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 *Петренка Сергія Юрійовича*

академічної групи *125-18ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Войцех С.І			
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 *Петренку Сергію Юрійовичу* **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 «СмартХоумЮА»*

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

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, загальні теоретичні відомості, аналіз нормативно-правової бази	17.05.2021
Розділ 2	Обстеження об'єкту інформаційної діяльності, моделі порушника, аналіз ризиків і загроз, елементи політики безпеки.	29.05.2021
Розділ 3	Поточні, капітальні витрати, економічна доцільність створення політики безпеки.	05.06.2021

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

Дата видачі завдання: 08.01.2021р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ Петренко С.Ю
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 21 табл., 2 рис., 7 додатків, 13 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система ТОВ «СмартХоумЮА».

Предмет розробки: елементи політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «СмартХоумЮА».

Мета кваліфікаційної роботи: підвищення загального рівня інформаційної безпеки у інформаційно-телекомунікаційній системі.

У першому розділі розглянуто загальний стан питання, приведена причина створення КСЗІ та політики безпеки інформації, актуальність створення і проаналізована нормативна-правова база у сфері захисту інформації.

У другому розділі виконане обстеження об’єкту інформаційної діяльності(ОІД), де циркулює інформація з обмеженим доступом(ІзОД), аналіз відомостей про підприємство та особливості обробки інформації яка циркулює в компанії. Виходячи з цих даних, проаналізовано потенційні загрози та вразливості, розроблені моделі порушника та модель загроз. Згідно отриманих даних сформовані основні елементи політики безпеки інформації для інформаційно-телекомунікаційної системи(ІТС) задля мінімізації втрат ресурсів компанії.

В економічній частині здійснені розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації та визначена доцільність їх впровадження.

Практична значимість роботи полягає у підвищенні рівня інформаційної безпеки, для мінімізації потенційних витрат при загрозах інформації, з врахуванням властивості її обробки в ОІД.

МОДЕЛЬ ПОРУШНИКА, ПОЛІТИКА БЕЗПЕКИ ІНФОРМАЦІЇ, АКТ ОБСТЕЖЕННЯ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ,

ІНФОРМАЦІЙНІ ПОТОКИ, МОДЕЛЬ ЗАГРОЗ, ЗАХИСТ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

РЕФЕРАТ

Пояснительная записка: 87 с., 21 табл., 2 рис., 7 приложений, 13 источников.

Объект разработки: информационно-телекоммуникационная система ООО «СмартХоумЮА».

Предмет разработки: элементы политики безопасности информации информационно-телекоммуникационной системы ООО «СмартХоумЮА».

Цель квалификационной работы: повышение общего уровня информационной безопасности в информационно-телекоммуникационной системе.

В первом разделе рассмотрены общее состояние вопроса, приведена причина создания КСЗИ и политики безопасности информации, актуальность создания и проанализирована нормативно-правовая база в сфере защиты информации.

Во втором разделе выполнено обследование объекта информационной деятельности(ОИД) где циркулирует информация с ограниченным доступом(ИсОД), анализ сведений о предприятии и особенности обработки информации, которая циркулирует в компании. Исходя из этих данных, проанализированы потенциальные угрозы и уязвимости, разработанные модели нарушителя и модель угроз. Согласно полученным данным сформированы основные элементы политики безопасности информации для информационно-телекоммуникационной системы(ИТС) для минимизации потерь ресурсов компании.

В экономической части осуществлены расчеты капитальных затрат на внесение основных элементов политики безопасности информации и определена целесообразность их внедрения.

Практическая значимость работы заключается в повышении уровня информационной безопасности, для минимизации потенциальных расходов при угрозах информации, с учетом свойства ее обработки в ОИД.

МОДЕЛЬ НАРУШИТЕЛЯ, ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ, АКТ ОБСЛЕДОВАНИЯ, КОМПЛЕКСНАЯ СИСТЕМА

ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫЕ ПОТОКИ, МОДЕЛЬ УГРОЗ, ЗАЩИТА ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

ABSTRACT

Explanatory note: 87 p., 21 tables, 2 pictures, 7 applications, 13 sources.

Object of development: information and telecommunication system LLC «SmartHomeUA».

Subject of development: elements of information security policy of information and telecommunication system of LLC «SmartHomeUA».

The purpose of the qualification work: to increase the general level of information security in the information and telecommunication system.

The first section considers the general state of the issue, the reason for the creation information security policy, the relevance of the creation and analyzed the regulatory framework in the field of information protection.

The second section examines the object of information activities, which circulates information with limited access and analysis of enterprise information and features of processing information circulating in the company. Based on these data, potential threats and vulnerabilities are analyzed, and a model of the violator is developed. According to the obtained data, the main elements of the information security policy for this information and telecommunication system are formed in order to minimize the loss of the company's resources.

In the economic part, the main calculations of capital expenditures for the introduction of the main elements of information security policy to determine the feasibility of their implementation.

The practical significance of the work is to increase the level of information security to minimize the potential costs of information threats, taking into account the nature of its processing in the information and telecommunication system.

THREAT MODEL, INFORMATION SECURITY POLICY, INSPECTION ACT, VULNERABILITIES, INFORMATION SECURITY, RISK ASSESSMENT

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДТЗС – допоміжні технічні засоби і системи;

НСД – несанкціонований доступ;

КСЗІ – комплексна система захисту інформації;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ОІД – об'єкт інформаційної діяльності;

КС – комп'ютерна система;

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

БФП – багатофункціональний пристрій;

МНІ – Магнітні накопичувачі інформації;

ПЕМВН – Побічні електромагнітні випромінювання та наводи;

ІзОД – інформація з обмеженим доступом.

ЗМІСТ

ВСТУП

Сучасна підприємницька діяльність, яка стосується різних сфер економіки, постійно залежить від наявності та використання різних видів інформації, оскільки без необхідності кількості та якості інформації неможливо забезпечити розвиток бізнес-інститутів, заснованих на високотехнологічному виробництві, ефективні методи об'єднання. Тому в сучасному контексті розвитку ринкових відносин в економічній сфері інформація є унікальним видом товару з великою цінністю.

Інформаційна безпека являє собою організаційні та технічні заходи, спрямовані на захист та збереження інформації, різних видів обладнання та систем, що використовуються для роботи, зберігання та передачі даних. Завдяки державному нормативно-правовому забезпеченню законів, технології, стандарти та методи управління інформацією, підприємства та громадяни можуть розраховувати ефективний захист інформації.

Забезпечення інформаційної безпеки у підприємстві дає змогу захистити інформацію та інформаційну структуру від негативних впливів на неї. Такі дії можуть бути випадковими або навмисними, внутрішніми чи зовнішніми. Таке втручання може призвести до втрати конфіденційних даних, несанкціонованих змін або використання їх небажаними особами. Тому інформаційна безпека є важливим аспектом захисту бізнесу та забезпечує його безперервність.

Забезпечення надійної інформаційної безпеки підприємства може бути лише за умови використання певних комплексних заходів. Системи інформаційної безпеки повинні бути розроблені з урахуванням усіх поточних загроз та ризиків, а також потенційних майбутніх загроз. Тому важливо забезпечити регулярність моніторингу та контролю. Передумовами є забезпечення контролю на кожному етапі використання інформації, починаючи з її доступу до інфраструктури компанії і закінчуючи втратою актуальності чи знищенням.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальний стан питання

Концепція загроз інформаційній безпеці виникла одночасно з появою інформаційного середовища. Спочатку це були ознаки викрадення, неправильного використання та пошкодження даних в комп'ютері. Пізніше, з розвитком інформаційних мереж, небезпека даних стала способом видалення неправдивої інформації та вірусів через мережу. В даний час проблеми безпеки стосуються майже кожного представника глобального інформаційного середовища. Україна є активним учасником процесу інформаційного життєвого циклу. Це відбувається як на міжнародному рівні, так і в межах кожного підприємства.

Сьогодні актуальним є питання підвищення інформаційної безпеки підприємств, що значною мірою залежить від рівня інформаційної безпеки. Рівень інформаційної безпеки впливає на розвиток та організацію науково-технічних інновацій у процесі виробництва, стабілізуючи економічного зростання.

Розвиток бізнесу зазнає кардинальних змін під впливом конкуренції та глобалізації. Міжнародна арена економічної інтеграції безпосередньо пов'язана з диверсифікованими процесами розширення та поглиблення глобальних економічних видносин, які посилюються активацією факторів і результатів та залученням компаній до міжнародних операцій (на мікрорівні) під впливом глобальних процесів.

З розвитком науки і техніки потік клієнтів зростає, особливо збільшується кількість фінансових послуг. В процесі швидкого економічного зростання у здійсненні господарської діяльності роль інформаційної безпеки підприємств зростає.

Під час своєї діяльності підприємець повинен задовольнити потребу в отриманні, обробці, зберіганні, передачі, пересиланні та розпорядженні

інформацією. Якщо інформація представляє цінність для підприємця, її потрібно захищати від зловмисників. Цінність визначається низкою факторів, що включають корисність, надійність, час, актуальність. Для захисту даних слід заблокувати всі можливі канали витоку та забезпечити надійне зберігання даних. Загрози інформаційної безпеки поділяються на внутрішні та зовнішні.

Зовнішні зловмисні дії можуть бути такими як, копіювання цінних документів чи їх викрадення, крадіжка та пошкодження флеш-карт або носіїв з даними, втрата інформації у процесі її передачі через мережу Інтернет, передача інформації до конкурентів за допомогою інсайдерів через переманювання персоналу.

До найбільш поширених внутрішніх загроз відносяться крадіжка, зараження інформації вірусами, або пошкодження файлів службовцями компанії. До причин внутрішніх загроз відносяться як причини психологічного стану через погані відносини між співробітниками підприємства, незадоволення співробітників рівнем заробітної плати, погані відносини між співробітником та керівниками підприємства.

Психологи стверджують, що близько 25% усіх працівників розкривають інформацію, продають її або передають конкурентоспроможним компаніям для отримання додаткового доходу. Захист даних на підприємстві дуже важливий і є необхідним коли компанія укладає контракт зі своїми працівниками, особливо якщо цей працівник займає керівну посаду в компанії. Небезпека, перш за все, полягає у загрозі інформації, що зберігається в інформаційній системі підприємства. Ця система включає спеціальні програми компанії, програмні оболонки, текстові редактори, програмні пакети, бази даних.

1.2 Необхідність побудови КСЗІ на підприємстві

Відповідно до чинного законодавства України і вимог окремих нормативних положень Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" обов'язковому захисту інформації підлягає інформація, що є власністю держави, або інформація з обмеженим доступом, вимоги по захисту якої встановлені законом, в тому числі і персональні дані громадян.

1.3 Політика інформаційної безпеки

Перш ніж пропонувати будь-які рішення по організації системи захисту інформації, належить розробити політику безпеки. Політика безпеки - набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів та програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту. Для кожної конкретної організації політика безпеки повинна бути індивідуальною, залежною від конкретної технології обробки інформації, використовуваних програмних і технічних засобів, розташування організації і т. д.

Організаційно політика безпеки визначає порядок подання та використання прав доступу користувачів, а також вимагає звітності користувачів за свої дії в питаннях безпеки. Система захисту інформації виявиться ефективною, якщо вона буде надійно забезпечувати виконання правил політики безпеки. Етапи побудови організаційної політики безпеки - це внесення в опис об'єкта структури цінностей

і проведення аналізу ризику, визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності. Перш за все необхідно скласти детальний опис мети побудови системи безпеки об'єкта, яка виражається через сукупність факторів або критеріїв, уточнюючих мету. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив). Фактори безпеки, в свою чергу, можуть поділятися на правові, технологічні, технічні та організаційні.

Розробка політики безпеки організації, як формальної, так і неформальної безумовно, нетривіальне завдання. Експерт повинен не тільки володіти відповідними стандартами і добре розбиратися в комплексних підходах до забезпечення захисту інформації організації, але і, наприклад, виявляти детективні здібності при виявленні особливостей побудови інформаційної системи та існуючих заходів по організації захисту інформації. Аналогічна проблема виникає в подальшому при необхідності аналізу відповідності рекомендацій політики безпеки реальному стану речей. Необхідно за обраним критерієм відібрати свого роду «контрольні точки» і порівняти їх практичну реалізацію з еталоном, що задається політикою безпеки.

У загальному випадку можна виділити такі процеси, пов'язані з розробкою і реалізацією політики безпеки:

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

– облік матеріальних або інформаційних цінностей;

– моделювання загроз інформації системи;

– власне аналіз ризиків з використанням того чи іншого підходу – наприклад, вартісний аналіз ризиків.

2. Заходи з оцінювання відповідності заходів щодо забезпечення захисту інформації системи обраного прикладу: стандарт, профіль захисту тощо.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту.

4. Дії, пов'язані зі збиранням, зберіганням і обробкою статистики щодо подій пов’язаною з безпекою для організації.

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назва цього способу, як правило, визначає назву політики безпеки.

Для вивчення властивостей способу управління доступом створюється його формальний опис – математична модель. При цьому модель повинна відображати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в сенсі даного управління. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно. Відзначимо лише, що для розробки моделей застосовується широкий спектр математичних методів моделювання, теорії інформації, графів та ін.

На даний час найкраще вивчені два види політики безпеки: виборча і повноважна, засновані, відповідно, на виборчому і повноважному способах керування доступом.

Крім того, існує набір вимог, що підсилюють дію цих політик і призначені для управління інформаційними потоками в системі. Слід відзначити, що засоби захисту, призначені для реалізації будь-якого з названих способів управління доступом , дають тільки можливості для надійного управління доступом чи інформаційними потоками.

Основою виборчої політики безпеки є виборче керування доступом, яке має на увазі, що:

- всі суб'єкти і об'єкти системи повинні бути ідентифіковані;

- права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого управління доступом застосовується модель системи на основі матриці доступу, іноді її називають матрицею контролю доступу. Така модель отримала назву матричної. Матриця доступу являє собою

прямокутну матрицю, в якій об'єкту системи відповідає рядок, а суб'єкту – стовпець. На перетині рядка і стовпця матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Зазвичай виділяють такі типи доступу суб'єкта до об'єкта, як «доступ на читання», «доступ на запис», «доступ на виконання» та ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до правил, що існують в даній системі. Визначення і зміна цих правил також є завданням матриці доступу.

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеного у відповідній клітинці матриці доступу. Зазвичай виборче управління доступом реалізує принцип «що не дозволено, то заборонено», який передбачає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу[1].

1.4 Нормативно-правова база

За усі роки існування інформаційних технологій у державі було запроваджено велику кількість законів, документі та нормативних актів, які суцільно регламентують загальну функціональність певних систем захисту інформації в ІТС. Усе це створило нормативно-правову базу зі своїми особливостями щодо модифікації, зберігання, одержання інформації та експлуатації усіх цих ресурсів для забезпечення захисту. Воно визначає, забезпечує та регламентує властивість самої інформації, відповідальність та порядок дій для забезпечення її захисту в ІТС враховуючи способи як керування системою так і управління доступу до неї.

Створюючи комплекс системи захисту інформації, об`єднуються такі складові, як:

- Організаційних та інженерних заходи;
- програмно-апаратних засоби.

Для їх доцільного об’єднання, слід дотримуватись вимог значної кількості нормативно-правових документів, актів та стандартів з технічного захисту інформації. Їх впровадження та формування в Україні здійснюється регулярно, що підтримує актуальну інформаційну базу по забезпеченню захисту інформації в ІТС. Через них можна в межах однієї організації або самої ІТС врахувати усі особливості, умови та засоби обробки інформації у ній. Нижченаведені документи використовують свою встановлену термінологію та визначення, які і будуть застосовуватися під час розробки політки безпеки згідно технічного захисту інформації у ІТС.

Для виконання роботи, слід враховувати такі закони, постанови та положення:

1) Конституція України – основний документ, який визначає державний устрій, систему та принципи, за якими функціонують державні органи, виборчу систему, права та обов'язки уряду, суспільства та громадян.

2) Закон України «Про інформацію» – визначає найважливіші методи доступу, використання, розповсюдження та зберігання інформації. Цей закон відображає право особам для отримання інформації щодо всіх аспектів суспільного та регіонального життя в інформаційній системі України, визначає статус учасників інформаційного спілкування, регулює доступ до інформації та забезпечує її захист, а також дає захист особистості та спільноту від неправдивої інформації.

3) Закон України «Про захист персональних даних» – закон регулює правовідносини, які відносяться до захисту та обробки персональних даних, і направлений на захист основних прав і свобод людей та громадян, включаючи права на приватне життя, пов’язане з обробкою їх персональних даних.

4) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» – закон, який здійснює нагляд за взаємовідносинами у галузі захисту інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, регулює об’єкти та суб’єкти захисту,

які відносяться до системи, зі встановленням зв'язку між власниками системи, користувачами та власниками даних.

5) Закон України «Про електронний цифровий підпис» – закон визначає правовий статус електронних цифрових підписів та регулює порядок взаємодії в результаті використання електронних цифрових підписів. Він не застосовується до відносин, що виникають внаслідок використання інших типів електронних підписів, включаючи зображення, які переведені в електронний варіант з власноручно написаними підписами.

6) Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373;

7) Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229.

З ціллю забезпечення безпеки інформації слід враховувати рекомендації, вимоги та стандарти які описані в таких документах як:

- ДСТУ ISO/IEC 27001:2015 - Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою – стандарт створений для визначення вимог для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та постійного вдосконалення системи управління інформаційною безпекою (СУІБ) [2].

- ДСТУ ISO/IEC 27002:2015 - Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT) – міжнародний стандарт розроблено для організацій для використання як довідкової інформації щодо вибору заходів безпеки під час впровадження СУІБ на базі ISO/IEC 27001 або як настанову для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Цей стандарт також призначено для використання в розробленні настановних документів з управління інформаційною безпекою, специфічних для промисловості та організацій, з урахуванням специфічних ризиків інформаційної безпеки їх середовища [3].

- ДСТУ ISO/IEC 27005:2019 – Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT) – стандарт надає настанови для управління ризиками інформаційної безпеки. Підтримує основні концепції, визначені в ISO/IEC 27001, і розроблений для сприяння задовільному впровадженню інформаційної безпеки на основі підходу з управління ризиками [4].

- НД ТЗІ 1.1-002-99 – визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання як:

1) визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

2) створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

3) оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача [5].

- НД ТЗІ 2.5-004-99 – нормативний документ установлює критерії оцінки захищеності інформації, що обробляється в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту) [6].

- НД ТЗІ 2.5-005-99 – документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу. Мета цього документа —надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі [7].

- НД ТЗІ 1.6-005-2013 – визначає загальні вимоги з категоріювання, ознаку, за якою здійснюється категоріювання, а також порядок категоріювання об’єктів інформаційної діяльності, в тому числі об’єктів електронно-обчислювальної техніки, де циркулює (обробляється технічними засобами та/або озвучується)інформація з обмеженим доступом, що не становить державної таємниці [8].

- НД ТЗІ 1.1-003-99 – документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації [9].

Інформація з обмеженим доступом – інформація з правами доступу до якої обмежено встановленими певними правовими нормами і\або правилами [10].

До таємної інформації належить інформація, що містить відомості, які становлять державну, а також іншу передбачену законом таємницю [11].

Конфіденційна інформація – є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [10].

Інформаційний ресурс — сукупність документів у інформаційних системах. Документом Закон України «Про інформацію» визначає формат отримання, зберігання, розповсюдження та використання інформації шляхом її запису на магнітні, кіно-, відео-, фото- чи інші носії інформації. Поняття "документи" має важливе значення, оскільки документи є частиною джерела інформації і мають юридичні наслідки. Інформація з обмеженим доступом (за умови захисту) може оброблятися, передаватися та зберігатися ресурсами ІТС, такими як сервери, робочі станції, пристрої зберігання даних, периферія (принтери, з’ємні носії),

мережеве обладнання, системи та програмне забезпечення, яке з'єднане з об'єктами ІТС для взаємодії з інформацією[10].

1.5 Постановка задачі

Нормативна-правова база дає достатнє уявлення щодо правильності і доцільності впровадження системи захисту інформації. Тому для розробки елементів ПБ необхідно проаналізувати основні особливості ОІД, особливості його розташування, функціонування, загальну структуру та компоненти пристроїв, апаратне та програмне забезпечення, його підключення, характер конфігурації, їх розміщення, архітектура та топологія, існуючі програмно-апаратні засоби захисту інформації. Також слід приділити увагу на особливості обробки та циркуляції інформації у системі.

Мета цього аналізу – надання повної інформаційної бази у можливості захисту даних, виявити компоненти ІТС, що вимагають підвищених вимог до безпеки даних, та здійснити додаткові заходи безпеки у ній.

1.6 Висновок

У цьому розділі було описано загальний стан питання щодо необхідності захисту інформації у підприємствах включаючи і необхідність створення КСЗІ.

Також немало уваги приділено до самої політики безпеки, а саме доцільності її розробки, вид та загальні правила, пов'язані з впровадженням її у будь-яке середовище, де необхідний захист інформації. Усе це закріплено нормативно-правовою базою для встановлення правил та стандартів щодо забезпечення захисту інформації. Вона регулярно оновлюється у державному устрої та актуалізується під нинішній час у світовому інформаційному розвитку.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Опис ситуаційного плану

Підприємство знаходиться в цегляній будівлі за адресою м. Дніпро, проспект Лемура, 36.

Несучі стіни зроблені з білої цегли. Перекриття зроблені з використанням залізобетонних плит. Вікна металопластикові. Будівля з білої цегли має плоский дах. фундамент виконаний з використанням залізобетонних забивних паль.

Будівля поділена на 2 частини, перша – одноповерхова Г-образна адміністративна будівля з торгівельними підприємствами, друга – на північно-північно-східному боці 8-поверхова адміністративна будівля з офісними приміщеннями до яких можливо потрапити с внутрішнього двору будівлі за допомогою ліфту або сходами.

До будівлі підведені електропостачання та водопостачання. Територія, де розташована будівля охороняється службою охорони. Вхід у будівлю через металеві двері. Ввійти можна через внутрішній двір або при необхідності з запасного(з північно-східної сторони).

Режим допуску до території будівлі забезпечується таким чином:

У робочий час забезпечується силами охорони (приватна фірма) та системою контролю управління доступу(необхідний спеціальний пропуск або документи для в'їзду на територію). Чергові знаходяться біля КПП з шлагбаумом у в'їзді на внутрішнього територію будівлі.

У неробочий час забезпечується силами охорони(приватна фірма) з використанням відеоспостереження.

Схема заземлення зображена на ситуаційному плані, заземлення іде від північно-східної частини будівлі до розподільного щита.

Розподільний щит знаходиться у середині будівлі з північної сторони, також на кожному поверсі встановлена своя окрема щитова, яка іде у щитову кожного офісного приміщення.

Перетворювач електроенергії – трансформаторна підстанція №27, яка знаходиться на території будівлі та з'єднана с щитовою.

Лінії системи опалення проходять під землею до підвалу будівлі і потім розмежується вертикально до інших приміщень.

Лінія системи водопостачання (в будівлю заходить металева труба, і після лічильника йде пластикова) і каналізація (ПВХ труби).

Лінія системи інтернет провайдера (оптоволоконний кабель) - прокладений в межах КЗ.

Ситуаційний план ОІД приведений в додатку Б.

Територія будівлі огороджена двометровим металевим парканом у вигляді грат з різними візерунками, навколо будівлі прокладена асфальтована дорога з місцями для паркування. Найближчими об'єктами до офісу є: адміністративна будівля №8 (5 метрів), трансформаторна підстанція №27 (73 м), адміністративна будівля №9 (56 метрів), ТЦ «АСТРА» (90метрів) (Табл. 2.1).

Таблиця 2.1 – Характеристика будівель та споруд

№	Найменування	Адреса	Кількість поверхів	Мінімальна відстань до ОІД, м
1	Магазин «Універсам»	проспект Лемура 37а	3	98
2	Виробничий корпус	проспект Лемура 37	1	144
3	Господарський корпус	проспект Лемура 37	1	115
4	Господарський корпус	проспект Лемура 37	1	102
5	ТЦ «АСТРА»	проспект Лемура 32б	2	90
6	Гаражі на території корпусу	проспект Лемура 36	1	87
7	Трансформаторна підстанція №27	проспект Лемура 36	1	73
8	Адміністративна будівля	проспект Лемура 36	1	5
9	Адміністративна будівля	проспект Лемура 38	2	56

Продовження таблиці 2.1

№	Найменування	Адреса	Кількість поверхів	Мінімальна відстань до ОІД, м
10	Господарський корпус	проспект Лемура	1	67
11	Адміністративна будівля	проспект Лемура 36	8	0
12	Господарський корпус	проспект Лемура 36	1	65

2.2 Опис генерального плану

Приватне підприємство «СмартХоумЮА», яке основано у 2020 р.. Підприємство займається розробкою\проектуванням\монтажем різних приладів та пристроїв для «Розумного дому» під замовлення. Штат складається з 6 працівників.

Приміщення, де циркулює інформація з обмеженим доступом (ІзОД) розташоване на третьому поверсі 9-ти поверхового будинку з адміністративними приміщеннями.

Контрольована зона(КЗ) – обмежена зовнішніми стінами будівлі з південно-західних до південно-східних сторін, з інших боків внутрішніми стінами(коридором та іншими офісними приміщеннями). Над стелею та під підлогою знаходяться інші офісні приміщення. Вхідні двері метал\мдф з двома замками (циліндричними) під ключ.

Режим КЗ забезпечується таким чином:

У робочий час режим доступу до КЗ виконується з 10:00 ранку після відчинення дверей з двома циліндричними замками під ключ працівником підприємства, клієнти можуть заходити у офіс після обговорення часу зустрічі, для того, щоб зустріти його одним з працівників для проходження через контроль доступу до будівлі де знаходиться офіс. Клієнт може перебувати у кабінеті

директора або офісу, для надання створення замовлення, або надання додаткової інформації для нього.

У неробочий час офіс ставиться під охорону за допомогою централізованих систем сигналізації з 21:00 вечора до 9:00 ранку з зачиненням головних вхідних дверей у офіс.

Прибирання проводиться раз у 3 дні з 10 до 11 годин.

Вікна металопластикові, одностворчасті. На кожному вікні встановлені жалюзі. крім вікна у коридорі.

Загальна характеристика офісу(КЗ):

- Загальна площа усіх приміщень КЗ – 155 м^2.
- Товщина несущих стін(біла цегла) – 50 см.
- Товщина перегородок(гіпс) – 20 см.
- Висота стель в приміщеннях – 250 см.

Розміри приміщень КЗ:

- Офіс – 27,4 м2.
- Кабінет Директора – 22,4 м^2.
- Технічний Відділ – 27.2 м^2.
- Склад – 25.5 м^2.
- Кухня – 9.1 м^2.
- Коридор – 31.9 м^2.

Розетки, які являють собою елементами електропостачання в усіх приміщеннях виконані трьох дротовими с заземленням, ці лінії систем підключені к щитової(ЩО-12) у Технічному відділі, яка з'єднана до поверхової(ЩО-3) далі по загальному коридору.

Вимикачі системи освітлення одноклавішні, які підключені к щитовій(ЩО-12) у технічному відділі, яка з'єднана з поверховою(ЩО-3) далі по загальному коридору.

Лінії системи освітлення виконані силовими кабелями вініл-вініл-голий(ВВГ) та з'єднують стельові світлодіодні лампи.

Система охоронно-пожежної сигналізації – об'єкт знаходиться під охороною, за допомогою централізованої системи охоронно-пожежної сигналізації, яка поєднана з загальним пунктом охорони.

План охоронно-пожежної сигналізації яка знаходиться в КЗ наведена у додатку Г.

Система вентиляції, яка проведена до кожного приміщення – приточно-витяжна, план який наведений в додатку В.

Система опалення, яка знаходиться у кожному приміщені – біметалічні радіатори з металопластиковими трубами. Розводка вертикальна яка надходить з підвального приміщення.

Локальна мережа - кручена пара, яка прокладена в КЗ від щитової провайдеру на поверсі (№3) і не виходить за його межі.

Схема генерального плану підприємства наведена в додатку В.

Перелік основних та допоміжних технічних засобів наведені у таблицях 2.2-2.4.

Таблиця 2.2 – Опис основних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елементу до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
1	Системний блок РС-1	HP	Initio I1170	ZXF958471	У столі	1,5	1,3
2	Системний блок РС-2			ZXF958472	У столі	1,5	0,9
3	Системний блок РС-3			ZXF958473	У столі	1,5	0,9
4	Системний блок РС-4			ZXF958474	У столі	2,5	0,8
5	Системний блок РС-5			ZXF958475	У столі	1,5	1,6

Продовження таблиці 2.2

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елементу до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
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	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
16	БФП-1	Canon	MF4410	MF847161	На столі	1,5	1,4
17	БФП-2	Canon	MF4410	MF847162	На столі	1,5	1,9
18	Маршрутизатор	Keenetic	Giant KN-2610	DLD79894	На стіні	4	1,4
19	Зовнішній накопичувач ES-1	Toshiba	Canvio Basics	410EK3AA	У сейфі	1	2

Таблиця 2.3 – Опис допоміжних технічних засобів системи охоронно-пожежної сигналізації

№	Найменування	Модель	Серійний номер	Розташування	Мінімальна відстань від елементу до кордонів КЗ, м	Мінімальна відстань до ОТЗ, м
1	Орион NOVA 16	ППКОП	320156230 65120	Коридор	0,5	2
2	LD-95	Сирена світлошумова	486468684 68486	Загальний коридор	0	3
3	ЭСМК-8	Магніто-контактний	Б/Н	Коридор (двері)	0,3	3
4	ЭСМК-4	Магніто-контактний	Б/Н	Кабінет Директора, (двері і вікна)	0,3	2
5					0,3	2
6					4	3
7				Офіс (двері і вікна)	0,3	2
8					4	3
9					0,3	2
10				Кухня (двері і вікна)	2	5
11					0,3	5
12				Технічний Відділ (двері)	3	3
13				Коридор (вікно)	1,5	5
14				Склад (двері)	4	5
15	АСТРА-621	Комбінований сповіщувач руху та розбиття скла	Б/Н	Офіс	4	1,3
16					4	2,5
17				Кухня	4	5
18				Кабінет Директора	4	1,5

Продовження таблиці 2.3

№	Найменування	Модель	Серійний номер	Розташування	Мінімальна відстань від елементу до кордонів КЗ, м	Мінімальна відстань до ОТЗ, м
19	Satel Topaz	Інфрачервоний сповіщувач руху	48646868468443	Технічний Відділ	3	2
20			48646868468444	Коридор	0,5	3
21			48646868468445	Склад	4	5
22	Артон СПД Кадет	Датчики диму	48646868468487	Склад	2	5
23			48646868468489		2	5
24			48646868468480	Технічний Відділ	2	0,9
25			48646868468481		2	0,9
26			48646868468482	Кухня	1,5	5
27			48646868468483	Офіс	2	0,8
28			48646868468484	Кабінет Директора	2	1,3
29	SPR-1	Кнопка пожежі	48646868612848	Коридор	0,3	2,5
30	ИРТС	Кнопка тривоги	48646862346848	Кабінет Директора	1,5	1

Таблиця 2.4 – Опис допоміжних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елементу до кордонів КЗ, м	Мінімальна відстань до ОТЗ, м
1	Навісна Led лампа освітлення	TL-Office	15 L600 O 4K	KIB465661	На стелі	2	1
2				KIB465662		2,1	3
3				KIB465663		2,3	2
4				KIB465664		2,3	3
5				KIB465665		1,7	5
6				KIB465666		3	4
7				KIB465667		5	3
8				KIB465668		5	5
9				KIB465669		3	7
10				KIB465670		2	0,9
11				KIB465671		2	1
12				KIB465672		2	4
13				KIB465673		2	7
14	Маніпулятор миша 1	4a-tech	OP-720	MAT41575	На столі	1,4	0,2
15	Маніпулятор миша 2			MAT41576	На столі	1,3	0,2
16	Маніпулятор миша 3			MAT41577	На столі	1,5	0,2
17	Маніпулятор миша 4			MAT41578	На столі	2,3	0,2
18	Маніпулятор миша 5			MAT41579	На столі	1,4	0,2
19	Телефон 1	Xiaomi	Redmi 9a	C4C4G6S6F1	перенос ний	-	-
20	Телефон 2	Aple	Iphone 8	1Z2X3C6V5B	перенос ний	-	-
21	Телефон 3	OPPO	Reno 4	A4S5D6FG48	перенос ний	-	-
22	Телефон 4	Google	Pixel 5	T9G6B3V2F5	перенос ний	-	-
23	Телефон 5	Honor	X10	D2C5D6F335	перенос ний	-	-

2.3 Обстеження обчислювальної системи

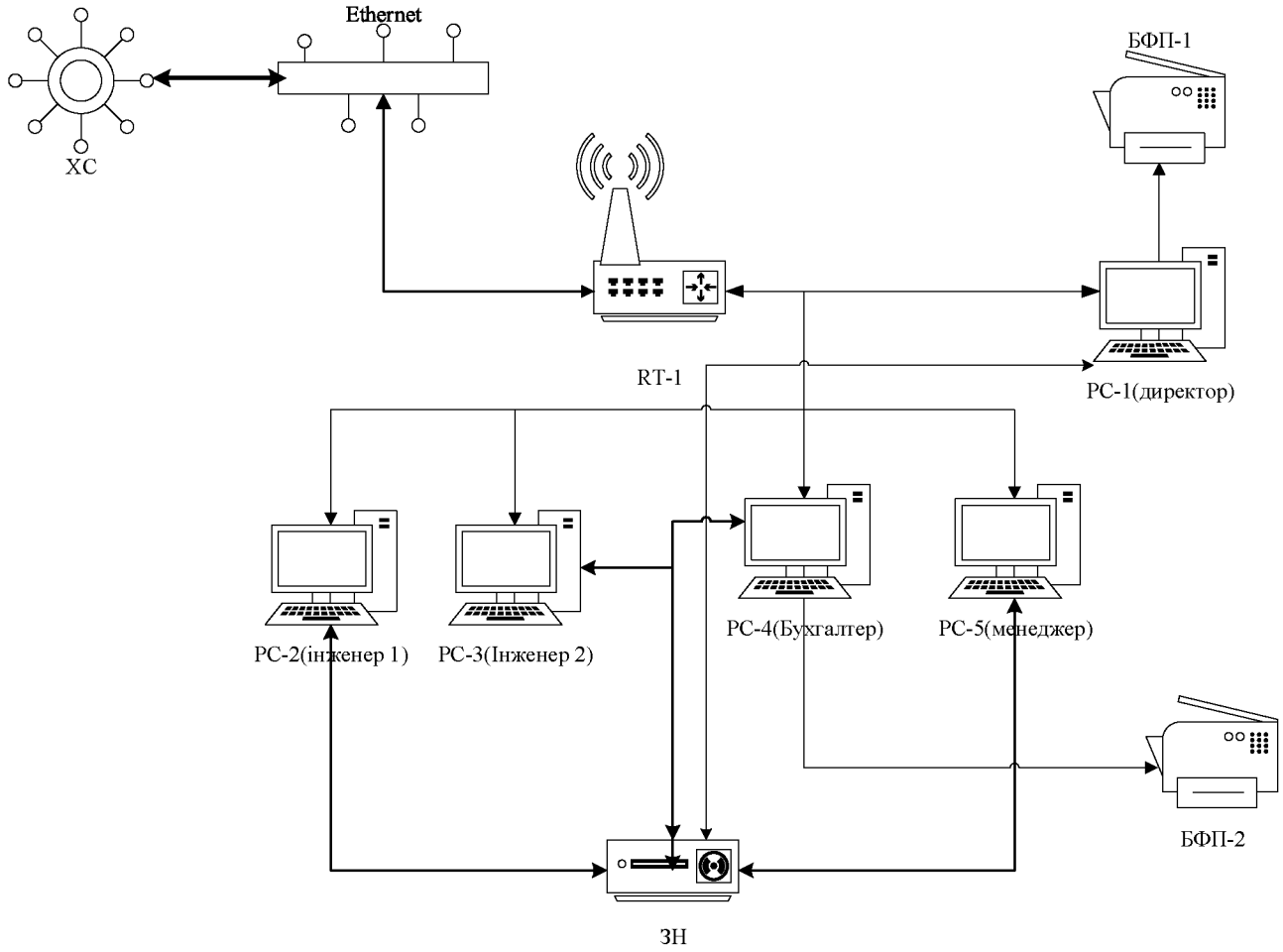


Рисунок 2.1 – Структурна схема підключення ОТЗ

Усі клавіатури до системних блоків підключені через роз'єм PS\2

Усі миші до системних блоків підключені через роз'єм USB

До приміщення від лінії систем інтернет провайдера надходить кручена пара від провайдера «Воля», яка підключена до роутеру, усі системні блоки під'єднані до мережі Інтернет через архітектуру «Зірка» за допомогою крученої пари в роз'єм RJ-45. Сітка накладена однорангова. Доступ до мережі інтернет відкритий для з'єднання з хмарним сховищем через OneDrive.

БФП під'єднані до ПК Директора та ПК Бухгалтера через USB роз'єм.

Маршрутизатор(RT-1) також являє собою точку доступу WI-FI з обмеженим доступом(тільки працівники знають пароль) з виходом в інтернет для власних потреб.

РС-2/3 інженерів отримують замовлення від клієнта або директора для подальшого виконання замовлення.

РС-4 бухгалтера створює обліки, персональні дані працівників, зарплатні відомості, які можуть бути відтворенні у паперовому вигляді при необхідності за допомогою БФП-1.

РС-5 менеджера створює\заповнює клієнтську базу, домовляється з клієнтами, створює данні замовлень.

РС-1 директора створює\заповнює клієнтську базу, домовляється з клієнтами, створює данні замовлень, приймає плани об'єктів замовників. Дані при необхідності можуть бути відтворенні у паперовий вигляд за допомогою БФП-1.

Зовнішній накопичувач(ЗН) використовується для резервного копіювання даних з ПК працівників в разі необхідності та потім зберігається у сейфі директора.

Хмарне сховище використовується для зберігання зарплатних відомостей та робочого графіку працівників.

Характеристика апаратного забезпечення та перелік ПЗ в ІТС занесені у таблиці 2.5-2.6.

Таблиця 2.5 – Характеристика апаратного забезпечення обчислювальної системи

№	Назва	Характеристики	Серійний номер
1	Персональний комп'ютер(PC1)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666661
2		Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66641
3		Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45711
4		Блок живлення: GameMax GM400 OEM	BP40817151
5		Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D1
6	Персональний комп'ютер(PC2)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666662
7		Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66642
8		Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45712
9		Блок живлення: GameMax GM400 OEM	BP40817152
10		Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D2
11	Персональний комп'ютер(PC3)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666663
12		Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66643
13		Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45713
14		Блок живлення: GameMax GM400 OEM	BP40817153
15		Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D3
16	Персональний комп'ютер(PC4)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666664
17		Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66644
18		Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45714
19		Блок живлення: GameMax GM400 OEM	BP40817154
20		Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D4
21	Персональний комп'ютер(PC5)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666665
22		Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66645
23		Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45715
24		Блок живлення: GameMax GM400 OEM	BP40817155
25		Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D5

Таблиця 2.6 – Перелік ПЗ в ІТС

№	Найменування ПО	Версія ПЗ	Пристрій	Тип ліцензії	Тип
1	Windows 10 Enterprise	ver.1909 Build 13512,109	PC-1	Комерційна	Системне
			PC-2		
			PC-3		
			PC-4		
			PC-5		
2	Arduino IDE	ver.231	PC-1	Безкоштовне	Прикладне
			PC-2		Прикладне
			PC-3		Прикладне
3	Norton 360 Deluxe	ver.22.20.5.39	PC-1-5	Комерційна	Спеціалізоване
4	MS Office 2016 pro	ver.16.150.0.1	PC-1-5	Комерційна	Прикладне
5	Microsoft Edge	ver.1.6543	PC-1-5	Безкоштовне	Прикладне
6	Cisco Packet Tracer	ver.8.0	PC-1-3	Безкоштовне	Прикладне
7	Viber	ver.12.1	PC-1-5	Безкоштовне	Прикладне
8	Microsoft One Drive	ver.422.33	PC-1-5	Комерційна	Прикладне
9	CCleaner	ver 5.7	PC-1-5	Безкоштовне	Прикладне

2.4 Обстеження інформаційного середовища

Таблиця 2.7 - Інформація яка циркулює на ОІД

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання	РК	РЦ	РД
1	Зарплатні відомості	Відкрита	немає	Всі працівники	PC-1, ХС	2	2	2
2	Особисті справи співробітників	ІзОД	Конфіденційна інформація	Директор, Бухгалтер	PC-1, ЗН -1	2	2	2
3	Клієнтська база	ІзОД	Конфіденційна інформація	Директор, Менеджер	PC-1	2	2	3

Продовження таблиці 2.7

№	Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання	РК	РЦ	РД
4	Бухгалтер-ські звіти	ІзОД	Конфіденційна інформація	Директор, Бухгалтер	РС-1, ЗН -1	2	2	3
5	Вхідні Плани об’єктів замовників	ІзОД	Конфіденційна інформація	Директор, Інженер1-2	РС-2, ES-1	3	3	3
6	Вихідні Плани об’єктів замовників	ІзОД	Конфіденційна інформація	Інженер1-2	РС-2, ЗН -1	3	3	3
7	Робочий графік	Відкрита	немає	Всі працівники	РС-5, ХС	1	1	1
8	Дані замовлень	ІзОД	Конфіденційна інформація	Інженер1-2, Директор, Менеджер	РС-5, ЗН-1	3	2	3

ХС – Хмарне сховище ; ЗН – Зовнішній накопичувач

Для інформації яка циркулює на ОІД(Таб.2.7) були використані рівні властивостей, що описані далі.

Рівні конфіденційності:

– К1 – 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;

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

– К3 – рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 – рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 – критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності:

- Ц1– рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

- Ц2 – рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

- Ц3 – рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

- Ц4 – рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

- Ц5 – критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

- Д1– рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

- Д2 – рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

- Д3 – рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

- Д4 – рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

- Д5 – критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Схема інформаційних потоків зображена на рисунку 2.2. В таблиці 2.8 представлені користувачі в ІТС з ролями у системі в ній.

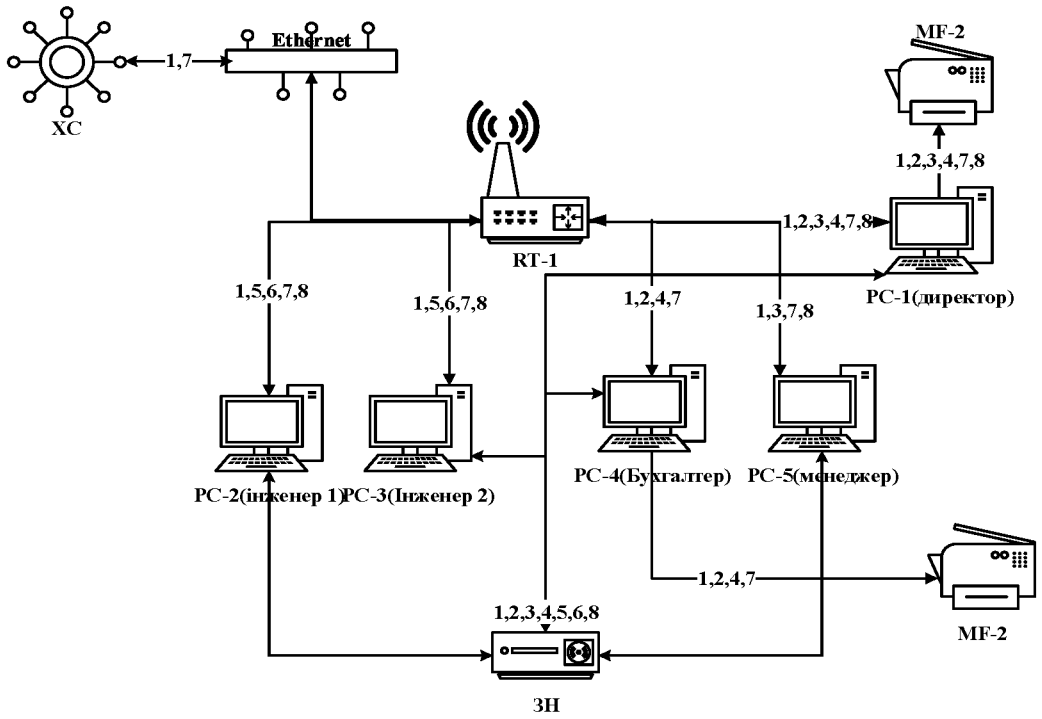


Рисунок 2.2 – Схема інформаційних потоків

Таблиця 2.8 – Користувачі

ПІБ	Посада	Рівень кваліфікації	Використовує пристрій	Роль у системі
Петренко Сергій Юрійович	Директор	Досвідчений	PC-1	Користувач
Коваленко Микола Іванович	Інженер 1	Досвідчений	PC-2	Користувач
Олійник Микола Іванович	Інженер 2	Досвідчений	PC-3	Користувач
Ткаченко Володимир Іванович	Бухгалтер	Середній	PC-4	Користувач
Шевченко Володимир Миколайович	Менеджер	Середній	PC-5	Користувач
Коваль Василь Іванович	Системний адміністратор	Досвідчений	PC-1-5	Адміністратор

2.5 Опис умов зберігання і використання інформації

Робота з даними ведеться у паперовому та електронному вигляді.

Зарплатні відомості – створюються бухгалтером за допомогою офісного ПЗ після схвалення її директором через локальну мережу, копія відсилається на Хмарне сховище с доступом до всіх працівників.

Робочий графік – створюються менеджером за допомогою офісного ПЗ, копія відсилається на Хмарне сховище с доступом до всіх працівників.

Особисті справи співробітників – Створюються бухгалтером за допомогою офісного ПЗ, копії якого зберігаються у паперовому вигляді та на зовнішньому накопичувачі у сейфі директора.

Клієнтська база – створюються менеджером та заповнюються ним або директором, копія яких зберігається на зовнішньому накопичувачі у сейфі директора.

Бухгалтерські звіти – створюються бухгалтером за допомогою офісного ПЗ після схвалення її директором через локальну мережу, копії якого зберігаються у паперовому вигляді та на зовнішньому накопичувачі у сейфі директора.

Вхідні Плани об’єктів замовників – приймаються у електронному вигляді через пошту, мессенджери або через зовнішній носій до ПК директора або паперовому (для відцифрування їх у майбутньому) та передаються інженерам. Копії зберігаються на зовнішньому носії у сейфі директора. Являють собою точні плани об’єктів, які потім заносяться у спеціалізоване ПЗ для роботи з ним.

Вихідні Плани об’єктів замовників – зберігаються у ПК інженерів під час їх обробки, копії(після схвалення та затвердження підсумкового варіанту їх клієнтом) зберігаються на зовнішньому носії у сейфі директора. Являє собою точні плани об’єктів замовників, з розташуванням у ньому нових пристроїв, які будуть задовольняти вимоги заказу клієнта, та плани реалізації їх підсумкового монтажу. Можуть також тримати у собі програмні коди для мікропроцесорів які

потім будуть застосовуватись в обладнанні, яке встановлюватимуть на об'єкті замовника.

Дані замовлень – являє собою інформацію про місцезнаходження об'єкту, його основну характеристику та вимоги клієнта. Створюються менеджером або директором за допомогою офісного ПЗ, копії зберігаються на зовнішньому носії у сейфі директора.

2.6 Модель порушника

Модель можна відобразити системою таблиць(Табл 2.9-2.16). Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них вказується в дужках і оцінюється за 4-бальною шкалою.

Таблиця 2.9 – Категорії порушників, визначених у моделі

Позначення	Визначення категорії	Рівень загрози
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення(електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2

ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 2.10 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушника	Рівень загроз
М1	безвідповідальність	1
М2	самоствердження	2
М3	корисливий інтерес	3
М4	Професійний обов'язок	4

Таблиця 2.11 – специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.12 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації	4

	систем обробки інформації	

Таблиця 2.13 – Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника	Рівень загроз
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 2.14 – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника	Рівень загроз
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Є два варіанти сумарного рівня загроз для окремих категорій можливих порушників:

1)внутрішній порушник «ПВ» - варіант мінімальних загроз з причини безвідповідального ставлення до виконання своїх посадових обов’язків;

2)зовнішній порушник «ПЗ4» (агент конкурентів або закордонних спецслужб «під прикриттям») - варіант максимальних загроз з причини цілеспрямованих несанкціонованих дій з метою модифікації або викрадення інформації.

Таблиця 2.15 – Модель порушника

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ1	М2	К3	З2	Ч2	Д3	13
	1	2	3	2	2	3	
	ПЗ4	М4	К4	З4	Ч4	Д1	21
	4	4	4	4	4	1	
Бухгалтер	ПВ1	М1	К2	З1	Ч1	Д3	9
	1	1	2	1	1	1	
	ПЗ4	М4	К4	З4	Ч2	Д2	20
	4	4	4	4	2	2	
Менеджер	ПВ1	М1	К2	З1	Ч1	Д3	9
	1	1	2	1	1	3	
	ПЗ4	М4	К4	З4	Ч2	Д2	20
	4	4	4	4	2	2	
Інженер 1-2	ПВ3	М2	К3	З2	Ч3	Д3	17
	3	2	3	2	3	3	
	ПЗ4	М4	К4	З4	Ч3	Д3	22
	4	4	4	4	3	3	
Системний адміністратор	ПВ4	М3	К3	З3	Ч3	Д3	19
	4	3	3	3	3	3	
	ПЗ4	М4	К4	З4	Ч4	Д4	24
	4	4	4	4	4	4	

Після зведення усіх даних 1-го варіанту в одну таблицю враховуючи дані з таблицею 2.9 отримаємо модель зовнішнього та внутрішнього порушника безпеки інформації, які внесені у таблицю 2.16.

Таблиця 2.16 – Модель зовнішнього та внутрішнього 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	Ч2	Д3	13
Бухгалтер	М1	К2	З1	Ч1	Д3	8
Менеджер	М1	К2	З1	Ч1	Д3	8
Інженер 1	М3	К3	З2	Ч3	Д3	16
Інженер 2	М3	К3	З2	Ч3	Д3	16

Продовження таблиці 2.16

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Системний адміністратор	М3	К3	З3	Ч3	Д3	19
Зовнішні порушники						
Наємний персонал	М3	К1	З1	Ч1	Д1	7
Хакери	М3	К3	З3	Ч4	Д3	16
Колишні робітники	М2	К3	З2	Ч2	Д3	12
Конкуренти	М3	К3	З3	Ч4	Д3	16

Згідно Таблиці 2.16 найбільшу загрозу, що має відношення до проблеми захисту інформації, становлять системний адміністратор та інженери. Роботу цього персоналу ніхто не контролює, тому необхідно найняти адміністратора безпеки, який буде контролювати їх роботу, оскільки вони є основними потенційними порушниками безпеки інформації.

2.7 Модель загроз для інформації в ІТС

Інформація яка циркулює в ІТС:

- робочий графік;
- зарплатні відомості;
- клієнтська база;
- особисті справи співробітників;
- бухгалтерські звіти;
- вхідні плани об’єктів замовників;
- вихідні плани об’єктів замовників;
- дані замовлень.

Опис моделі загроз (у частині, що стосується переліку можливих способів реалізації загроз та їх класифікації), має бути викладений настільки детально, щоб

дозволяти (на етапі аналізу ризиків, пов'язаних з реалізацією загроз для інформації в ІТС) однозначне визначення як збитків, що завдаються у випадку успішної реалізації загрози, так і ймовірності реалізації загрози (здійснення атаки) в певний спосіб. Потенційні загрози наведені у таблиці 2.17.

Таблиця 2.17 – Потенційні загрози

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
1. Загрози об'єктивної природи					
1.1.	Стихійні явища (пожежа, аварії)		+	+	+
1.2.	Збої та відмови системи електроживлення		+	+	
1.3	Збої, відмови та пошкодження носіїв інформації			+	
2. Загрози суб'єктивної природи					
2.1.1	Несанкціоноване підключення до технічних засобів	+	+		
2.1.2	Несанкціоноване підключення до каналів зв'язку(Wi-fi\LAN)	+	+		
2.1.3	Читання даних, що виводяться на екран, роздруковуються, читання залишених без догляду документів	+	+		
2.1.4	Несанкціоноване перехоплення інформації за рахунок витоку інформації за рахунок ПЕМВН	+			
2.1.5	Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу	+			
2.2	Порушення нормальних режимів роботи				
2.2.1	Зараження системи комп'ютерними вірусами		+	+	+
2.2.2	Втрата (розголошення) засобів розмежування доступу (паролів), магнітних носіїв інформації тарезервних копій	+	+	+	
2.2.3	Модифікація компонентів програмного та інформаційного забезпечення		+	+	+
2.2.4	Використання недозволеного програмного забезпечення або модифікація компонентів програмного та інформаційного забезпечення		+	+	+
2.2.5	Пошкодження носіїв інформації			+	
2.2.6	Вхід у систему недопущених осіб, які не мають допуску (подолання систем захисту)	+	+	+	
2.3	Помилки персоналу				
2.3.1	Отримання сторонньою особою інформації від персоналу ІТС	+			
2.3.2	Пошкодження носіїв персоналом ІТС			+	
2.3.3	Порушення технології обробки, введення та виведення інформації, роботи з МНІ (резервними копіями, еталонами та дистрибутивами)		+	+	

У відповідності до наведених даних, маємо більш конкретизований та детальний перелік актуальних суттєвих загроз інформації за їх антропогенними та техногенними факторами які наведені в таблиці 2.18.

Таблиця 2.18 – Суттєві загрози інформації

№	Опис загрози	Джерело	Вразливість	Можливі наслідки	Пору шення
Техногенні					
1	Раптові скачки напруги під час роботи ІТС	Зовнішнє	Відсутність приладів безперебійного живлення з системою вирівнювання напруги та аварійного електропостачання	Можлива втрата доступу до ПК працівників(при відключеній системи електроживлення або заміну комплектуючих, які вийшли з ладу) можливе тимчасове призупинення роботи та фінансові витрати	Д,Ц
2	Неможливість підключення до хмарного сховища	Зовнішнє	Збої в роботі інтернет мережі з боку провайдера в офісі, або проблеми з боку хмарного сховища	Втрата доступу до хмарного сховища	Д
Антропогенні					
3	Огляд на робочі місця директора та менеджера з вікон	Зовнішнє (конкуренти)	Не постійно закриті жалюзі, коли як з вікна видно монітор менеджера та директора і плани замовників або документів на столі директора	Конкуренти можуть використовують дрони або іншим способом, тому що офіс знаходиться на 3-ому поверсі	К

Продовження таблиці 2.18

№	Опис загрози	Джерело	Вразливість	Можливі наслідки	Порушення
4	Використовування точки доступу(Wi-Fi) у локальній мережі з вільним доступом до інтернету	Зовнішнє (конкуренти\ хакери)	Використання бездротової мережі(Wi-Fi) для власних потреб працівниками	Зловмисника можуть через бездротову мережу отримати доступ до локальної	К, Д, Ц
5	Використання зовнішніх накопичувачів працівників та клієнтів на ОІД	Внутрішні (працівники) Зовнішні (клієнти)	Недостатньо систематичному оновленні сигнатур антивірусного ПЗ на ПК працівників	На зовнішніх накопичувачах, можуть бути заражені вірусами або містити шкідливі для функціонування системи програмами\процесами, можливе тимчасове призупинення роботи	К, Д, Ц
6	Відкриття фішингового листу, або перехід по стороннім посиланням	Внутрішні (працівники)	Відсутності систематичного інструктажу працівників середньої кваліфікації	Втрата доступу\даних з ПК працівника, можливе тимчасове призупинення роботи та фінансові витрати	К, Д
7	Копіювання доступної інформації на зовнішні носії	Внутрішні (працівники)	Відсутності контролю за носіями інформації на ПК працівників	Створення копій інформації яка має обмежений доступ	К
8	Передача доступної інформації через електронні	Внутрішні (працівники)	Відсутності контролю за потоками інформації на ПК працівників	Передача копій інформації яка має обмежений доступ	К

	ресурси				

Продовження таблиці 2.18

№	Опис загрози	Джерело	Вразливість	Можливі наслідки	Порушення
9	Несанкціоно-ване встановлення додаткового ПЗ	Внутрішні (працівники)	Відсутності контролю за інсталяцією програм на ПК працівників	Можлива тимчасова зупинка роботи та фінансові витрати	К, Д, Ц
10	Крадіжка або заміна робочого носія інформації з ПК працівників	Внутрішні (працівники)	У відсутності контролю над діяльністю системного адміністратора при обслуговуванні	Можливі фінансові витрати при потраплянні ІзОД до конкурентів	К, Д
11	Підкупи або шантаж працівника\ів підприємства конкурента-ми	Внутрішні (працівники)	Відсутнє відповідальне лице за моніторингом дій через журнал аудиту або недостатньо замотивований робітник чи їх поганий підбір	Можливі фінансові витрати при потраплянні ІзОД до конкурентів	К

Для розрахунку суми суттєвих загроз, які представленні у таблиці 2.18 треба урахувати 3 рівні ризиків, збитків і порушень та занести їх у таблицю 2.19:

- 3 бали – якщо реалізація загрози надає великих збитків і порушень;
- 2 бали – якщо реалізація загрози надає помірних збитків і порушень;
- 1 бал – якщо реалізація загрози надає незначних збитків і порушень;

Таблиця 2.19 – Рівень загроз інформації

№	Рівень		Рівень			Сума загроз
	ризиків	збитків	К	Д	Ц	
1	1	2	1	2	2	8

2	1	1	1	1	1	5

Продовження таблиці 2.19

№	Рівень		Рівень			Сума загроз
	ризиків	збитків	К	Д	Ц	
3	2	2	2	1	1	8
4	2	2	3	3	2	12
5	2	2	3	1	2	10
6	1	1	1	1	1	5
7	1	2	2	1	1	7
8	1	2	2	1	1	7
9	2	2	1	2	2	9
10	2	3	3	3	2	13
11	1	2	2	2	2	9

Таким чином, найвищу суму небезпеки мають:

– використання точки доступу(Wi-Fi) у локальній мережі з вільним доступом до інтернету;

– крадіжка або заміна робочого носія інформації з ПК працівників;

– використання зовнішніх накопичувачів працівників та клієнтів на ОІД.

2.8 Вибір профілю захищеності

АС підприємства – це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу і відноситься до АС «3» класу. Для АС «3» класу обрано наступний профіль захищеності:

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

КД–2 – базова довірча конфіденційність. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КА–2 – базова адміністративна конфіденційність. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

КО–1 – Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КВ–1 – Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

ЦД–1 – Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Користувача і захищеного об'єкта користувача і захищеного об'єкта.

ЦА–2 – Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Користувача і захищеного об'єкта користувача і захищеного об'єкта.

ЦО–1 – Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

ЦВ–1 – 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.

ДР–1 – Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

ДВ–1 – 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.

НР–2 – КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

НИ–2 – Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути.

НК–1 – Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО–2 – Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора.

НЦ–2 – Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

НТ–2 – Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

НВ–1 – 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 [6].

2.9 Політика розмежування доступу

Мета політики:

Створення регламенту доступу користувачів до ресурсів обчислювальної системи.

Область дії:

Область дії політики розмежування доступу розповсюджується на всіх співробітників підприємства.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики розмежування доступом є системний адміністратор.

Політика безпеки:

Регламентовані цією політикою атрибути доступу мають бути призначені відповідним користувачам системним адміністратором з використанням вбудованих засобів розмежування доступу DeviceLock Endpoint DLP Suite.

Атрибути доступу, відповідно до посадових обов'язків користувачів, зазначені у таблиці 2.20 (пояснення до таблиці вказане після матриці доступу).

Таблиця 2.20 – Атрибути доступу

Користувач	Інформація	ПЗ
Системний адміністратор	1 – Ч 2 – Ч	10 – Вк, Вст, О, В 11 – Вк, Вст, О, В 12 – Вк, Вст, О, В 13 – Вст, О, В 14 – Вк, Вст, О, В 15 – Вк, Вст, О, В 16 – Вк, Вст, О, В 17 – Вст, О, В 18 – Вст, О, В
Менеджер	1 – Ч, З, К, М, Д, В 2 – Ч 3 – С, Ч, З, К, М, В 8 – С, Ч, З, К, М, В	10 – Вк 14 – Вк 15 – Вк 16 – Вк
Директор	1 –Ч 2 – С, Ч, З, К, М, Д, В 3 – С, Ч, З, К, М, Д, В 4 – Ч 5 – Ч 6 – С, Ч, З, К, М, Д, В	10 – Вк 13 – Вк 14 – Вк 15 – Вк 16 – Вк 17 – Вк

	7 – С, Ч, З, К, М, Д, В 8 – С, Ч, З, К, М, Д, В	
Інженер 1-2	1 – Ч 2 – Ч 6 – С, Ч, З, К, М, В 7 – С, Ч, З, К, М, В 8 – Ч	10 – Вк 13 – Вк 14 – Вк 15 – Вк 16 – Вк 17 – Вк

Продовження таблиці 2.20

Користувач	Інформація	ПЗ
Бухгалтер	1 – Ч 2 – Ч 4 – С, Ч, З, К, М, Д, В 5 – С, Ч, З, К, М, Д, В	10 – Вк 14 – Вк 15 – Вк 16 – Вк
Адміністратор безпеки	1 – Ч 2 – Ч 9 – С,Ч,З,К,М,Д,В.	10 – Вк 14 – Вк 15 – Вк 16 – Вк 18 – Вк

Перелік ПЗ та інформації:

1 робочий графік(інформація);

2 зарплатні відомості(інформація);

3 клієнтська база(інформація);

4 особисті справи співробітників(інформація);

5 бухгалтерські звіти(інформація);

6 вхідні плани об’єктів замовників(інформація);

7 вихідні плани об’єктів замовників(інформація);

8 дані замовлень(інформація);

9 журнал подій(інформація);

10 пакет Office 365 Business преміум (Word, Excel, PowerPoint, Outlook, SharePoint, OneDrive, OneNote, Microsoft Teams, Publisher, Access) (програмне забезпечення);

11 CCleaner ver 5.7(програмне забезпечення);

12 Norton 360(програмне забезпечення);

13 Cisco Packet Tracer(програмне забезпечення);

14 Viber(програмне забезпечення);

15 Microsoft One Drive(програмне забезпечення);

16 Microsoft EDGE(програмне забезпечення);

17 Arduino IDE(програмне забезпечення).

18. DeviceLock Endpoint DLP Suite(програмне забезпечення).

Для інформації:

- С – створення;
- Ч – читання;
- З – зберігання;
- К – копіювання;
- М – модифікація;
- Д – друк;
- В – видалення/знищення.

Для ПЗ:

- Вст – встановлення;
- Вк – використання ;
- О – оновлення;
- В – видалення/знищення.

Політика безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

2.10 Політика резервного копіювання

Мета політики:

Створення регламенту резервного копіювання технологічної інформації (тобто групових політик, конфігурацій ПЗ і т.д.) на підприємстві, для запобігання простою у роботі у разі збоїв та відмов.

Область дії:

Область дії політики резервного копіювання розповсюджується на системного адміністратора.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики резервного копіювання є системний адміністратор.

Політика безпеки:

При резервному копіюванні рекомендується використовувати декілька резервних копій, що будуть зберігатися на різних зовнішніх носіях. При додаванні резервної копії на знімний носій, вона заноситься до теки, ім'я якої повинно містити порядковий номер резервної копії та дату резервного копіювання.

Технологічну інформацію, конфігурації ПЗ і т.д. необхідно копіювати на окремі з'ємні носії, які має право використовувати лише системний адміністратор. Резервне копіювання цих даних має проводитися як мінімум раз на місяць.

Рекомендується для резервного копіювання та відновлення системи використовувати ПЗ «Veeam Backup & Replication», яке сумісне з засобами Active Directory. Засобами ПЗ «Veeam Backup & Replication» системний адміністратор повинен створити архів, що містить необхідну технологічну інформацію.

До технологічної інформації, що підлягає резервному копіюванню належать:

– групові політики;

– атрибути розмежування доступу;

– конфігурації ПЗ;

– дані про облікові записи.

Рекомендується проводити періодичний аналіз стану ПК працівників використовувати ПЗ «Viktoria» для перевірки стану жорстких дисків. У разі

виникнення підозри на можливість виникнення збоїв або відмов, системний адміністратор повинен провести позачергове резервне копіювання. У разі виникнення відмови у роботі носіїв інформації, з ПК знімається пломба системного адміністратора, замінюється носій з виконанням необхідного обсягу для подальшої роботи з обчислювальною технікою, після чого встановлюється нова пломба системного адміністратора. Сам носій, який відмовив у роботі, потрібно негайно фізично знищити задля унеможливлення відновлення даних які були в ньому.

Після проведення кожного резервного копіювання системний адміністратор повинен надати директору звіт із вказанням переліку технологічної інформації та дати резервного копіювання.

Оскільки деякі документи(робочий графік та зарплатні відомості) постійно завантажуються на хмарне сховище через ПК Директора, вони не потребують додаткового резервного копіювання.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює системний адміністратор підприємства. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

2.11 Політика використання доступу до Інтернет мережі

Мета політики:

Створення достатнього рівня інформаційної безпеки через введення правил і інструкцій для працівників для виконання своїх прямих обов'язків в мережі Інтернет.

Область дії:

Політика поширюється на співробітників підприємства, які використовують мережу Інтернет для виконання своїх прямих обов'язків. Дана політика безпеки не відміняє інші політики.

Відповідальні особи політики:

Відповідальною особою за виконання політики використання доступу до мережі Інтернет є кожний працівник підприємства.

Політика:

Якщо маршрутизатор, який з'єднує усі ПК має функцію точки доступу(WI-FI) то її необхідно негайно вимкнути, для запобігання підключення несанкціонованих пристроїв до мережі ІТС.

Доступ до мережі Інтернет виконувати лише через прив'язаного до працівника певного робочого місця в ІТС підприємства,

Використання мережі Інтернет можливо лише для:

– отримання та обробки замовлень;

– збору інформації задля виконання замовлень;

– збору, пошуку, обробок досліджень і розробок;

– пошуку інформації для актуалізації у фінансових, законодавчих питаннях, якщо вона безпосередньо стосується або відносяться для виконання посадових обов'язків.

Забороняється:

– проводити у різних іграх за комп’ютером у вільний час або під час роботи;

– використовувати будь-яку діяльність не від імені фірми;

– передавати будь-яку конфіденційну інформацію третім особам;

– виконувати заходи які проти кодексу ділової етики компанії, законодавства, політики або процедури підприємства;

– доступ до неавторизованої інформації і її копіювання;

– доступ до системи під іншим паролем.

Також використання електронної пошти, дошок оголошень, чат-кімнат в робочий час, на устаткуванні фірми і застосовуючи імена користувачів і паролі фірми в особистих цілях, для переговорів з друзями і членами сім'ї розглядається як експлуатація ресурсів компанії в особистих цілях і категорично забороняється. Жодних виключень не робиться з даного питання для обідніх перерв і неробочого часу.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

Порядок і періодичність перегляду

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

2.12 Політика чистого робочого місця

Мета політики:

Запобігання витоку, зміни та\або втрати ІзОД на робочій обчислювальній системі працівників.

Область дії:

Політика чистого робочого місця поширюється на співробітників підприємства, які використовують своє робоче місце.

Відповідальні особи політики:

Відповідальною особою за виконання політики чистого робочого місця є кожний працівник підприємства.

Політика:

Кожен працівник компанії має своє певне робоче місце з закріпленим ПК та технікою. Під час покидання робочого місця, працівник повинен заблокувати або вимкнути свій ПК. Якщо працівник збирається покидати робоче місце то повинен забирати усі свої технічні засоби (телефон, планшет, ноутбук тощо.), Уся інформація (електронна або паперова), яка підлягає утилізації, повинна бути знищена у найкоротші строки. Електронна інформація знищується за допомогою глубокого форматування носія, а паперова через шредер.

ІзОД, яка надходить з БФП, повинна негайно видалятися з нього. Паперова ІзОД або зовнішні носії з ним, в кінці робочого дня повинна бути схована у ящик або шкаф, які зачиняються на замок. Залишаючи місце роботи, працівник повинен тримати його у чистоті.

Усі логіни та паролі повинні видаватися системним адміністратором та зберігаються тільки за допомогою електронної пошти, задля мінімізації інформації на паперових носіях.

Забороняється:

Працівникам використовувати техніку або ПК, яка закріплена до іншого працівника компанії.

Доступ та використання ПК працівника.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

Порядок і періодичність перегляду

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

2.13 Політика застосування та використання паролів

Мета політики:

Встановлення норм та стандартів для створення сильних паролів з їх захистом, зберіганням та частотою їх зміни.

Область дії:

Політика поширюється на всіх співробітників підприємства, які використовують систему, обладнання, в якій так чи інакше використовує або надає доступ до ІзОД.

Відповідальні особи політики:

Відповідальною особою за виконання політики застосування та використання паролів є кожний працівник підприємства.

Політика:

Паролі системних облікових записів (адміністратора домену, локального адміністратора, root і т. Д.) повинні змінюватися кожні 4 місяці.

Всі паролі системних облікових записів, а також паролі додатків і активного обладнання необхідно зберігати в базі даних в зашифрованому вигляді, доступ до якої обмежений.

Термін дії паролів облікових записів домену повинен складати не більше 9 місяців. Рекомендований інтервал зміни пароля 6 місяців.

Пароль облікового запису користувача, який має адміністративні привілеї, отримані за допомогою членства в групі або за допомогою програм, повинен бути унікальний по відношенню до інших паролів облікових записів даного користувача.

Пароль отриманий користувачем, необхідно змінити при першому вході в систему.

Всі паролі користувачів, а також системні паролі повинні відповідати таким вимогам як:

- Включати поєднання букв верхнього та нижнього регістрів (наприклад, a-z, A-Z).

- Включає цифри і знаки пунктуації(наприклад, 0-9,! @ # $% ^ & * () _ + | ~ - = \ ` {} [[]]:«; '<>?,. /).

- Складається з восьми і більше символів.

- Не має бути словом на будь-якій мові, діалекті, сленгу, жаргоні і т.д.

- Не має бути заснований на персональній інформації, наприклад прізвища, дати народження і т.д.

Приклад сильного паролю: DL14n!U@KbR6

Забороняється:

Забороняється передача паролів користувачам за допомогою поштових повідомлень або іншим відкритим способом через Інтернет.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

Порядок і періодичність перегляду

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

2.14 Політика застосування антивірусного ПЗ

Мета політики:

Зменшення ризику зараження ІТС шкідливими програмними засобами.

Область дії:

Політика поширюється на всіх співробітників підприємства

Відповідальна особа:

Відповідальною особою за виконання політики доступу є системний адміністратор.

Політика:

Антивірусне ПЗ на всіх пристроях працівників повинно оновлюватися регулярно при постачанні нових версій продукту від його розробників системним адміністратором для збільшення бази сигнатур у ньому.

Сканування антивірусним ПЗ повинно проводитись щоденно на кожному ПК працівників. Усі зовнішні носії при підключенні до ІТС повинні бути скановані антивірусом задля запобігання зараженню шкідливими ПЗ. Також потрібно здійснювати перевірку усіх даних, одержані через мережу Інтернет.

Негайно сповістити системного адміністратора в випадках спрацьовування антивірусного ПЗ що встановлено на ПК. Негайно сповістити системного адміністратора при виникненні підозр на активність шкідливої програми, що виражається в нетиповій роботі, встановлених на ПК програм, поява графічних і звукових ефектів, викривлення даних, пропажі файлів і директорій, частій появі повідомлень про системні помилки, самостійних перезапусках операційної системи, «підвисання» та ін.

Відповідальність:

За невиконання цих правил полягає дисциплінарне покарання або сплата штрафу, розмір якого залежить від наявності та фатальності наслідків.

Порядок і періодичність перегляду

Політики безпеки переглядається раз на рік директором. У разі виникнення форс-мажорних ситуацій політика безпеки може бути переглянута раніше вказаного терміну.

2.15 Висновок

Під час виконання спеціального розділу було виконане обстеження об’єкту інформаційно-телекомунікаційної системи, враховуючи сферу діяльності та інформаційні потоки підприємства. Виходячи з цих даних, проаналізовано потенційні загрози та вразливості, розроблена модель порушника. Згідно отриманих даних сформовані основні елементи політики безпеки інформації для даної ІТС задля мінімізації втрат ресурсів компанії.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Одна з вагомих цілей захисту інформаційних ресурсів від загроз є мінімізація збитків через порушення інформаційної безпеки підприємства. Метою виконання економічних розрахунків кваліфікаційної роботи є обґрунтування доцільності запровадження запропонованих в роботі рішень.

Для виконання економічного розділу необхідно:

- розрахувати капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення та ін.;

- розрахувати річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

- визначити річний економічний ефект;

- визначити показники економічної ефективності.

3.1 Розрахунок витрат на впровадження політики безпеки

Спочатку, необхідно визначити трудомісткість розробки політики безпеки інформації.

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

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_в$ – тривалість розробки концепції безпеки інформації у організації;

$t_а$ – тривалість процесу аналізу ризиків;

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

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

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_д$ – тривалість документального оформлення політики безпеки. Таким чином трудомісткість розробки політики безпеки дорівнює:

$$t = 15+8+13+12+5+11+7$$

$$t = 71 \text{ год.}$$

Розрахуємо витрати на створення ПБ. Розрахунок проводиться за формулою 3.2:

$$K_{рп} = З_{зп} + З_{мч} \text{ грн.} \quad (3.2)$$

де $K_{рп}$ – витрати на створення політики безпеки;

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки;

$З_{мч}$ – вартість витрат машинного часу, що необхідні для створення ПБ. Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, годин;

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

Средньогодинна заробітна плата спеціаліста з інформаційної безпеки становить – 83 грн/год.

Відповідно до формули 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 71 \text{ год} \cdot 83 \text{ грн/год},$$

$$З_{зп} = 5893 \text{ грн}.$$

У свою чергу, витрати машинного часу визначаються за формулою 3.4:

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

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

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

Вартість 1 години машинного часу ПК визначається за формулою 3.5:

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

де P – встановлена потужність ПК, кВт;

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

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

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

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

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

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

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

$$C_{мч} = 0{,}5 \cdot 1 \cdot 1{,}57 + (14000*0{,}6)\backslash 1920 + (8700*0{,}4)\backslash 1920 \text{ грн},$$

$$C_{мч} = 6{,}97 \text{ грн.}$$

$$З_{мч} = 6{,}97*71=494{,}87 \text{ грн.}$$

Отже, витрати на створення ПБ за формулою 3.2 становлять:

$$K_{рп} = 494{,}87+5893= 6387{,}87 \text{ грн.}$$

В результаті розрахунків, вартість розробки ПБ становить – 6387,87 гривень.

Повна вартість капітальних витрат розраховується за формулою 3.6:

$$K = K_{рп} + K_{аз} + K_{зпз} + K_{пр} + K_{навч} + K_{н} \text{ грн.} \quad (3.6)$$

де $K_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн. Зовнішні консультанти не наймалися, тому даний коефіцієнт не враховується;

$K_{зпз}$ – вартість закупівлі ліцензійного основного й додаткового ПЗ, тис. грн. Були придбані 5 ліцензій на ПЗ DeviceLock вартість яких складає 10250 грн.

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

$K_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн. Було закуплено джерело безперебійного живлення LogicPower LPM-U1550VA у кількості трьох пристроїв які складають 10350 грн та пломби для опечатування, ціна яких 120 грн.

$K_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн. Технічні фахівці і обслуговуючий персонал не має потребі в навчанні або

курси для актуалізації знань у вільному доступі, тому даний коефіцієнт не враховується.

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Втрати на встановлення додаткового обладнання становлять 400 грн.

Таким чином, згідно з формулою 3.6:

$$K = 10250+10350+120+400+6388=27508 \text{ грн.}$$

3.2 Розрахунок поточних(експлуатаційних) витрат

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

Поточні витрати розраховуються за формулою 3.7:

$$C = C_a + C_з + C_е + C_{пз} \text{ грн,} \quad (3.7)$$

де $C_з$ – річний фонд заробітної плати інженерно-технічного персоналу;

$C_е$ – вартість електроенергії, що споживається апаратурою;

$C_{пз}$ – річні витрати на оновлення ліцензії ПЗ.

$C_а$ – річний фонд амортизаційних відрахувань. А саме придбане обладнання, яке складається з трьох пристроїв джерела безперебійного живлення в загальній сумі на 10350 грн. Мінімальний термін амортизації 2 роки, тому річний фонд складає:

$$C_а = 10350 / 2 = 5175 \text{ грн.}$$

У свою чергу, витрати на заробітну плату інженерно-технічного персоналу розраховуються за формулою 3.8:

$$C_з = З_{осн} + З_{дод1} \text{ грн}, \quad (3.8)$$

де $З_{осн}$ – основна заробітна плата працівника з інформаційної безпеки складає 7800 грн і відповідно 93600 грн на рік, але підприємство потребує спеціаліста на 0,5 ставки;

$З_{дод1}$ – додаткова заробітна плата яка складає 10% від основної заробітної плати;

За формулою 3.8 можна розрахувати:

$$C_з = (93600 + 9360) \cdot 0{,}5 = 51480 \text{ грн.}$$

Річні витрати на поновлення ліцензії складаються з замовленням Norton 360 Deluxe на 1 рік для 5 ПК (800 грн) та DeviceLock Endpoint DLP Suite на 1 рік (10250 грн).

Загалом, річні витрати на поновлення ліцензії ПЗ становлять:

$$C_{пз} = 11050 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою становить розраховують за формулою 3.9:

$$C_е = P \cdot F_р \cdot Ц_е, \text{ грн} \quad (3.9)$$

де P – встановлена потужність апаратури інформаційної безпеки яка на 5 ПК працівників складає 2,5 кВТ ;

F_p – річний фонд робочого часу системи інформаційної безпеки складає 1920 год;

$Ц_е$ – тариф на електроенергію який складає 1,57 грн/кВт годин

$$C_е = 2,5 \cdot 1920 \cdot 1,57 = 7536 \text{ грн.}$$

Отже повна вартість річних експлуатаційних витрат становить:

$$C = 7536 + 11050 + 5175 + 51480 = 75241 \text{ грн.}$$

Таким чином повна вартість річних експлуатаційних витрат становить 75241 грн.

3.3 Розрахунок витрат при виникненні загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї. Для подальших розрахунків потрібно знати загальну суму заробітної плати працівників обслуговування та співробітників підприємства, місячна плата яких зазначена в таблиці 3.1.

Таблиця 3.1 – Заробітна плата працівників підприємства

Посада	Розмір заробітної плати в місяць, грн
Директор	18000
Інженер 1	10000
Інженер 2	10000
Бухгалтер	8000
Системний адміністратор	5000
Адміністратор безпеки	4700

Менеджер	8000

Загальна сума заробітних плат співробітників підприємства становить 54000 грн. Загальна сума заробітних плат працівників обслуговування становить 9700 грн.

Необхідні вхідні данні для розрахунку:

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.10:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки становить 3 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу становить 1 година;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі становить 2 години;

$З_о$ – заробітна плата співробітників обслугованого персоналу, 9700 грн/місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 54000 грн/місяць;

$Ч_о$ – чисельність обслугованого персоналу 2 особи.

$Ч_с$ – чисельність співробітників атакованого вузла 5 осіб.

$О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік становить 1500000 грн;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 3000 грн;

$І$ – число атакованих вузлів або сегментів корпоративної мережі становить 5;

N – середнє число атак на рік 8.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі яка розраховується формулою 3.10 становить:

$$U = П_п + П_в + V \text{ грн}, \quad (3.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

$П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

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

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки які використовуються у формулі 3.11:

$$П_п = \frac{\sum З_с \cdot Ч_с}{F} \cdot t_п \text{ грн}, \quad (3.11)$$

де F – місячний фонд робочого часу при 1920 годинам на рік це 160 годин на місяць;

$$П_п = ((54000 \cdot 5/160)) \cdot 3 = 5062{,}5 \text{ грн}.$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових які використовуються у формулі 3.12:

$$П_в = П_{ви} + П_{пв} + П_{зч} \text{ грн}, \quad (3.12)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

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

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

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$ які використовуються у формулі 3.13:

$$П_{ви} = \frac{\sum З_С \cdot Ч_С}{F} \cdot t_{ви} \text{ грн}, \tag{3.13}$$

$$П_{ви} = ((54000 \cdot 5/160)) \cdot 2 = 3375{,}5 \text{ грн}.$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_В$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів) які використовуються у формулі 3.14:

$$П_{пв} = \frac{\sum З_О \cdot Ч_О}{F} \cdot t_в \text{ грн}, \tag{3.14}$$

$$П_{пв} = ((9700 \cdot 2/160)) \cdot 1 = 121{,}25 \text{ грн}.$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі які використовуються у формулі 3.15:

$$V = \frac{О}{F_r} \cdot (t_п + t_в + t_{ви}) \text{ грн}, \tag{3.15}$$

де F_r – річний фонд робочого часу.

$$V = 1500000 / 1920 \cdot (3 + 1 + 2) = 4687{,}5 \text{ грн.}$$

Отже упущена вигода згідно формули 3.12 становить:

$$П_в = 3375{,}5 + 121{,}25 + 3000 = 6496{,}75 \text{ грн.}$$

Отже упущена вигода згідно формули 3.10 становить:

$$U = 5062{,}5 + 4687{,}5 + 6496{,}75 = 16248{,}75 \text{ грн.}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі організації розраховується за формулою 3.16.

$$В = \sum_i \sum_n U. \quad (3.16)$$

$$В = 5 \cdot 8 \cdot 16248{,}75 = 649\,950 \text{ грн.}$$

3.4 Визначення та аналіз показників економічної ефективності

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою 3.17:

$$E = B \cdot R - C \text{ грн}, \quad (3.17)$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці яка складає 0,4;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн. Отже, економічний ефект становить:

$$E = 649\,950 \cdot 0{,}4 - 75241 = 184739 \text{ грн.}$$

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (ТСО) не використовується, оскільки було визначено величину відверненого збитку;

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.18:

$$ROSI = \frac{E}{K}, \text{ частки одиниці} \qquad (3.18)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, 24958 грн.

Таким чином,

$$ROSI = 184739 / 27508 = 6{,}72.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.19:

$$T_O = \frac{E}{K} = \frac{1}{ROSI} = 0{,}15 \text{ року.} \qquad (3.19)$$

3.5 Висновок

Під час виконання економічної частини проведені основні розрахунки капітальних витрат на внесення основних елементів політики безпеки інформації, щоб визначити доцільність їх впровадження.

А саме під час підрахунків було визначено, що:

1. Капітальні витрати на впровадження на експлуатацію політики безпеки інформації становить 27508 грн.

2. Повна вартість річних експлуатаційних витрат становить 75241 грн.

3. Загальний збиток від атаки складатиме 649 950 грн.

4. Загальний ефект від впровадження системи інформаційної безпеки становить 184739 грн.

5. Термін окупності капітальних інвестицій складає 0,15 року.

Отже дані які були отримані в ході виконання економічної частини, вказують на доцільність впровадження розроблених елементів політики безпеки.

ВИСНОВКИ

Об’єкт розробки кваліфікаційної роботи є інформаційно телекомунікаційна система ТОВ «СмартХоумЮА».

Під час виконання першого розділу кваліфікаційної роботи вирішений загальний стан питання щодо необхідності захисту інформації у підприємствах включаючи і підстави до створення КСЗІ. Була розглянута політика безпеки, а саме доцільність її розробки, види та загальний опис, пов’язаний з впровадженням її у будь-яке середовище, де необхідний захист інформації. Також наведені основні відомості щодо нормативно-правової бази яка використовується для забезпечення захисту інформації.

В ході виконання другого розділу було виконане обстеження об’єкту інформаційно-телекомунікаційної системи та проаналізовані особливості обробки інформації в ній. Через отримані результати визначені потенційні загрози та вразливості і була розроблена модель порушника. Відповідно отриманих даних сформовані основні елементи політики безпеки такі як політика розмежування доступу, відвідування території підприємства сторонніми особами, резервного копіювання, чистого робочого столу, застосування та використання паролів і застосування антивірусного ПЗ.

Виконання економічного розділу підтвердило доцільність впровадження розроблених елементів політики безпеки через отримані дані. До цих даних відносяться розрахунки щодо капітальних витрат на введення в експлуатацію ПБ, річних експлуатаційних витрат, загальний ефект після впровадження розроблених елементів ПБ та період окупності даних інвестицій на засоби захисту.

ПЕРЕЛІК ПОСИЛАНЬ

1 Завгородний В. И. Комплексная система защиты в компьютерных системах: Учебное пособие. - М. : Логос; ПБОЮЛ Н. А. Егоров, 2001. – 264 с.

2 ДСТУ ISO/IEC 27001:2015 [Електронний ресурс] // ДСТУ. – 2015. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910

3 ДСТУ ISO/IEC 27002:2015 [Електронний ресурс] // ДСТУ. – 2015. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911

4 ДСТУ ISO/IEC 27005:2019 [Електронний ресурс] // ДСТУ. – 2019. – Режим доступу до ресурсу:http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

5 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу " [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-002-99.pdf.

6 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-004-99.pdf.

7 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 28.04.1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/2.5-005%20-99.pdf

8 НД ТЗІ 1.6-005-2013 "Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.6-005-2013.pdf

9 НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf

10 Закон України "Про інформацію" [Електронний ресурс] // 2657-XII. – 16.07.2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

11 Закон України "Про державну таємницю" [Електронний ресурс] // 3855-XII. – 24.10.2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/3855-12#Text

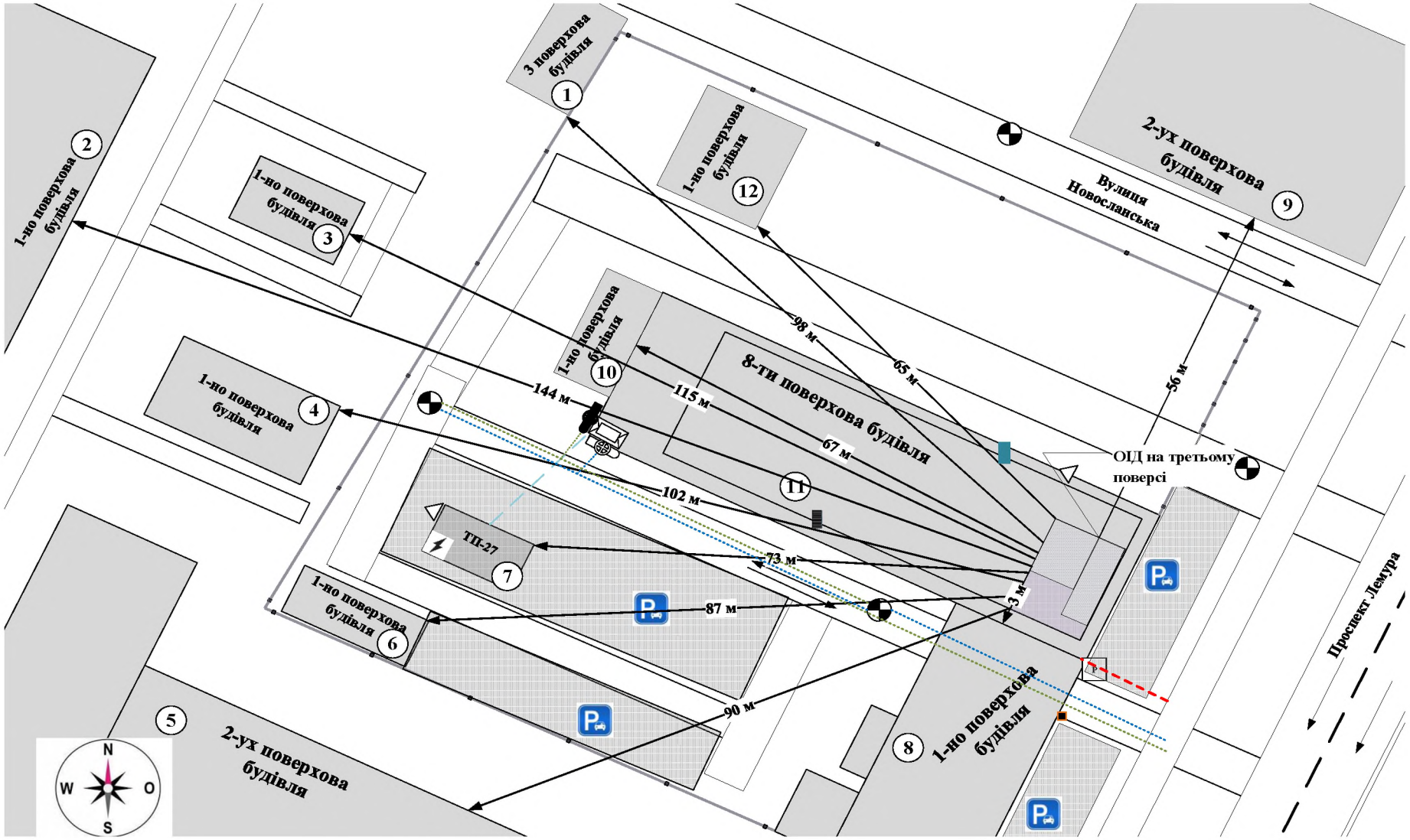
12 Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герас іна, Д.С. Тимофєєв, О.В. Кру чінін , Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. –47 с.

13 Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка» , 2019. – 16с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

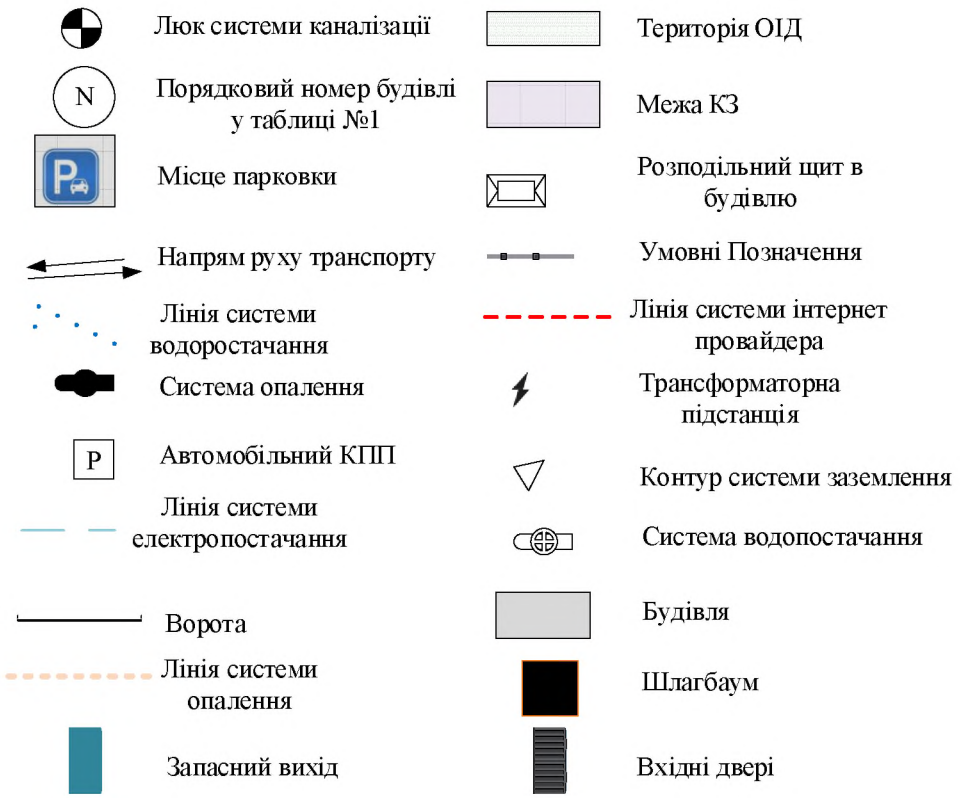
№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	4	
2	А4	Список умовних позначень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	10	
6	А4	Спеціальна частина	41	
7	А4	Економічна частина	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	3	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	
16	А4	Додаток Є	1	

ДОДАТОК Б. Ситуаційний план ОІД

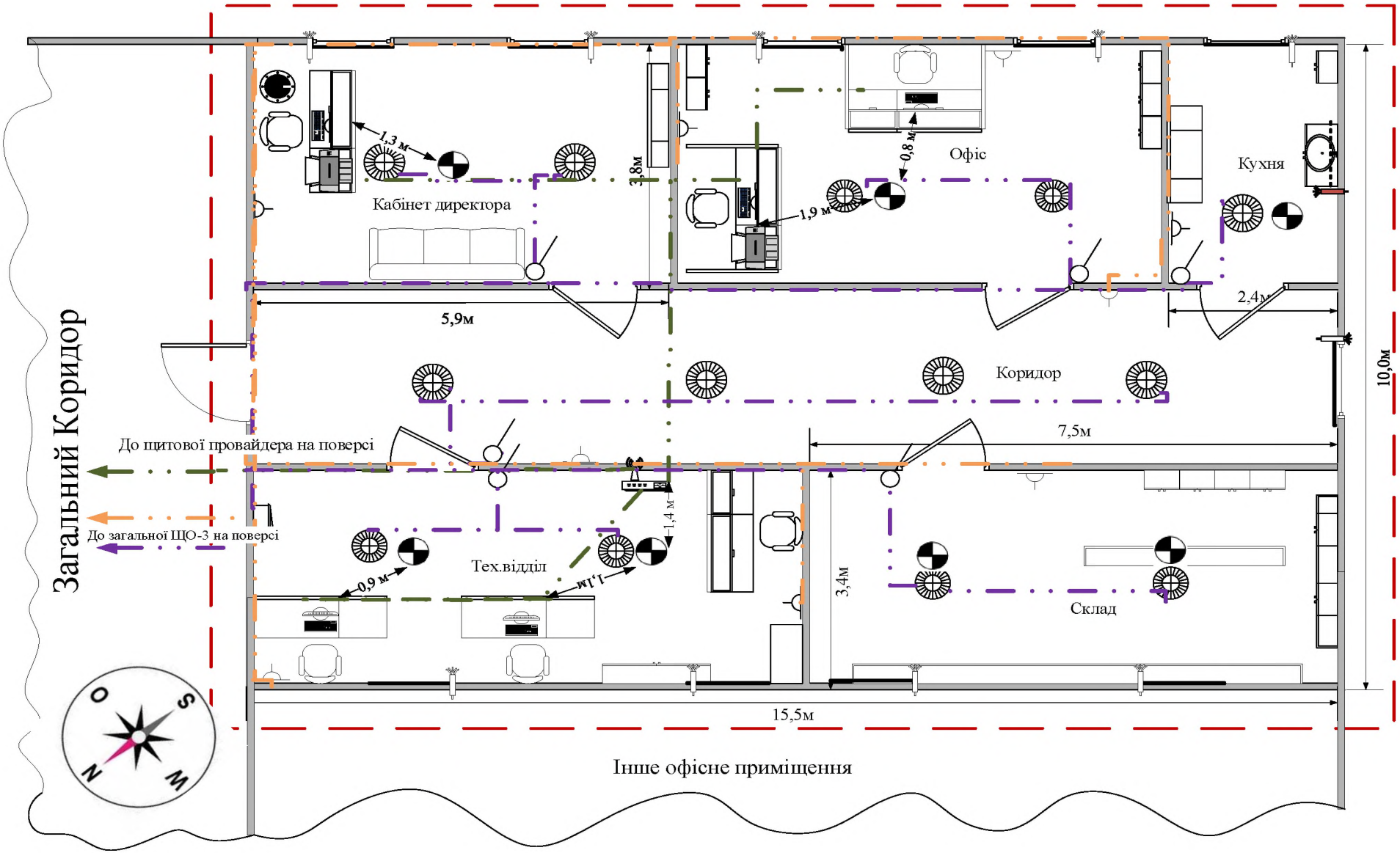


Масштаб 1:100

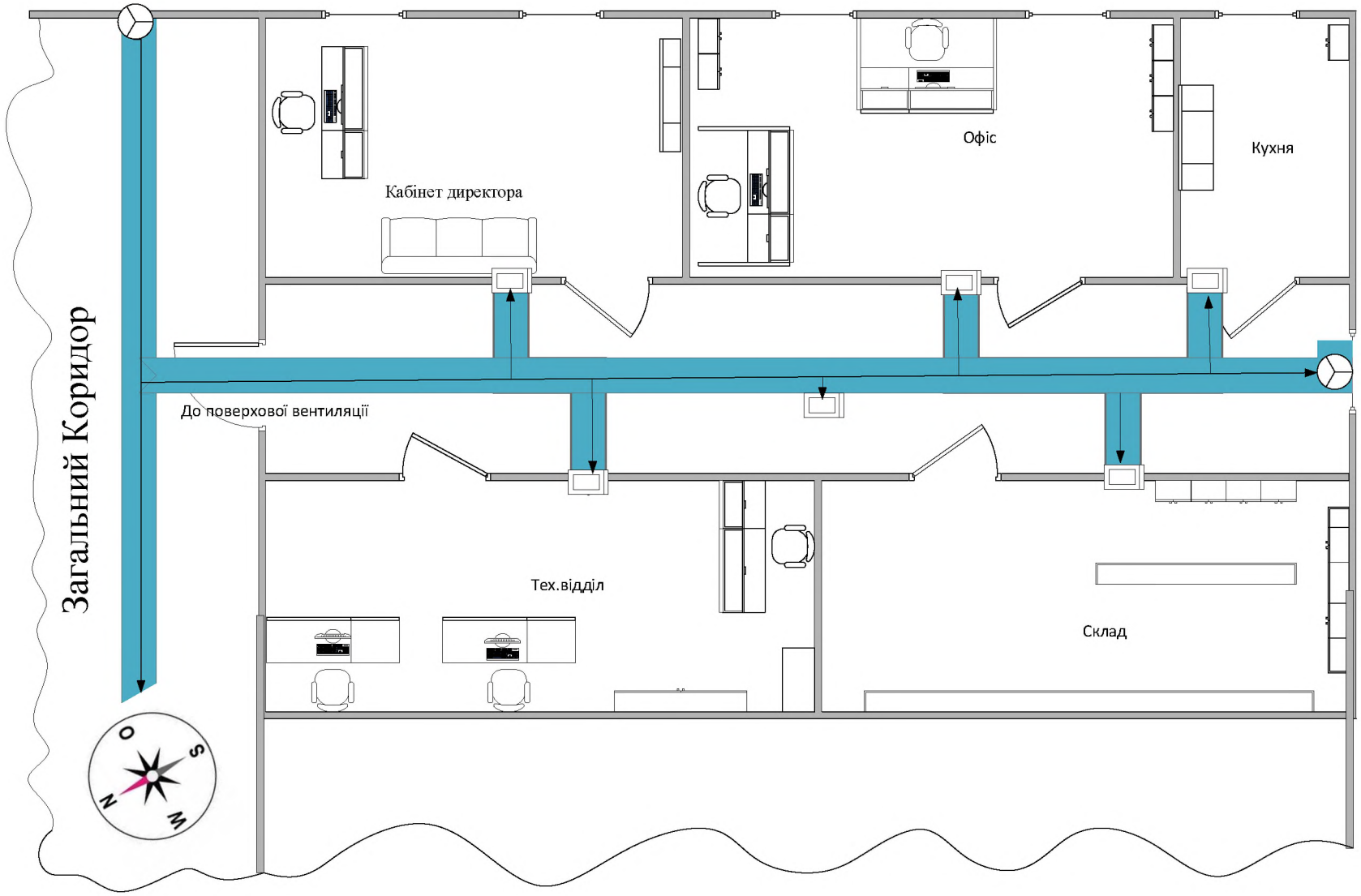
Умовні позначення до Ситуаційного плану:



ДОДАТОК В Генеральний план та план вентиляції ОІД



План Вентиляції ОІД:



Умовні позначення до Генерального плану і плану вентиляції:


Батарея опалення

Зона ОІД


Лінія системи водопостачання


Лінія системи освітлення


Пожежний сповіщувач


Стояк Зливу-подачі води


Сейф


БФП


Шахта вентиляції

Напрям руху повітря


Маршрутизатор и точка доступу


Елемент системи електропостачання


Елемент системи освітлення


Лінія системи електропостачання

Стояк Системи опалення

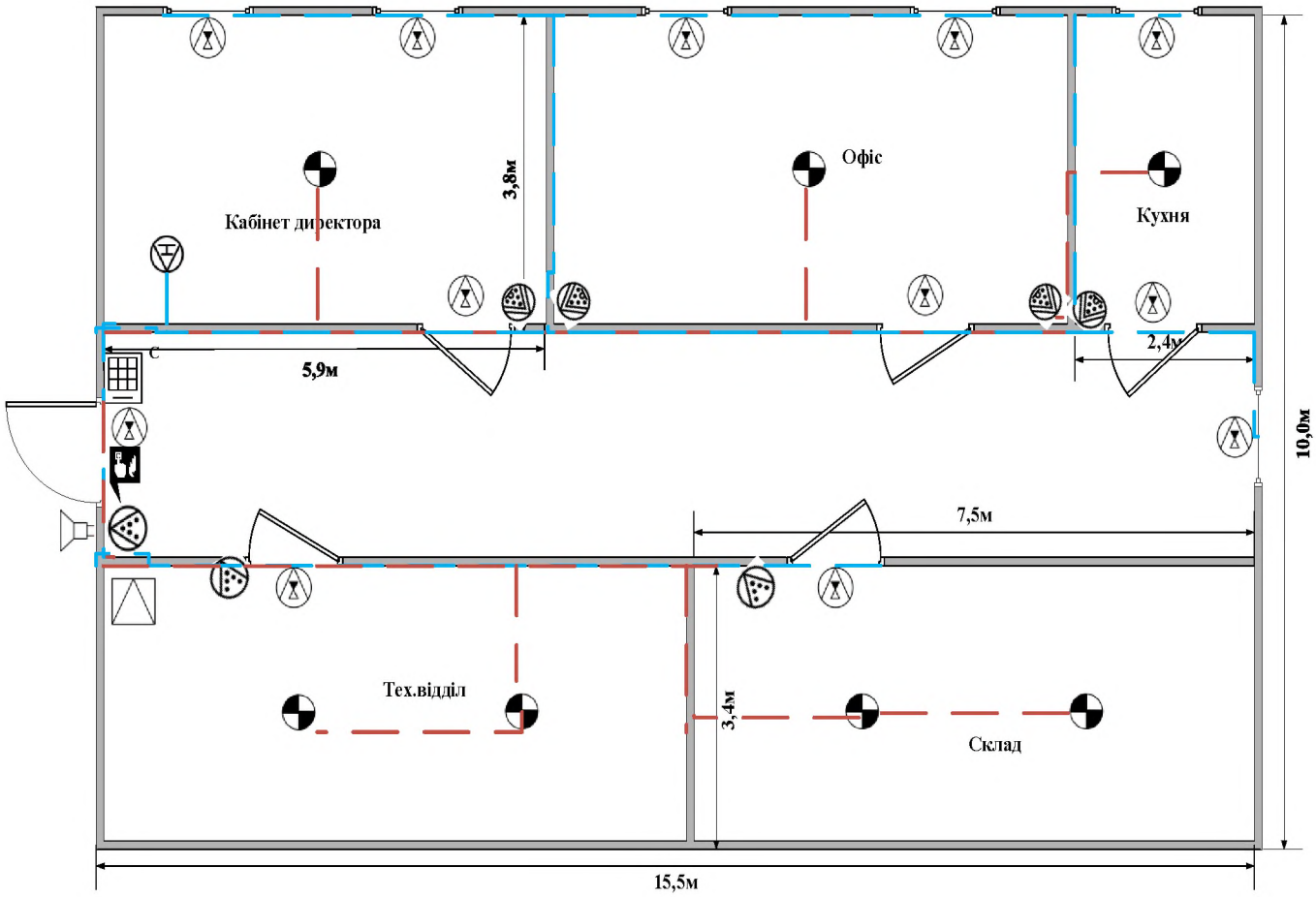

Електрична щитова №12


Лінія системи мережевого з’єднання


Решітка вентиляційної шахти


Продовження вентиляційної шахти на поверх вище

ДОДАТОК Г. План системи охоронно-пожежної сигналізації



Умовні позначення

- Пожежний димовий сповіщувач
- Магнітоконтактний сповіщувач
- Скомбінований (ІЧ+акустичний) сповіщувач
- Об'ємний інфрачервоний сповіщувач
- Лінії постачання пожежних сповіщувачів
- Лінії постачання охоронних сповіщувачів
- Тревожна кнопка
- Пожежна кнопка
- Світлошумовий сповіщувач
- ПКП
- С Клавіатура

ДОДАТОК Д. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

Петренко_С.Ю._125-18ск-1.docx

Петренко_С.Ю._125-18ск-1.pptx

ДОДАТОК Е. Відгук керівника економічного розділу

Відгук керівника економічного розділу:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Є. Відгук керівника кваліфікаційної роботи

Відгук керівника кваліфікаційної роботи:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)