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

Інститут електроенергетики Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента **Циватого Дениса Олександровича**
академічної групи *125-18ск-1*
спеціальності *125 Кібербезпека*
спеціалізації[1]
за освітньо-професійною програмою *бакалавр*

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ФОП «Devcorp»***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Флоров С.В.			
розділів:	ст. викл. Начовний І.І.			
спеціальний	.			
економічний	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 ***Циватому Денису Олександровичу*** **академічної групи** ***125-18ск-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***125 Кібербезпека***
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ФОП «Devcorp»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021р. № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	*Стан питання. Постановка задачі*	20.05.2021
Розділ 2	*Обстеження інформаційно-телекомунікаційної системи. Аналіз загроз та вразливостей. Аналіз стану захищеності інформаційно-телекомунікаційної системи приватного підприємства ФОП "Devcorp" Розробка політики безпеки інформації.*	25.05.2021
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	16.06.2021

Завдання видано: _____ Начовний І.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.05.2021.

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання: _____ Циватий Д.О
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 74 ст., 2 рис., 14 табл., 8 додатків, 14 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи ФОП “Devcorp”

Мета проекту: підвищення рівня захищеності інформації в інформаційно-телекомунікаційної системи ФОП “Devcorp”

У першому розділі проведений аналіз нормативно–правової бази у сфері захисту інформації, озвучено стан загроз захисту інформації безпосередньо на об’єкті, також вказані підстави та етапи створення КСЗІ та ПБ.

У другому розділі була описана необхідність створення комплексної системи захисту інформації, опис сфери діяльності підприємства, виконаний акт обстеження об’єкту інформаційної діяльності. Під час виконання другого розділу був проведений аналіз загроз та вразливостей, згідно із отриманими даними були розроблені елементи політики безпеки інформації, які направлені на мінімізацію загроз втрат важливих ресурсів компанії

В економічній частині проведений розрахунок капітальних витрат на впровадження створених елементів політик безпеки інформації.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки ФОП “Devcorp”, які підвищать рівень захисту інформації.

ПОЛІТИКА БЕЗПЕКИ, ВРАЗЛИВОСТІ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, АНАЛІЗ РИЗИКІВ

РЕФЕРАТ

Пояснительная записка: 74 с., 2 рис., 14 табл., 8 приложений, 14 источников.

Объект разработки: политика безопасности информации информационно телекоммуникационной системы ФОП "Devcorp"

Цель проекта: повышение уровня защищенности информации в информационно-телекоммуникационной системы ФОП "Devcorp"

В первой главе проведен анализ нормативно-правовой базы в сфере защиты информации, озвучено состояние угроз защиты информации непосредственно на объекте, также указаны основания и этапы создания КСЗИ и ПБ.

Во втором разделе была описана необходимость создания комплексной системы защиты информации, описание сферы деятельности предприятия, выполненный акт обследования объекта информационной деятельности. Во время выполнения второго раздела был проведен анализ угроз и уязвимостей, согласно полученным данным были разработаны элементы политики безопасности информации, направленных на минимизацию угроз потерь важных ресурсов компании

В экономической части произведен расчет капитальных затрат на внедрение созданных элементов политик безопасности информации.

Практическое значение проекта заключается в повышении уровня информационной безопасности ФЛП "Devcorp", которые повысят уровень защиты информации.

ПОЛИТИКА БЕЗОПАСНОСТИ, УЯЗВИМОСТИ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, АНАЛИЗ РИСКОВ

ABSTRACT

Explanatory note: 74p., 2 fig., 14 tables,8applications,14 sources.

Object of elaboration: information security policy of information and telecommunication system of PE "Devcorp"

The purpose of the project: to increase the level of information security in the information and telecommunication system of PE "Devcorp"

The first section analyzes the regulatory framework in the field of information protection, voices the state of threats to information protection directly at the site, as well as the grounds and stages of creation of complex information security systems and security policy.

The second section described the need to create a comprehensive system of information protection, a description of the scope of the enterprise, the act of inspection of the object of information activities. During the implementation of the second section, an analysis of threats and vulnerabilities was carried out, according to the obtained data, elements of information security policy were developed, which are aimed at minimizing the threat of loss of important company resources.

In the economic part, the calculation of capital costs for the implementation of the created elements of information security policies.

The practical significance of the project is to increase the level of information security of PE "Devcorp", which will increase the level of information protection.

SECURITY POLICY, VULNERABILITIES, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, OBJECT OF INFORMATION ACTIVITY, RISK ANALYSIS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДСТУ – державний стандарт України;

ЕОМ – електронно-обчислювальна машина;

ЗУ – закон України;

ІБ – інформаційна безпека;

ІТС – інформаційно-телекомунікаційна система;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

НДТЗІ – нормативний документ в галузі технічний захист інформації.

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЕМВ – побічне електромагнітне випромінювання;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПЗП – постійний записуючий пристрій.

СКУД – система контролю та управління доступом;

СУБД – система управління базами даних;

ФОП – фізична особа-підприємець;

ЗМІСТ

ВСТУП

Політика безпеки - це сукупність норм і правил, що визначають прийняті в організації заходи щодо забезпечення безпеки інформації, пов'язаної з діяльністю організації. Тільки людина, яка чітко усвідомлює цілі організації і умови її функціонування, може визначити, яку інформацію необхідно захищати і наскільки істотними можуть стати втрати від несанкціонованого поширення, спотворення або руйнування інформації.

Широке поширення обчислювальної техніки як засобу обробки інформації привело до інформатизації суспільства і появи принципово нових інформаційних технологій.

Різноманіття умов, що сприяють неправомірному оволодінню конфіденційною інформацією, викликає необхідність використання не менш різноманітних способів, сил і засобів для забезпечення інформаційної безпеки.

Всі системи і електронні мережі підпадають під загальне визначення "систем промислової автоматики і контролю" (IACS). Під терміном безпеку IACS розуміється запобігання незаконного або небажаного проникнення, навмисного або ненавмисного втручання в штатну і заплановану роботу, або отримання неналежного доступу до інформації, що захищається. Кібербезпека поширюється на комп'ютери, мережі, операційні системи, програми та інші програмовані конфігуруються компоненти системи IACS.

Дотримання основних вимог інформаційної безпеки (ІБ) дає можливість зберігати в недоторканності фізичні та цифрові дані, що захищаються від розкриття, використання (в тому числі модифікації), верифікації або повного (часткового) знищення, тобто повністю від несанкціонованого доступу до неї.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Безпека інформації - це стан інформації, інформаційних ресурсів та інформаційних систем, при якому з необхідною імовірністю забезпечується захист інформації (даних) від витоку, розкрадання, втрати, несанкціонованого знищення, модифікації (підробки), копіювання, блокування інформації

Для захисту різних видів інформації розробляється комплексна система захисту інформації та політика безпеки інформації.

Метою кваліфікаційної роботи є виконання обстеження для пошуку та виявлення вразливостей в інформаційній системі ОІД. А також складення політик безпеки та техніко-економічне обґрунтування доцільності впровадження розроблених ПБ.

Дуже важливим є створення політики інформаційної безпеки для створюваної інформаційної системи з урахуванням вже функціонуючих об'єктів інформаційного простору організації і самої інформаційної мережі, включаючи апаратне, програмне і мережеве забезпечення. Це пов'язано з тим, що при впровадженні системи в експлуатацію, не можна допустити порушення створеного і підтримуваного в організації рівня інформаційного захисту та, безумовно, необхідно забезпечити захист інформації для створюваної ІС.

Тому була прийнята правова основа політики, так як законодавчий рівень передбачає розробку і впровадження в практику законодавчих, підзаконних та інших нормативних актів, що регламентують питання інформаційної безпеки в автоматизованих системах на державному рівні.

Організаційний рівень передбачає розробку і контроль виконання комплексів заходів з підтримки режиму інформаційної безпеки конкретних автоматизованих систем. Основним завданням організаційного рівня

забезпечення інформаційної безпеки є вироблення комплексної політики безпеки, організація її ефективної реалізації на об'єктах автоматизації. Стосовно до персоналу, що працює з автоматизованими системами, політика безпеки повинна обов'язково містити комплекси внутрішніх нормативних, організаційних і операційних регуляторів, що включають в себе методи підбору і розстановки кадрів, їх підготовки і підвищення кваліфікації, забезпечення дисципліни. Організаційний рівень в обов'язковому порядку повинен включати в себе заходи з фізичного захисту приміщень та обладнання від загроз різної природи, а також деякі інші.

1.2 Аналіз нормативно-правової бази у сфері інформаційної безпеки

Нижче наводиться список законодавчих актів, нормативно-правових актів та нормативних актів щодо інформаційної безпеки в Україні.

1. Закони України:

1.1 Закон України «Про інформацію» від 02.10.1992 № 2657-XII

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

1.2 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

1.3 Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

1.4 Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

2. Постанови КМУ:

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

Ці Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

2.2 Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736

Ця Інструкція визначає єдині вимоги до ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації (далі - документи), що містять службову інформацію, зібрану під час провадження оперативно-розшукової, контррозвідувальної діяльності, діяльності у сфері оборони держави, та іншу службову інформацію, в органах державної влади, інших державних органах,

3. Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

3.1 НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі

Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах (далі - ІТС) - порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

3.2 Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ).

Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

3.3 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі

Цей нормативний документ системи технічного захисту інформації встановлює вимоги до структури та змісту нормативного документу, що регламентує діяльність служби захисту інформації в автоматизованій системі - “Положення про службу захисту інформації в автоматизованій системі”.

НД ТЗІ призначений для суб’єктів відносин діяльність яких пов’язана з обробкою в автоматизованих системах інформації, що підлягає захисту згідно з нормативно-правовими актами, а також для розробників комплексних систем захисту інформації в автоматизованих системах.

Використання цього НД ТЗІ створює умови для запровадження єдиного підходу щодо визначення і формування завдань, функцій, структури, повноважень служби захисту інформації, а також організації її робіт з захисту інформації впродовж всього життєвого циклу автоматизованих систем в державних органах, на підприємствах, в установах та організаціях усіх форм власності.

3.4 НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ (далі — Критерії) — установлює критерії оцінки захищеності інформації, оброблюваної 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).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

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

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

Цей документ призначений для постачальників , споживачів , автоматизованих систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації (інформації, яка потребує захисту), а також для державних органів, які здійснюють функції контролю за обробкою такої інформації.

Мета цього документа — надання нормативно-методологічної бази для вибору і реалізації вимог з захисту інформації в автоматизованій системі.

3.6 НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2

Цей документ визначає вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 і установлює згідно з визначеними НД ТЗІ 2.5-004 специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їх реалізації у комплексах засобів захисту інформації (стандартний функціональний профіль захищеності).

Мета цього документа – надання нормативно-методологічної бази під час розроблення комплексів засобів захисту від НСД до конфіденційної інформації, яка обробляється в АС класу 2, створення комплексної системи захисту інформації в установі (організації), проведення аналізу та оцінки захищеності інформації від несанкціонованого доступу в системах такого класу, а також рекомендацій для визначення необхідного функціонального профілю захищеності інформації в конкретній АС.

3.7 НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу

Цей нормативний документ системи технічного захисту інформації встановлює вимоги до технічних та організаційних заходів захисту інформації WEB-сторінки в мережі Інтернет.

Згідно з визначеними НД ТЗІ 2.5-004-99 специфікаціями він встановлює мінімально необхідний перелік послуг безпеки інформації та рівнів їх реалізації у комплексах засобів захисту інформації WEBсторінки від несанкціонованого доступу.

Мета цього НД ТЗІ – надання нормативно-методологічної бази для розроблення комплексу засобів захисту від несанкціонованого доступу до інформації WEB-сторінки під час створення комплексної системи захисту інформації.

3.8 НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі

Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, призначеній для оброблення, зберігання і передачі інформації з обмеженим доступом або інформації, захист якої гарантується державою

3.9 НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу

Цей нормативний документ (НД ТЗІ) встановлює єдині вимоги до порядку створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу (НСД) в комп'ютерних системах та захищених від несанкціонованого доступу компонентів обчислювальних систем (далі – засоби ТЗІ).

Дія НД ТЗІ поширюється на апаратні, програмні та програмно-апаратні засоби ТЗІ, призначені для використання в комп'ютерних системах, де

обробляється, накопичується, зберігається та передається інформація, що підлягає технічному захисту.

3.10 Автоматизовані системи. Вимоги до змісту документів РД 50-34.698

Методичні вказівки поширюються на автоматизовані системи (АС), що використовуються в різних сферах діяльності (управління, дослідження, проектування), Включаючи їх поєднання, і встановлюють вимоги до змісту документів, що розробляються при створенні АС.

3.11 Технічне завдання на створення автоматизованої системи. ДСТУ 34.602-89

Стандарт поширюється на автоматизовані системи (АС) для автоматизації різних видів діяльності (управління, проектування, дослідження і т. п.), включаючи їх поєднання, і встановлює склад, зміст, правила оформлення документа «Технічне завдання на створення (розвиток або модернізацію) системи »(далі - ТЗ на АС).

3.12 НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

Цей нормативний документ технічного захисту інформації (НД ТЗІ) визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

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

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

- оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

1.3 Види інформації. Порядок доступу до інформації

Для побудови КСЗІ та створення ПБ важливо спочатку чітко зрозуміти, що таке інформація і яка вона буває.

Відповідно до інформація - будь-які дані, які можна зберігати на фізичному носії або відображати в електронному вигляді.

Відповідно до наказу про доступ, інформація поділяється на відкриту та обмежену інформацію. Будь-яка інформація є відкритою, крім випадків, передбачених законодавством щодо обмеженого доступу до інформації

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація .

Конфіденційність - це інформація про фізичну особу, а також інформація про те, що доступ обмежно фізичною або юридичною особою, за винятком досліджень з питань влади. Конфіденційна інформація може розповсюджуватися на прохання (згоду) зацікавленої особи у встановленому нею порядку відповідно до встановлених нею умов, а також в інших випадках, визначених законом .

Порядок отримання інформації, перелік користувачів та їх повноваження щодо цієї інформації визначається власником інформації. Порядок доступу до державних інформаційних ресурсів чи інформації з обмеженим доступом, вимоги до захисту, встановлені законом, перелік користувачів та їх повноваження стосовно цієї інформації, визначаються законом. У випадках, передбачених законом, доступ до інформації в системі може бути здійснений без згоди її власника в порядку, встановленому законом.

1.4 Підстави створення КСЗІ

Головна мета створення системи захисту інформації - її надійність. Система ЗІ(захисту інформації) - це організована сукупність об'єктів і суб'єктів ЗІ, використовуваних методів і засобів захисту, а також здійснюваних захисних заходів.

Але компоненти ЗІ, з одного боку, є складовою частиною системи, з іншого - самі організовують систему, здійснюючи захисні заходи.

Оскільки система може бути визначена як сукупність взаємопов'язаних елементів, то призначення СЗІ полягає в тому, щоб об'єднати всі складові захисту в єдине ціле, в якому кожен компонент, виконуючи свою функцію, одночасно забезпечує виконання функцій іншими компонентами і пов'язаний з ними логічно і технологічно.

Надійність захисту інформації прямо пропорційна системності. При неузгодженості між собою окремих складових ризик «проколів» в технології захисту збільшується.

По-перше, необхідність комплексних рішень полягає в об'єднанні в одне ціле локальних СЗІ, при цьому вони повинні функціонувати в єдиній «зв'язці». Як локальних СЗІ можуть бути розглянуті, наприклад, види захисту інформації (правова, організаційна, інженерно-технічна).

По-друге, необхідність комплексних рішень обумовлена призначенням самої системи. Система повинна об'єднати логічно і технологічно всі складові захисту. Але з її сфери випадають питання повноти цих складових, вона не враховує всіх факторів, які надають або можуть впливати на якість захисту. Наприклад, система включає в себе якісь об'єкти захисту, а всі вони включені чи ні - це вже поза межами системи.

Тому якість, надійність захисту залежать не тільки від видів складових системи, але і від їх повноти, яка забезпечується при врахуванні всіх чинників і обставин, що впливають на захист. Саме повнота всіх складових системи захисту, що базується на аналізі таких факторів і обставин, є другим призначенням комплексності.

При цьому повинні враховуватися всі параметри уразливості інформації, потенційно можливі загрози її безпеці, охоплюватися всі необхідні об'єкти захисту, використовуватися всі можливі види, методи і засоби захисту та необхідні для захисту кадрові ресурси, здійснюватися всі витікаючі з цілей і завдань захисту заходу.

По-третє, тільки при комплексному підході система може забезпечувати безпеку всієї сукупності інформації, що підлягає захисту, і при будь-яких обставинах. Це означає, що повинні захищатися всі носії інформації, у всіх компонентах її збору, зберігання, передачі і використання, в усі час і при всіх режимах функціонування систем обробки інформації.

У той же час комплексність не виключає, а, навпаки, передбачає диференційований підхід до захисту інформації, в залежності від складу її носіїв, видів таємниці, до яких віднесена інформація, ступеня її конфіденційності, засобів зберігання і обробки, форм і умови прояву уразливості, каналів і методів несанкціонованого доступу до інформації.

Таким чином, значимість комплексного підходу до захисту інформації складається:

- в інтеграції локальних систем захисту;
- в забезпеченні повноти всіх складових системи захисту;
- в забезпеченні всеосяжність захисту інформації.

Виходячи з цього, можна сформулювати наступне визначення:

«Комплексна система захисту інформації - система, повно і всебічно охоплює всі предмети, процеси і фактори, які забезпечують безпеку всієї інформації, що захищається» .

1.5 Етапи створення політики безпеки інформації

З урахуванням цих особливостей розробки складного комплексу організаційних і програмно-технічних заходів процес створення політики інформаційної безпеки буде складатися з наступних етапів:

- проведення аудиту стану інформаційної безпеки з використанням власних ресурсів і залучених експертів;
- аналіз виявлених ризиків, розробка, пропозиція і захист можливих сценаріїв побудови систем оборони;

- розробка стандартів системи інформаційної безпеки, узгодження їх з усіма причетними службами;
- вибір оптимальних, економічно вигідних і впроваджуваних рішень захисту інформаційної безпеки;
- розробка нормативно-правової документації щодо забезпечення інформаційної безпеки, починаючи від політик верхнього рівня і закінчуючи стандартами роботи з базами даних і комп'ютерною технікою;
- погодження та затвердження розроблених документів на рівнях рад директорів і виконавчого органу компанії;
- впровадження документів, їх апробація;
- супровід ефективної роботи всіх створених секторів безпеки, доробка документів;
- перевірка якості роботи систем безпеки, їх аудит та вдосконалення.

Всі ці етапи вимагають уважного ставлення до будь-якої процедури, впровадження якої має здійснюватися з урахуванням думки всіх підрозділів, узгодження всіх необхідних документів, в іншому випадку неминуче виникнення конфлікту інтересів різних департаментів. Його наявність істотно ускладнить роботу компанії.

1.6 Постановка задачі

Зауважуючи вищенаведені пункти, для доцільної розробки політики безпеки підприємства потрібно виконати обстеження ОІД, проаналізувати загрози та вразливості ,а також виявити їх джерела.

Розробити положення політики безпеки.

Техніко-економічно обґрунтувати важливість впровадження розроблених політик безпеки.

1.7 Висновки

Перший розділ кваліфікаційної роботи описує:

- концепція інформаційної безпеки;
- аналіз нормативно-правової бази;
- види інформації, порядок доступу до неї;
- підстави для створення КСЗІ;
- єтапи створення політики безпеки;
- постановку задачі.

Таким чином, вирішена необхідність дослідження об'єкта і виявлення основних загроз і вразливостей, реалізація яких призведе до порушення інформаційних активів, що циркулюють в ІТС підприємства.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальні відомості про підприємство

Приватне підприємство «Devcorp», яке було основане у 2019 р.. Її складається штат з 5 працівників. Зараз компанія поступово зростає та популяризується у своїй діяльності.

Адреса : 49000, м.Дніпро, вул.Барикадна 10

Специфікація діяльності підприємства:

Підприємство займається розробкою програмного забезпечення на замовлення.

Приміщення, де циркулює інформація з обмеженим доступом (ІзОД) розташований на третьому поверсі 7-ти поверхового будинку з адміністративними приміщеннями.

Працює 5 днів на тиждень. З понеділка по п’ятницю з 9:00 до 20:00. Вихідні – суббота та неділя.

Штат працівників: директор(1 особа), бухгалтер(1 особа), розробник(2 особи),системний адміністратор (1 особа).

2.2 Обстеження ОІД

2.2.1 Опис ситуаційного плану

Об’єктом інформаційної діяльності є офіс приватного підприємства – ФОП «Devcorp».

Офіс, де циркулює інформація з обмеженим доступом (ІзОД) розташований на третьому поверсі 7-ти поверхового будинку з адміністративними приміщеннями. Офіс має 4 вікна, які виходять у зовнішній двір будівлі.

Стіни будівлі, в якій знаходиться ОІД зроблені з червоної цегли

(25х12х6,5 см). Фундамент виконаній з використанням залізнобетонних забивних паль. Будівля має плоский дах. Дах — покритий рубемастом з товстим бітумних шаром на нижньому боці та грубозернистим посипанням з верхнього боку, територія навколо будівлі повністю покрита плиткою.

Підприємство знаходиться в цегляній будівлі. Товщина зовнішніх стін 52см(2 шари цегли та штукатурка)

Внутрішні несучі стіни також зроблені з червоної цегли ,товщина 250 мм(1 шар цегли з цементом і штукатурка). Перекриття зроблені з використанням залізобетонних плит, товщиною 220 мм.

Вікна металопластикові, одностворчасті , розмірами 1320 х 870 мм.

Вхід до офісу – одностворчасті металеві двері, розмірами 1020 х 2070 мм.

Міжкімнатні двері – одностворчасті металопластикові, розмірами 1300 х 2000 мм.

Офіс має висоту 2,55 м , стеля підвісна, з конструкцією кріплення Грільято. Підлога в офісі – паркет та плитка у туалеті.

Ліворуч від будівлі знаходиться 3 жилих будинка та трансформаторна підстанція, праворуч – 3 жилих будинка 2 адміністративні будівлі та 1 гараж , позаду – будинок в якому ведуться ремонтні роботи .

В таблиці 2.1 наведені харектеристики будівель та споруд розташованих поряд з офісом підприємства. Найбільш найближчими об'єктами до офісу є: 2 жилих будинка (45м та 53м)

Система електропостачання підключена до трансформаторної підстанції №7, яка має сторонніх споживачів і знаходиться за межами КЗ.

Система опалення підключена до міської системи опалення та знаходиться за межами КЗ.

Системи каналізації та водопостачання підключені до міської системи, знаходяться за межами КЗ.

Усі пристрої заземлені на загальний контур заземлення, що замкнут та виходить за межі КЗ. Безпосередньо у приміщенні заземлення немає.

Таблиця 2.1. Характеристика будівель та споруд.

№	Название	Адрес	Кол-во этажей	Минимальное расстояние до объекта, м
1	Жилий будинок	ул. Барикадна, 8	3	45
2	Жилий будинок	ул. Барикадна, 20	3	96
3	Жилий будинок	ул. Барикадна, 22	3	112
4	Административное здание	ул. Барикадна, 22а	2	123
5	Гаражі	ул. Барикадна	1	22
6	Гаражі	ул. Барикадна	1	81
7	Трансформаторна підстанція	ул. Барикадна, 8	1	46
8	Жилий будинок	ул. Барикадна, 20	3	93
9	Гаражі	ул. Барикадна	1	109
10	Гаражі	ул. Барикадна	1	32
11	Жилий будинок	ул. Барикадна, 8	1	53
12	Довгобуд	ул. Барикадна	3	67

Система вентиляції використовується приточно-витяжна.

Контрольована зона обмежена зовнішніми стінами з усіх сторін ,знизу підлою ,зверху стелею .

Режим КЗ забезпечується таким чином :

У робочий час забезпечується співробітниками та системою контролю управління доступу. Чергові знаходяться біля КПП, біля входу. У випадку натискання тривожної кнопки приїзджає наряд приватної охорони. Сигналізація КЗ входить до складу системи сигналізації всієї будівлі.

У неробочий час забеспечується силами охорони(приватна фірма)з використанням відеоспостереження, вхідними залізними дверями. Також застосовується автономна сигналізація , пульт управління знаходиться біля чергових ,біля входу.

Схема заземлення зображена на ситуаційному плані в ДОДАТКУ Ґ, заземлення іде від трансформаторної будки до розподільного щита .Безпосередньо у приміщенні заземлення немає.

Задіяні лінії комунікації

• Мережа інтернет - оптоволоконний кабель, який прокладений в межах КЗ і виходить за його межі.

• Локальна мережа - кручена пара, яка прокладена в КЗ і не виходить за його межі.

• Електрична мережа - загальна на багатоповерховий будинок, тому проходить в КЗ і виходить в інші приміщення будівлі.

• Перетворювач електроенергії - трансформаторна підстанція, яка знаходиться за території будівлі, поза КЗ.

• Вентиляційна система - знаходиться в межах КЗ.

• Опалення і водопровід - загальні додому, тому проходять через КЗ і виходять в інші приміщення.

Контрольована Зона(КЗ) - обмежена зовнішніми стінами будівлі з західної сторони, з інших сторін знаходяться коридор та інші офісні приміщення. Над стелею та під підлогою знаходяться інші офісні приміщення.

Обьект інформаційної діяльності розсташований на 3 поверсі 7 поверхової будівлі за адресою вул.Барикадна 10

Розміри приміщень ОІД

• Кабінет розробників – 34,4 м2

• Кабінет Директора – 34,4 м2

• Кабінет бухгалтера - 25.2 м2

• Конференц зал - 32 м2

• Туалет - 12 м2

• Коридор - 35м2

• Загальна площа усіх приміщень КЗ – 173 $м^2$.

Розетки в приміщенях з заземленням підключені до щитової, що знаходиться на поверсі по загальному коридору

Вимикачі освітлення двохклавіішні, також під'єднані до щитової що знаходиться на поверсі далі по коридору . Освітлення світлодіодне. Освітлення під'єднане силовими кабелями ВВГ

Об'єкт знаходиться під охороною, за допомогою централізованої системи охоронно-пожежної сигналізації, яка зв'язана з загальним пунктом охорони, схема якого наведена у ДОДАТКУ Є .

Стеля в приміщенях КЗ – підвісна.

Вентиляційна система яка проведена до кожного приміщення – приточно-витяжна, план якої наведений в ДОДАТКУ Е

Опалювальна система яка знаходиться у кожному приміщені – біметалічні радіатори з металопластиковими трубами.

Локальна мережа - кручена пара, яка прокладена в КЗ від щитової провайдеру на поверсі і не виходить за його межі.

В таблиці 2.2 наведений опис основних технічних засобів ОІД

В таблицях 2.3-2.4 наведений список допоміжних технічних засобів

Генеральний план та план комунікацій наведено у ДОДАТКУ Д та ситуаційний план наведено у ДОДАТКУ Ґ.

Таблиця 2.2 – опис основних технічних засобів

Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
Системний блок PC-1	ZEVS	8005UX	DFH 987561	На столі	0.4	1,3
Системний блок PC-2			DFH 987616	На столі	0.5	0,9
Системний блок PC-3			DFH 875123	На столі	0.7	0,9
Системний блок PC-4			DFH 212458	На столі	0.8	0,8
Монітор 1	Samsung	C24F390FHI	DFG789546	На столі	0.7	1,3
Монітор 2			DFG799824	На столі	0.8	0,9
Монітор 3			DFG444531	На столі	1	0,9
Монітор 4			DFG789854	На столі	1.1	0,8
Клавіатура 1	4a-tech	A4tech V7M Bloody	FDH169879	На столі	0.6	1,3
Клавіатура 2			FDH564548	На столі	0.7	0,9
Клавіатура 3			FDH158743	На столі	0.9	0,9
Клавіатура 4			FDH158744	На столі	1	0,8
БФП	Canon	MF4410	MF847161	Поряд зі столом	3.5	1,4
БФП	Canon	MF4410	MF847162	Поряд зі столом	0.6	1,9
Маршрутизатор	Xiaomi	Xiaomi Mi WiFi Router	KLM798941	На стіні	1	1,4

		4A R4A				

Таблиця 2.3 – опис допоміжних технічних засобів(системи охоронно-пожежної сигналізації)

Найменування	Тип	Серійний номер	Розташування	Мінімальна відстань від елем. до кордонів ОІД, м	Мінімальна відстань до ЕОТ, м
ОРИОН 16І.3.2	ППКОП	21321311323	Коридор	0,5	2
Гном-1 New	Сирена світлошумова	31654914319	Коридор	0	3
ИО 102-2	Магнітоконтактний	19874989978	Коридор\двері	0,3	3
ИО 102-6	Магнітоконтактний	Б/Н	Каб. Директора\двері і вікна	0,3	2
				0,3	2
				4	3
			Конференц зал\двері і вікна	0,3	2
				4	3
				0,3	2
			Туалет\двері і вікна	2	5
				0,3	5
			Кабинет розробників\двері	3	3
			Кабинет бухгалтера\двері	4	5
АСТРА-621	Комбінований сповіщувач руху та розбиття скла	13131321356	Кабинет директора	4	1,3
		23165488979			
		30164897799			
		34987897987	Конференц зал	4	1,5
		34654897869	Туалет	3	2
		74897542489	Коридор	0,5	3
		68796546487	Кабинет розробників	0,5	1,7
		69879687989	Кабинет бухгалтера	4	5
Артон СПД Кадет	Датчики диму	31654897998	Кабинет розробників	2	5
		85748798799		2	5
		65789797987	Туалет	2	0,9
		65479879879		2	0,9
		65746416547	Конференц зал	1,5	5
		63546987899	Кабинет бухгалтера	2	0,8
		65489798751	Каб. Директора	2	1,3
SPR-8L	Кнопка пожежі	63548979888	Коридор	0,3	2,5
Exit-EB53	Кнопка тривоги	32165478979	Каб. Директора	1,5	1

Таблиця 2.4 – опис допоміжних технічних засобів

Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ОТЗ, м
Навісна Led лампа освітлення	TL-Office	Horoz Electric	HGH465661	На стелі	2	1
			HGH321654		2,1	3
			HGH231658		2,3	2
			HGH898995		2,3	3
			HGH565488		1,7	5
			HGH648979		3	4
			HGH648998		5	3
			HGH465648		5	5
			HGH988976		3	7
			HGH565663		2	0,9
			HGH321348		2	1
			HGH321589		2	4
Маніпулятор миша 1	Logitech	Logitech M185	DFG321651	На столі	1,4	0,2
Маніпулятор миша 2			DFG165499	На столі	1,3	0,2
Маніпулятор миша 3			DFG489745	На столі	1,5	0,2
Маніпулятор миша 4			DFG636598	На столі	2,3	0,2
Телефон 1	Xiaomi	Redmi 8a	S2FDG156SG	Переносний	-	-
Телефон 2	Xiaomi	Redmi 7pro	E3RY241E56	Переносний	-	-
Телефон 3	Xiaomi	Redmi 8	MNT321NM3	Переносний	-	-
Телефон 4	Xiaomi	Redmi 6	WRE1Q3EW2	Переносний	-	-

2.2.2 Обстеження обчислювальної системи ОІД

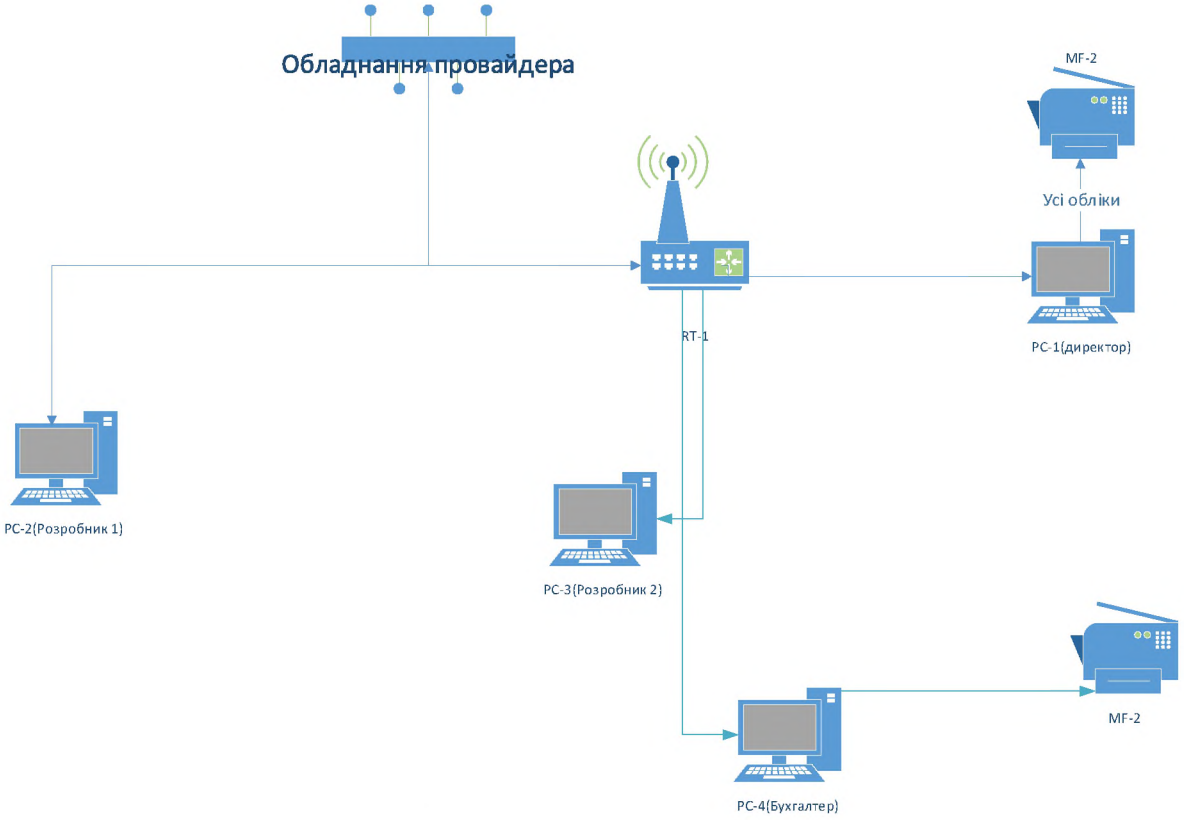


Рисунок 2.1 – Структурна схема підключення ОТЗ

Усі клавіатури до системних блоків підключені через роз'єм USB

Усі миші до системних блоків підключені через роз'єм USB

До приміщення надходить кручена пара, яка підключена до роутеру, усі системні блоки під'єднані на пряму до мережі Інтернет через роутер за допомогою крученої пари в роз'єм RJ-45. Сітка однорангова.

БФП під'єднані до певних ПК (1 до ПК Директора , 2 до ПК Бухгалтера) через USB Type B роз'єм.

Роутер також являє собою точкою доступу WI-FI з обмеженим доступом шифрування WPA2 (тільки працівники знають пароль) з виходом в інтернет для використання працівниками для робочих потреб .

Схема мережі з інформаційними потоками

РС-4 – Бухгалтер створює бухгалтерський звіт і відпраляє його директору на узгодження.

РС-1,4 – Персональні данні співробітників зберігаються на комп'ютерах бухгалтера і директора. Та за необхідності можуть бути роздруковані на принтері та передаватись між комп'ютерами через локальну мережу .

РС-4 – Клієнтська база зберігається виключно на комп'ютері бухгалтера

РС-1 – Данні замовлення оброблюються на ПК директора та передаються розробникам 1 та 2

РС-4 – Зарплатні відомості формуються бухгалтером відправляються на узгодження директору та після узгодження відправляються розробникам 1 та 2

РС-1 – Робочій графік формується директором та відправляєтся розробникам 1 та 2

РС-2-3 – Розробники створюють вихідний код ПЗ після перевірки його функціонування відправляють на узгодження директору

ІТС ОІД являє собою мережу типу «зірка», побудовану з використанням роутеру(який також являється точкою доступу).

Обчислювальна система у офісі:

1 чотири ПЕОМ Microsoft Windows 10 Professional

2 один роутер на 8 портів

3 програмні засоби активного мережевого обладнання

4 два багатофункціональних пристроя(БФП)

5 прикладне ПЗ (Visual Studio, ADOBE PHOTOSHOP 2020, AMD SOFTWARE, Microsoft Edge v1.6543, Telegram, Adobe Dreamweaver 2020)

В таблиці 2.5 неведені характеристики основних технічних засобів ОІД.

В таблиці 2.6 наведене програмне забезпечення, яке використовується в ІТС.

Таблиця 2.5 – Характеристики ОТЗ

Назва	Характеристики	Серійний номер
Персональний комп'ютер(PC1)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666661
	Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66641
	Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45711
	Блок живлення: GameMax GM400 OEM	BP40817151
	Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D1
Персональний комп'ютер(PC2)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666662
	Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66642
	Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45712
	Блок живлення: GameMax GM400 OEM	BP40817152
	Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D2
Персональний комп'ютер(PC3)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666663
	Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66643
	Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45713
	Блок живлення: GameMax GM400 OEM	BP40817153
	Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D3
Персональний комп'ютер(PC4)	Оперативна пам'ять: Goodram DDR4-2666 8192MB PC4-21300	HYG666664
	Жорсткий диск: Western Digital Blue 1TB 7200rpm 64MB	WDBS66644
	Твердотільний накопичувач: Kingston SSDNow A400 120GB 2.5" SATAIII 3D TLC	KSSD45714
	Блок живлення: GameMax GM400 OEM	BP40817154
	Процесор: AMD Ryzen 3 2200G (3.5 - 3.7 ГГц)	RPC2345D4

Таблиця 2.6 – Перелік ПЗ в ІТС

№	Найменування ПО	Пристрій	Тип ліцензії	Тип
1	Windows 10 Pro 1909 Build 13512,109	PC-1	Комерційна	Системне
		PC-2		
		PC-3		
		PC-4		
2	ADOBE PHOTOSHOP 2020	PC-1	Комерційна	Прикладне
		PC-2		Прикладне
		PC-3		Прикладне
		PC-4		Прикладне
3	AMD SOFTWARE	PC-1-4	Безкоштовне	Прикладне
5	Microsoft Edge v1.6543	PC-1-4	Безкоштовне	Прикладне
6	Visual Studio 2019	PC-1-4	Комерційна	Прикладне
7	Telegram	PC-1-4	Безкоштовне	Прикладне
8	Adobe Dreamweaver 2020	PC-1-4	Комерційна	Прикладне

2.2.3 Інформаційне середовище

Інформація підприємства зберігається на електронних та паперових носіях.

Детально данні наведено в таблиці 2.7.

Таблиця 2.7 – Інформація, що циркулює на підприємстві

Інформація	Режим доступу	Правовий режим	Працівники, що мають доступ	Місце зберігання	Вимоги
Зарплатні відомості	З обмеженим доступом	Конфіденційна інформація	Всі працівники	РС-1	Конфіденційність
Особисті справи співробітників	З обмеженим доступом	Конфіденційна інформація	Директор	РС-1,4	Конфіденційність
Клієнтська база	З обмеженим доступом	Конфіденційна інформація	Директор	РС-1	Конфіденційність Цілісність Доступність
Бухгалтерські звіти	З обмеженим доступом	Конфіденційна інформація	Директор, Бухгалтер	РС-1, РС-4	Конфіденційність Цілісність Доступність
Вихідний код ПЗ	З обмеженим доступом	Конфіденційна інформація	Розробник1-2	РС-2, РС-3	Конфіденційність Цілісність Доступність
Робочий графік	З відкритим доступом	Відкрита	Всі працівники	РС-1, РС-4	-
Дані замовлень	З обмеженим доступом	Конфіденційна інформація	Розробник1-2, Директор	РС-1-4	Конфіденційність Доступність

Визначення рівня конфіденційності, цілісності та доступності інформації описане у таблиці 2.8.

Таблиця 2.8 – Визначення рівня конфіденційності, цілісності та доступності інформації

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Зарплатні відомості	К1	Ц1	Д1
Особисті справи співробітників	К2	Ц2	Д2
Клієнтська база	К3	Ц3	Д3
Бухгалтерські звіти	К4	Ц5	Д3
Вихідний код ПЗ	К3	Ц4	Д4
Робочий графік	К1	Ц1	Д1
Дані замовлень	К1	Ц2	Д2

Для класифікації інформації 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.

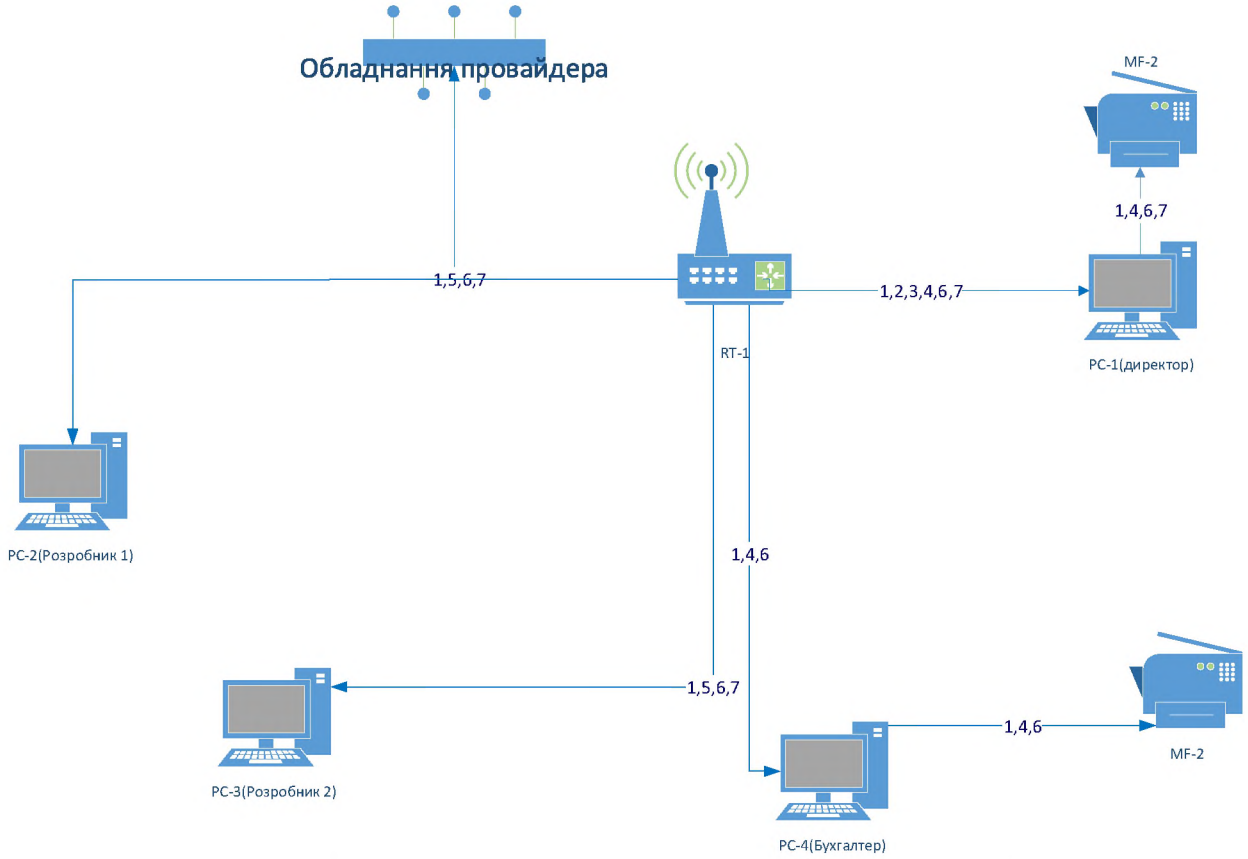


Рисунок 2.2 – Схема інформаційних потоків

2.2.4 Середовище користувачів

Таблиця 2.9 – Середовище користувачів

Посада	Роль в системі	Рівень доступу	Рівень кваліфікації	Обладнання	Час роботи
Директор	Адміністратор з повними правами	Читання, запис, видалення	Досвідчений	PC-1	10:00-19:00
Розробник 1-2	Користувач	Читання, запис	Досвідчений	PC-2-3	10:00-20:00
	Користувач	Читання, запис,			10:00-20:00
Бухгалтер	Адміністратор без прав на налаштування системи	Читання, запис, видалення	Середній	PC-4	10:00-20:00
Системний адміністратор	-	-	Досвідчений	-	В робочий час

Матриця керування доступом працівників підприємства до інформації описана у таблиці 2.10.

Таблиця 2.10 – Матриця керування доступом

Посада	Доступ	Рівень доступу
Директор	Зарплатні відомості	R W S
	Особисті справи співробітників	R W S
	Дані замовлень	R W S
	Бухгалтерські звіти	R W S
	Робочий графік	R W S
Бухгалтер	Бухгалтерські звіти	R W
	Зарплатні відомості	R W S
	Робочий графік	R
	Особисті справи співробітників	R
	Клієнтська база	R
Розробники	Дані замовлень	R
	Зарплатні відомості	R
	Робочий графік	R
	Вихідний код ПЗ	R W X S
Системний адміністратор	Зарплатні відомості	R
	Робочий графік	R

Де R – читання ,W – запис, X – виконання, S – відправлення.

2.3 Аналіз загроз та вразливостей

Модель можна відобразити системою таблиць(Табл 2.10-2.11). Для побудови моделі використовуються усі можливі категорії порушників для більш точного їх аналізу. Рівень загрози оцінюється за 4-бальною шкалою.

Таблиця 2.10 – 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 2.11 – Модель порушника

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Внутрішні порушники						
Директор	М2	К2	З2	Ч3	Д2	11
Бухгалтер	М3	К1	З1	Ч3	Д2	10
Розробник 1	М3	К3	З2	Ч3	Д2	13
Розробник 2	М3	К3	З2	Ч3	Д2	13
Системний адміністратор	М3	К3	З2	Ч4	Д4	16
Зовнішні порушники						
Наємний персонал	М3	К2	З1	Ч1	Д1	8
Хакери	М3	К3	З3	Ч4	Д3	16
Колишні робітники	М2	К3	З2	Ч2	Д3	12
Конкуренти	М3	К3	З3	Ч4	Д3	16

М1 – безвідповідальність.

М2 – самоствердження.

М3 – корисливий інтерес.

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

К2 - володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування.

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

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

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

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

Ч1 - під час повної бездіяльності ІТС з метою відновлення та ремонту.

Ч2 - під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації.

Ч3 - під час функціонування ІТС (або компонентів системи).

Ч4 - як у процесі функціонування ІТС, так і під час призупинки компонентів системи.

Д1 - усередині приміщень, але без доступу до технічних засобів ІТС.
Д2 - з робочих місць користувачів (операторів) ІТС.
Д3 – дистанційно.
Д4 - з доступом у зону керування засобами забезпечення безпеки ІТС.

Висновок: найбільшу загрозу становлять системний адміністратор та розробники. Вразливість у розмежуванні доступу. Вони є основними поршниками для безпеки інформації, тому потрібно найняти адміністратора який буде їх контролювавати.

2.4 Модель загроз для інформації в ІТС

Інформація, що циркулює в ІТС:
- зарплатні відомості
- особисті справи співробітників
- клієнтська база
- бухгалтерські звіти
- Вихідний код ПЗ
- робочий графік
- дані замовлень

В таблиці 2.12 наведений опис потенційних загроз та ризика за допомогою яких можно розрахувати, як збитки що виникнуть в разі успішної реалізації загрози, так і саму вірогідність загрози.

Таблиця 2.12 – Потенційні загрози для інформації в ІТС

№	Потенційні загрози для інформації в ІТС	Ризики для			
		К	Ц	Д	С
	1. Загрози об'єктивної природи				
1.1.	Збої та відмови системи електроживлення			+	+
1.2	Стихійні явища(пожежа,аварія)		+	+	+
1.3.	Збої та відмови програмного забезпечення		+	+	+
	2. Загрози суб'єктивної природи				
2.1	**Зовнішні загрози**				
2.1.1	Несанкціоноване підключення до технічних засобів	+	+		
2.1.2	Несанкціоноване підключення до каналів зв'язку	+	+		
2.1.3	Читання даних, що виводяться на екран, , 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	Розголошення засобів розмежування доступу (паролів)	+	+	+	
2.2.2	Зараження системи комп'ютерними вірусами		+	+	+
2.2.3	Несанкціонована передача/розголошення ІзОД	+			
2.2.4	Модифікація компонентів програмного та інформаційного забезпечення		+	+	+
2.2.5	Пошкодження носіїв інформації			+	
2.2.6	Вхід у систему недопущених осіб (подолання систем захисту)	+	+	+	
2.3	**Помилки персоналу**				
2.3.1	Помилки користувачів (впровадження і використання програм, що не є необхідними для виконання службових обов'язків; запуск програм, здатних викликати критичні зміни в системі)		+	+	
2.3.2	Отримання сторонньою особою інформації у персоналу ІТС	+			
2.3.3	Пошкодження носіїв персоналом ІТС			+	
2.3.4	Недбале зберігання та облік документів	+	+	+	

За наведеними в таблиці 2.12 даними маємо розподілення загроз на антропогенні та техногенні фактори.

Серед техногенних можна виділити:

Скачки напруги можуть призвести до виходу з ладу технічних засобів(ПК,принтерів), у результаті можливе порушення цілісності та/або доступності інформації. Уразливість несправній роботі трансформаторної

підстанції, відсутності приладів безперебійного живлення. Можлива втрата доступу до ПК працівників, призупинення роботи і як наслідок фінансові втрати.

Збій в роботі встановленого програмного забеспечення може викликати пошкодження виконуваних файлів та призвести до утрати цілістності файлу. Уразливість у неналаштованому автозбереженні в данній програмі. Можлива втрата файлу який розробляється та як наслідок фінансові втрати.

Пошкодження носіїв персоналом ІТС, яке призвело до втрати доступу до інформації. Уразливість у відсутності механізмів резервного копіювання. Порушення доступності.

Серед антропогенних можна виділити:

На підприємстві є три вікна через які можливо побачити ПК директора або телевізор у конференц-залі. Уразливість у видимості робочих місць з вікна. Може призвести до порушення конфіденційності і як наслідок втрати ІзОД.

Перехід по стороннім посиланням працівниками компанії. Уразливість у відсутності систематичного інструктажу працівників. Можлива тимчасова втрата доступу до ПК або втрата ІзОД. Порушення доступності та конфіденційності.

Розробники можуть скопіювати розроблювальні проекти на свої носії інформації. Уразливість ненаявності систем контролю за підключенням зовнішніх носіїв до ПК або недостатньо частому оновлені антивірусного ПЗ. Оскільки на накопичувачах можуть бути віруси різного типу, вони можуть призвести до втрати, як конфіденційності так цілосності і доступності.

Працівники можуть встановлювати стороннє додаткове ПЗ. Уразливість у відсутності механізмів контролю за запуском програм. Можлива зупинка роботи і як наслідок фінансові втрати. Порушення конфіденційності, цілосності і доступності.

Клієнти які приходять в конференц зал на узгодження умов можуть побачити ІзОД. Уразливість у неконтролюванні клієнта напротязі всього часу

його находження на території КЗ. Порушення конфіденційності. Можливі фінансові втрати при потраплянні ІзОД до конкурентів.

Заміна або модифікація носіїв інформації системним адміністратором під час проведення планового технічного обслуговування. Треба контролювати дії системного адміністратора під час його знаходження в офісі. Може призвести до порушення конфіденційності, цілосності та доступності. Та як наслідок фінансовим встратам через кожний з цих чинників.

2.5 Вибір заходів захисту інформації в ІТС підприємства

Вибір профілю захищенності

АС підприємства –АС «3» класу. Тобто, це розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу. Для даної АС «3» класу обрано наступний профіль захищенності:

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

Опис послуг безпеки наведено у таблиці 2.13.

Таблиця 2.13 – Профіль захищеності ІТС

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використання об'єктів	КО-1 (повторне використання об'єктів)
	Конфіденційність при обміні	КВ-1(мінімальна конфіденційність при обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність при обміні
Доступності	Використання ресурсів	ДР-1. Квоти
	Відновлення після збоїв	ДВ-1. Ручне відновлення
Спостережності	Реєстрація	НР-2. Захищений журнал
	Ідентифікація і автентифікація	НИ-2. Одиночна ідентифікація і автентифікація
	Достовірний канал	НК-1. Однонаправлений достовірний канал
	Розподіл обов'язків	НО-2. Розподіл обов'язків адміністраторів
	Цілісність комплексу засобів захисту	НЦ-2. КЗЗ з гарантованою цілісністю
	Самотестування	НТ-2. Самотестування при старті
	Ідентифікація і автентифікація при обміні	НВ-1: Автентифікація вузла

КД — довірча конфіденційність;

КА — адміністративна конфіденційність;

КО — повторне використання об’єктів;

КК — аналіз прихованих каналів;

КВ — конфіденційність при обміні.

ЦД — довірча цілісність;

ЦА — адміністративна цілісність;

ЦО — відкат;

ЦВ — цілісність при обміні.

ДР — використання ресурсів;

ДС — стійкість до відмов;

ДЗ — гаряча заміна;

ДВ — відновлення після збоїв.

НР — реєстрація;

НИ — ідентифікація и автентифікація;

НК — достовірний канал;

НО — розподіл обов’язків;

НЦ — цілісність КЗЗ;

НТ — самотестування;

НВ — автентифікація при обміні;

НА — автентифікація відправника;

НП — автентифікація одержувача.

КД–2 – базова довірча 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.

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 27 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 – 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.

2.6 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 паролів користувачами системи є системний адміністратор.

Політика безпеки: Регламентовані цією політикою атрибути доступу мають бути призначені відповідним користувачам системним адміністратором з використанням вбудованих засобів розмежування доступу Active Directory.

Атрибути доступу, відповідно до посадових обов'язків користувачів, зазначені у таблиці 2.14

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

Відповідальність: Відповідальність за невиконання політики безпеки несе системний адміністратор, у разі не дотримання рекомендацій щодо розмежування доступу та інші користувачі, у разі порушення правил розмежування доступу.

Таблиця 2.14 – Атрибути доступу

Користувач	Інформація	ПЗ
Директор	1 – С, Ч, З, К, М, Д, В 2 – С, Ч, З, К, М, Д, В 4 – С, Ч, З, К, М, Д, В 6 – С, Ч, З, К, М, Д, В 7 – С, Ч, З, К, М, Д, В	8 – Вк 11 – Вк 12 – Вк 13 – Вк
Системний адміністратор	1 – Ч 6 – Ч	8 – Вк, Вст, О, В 9 – Вк, Вст, О, В 10 – Вк, Вст, О, В 11 – Вст, О, В 12 – Вк, Вст, О, В 13 – Вк, Вст, О, В 14 – Вк, Вст, О, В
Розробники 1-2	1 – Ч 5 – С, Ч, З, К, М, В 6 – Ч 7 – Ч	8 – Вк 9 – Вк 10 – Вк 11 – Вк 13 – Вк 14 – Вк
Бухгалтер	1– С, Ч, З, К, М, Д, В 2– Ч 3 – Ч 4 – С, Ч, З, К, М, Д, В 6 – Ч	8 – Вк 12 – Вк 13 – Вк

Перелік ПЗ та інформації:

1 зарплатні відомості (інформація);

2 особисті справи співробітників (інформація);

3 клієнтська база(інформація);

4 бухгалтерські звіти (інформація);

5 Вихідний код ПЗ (інформація);

6 робочий графік (інформація);

7 дані замовлень(інформація);

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

9 ADOBE PHOTOSHOP 2020 (програмне забезпечення);

10 AMD SOFTWARE (програмне забезпечення);

11 Visual Studio 2019 (програмне забезпечення);

12 Telegram (програмне забезпечення);

13 Microsoft Edge v1.6543 (програмне забезпечення);

14 Adobe Dreamweaver 2020 (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.

2.7 Політика відвідування території підприємства сторонніми особами

Мета політики: Створення регламенту доступу сторонніх осіб до території підприємства, захист від проникнення у приміщення зловмисників або конкурентів через відсутність контролю за переміщенням відвідувачів у робочий час. Політика встановлює порядок організації пропускного режиму в організацію, порядок контролю за переміщенням відвідувачів, а також встановлює відповідальність за порушення відповідних правил.

Область дії:

Область дії політики безпеки відносно відвідування території підприємства сторонніми особами розповсюджується, насамперед, на всіх осіб, що мають намір отримати доступ до території підприємства, але не є співробітниками підприємства та на співробітників, що визначаються відповідальними за перебування сторонніх осіб на підприємстві.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики відвідування території підприємства сторонніми особами є охоронець .

Політика безпеки:

Контроль доступу до території підприємства реалізується замком на вхідних дверях. Кожний робітник, при зарахуванні у штат, отримує персональний ключ, яку забороняється передавати третім особам.

Інших відвідувачів (партнерів, клієнтів, претендентів на вакантне місце тощо) має зустріти директор, або співробітник, що письмово вповноважений на це директором, він має супроводжувати відвідувача, поки той знаходиться на території підприємства.

Також, обов'язковою умовою для отримання допуску на територію підприємства є реєстрація у журналі відвідувачів, що знаходиться у охоронця. До журналу заноситься прізвище, ім'я, по батькові відвідувача, фіксується час, коли відвідувач зайшов на територію підприємства

(засвідчується його підписом) та час коли він вийшов з території підприємства (також засвідчується його підписом). Для перевірки істинності наданих відвідувачем даних можуть бути використані наступні документи:

– паспорт;

– водійські права;

– закордонний паспорт.

Неконтрольоване перебування відвідувачів (тобто, відсутність супроводу відповідальної особи) дозволяється лише у зоні очікування відвідувачів, тобто у передпокої.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролюється охоронцем за допомогою аналізу журналу відвідувачів. 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. Після ознайомлення з даною політикою користувач має підписатися у спеціальному журналі з техніки безпеки.

Порядок та періодичність перегляду:

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

Відповідальність:

Відповідальність за дії відвідувача несе, директор, або робітник, що був визначений відповідальним за перебування відвідувача на території підприємства. Відповідальність за невиконання цих правил полягає у дисциплінарному покаранні або сплаті штрафу, розмір якого залежить від наявності та фатальності наслідків.

2.8 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 (2 і більше), що будуть зберігатися на різних знімних носіях. При додаванні резервної копії на знімний носій, вона заноситься до теки, ім'я якої повинно містити порядковий номер резервної копій та дату резервного копіювання.

Технологічна інформація, конфігурації ПЗ і т.д. необхідно копіювати на окремі знімні 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 належить:

– групові політики;

– атрибути розмежування доступу;

– конфігурації ПЗ;

– дані про облікові записи.

Рекомендується проводити періодичний аналіз стану серверу: використовувати ПЗ «Viktoria» для перевірки стану жорстких дисків. У разі виникнення підозри на можливість виникнення збоїв або відмов, 60 системний адміністратор повинен провести позачергове резервне копіювання.

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

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.9 Політика безпеки відносно паролів

Мета політики безпеки:

Встановити правила використання паролів для доступу до

електронних документів, а також використання паролів для підключення до безпровідної мережі підприємства. Користувачі системи повинні дотримуватися вимог, що висвітлюються в даній політиці. Виконання вимог даної політики відносно паролів підвищує рівень

захищеності інформаційних ресурсів, що циркулюють та обробляються на підприємстві.

Область дії:

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ до електронних документів або підключаються до АС підприємства за допомогою безпровідної мережі.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики паролів користувачами системи є системний адміністратор підприємства.

Політика безпеки:

Паролі системного рівня:

– паролі створюються системним адміністратором. Директором підприємства встановлюється резервний пароль доступу до системи на випадки надзвичайних подій;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

– символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше п’яти символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері або зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати; зміні особи, що займає посаду системного адміністратора);

– паролі не мають повторюватися принаймні 3 рази;

– забороняється використовувати один і той самий символ більше двох разів підряд.

Паролі рівня користувачів:

– паролі генеруються користувачами особисто та вони мають відповідати приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 3 місяці (чи раніше при виникненні загрози розголошення пароля чи його втрати; зміні осіб на посадах передбачених на підприємстві);

– забороняється використовувати один і той самий символ більше двох разів підряд;

– паролі не мають повторюватися принаймні 3 рази.

Паролі для доступу до безпровідної мережі:

– паролі генеруються користувачами особисто та вони мають відповідно приведеним нижче критеріям;

– ідентифікатори та паролі користувачів мають бути унікальними;

– паролі мають бути довжиною не менше ніж 8 символів, що відносяться до 3 з 4 наступних категорій:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

– символі відмінні від букв чи цифр (наприклад: !,$,%,#);

– пароль не має містити ім’я облікового запису, довжиною більше двох символів;

– паролі заборонено передавати третім особам, не мають вставлятися до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді деінде;

– паролі мають змінюватися кожні 6 місяців (чи раніше при виникненні загрози розголошення пароля чи його втрати);

– забороняється використовувати один і той самий символ більше двох разів підряд;

– паролі не мають повторюватися принаймні 3 рази.

Затвердження політики:

Політика безпеки розробляється системним адміністратором та підписується директорам закладу при прийнятті усіх розділів політики.

Дії з виконання політики:

Виконання політики безпеки контролює системний адміністратор підприємства за допомогою вбудованих засобів автентифікації в ОС. При прийнятті (зміні) політики безпеки кожен працівник має бути ознайомлений не пізніше, чим за 5 робочих днів до прийняття нової редакції даної політики. При ознайомленні з даною політикою безпеки користувач має підписатися, що він ознайомлений з нею, та зобов’язується виконувати встановлені цим документом правила.

Порядок та періодичність перегляду:

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

Відповідальність:

Співробітники, що ознайомились з політикою безпеки несуть повну відповідальність за збереження паролів. До співробітників, що порушили дану політику безпеки, будуть прийняті дисциплінарні міри.

2.10 Політика антивірусного захисту

Мета. Створення вимог, які повинні зустрічатися всіма комп'ютерами, сполученими з мережею комп’ютерів "Devcorp", щоб гарантувати ефективний захист від вірусів.

Сфера застосування. Правила ПБ мають виконувати всі працівники організації.

Зміст політики. Загальна частина – встановлює наступні загальні правила, які слід виконувати для вирішення проблемі вірусу:

· завжди підтримуйте корпоративні вимоги, підтримка антивірусного ПЗ є необхідною для корпоративного вузла. Завантажте і підтримуйте поточну версію; завантажте і встановіть модифікації антивірусного програмного забезпечення, як тільки вони стають доступними;

· НІКОЛИ не відкривайте будь-які файли або макрокоманду, що торкається електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаліть ці повідомлення негайно, потім видаліть їх за допомогою спорожнення вашого сміття;

· видаліть Spam, ланцюг і іншу електронну пошту, які не мають атрибутів Вашої кампанії відповідно до політики безпеки;

· ніколи не завантажуйте файли від невідомих або підозрілих джерел;

· уникайте прямого дискового доступу (читання/запис), за винятком того, що відповідає необхідним діловим вимогам;

· перед використанням завжди скануйте носій від невідомого джерела на предмет вірусів;

· регулярно дублюйте критичні дані і системні конфігурації зберігайте їх в безпечному місці;

· якщо лабораторна перевірка встановлює конфлікт з антивірусним ПЗ, запустить антивірусну утиліту, що гарантує незабрудненість машини, блокуйте ПЗ, потім двинути лабораторну перевірку. Тільки після лабораторної перевірки дозволяйте використовувати антивірусне ПЗ. Під час

блокування антивірусного ПЗ блоковано, ні в якому разі не завантажуйте будь-які додатки, які могли б перенести вірус.

· нові віруси відкриваються майже щодня. Періодично перевіряйте Антивірусну політику відділу і ці рекомендації для внесення змін.

Відповідальність. Будь-який працівник, що порушує цю політику, повинен піддаватися дисциплінарним стягненням аж до звільнення з роботи.

2.11 Політика використання мережі Інтернет на підприємстві

Мета політики:

Підвищити рівень інформаційної безпеки компанії шляхом введення правил і інструкцій для співробітників, які при виконанні своїх прямих обов'язків використовують Інтернет.

Область дії:

Політика поширюється на співробітників закладу, які при виконанні своїх прямих обов'язків використовують мережу Інтернет. Дана політика безпеки не відміняє інші політики.

Відповідальні особи політики:

Відповідальною особою за виконання політики доступу є системний адміністратор підприємства.

Політика:

Доступ до мережі Інтернет виконувати лише через устаткування і системи підприємства.

Використання мережі Інтернет можливо лише для:

– отримання та обробки замовлень;

– підтримки і розвитку бізнесу і комунікації співробітників фірми;

– досліджень і розробок;

– збору інформації для більшої обізнаності у фінансових, законодавчих питаннях, якщо ці питання безпосередньо впливають на виконання своїх посадових обов'язків.

Забороняється:

– грати на комп'ютері в робочий час і під час обіду;

– вести діяльність не від імені фірми;

– передавати конфіденційну інформацію третім особам;

– здійснювати дії що суперечать статуту ділової етики підприємства, законодавству, політикам і процедурам підприємства;

– доступ до неавторизованої інформації і її копіювання;

– доступ до системи під іншим паролем.

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:

У разі явного порушення даної політики працівником підприємства, будуть застосовані дисциплінарні міри.

Порядок і періодичність перегляду

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

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:

$$t = 14+10+15+9+5+12+9$$

$$t = 74 \text{ год.}$$

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 – 95 грн/год.

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

$$З_{зп} = 74 \text{ год} \cdot 95 \text{ грн/год},$$

$$З_{зп} = 7030 \text{ грн}.$$

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.

$$C_{мч} = 0{,}65 \cdot 1 \cdot 1{,}57 + (12000*0{,}04)\backslash 1920 + (13300*0{,}1)\backslash 1920 \text{ грн},$$

$$C_{мч} = 1{,}97 \text{ грн.}$$

$$З_{мч} = 1{,}97*74=145{,}78 \text{ грн}$$

Отже, витрати на створення ПБ за формулою 3.2 становлять:

$$K_{рп} = 145{,}78+7030= 7175{,}78 \text{ грн.}$$

В результаті розрахунків, вартість розробки ПБ становить – 7175, 78 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 4 ліцензії на ПЗ CoSoSys Endpoint Protector вартість яких складає 2120 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-L825VA у кількості 4 пристроїв які складають 7020 грн та пломби для опечатування, ціна яких 160 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 бескоштовні, тому даний коефіцієнт не враховується.

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн. Втрати на встановлення додаткового обладнання становлять 600 грн.

Таким чином, згідно з формулою 3.6:

$$K = 2120+7020+160+600+7176=17076 \text{ грн.}$$

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:

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

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, який складається з 4 безперебійних джерел живлення загальною сумою 7020 грн;

$$C_а=7020/2=3510$$

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 9800 грн і відповідно 117600 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:

$$С_з = (117600 + 11760) \cdot 0,5 = 64680 \text{ грн}$$

Річні витрати на поновлення ліцензії складаються з замовленням CoSoSys Endpoint Protector на 1 рік (2120 грн).

Загалом, річні витрати на поновлення ліцензії ПЗ становлять:

$$С_{пз} = 2120 \text{ грн.}$$

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

$$С_е = P \cdot F_р \cdot Ц_е, \text{ грн} \qquad (3.9)$$

де P – встановлена потужність апаратури інформаційної безпеки яка на 4 ПК працівників складає 2,6 кВТ ;

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

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

$$С_е = 2,6 \cdot 1920 \cdot 1,57 = 7837 \text{ грн;}$$

Отже повна вартість річних експлуатаційних витрат становить:

$$C = 7837 + 2120 + 3510 + 64680 \text{ грн},$$

Таким чином повна вартість річних експлуатаційних витрат становить 78147 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	21000
Розробник 1	16000
Розробник 2	16000
Бухгалтер	12000
Системний адміністратор	7000

Загальна сума заробітних плат співробітників підприємства становить 72000 грн.

Необхідні вхідні данні для розрахунку:

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

t_n – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

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

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

$З_о$ – заробітна плата співробітників обслугованого персоналу, становить 7000

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 72000 грн/місяць;

$Ч_о$ – чисельність обслугованого персоналу 1 особи.

$Ч_с$ – чисельність співробітників атакованого вузла 4 осіб.

$О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік становить 1000000 грн;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 2000 грн;

I – число атакованих вузлів або сегментів корпоративної мережі становить 4;

N – середнє число атак на рік 8.

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

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

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;

$$П_п = ((72000 \cdot 4/160)) \cdot 3 = 5400 \text{ грн}$$

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:

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

$$П_{ви} = ((72000 \cdot 4/160)) \cdot 2 = 3600 \text{ грн}$$

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

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

$$П_{пв} = ((7000 \cdot 1/160)) \cdot 1 = 43{,}75 \text{ грн}$$

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:

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

де F_r – річний фонд робочого часу.

$$V = 1000000 / 1920 \cdot (3 + 1 + 2) = 3125 \text{ грн}$$

Отже упущена вигода згідно формули 3.12 становить:

$$П_в = 3600 + 43{,}75 + 3000 = 6643{,}75 \text{ грн}$$

Отже упущена вигода згідно формули 3.10 становить:

$$U = 5400 + 3125 + 6643{,}75 = 15168{,}75 \text{ грн}$$

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

$$В = \sum_i \sum_n U. \quad (3.16)$$

$$В = 4 \cdot 8 \cdot 15168{,}75 = 485376 \text{ грн}$$

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 0,3;

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

$$E = 485376 \cdot 0{,}4 - 78147 = 116003.4 \text{ грн.}$$

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 $Т_о$.

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 Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

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

Таким чином,

$$ROSI = 116003.4 / 17076 = 4,72.$$

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:

$$T_O = \frac{E}{K} = \frac{1}{ROSI} = 0,14 \text{ року.} \qquad (3.19)$$

3.5 Висновок економічної частини

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 17076 грн.

2. Повна вартість річних експлуатаційних витрат становить 117600 грн.

3. Загальний збиток від атаки складатиме 485376 грн.

4. Загальний ефект від впровадження системи інформаційної безпеки становить 116003.4 грн.

5. Термін окупності капітальних інвестицій складає 0,14 року.

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

ВИСНОВКИ

У першому розділі кваліфікаційної роботи описано стан питання, проаналізовано нормативно-правову базу, на основі якої визначено підстави та етапи створення КСЗІ та ПБ.

Таким чином визначено необхідність здійснення обстеження об'єкту та виявлення основних загроз та вразливостей, реалізація яких призведе до порушення властивостей інформації, що циркулює в ІТС підприємства.

У спеціальній частині наведено основні відомості про підприємство. Виконано обстеження інформаційної системи, фізичного середовища, середовище користувачів. Описано технологію обробки інформації та функціональний профіль захисту.

Окрім цього, виконано категоріювання інформації, що обробляється в ІТС та визначено основні загрози та вразливості, їх джерела та складено модель порушника.

Отримані результати обстеження були використані для розробки ПБ ІТС приватного підприємства ФОП “Devcorp”. На їх основі розроблено збірку правил відносно створення паролів, антивірусного захисту, використання мережі інтернет, фізичного доступу до сервера.

Розроблені рекомендації повинні сприяти забезпеченню належного стану захищеності ІТС підприємства.

В третьому розділі було проведено розрахунки капітальних витрат на введення в експлуатацію політики безпеки інформації, річних експлуатаційних витрат на підтримку заходів захисту, регламентованих політикою безпеки.

В ході розрахунків з’ясовано, що введення в експлуатацію засобів та заходів захисту вигідне для підприємства.

Отже, впровадження та використання обраних проектних рішень повністю доцільне, і сприяє забезпеченню належного стану захищеності інформації, що циркулює в ІТС підприємства.

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 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2000. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341

13 Загрози інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: http://www.security.ase.md/publ/ru/pubru91/

14 Опис інформаційної безпеки підприємства [Електронний ресурс] – Режим доступу до ресурсу: https://bcs.kiev.ua/infosecurity

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних позначень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	13	
6	А4	Спеціальна частина	38	
7	А4	Економічна частина	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Ґ	1	
15	А4	Додаток Д	2	
16	А4	Додаток Е	3	
17	А4	Додаток Є	1	

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

Циватий_Д.О._125-18ск-1.docx
Циватий_Д.О._125-18ск-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

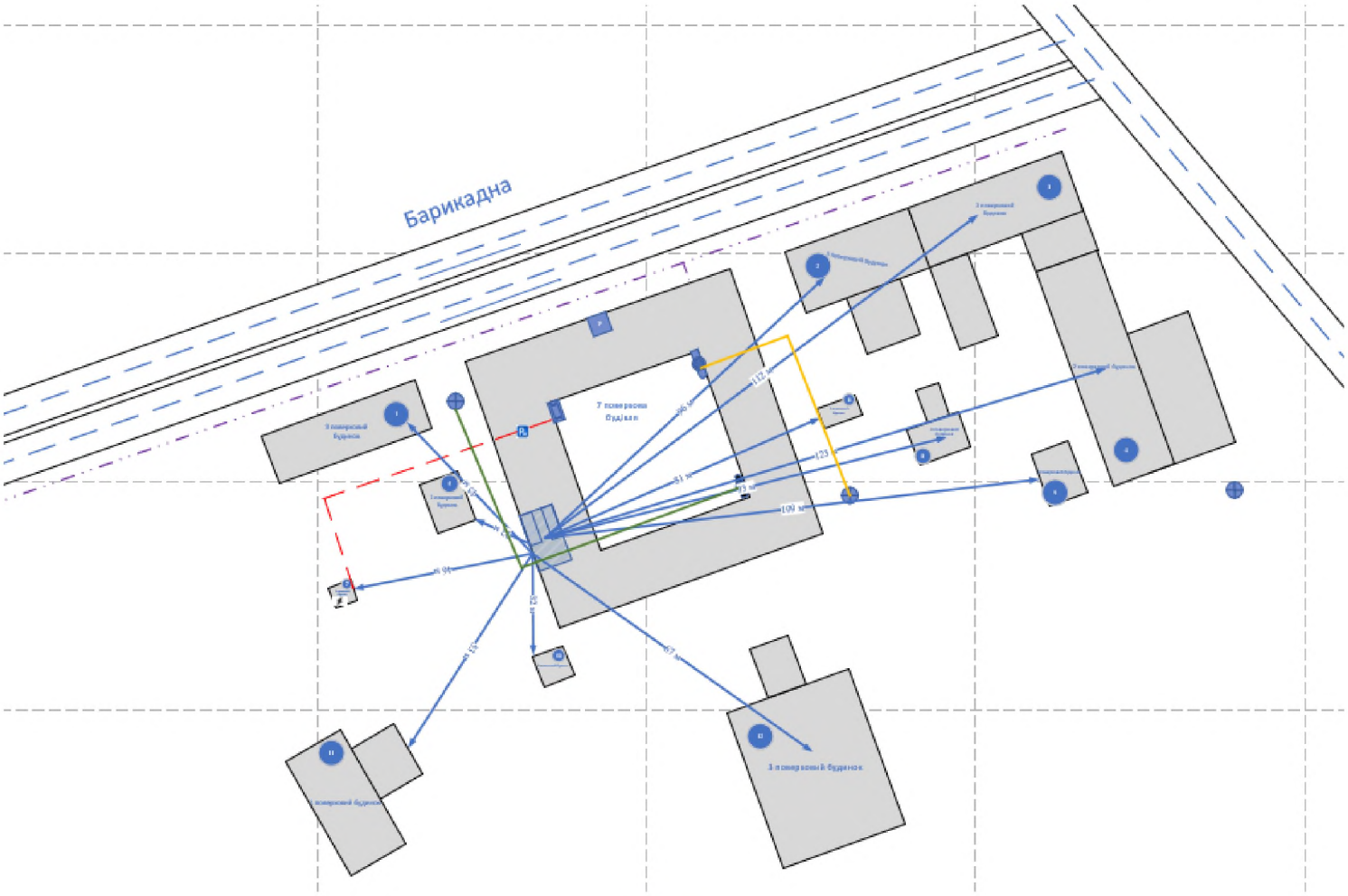
Відгук керівника економічного розділу:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

ДОДАТОК Ґ



Умовні Позначення

Люк системи каналізації

Порядковий номер будівлі у таблиці №1

Місце парковки

Напрям руху транспорту

Територія ОІД

Межа КЗ

Розподільний щит в будівлю

Трансформаторна підстанція

Контур системи заземлення

лінія система водопостачання

Будівля

Система опалення

Автомобільний КПП

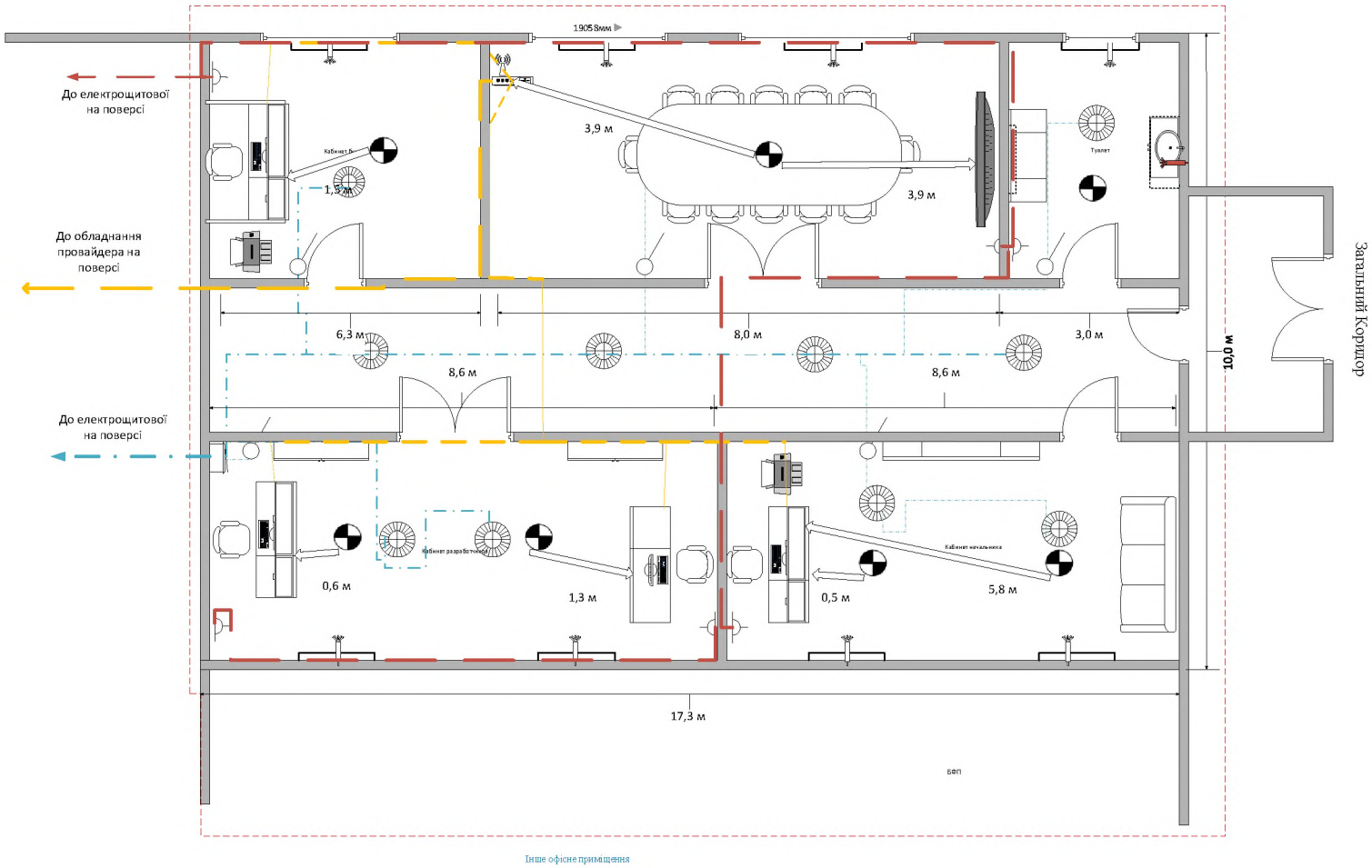
Лінія систем електропостачання

Лінія систем зв’язку

Лінія водопостачання

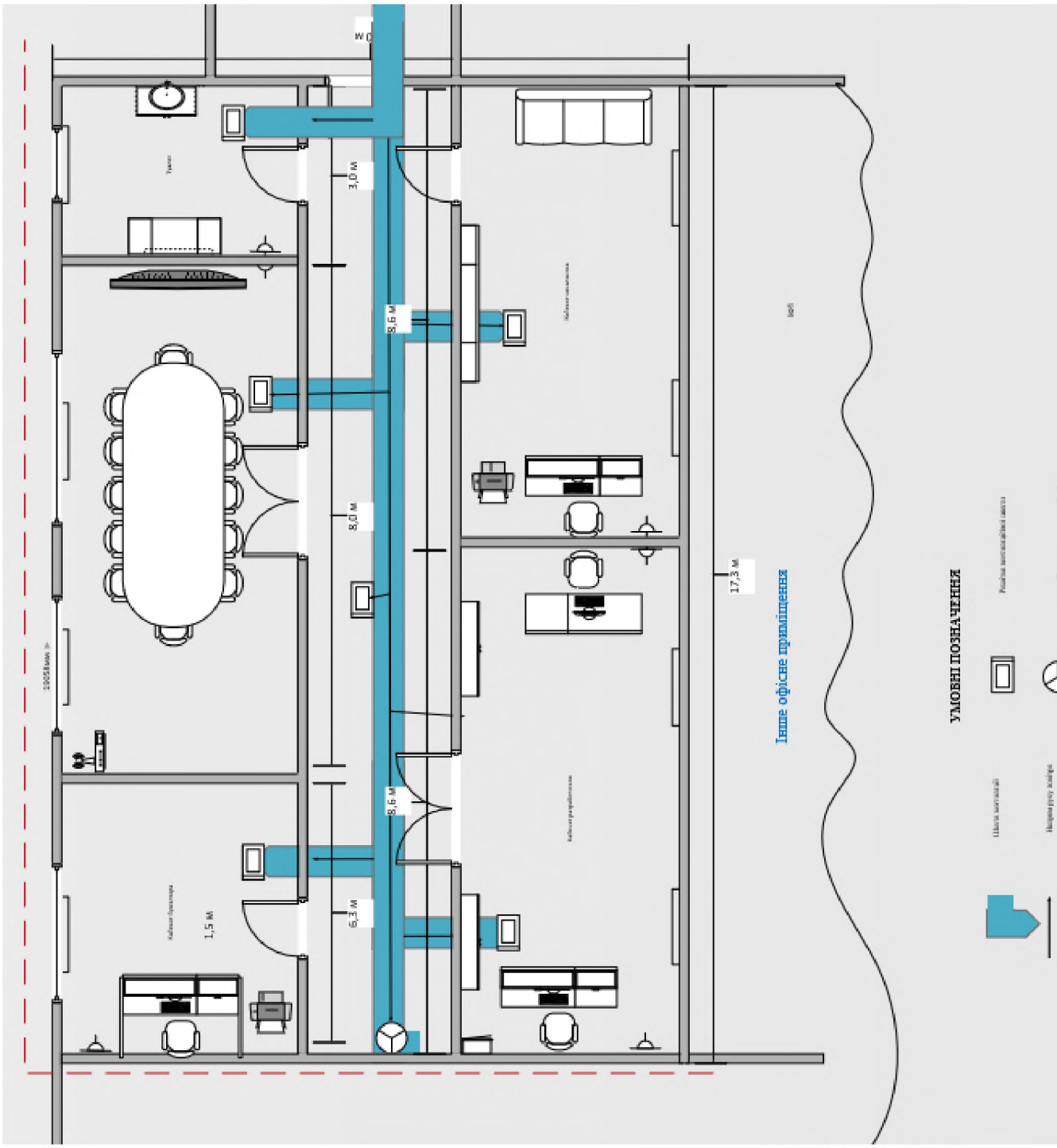
Лінія теплопостачання

ДОДАТОК Д

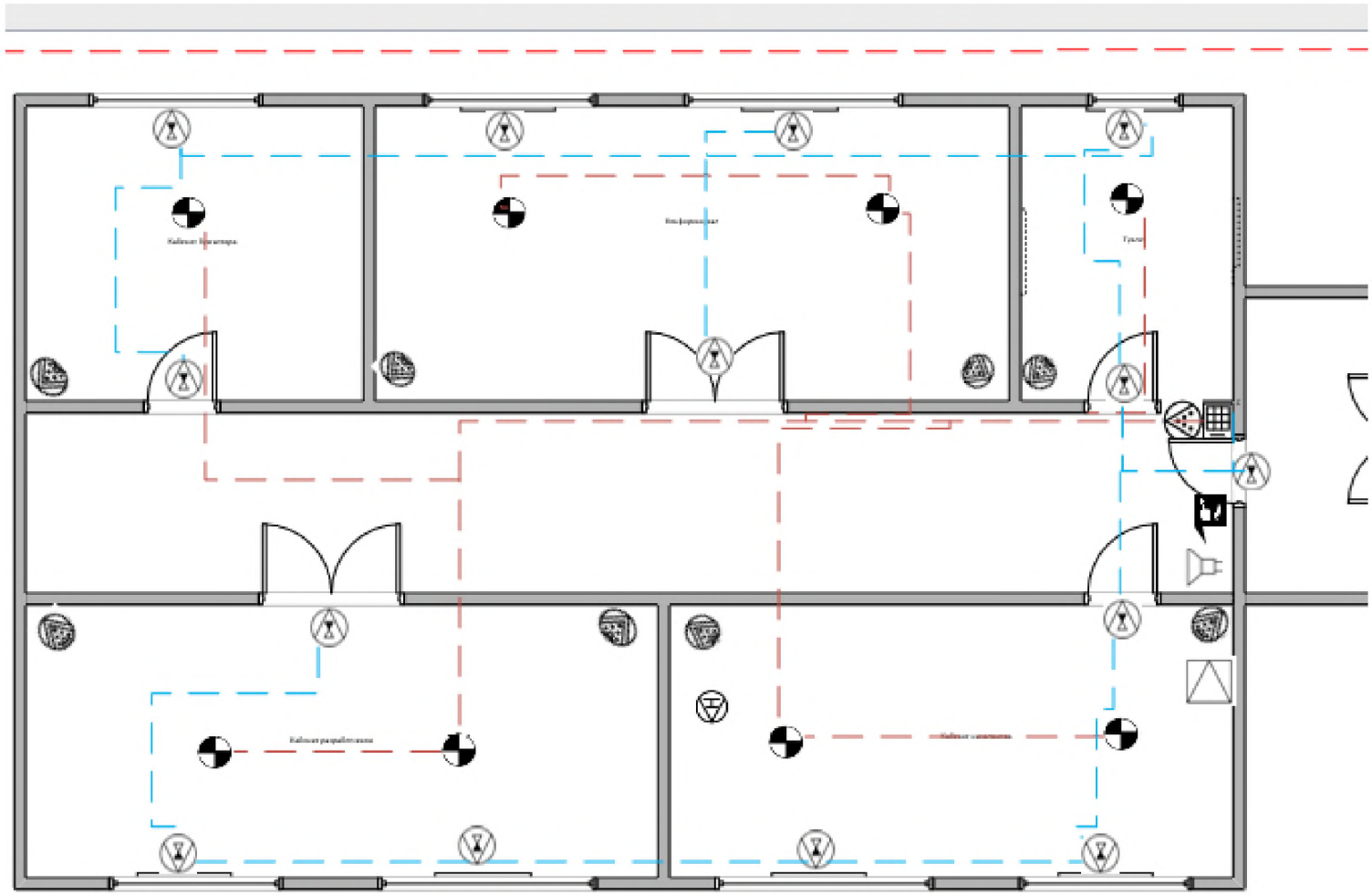

До електрощитової на поверсі
До обладнання провайдера на поверсі
До електрощитової на поверсі
1905 8мм
3,9 м
3,9 м
1,5 м
6,3 м
8,0 м
3,0 м
8,6 м
8,6 м
10,0 м
Загальний Коридор
0,6 м
1,3 м
0,5 м
5,8 м
17,3 м
Інше офісне приміщення

Умовні позначення

ДОДАТОК Е


3,0 м
8,6 м
8,0 м
8,6 м
6,3 м
1,5 м
17,3 м
Інше офісне приміщення
УМОВНІ ПОЗНАЧЕННЯ

ДОДАТОК Є



Умовні позначення

Пожежний димовий сповіщувач

Магнітоконтактний сповіщувач

Скомбінований (ІЧ + акустичний) сповіщувач

Об'ємний інфрачервоний сповіщувач

Тревожна кнопка

ПКП

Клавіатура

Пожежна кнопка

світлошумовий сповіщувач

Лінії постачання пожежних сповіщувачів

Лінії постачання охоронних сповіщувачів

N

W

O

S