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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Романюка Едуарда Олександровича*

академічної групи *125-18-3*

спеціальності *6.170103 Управління інформаційною безпекою*

спеціалізації[1]

за освітньо-професійною програмою

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

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний				
Рецензент				
Нормоконтролер	ст .викладач Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Романюк Е. О*** **академічної групи** ***125-18-3***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***6.170103 Управління інформаційною безпекою***
(код і назва спеціальності)

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

затверджену наказом ректора НТУ «Дніпровська політехніка» від 18.05.2022 № 268-с.

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи ТОВ «Сладко Дніпро». Розробка моделі загроз.*	20.03.2022
Розділ 2	*Аналіз стану захищеності інформаційно-телекомунікаційної системи ТОВ «Сладко Дніпро». Розробка політики безпеки інформації.*	30.05.2022
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	10.06.2022

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 14.01.2022р.

Дата подання до екзаменаційної комісії: 10.06.2022р.

Прийнято до виконання _____ Романюк Е.О.
(підпис студента) (прізвище, ініціал

РЕФЕРАТ

Пояснювальна записка: 90 с., 4 рис., 15 табл., 4 додатка, 7 джерел.

Об'єкт розробки: Політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ "Сладко Дніпро".

Мета проекту: Розробка політики безпеки об'єкту інформаційної діяльності.

У першому розділі описаний об'єкт: рід діяльності, інформаційна система, устаткування, програмне забезпечення, інформаційні потоки. Також виконана: класифікація інформації, що обробляється в ІТС, визначений перелік джерел загроз, перелік вразливостей та перелік актуальних для ІТС загроз.

У другому розділі описано існуючий профіль захищеності та виконано вибір нового профілю захищеності підприємства, також були розроблені рекомендації, щодо забезпечення інформаційної безпеки ОІД.

В третьому розділі були розраховані витрати на впровадження та щорічну підтримку політики безпеки. Окрім цього, була доведена економічна доцільність введення в експлуатацію рекомендацій щодо політики безпеки, розроблених в другому розділі.

Практичне значення проекту полягає в підвищенні рівня інформаційної безпеки ТОВ "Сладко Дніпро"

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ.

РЕФЕРАТ

Пояснительная записка: 90 с., 4 рис., 15 табл., 4 приложения, 7 источников.

Объект разработки: Политика безопасности информации информационно-телекоммуникационной системы ООО "Сладко Днепр".

Цель проекта: Разработка политики безопасности объекта информационной деятельности.

В первом разделе описан объект: род деятельности, информационная система, оборудование, программное обеспечение, информационные потоки. Также выполнена классификация информации, которая обрабатывается в ИТС, определён перечень источников угроз, перечень уязвимостей и перечень актуальных для ИТС угроз.

Во втором разделе описано существующий профиль защищенности и выполнен выбор нового профиля защищенности предприятия, также были разработаны рекомендации, касательно обеспечения информационной безопасности ОІД.

В третьем разделе были рассчитаны затраты на введение и ежегодную эксплуатацию политики безопасности. Кроме того, была доказана целесообразность введения в эксплуатацию рекомендаций касательно политики безопасности, разработанных во втором разделе.

Практическое значение проекта состоит в повышении уровня информационной безопасности ООО "Хмільна Крамниця"

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ.

THE ABSTRACT

Explanatory note: 90 p., 4 fig., 15 tables, 4 applications, 7 sources.

Object of elaboration: Information Security Policy for information and telecommunication system of "Sladko Dnipro" LLC.

Project Objective: Development a security policy for object of information activities.

The first section describes the object: type of activity, information system, equipment, software, information flows. Also the information that is processed in the ITS has been classified, list of the threat sources, list of vulnerabilities and list of threats that are relevant for ITS have been created.

In the second section has been described an existing security profile and selected the new security profile for the company, also have been developed recommendations for ensuring information security of the object of information activity.

In the third section, the costs for implementation and annual support of the security policy have been calculated. In addition, the economical feasibility of commissioning the security policy guidelines, developed in the second section, has been calculated.

The practical significance of the project is to increase the level of information security of "Sladko Dnipro " LLC.

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

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – Автоматизоване робоче місце;

НДМ – Недокументовані можливості;

НСД – Несанкціонований доступ;

ЗЗІ - Засоби захисту інформації;

АС - Автоматизована система;

ІТС – Інформаційно-телекомунікаційна система;

КСЗІ – Комплексна система захисту інформації;

ТОВ – Товариство з обмеженою відповідальністю;

ПЗ – Програмне забезпечення;

ІОД – Інформація з обмеженим доступом

БД – База даних;

ІНН – Ідентифікаційний номер;

ВАТ – Відкрите акціонерне товариство;

ОІД – Об'єкт інформаційної діяльності;

КЗ – Контроль захисту;

ЗМІ – Засоби масової інформації;

МСФЗ – Міжнародні стандарти фінансової звітності;

ІТ – Інформаційні технології;

SLA – Service Level Agreement (Соглашение об уровне услуг);

ЕОМ – Електронно-обчислювальна машина.

ЗМІСТ

ВСТУП

На сьогоднішній день все більш значимим виступає поняття інформатизації. Вона захоплює нові простори і розповсюджується на більшість сфер нашого життя, у тому числі: на економічний простір, сферу охорони здоров'я, культурний розвиток нації, виробничу та наукову сферу тощо.

В кожній ІТС існує така інформація, властивості якої, а саме конфіденційність, цілісність та/або доступність, потрібно зберегти згідно з законодавством України або згідно з інтересами власника системи. Для того, щоб захистити інформацію від небажаного ознайомлення, модифікації, видалення, тощо, в організаціях в тому числі створюється політика безпеки інформації. Створенням такої політики повинен займатись фахівець з інформаційної безпеки.

Для того, щоб створити політику безпеки, необхідно спочатку проаналізувати існуючі на ОІД умови, зробити висновок щодо можливих вразливостей, джерел загроз та загроз, оцінити їх критичність та визначити умови, за яких можна ними знехтувати. На основі цих досліджень можна буде зробити висновок, які питання мають бути розглянуті в політиці безпеки.

Для забезпечення ефективності політики безпеки, необхідно, щоб у ній були зазначені чіткі правила та інструкції для кожного відповідального робітника, вказана відповідальність та можливі штрафні санкції у разі невиконання вимог. Політика повинна бути завжди актуальною, тому її необхідно періодично оновлювати, розробляти нові її розділи, тощо, у відповідності до нових умов функціонування ІТС, нових викликів та нових потреб.

Таким чином, мета цієї роботи зводиться до розробки необхідних розділів політики безпеки, що забезпечуватимуть захист від існуючих в ІТС загроз. Для того, щоб створити такі розділи, необхідно, як вже було зазначено, проаналізувати існуючі на ОІД умови і зробити відповідні висновки, що і було зроблено. Отримані результати показують, з якими загрозами інформаційній

безпеці можуть зіткнутися, зокрема, дизайнерські компанії, як можуть бути знижені відповідні ризики та які профілактичні заходи можуть бути застосовані. Процес створення КСЗІ, у тому числі обстеження ОІД та розробку політики безпеки інформації, 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».

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ТОВ «Сладко Дніпро»

Об`єктом інформаційної діяльності є філіал товариства з обмеженою відповідальністю «Сладко Дніпро». Адреса: Дніпропетровська область, м. Дніпро, пр. Гагаріна, буд. 21, 3 поверх.

Організація надає наступні послуги:

- обробка замовлень з само виносом;
- обробка замовлень з доставкою;
- консультація клієнтів стосовно продукції;
- реєстрація клубних карток.

Організація працює з понеділка по неділю з 8:00 до 22:00 з плаваючими вихідними. У неробочий час територія підприємства стає під охорону фірми «КРОК», цілісність території забезпечується системою охоронно-пожежної сигналізації.

1.2 Обґрунтування необхідності створення КСЗІ

Згідно ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством. Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації. Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.[1]

Згідно НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка є власністю держави, належить до державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. Якщо в ІТС обробляються інші види інформації, то вимоги цього нормативного документа суб'єкти системи ТЗІ можуть використовувати як рекомендації.

Роботи зі створення КСЗІ виконуються організацією-власником (розпорядником) ІТС з дотриманням вимог нормативно-правових актів щодо провадження господарської діяльності у сфері захисту інформації.[2]

Підсумовуючи, згідно з прийнятим власником інформації рішенням, на підприємстві має бути створена КСЗІ, виходячи з того в ІТС обробляється інформація, що є комерційною таємницею, та інформація, захист якої передбачається договорами між клієнтами та компанією.

Виходячи з того в ІТС обробляється інформація, що є комерційною таємницею та інформація, захист якої передбачається інформаційною політикою підприємства (за рішенням власника інформації) та/або законодавством України, має бути створена КСЗІ.

1.3 Обстеження ОІД

1.3.1 Відомості про фізичне середовище ОІД

Стіни будівлі, в якій знаходиться ОІД, – цегляні та покриті армованим бетоном. Фундамент – плитний, 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.

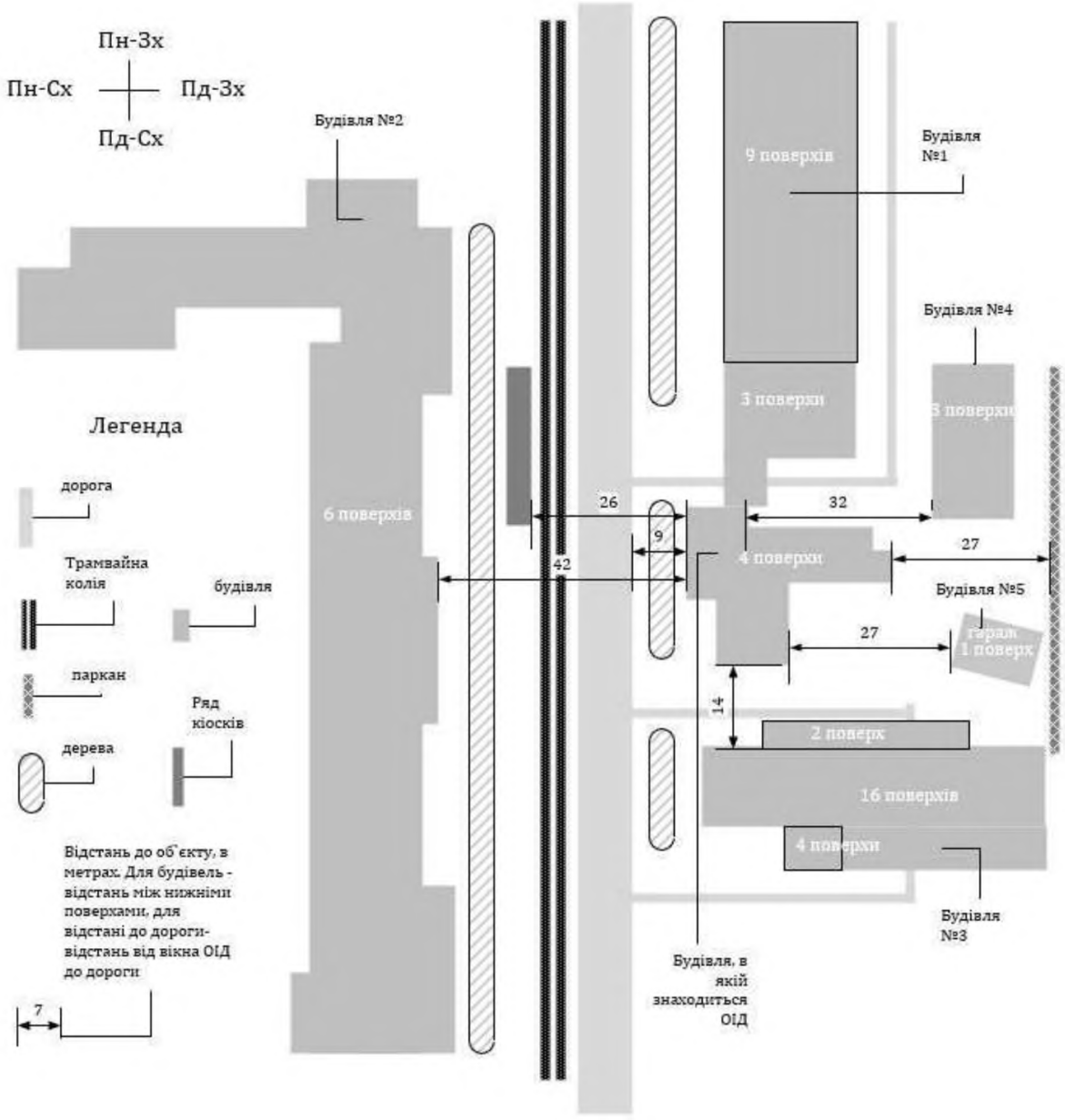

Рисунок 1.1 – Ситуаційний план ОІД

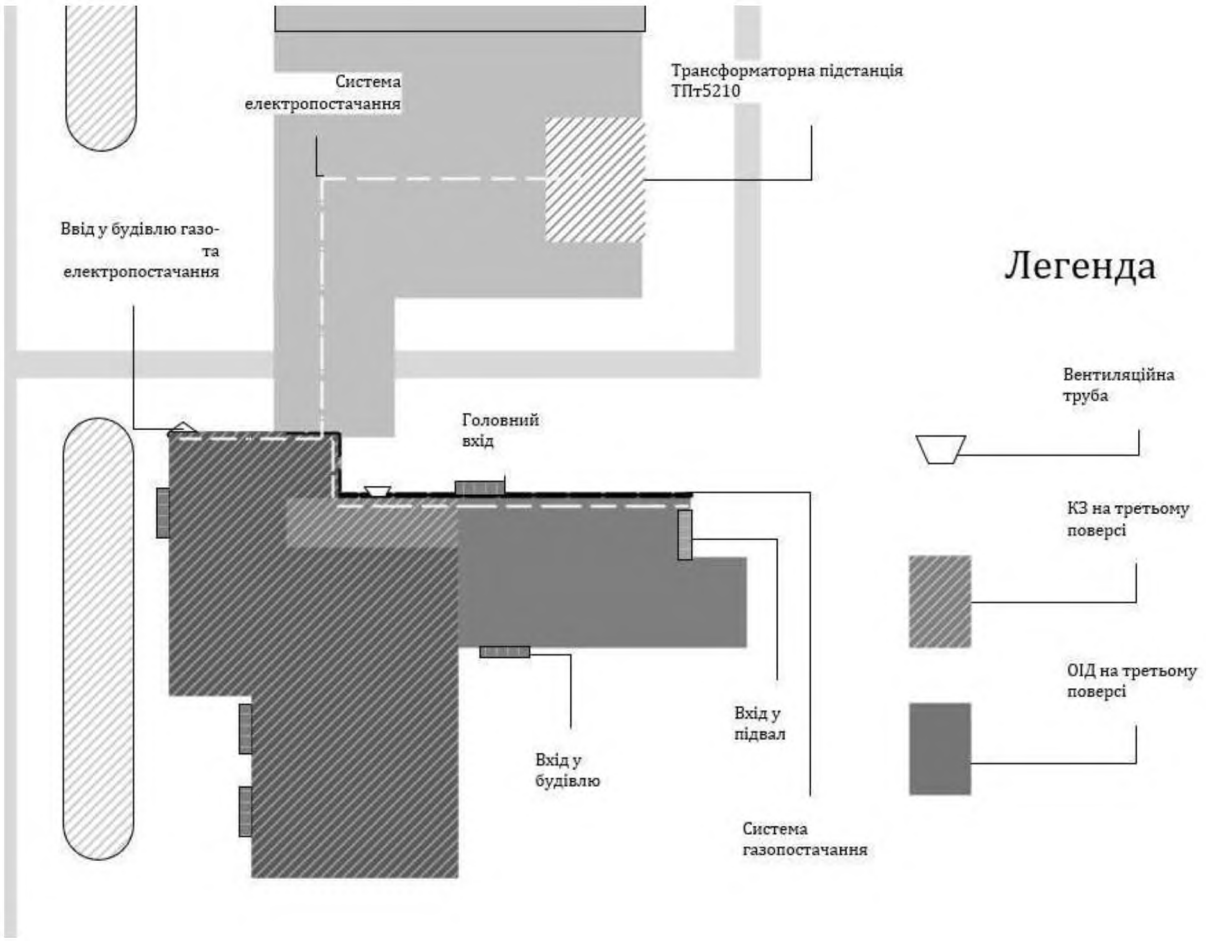

Рисунок 1.2 – Комунікації

На заході від ОІД знаходиться проспект Гагаріна, найкоротша відстань до нього - 9м. На проспекті інтенсивно рухається транспорт, ширина проїзної частини – близько 10м, 2 полоси руху в кожний бік. В таблиці 1.1 наведено будівлі, що знаходяться поруч з ОІД.

Таблиця 1.1 – Будівлі, що знаходяться поруч з ОІД

Порядковий номер	Тип об`єкту	Адреса	Розташування відносно ОІД	Мінімальна відстань до ОІД	Додатково
1	Національна металургійна академія України	пр. Гагаріна,17	Пн-Сх	0м	

Продовження таблиці 1.1

Порядковий номер	Тип об`єкту	Адреса	Розташування відносно ОІД	Мінімальна відстань до ОІД	Додатково
2	Український державний хіміко технологічний університет	пр. Гагаріна, 8	Зх	42м	
3	Адміністративно -житловий комплекс	пр. Гагаріна, 23	Пд	10м	В будівлі знаходиться кафе «Пузата хата», його вікна виходять на ОІД
4	Покинута будівля	пр. Гагаріна, 19	Сх	32м	
5	Гараж		Пд-Сх	27м	

Внутрішні та зовнішні стіни офісу -цегляні. Товщина зовнішніх стін -380 мм, внутрішніх несних стін -250 мм, внутрішніх перегородок – 65 мм. Вікна металопластикові, подвійні, 2100 х 1500 мм. Вхідні двері – алюмінієві – 1000 мм шириною і висотою 2100 мм. Замок - моноблок тринаправленого закривання зі сталі, закривається вбудованим циліндром з унікальним розміщенням пінів в трьох площинах. Міжкімнатні двері – дерев`яні 90 х 2100 мм і 80 х 2100 мм. Офіс має висоту 3 м (від підлоги до стелі), присутня натяжна стеля. Підлога на підприємстві – ковролін і плитка.

На південному заході від офісу знаходяться магазин одягу і сервісний центр, що спеціалізується на ремонті комп`ютерів. На другому поверсі (знизу ОІД) знаходиться салон краси. На четвертому (зверху ОІД) – приміщення ремонтується (планується офіс).

У нічний час на підприємстві працює відеоспостереження – камери спрямовані на двері всередині будівлі і по периметру будівлі ззовні. На підприємстві у нічний час працюють інфрачервоні датчики руху.

Сигналізація передає сигнал про несанкціонований доступ на пульт охоронного агентства «Крок». На рисунку 1.3 наведено генеральний план ОІД.

1.3.2 Загальні відомості про будівлю, в якій розташований ОІД

ОІД розташований на 2 поверсі 6-поверхової будівлі.

Централізовані системи опалення, водопостачання, водовідводу, вентиляції виходять за межі контрольованої зони. Вентиляція організована за допомогою вентиляційних труб.

Стіни будівлі, в якій знаходиться ОІД зроблені з вогнестійкої силікатної цегли (25х12х6,5 см). Фундамент – стрічковий, дах – покритий руберойдом з грубозернистим посипанням з лицьового боку і полімерною плівкою з наплавляємого боку полотна, територія навколо будівлі покрита асфальтом.

Внутрішні та зовнішні стіни офісу – цегляні. Товщина зовнішніх стін – 380 мм (3 шари цегли із цементом та внутрішньою штукатуркою), внутрішніх несучих стін – 250 мм (3 шари цегли із цементом та штукатуркою), внутрішніх перегородок – 65 мм (металоконструкція та гіпсокартон). Вікна – металопластикові, подвійні, 2100 х 1500 мм. Вхідні двері – металопластикові двостулкові з подвійним армованим склом – 2000 мм шириною і висотою 2500 мм. Замок - вирізаний зі сталі, закривається вбудованим циліндром під ключ з перфорацією. Міжкімнатні двері – металопластикові 90 х 2100 х 100 мм. Офіс має висоту 3 м (від підлоги до стелі), стеля – натяжна, з металевим коробом по периметру стелі. Підлога на підприємстві – лінолеум і плитка (у кафетерії та туалеті).

Поверх над ОІД пустий, поверх під ОІД орендується продуктовим магазином та магазином взуття.

Комп'ютери кожного з відділів з'єднані в локальну мережу і мають вихід в Інтернет через безлімітне ADSL-підключення від ВАТ «Київстар».

На рисунку 1.2 зображена схема приміщень ОІД (генеральний план ОІД) із вказанням схеми розміщення комунікацій, систем відеоспостереження, основних та допоміжних технічних засобів.

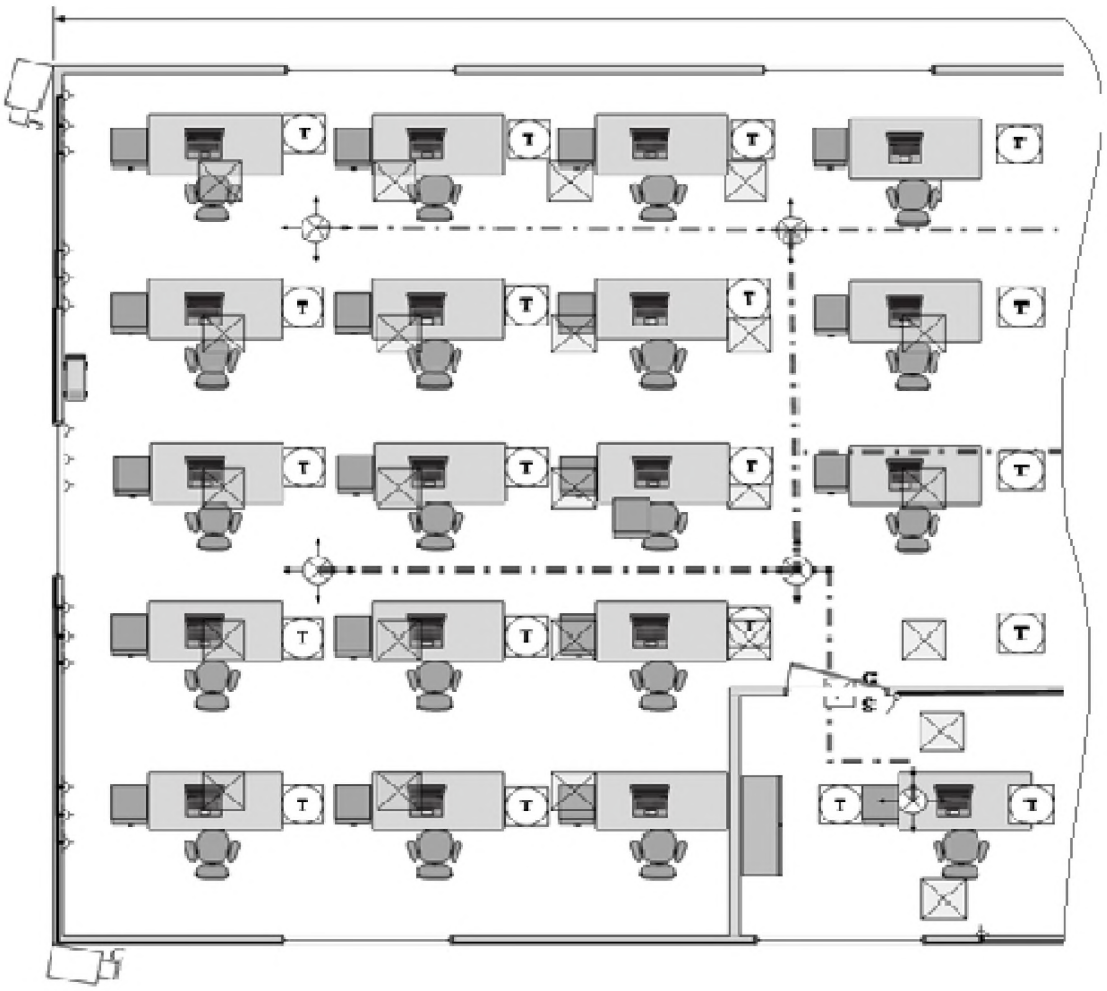

Рисунок 1.3 Генеральний план ОІД

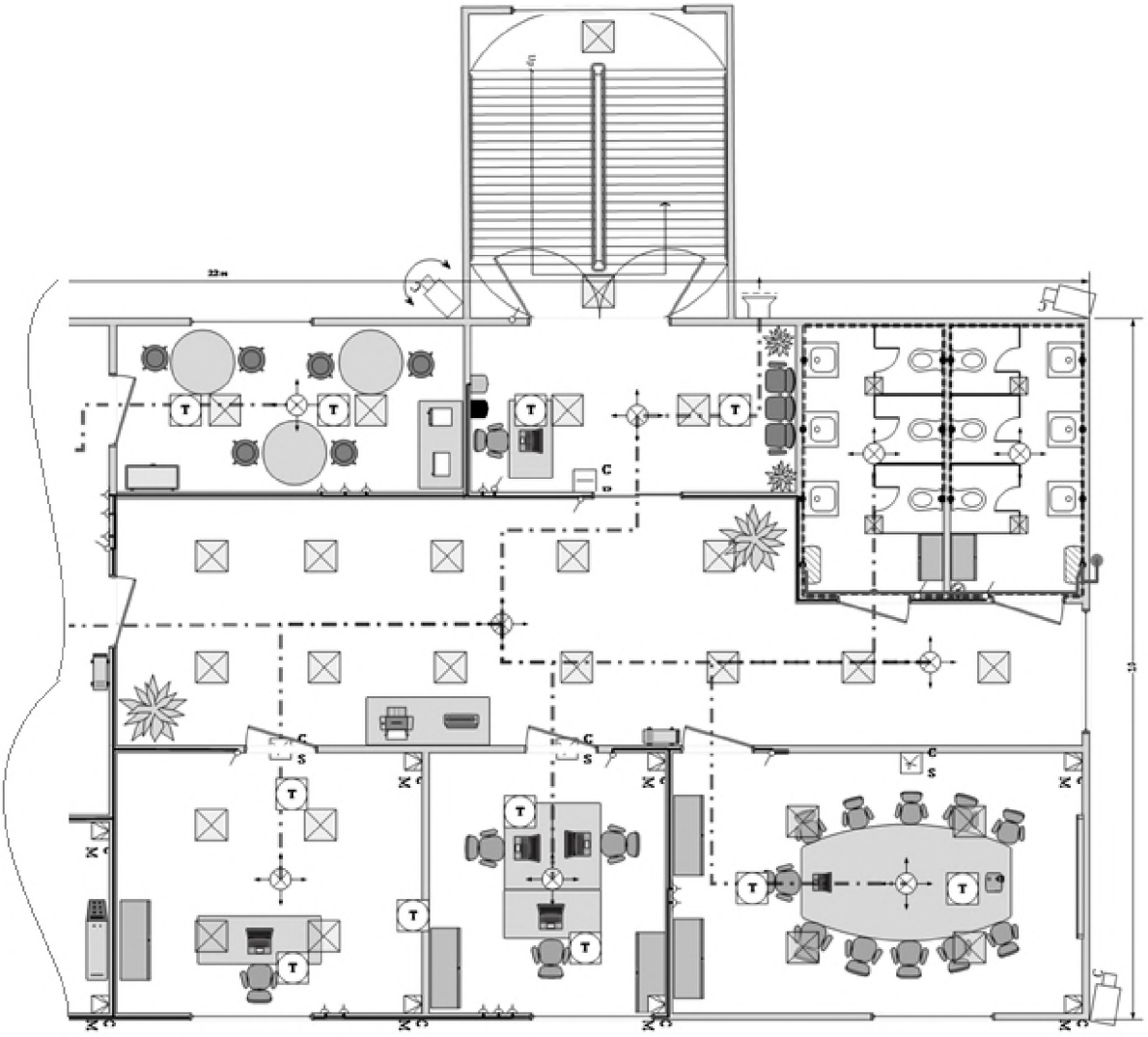

Рисунок 1.3 – Генеральний план ОІД – продовження, частина 2

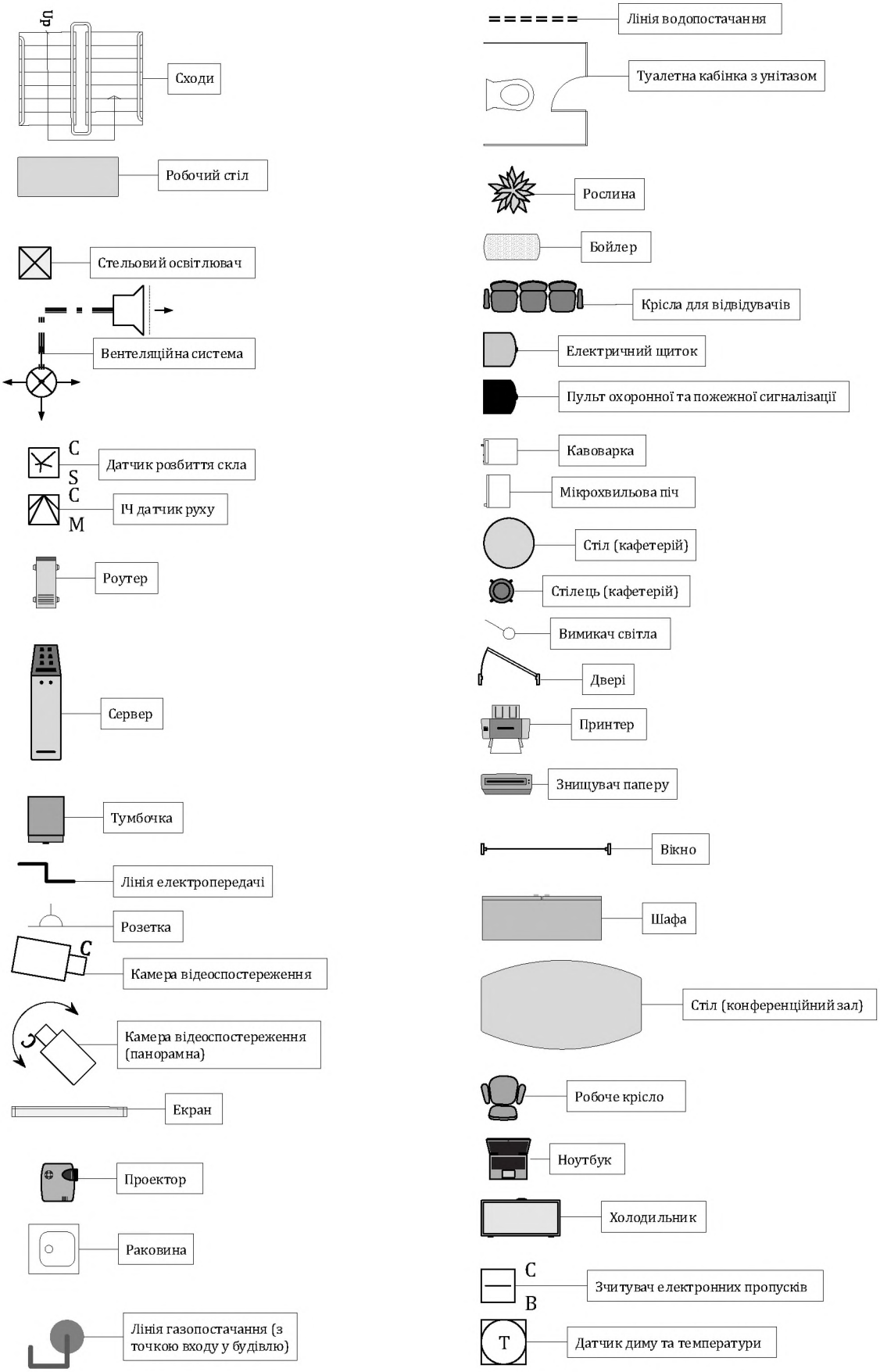

Рисунок 1.4 – Генеральний план ОІД – продовження, легенда

1.3.3 Основні та допоміжні технічні засоби

Зображені на рисунку 1.2 основні та допоміжні технічні засоби, більш детально описані із вказанням відстані до меж контрольованої зони у таблиці 1.2.

Таблиця 1.2 – Опис основних технічних засобів та допоміжних технічних засобів

Тип	Модель	Місцезна-ходження	Мінімальна відстань до межі ОІД або ліній, що виходять за межі ОІД	Кількість
Миша	Logitech M170 Wireless Black	Відділ операторів	1,5 м	25
		бухгалтерія	1,7 м	
		Кабінет директора	1,6 м	
		Пункт охорони	0,7 м	
		Конференційний зал	2,2 м	
		Кабінет системного адміністратора	1 м	
Ноутбук	Lenovo IdeaPad 320-14IAP (80XQ007ARA) Onyx Black	Відділ операторів	1,5 м	25
		бухгалтерія	1,7 м	
		Кабінет директора	1,6 м	
		Пункт охорони	0,7 м	
		Конференційний зал	2,2 м	
		Кабінет системного адміністратора	1 м	
Принтер	Canon MAXIFY MB5140 with Wi-Fi (0960C007AA)	Коридор	2 м	1

Продовження таблиці 1.2

Тип	Модель	Місцезна-ходження	Мінімальна відстань до межі ОІД або ліній, що виходять за межі ОІД	Кількість
Знищувач документів	shredMARK 1203X	Коридор	2 м	1
Холодильник	GORENJE R6192LB	Кафетерій	0,1 см	1
Сервер	Dell PowerEdge T30 (210-AKHI)	Кабінет системного адміністратора	0,1 м	1
Роутер	Mercusys MW301R	Відділ операторів	0,1 м	3
		Коридор	0,1 м	
Кавова машина	PHILIPS Daily Collection (HD7459/20)	Кафетерій	0,1 м	1
Мікрохвильова піч	MYSTERY MMW-2013	Кафетерій	0,1 м	1
Мультимедійний проектор	Epson EB-X41 (V11H843040)	Конференційний зал	1,5 м	1

1.3.4 Обчислювальна система ОІД

На підприємстві використовуються 25 ноутбуків, 3 wi-fi роутери, 1 сервер, 1 мультимедійний проектор, 1 принтер. За ноутбуками працюють закріплені за ними користувачі (окрім ноутбуку, що знаходиться в конференційній залі – за нього відповідає працівник, що бере його для проведення презентацій чи конференцій). Компанія використовує зв'язок з віддаленим сервером, з яким відбувається синхронізація бази даних клієнтів та інформації про продукцію. Також на віддалений сервер відвантажуються розпорядчі документи директора та документація бухгалтерії.

Усі користувачі мають доступ в Інтернет. Топологія мережі – «зірка», усі ноутбуки, сервер та принтер підключені до одної мережі (два роутери

ретранслюють сигнал від першого, збільшуючи зону покриття мережі). Сервер керує протоколами: DNS, FTP, DHCP.

Потрібно зазначити, що система інтегрована і має модульну структуру. Надалі буде розглядатися частина системи, виділена на структурній схемі мережі компанії, що зображена на рисунку 1.3.

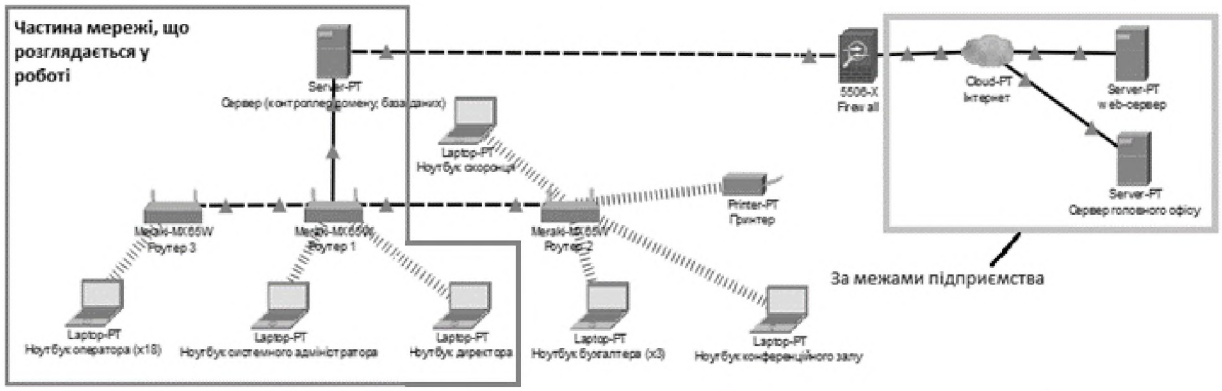

Рисунок – 1.5 Структурна схема мережі компанії

Операційна система, встановлена на ноутбуках: Windows 8.1 Professional (білд 9600) (корпоративна ліцензія), операційна система на сервері: Windows Server 2016 (білд 14393.0).

Таблиця 1.3 – Опис основних технічних засобів та їх характеристик

Пристрій	Компонент	Характеристика	Інвентарний номер
Ноутбук (Lenovo IdeaPad 320-14IAP (80XQ007ARA) Onyx Black)	Екран	Діагональ екрану 14 " Дозвіл екрану 1366x768 HD Тип матриці TN Покриття екрану Матове	000000143 – 000000160
	Процесор	Модель центрального процесора: Pentium N4200 Кількість ядер: 4 ядра Частота центрального процесора: 1,1 (2,5) ГГц	

Продовження таблиці 1.3

Пристрій	Компонент	Характеристика	Інвентарний номер
Ноутбук (Lenovo IdeaPad 320-14IAP (80XQ007ARA) Onyx Black)	ОЗУ	Обсяг ОЗУ: 4 ГБ Максимальний обсяг ОЗУ: 8 ГБ Кількість слотів ОЗУ: 1 Тип оперативної пам'яті: DDR3L Частота оперативної пам'яті: 1600 МГц	000000143 – 000000160
	Жорсткий диск	Обсяг накопичувача: 500 ГБ Тип накопичувача: HDD Серійний номер: 520BF0634 – 520BF0651	
	Відеокарта	Виробник відеокарти: AMD Модель графічного процесора: Radeon 530 Обсяг відео пам'яті: 2 ГБ Тип відеокарти: Дискретний Тип пам'яті відеокарти: DDR5	
	Веб камера	Дозвіл веб-камери: 0,3 Мп	
	Інтерфейси	Оптичний привід Без дисковода Тип бездротової мережі: Wi-Fi 802.11 ac Bluetooth: Версія 4.1 HDMI: Є Кількість: USB 2.0 1 шт. Кількість: USB 3.1 1 шт. Кардрідер: 4 в 1	
Сервер (Dell PowerEdge T130)	Процесор	Тип процесора: Чотирьохядерний Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц) Кількість гнізд під процесори: 1 Чіпсет: Intel C236 Охолодження процесора: BOX	000000161

Продовження таблиці 1.3

Пристрій	Компонент	Характеристика	Інвентарний номер
Сервер (Dell PowerEdge T130)	ОЗУ	Об'єм оперативної пам'яті: 8 ГБ Архітектура: 4 слота DIMM Максимальний обсяг ОЗУ: до 64 ГБ, DDR4, 2133 ГГц	000000161
	Жорсткий диск	1 ТБ, SATA Entry NHP Серійний номер: 380FX078S	
	Інтерфейси	Інтерфейс HDD: SATA Оптичний привід: DVD +/- RW Передня панель: 2 x USB 3.0 2 x USB 2.0 3.5 мм вхід для навушників 3.5 мм вхід для мікрофона Задня панель: 4 x USB 3.0 1 x PS / 2 для підключення клавіатури і мишки 1 x DisplayPort 1 x HDMI 1 x LAN (RJ-45) 1 x COM (послідовний порт) 1 x аудіовхід 1 x аудіовихід 1 x роз'єм для мікрофона Слоти розширення: 1 x PCIe x16 3.0 1 x PCIe x16 3.0 (x4)	

Продовження таблиці 1.3

Пристрій	Компонент	Характеристика	Інвентарний номер
Сервер (Dell PowerEdge T130)	Інтерфейси	1 x PCIe x4 3.0 1 x PCI	000000161
	Додаткові характеристики	Порт локальної мережі: Intel I219-LM гігабіт Ethernet (10/100/1000) Блок живлення: 290 Вт Кількість LAN (RJ-45): 1 Швидкість LAN: Gigabit Ethernet Частота роботи Wi-Fi: 2.4 ГГц Швидкість LAN портів: 100 Мбіт/с Швидкість Wi-Fi: 300 Мбіт/с WAN-порт: Ethernet Шифрування: WPA-PSK / WPA-PSK2	
Роутер (Mercusys MW301R)	Загальні характеристики	Частота роботи Wi-Fi: 2.4 ГГц Швидкість LAN портів: 100 Мбіт/с Швидкість Wi-Fi: 300 Мбіт/с WAN-порт: Ethernet Шифрування: WPA-PSK / WPA-PSK2	000000162 – 000000164
	Інтерфейси	2x10/100 Мбіт/с Ethernet LAN 1x10/100 Мбіт/с Ethernet WAN	
	Бездротові можливості	802.11b 802.11g 802.11n	
	Антени	Конструкція антен: Незнімні Кількість антен: 2 зовнішні антени	

Продовження таблиці 1.3

Пристрій	Компонент	Характеристика	Інвентарний номер
Роутер (Mercusys MW301R)	Підтримка протоколів	DHCP PPPoE L2TP PPTP	000000162 – 000000164
	Інші функції	Функції бездротової мережі: WDS bridge Тип WAN: динамічний IP-адресу/статичний IP-адресу/PPPoE/PPTP/L2TP Управління: контроль доступу, локальне управління, віддалене управління DHCP: сервер Перенаправлення портів: віртуальний сервер, UPnP, DMZ Динамічний DNS: Oray Брандмауер: прив'язка по IP і MAC-адресу Протоколи: IPv4	
	Корпус	Колір: білий Розміри:135.77 x 93.31 x 25.85 мм	
Принтер (Canon MAXIFY MB5140 with Wi-Fi (0960C007AA))	Загальні характеристики	Технологія друку: струменевий друк Максимальна роздільна здатність друку: 600x1200 dpi Мережеві інтерфейси: Wi-Fi/Ethernet Розширення зображення принтера: Принтер: 600x1200 точок на дюйм Кількість кольорів: 4	000000165

Продовження таблиці 1.3

Пристрій	Компонент	Характеристика	Інвентарний номер
Принтер (Canon MAXIFY MB5140 with Wi-Fi (0960C007AA))	Формат і щільність паперу	Формат паперу: Звичайний папір: A4, A5, B5, LTR, LGL, конверт Фотопапір: A4, LTR, 20x25 см, 13x18 см, 10x15 см Формати, що встановлюються користувачем: ширина 89-215.9 мм; довжина 127-355.6 мм Щільність паперу: Звичайний папір: 64 - 105 г / м² Фотопапір Canon: до 275 г / м² швидкість друку A4: 15.5 зобр. / Хв (кольоровий режим); 24 зобр. / Хв (монохромний режим)	000000165

На ноутбуках працівників встановлене програмне забезпечення, що необхідне для виконання їх професійних обов’язків.

Таблиця 1.4 – Опис встановленого ПЗ

Тип ПЗ	Повна назва	Версія	Ліцензія
Системне, спеціалізоване	AVG AntiVirus FREE	19.3.2369	Free
Прикладне	Крамниця-CRM	1.0	Власне ПО компанії для обслуговування клієнтів у режимі чату
Спеціалізоване	Wireshark	2.6.5	GNU GPL
Спеціалізоване	CCleaner	5.50.0.6911	Free Edition
Спеціалізоване	Network Inventory Advisor	3.6.0	–
Спеціалізоване	PDQ Deploy	1.1.2	–

Продовження таблиці 1.4

Тип ПЗ	Повна назва	Версія	Ліцензія
Прикладне	Пакет Office 365 Business преміум (Word, Excel, PowerPoint, Outlook, SharePoint, OneDrive, OneNote, Microsoft Teams, Publisher, Access)	11425.20202	Корпоративна

Перелік персоналу, що має відношення до обраної частини ОІД, та їх обов'язки:

1 директор:

– затвердження документів на оплату праці співробітників;

– прийняття рішень щодо прийняття на роботу, звільнення та заохочення працівників, поліпшення їх мотивації;

– забезпечення ефективної взаємодії всіх структурних підрозділів організації, контроль їх діяльності;

– вживання заходів щодо покращення умов праці на підприємстві;

2 системний адміністратор:

– слідкування за станом локальної мережі, підтримання її в належному стані;

– встановлення необхідного ПЗ;

– перевірка журналів подій

– відповідальність за інформаційну безпеку на підприємстві, проведення необхідних заходів та відповідна модернізація системи;

– відповідальність за резервне копіювання;

– встановлення і конфігурування оновлень операційної системи;

– керування сервером;

3 оператори контактного центру:
- консультування клієнтів стосовно продукції;
- обробка замовлень;
- перевірка наявності продукції у точках роздрібної торгівлі;

4 прибиральниця:
- прибирання приміщення підприємства у встановлений час.

1.3.5 Інформаційне середовище ОІД

У цьому розділі описана інформація, що циркулює в ІТС. Перелік інформації з вказання режиму доступу та правового режиму поданий у таблиці 1.5.

Таблиця 1.5 – Інформація, що циркулює на об’єкті

№	Інформація	Режим доступу	Правовий режим
1	Розпорядження директора	Відкрита	–
2	Звіти старших зміни	Відкрита	–
3	Звіти системного адміністратора	З обмеженим доступом	Конфіденційна
4	Персональні дані клієнтів	З обмеженим доступом	Конфіденційна
5	Дані про продукцію на складі	З обмеженим доступом	Комерційна таємниця
6	Дані про замовлення	З обмеженим доступом	Комерційна таємниця
7	Інформація про продукцію	Відкрита	–

У таблиці 1.6 описана класифікації інформації за наступними властивостями:

- конфіденційність;

– цілісність;

– доступність.

Таблиця 1.6 – Класифікація інформації, за властивостями (конфіденційність, цілісність, доступність)

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Розпорядження директора	К2	Ц4	Д4
Звіти старших зміни	К1	Ц4	Д3
Звіти системного адміністратора	К4	Ц3	Д3
Персональні дані клієнтів	К5	Ц4	Д5
Дані про продукцію на складі	К4	Ц3	Д5
Дані про замовлення	К1	Ц4	Д4
Інформація про продукцію	К1	Ц3	Д4

Для класифікації інформації були використані рівні властивостей, що описані далі.

Рівні конфіденційності:

– К1– рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

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

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

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

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

Рівні цілісності:

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

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

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

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

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

Рівні доступності:

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

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

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

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

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

Підсумовуючи, маємо наступний перелік об'єктів АС:

1 Розпорядження директора *(інформація);*

2 Звіти старших зміни *(інформація);*

3 Звіти системного адміністратора *(інформація);*

4 Персональні дані клієнтів *(інформація);*

5 Дані про продукцію на складі *(інформація);*

6 Дані про замовлення *(інформація);*

7 Інформація про продукцію *(інформація);*

8 AVG AntiVirus FREE *(програмне забезпечення);*

9 Крамниця-CRM *(програмне забезпечення)*

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

11 Wireshark *(програмне забезпечення);*

12 CCleaner *(програмне забезпечення);*

13 Network Inventory Advisor *(програмне забезпечення);*

14 PDQ Deploy *(програмне забезпечення).*

Нижче наведена технологія обробки інформації в ІТС, що описую порядок та перелік дії, що виконуються над інформацією:

Розпорядження директора завантажуються на сервер, після цього з ними можуть ознайомитись робітники. Після завантаження на сервер розпорядження директора відвантажуються на віддалений сервер до головного офісу компанії.

Звіти старших зміни складаються операторами, що визначені старшими зміни у конкретний день і передаються директору, шляхом завантаження їх на сервер, де, в свою чергу, з ними може ознайомитись директор.

Звіти системного оператора складаються системним адміністратором на основі даних про мережу і окремих робочих станцій і передаються директору, шляхом завантаження їх на сервер, де, в свою чергу, з ними може ознайомитись директор.

Персональні дані клієнтів використовуються операторами у разі замовлення клієнтом продукції додому або на конкретне відділення роздрібної торгівлі, для ідентифікації клієнта кур'єром, або продавцем відділення. При складанні замовлення оператор вказує прізвище, ім'я та номер клубної картки клієнта. Персональні дані клієнтів зберігаються на сервері. На сервер завантажуються з віддаленого сервера у головному офісі компанії.

Дані про продукцію на складі використовуються операторами при складанні замовлення у випадку, коли конкретна продукція відсутня у вибраному клієнтом відділенні роздрібної торгівлі і потрібно додатково перевірити її наявність на складі та організувати доставку зі складу до вибраного клієнтом відділення. Також дані про продукцію на складі використовуються операторами при замовленні клієнтом продукції додому, для перевірки наявності конкретної продукції, та організації її доставки за вказаною клієнтом адресою.

Дані про замовлення використовуються операторами при складанні замовлень від клієнтів. Дані про замовлення потрапляють на ноутбуки операторів та сервер з веб-серверу. Дані про замовлення обробляються операторами за допомогою власного ПЗ підприємства Крамниця-CRM.

Інформація про продукцію використовується операторами у випадку, коли клієнту потрібна додаткова консультація при складанні замовлення. Оператору заборонено розповідати подробиці виготовлення.

У доповнення до технології обробки інформації, на рисунку 1.4 схема інформаційних потоків на підприємстві

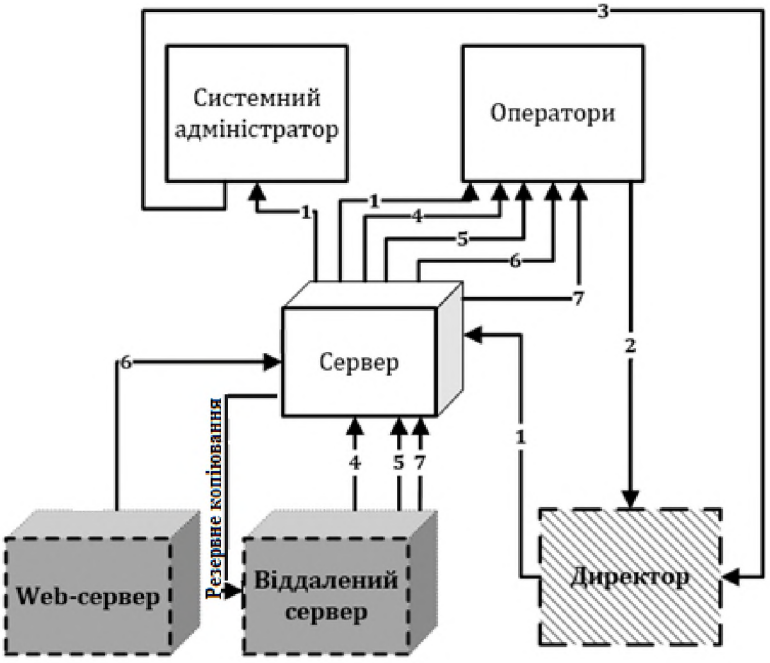

Рисунок 1.4 Інформаційні потоки на підприємстві

Аналізуючи існуючі атрибути доступу, можна скласти матрицю доступу, що буде описувати можливості користувачів АС відносно об'єктів.

Матриця доступу наведена у таблиці 1.7, розшифрування умовних позначень матриці доступу вказане після таблиці 1.7.

Таблиця 1.7 – Матриця доступу до інформації та ПЗ

Користувачі	Інформація	ПЗ	Елементи КС
Системний адміністратор	1 – Ч, З, К, Д, В 3 – С, Ч, З, К, М, Д, В	8 – Вк, Вст, О, В 9 – Вк, Вст, О, В 10 – Вк, Вст, О, В 11 – Вк, Вст, О, В 12 – Вк, Вст, О, В 13 – Вк, Вст, О, В 14 – Вк, Вст, О, В	Користування одним ноутбуком, доступ до Інтернету, доступ до сервера по локальній мережі.
Оператори контактного центру	1 – Ч, З, К, Д, В 2 (звичайний оператор) – Ч, З, К, Д, В 2 (старший зміни) – С, Ч, З, К, М, Д, В	9 – Вк, Вст, О, В 10 – Вк, Вст, О, В	Користування одним ноутбуком, доступ до Інтернету, доступ до сервера по локальній мережі.

Продовження таблиці 1.7

Користувачі	Інформація	ПЗ	Елементи КС
Оператори контактного центру	4 – Ч, З, К, М 5 – Ч 6 – Ч, З, К, М, Д, В 7 – Ч, З, К, М, Д, В		
Директор	1 – С, Ч, З, К, М, Д, В 3 – Ч, З, К, М, Д, В	10 – Вк, Вст, О, В	Користування одним ноутбуком, доступ до Інтернету, доступ до сервера по локальній мережі.

Дії, що можуть виконуватись з інформацією:

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

Дії, що можуть виконуватись з ПЗ:

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

1.4 Аналіз загроз інформації, що циркулює на ОІД

1.4.1 Аналіз джерел загроз

Для інформації, що обробляється в ІТС можуть бути характерними такі види джерел загроз:

1. Антропогенні;
   1.1 Внутрішні;
      1.1.1 Системний адміністратор;
      1.1.2 Оператори контакт-центру;
      1.1.3 Директор;
      1.1.4 Прибиральниця;
   1.2 Зовнішні;
      1.2.1 Конкуренти;
      1.2.2 Злочинці;
      1.2.3 Хакери;
2. Техногенні;
      2.1 Сервер та ПЗ, що встановлене на ньому;
      2.2 Ноутбуки, ПЗ, встановлене на них;
3. Стихійні;
      3.1 Пожежа;
      3.2 Форс-мажорні обставини – інші непередбачені обставини.

У таблиці 1.8 проводиться аналіз ступеню небезпеки з боку того чи іншого джерела загроз.

Таблиця 1.8 – Ранжування загроз

Джерело загрози	К1	К2	К3	К загальне
Системний адміністратор	5	3	4	0,480
Оператори контакт центру	4	2	4	0,256
Директор	4	2	4	0,256
Прибиральниця	3	1	2	0,048
Конкуренти	3	5	5	0,600

Продовження таблиці 1.8

Джерело загрози	К1	К2	К3	К загальне
Злочинці	1	4	3	0,096
Хакери	3	5	4	0,480
Сервер та ПЗ, що встановлене на ньому	5	3	4	0,480
Ноутбуки, ПЗ, встановлене на них;	5	3	3	0,360
Пожежа	3	4	3	0,288
Форс-мажорні обставини – інші непередбачені обставини	2	4	3	0,192

Надалі описуються рівні, що були використання для ранжування джерел загроз.

К1 – визначає ступінь доступності до об’єкта:

– 1 – джерело дуже віддалене від об’єктів захисту і не може впливати на нього (для техногенних) / немає доступу до об’єкта (для антропогенних) / на ОІД відсутні будь-які передумови виникнення джерела загрози (для стихійних);

– 2 – джерело дуже віддалене від об’єктів захисту, але все ще може впливати на нього (для техногенних) / можливо отримати віддалений доступ до об’єкта (для антропогенних) / на ОІД є деякі передумови виникнення джерела загрози, але імовірність їх прояву дуже мала (для стихійних);

– 3 – джерело знаходиться поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних) / джерело має обмежений доступ до технічних і програмних засобів обробки інформації (для антропогенних) / довгий час не було жодного прояву джерела загрози, втім, є передумови для його появи (для стихійних);

– 4 – джерело знаходиться в тому ж приміщенні (для техногенних) / джерело має доступ до технічних і програмних засобів обробки інформації, що захищається, але це не є його функціональним обов'язком (для антропогенних) / ОІД не знаходиться у зоні дії катаклізмів, втім, імовірність прояву джерела загрози висока (для стихійних);

– 5 – сам об'єкт містить джерело загрози (для техногенних) / джерело має повний доступ до технічних і програмних засобів обробки інформації, що захищається, а також максимальні повноваження доступу. (для антропогенних) / ОІД знаходиться у зоні дії катаклізмів (для стихійних).

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

– 1 – виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей / техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником / на ОІД немає жодних можливостей для виникнення джерела загрози;

– 2 – виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози / ПЗ та техніка оновлюється не постійно / на об'єкті є умови, що запобігають прояву джерела загрози;

– 3 – виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загроз / ПЗ та техніка вразливі для деяких атак / прояв джерела загрози можливий, але швидше за все він не зможе проявити себе;

– 4 – виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози / відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка / прояв джерела загрози можливий;

– 5 – мета виконавця; виконавець є експертом у методах, що реалізують загрозу (наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське ПЗ, тощо / умови сприяють прояву джерела загрози.

К3 – фатальність наслідків:

– 1 – ОІД нічого не втратить, або наслідки будуть позитивними;

– 2 – Наслідками можна знехтувати;

– 3 – Наслідки відчутні, але несуттєві;

– 4 – Наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу;

– 5 – Наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

Проаналізувавши обчислення, можна зробити висновок, що можна знехтувати такими джерелами загроз (К загальне <= 0,2):

– прибиральниця;

– злочинці;

– форс-мажорні обставини.

1.4.2 Аналіз вразливостей

Провівши аналіз заданих умов на ОІД, можна зробити висновок, що для даної ІТС можливі такі вразливості:

1 Об’єктивні;

1.1 Технічні канали витоку інформації;

1.2 Можливість несанкціонованого підключення до бездротової мережі;

1.3 Використання неліцензійного ПЗ;

1.4 Відсутність коректного розмежування прав доступу до об’єктів;

1.5 Відсутність механізмів протидії несанкціонованому підключенню знімних пристроїв до робочих станцій;

2 Суб’єктивні;

2.1 Помилки робітників;

2.2 Відсутність контролю за переміщенням відвідувачів у денний час – відсутність регламентованого порядку відвідувань території підприємства;

2.3 Відсутність контролю за встановленням та оновленням ПЗ;

2.4 Відсутність системи пожежогасіння;

2.5 Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення;

3 Випадкові;

3.1 Збій ;

3.2 Відмова;

3.3 Псування матеріальних носіїв інформації.

Таблиця 1.9 – Ранжування вразливостей

Вразливість	К1	К2	К3	К загальне
Технічні канали витоку інформації	3	2	3	0,144
Можливість несанкціонованого підключення до бездротової мережі	3	3	5	0,360
Використання неліцензійного ПЗ	3	2	4	0,192
Відсутність коректного розмежування прав доступу до об'єктів	5	5	4	0,800
Відсутність механізмів протидії несанкціонованому підключенню знімних пристроїв до робочих станцій	4	4	4	0,512
Помилки робітників	2	5	5	0,400
Відсутність регламентованого порядку відвідувань території підприємства	3	4	5	0,480
Відсутність контролю за встановленням та оновленням ПЗ	4	3	5	0,480

Продовження таблиці 1.9

Вразливість	К1	К2	К3	К загальне
Відсутність системи пожежогасіння	2	4	4	0,192
Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення	4	4	5	0,640
Збій	3	3	5	0,360
Відмова	3	3	4	0,288
Псування матеріальних носіїв	2	3	4	0,192

інформації				

Надалі описуються рівні, що були використання для ранжування вразливостей.

К1 – ступінь впливу вразливості на фатальність наслідків:

– 1 – використання вразливості не призведе до серйозних наслідків;
– 2 – вразливість може призвести до реалізації загрози, але ймовірність цього досить мала;
– 3 – використання вразливості може призвести до реалізації загрози;
– 4 – використання вразливості швидше за все призведе до реалізації загрози;
– 5 – використання вразливості точно призведе до реалізації загрози.

К2 – можливість та зручність використання вразливості:

– 1 – вразливість неможливо або надзвичайно важко використати;
– 2 – використання вразливості потребує великої кількості часу та ресурсів;
– 3 – для використання вразливості необхідні певні умови;
– 4 – вразливість може використати будь-яка людина, яка володіє необхідними знаннями, вміннями чи привілеями;
– 5 – вразливість може використати практично будь-хто.

К3 - кількість елементів об’єкта, яким характерна вразливість:

– 1 – 0-1 елемент;
– 2 – 2-9 елементів;
– 3 – 10-14 елементів;
– 4 – 15-25елементів;
– 5 – 25+ елементів.

Проаналізувавши обчислення, можна зробити висновок, що можна знехтувати такими вразливостями (К загальне <= 0,2):

– Технічні канали витоку інформації;
– Псування матеріальних носіїв інформації.

1.4.3 Аналіз загроз

Таким чином маємо наступний перелік актуальних джерел загроз:

– Д1 – Системний адміністратор;
– Д2 – Оператори контакт центру;
– Д3 – Директор;
– Д4 – Конкуренти;
– Д5 – Хакери;
– Д6 – Сервер та ПЗ, що встановлене на ньому;
– Д7 – Ноутбуки, ПЗ, встановлене на них;
– Д8 – Пожежа;

та перелік актуальних вразливостей:

– В1 – Можливість несанкціонованого підключення до бездротової мережі;
– В2 – Використання неліцензійного ПЗ;
– В3 – Відсутність коректного розмежування прав доступу до об’єктів;
– В4 – Відсутність механізмів протидії несанкціонованому підключенню знімних пристроїв до робочих станцій;
– В5 – Помилки робітників;
– В6 – Відсутність регламентованого порядку відвідувань території підприємства;
– В7 – Відсутність контролю за встановленням та оновленням ПЗ;
– В8 – Відсутність системи пожежогасіння;
– В9 – Відсутність регламентованого порядку встановлення та планової зміни паролів, критеріїв до їх створення;
– В10 – Збій;
– В11 – Відмова;

Надалі можна порахувати критичність від використання певних вразливостей певним джерелом (актуальність конкретних загроз, коефіцієнтами виступають добутки коефіцієнтів небезпеки джерела і вразливості).

Таблиця 1.10 Ранжування загроз

Вразливості	В1	В2	В3	В4	В5	В6	В7	В8	В9	В10	В11
Джерела загроз											
Д1	-	0.092	0,384	-	-	-	-	-	-	-	-
Д2	-	0,074	0,205	0,131	-	-	-	-	-	-	-
Д3	-	0,074	-	-	-	-	-	-	-	-	-
Д4	0,216	-	-	-	-	0,288	-	-	0,384	-	-

Продовження таблиці 1.10

Вразливості	В1	В2	В3	В4	В5	В6	В7	В8	В9	В10	В11
Джерела загроз											
Д5	0,173	-	-	-	0,192	0,230	0,230	-	0,307	-	-
Д7	-	-	-	-	-	-	-	-	-	0,130	0,104

Д8	-	-	-	-	-	-	-	0.055	-	-	-

Таким чином, використовуючи пороговий коефіцієнт 0,1, можна знехтувати наступними загрозами:

– Ураження системи вірусами з неліцензованого ПЗ (Д1В2/Д2В2/Д3В2);

– Знищення інформації та матеріальних цінностей пожежею (Д8В8);

Актуальними можна вважати такі загрози:

– Злам мережі, порушення нормального функціонування системи (Д4В1/Д5В1);

– Несанкціоноване ознайомлення/модифікація/видалення інформації (Д1В3/Д2В3);

– Несанкціоноване копіювання інформації на знімні носії (Д2В4);

– Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи (Д5В5);

– Несанкціоноване ознайомлення /модифікація/видалення інформації, крадіжка/псування матеріальних цінностей конкурентами та зловмисниками (Д4В6/Д5В6);

– Використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами (Д5В7);

– Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди (Д4В9/Д5В9);

– Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює (Д6В10/Д7В10);

– Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи (Д6В11/Д7В11).

Надалі потрібно класифікувати загрози за їх

Таблиця 1.11 Класифікація загроз за впливом на властивості інформації

Загрози	Які властивості інформації порушуються		
	К	Ц	Д

Загрози	Які властивості інформації порушуються		
	К	Ц	Д
Злам мережі, порушення нормального функціонування системи	+	+	+
Несанкціоноване ознайомлення/модифікація/видалення інформації	+	+	+
Несанкціоноване копіювання інформації на знімні носії	+	–	–
Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи	+	+	–
Несанкціоноване ознайомлення /модифікація/видалення інформації, крадіжка/псування матеріальних цінностей конкурентами та зловмисниками	+	+	+

Продовження таблиці 1.11

Загрози	Які властивості інформації порушуються		
	К	Ц	Д
Використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами	+	+	–
Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди	+	+	–
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює	–	+	+
Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи	–	–	+

1.5 Висновок і постановка задачі

У першому розділі описаний об'єкт:

- вид його діяльності;
- загальна інформація про будівлю, у якій розташований ОІД;
- відомості про устаткування;
- відомості про інформаційну систему і інформаційні потоки;
- відомості про персонал та доступ персоналу до об’єктів АС.

У технічному завданні виконаний аналіз загальної моделі загроз, визначений перелік джерел загроз і існуючих проблем у системі безпеки.

В результаті проведеного обстеження ОІД побудовано модель загроз, які актуальні для даної ІТС, було класифіковано інформацію, що зберігається і циркулює на підприємстві та виявлено ресурси, які потребують найбільшого рівня інформаційної безпеки. Отримані результати будуть використані для розробки рекомендацій щодо оновлення ПБ ІТС «Сладко Дніпро».

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінки існуючого стану захищеності

Відповідно до 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]

Таким чином, необхідно, відповідно до класу системи, провести аналіз існуючого функціонального профілю, а також розробити новий функціональний профіль, що вимагав би вимогам, необхідним для запобігання загроз, описаних у першому розділі кваліфікаційної роботи.

Враховуючи те, що подана ІТС багатокористувачева та розподілена, можна дійти висновку, що це АС 3 класу.

Існуючий профіль захищеності:

3.КЦД.1 = {КО-1, КВ-1, ДР-1, НР-2, НИ-2, НО-1, НТ-2}

Рекомендований профіль захищеності:

3.КЦД.2 = {КА-2, КО-1, КВ-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НО-1, НТ-2}

Таблиця 2.1 – Критерії захищеності інформації

Критерії	Механізми реалізації (3.КЦД.1)	Механізми реалізації (3.КЦД.2)
КА-2	–	Розмежування прав доступу за допомогою засобів Active Directory
КО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
КВ-1	Використання протоколу SSL	Використання протоколу SSL
ЦА-2	–	Розмежування прав доступу за допомогою засобів Active Directory
ЦО-1	Засоби Active Directory	Засоби Active Directory (засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів, у тому числі, додаткове використання «*Veeam Endpoint Backup*»)
ДР-1	Засоби Active Directory	Засоби Active Directory
ДВ-1	Засоби Active Directory	Засоби Active Directory (засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів, у тому числі, додаткове використання «*Veeam Endpoint Backup*»)
НР-2	Вбудовані засоби Windows (журнал подій)	Вбудовані засоби Windows (журнал подій)
НИ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
НТ-2	AVG AntiVirus FREE	AVG AntiVirus FREE

Базова адміністративна конфіденційність (КА-2).

Послуга адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів до користувачів. В системі, яка реалізує послугу адміністративна конфіденційність на рівні КА-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.

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).

Ця послуга дозволяє адміністратору чи спеціально авторизованому користувачу керувати потоками інформації від користувачів і процесів до захищених об'єктів. Згідно з політикою адміністративної цілісності (в повній аналогії з адміністративною конфіденційністю) об'єкту привласнюються атрибути доступу, що визначають домен, якому повинні належати ті користувачі чи процеси, які намагаються модифікувати об’єкт. На даному рівні адміністратор може накладати обмеження на доступ до об'єктів з боку користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів. […]

ЦО-1. Обмежений відкат.

Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу 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, за допомогою яких можна безпечним чином повернути КС до нормального функціонування. […]

НР-2. Захищений журнал.

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

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

НИ-2. Одиночна ідентифікація і автентифікація.

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

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 КЗЗ перевірити 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. […][3]

2.2 Проектні рішення – рекомендації, щодо модернізації політики безпеки

2.2.1 Теоретична складова

Відповідно до НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки"

може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила. Далі для скорочення замість словосполучення "політика безпеки інформації" може використовуватись словосполучення "політика безпеки", а замість словосполучення "політика безпеки інформації, що реалізується послугою" — "політика послуги" і т. ін.

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

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

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

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

2.2.2 Організаційні заходи щодо забезпечення реалізації політики безпеки

На організаційному рівні повинні бути проведені наступні заходи:

1 розробка та впровадження посадових інструкцій користувачів та персоналу ІТС, а також інструкцій, якими регламентується порядок виконання робіт іншими особами з числа тих, що мають доступ до ІТС;

2 обмеження доступ в приміщення, в яких відбувається обробка та зберігання інформації з обмеженим доступом (детальніше у розділі *2.2.4 Політика відвідування території підприємства сторонніми особами*);

3 розробка та впровадження розпорядчої документи щодо правил перепусткового режиму на територію, де розташована ІТС (детальніше у розділі *2.2.4 Політика відвідування території підприємства сторонніми особами*);

4 розробка та впровадження розпорядчих документів щодо використання робочих станцій користувачами із зазначенням у них, що користувач несе матеріальну відповідальність за цілісність робочої станції;

5 розмежування прав користувачів ІТС із розділенням на групи користувачів, згідно з матрицею доступу, програмними методами ОС (детальніше у розділі *2.2.3 Політика розмежування доступу*);

6 встановлення максимальної кількості спроб для входу у систему, після якої обліковай запис буде заблокований;

7 впровадження механізмів контролю використання CD і DVD-дисководів, жорстких дисків, зовнішніх USB-носіїв, USB-портів (детальніше у розділі *2.2.7 Політика використання зовнішніх інтерфейсів робочих станцій*);

8 впровадження механізмів резервного копіювання з метою захисту локальних розділів диску від випадкового або навмисного форматування (детальніше у розділі *2.2.5 Політика резервного копіювання*);

9 впровадження регламенту оновлення програмного забезпечення (детальніше у розділі *2.2.8 Політика оновлення програмного забезпечення*);

10 впровадження регламенту створення та зміни паролів (детальніше у розділі *2.2.6 Політика вибору та зміни паролів*);

11 заборона користувачам завантаження, встановлення або оновлення будь-яких програм без відома системного адміністратора (детальніше у розділі *2.2.8 Політика оновлення програмного забезпечення*);

12 проведення навчально-кваліфікаційних заходів, перевірки та закріплення навичок персоналу стосовно роботи з обчислювальною технікою, з метою запобігання помилок персоналу, що можуть зашкодити підприємству у той чи інший спосіб.

2.2.3 Політика розмежування доступу

Мета політики:

Створення регламенту доступу користувачів до ресурсів обчислювальної системи.

Область дії:

Область дії політики розмежування доступу розповсюджується на всіх співробітників підприємства.

Відповідальні особи політики безпеки:

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

Політика безпеки:

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

Атрибути доступу, відповідно до посадових обов'язків користувачів, зазначені у таблиці 2.2 (пояснення до таблиці вказане після матриці доступу).

Таблиця 2.2 – Рекомендовані атрибути доступу

Користувач	Інформація	ПЗ
Системний адміністратор	1 – Ч 3 – С, Ч, З, К, М, Д, В	8 – Вк, Вст, О, В 9 – Вк, Вст, О, В

Користувач	Інформація	ПЗ
		10 – Вк, Вст, О, В 11 – Вк, Вст, О, В 12 – Вк, Вст, О, В 13 – Вк, Вст, О, В 14 – Вк, Вст, О, В
Оператор х18	1 – Ч 2 (старший зміни) – С, Ч, З, К, М, Д, В 4 – Ч 5 – Ч 6 – Ч 7 – Ч	12 – Вк 13 – Вк 14 – Вк
Директор	1 – С, Ч, З, К, М, Д, В 3 – Ч	10 – Вк

Перелік ПЗ та інформації:

1 Розпорядження директора *(інформація);*

2 Звіти старших зміни *(інформація);*

3 Звіти системного адміністратора *(інформація);*

4 Персональні дані клієнтів *(інформація);*

5 Дані про продукцію на складі *(інформація);*

6 Дані про замовлення *(інформація);*

7 Інформація про продукцію *(інформація);*

8 AVG AntiVirus FREE *(програмне забезпечення);*

9 Крамниця-CRM *(програмне забезпечення);*

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

11 Wireshark *(програмне забезпечення);*

12 CCleaner *(програмне забезпечення);*

13 Network Inventory Advisor *(програмне забезпечення);*

14 PDQ Deploy *(програмне забезпечення).*

Для інформації:

– С – створення;

– Ч – читання;

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

Для ПЗ:

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

Порядок та періодичність перегляду:

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

Відповідальність:

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

2.2.4 Політика відвідування території підприємства сторонніми особами

Мета політики:

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

Область дії:

Область дії політики безпеки відносно відвідування території підприємства сторонніми особами розповсюджується, насамперед, на всіх осіб, що мають намір

отримати доступ до території підприємства, але не є співробітниками підприємства та на співробітників, що визначаються відповідальними за перебування сторонніх осіб на підприємстві.

Відповідальні особи політики безпеки:

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

Політика безпеки:

Контроль доступу до території підприємства реалізується електронним замком на вхідних дверях. В якості ключів використовуються магнітні картки. Кожний робітник, при зарахуванні у штат, отримує персональну картку, яку забороняється передавати третім особам. Для осіб, що регулярно відвідують територію підприємства, але не є співробітниками компанії, виготовляються тимчасові картки.

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

Також, обов'язковою умовою для отримання допуску на територію підприємства є реєстрація у журналі відвідувачів, що знаходиться у охоронця. До журналу заноситься прізвище, ім'я, по батькові відвідувача, фіксується час, коли відвідувач зайшов на територію підприємства (засвідчується його підписом) та час коли він вийшов з території підприємства (також засвідчується його підписом). Для перевірки істинності наданих відвідувачем даних можуть бути використані наступні документи:

– паспорт;
– водійські права;
– закордонний паспорт.

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

Дії з виконання політики інформаційної безпеки:

Виконання політики контролюється охоронцем за допомогою аналізу журналу відвідувачів, нагляду за територією підприємства за допомогою системи відеоспостереження. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики. Після ознайомлення з даною політикою користувач має підписатися у спеціальному журналі з техніки безпеки.

Порядок та періодичність перегляду:

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

Відповідальність:

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

2.2.5 Політика резервного копіювання

Мета політики:

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

Область дії:

Область дії політики резервного копіювання розповсюджується на системного адміністратора.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики резервного копіювання є системний адміністратор.

Політика безпеки:

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

Технологічна інформація, конфігурації ПЗ і т.д. необхідно копіювати на окремі знімні носії, які має право використовувати лише системний адміністратор. Резервне копіювання цих даних має проводитися як мінімум раз на місяць.

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

До технологічної інформації, що підлягає резервному копіюванню належить:

– групові політики;
– атрибути розмежування доступу;
– конфігурації ПЗ;
– дані про облікові записи.

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

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

Оскільки документи постійно завантажуються на локальний сервер за віддаленого серверу, а документи, що створюються, власне, співробітниками філіалу відвантажуються до головного офісу (на віддалений сервер), вони не потребують додаткового резервного копіювання.

Дії з виконання політики інформаційної безпеки:

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

Порядок та періодичність перегляду:

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

Відповідальність:

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.2.6 Політика вибору та зміни паролів

Мета політики:

Встановити правила використання паролів для входу у систему. Користувачі системи повинні дотримуватися вимог, що регламентуються даною політикою. Виконання вимог даної політики підвищує рівень захищеності інформаційних ресурсів, що циркулюють та обробляються на підприємстві.

Область дії:

Область дії політики безпеки відносно паролів розповсюджується на всіх користувачів, що мають доступ електронних документів.

Відповідальні особи політики безпеки:

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

Політика безпеки:

– паролі видаються системним адміністратором особисто, відповідальність за видачу паролів згідно приведеним нижче критеріям несе системний адміністратор.

– паролі користувачів мають бути унікальними і не повинні повторюватись;

– паролі мають бути довжиною не менше ніж 8 символів (але не більше 16 символів) і повинні включати у себе:

– латинські заголовні букви (A-Z);

– латинські прописні букви (a-z);

– цифри (0-9);

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

– пароль не має містити ім'я облікового запису;

– паролі заборонено передавати третім особам;

– паролі не можна вставляти до тексту програм, чи записуватися на папері чи зберігатися в незашифрованому вигляді;

– паролі мають змінюватися кожні 3 місяці (чи раніше при виникненні загрози розголошення пароля чи його втрати).

При створенні паролю рекомендується використовувати метод «півслова». У такому випадку, частина паролю, що генерується системним адміністратором має бути не коротшою ніж 8 символів, а частина, що генерується системою не має містити повторюваних символів.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює системний адміністратор підприємства за допомогою вбудованих засобів аутентифікації в ОС. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики. Після ознайомлення з даною політикою користувач має підписатися у спеціальному журналі з техніки безпеки.

Порядок та періодичність перегляду:

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

Відповідальність:

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

2.2.7 Політика використання зовнішніх інтерфейсів робочих станцій

Мета політики:

Встановити правила використання зовнішніх інтерфейсів робочих станцій. Користувачі системи повинні дотримуватися вимог, що регламентуються даною політикою.

Область дії:

Область дії політики безпеки використання зовнішніх інтерфейсів робочих станцій розповсюджується на всіх користувачів, що мають доступ електронних документів та не мають права на використання зовнішніх інтерфейсів робочих станцій відповідно до своїх посадових обов'язків (оператори контактного центру).

Відповідальні особи політики безпеки:

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

Політика безпеки:

До зовнішніх інтерфейсів робочих станцій слід віднести CD/DVD-дисководи та USB-порти.

CD/DVD-дисководи мають бути вимкнені на апаратному рівні системним адміністратором на усіх робочих станція користувачів, відносно яких діє ця політика.

CD/DVD-дисководи можуть бути використані лише системним адміністратором у разі виникнення потреби у встановленні і/або налагоджуванні системи. У такому разі, системний адміністратор має сповістити відповідного співробітника та директора у письмовій формі про проведення технічних робіт, не пізніше ніж за 2 дні. Після проведення робіт, системний адміністратор має подати

директору звіт про проведення технічних робіт з зазначенням причин та інвентарного номера робочої станції, на якій проводились роботи.

USB-порти мають бути опечатані системним адміністратором на усіх робочих станція користувачів, відносно яких діє ця політика. Пломба має містити підпис системного адміністратора. При опечатуванні системний адміністратор повинен робити запис у журналі використання зовнішніх інтерфейсів із вказанням номеру запису, дати опечатування та інвентарного номеру робочої станції. За наявності 2 і більше USB-портів, опечатування кожного порту відзначається окремим записом.

USB-порти можуть бути використані лише системним адміністратором у разі виникнення потреби у встановленні і/або налагоджуванні системи. У такому разі, системний адміністратор має сповістити відповідного співробітника та директора у письмовій формі про проведення технічних робіт, не пізніше ніж за 2 дні. У день проведення технічних робіт з USB-порта знімається опечатування. При знатті опечатування робиться відповідний запис у журналі використання зовнішніх інтерфейсів із вказанням номеру запису, дати опечатування та інвентарного номеру робочої станції. Після проведення робіт, системний адміністратор має знову опечатати USB-порт за вказаною вище процедурою та подати директору звіт про проведення технічних робіт з зазначенням причин та інвентарного номера робочої станції, на якій проводились роботи.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює системний адміністратор, раз на тиждень перевіряючи цілісність печаті та її істинність. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

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

Відповідальність:

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

2.2.8 Політика оновлення програмного забезпечення

Мета політики:

Встановити правила та порядок оновлення програмного забезпечення.

Область дії:

Область дії політики оновлення програмного забезпечення розповсюджується на всі робочі станції.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики є системний адміністратор.

Політика безпеки:

Рекомендується створити регламент планової перевірки актуальності версії. Строки перевірки мають перепадати на 1-5 число кожного нового календарного місяця. Оновлення ПЗ має проводити тільки системний адміністратор.

Системний адміністратор повинен перевіряти кожну нову версію програмного забезпечення у захищеному середовищі, наприклад – на віртуальній машині. Після тестування нової версії, системний адміністратор повинен відправити директору запит із проханням дозволу проведення технічних робіт з оновлення ПЗ. За 3 дні до схваленого оновлення, системний адміністратор повинен сповістити усіх працівників письмово та в електронному вигляді про планове оновлення ПЗ.

Після проведення оновлення ПЗ, системний адміністратор повинен надати директору звіт про проведення технічних робіт з оновлення та налагодження програмного забезпечення, що повинен містити:

- назву ПЗ;
- дату оновлення;
- номер старої версії;
- номер нової версії.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює директор підприємства, контролюючи звітність системного адміністратора про оновлення ПЗ. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

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

Відповідальність:

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.2.9 Політика захисту мережі

Мета політики:

Підвищити рівень захищеності та стійкості мережі до зламу.

Область дії:

Область дії політики захисту мережі розповсюджується на мережеве покриття Wi-Fi.

Відповідальні особи політики безпеки:

Відповідальною особою за виконання політики є системний адміністратор.

Політика безпеки:

Усі дії, пов’язані з забезпеченням безпеки мережі повинні виконуватися системним адміністратором.

Для забезпечення надійного захисту рекомендується змінювати пароль для роутерів кожні 2 місяці. Пароль генерує системний адміністратор використовуючи правила створення паролів, описані в політиці вибору та зміни паролів.

Рекомендується змінювати пароль для Wi-Fi мережі кожен місяць (наприклад 1 числа кожного місяця). Пароль генерує системний адміністратор використовуючи правила створення паролів, описані в політиці вибору та зміни паролів. Для кожної окремої робочої станції пароль вводиться окремо системним адміністратором, що дозволяє мінімізувати кількість осіб, що знають пароль.

Рекомендується вимкнути видимість точки доступу, задля унеможливлення виявлення її без спеціалізованого обладнання.

Режим WPS повинен бути вимкненим у налаштуваннях роутерів, оскільки він вважається нестійким до зламу.

Рекомендується вимкнути протокол DHCP та використовувати список довірених MAC-адрес, задля унеможливлення виділення IP-адреси при спробі несанкціонованого підключення.

Рекомендується вимкнути функцію віддаленого доступу у налаштуваннях роутерів, задля унеможливлення отримання доступу до них через мережу Інтернет.

Рекомендується знизити рівень сигналу до такого рівня, щоб сигнал можна буде виявити лише на території підприємства.

Дії з виконання політики інформаційної безпеки:

Виконання політики контролює директор підприємства, контролюючи звітність системного адміністратора про стан мережі. При прийнятті (зміні) політики безпеки кожен співробітник, якого стосується політика, має бути сповіщений не пізніше, ніж за 5 робочих днів до прийняття нової редакції даної політики.

Порядок та періодичність перегляду:

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

Відповідальність:

Відповідальність за невиконання політики безпеки несе системний адміністратор.

2.3 Висновок спеціального розділу

В спеціальній частині було проаналізовано існуючий функціональний профіль захищеності, обрано новий профіль, що відповідає вимогам, необхідним для підвищення стану захищеності. Було розроблено перелік організаційних заходів, метою яких є підведення стану захищеності АС до необхідного рівня.

Окремою увагою відзначено вирішення актуальних для даного підприємства проблем інформаційної безпеки, описаних у першому розділі в моделі загроз.

Таким чином, були розроблені рекомендації, щодо доповнення та оновлення існуючої на підприємстві політики інформаційної безпеки стосовно наступних аспектів:

- розмежування доступу до інформаційних ресурсів АС;
- перепустковий режим підприємства;
- резервне копіювання;
- створення та зміна паролів;
- оновлення ПЗ;
- захист мережі.

РОЗДІЛ 3. ЕКОНОМІЧНА ЧАСТИНА

3.1 Мета техніко-економічного обґрунтування дипломного проекту

Метою виконання економічного розділу є визначення економічної доцільності використання запропонованих засобів та заходів інформаційної безпеки на ТОВ «Сладко Дніпро».

Для визначення цього необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити обсяги 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.

3.2 Визначення витрат на розробку політики безпеки інформації

3.2.1 Розрахунок капітальних (фіксованих) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.[6]

За методикою Gartner Group до фіксованих (капітальних) варто відносити наступні витрати:

– вартість розробки проекту інформаційної;

– витрати на залучення зовнішніх консультантів;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– вартість створення основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

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

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Відповідно до специфіки розробленої ПБ та конкретних рішень, обраних у цій політиці, актуальними капітальними витратами можна вважати наступні:

– вартість розробки проекту інформаційної безпеки;

– вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ);

– витрати на первісні закупівлі апаратного забезпечення;

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

– витрати на навчання технічних фахівців і обслуговуючого персоналу.

Розрахунок вартості розробки політики безпеки здійснюється з використанням двох показників – трудомісткості розробки ПБ і витрат на її розробку.

Трудомісткість у даному випадку буде розраховуватися за формулою 3.1:

$$t = t_{об} + t_{а} + t_{вз} + t_{озб} + t_{д\ год}, \qquad (3.1)$$

де $t_{об}$ – тривалість проведення обстеження АС підприємства; $t_{а}$ – тривалість процесу аналізу ризиків; $t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту; $t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації; $t_{д}$ – тривалість документального оформлення політики безпеки.

Показники часу, витраченого на розробку політики інформаційної безпеки наведені у таблиці 3.1.

Таблиця 3.1 – Часові показники трудомісткості розробки ПБ

Показник	Значення, год
$t_{об}$	65
$t_{а}$	16
$t_{вз}$	10
$t_{озб}$	16
$t_{д}$	16

Згідно з формулою 3.1 трудомісткість розробки ПБ становить:

$$t = 65\,год + 16\,год + 10\,год + 16\,год + 16\,год,$$

і, таким чином,

$$t = 123\,год.$$

Надалі потрібно розрахувати витрати на створення ПБ ($К_{рп}$), використовуючи наступні показники – витрати на заробітну плату спеціаліста з інформаційної безпеки ($З_{зп}$) та вартість витрат машинного часу ($З_{мч}$). Розрахунок проводиться за формулою 3.2:

$$К_{рп} = З_{зп}\,грн. \qquad (3.2)$$

У свою чергу, витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

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

де t – загальна тривалість розробки політики безпеки, годин; $З_{іб}$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину. Средньогодинна заробітна плата спеціаліста з інформаційної безпеки, в загальному випадку, становить – 72 грн/год.

Згідно з формулою 3.3, витрати на заробітну плату спеціаліста ІБ становлять:

$$З_{зп} = 123\,год \cdot 72\,грн/год,$$

і, таким чином,

$$З_{зп} = 8856\,грн.$$

Тож, витрати на створення ПБ за формулою 3.2 становлять:

$$К_{рп} = 8856\,грн.$$

У результаті розрахунків, маємо вартість розробки ПБ – 8856 гривень.

У даному конкретному випадку повна вартість капітальних витрат розраховується за формулою 3.4:

$$К = К_{рп} + К_{навч}\,грн. \qquad (3.4)$$

Під $К_{навч}$, мається на увазі одноразовий кваліфікаційний захід для співробітників, з питань ознайомлення з новою редакцією політики безпеки. Даний захід проводиться спеціалістом ІБ, тому додатково йому виплачується сума у розмірі 500 грн, окрім виплати за розробку нової редакції ПБ.

Тож, згідно до формули 3.4, повна вартість капітальних витрат становить:

$$К = 8856\ грн + 500\ грн,$$

і, таким чином,

$$К = 9356\ грн.$$

3.2.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.[6]

Для даного підприємства актуальними будуть наступні витрати:

– заробітна плата обслуговуючого персоналу;

– кваліфікаційні заходи та перевірка знань персоналу стосовно правил, регламентованих політикою безпеки;

– технічне й організаційне адміністрування й сервіс.

Оскільки методи захисту, передбачені політикою безпеки, мають більш організаційний характер, поточними витратами можна вважати заробітну платню системного адміністратора, витрати на опечатування зовнішніх інтерфейсів робочих станцій та витрати пов’язані з діяльністю користувачів, тож поточні витрати розраховуються за формулою 3.5:

$$С = С_{за} + С_{оп} + С_{дк}\ грн, \qquad (3.5)$$

де $С_{за}$ – витрати на заробітну плату системного адміністратора; $С_{оп}$ – витрати на опечатування зовнішніх інтерфейсів робочих станцій; $С_{дк}$ – витрати, пов’язані з діяльністю користувачів.

У свою чергу, витрати на заробітну плату системного адміністратора розраховуються за формулою 3.6:

$$C_{запад} = З_{дод1} + З_{дод2}\ грн, \quad (3.6)$$

Де $З_{дод1}$ – додаткова заробітна плата системного адміністратора за проведення кваліфікаційних заходів та перевірку знать та навичок персоналу стосовно правил, регламентованих політикою безпеки; $З_{дод1}$ – додаткова заробітна плата системного адміністратора за додаткові обов'язки – відповідальність за виконання деяких розділів політики безпеки інформації.

Додаткова заробітна платня №1 складає 500 грн за проведення одного кваліфікаційного заходу. Такі заходи планується проводити раз на 2 місяці, тож фактично за місяць системний адміністратор отримуватиме 250 грн додаткової заробітної платні №1 на місяць. Додаткова платня №2 враховуватиме обсяг відповідальності, що покладатиметься на системного адміністратора політикою безпеки. Таким чином, розмір додаткової заробітної платні №2 становитиме – 1000 грн/місяць.

За формулою 3.6, можна розрахувати:

$$C_{запад} = (250\ грн\ +\ 1000\ грн) \cdot 12\ місяців,$$

і, таким чином,

$$C_{запад} = 15000\ грн.$$

Поточні витрати за опечатування зовнішніх інтерфейсів на рік включатимуть у себе вартість 2 журналів (200 грн) опечатування та 150 пломб-наліпок (450 грн). Тож:

$$C_{оп} = 200\ грн + 450\ грн,$$

і, таким чином,

$$C_{оп} = 650\ грн.$$

Витрати, пов'язані з діяльністю користувачів мають під собою на увазі витрати, що спричинені професійною діяльністю. Такою діяльністю вважається перенавантаження серверу і частий перезапис інформації на жорстких дисках

серверу у процесі роботи, що приведе сервер у неробочий стан. Такі витрати включають у себе вартість полагодження серверу, профілактична заміна компонентів. За рік, вартість таких витрат сягатиме 1500 грн. Тож:

$$C_{дк} = 1500\ грн.$$

Розрахунок повної вартості експлуатаційних витрат за формулою 3.5:

$$C = 15000\ грн + 650\ грн + 1500\ грн,$$

і, таким чином,

$$C = 17150\ грн.$$

3.3 Оцінка величини збитку у разі реалізації загроз

Метою цієї оцінки є визначення обсягів матеріальних збитків, виходячи з імовірності реалізації конкретної загрози й можливих матеріальних втрат від неї.

Далі буде вказано загрози з можливим економічним впливом на підприємство:

1 злам мережі, порушення нормального функціонування системи призводить до простою на підприємстві;

2 несанкціоноване ознайомлення з інформацією (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

3 несанкціонована модифікація/видалення інформації (співробітниками) призведе до порушення робочого процесу, що у свою чергу призведе до втрати частини запланованого заробітку;

4 несанкціоноване копіювання інформації на знімні носії (співробітниками) може призвести до розголошення інформації, що є інформацією з обмеженим доступом, наприклад, – закриті дані про продукцію, що виступають комерційною таємницею, що в свою чергу може

призвести до втрати частини запланованого заробітку через використання цих даних конкурентами;

5 помилки персоналу, що дозволяють зловмисникам отримати доступ до системи мають схожий ефект зі зламом мережі;

6 несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками має схожий ефект з несанкціонованим ознайомленням з інформацією працівниками;

7 несанкціонована модифікація/видалення інформації конкурентами та зловмисниками має схожий ефект з несанкціонованою модифікацією/видаленням інформації співробітниками;

8 крадіжка/псування матеріальних цінностей (об'єктів ІТС) конкурентами та зловмисниками призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

9 використання недоліків неоновленого ПЗ для отримання доступу до мережі хакерами має схожий ефект зі зламом мережі;

10 злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди має схожий ефект зі зламом мережі;

11 збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює, у свою чергу це призведе до простою у функціонуванні підприємства, та як наслідок – до втрати частини запланованого заробітку;

12 відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи, що в свою чергу призведе до втрати частини запланованого заробітку.

Для розрахунку збитків від реалізації даних загроз потрібно використати формулу 3.7:

$$U = П_п + П_в + V\,грн, \qquad (3.7)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн; $П_в$ – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн; V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

У свою чергу, для розрахунку $П_п$, $П_в$ *і* V, використовують формули 3.8, 3.9, 3.10 відповідно.

$$П_п = \frac{\sum Зс}{F} \cdot t_п \ грн, \tag{3.8}$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_в = П_{ви} + П_{пв} + П_{зч} \ грн, \tag{3.9}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн; $П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн; $П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{О}{F} \cdot (t_п + t_в + t_{ви}) \ грн, \tag{3.10}$$

де F – місячний фонд робочого часу; $О$ – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у місяць; $t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

У свою чергу, $П_{ви}$ і $П_{пв}$ розраховуються за формулами 3.11 і 3.12 відповідно.

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} \ грн, \qquad 3.11$$

де F – місячний фонд робочого часу; $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць; $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_{в} \ грн, \qquad 3.12$$

де F – місячний фонд робочого часу; $З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць; $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

Відповідно до пронумерованого вище списку загроз, можна розрахувати ймовірні збитки. Враховуючи той факт, що деякі загрози мають схожі наслідки, розрахунки будуть проводитись для одного випадку з групи подібних, але надалі буде враховуватись кількість можливих подій на рік та ймовірність їх виникнення.

Відповідно до переліку загроз, вказаного вище, для загроз №1, №5, №9, №10 збитки від реалізації однієї з цих загроз розраховуються за формулами 3.7–3.11:

$$П_п = 13000 \ грн \cdot 14 \ чол/212 \ год \cdot 3 \ год,$$

$$П_п = 2575{,}47 \ грн.$$

$$П_{ви} = 0 \ грн.$$

$$П_{зч} = 0 \ грн.$$

$$П_{пв} = 14000 \ грн/212 \ год \cdot 1 \ год,$$

$$П_в = 66{,}03 \ грн.$$

$$П_в = 0 \ грн + 66{,}03 \ грн + 0 \ грн,$$

$$П_в = 66{,}03 \text{ грн.}$$

$$V = 3001065 \text{ грн}/212 \text{ год} \cdot (3 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 56623{,}86 \text{ грн.}$$

І таким чином,

$$U = 2575{,}47 \text{ грн} + 66{,}03 \text{ грн} + 56623{,}86 \text{ грн},$$

$$U = 59264{,}5 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз №1, №5, №9 або №10 становитиме – 59264 грн 50 копійок.

Для загроз №2, №4, №6 потрібно враховувати не збитки, а розмір не одержаної вигоди від реалізації однієї з цих загроз. Експертним висновком розмір неодержаної вигоди визначені у розмірі – 90031,95 грн/місяць (3% від планового місячного прибутку підприємство не буде отримувати).

Оскільки загрози №8 та №12 мають схожі наслідки, розмір збитку від реалізації однієї з загроз буде таким самим і для іншої і буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн}/212 \text{ год} \cdot 24 \text{ год},$$

$$П_п = 1471{,}70 \text{ грн.}$$

$$П_{ви} = 0 \text{ грн.}$$

Враховуючи специфіку роботи підприємства, одним з найцінніших ресурсів компанії є робочі станції (ноутбуки), тому в якості показника $П_{зч}$ враховується вартість заміни ноутбука.

$$П_{зч} = 8000 \text{ грн.}$$

$$П_{пв} = 14000 \text{ грн}/212 \text{ год} \cdot 120 \text{ год},$$

$$П_в = 7924{,}52 \text{ грн.}$$

$$П_в = 0 \text{ грн} + 7924{,}52 \text{ грн} + 8000 \text{ грн},$$

$$П_в = 15924{,}52 \text{ грн.}$$

$$V = 1478 \text{ грн/212 год} \cdot (120 \text{ год} + 1 \text{ год} + 0 \text{ год}),$$

$$V = 823{,}58 \text{ грн.}$$

І таким чином,

$$U = 1471{,}70 \text{ грн} + 15924{,}52 \text{ грн} + 823{,}58 \text{ грн},$$

$$U = 18219{,}8 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загрози №8 становитиме – 18219 грн 80 копійок.

Оскільки загроз № 3, № 7 та №11 мають подібні наслідки, збиток від їх реалізації буде розраховуватись за формулами 3.7–3.11:

$$П_п = 13000 \text{ грн} \cdot 14 \text{ чол/212 год} \cdot 3 \text{ год},$$

$$П_п = 2575{,}47 \text{ грн.}$$

$$П_{ви} = 14000 \text{ грн/212 год} \cdot 3 \text{ год},$$

$$П_{ви} = 198{,}11 \text{ грн.}$$

$$П_{зч} = 0 \text{ грн.}$$

$$П_{пв} = 0 \text{ грн.}$$

$$П_в = 198{,}11 \text{ грн} + 0 \text{ грн} + 0 \text{ грн},$$

$$П_в = 198{,}11 \text{ грн.}$$

$$V = 3001065 \text{ грн/212 год} \cdot (3 \text{ год} + 3 \text{ год} + 0 \text{ год}),$$

$$V = 84935{,}80 \text{ грн.}$$

І таким чином,

$$U = 2575{,}47 \text{ грн} + 198{,}11 \text{ грн} + 84935{,}80 \text{ грн},$$

$$U = 87709{,}30 \text{ грн.}$$

Тобто, збиток від одноразової реалізації загроз № 3, № 7 або №11 становитиме – 87709 грн 30 копійок.

Таким чином, маючи дані про можливі збитки від реалізації загроз можна провести розрахунок збитків на рік від реалізації даних загроз. Зводні дані та кінцева величина збитку зазначені у таблиці 3.2:

Таблиця 3.2 – Розрахунок річних обсягів збитків від реалізації загроз

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Злам мережі, порушення нормального функціонування системи	59264,5	1	0,54	32002,83

Продовження таблиці 3.2

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Несанкціоноване ознайомлення з інформацією (співробітниками)	90031,95	1	0,3	27009,59
Несанкціонована модифікація/видалення інформації (співробітниками)	87709,30	2	0,3	52625,58
Несанкціоноване копіювання інформації на знімні носії (співробітниками)	90031,95	1	0,32	28810,22
Помилки персоналу, що дозволяють зловмисникам отримати доступ до системи	59264,5	1	0,70	41485,15

Несанкціоноване ознайомлення з інформацією конкурентами та зловмисниками	90031,95	1	0,5	45015,98
Злам слабких паролів, крадіжка паролів з метою проникнення у систему та завдання їй тієї чи іншої шкоди	59264,5	1	0,72	42670,44
Збої у функціонуванні системи, що призводять до втрати чи пошкодження інформації, що в ній циркулює	87709,30	1	0,36	31575,35

Продовження таблиці 3.2

Загроза	Збиток від одиничної реалізації загрози, грн	Передбачувана кількість реалізацій загрози на рік, шт	Вірогідність реалізації загрози	Річні збитки від реалізації загрози, грн
Відмова технічних засобів, яка призводить до зупинки у процесі функціонування системи	18219,8	1	0,36	6559,13
ЗАГАЛОМ				372581.72

Для розрахунку коефіцієнтів вірогідності були використані дані з таблиць 1.8 і 1.9, а саме – коефіцієнти К2, що відповідають за мотивацію джерела загрози і зручність використання вразливості відповідно. Рівні коефіцієнта К2 були відповідно змінені на часткову шкалу (1 – 0,2; 2 – 0,4; 3 – 0,6; 4 – 0,8; 5 – 1). На підставі коефіцієнтів К2 джерела і коефіцієнтів К2 вразливості експертним

шляхом були визначені коефіцієнти вірогідності реалізації зазначених вище загроз.

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

Загальний ефект від впровадження системи інформаційної безпеки розраховується за формулою :

$$E = B \cdot R - C \text{ грн}, \tag{3.13}$$

де B – загальний збиток від атаки на вузол корпоративної мережі, грн; R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці; C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Тож, економічний ефект становить:

$$E = 372581{,}72 \text{ грн} - 17150 \text{ грн},$$

$$E = 355431{,}72 \text{ грн}.$$

В загальному вигляді, оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

- сукупна вартість володіння (ТСО);
- коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);
- термін окупності капітальних інвестицій T_o.

У даному випадку ТСО не використовується, оскільки було визначено величину відверненого збитку.

ROSI, у свою чергу, показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки, розраховується за формулою 3.14:

$$ROSI = E / K, \tag{3.14}$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн; K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Тож,

$$ROSI = 372581,72 \text{ грн} / 9356 \text{ грн},$$

$$ROSI = 39,8.$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $E_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект вважається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта, розраховується за формулою 3.15:

$$\text{ROSI} > (N_{деп} - N_{інф}) / 100 \qquad (3.15)$$

де $N_{деп}$ = 19 – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %; $N_{інф}$ = 8 – річний рівень інфляції, %.

39,8 > 0,11, отже проект є економічно доцільним.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупаються за рахунок загального ефекту від впровадження системи інформаційної безпеки, розраховується за формулою 3.16:

$$T_o = E / K = 1 / ROSI = 0,025 \text{ року}. \qquad (3.16)$$

3.5 Висновок економічного розділу

В цьому розділі були проведені розрахунки капітальних та поточних витрат на введення та експлуатацію засобів захисту, що рекомендовані політикою безпеки.

В ході розрахунків було з’ясовано що введення в експлуатацію засобів та заходів захисту є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (0,025 року), а коефіцієнт ефективності перевищує

річний рівень прибутковості альтернативного варіанта (39,8 > 0,11). Тож, впровадження та використання обраних проектних рішень повністю доцільне.

ВИСНОВОК

Під час виконання кваліфікаційної роботи було виконано обстеження об'єкта інформаційної діяльності відповідно до порядку обстеження, описаному в НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Окрім цього було проведена класифікація інформації що циркулює в ІТС ТОВ «Сладко Дніпро» та яка підлягає захисту. Класифікація проводилась відповідно до положень ЗУ «Про інформацію», якими регламентується перелік інформації що може, або не може бути інформацією з обмеженим доступом.

Після визначення вхідних даних, була проведена класифікація існуючих в ІТС загроз та їх джерел, шляхом експертної оцінки з використанням рекомендацій, описаних у документі ISO/IEC TR 13335-3:1998. Окрім цього було визначено клас автоматизованої системи (відповідно до НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу») та оцінено існуючий стан захищеності, шляхом аналізу існуючого функціонального профілю, а також розроблено новий функціональний профіль (відповідно до НД ТЗІ 3.7-003 -2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»), що відповідає вимогам, необхідним для запобігання інцидентів ІБ.

На основі отриманих даних був розроблений комплекс рекомендацій, щодо підвищення стану захищеності ІТС ТОВ «Сладко Дніпро». Доцільність використання даних рекомендацій, в свою чергу, була обґрунтована у економічній частині кваліфікаційної роботи.

ПЕРЕЛІК ПОСИЛАНЬ

1 Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]: закон України редакції від 19.04.2014 № 1170-VII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр

2 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]: НД ТЗІ 3.7-003-05 від “8” листопада 2005 №125. – Режим доступу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074

3 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-004-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/

4 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 2.5-005-99 від 07.01.1999. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/

5 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 1.1-002-99 від 07.01.1999. – Режим доступу: www.dsszzi.gov.ua/dsszzi/

6 Експлуатацію систем інформаційної безпеки [Електронний ресурс] – Режим доступу: https://lektsii.org/15-1904.html

7 Рекомендації щодо захисту Active Directory: Частина 1. Бекап контролера домену [Електронний ресурс]. – 2016. – Режим доступу : https://www.veeam.com/blog/ru/backing-up-domain-controller-best-practices-for-adprotection.html.

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість аркушів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	Розділ 1. Стан питання. Постановка задачі	36	
6	А4	Розділ 2. Спеціальна частина	22	
7	А4	Розділ 3. Економічна частина	16	
8	А4	Висновок	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А. Відомість матеріалів дипломної роботи	1	
11	А4	Додаток Б. Перелік документів на оптичному носії	1	
12	А4	Додаток В. Відгук керівника економічного розділу	1	
13	А4	Додаток Г. Відгук керівника дипломної роботи	1	

ДОДАТОК Б. Перелік документів на оптичному носії

– Романюк Е.О. 125-18-3.docx
– Романюк Е.О. 125-18-3.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

«Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «Сладко Дніпро»

студента групи 125-18-3 Романюка Едуарда Олександровича

Кваліфікаційна робота за спеціальністю «6.170103 Управління інформаційною безпекою» Романюка Е.О. представлена пояснювальною запискою на 90 с., 9 рис., 14 табл., 4 додатка, 7 джерел.

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

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

У економічному розділі були розраховані витрати на впровадження політики безпеки та доцільність проектних рішень

До недоліків проекту слід віднести окремі незначні невідповідності вимогам оформлення.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки "добре", а Романюк Едуард Олександрович присвоєння йому кваліфікації "фахівець з організації інформаційної безпеки" освітньо-кваліфікаційного рівня "бакалавр".

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.