається визначення поняттям «захист інформації» і «інформація». «Захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.» [9].

В постанові Кабінеті міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційний та інформаційно-телекомунікаційних системах» розкрито наступні терміни:

«Автентифікація – процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора.

Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається

системою.» Також у цьому Положенні висвітлено види інформації, що підлягають захисту:

«Відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі – відкрита інформація).

Конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації".

Службова інформація.

Інформація, яка становить державну або іншу передбачену законом таємницю (далі – таємна інформація).

Інформація, вимога щодо захисту якої встановлена законом.

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію

можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до службово інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.»[10].

В НД ТЗІ 1.1-002-00 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу розкрито поняття політики безпеки:

«Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.7

Політика безпеки інформації в АС є частиною загальної політики безпеки організації і може успадковувати, зокрема, положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації може бути індивідуальною і може залежати від технології обробки інформації, що реалізується, особливостей ОС, фізичного середовища і від багатьох інших чинників. Тим більше, одна й та ж сама АС може реалізовувати декілька різноманітних технологій обробки інформації. Тоді і політика безпеки інформації в такій АС буде складеною і її частини, що відповідають різним технологіям, можуть істотно відрізнятись.

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

Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована. Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із аписами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.» [11].

У стандарті ДСТУ ISO/IEC 27005:2015 наведено рекомендації для менеджменту ризиків інформаційної безпеки, що включають інформацію і менеджмент ризиків безпеки технологій телекомунікацій. Методи, описані в цьому стандарті, відповідають загальним поняттям, моделям і процесам, вказаним в ДСТУ ISO/IEC 27001:2015 [12].

1.3 Постановка задачі

Враховуючи актуальність проблеми з забезпечення інформаційної безпеки на підприємстві, аналізу динаміки розвитку загроз у світі протягом останніх років і актуальних загроз для малих підприємств необхідно забезпечити гідний рівень захищеності інформації. Проаналізувавши нормативно-правову базу, досягти необхідного рівня захищеності інформації можна шляхом створення КСЗІ.

Виходячи з нормативно-правових актів, під час створення і розробки КСЗІ, необхідно провести аналіз і описати:

- вид діяльності підприємства;
- фізичне середовища функціонування;
- інформаційну систему на підприємстві;
- побудувати модель порушника і модель загроз;
- виявити вразливості;
- розробити елементи політики безпеки інформації.

Висновок

У першому розділі кваліфікаційної роботи було проаналізовано темпи росту кіберзлочинності в світі, основні загрози кіберпростору. Також було наведено основні види внутрішніх і зовнішніх загроз для малих підприємств.

Було проведено аналіз нормативно-правової бази, за результатами чого було поставлено задачі для другої частини кваліфікаційної роботи.

ПРАКТИЧНА ЧАСТИНА

2.1 Загальні відомості про вид діяльності ТОВ «Інтайм»

Основним видом діяльності ТОВ «Інтайм» є оптово-роздрібний продаж комплектуючих до мобільних телефонів як в просторі Інтернет на власному веб-сайті, так і на території власного магазину.

Діяльність організації пов'язана з взаємодією як з юридичними, так і фізичними особами, надаючи їм відомості щодо наявного товару в магазині.

На підприємстві циркулює інформація, що містить комерційну таємницю і персональні дані.

Підприємство функціонує 7 днів на тиждень, без перерв з 10.00 до 20.00. Вихід на обідню перерву здійснюється через дозвіл керівництва на території приміщення. Штат співробітників підприємства на постійній основі налічує 9 співробітників, з них директор – 1 особа, менеджера – 3 особи, продавці – 3 особи, охоронці – 2 особи. Також за необхідністю підприємство користується послугами найманого системного адміністратора, що оновлює ПЗ та налаштовує апаратну складову ПК.

2.2 Обґрунтування необхідності в створенні КСЗІ

Виходячи з положень чинного законодавства України щодо захисту інформації, необхідно обмежити доступ до деяких видів інформації. Директором підприємства було видано акт про категоріювання об'єкта (див. ДОДАТОК Е). Для цього, за розпорядженням власника інформації (див. ДОДАТОК Ж), 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 цієї інформації. Рішення щодо створення і впровадження КСЗІ покладається на власника системи, оскільки він несе повну відповідальність за її збереження.

2.3 Обстеження фізичного середовища ОІД

Підприємство розташовано на першому поверсі одноповерхового офісного будинку за адресою Маршала Малиновського 2.

Стіни будівлі виконані з білої цегли, дах плоский. Фундамент виконаний з бетону. Вікна металопластикові. Є 1 вхідні металопластикові двері з двома замками зі звичайними ключами. До будівлі підведено електро- та водопостачання під землею.

Будівля поділена на багато офісних, торгових та складських приміщень з системою коридорів та переходів в середині

Навколо будівлі розташовані місця для паркування, територія охороняється службою охорони.

Контрольована зона обмежена з північно-західної, північної та північно-східної сторін цегляною стіною, за якою інші офісні, складські та торгові приміщення, з інших сторін обмежена стінами будівлі.

У комплексу власне заземлення, схема зображена на рис. 2.1.

Розподільний щит встановлено зі східної сторони, у деяких приміщеннях встановлені власні щитові.

Заключено договір з охоронною службою – у разі необхідності (виклик за телефоном), приїжджа силова бригада.

Режим на КЗ у робочій час контролює штатний охоронець підприємства котрий у разі необхідності викликає службу охорони шляхом дзвінка на гарячу лінію.

У неробочий час режим забезпечується охоронцем офісного комплексу, сигналізацією на підприємстві (сигналізація на відкриття дверей, вікон та на об’єм, котрі подають сигнал до охоронної фірми у разі спрацювання).

Найближчі будівлі до офісного центру (див. табл. 2.1):

- Магазин №2 – 20м

- Автомийка №3 – 20м
- Магазин №6 – 50м
- Магазин №7 – 50м

До будівлі під’єднані наступні комунікації:

- лінії під’єднання до інтернет-провайдеру представлена оптоволоконним кабелем, прокладеним поза меж КЗ надземним шляхом до обладнання провайдера у сусідній будівлі.
- лінія електропостачання загальна на весь комплекс і виходить в інші приміщення будівлі, трансформаторна підстанція знаходиться поза межами будівлі, під’єднується наземно, у будівлі власний електричний щиток, що знаходиться у спеціальному приміщенні.
- водопровід та каналізація загальні для комплексу від районної водонапірної станції, проходять у межах КЗ та виходять в інші приміщення. У разі необхідності, у будівлі встановлені крани для обмеження доступу води.

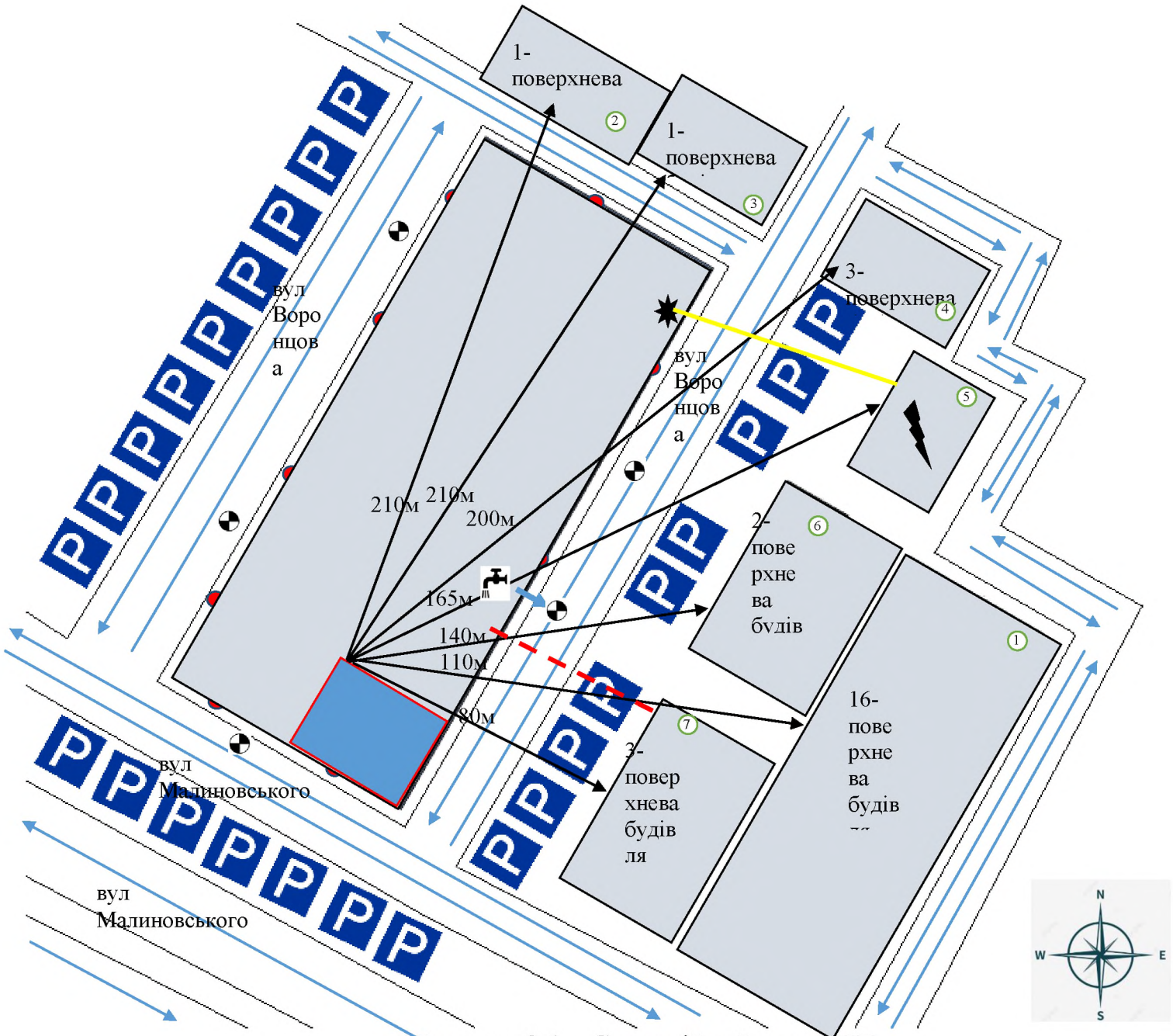


Рисунок 2.1 – Ситуаційний план ОІД

Умовні позначення

- Місце для паркування
- Номер будинку
- Вхідні двері
- Напрям руху
- Трансформаторна підстанція ТпТ-112
- Лінія електромережі
- Лінія мережі водопостачання
- Лінія мережі Інтернет
- Межа КЗ
- Територія ОІД
- Межа будівлі
- «Кранове» приміщення
- Каналізаційний люк
- Електричний щиток у приміщенні

Таблиця 2.1 – Характеристика будівель та споруд.

№	Найменування	Адреса	Кіл-сть поверхів	Мінімальна відстань до ОІД, м
1	Житловий будинок	Малиновського, 16	16	85
2	Магазин	Малиновського, 8	1	180
3	Автомийка	Малиновського, 6	1	175
4	Аптека	Малиновського, 5	3	191
5	Трансформаторна підстанція	Малиновського	1	172
6	Магазин	Малиновського, 8	2	67
7	Магазин	Малиновського, 8а	3	53

Приміщення, де циркулює інформація з обмеженим доступом розташоване на першому поверсі одноповерхневого будинку з офісними, торговими та складськими приміщеннями. У приміщенні використані одностворчасті металопластикові вікна.

Загальна площа 102м2, товщина несучих стін з білої цегли-60см, товщина перегородок 20см, висота стелі 3м.

Площа кабінету директора складає 8м2, площа кабінету менеджерів 17м2, площа торгової зали складає 58м2, площа кімнати охорони складає 12м2, площа туалету складає 5м2.

Електроживлення до освітлення підведено кабелями ВВГ, саме освітлення виконано на світлодіодних лампах. Перемикачі освітлення можуть знаходитись у двох становищах. Розетки із заземленням, при підключенні пристроїв використовується мережевий фільтр (див. рис. 2.2).

Вентиляційна система представлена приточною системою з алюмінію (див.рис 2.3).

Об’єкт знаходиться під охороною, встановлено централізовану систему охоронно-пожежної сигналізації, котра передає сигнал тривоги до диспетчерів

служби охорони та висилає СМС-повідомлення на телефон директора (див. рис. 2.4).

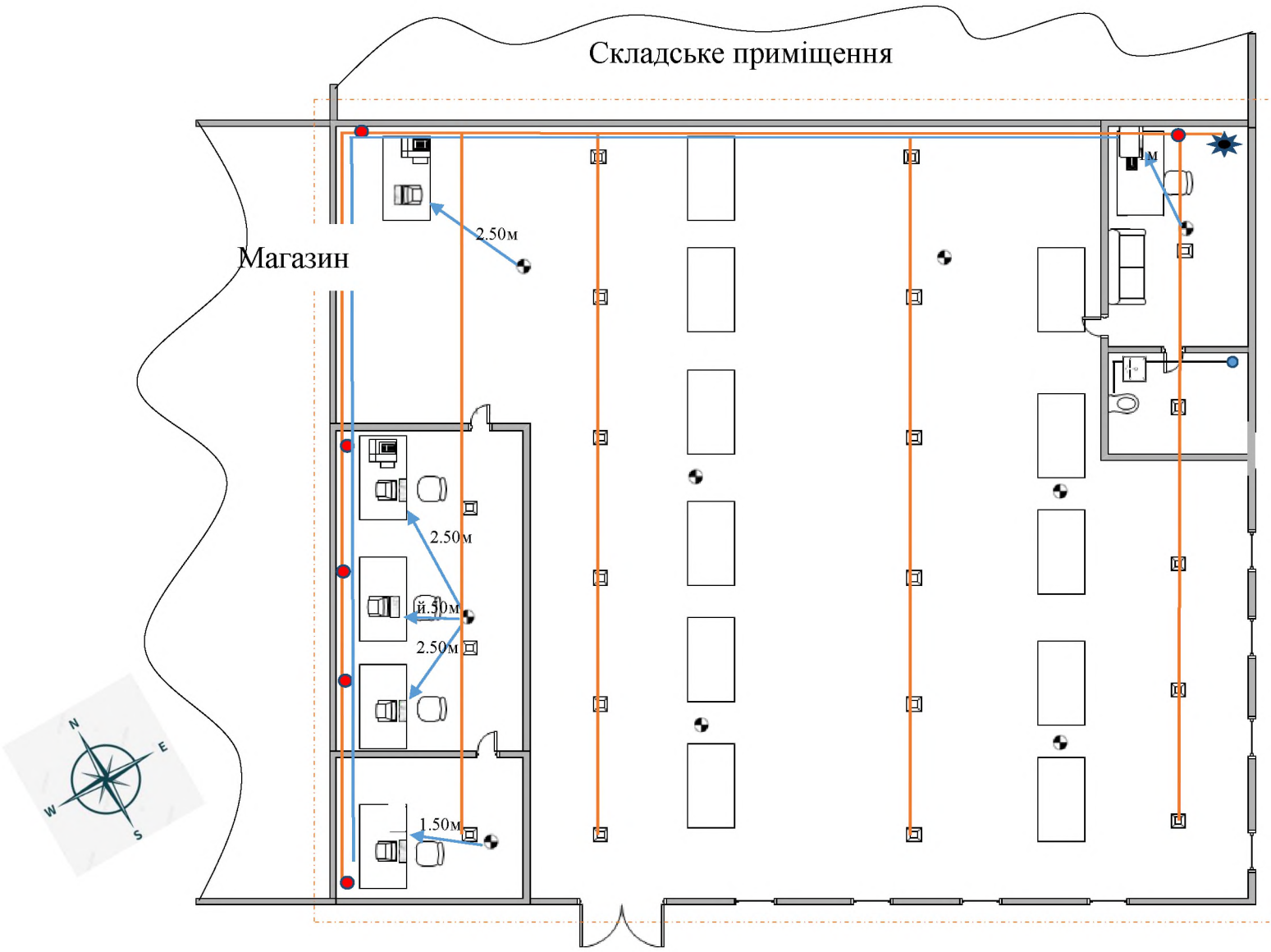


Рисунок 2.2 – Генеральний план ОІД

Умовні позначення

Димовий сповіщувач

Лінія мережі електроживлення

Водопровідний стояк

Монітор та системний блок

Розетка

Лінія мережі Інтернет

Водопровідна труба

Маршрутизатор і точка доступу

Електричний щит

Межа зони ОІД і КЗ

Елемент освітлення

Принтер

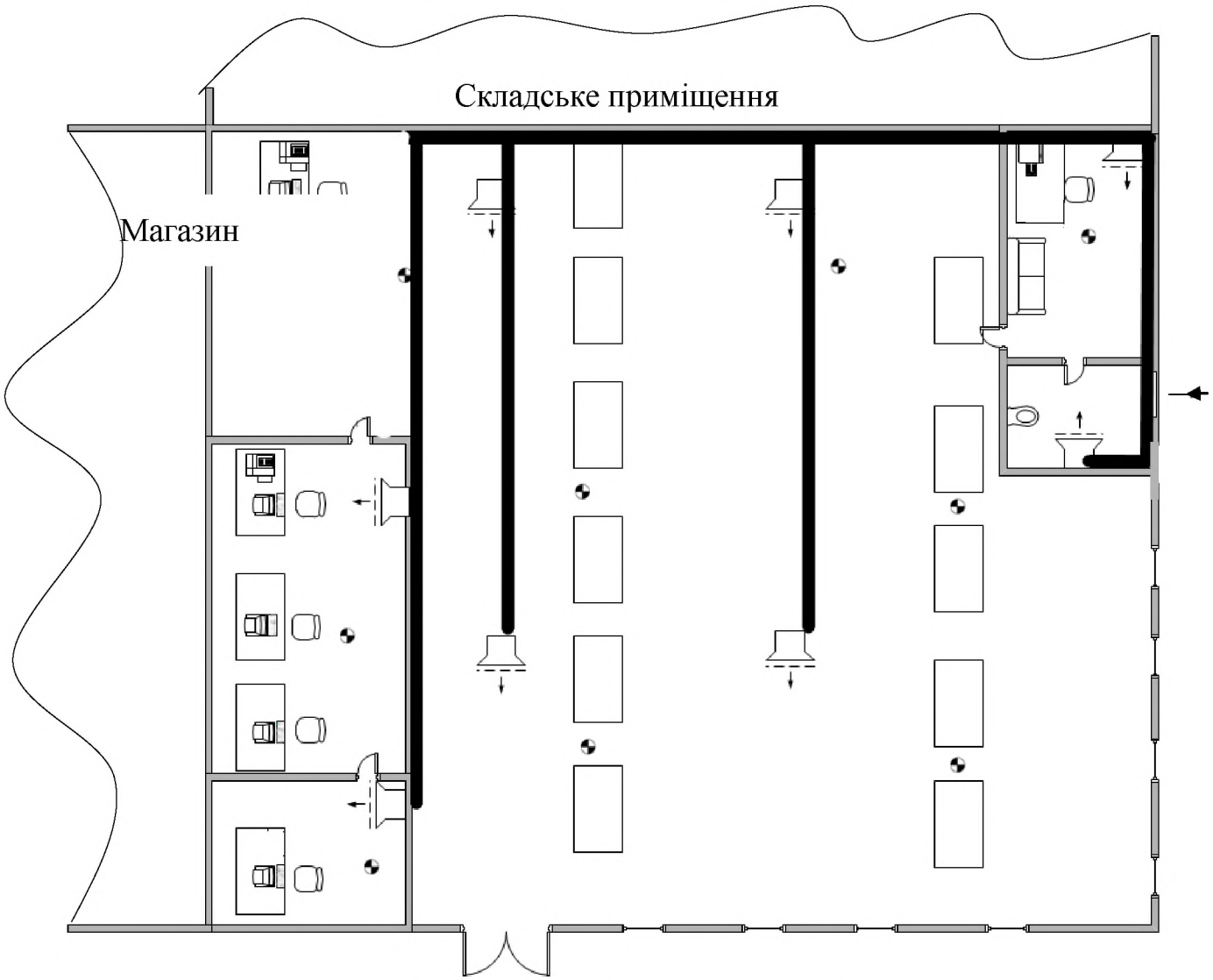
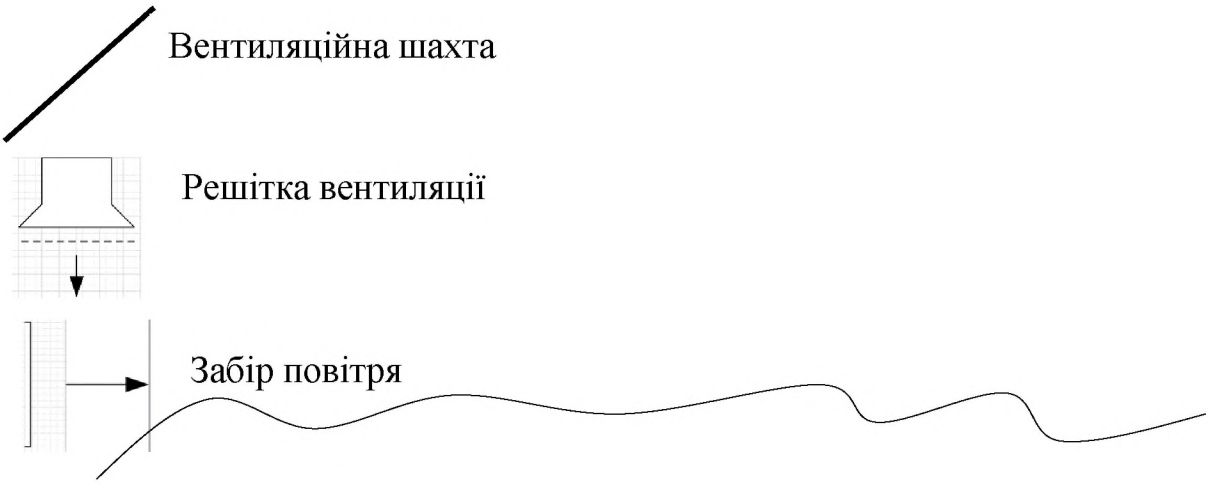


Рисунок 2.3 – Схема вентиляції



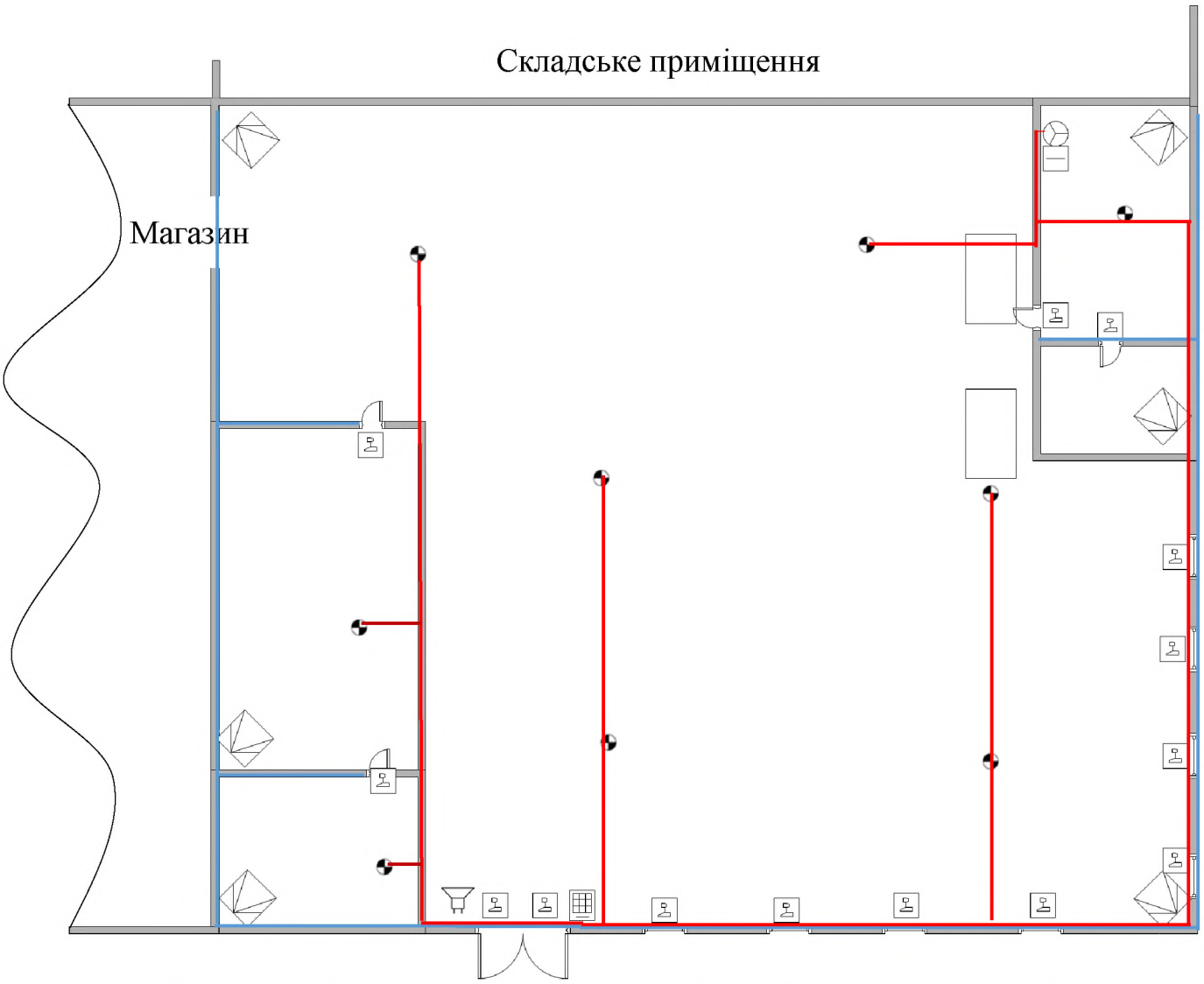


Рисунок 2.4 – схема протипожежної та аварійної системи охорони

1.1 Обстеження обчислювальної системи

Всі миші та клавіатури до системних блоків підключаються через роз'єм USB.

Локальна мережа представлена через кручену пару, вона підключається до роутера, звідки розводиться до комп'ютерів та під'єднується через роз'єм RJ-45.

Роутер являє собою також точку доступу Wi-Fi з обмеженим доступом (тільки для працівників підприємства, знаходиться під паролем) для вільної можливості виходу у мережу у разі необхідності.

Під'єднатися до принтерів можливо за допомогою Wi-Fi.

Лінія сигналізації проведена за допомогою дротів СКВВ.

За необхідності підприємство замовляє послуги системного адміністратора для профілактики актуальності системи (перевірка оновлень, перевірка обладнання). Структурну схему мережі зображено на рисунку 2.5. Перелік основних технічних засобів наведено у таблиці 2.2. У таблиці 2.3 наведено перелік ДТЗС.

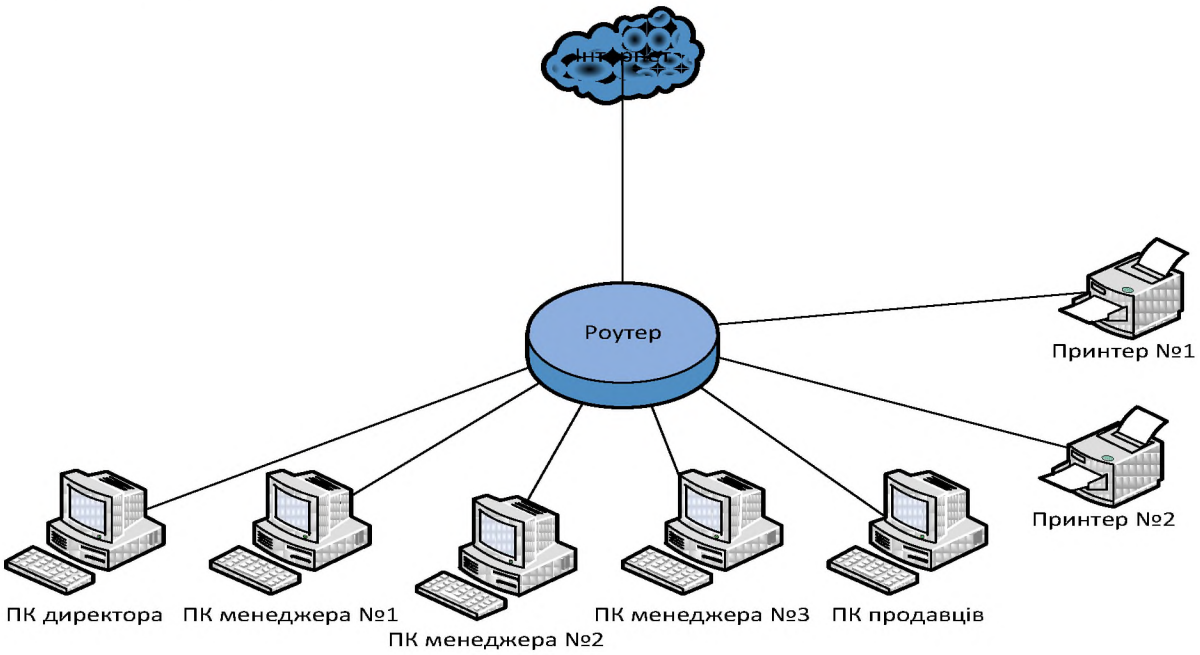


Рисунок 2.5 – Структурна схема мережі

Таблиця 2.2 – Опис основних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
1	Системний блок PC-1	Lenovo	V570c	ZXF958471	Під столом	1,5	1,3
2	Системний блок PC-2	Apple	Air	ZXF958472	Під столом	1,5	0,9
3	Системний блок PC-3	Asus	VivoBook	ZXF958473	Під столом	1,5	0,9
4	Системний блок PC-4	Xiaomi	RedmiBook 14	ZXF958474	Під столом	2,5	0,8
5	Системний блок PC-5	Expert PC	Ultimate	ZXF958475	Під столом	1,5	1,6
6	Монітор 1	LG	22MK430H-B	FF1234561	На столі	1,4	1,3
7	Монітор 2			FF1234562	На столі	1,3	0,9
8	Монітор 3			FF1234563	На столі	1,5	0,9
9	Монітор 4			FF1234564	На столі	2,3	0,8
10	Монітор 5			FF1234565	На столі	1,4	1,6
11	Клавіатура 1	4a-tech	A4Tech KR-83 PS/2	KBL158741	На столі	1,3	1,3
12	Клавіатура 1			KBL158742	На столі	1,5	0,9
13	Клавіатура 1			KBL158743	На столі	1,4	0,9
14	Клавіатура 1			KBL158744	На столі	2,4	0,8
15	Клавіатура 1			KBL158745	На столі	1,3	1,6
17	Принтер	XPrint	xp-q200	MF847162	На столі	1,5	1,9
18	Принтер	XPrint	xp-q200	MF847163	На столі	1,5	1,9
19	Маршрутизатор	D-link	D-Link DIR-825/AC/G	DLD798941	На столі	4	1,4

Таблиця 2.3 – Опис допоміжних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань	Мінімальна відстань

						від елем. до кордонів КЗ, м	до ОТЗ, м
1	Навісна Led лампа освітлення	TL-Office	15 L600 O 4K	KIB465661 KIB465662 KIB465663 KIB465664 KIB465665 KIB465666 KIB465667 KIB465668 KIB465669 KIB465670 KIB465671 KIB465672 KIB465673	На стелі	2 2,1 2,3 2,3 1,7 3 5 5 3 2 2 2 2	1 3 2 3 5 4 3 5 7 0,9 1 4 7
2	Маніпулятор миша 1	4a-tech	OP-720	MAT41575	На столі	1,4	0,2
3	Маніпулятор миша 2			MAT41576	На столі	1,3	0,2
4	Маніпулятор миша 3			MAT41577	На столі	1,5	0,2
5	Маніпулятор миша 4			MAT41578	На столі	2,3	0,2
6	Маніпулятор миша 5			MAT41579	На столі	1,4	0,2
7	Маніпулятор миша 5	4a-tech	OP-720	MAT41580	На столі	1,4	0,2
19	Телефон 1	Apple	IPhone x	C4C4G6S6F1	переносний	-	-
20	Телефон 2	Huawei	P10	1Z2X3C6V5B	переносний	-	-
21	Телефон 3	Xiaomi	Note 10	A4S5D6FG48	переносний	-	-
22	Телефон 4	Samsung	S10e	T9G6B3V2F5	переносний	-	-
23	Телефон 5	Honor	X10	D2C5D6F335	переносний	-	-

Продовження таблиці 2.3

24	Дунай-DAN-DKN	ППКОП	32015623065120	Торговий зал	0,5	2
25	LD-95	Сирена світлошумова	48646868468486	Торговий зал	0	3
26	ЭСМК-8	Магнітоконтактний	Б/Н	Вхідні двері	0,3	3
27	ЭСМК-4	Магнітоконтактний	Б/Н	Каб. Директора\двері	0,3 0,3	2 2
				Торговий зал\двері і вікна	0,3 0,3 0,3 0,3 0,3 0,3 0,3 0,3	2 4 6 8 10 12 8 6
				Кабінет охорони\двері	2	5
28	АСТРА-621	Комбінований сповіщувач руху та розбиття скла	Б/Н	Торговий зал	2 2	1,3 12
				Кабінет менеджерів	2	1.5
				Кабінет Директора	2	1,5
				Кабінет охорони	2	4
				Санвузол	2	8
29	Артон СПД Кадет	Датчики диму	48646868468487 48646868468489 48646868468480 48646868468481 48646868468482 48646868468483	Склад	5 6 7 8 6 5	5 5 7 10 12 5
			48646868468484	Директор	2	0,9
					2	0,9
			48646868468485	Менеджера	1,5	5
			48646868468486	Охорона	2	0,8
30	SPR-1	Кнопка пожежі	48646868612848	Кабінет охорони	0,3	2,5
31	ИРТС	Кнопка тривоги	48646862346848	Кабінет охорони	1,5	1
32	K-LED16	Клавіатура	48646868468485	Торговий зал	0,3	2,5

Таблиця 2.4 – Характеристики ОТЗ

№	Найменування	Специфікація	Користувач
1	ПК Lenovo V580c	Intel Core i3-2328M (2.2 ГГц) (Serial: 12FGH890Q1) / RAM Kingston 4 ГБ / HDD Western Digital 500 ГБ (Serial: AS789YU99) / Intel HD Graphics 3000	Директор
2	ПК Apple MacBook Air	Intel Core i3 (1.1 - 3.2 ГГц) (Serial: AS9876U99) / RAM 8 ГБ / SSD Western Digital 256 ГБ (Serial: AS789VB12) / Intel Iris Plus Graphics	Менеджер 1
3	ПК Asus VivoBook 15	Intel Core i3-6100U (2.3 ГГц) (Serial: AS78989HG) / RAM 8 ГБ / HDD Western Digital 1 ТБ(Serial: AS789YU99) / Intel HD Graphics 520	Менеджер 2
4	ПК Xiaomi RedmiBook 14	AMD Ryzen 7 3700U (2.3 - 4.0 ГГц) (Serial: AS789QW19) / RAM 16 ГБ / SSD Western Digital 512 ГБ (Serial: AS789YU87)/ AMD Radeon RX Vega 10 Graphics	Менеджер 3
5	ПК Expert PC Ultimate	Intel Core i3-6100U (2.3 ГГц) (Serial: AS789YUAS) / RAM 8 ГБ / HDD Western Digital 1 ТБ(Serial: AS789YU17) / Intel HD Graphics 520	Продавці

Програмне забезпечення, що використовується на підприємстві, наведено у таблиці 2.5.

Таблиця 2.5 – Перелік ПЗ в ІТС

№	Найменування ПО	Пристрій	Тип ПЗ	Строк закінчення ліцензії
1	Windows 10 Pro 1909 Build 13363,476	PC-1	Системне	Довічна
2	Windows 10 Pro 1909 Build 18363,446	PC-2	Системне	Довічна
3	Windows 10 Pro 1909 Build 12363,987	PC-3	Системне	Довічна
4	Windows 10 Pro 1909 Build 13512,109	PC-4	Системне	Довічна

Продовження таблиці 2.5

№	Найменування ПО	Пристрій	Тип ПЗ	Строк закінчення ліцензії
5	Windows 10 Pro 1909 Build 13363,781	PC-5	Системне	Довічна
6	1С Бухгалтерія 6.0	PC-1	Прикладне	19.02.2022
7	R-Keeper v7	Всі ПК	Прикладне	03.10.2024
8	Google Chrome 89.0.4389.114	Всі ПК	Прикладне	Довічна
9	Telegram Desktop 2.12.027	Всі ПК	Прикладне	Не потребує ліцензії
10	Microsoft Office 2019 14026.20246	Всі ПК	Прикладне	Довічна

2.4 Опис інформаційного середовища підприємства

Поточні замовлення компанія отримує від клієнтів напряму, продавці заносять цю інформацію до інформаційної системи R-Keeper, в разі необхідності, цю інформацію можна роздрукувати на принтерах. Далі продавець формує вантаж згідно із замовленням, передає клієнту замовлення. Інформація про завершення замовлення заносить в R-Keeper, формується запис про відпрацьоване замовлення.

Дані попередніх замовлень компанія отримує від клієнтів через засоби електронної скриньки, зберігається на комп'ютерах менеджерів в інформаційній системі R-Keeper , в разі необхідності потрібна інформація друкується на принтерах, та передається продавцям для подальшого використання (збір, обробка, передача та оплата замовлення та інші), після опрацювання замовлення паперові носії за регламентом знищуються, залишається лише запис в інформаційній системі R-Keeper про відпрацьоване замовлення.

У випадку роздрібного замовлення продавець приймає замовлення в покупця, заносячи замовлення в інформаційну систему R-Keeper. Це замовлення заноситься в особисту справу клієнта у випадку наявності клубної картки для накопичення бонусів. В свою чергу система відповідає, чи є в необхідній кількості товар, його поточну ціну і т.п. Після видачи замовлення, до системи заноситься інформація про оплату.

У випадку оптового замовлення продавець або менеджер приймає замовлення, заносячи його в систему. Система дає інформацію про наявність товарів на складі, поточну ціну, дату можливої доставки і тд. Після підтвердження і оплати замовлення в системі створюється нагадування про оптове замовлення, котре активується в день виконання замовлення.

Особисті справи співробітників зберігаються у паперовому вигляді у шухляді стола в кабінеті директора. Цю інформацію надає співробітник самостійно при працевлаштуванні, тобто в приміщенні є всього по одній копії особистої справи кожного працівника. При звільнені співробітника документи передаються звільненому співробітнику після трьох місяців з моменту звільнення, якщо співробітник їх не забрав, директор знищує їх самостійно (кожний паперовий носій рветься на 8 частин).

Інформація про клієнтів зберігається в інформаційній системі R-Keeper, доступ до інформації може отримати будь-який зареєстрований адміністратором (директором) користувач. Створювати запис про нового клієнта може будь-який зареєстрований користувач. Згідно з новими замовленнями, інформація про клієнта автоматично оновлюється системою. Ідентифікатором клієнта є його мобільний номер телефону.

Бухгалтерські звіти зберігаються і формуються на комп'ютері директора в системі 1С. Після формування, дана інформація передається до податкової служби засобами Інтернет. Юридична інформація, необхідна для функціонування підприємства зберігається у паперовому вигляді у столі директора.

Облікова інформація (залишки товару, поточна ціна) заноситься в систему віддаленим співробітником іншого підрозділу, зберігається в інформаційній системі R-Keeper, доступ до цієї інформації має кожний зареєстрований користувач, інформація оновлюється автоматично згідно з виконаними замовленнями.

Робочий графік формується менеджером підприємства на власному ПК. Після формування графіку, він розповсюджується кожному співробітнику за допомогою функціоналу Telegram Desktop.

Зарплатна відомість формується на основі даних про відпрацьовані замовлення на ПК директора.

Матрицю доступу до інформації користувачами наведено у таблиці 2.6.

Таблиця 2.6 – Матриця доступу до інформації

Вид інформації	Створення	Перегляд	Редагування	Видалення	Друк	Місце зберігання, доступ з іншого пристрою
Дані попередніх замовлень	Директор, менеджера	Директор, менеджера	Директор, менеджера	Директор, менеджера	Директор, менеджера	Віддалено, так
Поточні замовлення	Всі користувачі системи	Всі користувачі системи	Директор, Менеджера та автор	Директор, Менеджера та автор	Директор, Менеджера та автор	Віддалено, так
Відпрацьоване замовлення	Автоматично	Директор, менеджера	-	-	Директор, менеджера	Віддалено, так
Особисті справи співробітників	Директор	Директор	-	Директор	-	Кабінет директора, ні
Запис про клієнта	Всі користувачі системи	Всі користувачі системи	Директор, Менеджера або автоматично	Директор	Всі користувачі системи	Віддалено, так
Бухгалтерські звіти	Директор	Директор	Директор	Директор	Директор	PC1, ні
Облікова інформація	Віддалений користувач	Всі користувачі системи	Віддалений користувач	-	Всі користувачі системи	Віддалено, так

Продовження таблиці 2.6

Вид інформації	Створення	Перегляд	Редагування	Видалення	Друк	Місце зберігання, доступ з іншого пристрою
Робочий графік	Директор, менеджера	Всі користувачі системи	Директор, менеджера	Директор, менеджера	Всі користувачі системи	PC2, так
Зарплатна відомість	Директор	Директор	Директор	Директор	Директор	PC1, ні

Рівні конфіденційності, цілісності і доступності інформації, що циркулює на підприємстві, наведено у таблиці 2.7.

Таблиця 2.7 Рівні конфіденційності, цілісності та доступності

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Дані попередніх замовлень	К1	Ц4	Д2
Поточні замовлення	К1	Ц3	Д4
Відпрацьоване замовлення	К1	Ц1	Д1
Особисті справи співробітників	К3	Ц1	Д1
Запис про клієнта	К4	Ц4	Д4
Бухгалтерські звіти	К1	Ц3	Д2
Облікова інформація	К4	Ц2	Д3
Робочий графік	К0	Ц2	Д1
Зарплатна відомість	К1	Ц1	Д1

.

Рівні конфіденційності:

– К0 – рівень конфіденційності інформації, при якому можна знехтувати

збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

– К1 – рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К2 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К4 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

– Ц0– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц1 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц2 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц3 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц4 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д0– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д1 – рівень доступності інформації, при якому компанія зазнає

незначних збитків у разі втрати доступності інформації;

– Д2 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

– Д3 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

– Д4 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Інформаційні потоки на підприємстві зображено на рисунку 2.6.

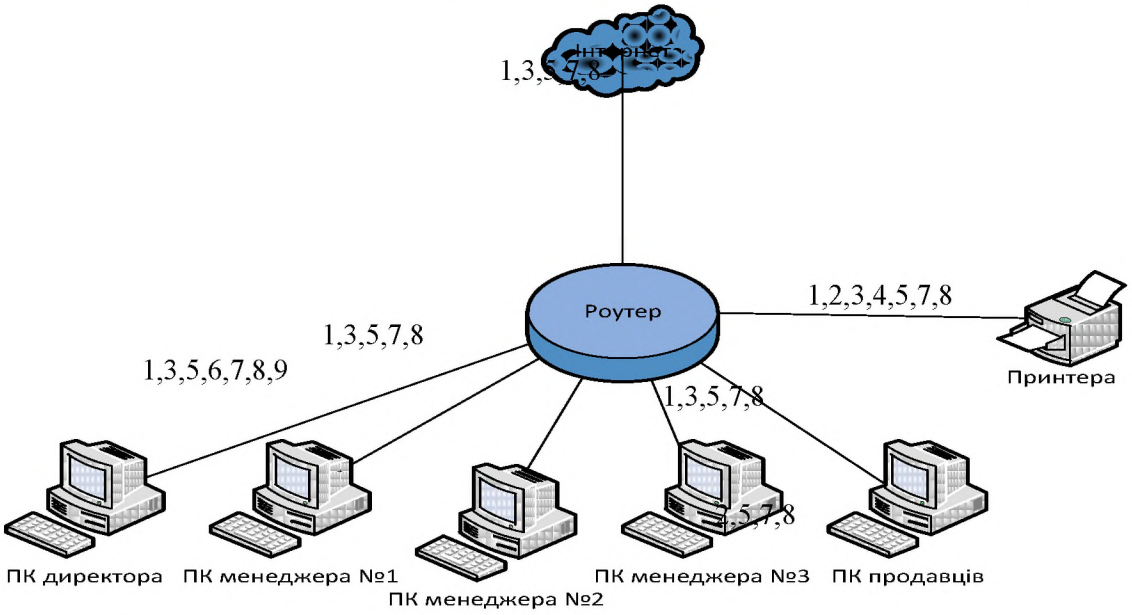


Рисунок 2.6 – Інформаційні потоки на підприємстві

2.5 Побудова моделі порушника

Виходячи з НД ТЗІ 1.1-003-99, модель порушника – абстрактний опис можливих дій порушника на основі його повноважень, знань, теоретичних і практичних можливостей. Порушників можна поділити на внутрішніх – співробітники підприємства, користувачі системи, і на зовнішніх – сторонні особи.

В моделі порушника визначаються:

– можлива мета порушника та її класифікація за ступенями небезпечності для системи;

– припущення про кваліфікацію порушника;
– категорії осіб, що можуть бути порушниками;
– припущення про характер дій порушника.

Метою порушника може бути:
– отримання необхідної інформації;
– отримання можливості внесення змін в інформаційні потоки;
– нанесення збитків.

Модель порушника наведено у таблиці 2.8.

Таблиця 2.8 Модель порушника

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Внутрішні порушники						
Директор	М2	К3	З2	Ч3	Д2	12
Менеджер 1	М3	К2	З1	Ч2	Д2	10
Менеджер 2	М3	К2	З1	Ч2	Д2	10
Менеджер 3	М3	К2	З1	Ч2	Д2	10
Продавець 1	М3	К1	З1	Ч1	Д2	8

Продовження таблиці 2.8

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Продавець 2	М3	К1	З1	Ч1	Д2	8
Продавець 3	М3	К1	З1	Ч1	Д2	8
Системний адміністратор	М3	К3	З3	Ч4	Д4	17
Віддалений користувач	М1	К2	З2	Ч2	Д2	9
Зовнішні порушники						
Найманий персонал	М3	К1	З1	Ч1	Д1	7
Хакери	М3	К3	З3	Ч4	Д3	16
Колишні робітники	М2	К1	З2	Ч2	Д3	10

Конкуренти	М3	К1	З3	Ч1	Д3	11

Мотиви порушень:

– М1 – безвідповідальність;

– М2 – самоствердження;

– М3 – корисливий інтерес.

Рівні обізнаності щодо функціонування ІТС:

– К1 – володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС;

– К2 – володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування;

– К3 – знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості.

Рівні можливостей щодо подолання системи захисту

– З1 – може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях.

– З2 – використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації.

– З3 – використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації.

Рівні можливостей за часом дії:

– Ч1 – під час повної бездіяльності ІТС з метою відновлення та ремонту;

– Ч2 – під час зупинки компонентів ІТС з метою технічного обслуговування та модернізації;

– Ч3 – під час функціонування ІТС (або компонентів системи);

– Ч4 – як у процесі функціонування ІТС, так і під час зупинки компонентів системи.

Рівні можливостей за місцем дії:

– Д1 – усередині приміщень, але без доступу до технічних засобів ІТС;

– Д2 – з робочих місць користувачів (операторів) ІТС;

– Д3 – дистанційно;

– Д4 – з доступом у зону керування засобами забезпечення безпеки ІТС.

Виходячи з даних таблиці 2.8, найбільшу небезпеку зсередини підприємства становлять системний адміністратор та директор, оскільки вони мають найвищий рівень обізнаності щодо ІТС та мають доступ до керування засобами забезпечення механізмів безпеки, володіють доступом до всієї інформації, що циркулює на підприємстві. Серед зовнішніх порушників найбільшу небезпеку становлять хакери, так як вони мають високий рівень кваліфікації, реалізувати загрозу можуть без прямого доступу до об'єкту.

2.6 Модель загроз

Виходячи з НД ТЗІ 1.1-003-99, модель загроз – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз. Загрози інформаційним ресурсам можна розділити на технічні, антропогенні або стихійні загрози, що можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, що зберігається в ній.

Розглянемо перелік загроз і їх вплив на доступність, цілісність і конфіденційність інформації (див. табл. 2.9) . Оскільки ОІД знаходиться поза зоною з активними природними катаклізмами, стихійні загрози не розглядаємо. Коефіцієнт небезпеки загроз розраховуємо за формулою (2.1):

$$К_{заг} = \frac{К1 * К2 * К3}{125} \quad (2.1)$$

де:

– К1, К2 і К3 – шкали оцінки загроз;

– 125 – максимальний добуток шкал загроз.

Таблиця 2.9 – Перелік загроз

Потенційні загрози для інформації в ІТС	Ризики для			К1	К2	К3	$К_{заг}$
	К	Ц	Д				
Загрози об'єктивної природи							
Збої та відмови системи електроживлення			+	2	2	2	0,64
Збої та відмови інтернет мережі			+	2	2	2	0,64
Загрози суб'єктивної природи							
Несанкціоноване підключення до технічних засобів	+	+		2	2	3	0,096
Несанкціоноване підключення до каналів зв'язку	+	+		2	1	1	0,016
Читання даних, що виводяться на екран	+			4	4	3	0,384

Продовження таблиці 2.9

Потенційні загрози для інформації в ІТС	Ризики для			К1	К2	К3	$К_{заг}$
	К	Ц	Д				
Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН	+			2	1	2	0,032
Несанкціонований перегляд інформації на паперових носіях за рахунок візуально-оптичного каналу	+			4	4	3	0,384
Порушення нормальних режимів роботи							
Розголошення засобів розмежування доступу (паролів)	+	+	+	4	3	4	0,384
Несанкціонована передача/розголошення ІзОД	+			2	2	2	0,064
Модифікація компонентів програмного та інформаційного забезпечення		+	+	1	2	2	0,032
Пошкодження носіїв інформації		+	+	4	4	4	0,512
Вхід у систему недопущених осіб (подолання систем захисту)	+	+	+	2	2	2	0,64

Помилки персоналу							
Порушення технології обробки, введення та виведення інформації		+	+	2	2	2	0,064
Отримання сторонньою особою інформації у персоналу ІТС	+			1	2	2	0,032
Пошкодження носіїв персоналом ІТС		+	+	3	2	2	0,096
Ураження шкідливим програмним забезпеченням	+	+	+	5	4	3	0,512

Можливість виникнення джерела (К1) – визначає ступінь доступності до об’єкта, що захищається (для антропогенних джерел), віддаленість від об'єкта, що захищається (для техногенних джерел)

Готовність джерела (К2) – визначає ступінь кваліфікації і привабливість здійснення діянь із боку джерела загрози (для антропогенних джерел), або наявність необхідних умов (для техногенних джерел).

Фатальність (К3) – визначає ступінь непереборності наслідків реалізації загрози. Кожен показник оцінюється експертно-аналітичним методом за п'ятибальною системою. Причому, 1 відповідає мінімальному обсягу впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальному.

2.7 Перелік вразливостей на підприємстві

Для ІТС можуть бути характерними наступні вразливості:

Техногенні:

– перебої на трансформаторній підстанції. Оскільки на об’єкті не використовуються джерела безперебійного живлення, в результаті скачку напруги можуть вийти з ладу робочі комп’ютери, що призведе до порушення доступності інформації;

– відсутній додатковий провайдер. У разі обриву неможливо отримати облікову інформацію, що призведе до порушення доступності.

Антропогенні:

– запуск стороннього ПЗ працівниками, уразливість в відсутності контролю за запуском стороннього ПЗ користувачами системи. Можливість зараження ПК вірусами, в результаті втрата конфіденційності, цілісності;

– використання зовнішніх носіїв працівниками. Уразливість в відсутності контролю за використанням зовнішніх носіїв, як наслідок, можливий імпорт та експорт файлів, можливість заразити ПК вірусами;

– перехід по стороннім посиланням в мережі Інтернет працівниками. Уразливість – відсутність інструктажу правил поведінки в Інтернеті для працівників, як наслідок, можлива втрата конфіденційності і доступності;

найманий системний адміністратор може встановлювати стороннє ПЗ на всі ПК працівників, повністю відсутній контроль за діями системного адміністратору, може призвести до втрати цілісності, доступності та конфіденційності.

2.8 Профіль захищеності

Згідно з НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

«Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.»[12].

АС відносимо до класу 3, оскільки система являє собою розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

За результатами аналізу загроз і вразливостей в ІТС підприємства було обрано наступний профіль захищеності системи:

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

«Базова довірча конфіденційність (КД-2). 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. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

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-1. Мінімальна 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.

Мінімальна довірча цілісність (ЦД-1). На даному рівні користувач, доменуякого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

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.

ЦВ-1: Мінімальна 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.

ДР-1. Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процесора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе

повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів.

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.

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 повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

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. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. 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-1. Виділення адміністратора. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

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.

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. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

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.»[14].

2.9 Розробка політики безпеки інформації

Виходячи із аналізу загроз у таблиці 2.9, необхідно розробити елементи політики безпеки інформації, що зможуть знизити рівень впливу тих загроз, що мають найбільший степінь небезпечності, а саме:

- читання даних, що виводяться на екран;
- несанкціонований перегляд інформації на паперових носіях за рахунок візуально-оптичного каналу;
- пошкодження носіїв інформації;
- ураження шкідливим програмним забезпеченням.

Виходячи з переліку найнебезпечніших загроз, розроблено політики безпеки інформації.

2.9.1 Політика безпеки «чистого столу»

Політика «чистого столу» повинна гарантувати, що всі паперові документи, що можуть містити ІзОД, вилучаються з візуальної видимості. Також умовами даної політики передбачено вилучення візуального контакту з

моніторами під час відсутності працівника на робочому місці.

Метою політики є встановлення вимог щодо правил зберігання паперових носіїв під час їхнього використання і збереження у недоступності для користувачів, що не мають доступ до інформації. Ця політика поширюється на всіх працівників підприємства.

Інструкція політики:

Співробітники зобов'язані гарантувати, що вся ІзОД буде захищена від стороннього доступу на робочому місці протягом робочого дня.

У випадку відсутності співробітника на робочому місці, ноутбук має бути заблокованим.

Наприкінці робочого дня всі ноутбуки підприємства має бути вимкнено.

Паперові носії інформації, що містять ІзОД, наприкінці робочого дня або у разі відсутності працівника на робочому місці, необхідно прибрати з поверхні робочого столу до ящику і закрити його на ключ.

Ключи від ящиків робочих столів забороняється залишати без нагляду і передавати будь-кому.

Забороняється занотовувати паролі на паперових носіях, зберігати їх на ноутбуках.

У випадку відправки документів, що містять ІзОД на друк, необхідно одразу після роздрукування вилучити з принтеру.

У випадку знищення паперових носіїв з ІзОД, носій необхідно знищити шляхом розривання кожного листу на 10 частин.

Знімні носії інформації необхідно зберігати у замкнених ящиках робочих столів.

Працівник, що порушив правила даної політики, зазнає дисциплінарного покарання у вигляді матеріального штрафу або звільнення, в залежності від серйозності наслідків.

2.9.2 Політика безпеки інформації з резервного копіювання

Метою політики є встановлення порядку резервного копіювання для подальшого відновлення працездатності АС при повній або частковій втраті інформації, викликаної збоєм чи відмовою апаратного або програмного забезпечення, помилками користувачів, надзвичайними обставинами(пожежі, стихійні лиха, тощо). Встановлення порядку відновлення інформації у разі необхідності. Забезпечення міри захисту від помилок людини або ненавмисного видалення файлів.

Інструкція політики.

Для інформації рівня користувача та рівня системи, що обробляється організацією, періодично повинна створюватися резервна копія. Носії резервного копіювання повинні зберігатися з достатнім захистом та належними умовами навколишнього середовища. Частота та ступінь резервного копіювання повинні

відповідати важливості інформації та прийнятому ризику, визначеному власником даних. Процес резервного копіювання та відновлення інформаційних ресурсів повинен бути задокументований та періодично переглядатися. Будь які системи, що надають резервне копіювання за межами сайтів, повинні бути очищенні від обробки найвищого рівня (конфіденційності) інформації що зберігається. Фізичні засоби управління доступом у місцях зберігання резервних копій, повинні відповідати або перевищувати фізичні засоби контролю вхідних систем. Крім того, носії резервного копіювання повинні бути захищені відповідно до найвищого рівня конфіденційності інформації, що зберігається. Необхідно здійснити процес підтвердження успішності резервного копіювання електронної інформації.

Резервні копії операційних систем та іншого інформаційно важливого ПЗ не повинні зберігатися в тому самому місці. що і операційне програмне забезпечення. Інформація про резервну копію системи повинна забезпечуватися

захистом від несанкціонованих змін та умов навколишнього середовища. Резервні копії повинні перевірятися раз на місяць, щоб переконатися, що вони підлягають відновленню. Для підтвердження надійності носія та цілісності інформації, резервна інформація повинна перевірятися з певною частотою. Резервні копії даних повинні мати наступні критерії і , які можна легко ідентифікувати за мітками та/або системою штрихового кодування:

- назва системи;
- дата створення;
- класифікація;
- контактна інформація.

Резервне копіювання необхідно виконувати за методом «3-2-1», згідно з яким буде створено 3 копії необхідної інформації, зберігатися копії повинні на двох різних носіях, третя копія повинна зберігатися поза межею офісу (хмарне сховище, знімний носій поза межею офісу).

Працівник, що порушив правила даної політики, зазнає дисциплінарного покарання у вигляді матеріального штрафу або звільнення, в залежності від серйозності наслідків.

2.9.3 Політика безпеки з антивірусного захисту

Метою політики є встановлення вимоги, яким повинні відповідати всі ноутбуки, підключені до мережі ТОВ «ІнТайм», щоб забезпечити ефективне виявлення та запобігання вірусам.

Інструкція політики:

Всі ноутбуки в організації повинні мати встановлене стандартне підтримуване антивірусне програмне забезпечення. Крім того, антивірусне програмне забезпечення та бази даних сигнатур вірусів повинні постійно

оновлюватися. Ноутбуки, заражені вірусом повинні бут видалені з мережі, поки вони не будуть підтвердженні як захищені від вірусів. Системний адміністратор відповідає за створення процедур, які забезпечують запуск антивірусного програмного забезпечення через регулярні проміжки часу. Будь-які дії з метою створення та/або розповсюдження шкідливих програм у мережах організації(віруси, хробаки, троянські коні, поштові бомби тощо) заборонені.

Рекомендовані процеси для запобігання проблемам з вірусами:

– забороняється відкривати файли або макроси, щ обули вкладені до електронного листа від невідомого джерела. Дані файли необхідно негайно видалити з ноутбуку;

– необхідно видалити спам та інші непотрібні електронні листи без переадресації, відповідно до політики допустимого використання;

– завантаження файлів з неперевірених джерел суворо забороняється;

– знімний носій перед використанням необхідно перевіряти на наявність шкідливого програмного забезпечення щоразу;

– необхідно забезпечити регулярне резервне копіювання критичних даних та конфігурацій системи, та зберігати їх згідно з політикою безпеки з резервного копіювання.

Працівник, що порушив правила даної політики, зазнає дисциплінарного покарання у вигляді матеріального штрафу або звільнення, в залежності від серйозності наслідків.

Будь-який виняток із політики повинен бути затверджений директором підприємства.

Висновок

У другому розділі було виконано обстеження ОІД, а саме:

– класифіковано інформацію, що зберігається і циркулює на підприємстві та потребує захисту;

– побудовано модель загроз та модель порушника, що можуть бути присутні в даній ІТС.

На основі аналізу моделі загроз було обрано найбільш актуальні загрози та для запобігання їх реалізації розроблені наступні політики безпеки:

– політика "чистого столу";

– політика антивірусного захисту;

– політика розмежування даних.

ЕКОНОМІЧНА ЧАСТИНА

3.1 Необхідність обґрунтування витрат на реалізацію політики безпеки

Метою розрахунків є економічне обґрунтування доцільності впровадження політики безпеки інформації. Для цього визначено економічну ефективність використання основних результатів, що отримані в ході виконання роботи.

Економічна доцільність визначається розрахунками:

– капітальних витрат, що потребують розроблені елементи політики безпеки;

– експлуатаційних витрат;

– річного економічного ефекту від впровадження інформаційної політики безпеки.

Капітальні витрати

Запропоновані елементи політики безпеки передбачають необхідність витрат на реалізацію. До заходів, що потребують витрат відноситься:

- політика "чистого столу";

- політика антивірусного захисту.

3.2 Визначення трудомісткості розробки політики безпеки інформації

Розрахунок витрат на розробку політику безпеки підприємства.

Тривалість створення політики безпеки визначається за формулою:

$$t=t_{ТЗ}+t_{В}+t_{А}+t_{ВЗ}+t_{ОЗБ}+t_{ОВР}+t_{Д}, \text{ годин} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпекиінформації, становить 7 год.;

$t_{В}$ – тривалість розробки концепції безпеки інформації у організації,становить 8 год.;

$t_А$ – тривалість процесу аналізу ризиків, становить 5 год.;

$t_{ВЗ}$ – тривалість визначення вимог до заходів, методів та засобів захисту становить4 год.;

$t_{ОЗБ}$ – тривалість вибору основних рішень з забезпечення безпеки інформації становить 6 год.;

$t_{ОВР}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації становить 7 год.;

$t_Д$ – тривалість документального оформлення політики безпеки становить 4 год.

t=7 год+8 год+5 год+4год+6год+7год+4год=41 год (3.1)

Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку безпеки інформації $К_{рп}$ складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$ за формулою 3.2:

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

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, грн;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$З_{зп} = 41 * 105 = 4305 \text{ грн}$$

Вартість машинного часу для розробки політики безпеки інформації на ноутбуці визначається за формулою 3.4:

$$З_{мч} = t * С_{мч}, \text{ грн} \quad (3.3)$$

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

$С_{мч}$ – вартість 1 години машинного часу ноутбуку, грн/година.

Вартість 1 години машинного часу ноутбуку визначається за формулою 3.5:

$$Смч = Р* tнал*Се+(Фзал*На/Fр)+(Клпз*На/ Fр), \text{ грн} \quad (3.4)$$

де Р – встановлена потужність ноутбуку, кВт;

tнал – кількість задіяних станцій під час написання політики безпеки;

Се – тариф на електричну енергію, грн/кВт година;

Фзал – залишкова вартість ноутбуку на поточний рік, грн;

На – річна норма амортизації на ноутбуці, частки одиниці;

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

Клпз – вартість ліцензійного програмного забезпечення, грн;

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

Оскільки на даному підприємстві встановлена потужність Р=0,4, а тариф на електричну енергію становить 1,91 грн/кВТ година, то:

$$Смч = 0,4 * 1,91 * 11 + (10400 * 0,5\backslash 1920) + (5141 * 0,5/1920) = 12,44 \text{ грн}$$

$$Змч = t * Смч = 41*12,44 = 510,04 \text{ грн}$$

3.3 Розрахунок капітальних (фінансових) витрат

Капітальні витрати розраховуються наступним чином:

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

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів тис.грн. Стороння організація не наймалась, тому даний коефіцієнт не враховується при розрахунках;

Кзпз – вартість закупівель ліцензійного основного і додаткового ПЗ, складає 25705грн;

Таблиця 3.1 Перелік придбаного ліцензійного ПЗ

Назва	Кількість	Вартість(грн)
Windows 10 Home	5	12960
Malwarebytes	5	6105
DeviseLock	5	6640
Всього		25705

Крп – вартість розробки політики інформаційної безпеки складає 4815,86грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис грн. Витрати на навчання системного адміністратора становлять 1600грн;

Кн – витрати на встановлення обладнання та налагодження системи інфомраційної безпеки, тис.грн.

Оскільки підприємство не закуповує апаратне забезпечення, для забезпечення інформаційної безпеки Каз та Кн не враховується.

$$Кзпз = 5141 * 5 = 25705 \text{ грн}$$

$$Крп = Ззп + Змч = 4305 + 510,04 = 4815,05 \text{грн}$$

$$К = 25705 + 4815,05 + 1600 = 32120,05 \text{ грн}$$

3.4Розрахунки поточних (експлуатаційних витрат)

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

$$С = Св + Ск + Сак, \text{ тис. грн} \qquad (3.7)$$

де Св – це витрати на оновлення системи;

Сак – це витрати викликані активністю користувачів системи, що складають 11 грн – пряма допомога, 120 грн – неформальне навчання, 140 – розробка додатків, 150 грн – робота з даними, 180 грн – формальне навчання, 300 грн – futz-фактор. Всього 1000грн.

Ск – це витрати на керування інформаційною безпекою, розрахунок відбувається за наступною формулою 3.8:

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос \qquad (3.8)$$

де Сн – це витрати на навчання адміністративного персоналу й кінцевих коритсувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації, що становлять 2000грн;

Са – це річний фонд амортизаційних відрахувань, що визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ). На підприємстві експлуатуються 5 ноутбуків, загальною вартістю 67000 грн. Вартість ПЗ для 5 комп'ютерів 25705 грн.

Загалом – 92705 грн. Мінімальний термін амортизації 2 роки. Ліквідаційна вартість 5 комп'ютерів - 2500грн., ліквідаційна вартість програмного забезпечення для 5 комп'ютерів – 500 грн.

$$Са = (92705 – 3000)/2 = 44852,5 \text{грн}$$

Сз – це річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, складає:

$$Сз = Зосн + Здод, грн \quad (3.9)$$

де Зосн – основна заробітна плата, складає 5000грн на місяць, відповідно 60000 на рік;

Здод – додаткова заробітна плата, складає 1000грн на місяць, відповідно 12000 на рік. В 2021 році ЄСВ складає 22% від фонду заробітної плати і становить

$$Сєв = 72000 * 22\% = 15840 грн$$

$$Сз = 60000 + 12000 + 15840 = 87840 грн$$

Сел – це вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року:

$$Сел = Р * Fр * Це, грн \quad (3.10)$$

де Р – встановлена потужність апаратури інформаційної безпеки 0.4 кВт для одного ноутбуку, для всього комплексу враховується повна кількість ноутбуків, яка складає 5, тобто 2кВт;

Fр – річний фонд робочого часу системи інформаційної безпеки складає 12 місяців * 30 робочих діб/міс * 10 робочих годин * 5 комп'ютерів = 18000;

Це – тариф на електроенергію, 1,91грн/кВт годин.

$$Сел = 2 * 18000 * 1,91 = 68760 грн$$

Со – це витрати на залучення сторонніх організацій для виконання деяких видів обслуговування та сертифікацію обслуговування персоналу (залучення сторонніх організацій не відбувається).

Стос – це витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає 1% від суми капітальних інвестицій у вигляді 321грн.

$$Ск = 2000 + 44852,5 + 87840 + 29040 + 68760 + 321 = 144973,5 грн$$

Маючи всі необхідні дані розраховуємо річні експлуатаційні витрати:

$$С = 144973,5 + 1000 = 145973,5 грн$$

Оцінка величини збиту

Таблиця 3.2 – Заробітна плата робітників на місяць

Посада	Розмір заробітної плати, грн
Директор	25000
Менеджера (3 особи)	3*15000=45000
Продавці (3 особи)	3*10000=30000
Охоронці (2 особи)	2*8000=16000
Всього	116000

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

Упущена вигода від простою атакованого вузла або сегмента становить:

$$U = Пп + Пв + V \qquad (3.11)$$

де Пп – оплачувані витрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

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

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

Місячний фонд робочого часу складає 300 годин. Час простою внаслідок атаки 6 годин:

$$Пп = (Зс /F)* t_a, \text{ грн} \qquad (3.12)$$

де Зс – загальна кількість витрат на заробітну плату співробітників за місяць

F – місячний фонд робочого часу;

t_a – час простою внаслідок атак.

Отже:

$$Пп = (116000/300) * 6 = 2320 \text{ грн.}$$

Витрати на відновлення працездатності (Пв) включають декілька складових:

Пви – витрати на повторне ведення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частини системи, грн.

Витрати на повторне введення інформації розраховуються:

$$Пви = (Зс/F) * t_{ви}, \text{ грн} \qquad (3.13)$$

де Зс – загальна кількість витрат на заробітну плату співробітників за місяць;

F – місячний фонд робочого часу;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками унаслідок атаки.

$$Пви = (116000/300) * 9 = 3480 \text{ грн}$$

Витрати на відновлення Ппв визначаються:

$$Ппв = (Зо/ F) * t_в \text{ ,грн} \qquad (3.14)$$

Де Зо – заробітна плата системного адміністратора;

F – місячний фонд робочого часу;

$t_{ви}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу.

$$Ппв = (11000/300) * 8 = 293 \text{ грн}$$

Пзч – вартість витрат на заміну устаткування або запасних частин складає 1800грн.

$$Пв = Пви + Ппв + Пзч \text{ грн} \qquad (3.15)$$

$$Пв = 3480 + 293 + 1800 = 5573 \text{ грн}$$

Витрати від зниження працездатності атакованої системи:

$$V = (O/Fг)(t_п+t_в+t_{ви}) \qquad (3.16)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, 6000000 грн за рік;

Fг – річний фонд часу роботи організації, становить 3568 год.;

$t_п$ – 6 годин простою внаслідок атак;

$t_в$ – 8 годин відновлення після атаки;

$t_{ви}$ – 9 годин повторного введення загубленої інформації.

$$V = (6000000/3568)*23 = 38677 \text{ грн}$$

Маючи всі потрібні дані, можна розрахувати упущену вигоду від атаки на ІТС організації:

$$U = 2320 + 5573 + 38677 = 46570 \text{ грн.}$$

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

$$B = \sum i \sum n U \qquad (3.17)$$

$$B = 4 * 5 * 46570 = 931400 \text{ грн.}$$

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

$$E = B * R - C \qquad (3.18)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, складає 931400 грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, становить 0,25 (якщо реалізація загроз найймовірніша 1 раз на 3 місяці, тобто 4 рази на рік);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, складає 145973 грн.

$$E = (931400 * 0.25) - 145973 = 86877$$

Аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень

додаткового прибутку приносить гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо інформаційної безпеки говорять не про прибуток, а про запобігання можливих витрат від атаки на вузол або сегмент корпоративної мережі, а отже:

$$ROSI = E/K \quad (3.19)$$

де Е – це загальний ефект від впровадження системи інформаційної безпеки, який становить 86877 грн;

К – це капітальні затрати, які становлять 32120 грн.

$$ROSI = 86866 / 32120 = 2,7$$

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

$$To = K \setminus E = 1/ ROSI, \text{ років} \quad (3.20)$$

$$To = 1 / 2,7 = 0,37 \text{ року (3 місяці)}$$

Висновок

Під час виконання економічної частини був проведений розрахунок та проаналізована доцільність впровадження політики безпеки інформації. Визначено економічну ефективність використання основних результатів. Капітальні витрати на впровадження інформаційної політики безпеки становлять 32120 грн., експлуатаційні витрати складають 145973 грн., а загальний збиток від атаки 931400 грн, ефект від впровадження системи інформаційної безпеки становить 86877 грн. Термін окупності капітальних інвестицій складає приблизно три місяці. Отримані дані говорять про те що впровадження створених елементів політик безпеки інформації є доцільними.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було:

– проаналізовано темпи росту кіберзлочинності в світі та Україні, зокрема наведена статистика порушень інформаційної безпеки у секторі малих підприємств;

– проаналізовано нормативно правову базу у сфері захисту інформації;

– виконано обстеження об'єкта інформаційної діяльності;

– класифіковано інформацію, що зберігаються і циркулює на підприємстві та потребує захисту;

– побудовано модель загроз та порушника в ІТС, за результатами яких було обрано профіль захищеності з урахуванням найбільш актуальних загроз, виконано аналіз інформаційних ризиків та для запобігання їх реалізації розроблені політики безпеки інформації, що стосуються організації відповідних методів захисту;

– був проведений розрахунок та проаналізована доцільність впровадження політики безпеки інформації.

Отримані дані говорять про те, що впровадження створених елементів політик безпеки інформації е доцільними.

ПЕРЕЛІК ПОСИЛАНЬ

1. Techexpert.ua Електронний ресурс . – 2020. – Режим доступу: https://techexpert.ua/ru/cybersecurity-covid/

2. 10Guards.com Електронний ресурс . – 2020. – Режим доступу: https://10guards.com/ru/articles/2020-cybersecurity-statistics/

3. Gigatrans.ua Електронний ресурс . – 2019. – Режим доступу: https://gigatrans.ua/ua/news/ddos-ataki-kak-ne-stat-mishenyu-hakerov-i-uberech-dannue-biznesa

4. Hi-tech.ua Електронний ресурс . – 2018. – Режим доступу: https://hi-tech.ua/blog/posledstviya-kiberatak-dlya-malogo-i-srednego-biznesa/?am_force_theme_layout=desktop

5. ESET.ua Електронний ресурс . – 2016. – Режим доступу: https://eset.ua/ua/news/view/796/tri-goda-posle-masshtabnoy-ataki-wannacry-uroven-rasprostraneniya-ugrozy-ne-snizhayetsya

6. Lab-automat Електронний ресурс . – 2021. – Режим доступу: https://lab-automat.ru/razvitie/17-ugroz-biznesa-kotorymi-vy-mozhete-upravlyat.html

7. НД ТЗІ 1.1-002-99 Електронний ресурс . – 1999. – Режим доступу: http://www.dut.edu.ua/uploads/l_1020_50809646.pdf

8. НД ТЗІ 3.7-003-2005 Електронний ресурс . – 2005. – Режим доступу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

9. Закон України «Про інформацію» Електронний ресурс .–1992.– Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

10. Постанова Кабінетів міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телеомунікаційних системах.» Від 29.03.2006 №373 поточка редакція від 13.10.2011 Електронний ресурс .–2006.– https://zakon.rada.gov.ua/laws/show/373-2006-%EF#Text

11. НД ТЗІ 2.5-005-99 Електронний ресурс . – 1999. – Режим доступу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf

12. НД ТЗІ 2.5-004-99 Електронний ресурс . – 1999. – Режим доступу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Стан питання. Постановка задачі	17	
5	А4	Спеціальна частина	35	
6	А4	Економічна частина	9	
7	А4	Висновки	1	
8	А4	Перелік посилань	2	
9	А4	ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи	1	
10	А4	ДОДАТОК Б. Перелік документів на оптичному носії	1	
11	А4	ДОДАТОК В. Відгук керівника економічного розділу	1	
12	А4	Додаток Г. Відгук керівника кваліфікаційної роботи	1	
13	А4	ДОДАТОК Д. Наказ на проведення обстеження ОІД	1	
14	А4	ДОДАТОК Е. Наказ но створення КСЗІ	1	

ДОДАТОК Б Перелік документів на оптичному носії

1 Кваліфікаційна робота – Лігачов Єгор 125-18ск-1.docx

2 Презентація – Лігачов Єгор 125-18ск-1.pptx

ДОДАТОК В. ВІДГУК КЕРІВІ4НКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу_____доц. Пілова Д.П.

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-18ск-1 Лігачова Єгора Тимуровича

на тему: «Політика безпеки інформаційно-телекомунікаційної системи ТОВ «ІнТайм»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 70 сторінках.

Метою кваліфікаційної роботи є підвищення рівня захищеності інформації в ІТС ТОВ "ІнТайм".

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: проведення обстеження ТОВ "ІнТайм", проведення аналізу ризиків інформаційної безпеки з виявленням загроз; створення документів з політики безпеки. Практичне значення результатів кваліфікаційної роботи полягає у підвищені рівня захисту інформації в ІТС організації, за рахунок розробки політик безпеки інформації.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано згідно із стандартами.

За час дипломування Лігачов Є.Т. 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 «добре» (85).

Керівник кваліфікаційної роботи проф. Кагадій Т.С.

Керівник спец. розділу Тимофєєв Д.С.

ДОДАТОК Д. Наказ про проведення обстеження ОІД

Товариство з обмеженою відповідальністю

«ІнТайм»

НАКАЗ

« »_____ Дніпро №_____

Про обстеження та категоріювання об'єктів інформаційної діяльності ТОВ "ІнТайм"

Відповідно до Положення про технічний захист інформації в Україні, затвердженого Указом Президента України від 27.09.1999 № 1229, Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29.03.2006 № 373, вимог нормативного документа системи технічного захисту інформації № 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", для проведення обстеження та категоріювання об'єктів наказую:

1. Створити комісію з обстеження та категоріювання об'єктів інформаційної діяльності ТОВ «ІнТайм», де циркулює інформація з обмеженим доступом, що не становить державної таємниці (далі – комісія) у складі:

Щепкін Р.О. – директор.

Іванов І.А. – системний адміністратор

2. Комісії провести обстеження та категоріювання об'єктів інформаційної діяльності ТОВ «ІнТайм», де циркулює інформація з обмеженим доступом, що не становить державної таємниці в терміни, які встановлені законодавством.

3. Контроль за виконанням даного розпорядження залишаю за собою.

Генеральний директор Щепкін Р.О.

ДОДАТОК Е. Наказ про створення КСЗІ

ФОРМА ТА ЗМІСТ АКТА КАТЕГОРІЮВАННЯ ОБ'ЄКТА

Гриф обмеження доступу
Прим. N ___

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
Директор Щепкін Р.О.
(посада, підпис, ініціали, прізвище)
29.05.2021

М. П.

АКТ

категоріювання _____
(найменування об'єкта категоріювання)

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

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

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
_____
(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 _____

Голова комісії _____ _____
(підпис) (ініціали, прізвище)

Члени комісії: _____ _____

(підпис) (ініціали, прізвище)

___.___.20__