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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Пінчука Костянтина Олександровича*

академічної групи *125-18ск-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Корнієнко В.І.			
розділів:				
спеціальний	ст викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Пінчуку К.О.* **академічної групи** *125-18ск-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка політики безпеки інформації інформаційно-Телекомунікаційної системи ТОВ «Шевченко»*

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Обстеження фізичного середовища, обстеження обчислювальної системи, визначення загроз і вразливостей	21.05.2021
Розділ 2	Визначення функціонального профілю захищеності, проектування політики безпеки	01.06.2021
Розділ 3	Обґрунтування витрат на впровадження політики безпеки	14.06.2021

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

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: 15.06.2021

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

РЕФЕРАТ

Пояснювальна записка: 67 ст., 8 рис., 15 табл., 4 додатків, 10 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Шевченко».

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

У першому розділі описаний об'єкт: рід діяльності, фізичне середовище, в якому знаходиться об’єкт, устаткування, інформаційна система, програмне забезпечення, інформаційні потоки. Виконано класифікацію інформації, що циркулює в ІТС, визначений перелік джерел загроз, перелік вразливостей та перелік актуальних для ІТС загроз.

У другому розділі описано наявні в ІТС критерії захищеності та виконано вибір нових додаткових рекомендованих критеріїв захищеності, були розроблені рекомендації щодо розділів політики безпеки, що забезпечують реалізацію рекомендованих критеріїв захищеності та захист від актуальних для підприємства загроз.

В третьому розділі були розраховані витрати на впровадження та щорічну підтримку засобів та заходів, описаних у запропонованих розділах політики безпеки, оцінено можливі збитки від реалізації актуальних загроз. Була визначена економічна доцільність введення в експлуатацію рекомендацій щодо політики безпеки, розроблених в другому розділі.

Практичне значення проекту полягає в підвищенні інформаційної безпеки ТОВ «Шевченко».

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ.

РЕФЕРАТ

Пояснительная записка: 67 с., 8 рис., 15 табл., 4 приложения, 10 источников.

Объект разработки: политика безопасности информации информационно-телекоммуникационной системы ООО «Шевченко».

Цель проекта: повышение уровня безопасности информации в ИТС ООО «Шевченко», разработка решений для защиты от угроз информационной безопасности.

В первом разделе описан объект: род деятельности, физическая среда, в которой находится объект, оборудование, информационная система, программное обеспечение, информационные потоки. Выполнена классификация информации, которая циркулирует в ИТС, определен список источников угроз, список уязвимостей и перечень актуальных для ИТС угроз.

Во втором разделе описаны присутствующие в ИТС критерии защищенности и осуществлен выбор новых дополнительных рекомендованных критериев защищенности, были разработаны рекомендации касательно разделов политики безопасности, которые обеспечивают реализацию рекомендованных критериев защищенности и защиту от актуальных для предприятия угроз.

В третьем разделе были рассчитаны затраты на внедрение и ежегодную поддержку средств и мероприятий, описанных в предложенных разделах политики безопасности, оценены возможные убытки от реализации актуальных угроз. Была определена экономическая целесообразность введения в эксплуатацию рекомендаций касательно политики безопасности, разработанных во втором разделе.

Практическое значение проекта состоит в повышении информационной безопасности ООО «Шевченко».

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ.

THE ABSTRACT

Explanatory note: 67 p., 8 fig., 15 tab., 4 appendices, 10 sources.

Object of elaboration: information security policy for information and telecommunication system of «Shevchenko» LLC.

The purpose of the project: increasing the level of information security in ITS «Shevchenko» LLC, creation of solutions for protection against threats to information security.

In the first section the object has been described: type of activity, the physical environment in which the object is located, equipment, information system, software, information flows. The classification of information that circulates in the ITS has beenmade, the list of threats sources, the list of vulnerabilities and the list of threats relevant to ITS have been defined.

In the second section has been described the security criteria available in the ITS and selected new additional recommended security criteria, have been created recommendations for security policy sections that ensure the implementation of the recommended security criteria and protection from current threats.

In the third section, the costs of implementation and annual support of the means and measures, described in the proposed sections of the security policy, have been calculated, and possible losses from the realization of relevant threats have been defined. The economic benefit of safety policy recommendations, developed in the second section, implementation has been determined.

The practical significance of the project is to increase information security of «Shevchenko» LLC.

SECURITY POLICY, MODEL OF THREATS, INFORMATION SECURITY, VULNERABILITIES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічний захист інформації;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

Все більше сфер діяльності людини переходить до глобальної інформатизації. В кожній інформаційній системі з'являється інформація, цілісність, доступність та конфіденційність грає дуже важливу роль для господаря інформації, вона набуває цінності, отже, її слід захищати від стороннього або внутрішнього втручання. Саме тому на сьогоднішній день створення заходів захисту інформації є завданням з високим пріоритетом.

Для створення належного засобу захисту інформації, а саме політики безпеки, необхідно обстежити обчислювальну систему та інформаційні потоки на ОІД, визначити можливі загрози для безпеки інформації. На основі даного обстеження можна зробити висновки щодо захищеності системи та визначити проблеми, що будуть вирішенні при виконанні актів політики безпеки.

Для ефективної роботи політики безпеки в ній необхідно визначити чіткі правила з використання інформаційної системи кожним співробітником, необхідно визначити відповідальних за дотриманням правил політики безпеки.

Процес створення політики безпеки, обстеження ОІД та створення КСЗІ описано в НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Для визначення функціонального профілю АС використовується НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» та НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» використовується для визначення функціонального профілю автоматизованої системи.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ОІД

Об`єктом інформаційної діяльності є агентство з розробки веб-додатків ТОВ «Шевченко», що спеціалізується на веб-дизайні і знаходиться за адресою: Дніпропетровська область, м. Дніпро, пр. Д. Яворницького, буд. 122. Будівля, де розташована організація – чотириповерхова, ОІД розташовано на першому поверсі. Організація надає послуги з веб-дизайну, а саме компанія створює ефективний дизайн для взаємодії з користувачем, поєднаний з інтерфейсом для мобільних додатків та веб-сторінок. Доловлюючись з іншими підприємствами, компанія працює на умовах аутсорсингу зі сторонніми компаніями, які, в свою чергу, диктують вимоги до розроблюємого проекту.

Підприємство працює п’ять робочих днів на тиждень з 9:00 до 18:00. Прибирання виконується кожен день з 12:00 до 12:30 найманими працівниками (прибиральником офісного центру). На підприємстві є обідня перерва з 12:00 до 13:00.

Ключі від офісу знаходяться у директора та у системного адміністратора. Підприємство підписало договір про отримання послуг від охоронної компанії. В неробочий час у разі спрацювання сигналізації до приміщення виїжджає силова бригада.

1.2 Обґрунтування необхідності створення КСЗІ

Згідно з НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»:

«6.1.1.1 Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

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

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

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

– оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.» [1]

Отже, згідно з прийнятим власником інформації рішенням, на підприємстві необхідно створити КСЗІ, оскільки в ІТС обробляється інформація, що є комерційною таємницею, та інформація, захист якої передбачається договорами між клієнтами та компанією. Також, необхідно захищати інформацію, що становить персональні дані клієнтів та робітників, згідно з Законом України «Про захист персональних даних»:

«Стаття 24. Забезпечення захисту персональних даних

1 Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.» [2]

Крім того, компанія планує розширювати ринок збуту, співпрацювати, в тому числі, з закордонними компаніями. Тому необхідно впроваджувати захист інформації на належному рівні для підвищення рівня довіри з боку клієнтів.

1.3Обстеження ОІД

1.3.1 Обстеження фізичного середовища ОІД

Стіни будівлі, в якій розташовано об'єкт виконано з білої цегли (силікатна). Фундамент виконано з бетону, дах покритий руберойдом, територія навколо будівлі покрита асфальтом. Ситуаційний план наведено на рисунку 1.1. На

рисунку 1.2 наведено комунікації у будівлі, де розташовано ІТС.

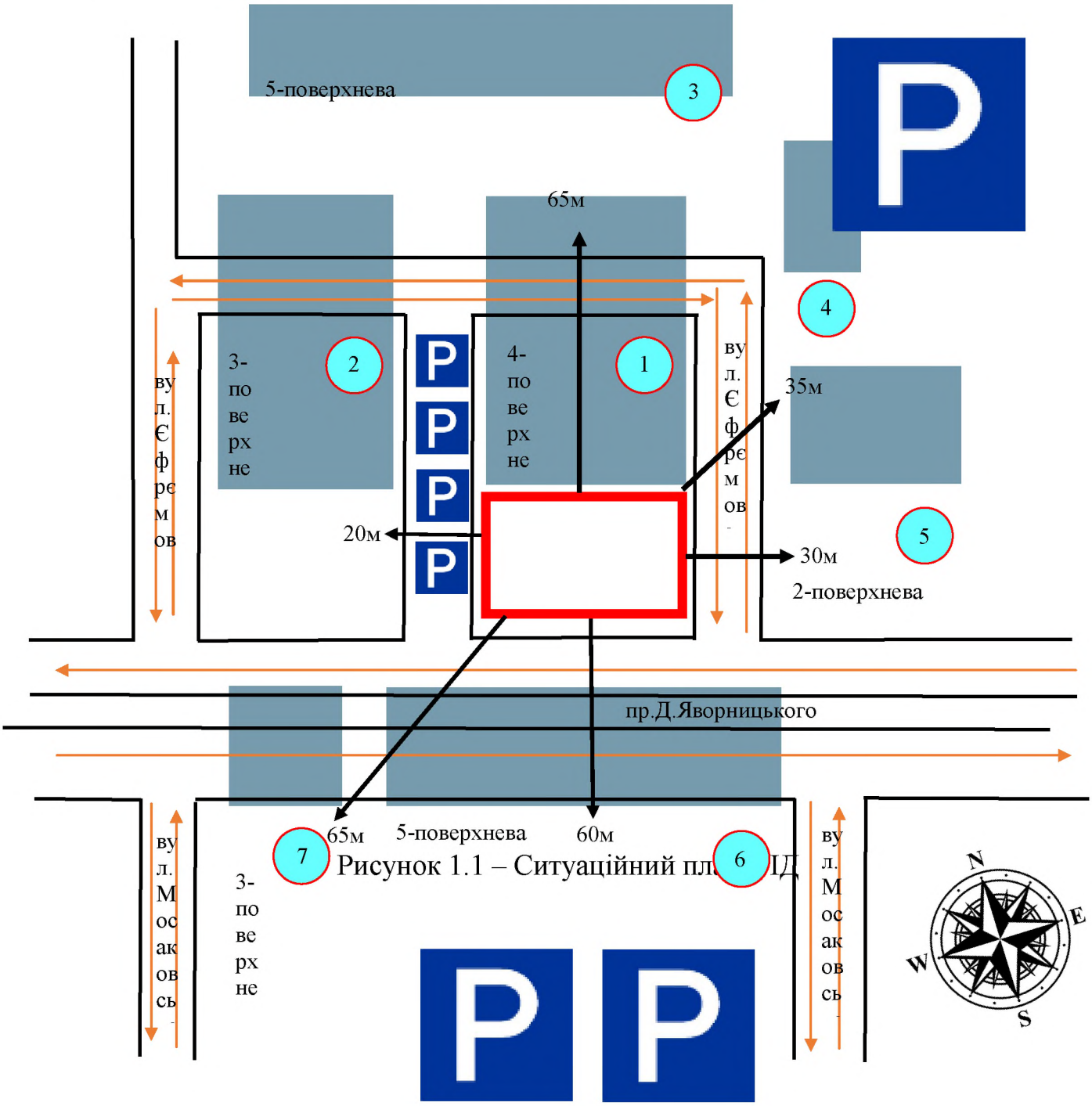


Рисунок 1.1 – Ситуаційний пл ІД

Умовні позначення

Місце для паркування

Напрям руху транспорту

№ Номер будівлі

Відстань від межі ОІД до будівель

Межа ОІД

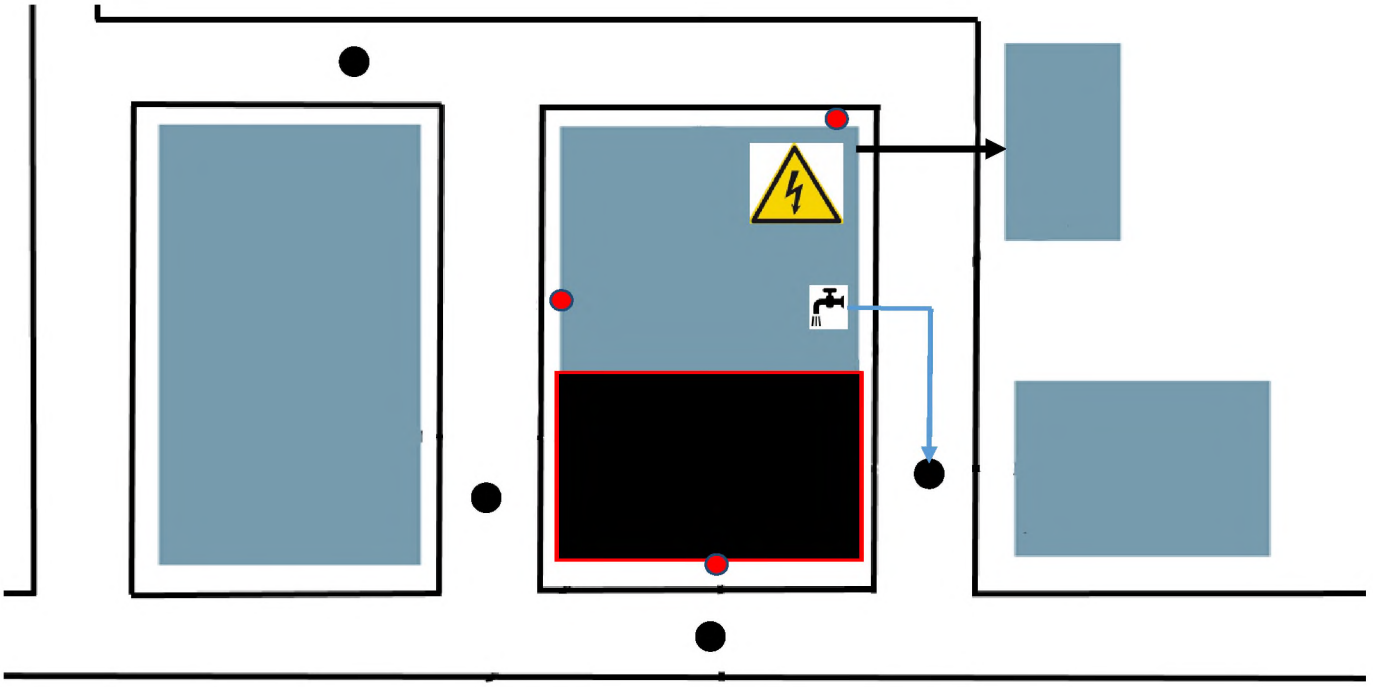


Рисунок 1.2 – Комунікації

Умовні позначення

Щитова

Люк

Лінія водопостачання

Межа КЗ

Під'єдання у будівлі до мережі водопостачання

Лінія електропостачання від ТП

Межа ОІД

Вхідні двері

В таблиці 1.1 наведено будівлі, що знаходяться поруч з ОІД.

Таблиця 1.1 – Будівлі, що знаходяться поруч з ОІД

Номер	Тип об`єкту	Адреса	Мінімальна відстань до ОІД
1	Офісна будівля, в якій знаходиться ОІД	Пр.Д.Яворницького,122	0м
2	Магазин	Пр.Д.Яворницького,121	20м
3	Житловий будинок	Пр.Д.Яворницького,125	65м
4	Трансформаторна підстанція ТпТ6112	Пр.Д.Яворницького,128	35м
5	Магазин	Пр.Д.Яворницького,134	30м
6	Житловий будинок	Пр.Д.Яворницького,133	60м
7	Житловий будинок	Пр.Д.Яворницького,131	65м

Вікна металопластикові. Вхідні двері залізні з двома замками, відчиняються звичайними ключами. Електропостачання надається з трансформаторної подстанції. Водопостачання підведено під землею. Будівлю поділено на декілька офісних приміщень. Внутрішні та зовнішні стіни офісу виконані з силікатної цегли. Товщина зовнішніх стін – 350 мм, внутрішніх несучих стін – 220 мм, внітрішні перегородки з гіпсокартону завтовшки 65 мм. Вікна металопластикові подвійний склопакет, 2100 х 1500 мм. Вхідні двері сталеві 1200 мм шириною і

висотою 2000 мм. Моноблочний замок, вікривається звичайним ключем. Висота стелі складає 3 м, підлогу виконано з паркету.

Контрольована зона обмежена з північної сторони цегляною стіною, за якою інші офісні приміщення, з інших сторін обмежена стінами будівлі. Розподільний щит загальний на всю будівлю, розташований з північної сторони.

Офіс заключив контракт з охоронною службою, у разі несанкціонованого проникнення на об'єкт, пульт передає повідомлення до диспетчерів охоронної служби.

На рисунку 1.3 наведено генеральний план ОІД. На рисунку 1.4 представлено комунікації, що знаходяться всередині будівлі.

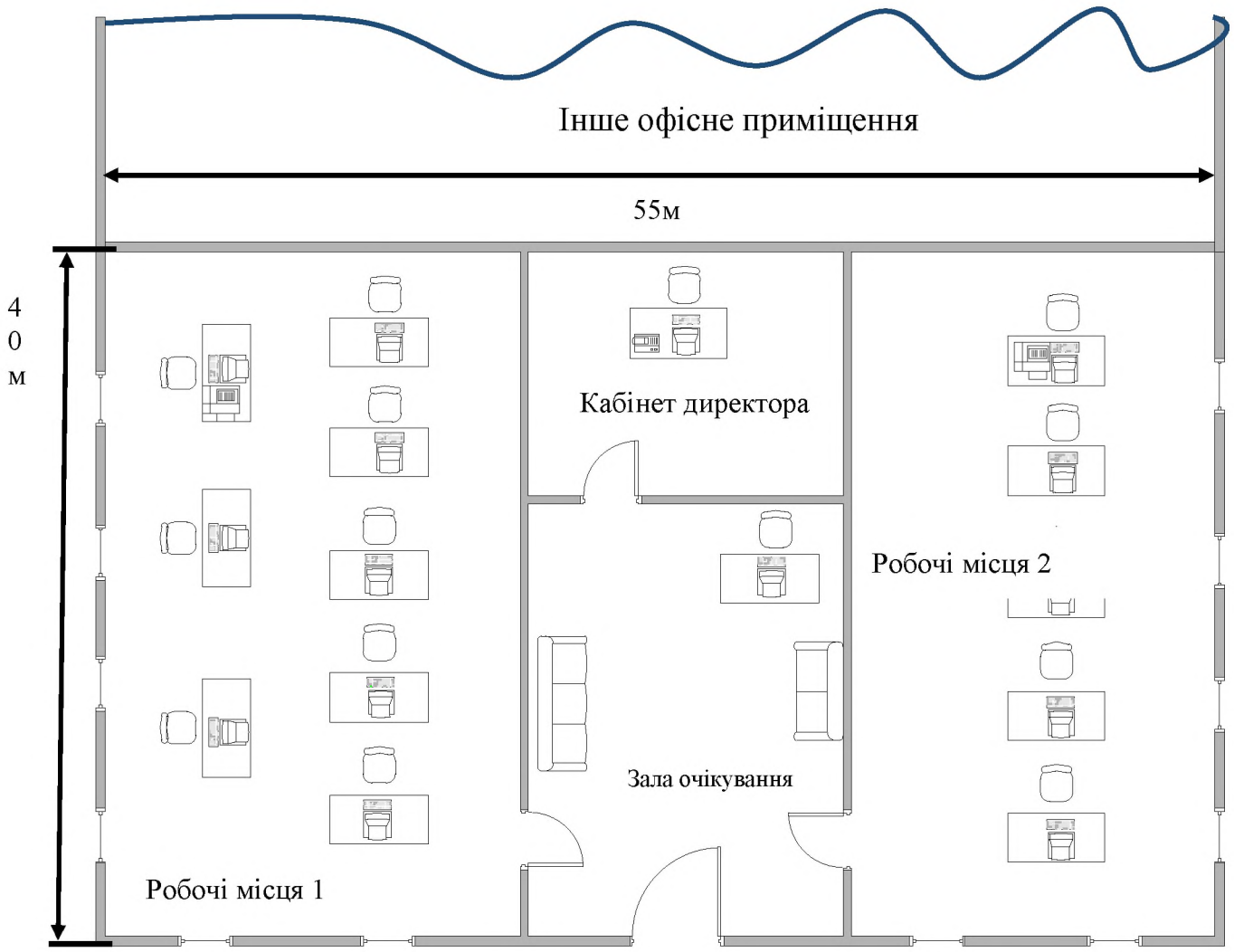
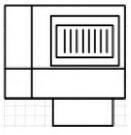


Рисунок 1.3 – Генеральний план ОІД

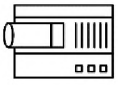
Умовні позначення

Стіна

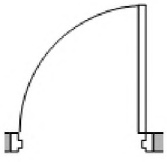


Багатофункціональний пристрій

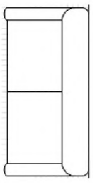
Стіл з ПК



Точка доступу



Двері



Диван

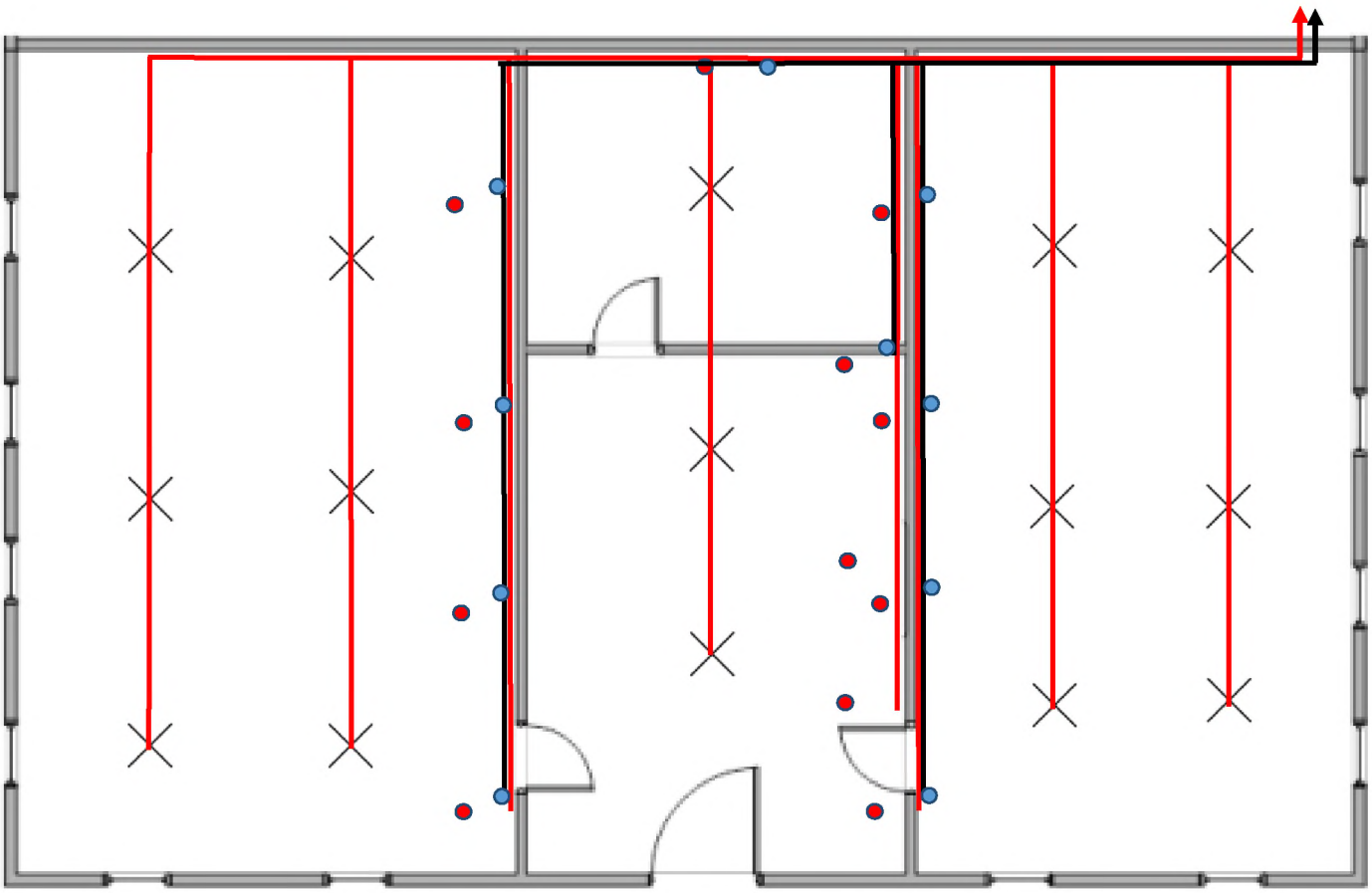
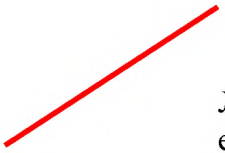


Рисунок 1.4 – Комунікації всередині будівлі

Умовні позначення

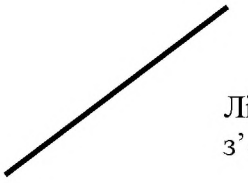


Лінія електроживлення

Електрична розетка

Лампа на стелі

Розетка RJ-45



Лінія Інтернет-з’єднання

На рисунку 1.5 зображено систему сигналізації на ОІД.

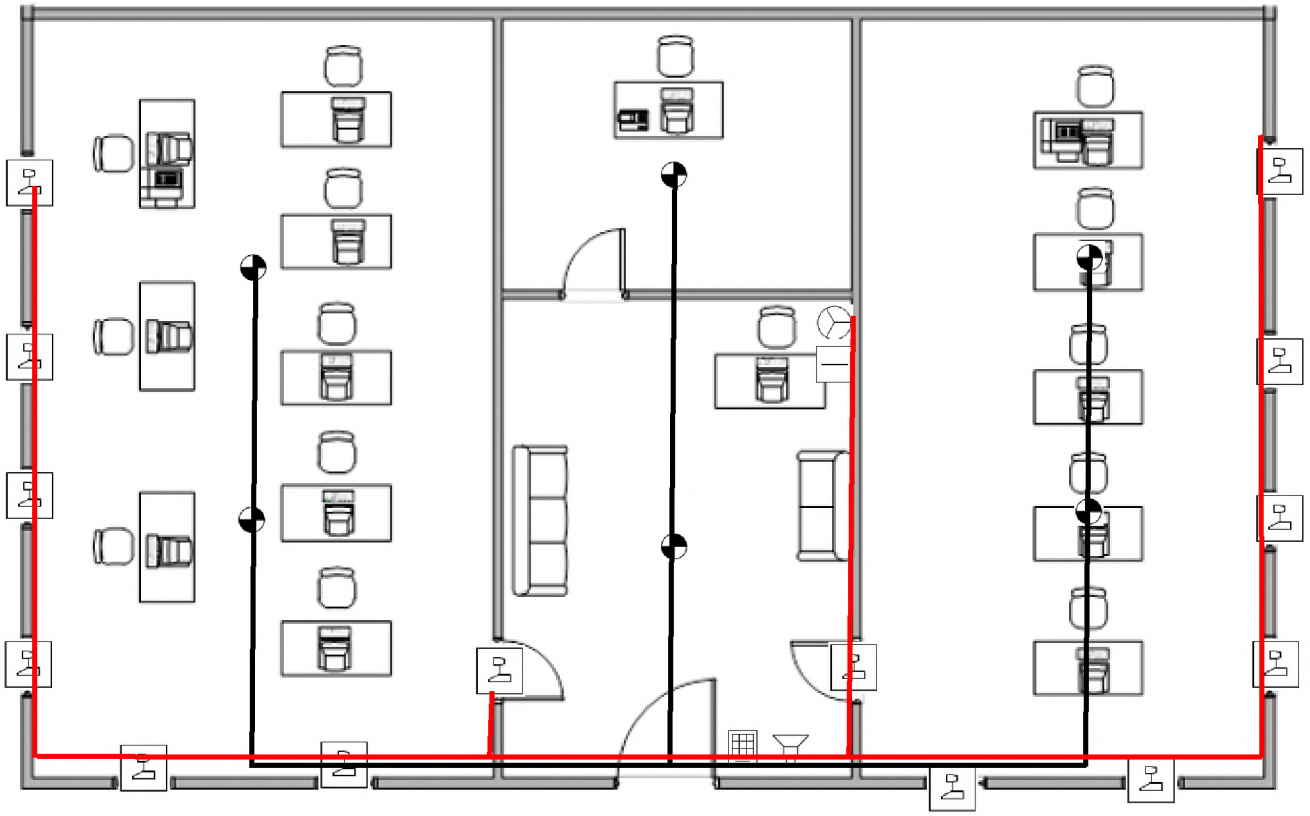
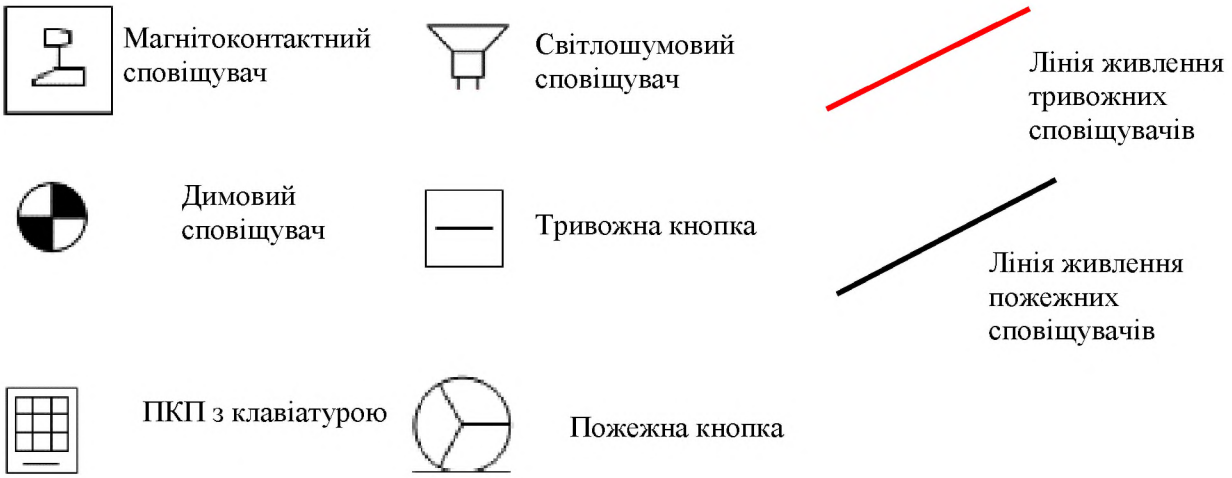


Рисунок 1.5 – Система сигналізації

Умовні позначення



Опис основних технічних засобів на ОІД наведено у таблиці 1.2.

Таблиця 1.2 – Опис основних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
1	Системний блок РС-1	Lenovo	V570c	ZXF958471	Під столом у залі очікування	1,5	1,3

Продовження таблиці 1.2

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
2	Системний блок PC-2	Apple	Air	ZXF958472	Під столом у кабінеті директора	1,5	0,9
3	Системний блок PC-3	Asus	VivoBook	ZXF958473	Під столом у кабінеті з робочими місцями №1	1,5	0,9
4	Системний блок PC-4	Xiaomi	RedmiBook 14	ZXF958474	Під столом у кабінеті з робочими місцями №2	2,5	0,8
5	Системний блок PC-5-15	Expert PC	Ultimate	ZXF958475-ZXF958485	Під столом у кабінеті з робочими місцями	1,5	1,6
6	Монітор 1	LG	22MK430H-B	FF1234561	На столі у залі очікування	1,4	1,3
7	Монітор 2			FF1234562	На столі у директора	1,3	0,9
8	Монітор 3			FF1234563	На столі у кабінеті з робочими місцями №1	1,5	0,9
9	Монітор 4			FF1234564	На столі у кабінеті з робочими місцями №2	2,3	0,8
10	Монітор 5-15			FF1234565-FF1234575	На столі у кабінеті з робочими місцями	1,4	1,6
11	Клавіатура 1	4a-tech	A4Tech KR-83 PS/2	KBL158741	На столі	1,3	1,3
12	Клавіатура 2			KBL158742	На столі	1,5	0,9
13	Клавіатура 3			KBL158743	На столі	1,4	0,9
14	Клавіатура 4			KBL158744	На столі	2,4	0,8
15	Клавіатура 5-15			KBL158745-55	На столі	1,3	1,6
16	БФП	XPrint	xp-q200	MF847162	На столі №1	1,5	1,9

Продовження таблиці 1.2

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ДТЗС, м
17	БФП	XPrint	xp-q200	MF847163	На столі у кабінеті з робочими місцями №2	1,5	1,9
18	Маршрутизатор	D-link	D-Link DIR-825/AC/G	DLD798941	На столі у кабінеті директора	4	1,4

Таблиця 1.3 – Опис допоміжних технічних засобів

№	Назва	Марка	Модель	Серійний номер	Розміщення	Мінімальна відстань від елем. до кордонів КЗ, м	Мінімальна відстань до ОТЗ, м
1	Навісна Led лампа освітлення	TL-Office	15 L600 O 4K	KIB465661 KIB465662 KIB465663 KIB465664 KIB465665 KIB465666 KIB465667 KIB465668 KIB465669 KIB465670 KIB465671 KIB465672 KIB465673 KIB465674 KIB465675	На стелі	2 2,1 2,3 2,3 1,7 3 5 5 3 2 2 2 2 2.2 2.3	1 3 2 3 5 4 3 5 7 0,9 1 4 7 3 5
2	Маніпулятор миша 1	4a-tech	OP-720	MAT41575	На столі у залі очікування	1,4	0,2
3	Маніпулятор миша 2			MAT41576	На столі у кабінеті директора	1,3	0,2
4	Маніпулятор миша 3			MAT41577	На столі у кабінеті з робочими місцями №1	1,5	0,2
5	Маніпулятор миша 4			MAT41578	На столі у кабінеті з робочими місцями №2	2,3	0,2
6	Маніпулятор миша 5			MAT41579	На столі у кабінеті з робочими місцями	1,4	0,2
7	Маніпулятор миша 5	4a-tech	OP-720	MAT41580	На столі	1,4	0,2

Інформація зберігається як у паперовому вигляді, так і на зйомних носіях. Паперові носії зберігаються в директора у шафі стола, зйомні носії інформації зберігаються у ящиках столів на робочих місцях.

1.3.2 Обстеження обчислювальної системи ОІД

На підприємстві використовується 15 персональних комп'ютерів, кожний з яких закріплений за певним працівником. Також на підприємстві присутні два багатофункціональних пристрої, котрі закріплені за кожним відділом розробників. Мережу Wi-Fi для сторонніх відвідувачів надає роутер, ця мережа окрема від локальної мережі працівників. Вся інформація, що необхідна для функціонування підприємства зберігається у хмарному сховищі компанії.

На рисунку 1.6 зображено структурну схему мережі організації, взаємозв'язок пристроїв та мереж між собою.

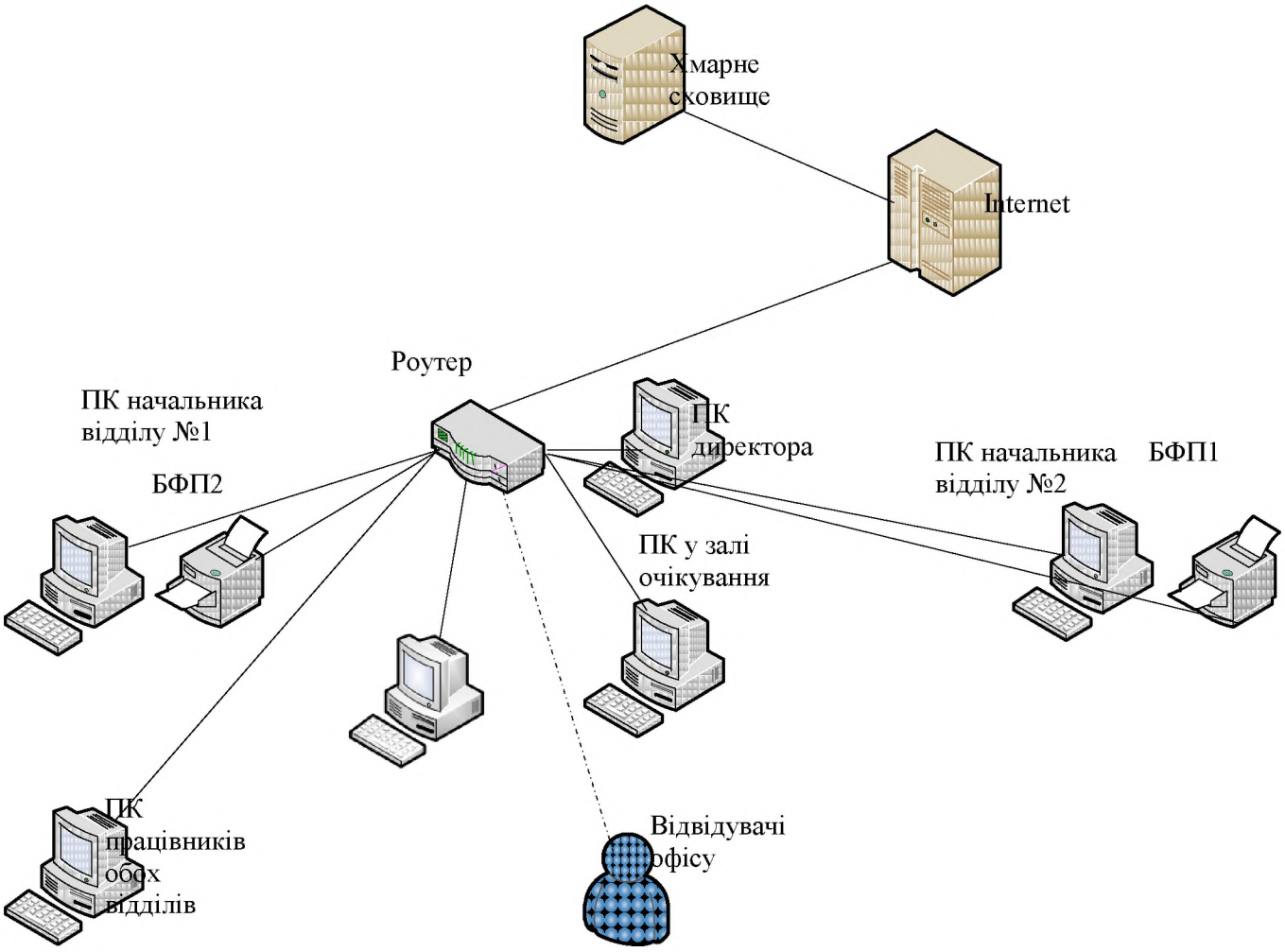


Рисунок 1.6 – Структурна схема мережі організації

Топологія мережі представлена «зіркою». Кожен з користувачів мережі має доступ до Інтренету. Кожен з комп'ютерів та принтерів під'єднується до мережі через кручену пару в окремій виділеній мережі до комутатору, відвідувачі офісу під'єднуються через Wi-Fi до окремої мережі. Роутер керує протоколом DHCP, який зазвичай вимкнено, IP-адреси статичні для пристроїв, що використовуються під час роботи. Wi-Fi мережа відкрита, але налаштування захищені паролем, який відомий лише системному адміністратору. Кожен ПК закріплений за певним працівником, відповідно до закріплення і розділяються права у системі. За торговим представником закріплено ПК-1, за директором – ПК-2, за менеджером першого відділу – ПК-3, за менеджером другого відділу ПК-5, за системним адміністратором ПК-4, за кожним із розробників ПК-6-15. Опис компонентів пристроїв наведено у таблиці 1.4.

Таблиця 1.4 – Опис пристроїв та їх компонентів

№	Найменування	Специфікація
1	ПК ZEVS PC 9350UX	Intel Core i5-3570 / RAM 16 ГБ / HDD 500 ГБ / Nvidia GTX1050 2GB
2	ПК Artline Gaming X48 v07	AMD Ryzen 5 1600 (3.2 - 3.6 ГГц) / RAM 8 ГБ / HDD 1 ТБ / Nvidia GeForce GTX 1650, 4 ГБ
3	ПК Everest Home 4070	Intel Core i3-10100F (3.6 - 4.3 ГГц) / RAM 8 ГБ / HDD 1 ТБ / NVidia GeForce GTX 1050 Ti, 4 ГБ
4	ПК HP 290 G1 MT	Intel Core i5-8500 (3.0 - 4.1 ГГц) / RAM 4 ГБ / HDD 1 ТБ / Intel UHD Graphics 630
5-15	ARTLINE Business B25 v26	Intel Pentium Gold G6400 (4.0 ГГц) / RAM 4 ГБ / SSD 120 ГБ / Intel UHD Graphics 610

На всіх комп'ютерах встановлено ліцензійний Windows 10. На підприємстві функціонує 6 зйомних носіїв, що закріплені за директором, начальниками відділів та системним адміністратором. Опис та характеристики встановленого ПЗ зазначено у таблиці 1.5.

Таблиця 1.5 – Опис встановленого в ІТС ПЗ

Тип ПЗ	Повна назва	Версія	Ліцензія	Де встановлено
Системне, спеціалізоване	Windows Defender	10.0.17763.1	корпоративна	Всі комп`ютери
Прикладне	Adobe Illustrator	20.0	корпоративна	Комп`ютери розробників
Прикладне	Adobe Photoshop	23.0.1	-	Комп`ютери розробників
Прикладне	Inkskape	0.92.4	GNU	Комп`ютери розробників
Спеціалізоване	Wireshark	2.6.5	GNU GPL	Комп'ютер системного адміністатора
Спеціалізоване	CCleaner	5.50.0.6911	Free Edition	Комп'ютер системного адміністатора
Спеціалізоване	Total Network Inventory 3	3.6.0	-	Комп'ютер системного адміністатора
Спеціалізоване	Total Software Deployment 2	1.1.2	-	Комп'ютер системного адміністатора
Прикладне	Microsoft Teams	1416	корпоративна	Всі комп`ютери
Прикладне	Microsoft Outlook	3.0.34	корпоративна	Всі комп`ютери
Системне, прикладне	Microsoft Edge	44.17763.1.0	корпоративна	Всі комп`ютери
Прикладне	MS Office 365 ProPlus	1808	корпоративна	Всі комп`ютери
Прикладне	Microsoft OneDrive	19.012.0121.0011	корпоративна	Всі комп`ютери
Прикладне	1С: Бухгалтерія	8.1	однокористувачева ліцензія – 2 шт.	Комп'ютер Директора

1.3.3Інформаційне середовище ОІД

Інформація, що циркулює та зберігається на підприємстві, правовий режим, режим доступу та місце зберігання наведено у таблиці 1.6.

Таблиця 1.6 – Інформація, що циркулює на об`єкті

№	Інформація	Режим доступу	Правовий режим	Місце зберігання
1	Накази керівництва	Для службового використання	Відкрита	Зберігається у хмарному сховищі або паперовому вигляді
2	Відомості про нові замовлення	Для службового використання	Комерційна таємниця	Зберігається у хмарному сховищі
3	Звіти з продажів	Для службового використання	Комерційна таємниця	Зберігається на комп'ютері директора та у хмарному сховищі та паперовому вигляді
4	Бухгалтерські звіти	Для службового використання	Конфіденційна	У електронному вигляді зберігаються на ПК директора та зовнішньому носії директора, у паперовому вигляді зберігається у шухляді стола директора
5	Готові замовлення	З обмеженим доступом	Комерційна таємниця	Зберігається на комп'ютерах розробників та у хмарному сховищі

Продовження таблиці 1.6

№	Інформація	Режим доступу	Правовий режим	Де зберігається
6	Архівовані завершені замовлення за договором з замовником	З обмежени мдоступом	Конфіденційна	Зберігається у хмарному сховищі
7	Замовлення на стадії розробки	Для службового використання	Комерційна таємниця	Зберігається на ПК розробників та хмарному сховищі
8	Клієнтська база	Для службового використання	Комерційна таємниця	Зберігається на ПК торгового представника
9	Персональні дані працівників	Для службового використання	Конфіденційна	Зберігається на паперових носіях у директора в шухляді
10	Відомості щодо заробітних плат	Для службового використання	Конфіденційна	Зберігається на ПК начальників відділів та ПК директора.
11	Дані для доступу до системи	Для службового використання	Конфіденційна	Зберігається на ПК системного адміністратора

Продовження таблиці 1.6

№	Інформація	Режим доступу	Правовий режим	Де зберігається
12	Звіт системного адміністратора	З обмеженим доступом	Для службового використання	Зберігається на ПК директора та на ПК системного адміністратора

Правила зберігання зйомних та паперових носіїв на підприємстві не регламентуються, спеціальні місця для зберігання відсутні. У таблиці 1.7 наведені рівні конфіденційності, цілісності та доступності інформації, що циркулює на підприємстві.

Таблиця 1.7 – Рівні конфіденційності, цілісності та доступності інформації

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Накази керівництва	К1	Ц3	Д2
Відомості про нові замовлення	К2	Ц4	Д4
Звіти з продажів	К1	Ц1	Д1
Бухгалтерські звіти	К3	Ц4	Д3
Готові замовлення	К4	Ц4	Д4
Архівовані завершені замовлення за договором з замовником	К0	Ц3	Д1
Замовлення на стадії розробки	К4	Ц1	Д3
Клієнтська база	К3	Ц3	Д3
Персональні дані працівників	К1	Ц2	Д2
Відомості щодо заробітних плат	К2	Ц4	Д4
Дані для доступу до системи	К3	Ц3	Д3
Звіт системного адміністратора	К2	Ц1	Д1

Рівні конфіденційності:

– К0 – рівень конфіденційності, при якому збитки у разі розкриття інформації третім особам не є суттєвими, не конфіденційна інформація;

– К1 – рівень, при якому компанія зазнає незначних збитків при розкритті інформації третім особам;

– К2 – компанія зазнає значних збитків при розкритті інформації третім особам;

– К3 – рівень, що може призвести до значної втрати репутації або великих матеріальних витрат;

– К4 – критичний рівень конфіденційності інформації, що може призвести до краху компанії

Рівні цілісності:

– Ц0 – рівень цілісності, втрата якого не понесе серйозної загрози для інформації;

– Ц1 – рівень, при втраті якого значних збитків компанія не зазнає;

– Ц2 – рівень, втрата якого може завдати відчутних збитків компанії;

– Ц3 – рівень, втрата якого може завдати значних матеріальних збитків;

– Ц4– рівень, що може призвести до закриття компанії

Рівні доступності:

– Д0 – рівень доступності, при втраті якого можна знехтувати втратою доступності інформації;

– Д1 – рівень доступності, при втраті якого компанія зазнає незначних збитків;

– Д2 – рівень доступності, при втраті якого компанія втратить репцтацію або зазнає значних збитків;

– Д3 – рівень, що може призвести до значних матеріальних втрат або дозначної втрати репутації організації;

– Д4 – критичний рівень, у разі втрати доступності може призвести до закриття компанії.

1.3.4 Середовище користувачів ІТС

Обов’язки керівництва і працівників:

Директор:

- затвердження відомостей, що містять інформацію про заробітну плату працівників;
- створення вакансій на сайтах для пошуку робітників, співбесіди з новими робітниками, звільнення та прийняття на роботу;
- організація ефективного взаємозв’язку всередині команди, контроль діяльності співробітників;
- ведення бухгалтерського обліку підприємства, ведення відповідної документації;
- звітність перед податковою службою;
- моніторинг позицій компанії на ринку, визначення цілей для підприємства;
- контроль якості послуг для клієнтів, зберігання іміджу підприємства серед конкурентів;
- реалізація поліпшення умов для робітників, контроль дотримання прав робітників;
- визначення розміру, оформлення відомостей та нарахування заробітної плати;
- визначення цін на замовлення компанії;
- контроль виконання вимог договорів з боку компанії перед клієнтами;

Системний адміністратор:

- контроль зафіксованих подій у журналі подій;
- моніторинг стану локальної мережі та підтримання її у дієздатності;
- інсталяція необхідного програмного забезпечення та актуалізація існуючого ПЗ;
- контроль інформаційної безпеки підприємства;

– модернізація обчислювальної системи за необхідності;

– у разі неполадок в обчислювальній системі, їх виправлення;

– створення резервних копій;

– відновлення системи після збоїв;

– конфігурація оновлень операційної системи.

Торговий представник:

– організація рекламної діяльності компанії, розповсюдження інформації про діяльність підприємства;

– аналіз ринку діяльності компанії, нововведень у сфері веб-дизайну;

– контроль виконання зобов`язань компанії перед клієнтами;

– аналіз ситуації на ринку, аналіз перспектив компанії, а також ризиків;

– укладання угод з клієнтами;

– контроль сплат клієнтами за виконані замовлення.

Розробники:

– виконання замовлень згідно з технічним завданням, виданим керівником підрозділу – створення, налагодження та розвертання продуктів компанії

Керівники відділів:

– створення технічного завдання згідно залученого договору с клієнтом, контроль за виконанням проектів, моніторинг своєчасності виконання певних етапів розробки.

Вся необхідна інформація для функціонування підприємства передається через хмарне сховище або зйомні носії інформації.

На рисунку 1.7 зображено інформаційні потоки на підприємстві.

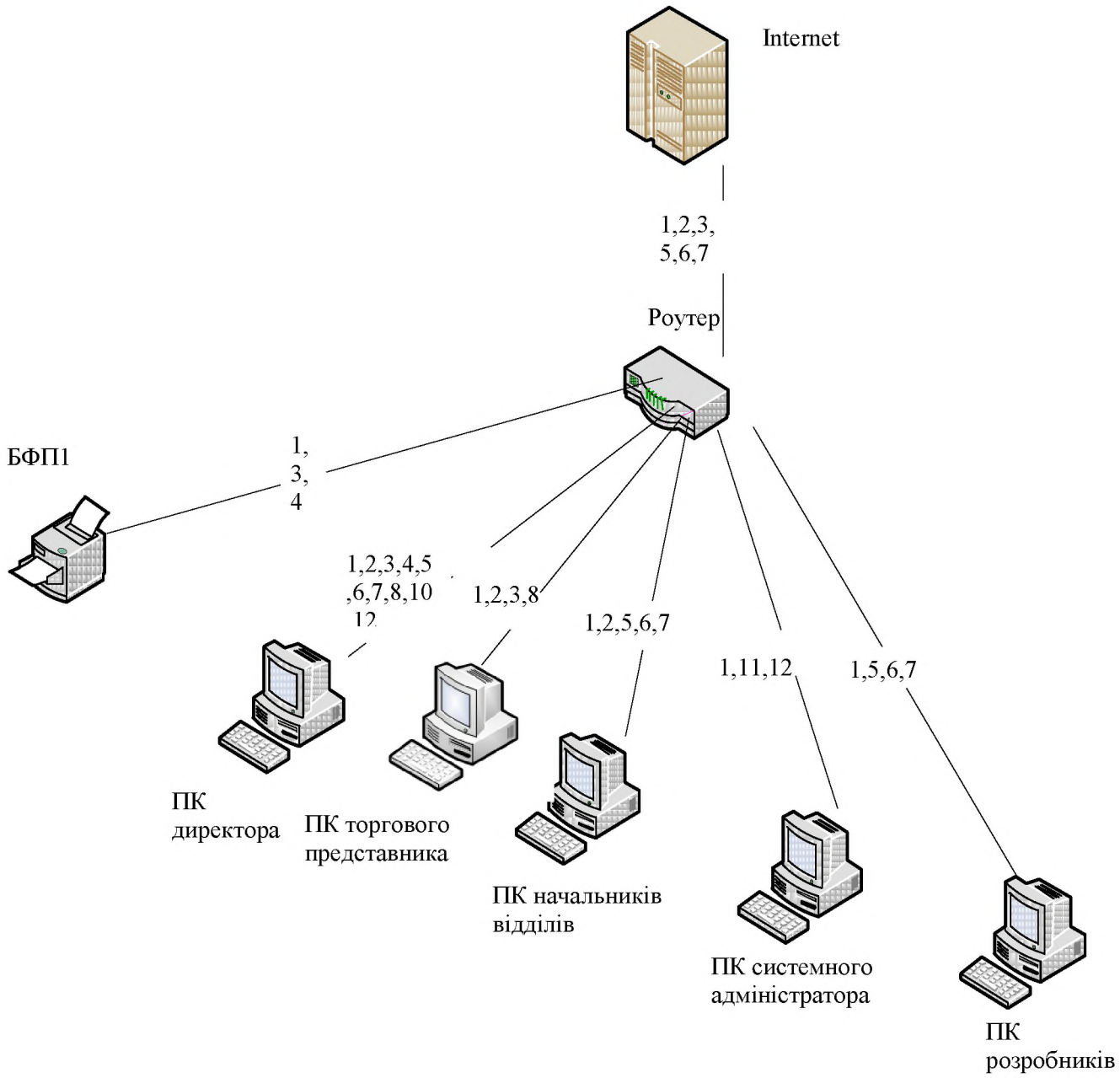


Рисунок 1.7 - Інформаційні потоки на підприємстві

Перелік документів та ПЗ (див. табл. 1.8):

1 Перелік документів;

1.1 Накази керівництва;

1.2 Відомості про нові замовлення;

1.3 Звіти з продажів;

1.4 Бухгалтерські звіти;

1.5 Завершені замовлення;

1.6 Архівовані завершені замовлення;

1.7 Замовлення на стадії розробки;

1.8 Клієнтська база;

1.9 Персональні дані працівників;

1.10 Зарплатні відомості;

1.11 Дані для доступу до системи;

1.12 Звіт системного адміністратора;

2 Перелік ПЗ;

2.1 Windows Defender;

2.2 Adobe Illustrator;

2.3 Adobe Photoshop;

2.4 Inkskape;

2.5 Microsoft Edge;

2.6 MS Office 365 ProPlus;

2.7 Microsoft OneDrive;

2.8 1С: Бухгалтерія;

2.9 Wireshark;

2.10 CCleaner;

2.11 Total Network Inventory 3;

2.12 Microsoft SharePoint;

2.13 Microsoft Teams;

2.14 Microsoft Outlook.

Матриця доступу програмного забезпечення та інформації наведено у таблиці 1.8.

Таблиця 1.8 Матриця доступу

Користувачі	Інформація	ПЗ	Елементи КС
Директор	1-в,к,ч,з,м,д,с 2-ч 3-в,к,ч,з,м,д,с 4-в,к,ч,з,м,д,с 5-ч,з 6-ч,з 7-ч,з 8-к,ч,м,д,с 9-з,с 10-в,к,ч,з,м,д,с 12-ч	5- вик 6- вик 7- вик 8- вик 13- вик 14- вик	Директор використовує лише власний ПК з доступом в Інтернет, також має доступ до хмарного сховища, за необхідністю використовує БФП
Системний адміністратор	1-ч,з 11-в,к,ч,з,м,д,с 12- в,к,ч,з,м,д,с	1-вик,о,вст 2-о,вст 3-о,вст 4-о,вст 5-вик,о 6-вик,о,вст 7-вик,о,вст 8-о,вист 9-вик,о,вст 10-вик,о,вст 11-вик,о,вст 12- вик,о,вст 13- вик,о,вст 14- вик,о,вст	У штатному режимі системний адміністратор використовує лише свій ПК, під час оновлення системи може використовувати будь'-які ПК на підприємстві, роутер та БФП.
Торговий представник	1-ч,з,д 2-к.ч,з,м,д,с 3-к,ч,з,м.д,с 5-ч 8-ч,з,м,д,с	5-вик 6-вик 7-вик 12-вик 13-вик 14-вик	Торговий представник використовує лише власний ПК з доступом в Інтернет, також має доступ до хмарного сховища, за необхідністю використовує БФП

Продовження таблиці 1.8

Користувачі	Інформація	ПЗ	Елементи КС
Начальники відділів	1-ч,з,д,с 2- ч,з,м,д,с 5- ч,з,д,с 6- ч,з,д,с 7- ч,з,м,д,с	2-вик 3-вик 4-вик 5-вик 6-вик 7-вик 12-вик 13-вик 14-вик	Начальники відділів використовують лише власні ПК з доступом в Інтернет, також мають доступ до хмарного сховища, за необхідністю використовують БФП
Розробники	1-к,ч,з 2-к,ч,з,д 5-ч,з,д 6-ч,з,д 7-к,ч,з,д	2-вик 3-вик 4-вик 5-вик 6-вик 7-вик 12-вик 13-вик 14-вик	Розробники використовують лише власні ПК з доступом в Інтернет, також мають доступ до хмарного сховища, за необхідністю використовують БФП

- В – видалення;
- К – копіювання;
- Ч – читання;
- З – зберігання;
- М – модифікація;
- Д – друк;
- С – створення;
- Вик – використання;
- О – оновлення
- Вст – встановлення.

Процеси і програми не мають ніяких обмежень стосовно взаємодії з інформацією, що циркулює у системі, також взаємодія зі сторонніми процесами, апаратною частиною та операційною системою не обмежено жодним чином.

Регламентація щодо доступу до ресурсів і інформації відсутня.

1.4 Аналіз загроз інформації

1.4.1 Перелік джерел загроз

Джерела загроз, що можуть бути характерними для інформації, що

обробляється в ІТС:

1. Антропогенні:
   1.1. Внутрішні:
      1.1.1. Розробники;
      1.1.2. Системний адміністратор;
      1.1.3. Торговий представник;
      1.1.4. Директор;
      1.1.5. Начальники відділів.
   1.2. Зовнішні:
      1.2.1. Конкуренти;
      1.2.2. Безвідповідальні клієнти;
      1.2.3. Хакери, злочинці.
2. Техногенні:
   2.1. Комп'ютери, інстальоване програмне забезпечення;
   2.2. Хмарне сховище.

Аналіз ступеню небезпеки з джерел загроз наведено у таблиці 1.9.

Таблиця 1.9 - Ранжування джерел загроз

Джерело загрози	К1	К2	К3	К загальне
Розробники	5	2	5	0,40
Начальники відділів	5	2	4	0,32
Системний адміністратор	5	3	4	0,48
Торговий представник	5	2	5	0,40
Директор	4	2	3	0,19
Конкуренти	2	5	5	0,40

Продовження таблиці 1.9

Джерело загрози	К1	К2	К3	К загальне
Безвідповідальні клієнти	2	2	2	0,06
Хакери, злочинці	2	4	4	0,26
Хмарне сховище	5	1	4	0,16
Комп'ютери та програмне забезпечення , встановлене на них	5	2	3	0,24

К1 – визначає ступінь доступності до об'єкта:

1 – для техногенних – джерело небезпеки віддалено від об'єкту, що охороняється і не може вплинути на об'єкт, для антропогенних – доступ до об'єкту захисту відсутній, для стихійних відсутні будь-які передумови виникнення джерела загрози для об'єкту захисту;

2 – для техногенних – джерело небезпеки віддалене від об'єкту, що охороняється, але може вплинути на об'єкт, для антропогенних – доступ до об'єкту захисту може бути реалізований дистанційно, для стихійних загроз є деякі передумови для виникнення джерела загрози, але ймовірність прояву дуже мала;

3 – для техногенних – джерело небезпеки знаходиться поблизу будівлі (або у тій самій будівлі), де знаходиться об'єкт, що охороняється, для антропогенних – наявний обмежений доступ до технічних і програмних засобів обробки інформації, що охороняється, завдяки існуючим обмеженням у системі, для стихійних – прояву джерела загрози довгий час не було, але є передумови для прояви джерела загрози;

4 – для техногенних – джерело небезпеки знаходиться в тому ж приміщенні, що і ОІД, для антропогенних – джерело має доступ програмних і технічних засобів обробки інформації, що захищається, але це не є його прямим функціональним зобов'язанням, для стихійних – імовірність прояви джерела загрози висока, але об'єкт, що захищається не знаходиться у зоні дії катаклізмів;

5 – для техногенних – об'єкт, що захищається, містить джерело загрози, для антропогенних – джерелу наданий повний доступ до програмних і технічних засобів обробки інформації, що захищається, максимальні повноваження доступу також присутні, для стихійних – об'єкт, що захищається, знаходиться у зоні

впливу катаклізмів.

К2 – присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу:

1 – на об'єкті, що охороняється, відсутні будь-які можливості для виникнення джерела загрози, програмне забезпечення та техніка постійно вдосконалюються, інсталяційні файли надходять від перевірених виробників та відбувається належним чином, виконавець не має відповідних можливостей для реалізації загрози, також може зазнати шкоди при реалізації загрози;

2 – виконавець не має достатніх знань та навичок для реалізації загрози, її виконання не є вигідним для нього, оновлення програмного забезпечення та техніки не регулярне, на об'єкті, що охороняється, є умови для запобігання проявлення джерела загрози;

3 – виконавець може навчитися необхідним методам для реалізації загрози, йому вигідна реалізація загрози, техніка та програмне забезпечення вразливі для деяких атак, джерело загрози може проявити себе з низькою вірогідністю;

4 – виконавець володіє навичками для реалізації загрози, необхідним для реалізації загрози, йому дуже вигідна реалізація загрози, програмне забезпечення не оновлюється, присутня неякісна техніка від ненадійних виробників;

5 – виконавець майстерно володіє навичками для реалізації загрози, маючи мету для реалізації, наявність старої або несправної техніки, неліцензійного ПЗ, умови сприяють прояву джерела загрози.

К3 – фатальність наслідків:

1 – підприємство не понесе втрат, або наслідки будуть позитивними;

1 – наслідки незначні, ними можна знехтувати;

2 – наслідки для підприємства відчутні, але несуттєві;

3 – наслідки для підприємства дуже відчутні;

4 – наслідки реалізації загрози можуть призвести до недовіри клієнтів, втрати репутації та збитків, що можуть призвести до краху компанії.

Проаналізувавши обчислення, можна зробити висновок, що можна знехтувати такими джерелами загроз (К загальне <= 0,20):

– директор;

– безвідповідальні клієнти;

– хмарне сховище.

1.4.2 Аналіз вразливостей

Для ІТС можуть бути характерними наступні вразливості:

1 Об’єктивні:

1.1. Технічні канали витоку інформації;

1.2. Можливість несанкціонованого використання гостьової бездротової мережі;

1.3. Використання неліцензійного ПЗ;

1.4. Відсутність інфрачервоних датчиків, датчиків на розбиття вікон;

2 Суб’єктивні;

2.1 Помилки робітників;

2.2 Відсутність контролю за відвідуванням сторонніми особами об’єкту, що захищається, у робочий час;

2.3 Відсутність контролю за передачею внутрішньої інформації через незахищене середовище;

2.4 Відсутність контролю за інсталяцією і оновленням програмного забезпечення;

2.5 Відсутність регламенту щодо використання зйомних носіїв інформації;

3 Випадкові;

3.1 Збій системи;

3.2 Відмова обладнання;

3.3 Псування фізичних носіїв інформації.

У таблиці 1.10 наведено вразливості та проведено їх оцінку.

Таблиця 1.10 - Ранжування вразливостей

Вразливість	К1	К2	К3	К загальне
Технічні канали витоку інформації	4	1	3	0,09
Можливість несанкціонованого використання гостьової бездротової мережі	3	4	1	0,09
Використання неліцензійного ПЗ	4	3	2	0,19
Відсутність інфрачервоних датчиків, датчиків на розбиття вікон	3	3	5	0,36
Помилки робітників	2	3	5	0,24
Відсутність контролю за відвідуванням сторонніми особами об'єкту, що захищається, у робочий час	4	5	5	0,80
Відсутність контролю за передачею внутрішньої інформації через незахищене середовище	3	3	5	0,36
Відсутність контролю за інсталяцією і оновленням програмного забезпечення	3	2	5	0,24
Відсутність регламенту щодо використання зйомних носіїв інформації	5	4	5	0,80
Збій системи	3	3	5	0,36
Відмова обладнання	4	2	5	0,32
Псування фізичних носіїв інформації	2	2	5	0,16

К1 – ступінь впливу вразливості на фатальність наслідків:

1 – у разі використання вразливості, підприємство не понесе серйозних наслідків;

2 – мала ймовірність того, що вразливість призведе до реалізації загрози;

3 – використання вразливості може призвести до реалізації загрози;

4 – використання вразливості з високою вірогідністю призведе до реалізації загрози;

5 – використання вразливості точно призведе до реалізації загрози.

К2 – можливість та зручність використання вразливості:

1 – використання вразливості неможливо або надзвичайно важко;

2 – для використання вразливості необхідно велика кількість часу і ресурсів;

3 – для використання вразливості необхідні певні умови;

4 – вразливість може використати будь-яка людина, яка володіє необхіднимизнаннями, вміннями чи привілеями;

5 – вразливість може використати практично будь-хто.

КЗ – кількість елементів об’єкта , яким характерна вразливість:

1 – вразливість характерна для одного елементу;

2 – вразливість характерна для декількох елементів;

3 – вразливість характерна для п’ятьох-десятьох елементів;

4 – вразливість характерна для десятьох-п’ятнадцятьох елементів ;

5 – вразливість характерна більше ніж для п’ятнадцятьох елементів в ІТС.

Виходячі з отриманих результатів, можна зробити висновок, що можна знехтувати такими вразливостями (К загальне <= 0,16):

- технічні канали витоку інформації;
- можливість несанкціонованого використання гостьової бездротової мережі;
- псування фізичних носіїв інформації.

1.4.3 Аналіз актуальних загроз

У таблиці 1.10 наведено матрицю загроз у вигляді зв'язку між загрозами безпеці інформації в ІТС з джерелами загроз і коефіцієнти небезпеки.

Таблиця 1.10 – Матриця загроз

Вразливість	Джерело						
	Розробники	Начальники відділів	Системний адміністратор	Торговий представник	Конкуренти	Хакери, злочинці	Комп'ютери та програмне забезпечення, встановлене на них
Використання неліцензійного ПЗ					0.07	0.05	
Відсутність інфрачервоних датчиків, датчиків на розбиття вікон					0.17	0.09	
Помилки робітників	0,09	0.09	0.1	0.09			
Відсутність контролю за відвідуванням сторонніми особами об'єкту, що захищається, у робочий час					0.32	0.2	
Відсутність контролю за передачею внутрішньої інформації через незахищене середовище					0.14	0.09	
Відсутність контролю за інсталяцією і оновленням програмного забезпечення							0.05

Продовження таблиці 1.10

Вразливість	Джерело						
	Розробники	Начальники відділів	Системний адміністратор	Торговий представник	Конкуренти	Хакери, злочинці	Комп'ютери та програмне забезпечення, встановлене на них
Відсутність регламенту щодо використання зйомних носіїв інформації	0.32	0.32	0.38	0.32	0.32	0.2	
Збій системи							0.08
Відмова обладнання							0.07

Таким чином, для ІТС актуальними є такі загрози:

– проникнення на об'єкт сторонніх осіб (злочинців або конкурентів) у неробочий час через відсутність інфрачервоних датчиків чи датчиків на розбиття вікон (К = 0,17);

– проникнення на об'єкт сторонніх осіб (злочинців або конкурентів) у робочий час через відсутність контролю за відвідуванням об'єкту, що охороняється (К = 0,32);

– загрози, пов'язані з використанням сторонніх інтернет-ресурсів з передачею внутрішніх документів через незахищене середовище (К= 0,14);

– можливість викрадення зйомних носіїв інформації через відсутність регламентації щодо їх використання (К = 0,38);

У таблиці 1.11 наведено перелік актуальних загроз із зазначенням їх впливу на властивості інформації, яка може бути уражена цими вразливостями (якщо загроза впливає на властивість, на перетині відповідної загрози та властивості стоїть знак +).

Таблиця 1.11 Вплив актуальних загроз на властивості інформації

Загроза	Властивості інформації, що порушуються		
	К	Ц	Д
Проникнення у приміщення злочинців або конкурентів у неробочий час через відсутність інфрачервоних датчиків чи датчиків на розбиття вікон	+	+	+
Проникнення на об'єкт сторонніх осіб (злочинців або конкурентів) у робочий час через відсутність контролю за відвідуванням об'єкту, що охороняється	+	+	+
Загрози, пов'язані з використанням сторонніх інтернет-ресурсів з передачею внутрішніх документів через незахищене середовище	+		
Можливість викрадення зйомних носіїв інформації через відсутність регламентації щодо їх використання	+		+

К – конфіденційність інформації;

Ц – цілісність інформації;

Д – доступність інформації.

1.5 Висновок і постановка задач

У першому розділі було виконано обстеження середовищ функціонування ІТС, спираючись на яке було побудовано модель загроз та порушника. Також було обґрунтовано необхідність розробки і впровадження політики безпеки інформації в ТОВ «Шевченко», було виконано обстеження

Характеристика можливих джерел загроз інформації та вразливостей було побудовано на основі отриманих даних. На основі аналізу цих характеристик було виділено актуальні для підприємства загрози інформації. Метою створення нових розділів політики інформаційної безпеки є побудова механізмів захисту від виділених загроз шляхом усунення або зменшення вразливостей. Тобто, необхідно створити розділи щодо:

– контролю відвідування об'єкта, що охороняється, сторонніми особами в робочий час;

– передачі документів в електронному вигляді в компанії, тобто, регламентуванняканалів передачі інформації;

– резервного копіювання;

– обліку зйомних носіїв, правил поводження з ними;

– збереження матеріальних носіїв.

А також необхідно створити рекомендації щодо поліпшення системи сигналізації для того, щоб запобігти виникненню загрози проникнення порушників у неробочий час.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності.

Згідно з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації 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.» [3]

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

«Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.» [4]

АС відносимо до класу 3, оскільки для передачі інформації використовується незахищене середовище Інтернет. Визначимо реалізовані на АС послуги інформаційної безпеки. Виходячи з цього, визначимо критерії захищеності, що необхідно додатково реалізувати в системі.

Існуючі в системі критерії захищеності: { КА-1, КО-1, ЦА-2, ДР-1, НР-2, НИ-2, НК-1, НО-1, НТ-2, НА-2, НП-1}.

Рекомендовані для системи критерії захищеності: { КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НТ-2, НА-2, НП-1}.

У таблиці 2.1 наведено критерії захищеності інформації та механізми, якими вони реалізуються або мають реалізовуватися (якщо їх реалізація тільки

планується у рекомендованому профілі).

Таблиця 2.1 Критерії захищеності інформації

Критерії	Механізми реалізації
КД-2	Розмежування прав доступу за допомогою функціоналу Active Directory та OneDrive
КО-1	Вбудований функціонал Microsoft Windows
ЦД-1	Розмежування прав доступу за допомогою функціоналу Active Directory та OneDrive
ЦО-1	Функціонал Active Directory – засоби для створення резервних копій інформації та засоби для відновлення групових політик та інших параметрів
ДР-1	Функціонал Active Directory
ДВ-1	Функціонал Active Directory – засоби для створення резервних копій інформації та засоби для відновлення групових політик та інших параметрів
НР-2	Вбудований функціонал Microsoft Windows – журнал подій
НИ-2	Вбудований функціонал Microsoft Windows
НК-1	Вбудований функціонал Microsoft Windows
НО-1	Вбудований функціонал Microsoft Windows
НТ-2	Вбудований функціонал Microsoft Windows Defender
НА-2	Функціонал OneDrive та електронної пошти Outlook
НП-1	Функціонал OneDrive

«Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні маєневисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

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

Перш ніж користувач або процес зможе одержати в своє розпорядження

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

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

ЦО-1. Обмежений відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

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

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

НР-2. Захищений журнал. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

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

НИ-2. Одиночна ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-1. Виділення адміністратора. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НТ-2. Самотестування при старті. Самотестування дозволяє КЗЗперевірити і

на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури,які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НА-2. Автентифікація відправника з підтвердженням. Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно становити, що даний об'єкт був відправлений (створений) певним користувачем. Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною. Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації. Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною.

НП-1. Базова автентифікація отримувача. Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем. Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації.» [3]

2.2 Проектні рішення – політика інформаційної безпеки

Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформаціїв комп'ютерних системах від несанкціонованого доступу»:

«Під політикою безпеки інформації слід розуміти набір законів, правил,

обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформаціїі спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила.

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

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

Частина політики безпеки, яка регламентує правила доступу користувачіві процесів до ресурсів КС, складає правила розмежування доступу.» [5]

Згідно з визначеними у першому розділі актуальних загроз, надалі необхідно вирішити завдання розробки частин політики безпеки, які б забезпечували виконання рекомендованих послуг інформаційної безпеки і захист інформації в ІТС від виявлених загроз.

На рівні організації забезпечення безпеки інформації повинні бути вироблені методи щодо:

– виконання робіт з оновлення системи сигналізації на об’єкті інформаційної діяльності;

– регулювання доступу сторонніх осіб до ресурсів АС, зокремадоступу сторонніх осіб в приміщення, де циркулює ІзОД;

– встановлення регламенту щодо доступу користувачами АС до носіїв інформації, визначення правил їх використання (зберігання, передача, створення);

– використання незахищених мереж для передачі даних (Інтернет);

– регламентації засобів та схем передачі інформації всередині компанії.

На технічному рівні забезпечення безпеки інформації повинні бути виробленіметоди щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації:

– виявлення і реєстрація небезпечних подій з метою здійснення постійного контролю або проведення службових розслідувань;

– резервне копіювання даних, критичних для функціонування підприємства;

– відновлення роботи АС після відмов та збоїв.

2.2.1 Рекомендації щодо покращення системи сигналізації

Мета застосування: створення механізмів захисту від загрози несанкціонованого доступу до приміщення, що охороняється, злочинцями або конкурентами через відсутність інфрачервоних датчиків чи датчиків на розбиття вікон.

Оскільки ОІД знаходиться на першому поверсі, на вікнах присутні решітки, але все одно є можливість їх знищення, в результаті чого можна потрапити у приміщення, розбивши вікно, тому необхідно встановити комбіновані інфрачервоні датчики у кожній кімнаті, оскільки також є можливість потрапити у приміщення через сусідні приміщення з північної сторони будівлі.

Рекомендована схема сигналізації на об’єкті, що охороняється, зображена на рисунку 2.1.

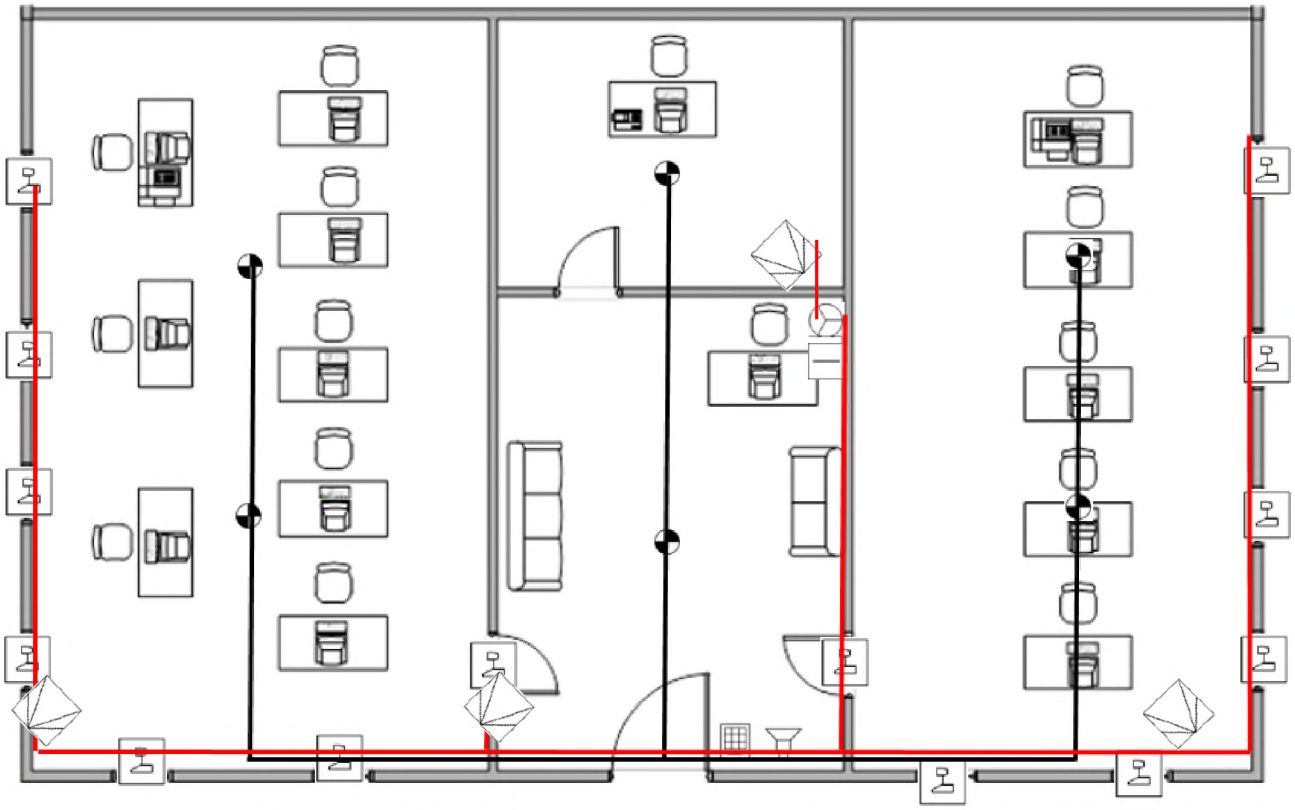


Рисунок 2.1 – Рекомендована схема сигналізації

Умовні позначення

2.2.2 Політика доступу сторонніх осіб в приміщення в робочий час

Мета політики:

Створення регламентації доступу сторонніми особами до ресурсів АС,

захист від проникнення у приміщення сторонніми особами, зокрема злочинцями або конкурентами у робочий час через відсутність контролю за відвідуванням приміщення, де циркулює ІзОД у робочий час.

Область дії:

Дана політика встановлює порядок роботи пропускного режиму до приміщень організації, порядок контролю за переміщенням по об'єкту відвідувачів, також визначає відповідальність для співробітників при порушені встановлених правил.

Ця політика відноситься до робітників організації, що під час своєї роботи мають контакт зі сторонніми особами, наприклад директор або начальники відділів під час співбесід з потенційно найманими робітника, або до торгового представника під час проведення переговорів з клієнтами стосовно замовлень або презентації готової продукції.

Політика безпеки:

Для забезпечення контролю доступу в приміщення, на підприємстві встановлюються електронні замки з доступом по картці на вхідні двері до робочих кабінетів розробників та кабінету директора. Кожному робітнику видається персональна картка, котру заборонено передавати стороннім особам, за виключенням ситуацій, описаних в даній політиці. Для відвідувачів, котрі тимчасово повинні мати доступ до об'єкту, але не працюють на постійній основі, виготовляється спеціальна картка. Для отримання доступу до приміщення, що охороняється, необхідно провести карткою по карткозчитувачу та на клавіатурі ввести PIN-код.

Якщо робітника звільнено з посади, системний адміністратор блокує його картку, а робітник має передати свою картку начальнику відділу. Видача карток співробітникам та особам з тимчасовим доступом до об'єкту, що охороняється, лягає під відповідальність начальників відділів, що має бути прописано у його посадовій інструкції.

Доступ до робочих кабінетів розробників без картки можливий лише з письмового дозволу директора та у супроводі начальника відповідного відділу. Відвідування підприємства без супроводу або картки можливо лише у

приміщенні, де не циркулює ІзОД – зала очікування.

Відповідальність:

У разі порушення безпеки політики підприємства, відповідальність за наслідки дій відвідувача несе співробітник, що порушив політику безпеки. Відповідальність за невиконання правил, описаних в політиці безпеки полягає у сплаті штрафу або звільнення, в залежності від критичності наслідків порушення.

2.2.3 Політика користування зйомними носіями інформації та збереження фізичних носіїв інформації

Мета політики:

Розробка механізмів захисту від загрози крадіжки паперових та зйомних носіїв інформації, неконтрольованого ознайомлення або знищення інформації, необхідної для функціонування підприємства.

Область дії:

В політиці описуються правила отримання і використання зйомних носіїв, правила їх використання, зберігання і переміщення. Даною політикою встановлюються правила щодо зберігання паперових носіїв інформації. Політика розповсюджується на кожного співробітника підприємства, який працює з ІзОД.

Політика безпеки:

Кожний зйомний носій інформації на підприємстві повинен підлягати обліку, кожному носію присвоюється відповідний інвентарний номер, кожен носій привласнюється певному користувачу або групі користувачів. За видачу зйомних носіїв несуть відповідальність керівники відділів. Видача та повернення носія користувачем (або групою користувачів) фіксується у журналах обліку зйомних носіїв (всього 2 журнали, на кожний відділ по одному), у котрому вказуються дані співробітника (або співробітників), котрому видано носій, час та дата видачі/повернення носія і інвентарний номер носія. Журнал зберігається у керівника відділу, перехресна видача/повернення носія між відділами неможлива.

Використовувати носії дозволяється тільки для виконання співробітниками своїхпрямих обов'язків. Забороняється виносити носії поза межі підприємства без

письмового дозволу начальника відділу, також забороняється використання носіїв на власній обчислювальній техніці. Забороняється передавати носії третім особам. У разі втрати або псування носія, робітник повинен повідомити про це керівника свого відділу.

Знищення носія дозволяється за рішенням керівника відділу, за яким закріплено носій. Під знищенням розуміється форматування кожної ланки пам'яті, після чого фізичне знищення носія шляхом псування плати, що забезпечить унеможливлення відновлення даних. Інформація про знищення носія заноситься у відповідний журнал обліку носіїв.

Знімні носії зберігаються і використовуються наступними групами користувачів:

- директор (1 USB-накопичувач);
- системний адміністратор (1 USB-накопичувач);
- начальники відділів (4 USB-накопичувачи).

Для зберігання носії інформації у кожнмоу з відділів необхідно встановити сейф, ключі від сейфу повинні зберігатися у начальників відділів. Також необхідно встановити сейф у кабінеті директора для збереження паперових носіїв інформації.

Забороняється зберігання носіїв з ІзОД без сейфів, як зйомних, так і паперових. Також необхідно заборонити неконтрольований друк паперових носіїв співробітниками відділів. Відповідальними за видачу паперових носіїв стають керівники відділів, про що буде написано в їх посадових інструкціях.

Необхідні налаштування групових політик: робітники, які не мають права використовувати зйомні носії, не мають можливості підключення будь-яких зйомних носіїв, окрім периферійних пристроїв. Для робітників, які мають використовувати зйомні носії під час роботи, необхідно заборонити використання незареєстрованих носіїв.

Для зйомних носіїв також рекомендовано застосувати вбудовану у Windows технологію BitLocker. Технологія дозволяє шифрувати дані на USB-накопичувачах та зйомних дисках – доступ можливий лише після вводу

відповідного паролю, є можливість налаштування роботи носія тільки при під'єднанні до певних пристроїв. Це рішення може захистити інформацію від несанкціонованого доступу від зовнішніх порушників, наприклад, конкурентів.

Щоб користувачі не могли самостійно вимикати BitLocker, необхідно зняти відмітку «Дозволити користувачам тимчасово призупиняти захист BitLocker і розшифрувати диски з даними».

Відповідальність:

Відповідальність за збереження зйомних і паперових носіїв покладається на керівників відповідних відділів. Відповідальність за налаштування групових політик покладається на системного адміністратора. Відповідальність за невиконання правил, описаних в політиці безпеки полягає у сплаті штрафу або звільнення, в залежності від критичності наслідків порушення.

2.2.4 Політика використання каналів передачі інформації в електронному вигляді

Мета політики:

Створення регламенту обміну інформацією на підприємстві від однієї особи до іншої та захисту від загроз, що виникають при передачі інформації через незахищене середовище.

Область дії:

В політиці встановлено порядок та методи передачі інформації в електронному вигляді між робітниками, а також правила, пов'язані з передачею інформації.

Ця політика розповсюджується на всіх співробітників компанії, що отримують чи передають інформацію незахищеними каналами передачі інформації.

Політика безпеки:

Накази директора для співробітників мають передаватися у паперовому вигляді, роздруковуючись на одному з БФП, директор на власному ПК створює файл наказу, після чого одразу передає на друк, накази у паперовому вигляді роздають начальники відділів згідно з призначенням наказу.

Інформація про нові замовлення передається торговому представнику шляхом електронної скриньки або у паперовому вигляді. В свою чергу, торговий представник переносить цю інформацію до хмарного сховища, після чого начальники відділів розподіляють завдання між розробниками у паперовому вигляді або через електронну скриньку.

Звіти з продажів, клієнтська база, звіти системного адміністратора передаються між робітниками за допомогою хмарного сховища.

Бухгалтерські звіти використовує лише директор, тому для передачі інформації такого типу використовуються лише зйомні носії, окрім випадків, коли необхідно передати інформації до податкової через мережу Інтернет.

Готові продукти компанії передається між робітниками за допомогою хмарного сховища, а до клієнтів передається засобами електронної скриньки.

Архівовані замовлення передаються виключно за допомогою засобів електронної скриньки.

Проекти на стадії розробки передаються за допомогою хмарного сховища або електронної скриньки.

Дані для входу до системи, зарплатні відомості та персональні дані працівників не передаються.

Для виконання правил цієї політики та контролю за їх виконанням рекомендується застосовувати групові політики Active Directory та встановлювати обмеження щодо використання певних документів окремими програмами. Для перешкоджання фішингу, необхідно блокувати ресурси, які не є необхідними для виконання своїх прямих обов'язків.

Відповідальність:

Контроль виконання правил політики покладається на системного адміністратора.

2.2.5 Політика резервного копіювання

Мета політики:

Створення правил проведення резервного копіювання документів та технологічно інформації на підприємстві. Тобто визначення способів створення

резервних копій і відповідальної особи, яка має контролювати за станом цих копій і у разі необхідності, їх відновлювати.

Область дії:

Політика стосується системного адміністратора, що відповідальний за відновлення системи після збоїв та створення резервних копій.

Політика безпеки:

Рекомендується виконувати резервне копіювання за правилом «3-2-1», згідно з яким має бути створено 3 резервні копії, які будуть збережені у двох різних форматах зберігання, і одна з копій має зберігатися поза офісом.

Перший примірник необхідної для функціонування підприємства технологічної інформації повинен бути скопійований на окремий зйомний носій, який може використовувати лише системний адміністратор. Друга резервна копія повинна бути на ПК системного адміністратора, третя копія повинна зберігатися у хмарному сховищі, доступ матиме лише системний адміністратор. Резервне копіювання необхідної для функціонування підприємства технологічної інформації повинне проходити раз на місяць.

Документи, що передаються за допомогою хмарного сховища, повинні зберігатися у відповідних каталогах (у тих самих, через які передаються).

В першу чергу необхідно забезпечити резервне копіювання документів, для яких доступність є критичною (з рівнем Д3 та Д4). У таблиці 2.2 наведено місця зберігання резервних копій документів і місця зберігання оригіналів цих документів (позначка + означає, що резервна копія документа повинна бути наявна на відповідному ресурсі).

Таблиця 2.2 – Зберігання документів

Документ	Місце зберігання документів			
	Зйомні носії	Хмарне сховище	ПК власника документу	ПК робітників, яким було передано документ
Накази керівництва	-	+	+	-
Відомості про нові замовлення	-	+	+	+
Звіти з продажів	-	-	+	-

Бухгалтерські звіти	+	-	+	+
Готові замовлення	-	+	+	+

Продовження таблиці 2.2

Документ	Місце зберігання документів			
Архівовані завершені замовлення за договором з замовником	-	+	+	-
Замовлення на стадії розробки	+	+	+	+
Клієнтська база	-	-	+	-
Відомості щодо заробітних плат	+	+	+	+
Дані для доступу до системи	+	-	+	-
Звіт системного адміністратора	-	-	+	-

Для резервного копіювання даних і відновлення системи рекомендується використовувати засоби Active Directory. Для відновлення даних, що втрачено, можна використовувати програму Aomei Backupper. При виявленні втрати даних необхідно відновити дані засобами програми, і занести їх на зйомний носій. Для перевірки стану жорстких накопичувачів слід використовувати безкоштовну програму Victoria.

Неліцензійні програми Total Network Inventory 3 та Total Software Deployment для аналізу мережі мають бути замінені на Spiceworks Help Desk, що також є безкоштовною і може виконувати ті ж самі функції і дозволяє більш ефективно виконувати моніторинг мережі і робочих пристроїв в ній.

Відповідальність:

Відповідальність за виконання умов політики несе системний адміністратор.

2.2.5 Політика використання Інтернету на підприємстві

Мета політики:

Створення механізмів захисту від неправомірної передачі ІзОД компанії через незахищене середовище та захист від фішингу за допомогою створення правил використання працівниками компанії мережі Інтернет.

Область дії:

Політика призначена для контролю дій всіх працівників підприємства під час роботи у мережі Інтернет. У політиці описуються права та обов'язки працівників під час користування мережею Інтернет.

Політика безпеки:

Використання мережі Інтернет дозволяється лише для виконання своїх прямих обов'язків:

- пошук довідкових матеріалів, що необхідні при виконанні своїх прямих обов'язків;
- збору нових для себе, необхідних для роботи відомостей;
- створення рекламної компанії підприємства, просування її у соціальних мережах.

Забороняється використовувати Інтернет для:

- передачі ІзОД незахищеними каналами;
- особистих цілей.

Системний адміністратор повинен встановити обмеження для доступу на всі сайти, окрім дозволених. Перелік дозволених сайтів оговорюється з начальниками відділів і у письмовому вигляді затверджується директором. Для цих цілей він може використовувати Wireshark або інший аналізатор трафіку. За рішенням директора може бути створено список співробітників, на які обмеження не накладаються і видано відповідний наказ. В такому разі системний адміністратор повинен буде розблокувати ці ресурси для зазначених директором користувачів.

Відповідальність:

Контроль за виконанням політики здійснює системний адміністратор. У

разі порушення правил політики, порушник отримає попередження, у разі повторного порушення буде накладено штраф.

2.3 Висновки

В другому розділі було проаналізовано наявний функціональний профіль захищеності в ІТС, виділено засоби забезпечення відповідних послуг. Було розроблено ряд організаційних заходів, метою яких було підняття рівня захищеності АС до біль високого рівню. Також було обрано нові додаткові критерії захищеності, що забезпечують належний рівень інформаційної безпеки.

Для забезпечення належної роботи критеріїв захищеності та для забезпечення захисту від існуючих на ОІД загроз було розроблено наступні розділи політики безпеки:

- контролю відвідування об’єкта, що охороняється, сторонніми особами в робочий час;
- передачі документів в електронному вигляді в компанії, тобто, регламентуванняканалів передачі інформації;
- резервного копіювання;
- обліку зйомних носіїв, правил поводження з ними;
- збереження матеріальних носіїв.

Також створено рекомендації щодо поліпшення працеспроможності системи сигналізації для того, щоб запобігти виникненню загрози проникнення третіми особами на об’єкт, що охороняється у неробочий час.

Додатково було розроблено розділ політики щодо використання мережі Інтернет, завдяки якій реалізується захист від неправомірної передачі документів через незахищене середовище та захист від фішингу.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є визначення чи є доцільним і вигідним використання запропонованих засобів та заходів інформаційної безпеки на ТОВ «Шевченко». Щоб з'ясувати це, необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити величину відвернених втрат та, на основі цього, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі розрахованих показників можна буде визначити, наскільки прибутковим або збитковим є запропонований проект.

3.1 Розрахунок капітальних витрат

До фіксованих (капітальних) варто відносити наступні витрати на ТОВ «Шевченко»:

– витрати на залучення зовнішніх консультантів (спеціаліста з розробки політики безпеки інформації);

– витрати на первісні закупівлі апаратного забезпечення (скомбіновані інфрачервоні датчики, сейфи для збереження носіїв інформації);

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання та налагодження системи інформаційної безпеки);.

Для підрахунку заробітної платні залученого працівника, який створює або дороблює політику безпеки, необхідно розрахувати трудомісткість розробки політики безпеки інформації. Вона визначається тривалістю кожної робочої операції цього працівника:

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

де $t_{ТЗ}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, становить 8 год.;

$t_{В}$ – тривалість розробки концепції безпеки інформації у організації,становить 12 год.;

$t_{А}$ – тривалість процесу аналізу ризиків, становить 4 год.;

$t_{ВЗ}$ – тривалість визначення вимог до заходів, методів та засобів захисту становить 3 год.;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації становить 5 год.;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації становить 6 год.;

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

t=8 год+12 год+4 год+3год+5год+6год+4год=42 год

У даному випадку, витрати на розробку політики безпеки інформації включають в себе лише заробітну плату спеціаліста, що розроблює політику безпеки. В оплату спеціалісту вже враховано плату за електроенергію, що він використає під час розробки політики безпеки, оскільки під час роботи він використовує лише власне обладнання без підключення до мережі електропостачання підприємства. Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) та визначається за формулою:

$$К_{пр} = З_{зп} = t * З_{іб}, \text{ грн} \qquad (3.2)$$

де: t =42 – загальна тривалість розробки політики безпеки, годин;

$З_{іб}$ =75 – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$К_{пр} = 42 * 75 = 3150$$

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

$$К = Кпр + Кзпз + Крп + Каз + Кнавч + Кн \qquad (3.3)$$

де Кпр – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів тис.грн. = 3150 грн;

Кзпз – вартість закупівель ліцензійного основного і додаткового ПЗ, складає 18480 грн;

Таблиця 3.1 Перелік придбаного ліцензійного ПЗ

Назва	Кількість	Вартість(грн)
Aomei Backupper	15	16425
Malwarebytes	AVG Internet Security	2055
Всього		18480

Крп – вартість розробки політики інформаційної безпеки включено у вартість проекту інформаційної безпеки;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів складає 4876 грн;

Таблиця 3.2 Перелік придбаного апаратного забезпечення і допоміжних матеріалів

Назва	Кількість	Вартість(грн)
Crow SWAN QUAD CRT	4	1456
Сейф	1	3420
Всього		4876

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис грн. Витрати на навчання системного адміністратора становлять 1000грн;

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, включено до вартості розробки.

$$К = 3150 + 18480 + 4876 + 1000 = 27506 \text{ грн}$$

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

$$С = Св + Ск + Сак, \text{ тис. грн} \quad (3.4)$$

де Св – це витрати на оновлення системи;

Сак – це витрати викликані активністю користувачів системи, що складають 22 грн – пряма допомога, 240 грн – неформальне навчання, 280 –

розробка додатків, 300 грн – робота з даними, 360 грн – формальне навчання, 600 грн – futz-фактор. Всього 2000грн.

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

$$Ск = Сн + Са + Сз + Сєв + Сел + Со + Стос \quad (3.5)$$

де Сн – це витрати на навчання адміністративного персоналу й кінцевих коритсувачів визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації, що становлять 1500грн;

Са – це річний фонд амортизаційних відрахувань, що визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ). Загально, ПЗ було придбано на 18480 грн., апаратного забезпечення на 4876 грн.

Загалом – 23356грн. Мінімальний термін амортизації 2 роки. Ліквідаційна вартість програмного забезпечення для 15 комп'ютерів – 1500 грн, ліквідаційна вартість апаратного забезпечення – 500грн.

$$Са = (23356 – 2000)/2 = 10678грн$$

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

$$Сз = Зосн + Здод, грн \quad (3.6)$$

де Зосн – основна заробітна плата, складає 15000грн на місяць, відповідно 180000 на рік;

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

$$Сєв = 180000 * 22\% = 39600 грн$$

$$Сз = 180000 + 12000 + 39600 = 231600 грн$$

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

$$Сел = Р * Fр * Це, грн \quad (3.7)$$

де Р – встановлена потужність апаратури інформаційної безпеки 0.5 кВт для одного ноутбуку, для всього комплексу враховується повна кількість

комп'ютерів, яка складає 15, тобто 7.5кВт;

Fр – річний фонд робочого часу системи інформаційної безпеки складає 12 місяців * 20 робочих діб/міс * 9 робочих годин * 15 комп'ютерів = 32400;

Це – тариф на електроенергію, 2,01грн/кВт годин.

$$Сел = 7,5 * 32400 * 2,01 = 488430 грн$$

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

Стос – це витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються за даними організації або у відсотках від вартості капітальних витрат, що складає 1% від суми капітальних інвестицій у вигляді 275грн.

$$Ск = 1500 + 10678+ 231600 + 39600 + 488430 + 275 = 772083 грн$$

Маючи всі необхідні дані розраховуємо річні експлуатаційні витрати:

$$С = 772083+ 2000 = 774083 грн$$

3.3 Оцінка величини збиту

Таблиця 3.2 – Заробітна плата робітників на місяць

Посада	Розмір заробітної плати, грн
Директор	30000
Торговий представник	12000
Начальник відділу х 2	2*15000=30000
Системний адміністратор	15000
Розробник х 10	12000*10=120000
Всього	207000

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

Упущена вигода від простою атакованого вузла або сегмента становить:

$$U = Пп + Пв + V \qquad (3.8)$$

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

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

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

Місячний фонд робочого часу складає 198 годин. Час простою внаслідок атаки 8 годин:

$$Пп = (Зс /F)* t_a, грн \qquad (3.9)$$

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

F – місячний фонд робочого часу;

t_a – час простою внаслідок атак.

Отже:

$$Пп = (207000/198) * 8 = 8364 грн.$$

Витрати на відновлення працездатності (Пв) включають декілька складових:

Пви – витрати на повторне ведення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни частини системи, грн.

Витрати на повторне введення інформації розраховуються:

$$Пви = (Зс/F) * t_{ви}, грн \qquad (3.10)$$

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

F – місячний фонд робочого часу;

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

$$Пви = (207000/198) * 15 = 15682 грн$$

Витрати на відновлення Ппв визначаються:

$$Ппв = (Зо/ F) * t_в ,грн \qquad (3.11)$$

Де Зо – заробітна плата системного адміністратора;

F – місячний фонд робочого часу;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну

мережу.

$$Ппв = (15000/198) * 8 = 607 грн$$

Пзч – вартість витрат на заміну устаткування або запасних частин складає 2800грн.

$$Пв = Пви + Ппв + Пзч грн \quad (3.12)$$

$$Пв = 15682 + 607 + 2800 = 19089 грн$$

Витрати від зниження працездатності атакованої системи:

$$V = (O/Fг)(t_п+t_в+t_{ви}) \quad (3.13)$$

де О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, 8000000 грн за рік;

Fг – річний фонд часу роботи організації, становить 2340 год.;

$t_п$ – 8 годин простою внаслідок атак;

$t_в$ – 8 годин відновлення після атаки;

$t_{ви}$ – 15 годин повторного введення загубленої інформації.

$$V = (8000000/3568)*23 = 51570 грн$$

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

$$U = 8364 + 19089 + 51570 = 79023 грн.$$

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

$$B = \sum i \sum n U \quad (3.14)$$

$$B = 4 * 15 * 79023 = 4741380 грн$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B * R – C \quad (3.15)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, складає 4741380 грн;

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

С – щорічні витрати на експлуатацію системи інформаційної безпеки, складає 774083грн.

$$E = (4741380 * 0.25) – 774083 = 411262$$

Аналіз показників економічної ефективності

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

$$ROSI = E/K \qquad (3.16)$$

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

К – це капітальні затрати, які становлять 32120 грн.

$$ROSI = 411262 / 27506 = 14,95$$

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

$$To = K \setminus E = 1/ ROSI, \text{ років} \qquad (3.17)$$

$$To = 1 / 14,95 = 0,07 \text{ року (1 місяць)}$$

3.5 Висновок

В цьому розділі було визначено розмір капітальних (32120 грн) та експлуатаційних (774083 грн) витрат на заходи і засоби інформаційної безпеки, розраховано термін окупності капітальних інвестицій (0,07 року). На основі розрахованих показників можна зробити висновок, що запропоновані заходи та засоби є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (менше одного місяця).

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було обґрунтовано необхідність створення КСЗІ на підприємстві ТОВ «Шевченко», виконано обстеження середовищ функціонування ІТС відповідно до НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

Виходячи з отриманих даних було виділено актуальні вразливості та побудовано модель загроз. Проведено аналіз існуючого в ІТС функціонального профілю захищеності.

Виходячи з проведеного аналізу, було розроблено окремі елементи політики інформаційної безпеки підприємства. Після цього, було проведено аналіз економічної вигідності запропонованих в розділах політики безпеки заходів і засобів.

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

2 Закон України "Про захист персональних даних" [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

3 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/.

4 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

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: www.dsszzi.gov.ua/dsszzi/.

6 Закон України "Про інформацію" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

7 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

8 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.com.ua/downloads/1.1-003-99.pdf.

9 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97 [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/.

10 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Стан питання. Постановка задачі	34	
6	А4	Спеціальна частина	17	
7	А4	Економічний розділ	8	
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	

ДОДАТОК Б. Перелік документів на оптичному носії

- Пінчук К. 125-18ск-1.docx
- Пінчук К. 125-18ск-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

на кваліфікаційну роботу студента групи 125-18ск-1 Пінчука Костянтина Олександровича на тему: «Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ «Шевченко»

Кваліфікаційна робота Пінчука К.О. представлена пояснювальною запискою на 70 сторінках.

Мета кваліфікаційної роботи – підвищення рівня безпеки інформації в ІТС ТОВ «Шевченко», розробка рішень для захисту від загроз інформаційної безпеки. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання кваліфікаційної роботи були вирішені наступні питання: аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для ОІД ТОВ «Шевченко», приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки "_____", а Пінчук Костянтин Олександрович – присвоєння йому кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека»

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

Керівник кваліфікаційної роботи професор Корнієнко В.І..

Дата:_____ Підпис: _____