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 *Шайдулова Євгенія Сергійовича*

академічної групи *125-16-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підприємства "Websofttonic"*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф Корнієнко В.І.			
розділів:				
спеціальний	ас. Ковальова Ю.В			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Шайдулову Євгенію Сергійовичу*** **академічної групи** ***125-16-2***
(прізвище ім'я по-батькові) (шифр)

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

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підриємства "Websofttonic"*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 26.05.20 №275-с

Розділ	Зміст	Термін виконання
Розділ 1	Загальний опис діяльності підприємства, аналіз нормативно правових документів.	29.03.2020
Розділ 2	Технічне обстеження, аналіз інформаційної системи підприємства	24.05.2020
Розділ 3	Розрахунки на реалізацію проекту	04.06.2020

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

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

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

РЕФЕРАТ

Пояснювальна записка: 72 сторінки, 7 рисунків, 16 таблиць, 4 додатка, 14 джерел.

Об'єкт дослідження: інформаційне поле комерційної структури «WebSofttonic»

Мета: визначення необхідності реалізації комплексу систем захисту інформації для підприємства, аналіз інформаційного поля компанії і розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

Методи розробки: спостереження, обстеження, аналіз, опис та розрахунки.

Робота містить 3 розділи і 11 підрозділів.

Перший розділ являє собою обстеження діяльності підприємства, дослідження нормативно-правової бази компанії та її простеження інформаційного простору і встановлення необхідності реалізації КСЗІ на даному підприємстві.

Другий розділ обґрунтовує технічну частину даної роботи. Створення актів та документів пов'язаних із аналізом інформаційного поля компанії, розробка КСЗІ.

Третій розділ представляє собою економічну частину діяльності підприємства, розрахунки витрат на реалізацію проекту, прорахунок поточних та капітальних витрат, надання рекомендацій стосовно зниженню витрат на реалізацію проекту.

По кожному розділу зроблено висновок і загальні підсумки стосовно всієї виконаної роботи.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, НОРМАТИВНО-ПРАВОВА БАЗА, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ.

РЕФЕРАТ

Пояснительная записка: 72 страницы, 7 рисунков, 16 таблиц, 14 приложений, 9 источников.

Объект исследования: Информационное поле коммерческой структуры «WebSofttonic»

Цель: Постановка задачи целесообразности реализации комплекса систем защиты информации на предприятии, анализ информационного поля компании и разработка механизмов защиты в сфере информационной безопасности организации, расчет затрат на реализацию проекта.

Методы разработки: наблюдение, обследование, анализ, описание, расчеты

Работа содержит 3 раздела и 11 подразделов.

Первый раздел представляет собой обследование деятельности предприятия, исследование нормативно-правовой базы компании, анализ информационного пространства и установление необходимости реализации КСЗИ на данного предприятия.

Второй раздел обосновывает техническую часть данной работы. Создание актов и документов связанных с анализом информационного поля компании, разработка КСЗИ.

Третий раздел представляет собой экономическую часть деятельности предприятия, расчеты затрат на реализацию проекта, просчет постоянных и капитальных расходов, предоставление рекомендаций относительно снижений затрат на реализацию проекта.

По каждому разделу сделано выводы и общие итоги в отношении всей выполненной работы.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КОМПЛЕКС СРЕДСТВ ЗАЩИТЫ, НОРМАТИВНО-ПРАВОВАЯ БАЗА, ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ

ABSTRACT

Explanatory Note: 72 pages, 7 drawings, 16 tables, 4 applications, 14 sources.

Object of study: Information field of the commercial structure "WebSofttonic"

Purpose: The goal of the feasibility of implementing a set of information security systems at the enterprise, the analysis of the company's information field and the development of protection mechanisms in the field of information security of the organization, the calculation of the costs of the project.

Development methods: observation, examination, analysis, description, calculations

The work contains 3 sections and 11 subsections.

The first section is a survey of the activities of the enterprise, a study of the regulatory framework of the company, an analysis of the information space and the establishment of the need to implement of the security systems in this enterprise.

The second section substantiates the technical part of this work. Creation of acts and documents related to the analysis of the information field of the company, development of the security systems.

The third section is the economic part of the enterprise, the calculation of costs for the implementation of the project, the calculation of fixed and capital costs, the provision of recommendations on reducing costs for the implementation of the project.

Conclusions and general results were made for each section in relation to all the work done.

INFORMATION SECURITY, COMPLEX OF MEANS OF PROTECTION, REGULATORY LEGAL FRAMEWORK, TECHNICAL MEANS OF PROTECTION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС — автоматизована система;

АТС – Автоматична телефонна станція

ДВ — відновлення після збоїв;

ДВ — стійкість до відмов;

ДЗ — гаряча заміна;

ДР — використання ресурсів;

ДТЗС - допоміжні технічні засоби та системи

ЗУ – Закон(-и) України

ІЗоД – Інформація з обмеженим доступом

ІР – інформаційні ресурси

ІС – інформаційна система

ІТС – Інформаційно-телекомунікаційна система

КА — адміністративна конфіденційність;

КВ — конфіденційність при обміні;

КД — довірча конфіденційність;

КЗ – контрольована зона

КЗЗ — комплекс засобів захисту;

КК — аналіз прихованих каналів;

КО — повторне використання об'єктів;

КС — комп'ютерна система;

НА — автентифікація відправника;

НВ — автентифікація при обміні;

НИ — ідентифікація і автентифікація;

НК — достовірний канал;

НО — розподіл обов'язків;

НП — автентифікація одержувача.

НПБ – нормативно-правова база

НР — реєстрація;

НСД — несанкціонований доступ;

НТ — самотестування;

НЦ — цілісність КЗЗ;

ОІД – Об’єкт інформаційної діяльності

ОС — обчислювальна система;

ПЕМВН – побічні електромагнітні випромінювання та наводки

ПЗ — програмне забезпечення;

ПЗ – програмне забезпечення

ПЗП — постійний запам’ятовуючий пристрій;

ПРД — правила розмежування доступу;

ЦА — адміністративна цілісність;

ЦВ — цілісність при обміні;

ЦД — довірча цілісність;

ЦО — відкат;

ЗМІСТ

ВСТУП

На сьогоднішній день задача підтримки достатнього рівня безпеки інформації на підприємстві являється однією з найважливіших. Оскільки галузь інформаційних технологій стрімко розвивається, абсолютна більшість підприємств використовують ІТС, з'являється все більше спеціалістів у цій сфері, а з ними і зловмисників.

Постійне вдосконалення комплексної системи безпеки інформації вигідне, як самому підприємству, так і його клієнтам. Оскільки викрадення, знищення або модифікація інформації може завдати значних репутаційних та фінансових збитків компанії та її клієнтам.

У більшості держав існують органи, які займаються питаннями безпеки інформації. Дані структури розробляють стандарти, закони та правила, які покращують життєдіяльність підприємств, суспільства та інших галузей які впливають на різні чинники життєздатності держави та її ресурсів.

У наступних розділах буде оглянуто організацію «Websofttonic», її життєдіяльність з точки зору підприємства, встановлено необхідність реалізації КСЗІ для ІТС даної компанії, виконано розрахунки на реалізацію КСЗІ виходячи із обстеження підприємства та зроблено висновки стосовно даної роботи.

У роботі було частково змінено інформацію, проте змінені дані на достовірність роботи не впливають

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про підприємство

Підприємство «Websofttonic» займається ремонтом та модернізацією механічних елементів для комп'ютерів, розробкою програмного забезпечення для невеликих за обсягом компаній. Організація почала вести власну діяльність з 2018 року. За 2 роки ведення власної діяльності було створенно приблизно 30-50 проектів в сфері інформаційних технологій. Головний офіс знаходиться у м. Дніпро за адресою Калнишевського 19а.

Працівники являють собою ключовий ресурс для продуктивності будь-яких компаній і реалізації певних проектів, продукції, тощо. Нижче буде надано таблицю, про загальний обсяг робітників даного підприємства:

Таблиця 1.1 - Штат працівників підприємства

Посада	Кількість працівників на посаді	Рівень кваліфікації
Директор	1	Високо-кваліфіковані робітники
Системний адміністратор	1	Високо-кваліфіковані робітники
Дизайнер	3	Кваліфіковані робітники
Програміст	3	Кваліфіковані робітники
Бухгалтер	1	Кваліфіковані робітники
Секретар	1	Не кваліфіковані робітники

Проте будь-яка компанія потребує переліку документів, які затверджені державним законодавством, котрі впливають та керують діяльністю організації.

У наступному підрозділі буде обстежено нормативно-правову базу підприємства, проведено аналіз нормативних документів і виходячи із пунктів, зроблено висновки стосовно необхідності КСЗІ для даної організації.

1.2 Нормативно-правова база підприємства

Згідно із ДСТУ 2732:2004 «Діловодство і архівна справа. Терміни та визначення»:

«Нормативно правова база – це обгрунтування, на державному рівні, діяльності будь-якого підприємства, незалежно від форми власності, сфери діяльності та масштабу. Діяльність всіх організацій / підприємств / установ завжди спирається на законодавство країни і на нормативні акти, які регулюють діяльність в певній сфері»

Виходячи із вищеописаного терміну, можна сказати, що нормативно правова база з точки зору діяльності підприємства, являє собою перелік нормативних документів, які керують комерційними чинниками компанії.

Обсяг та перелік даних документів залежить від діяльності організації, сфери галузі розробки продукції компанії, нормативної поведінки в залежності від встановлених державних законів, тощо.

Для ознайомлення з діяльністю підприємства було оглянуто перелік документів, які складають нормативно-правову базу підприємства. Було досліджено такі документи як:

- Трудовий договір;
- Журнал обліку пожежної безпеки;
- Журнал обліку технічної безпеки;
- Договір медичного страхування;
- Документ, що свідчить про комерційну таємницю підприємства.

1.3 Акт обстеження

Акт обстеження представляє собою документ аналітичного характеру, де описана інформація про ІТС підприємства. Формально, документ можна розподілити на декілька етапів:

1. Обстеження об’єктів фізичного характеру;
2. Аналіз програмно-апаратних ресурсів ІТС;
3. Дослідження профілю захищеності ІТС.

Характеристика об’єктів, де розташовані компоненти ІТС

Об’єктом інформаційної діяльності (ОІД) є приміщення товариства з обмеженою відповідальністю (ТОВ) «Websofttonic». Область діяльності – створення програмних продуктів.

ОІД знаходиться за адресою: Україна, м. Дніпро, вул. Калнишевського 19а, офіс № 4. Будівля, в якій знаходиться ОІД, що обстежується, має три поверхи і збудована з цегли та бетонних конструкцій. Прикладається ситуаційний план ОІД (Рисунок 1.1).

Навколо будівлі, де знаходиться ОІД, розміщені такі об’єкти: на півночі знаходяться 9-ти поверхова та 5-ти поверхова будівлі, а також 3 поверховий дитячий садок, на півдні знаходяться три 5-ти поверхових будівлі, на заході до будівлі знаходиться школа корпуси якої мають 3 та 1 поверхи, на сході знаходиться адміністративна будівля. Увесь список будівель та споруд в таблиці 1.2.

На території ІТС проходять такі системи комунікацій: лінії систем електропостачання, комп’ютерної мережі, телефонного зв’язку, пожежної та охоронної сигналізації, та системи водопостачання, опалення. На території офісного комплексу є два КПП з охороною, один з яких автомобільний. У робочий час будівля частково загальнодоступна, у неробочий час, вихідні та святкові дні допуск співробітників на об'єкт обмежений і проводитися за попередніми заявками від керівників підрозділів. У працівників є спеціальні ідентифікаційні картки, за якими здійснюється пропуск на територію офісного комплексу.

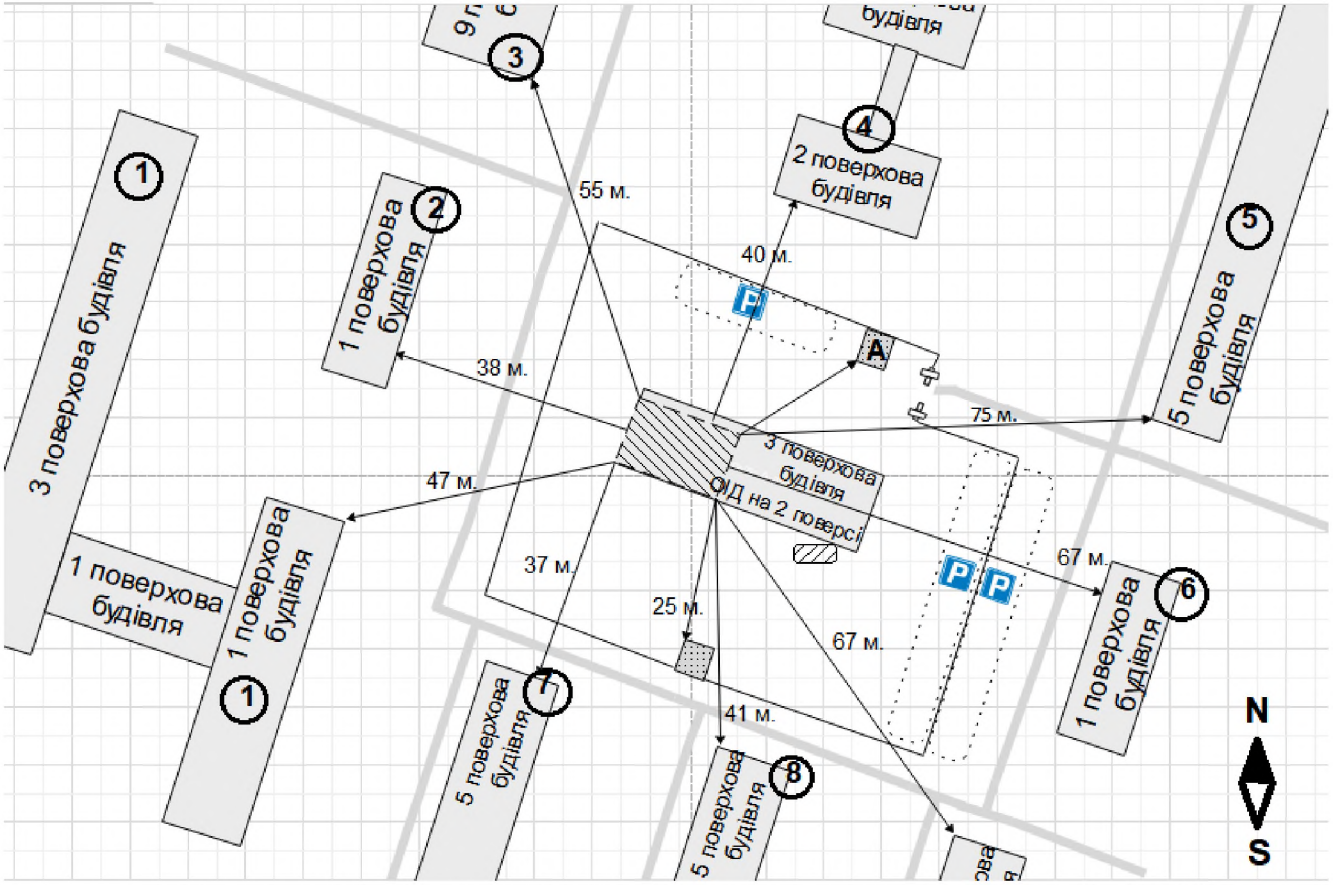


Рисунок 1.1 - Ситуаційний план підприємства у масштабі 1:1000 з умовними позначеннями

Умовні позначення

Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
Школа	3	вул. Богдана Хмельницького, 15	47
Хоз. Корпус при школі	1	вул. Богдана Хмельницького, 15	38
Житловий комплекс	9	вул. Богдана Хмельницького, 11а	55
Дит. садок	2	вул. Калнишевського, 68	40
Житловий будинок	5	вул. Калнишевського, 66	75
Адміністр. будівля	1	вул. Калнишевського, 70а	67
Житловий будинок	5	вул. Калнишевського, 17	37
Житловий будинок	5	вул. Калнишевського, 19	41

Таблиця 1.2 - Характеристика будівель та споруд

Опис фізичного середовища ОІД

ОІД, що обстежується, знаходиться на другому поверсі, стіни ОІД зроблені з цегли, товщина стін 25 см.; підлога та стеля є бетонні конструкції близько 10-12 см.; підвісна стеля зроблена з металу та пластику; ОІД має один вхід\вихід, на якому встановлені захисні металеві двері товщиною 75 мм. з кодовим замком; в ОІД 6 дверних міжкімнатних отворів, на 5 встановлені дерев'яні двері товщиною 30 мм. з засувним механізмом; до кабінету системного адміністратора встановлені захисні металеві двері товщиною 75 мм. з кодовим замком; в приміщені 7 віконних отвори, товщина вікна 24 мм.,

складаються с склопакету, металу та пластику.

На ОІД з західної та північної сторони має віконні отвори. З південної сторони знаходиться сусіднє приміщення, яке належить іншій організації. Приміщення має цегляні стіни товщиною 24 см., підлога та стеля є бетонні конструкції близько 10-12 см., підвісна стеля зроблена з металу та пластику,

приміщення має один вхід\вихід, на якому встановлені захисні металеві двері товщиною 75 мм. з кодовим замком.

На ОІД є такі лінії систем комунікацій: електропостачання, освітлення (Рисунок 1.2), водопостачання, опалення, вентиляція (Рисунок 1.3), телефонного зв'язку та комп'ютерної мережі (Рисунок 1.4), пожежна та охоронна сигналізації (Рисунок 1.5). Розетки мають паралельне з'єднання та підключається до електричної щитової офісу, що в свою чергу підключена до щитової на поверсі з міжповерховим переходом.

За межі ОІД, виходить лінії систем водопостачання, опалення, електроживлення та Інтернету.

На ОІД використовуються стаціонарні комп'ютери, ноутбуки, маршрутизатор, комутатор, сервер, офісна АТС, принтери та факси, повний список ресурсів приведений в таблиці 1.3 інвентаризаційна відомість апаратного забезпечення ІТС (Рисунок 1.7). Використовуються системи пожежної та охоронної сигналізації, список приведений в таблиці 1.4 інвентаризаційна відомість ДТЗС. Повна характеристика складу ІТС приведена в таблиці 1.5. На ОІД використовуються системні, прикладні та спеціальні програмні забезпечення, детальний опис в таблиці 1.6 інвентаризаційна відомість програмного забезпечення ІТС.

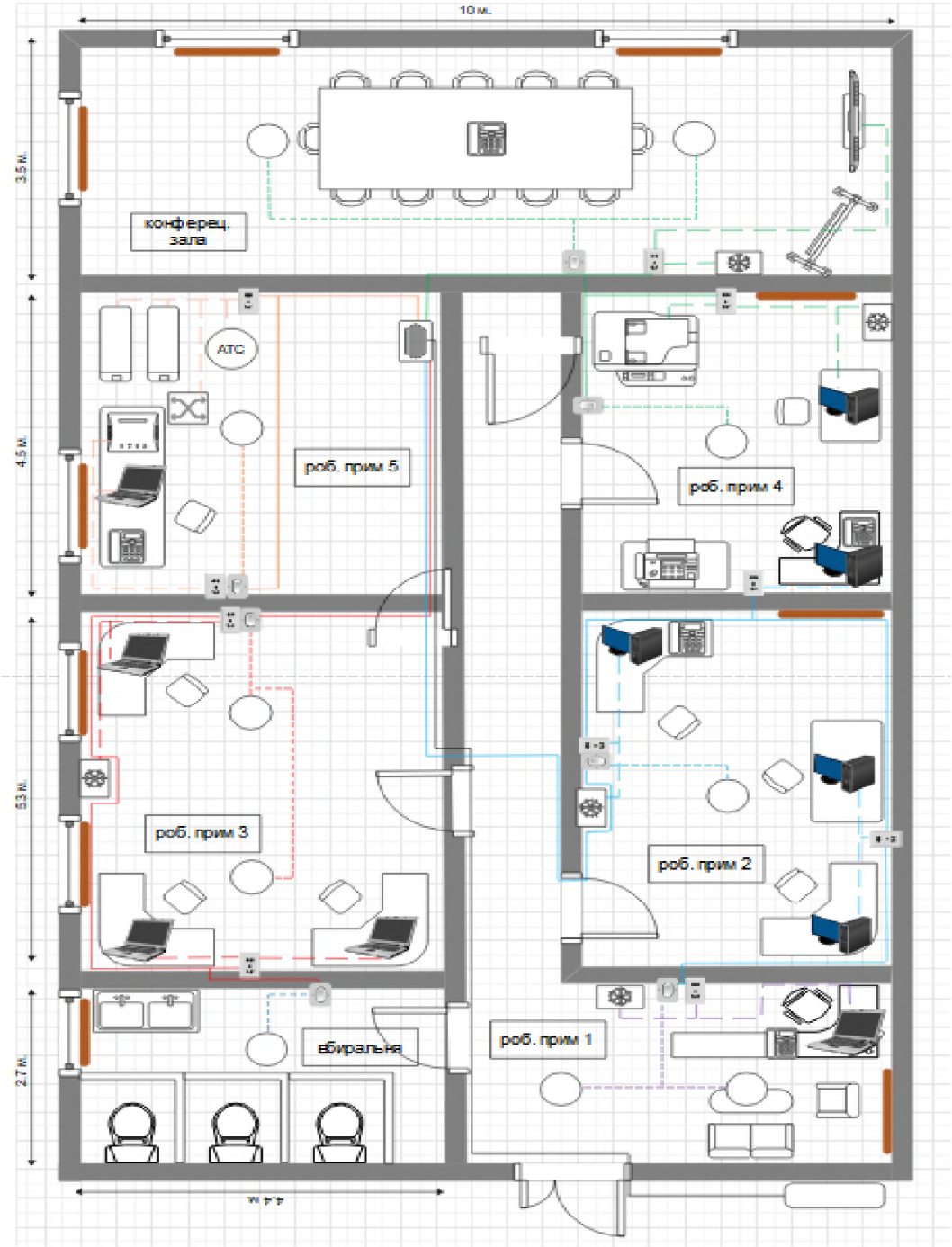


Рисунок 1.2 - Генеральний план. Лінії системи електропостачання та освітлення

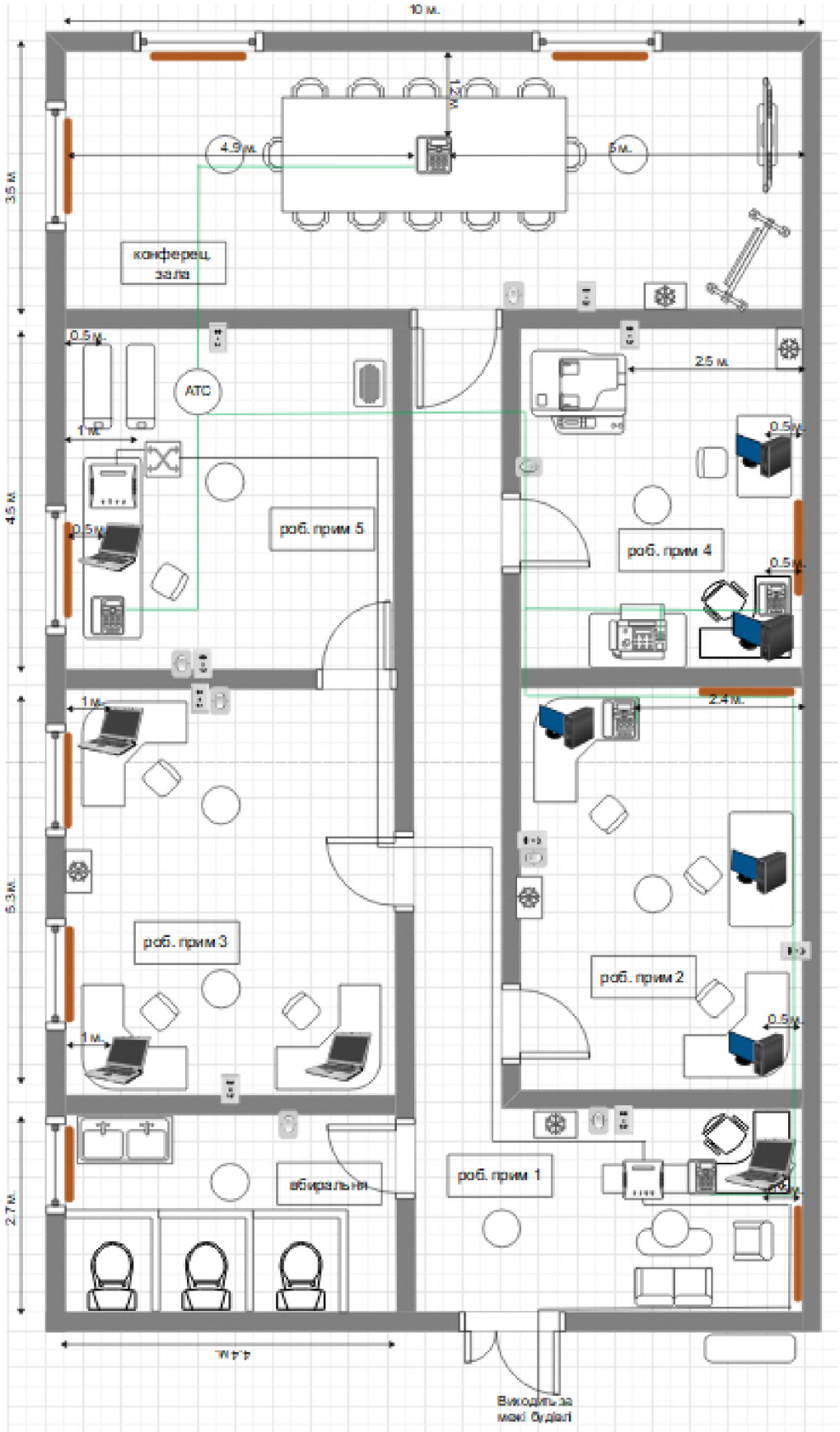


Рисунок 1.3 - Генеральний план. Лінії системи комп’ютерної мережі та телефонного зв’язку

Загальні позначення:


— робочий ПК


— робочий телефон


— електрична щитова офісу


— робочий ноутбук


— роутер


— розетка


— факс


— сервер


— вимикач системи освітлення

Лінії систем комп'ютерної мережі та телефону:

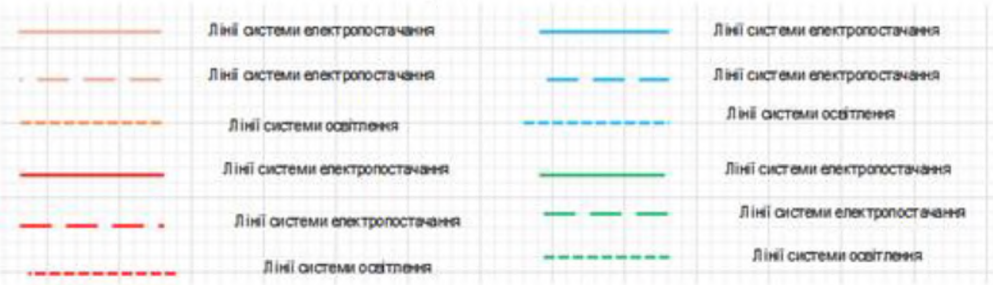
— лінія системи офісної АТС

— лінія системи комп'ютерної мережі

— відстань до границі ОІД

Лінії си

— лінія з'єднання офісної щитової до міжповерхової



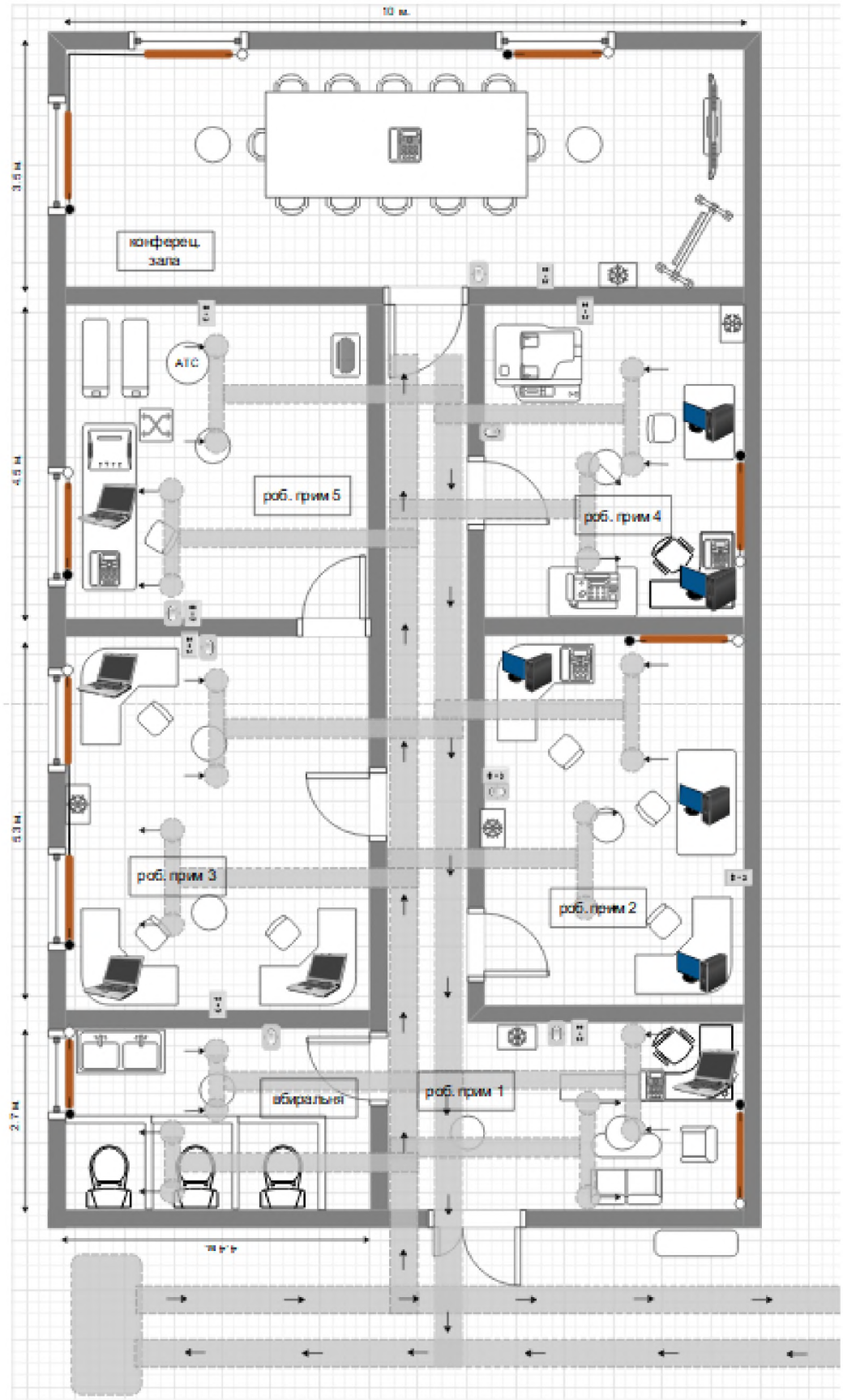


Рисунок 1.4 - Генеральний план. Системи опалення та вентиляції

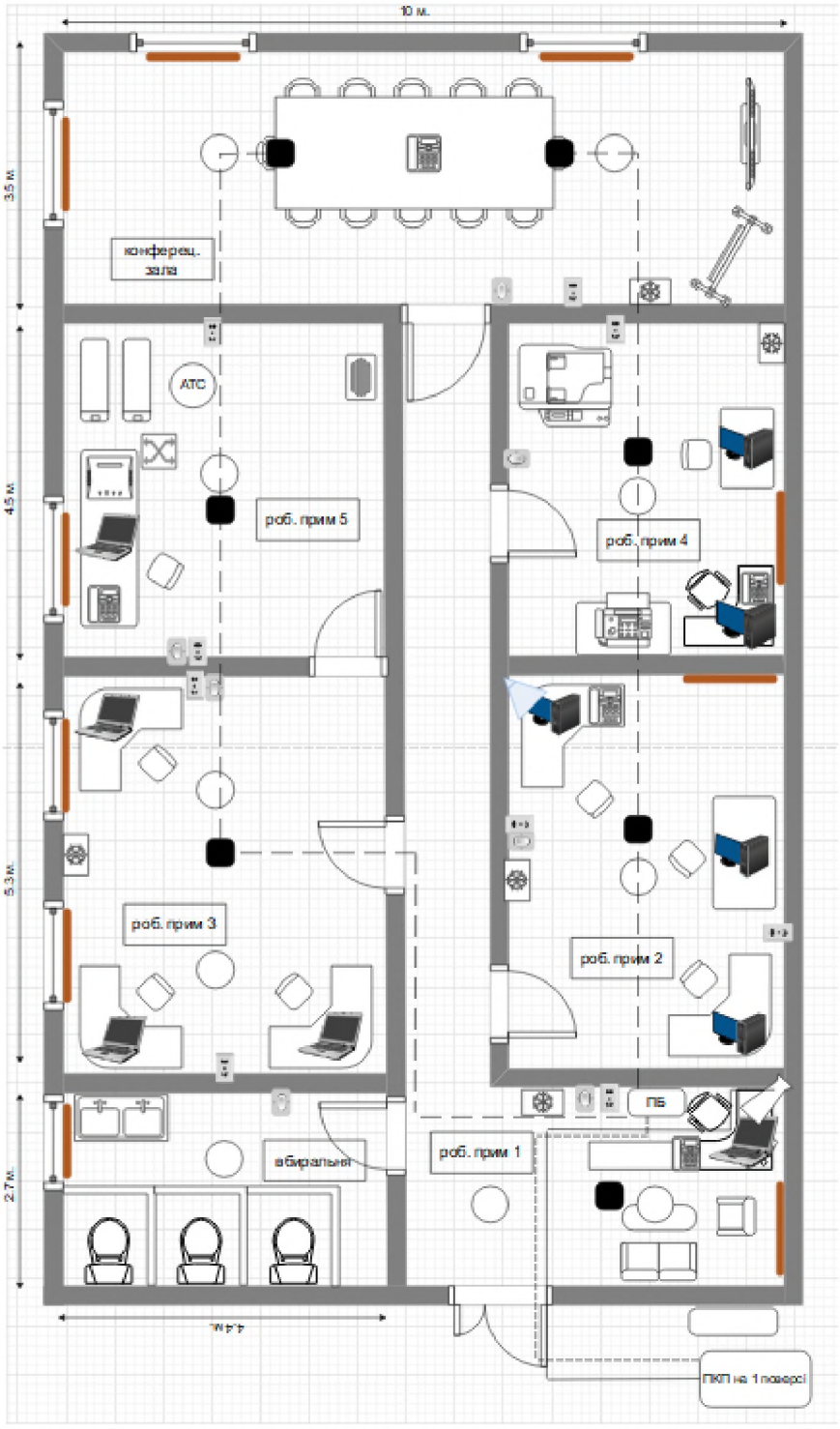
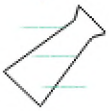


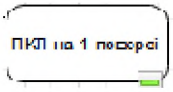
Рисунок 1.5 - Генеральний план. Лінії системи охоронної та пожежної сигналізації

Лінії систем охоронної та пожежної сигналізації:

— датчик диму



— камера відео-спостереження



ПКП на 1 поверсі

ПБ — периферійний блок

— — — — — — система ліній пожежної сигналізації

——————— — система ліній камери відеоспостереження

..... — лінія з'єднання ПБ с ПКП

Лінії системи вентиляції та опалення:

— шахта вентиляції

— напрям руху повітря

— повітря-забірник

— батарея опалення

— витяжна вентиляція

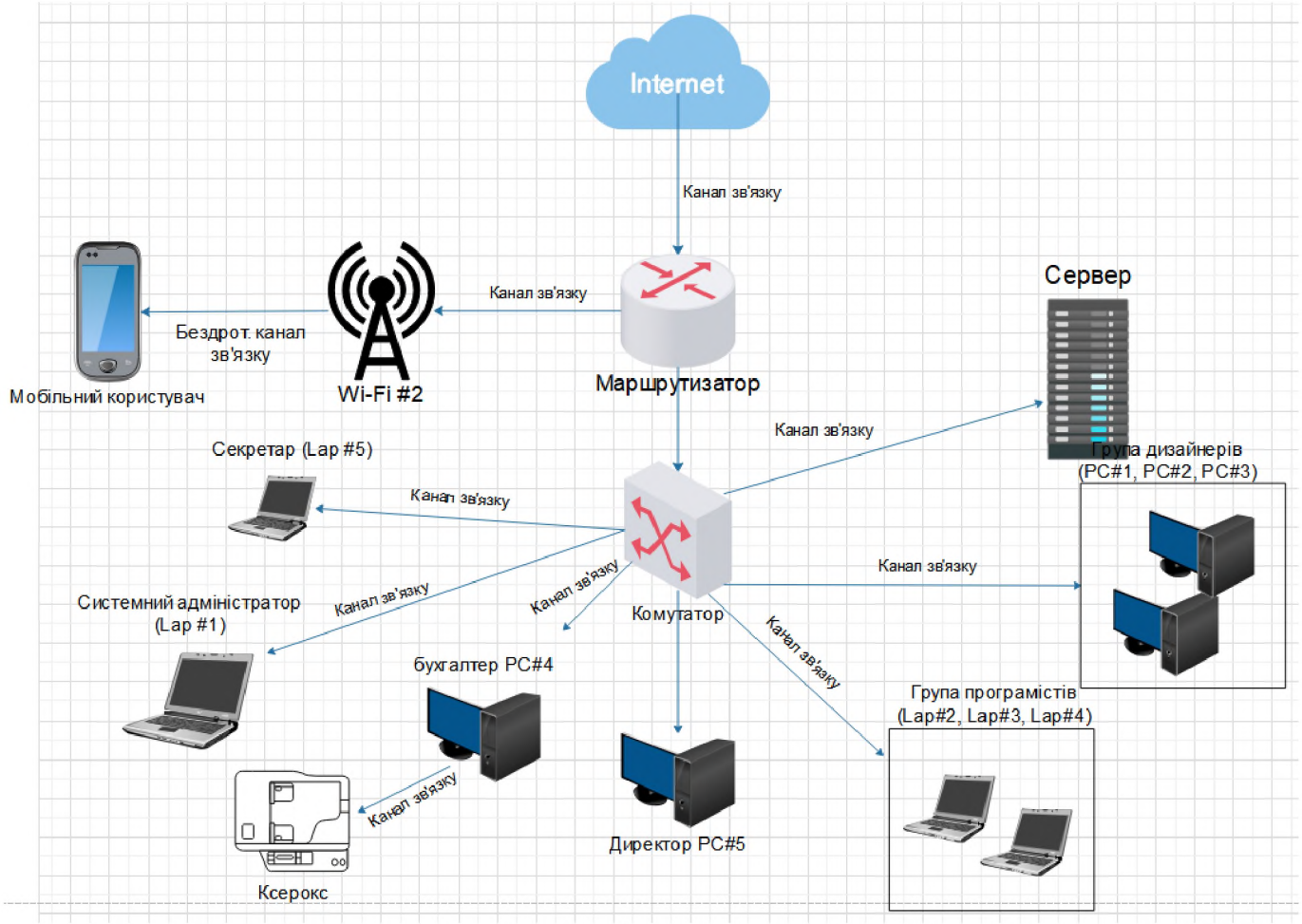


Рисунок 1.6 - Структурна схема ІТС

Таблиця 1.3 - Інвентаризаційна відомість апаратного забезпечення ІТС

Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
PCмонітор	Samsung	S27F358F	73252	Роб. Прим. 4 на столі	0.5
PC монітор	Samsung	S27F358F	65478	Роб. Прим. 4 на столі	0.5
PC монітор	Acer	HA220Qbid	16546	Роб. Прим. 2 на столі	3
PC монітор	Acer	HA220Qbid	87538	Роб. Прим. 2 на столі	0.5
PC монітор	Acer	HA220Qbid	63425	Роб. Прим. 2 на столі	0.5
PC блок	—	—	73809	Роб. Прим. 4 на підлозі	0.5

Продовження таблиці 1.3

Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
PC блок	—	—	98525	Роб. Прим. 4 на підлозі	0.5
PC блок	—	—	27563	Роб. Прим. 2 на підлозі	3
PC блок	—	—	06743	Роб. Прим. 2 на підлозі	0.5
PC блок	—	—	21755	Роб. Прим. 2 на підлозі	0.5
PC Клавіатура	Logitech	K280e USB	74421	Роб. Прим. 4 на столі	0.5
PC Клавіатура	Logitech	K280e USB	92379	Роб. Прим. 4 на столі	0.5
PC Клавіатура	Logitech	K280e USB	15515	Роб. Прим. 2 на столі	3
PC Клавіатура	Logitech	K280e USB	96041	Роб. Прим. 2 на столі	0.5
PC Клавіатура	Logitech	K280e USB	00490	Роб. Прим. 2 на столі	0.5
PC миш	Logitech	B100 USB	66267	Роб. Прим. 4 на столі	0.5
PC миш	Logitech	B100 USB	90543	Роб. Прим. 4 на столі	0.5
PC миш	Logitech	B100 USB	04274	Роб. Прим. 2 на столі	3
PC миш	Logitech	B100 USB	43115	Роб. Прим. 2 на столі	0.5
PC миш	Logitech	B100 USB	32896	Роб. Прим. 2 на столі	0.5
Ноутбук	Asus	X550VC	24672	Роб. Прим. 5 на столі	0.5
Ноутбук	Lenovo	330S-15IKB	78464	Роб. Прим. 3 на столі	1
Ноутбук	Lenovo	330S-15IKB	45243	Роб. Прим. 3 на столі	1
Ноутбук	Lenovo	330S-15IKB	46237	Роб. Прим. 3 на столі	2.8

Продовження таблиці 1.3

Назва	Марка	Модель	Серійний номер	Розміщення	Відстань до границі ОІД, м
Ноутбук	Asus	X550VC	24653	Роб. Прим. 1 на столі	0.5
Комутатор	D-Link	DGS-1026MP	15385	Роб. Прим. 3 на підлозі	1
Сервер	Dell	T40V14	67934	Роб. Прим. 5 на підлозі	0.5
Wi-Fi Роутер	TP-Link	Archer A7	19275	Роб. Прим. 5 на столі	1
Wi-Fi роутер	TP-Link	Archer A6	08737	Роб. Прим. 1 на столі	2
АТС	Panasonic	KX-TES824	87773	Роб. Прим. 5 на підлозі	2
Ксерокс	Canon	I-SENSYS MF112	00347	Роб. Прим. 4 на підлозі	2.5
Телефон	Panasonic	KX-DT521	18118	Конференц. зала на столі	1.2
Телефон	Panasonic	KX-DT521	35003	Роб. Прим. 5 на столі	0.5
Телефон	Panasonic	KX-DT521	25567	Роб. Прим. 4 на столі	0.5
Телефон	Panasonic	KX-DT521	25893	Роб. Прим. 2 на столі	2.4
Телефон	Panasonic	KX-DT521	37891	Роб. Прим. 1 на столі	1.4

Таблиця 1.4 - Інвентаризаційна відомість ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Камера відеоспостереження	GreenVision	LP4016	34535	Роб. Прим. 1 , на стелі в куту
Датчик диму	Артон	СПД-3.4	45784	Конференц. зала , на стелі
Датчик диму	Артон	СПД-3.4	04468	Конференц. зала , на стелі
Датчик диму	Артон	СПД-3.4	24506	Роб. Прим. 5, на стелі
Датчик диму	Артон	СПД-3.4	00655	Роб. Прим. 4, на стелі
Датчик диму	Артон	СПД-3.4	22406	Роб. Прим. 3, на стелі

Продовження таблиці 1.4

Назва	Марка	Модель	Серійний номер	Розміщення
Датчик диму	Артон	СПД-3.4	16853	Роб. Прим. 2, на стелі
Датчик диму	Артон	СПД-3.4	03244	Роб. Прим. 1, на стелі
Периферійний блок	Артон	-	26732	Роб. Прим. 1 , на стелі в куту
ПКП	Орион	4И.3.2	15064	Перший поверх

Таблиця 1.5 - Характеристика складу ІТС

Назва	Назва в ІТС	Характеристика	Серійний номер	Відповідальний
Робоча станція	PC#1	Процесор: IntelCore i5-9400F 2.9GHz / 8GT / 9MB/95Вт Материнська плата: AsusPrime1151 / 4 x DDR4 Відеокарта: Asus GeForce GTX 1650 S / 4GB / 128bit Жорсткий диск: WesternDigital 1TB Оперативна пам'ять: HyperX DDR4-3200 / 16384MB	63722 73110 84326 77649	Дизайнер
Робоча станція	PC#2	Процесор: IntelCore i5-9400F 2.9GHz / 8GT / 9MB/95Вт Материнська плата: AsusPrime1151 / 4 x DDR4 Відеокарта: Asus GeForce GTX 1650 Super 4GB / 128bit Жорсткий диск: WesternDigital 1TB Оперативна пам'ять: HyperX DDR4-3200 / 16384MB	28573 92877 34091 49002	Дизайнер
Робоча станція	PC#3	Процесор: IntelCore i5-9400F 2.9GHz / 8GT / 9MB/95Вт Материнська плата: AsusPrime1151 / 4 x DDR4 Відеокарта: Asus GeForce GTX 1650 Super 4GB / 128bit Жорсткий диск: WesternDigital 1TB Оперативна пам'ять: HyperX DDR4-2666 / 8192MB	37528 68275 93703 15738 97332	Дизайнер

Продовження таблиці 1.5

Назва	Назва в ІТС	Характеристика	Серійний номер	Відповідальний
Робоча станція	PC#4	Процесор: IntelCore i3-9100F 3.6GHz / 8GT / 6MB / 80Вт Материнська плата: AsusPrime1151 / 2 x DDR4 Жорсткий диск: WesternDigital 500GB Оперативна пам'ять: HyperX DDR4-2666/8192MB	63370 86054 71894 62803	Бухгалтер
Робоча станція	PC#5	Процесор: IntelCore i3-9100F 3.6GHz / 8GT / 6MB / 80Вт Материнська плата: AsusPrime1151 / 2 x DDR4 Жорсткий диск: WesternDigital 500GB Оперативна пам'ять: HyperX DDR4-2666 / 8192MB	77858 96042 21532 92671	Директор
Ноутбук	Lap#1	Екран 15.6" (1366x768) HD LED, глянцевий / IntelCore i7-7700M (3.8 ГГц) / RAM 16 ГБ / HDD 1 ТБ GeForce GT 950M, 2 ГБ LAN / Wi-Fi / Bluetooth веб-камера / 2.3 кг	37580	Системний адміністратор
Ноутбук	Lap#2	Екран 15.6" (1920x1080) Full HD, глянцевий з антибликовим покриттям / IntelCore i5-8250U (1.6 - 3.4 ГГц) / RAM 8 ГБ HDD 1 ТБ / AMD Radeon 540, 4 ГБ Wi-Fi / Bluetooth / веб-камера 1.87 кг	27766	Програміст
Ноутбук	Lap#3	Екран 15.6" (1920x1080) Full HD, глянцевий з антибликовим Покриттям / IntelCore i5-8250U (1.6 - 3.4 ГГц) / RAM 8 ГБ HDD 1 ТБ / AMD Radeon 540, 4 ГБ Wi-Fi / Bluetooth / веб-камера 1.87 кг	79533	Програміст

Продовження таблиці 1.5

Назва	Назва в ІТС	Характеристика	Серійний номер	Відповідальний
Ноутбук	Lap#4	Екран 15.6" (1920x1080) Full HD, глянцевий з антибликовим Покриттям / IntelCore i5-8250U (1.6 - 3.4 ГГц) / RAM 8 ГБ HDD 1 ТБ / AMD Radeon 540, 4 ГБ Wi-Fi / Bluetooth / веб-камера 1.87 кг	25748	Програміст
Ноутбук	Lap#5	Екран 15.6" (1920x1080) Full HD, глянцевий з антибликовим покриттям / IntelCore i5-8250U (1.6 - 3.4 ГГц) / RAM 8 ГБ HDD 1 ТБ / AMD Radeon 540, 4 ГБ / Wi-Fi / Bluetooth веб-камера / 1.87 кг	57391	Секретар
Комутатор	Commutator	1 Гбит / Ethernet 49.4 дБА / 370 Вт	98051	Системний адміністратор
Сервер	Server	IntelXeon (3.7 - 5.0 ГГц) 64 ГБ / 8GT / HDD: 2 x 2 ТБ / SSD: 2 x 500 ГБ Samsung	67374	Системний адміністратор
Wi-Fi Роутер	WiFi#1	1750 Мбит / 2.4 ГГц - 5 ГГц / VPN / Захист від DoS-атак Мережевий екран SPI	34675	Системний адміністратор
Wi-Fi Роутер	WiFi#2	1317 Мбит / 2.4 ГГц - 5 ГГц / VPN / Захист від DoS-атак Мережевий екран SPI	66545	Системний адміністратор
АТС	АТЕ	4 з'єднувальних елементи 20 Гц/25 Гц / 3,5 кг	79065	Системний адміністратор
Ксерокс	Ксерокс	Лазерний друк / 2400x600 dpi 910 Вт / 9 кг	15436	Бухгалтер

Таблиця 1.6 - Інвентаризаційна відомість програмного забезпечення ІТС

Назва	Тип	Опис	Тип ліцензії	Встановлено
Windows 10 (версія 1909)	Системне	Операційна система для персональних комп'ютерів і робочих станцій	Commercial	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5

Продовження таблиці 1.6

Назва	Тип	Опис	Тип ліцензії	Встановлено
Linux (Ubuntu 19.10)	Системне	Сімейство Unix-подібних операційних систем на базі ядра Linux	Freeware	Lap#1, Lap#2, Lap#3, Lap#4
WinRar (версія 5.80)	Системне	Архіватор файлів	Shareware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
ESET File Security (версія 7.1.12008)	Системне	Антивірусна програма	Commercial	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Драйвера (Nvidia 442.19)	Системне	ПЗ, за допомогою якого операційна система отримує доступ до приладу апаратного забезпечення	Freeware	PC#1, PC#2, PC#3, Lap#1
Microsoft Word (версія 2018)	Прикладне	Програми для створення, редагування та оформлення текстових документів	Commercial	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4
Microsoft PowerPoint (версія 2018)	Прикладне	Програми створення та показу наборів слайдів	Commercial	PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4
Microsoft Excel (версія 2018)	Прикладне	Програми, що дозволяють виконувати операції над даними, представленими в табличній формі	Commercial	PC#4, PC#5, Lap#1, Lap#5
Microsoft Access (версія 2018)	Прикладне	Засобив ведення, пошуку, розміщення і видачі великих масивів даних	Не ліцензійне	PC#4, PC#5, Lap#1

Продовження таблиці 1.6

Назва	Тип	Опис	Тип ліцензії	Встановлено
Microsoft Project (версія 2018)	Прикладне	Програма управління проектами	Не ліцензійне	PC#4, PC#5, Lap#1
Adobe Photoshop (версія CC 2017)	Прикладне	Засоби створення нерухомих і рухомих зображень	Commercial	PC#1, PC#2, PC#3
CorelDraw (версія 2018)	Прикладне	Засоби створення нерухомих і рухомих зображень	OpenSource	PC#1, PC#2, PC#3
Adobe After Effects (версія CC 2017)	Прикладне	Програмне забезпечення для редагування відео і динамічних зображень	Commercial	PC#1, PC#2, PC#3
3DS Max (версія 2017)	Прикладне	Програмне забезпечення для 3D-моделювання, анімації	Не ліцензійне	PC#1, PC#2, PC#3
Microsoft Edge (версія 44.18362.1.0)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Google Chrome (версія 80.0.3987)	Прикладне	Програми для роботи в комп'ютерній мережі	Freeware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Microsoft Outlook (версія 17)	Прикладне	Програми для роботи в комп'ютерній мережі	Commercial	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Adobe Illustrator (версія CC 2015)	Прикладне	Векторний графічний редактор	Commercial	PC#1, PC#2, PC#3

Продовження таблиці 1.6

Назва	Тип	Опис	Тип ліцензії	Встановлено
Fast Picture Viewer (версія 1.9.358.0)	Прикладне	Програма для перегляду зображень	Shareware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Windows Media Player (версія 12.0.18362.418)	Прикладне	Програма для відтворення відео- та аудіофайлів	Freeware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Adobe Reader (версія 15.0)	Прикладне	Програма для перегляду і друку pdf-файлів	Freeware	PC#1, PC#2, PC#3, PC#4, PC#5, Lap#1, Lap#2, Lap#3, Lap#4, Lap#5
Visual Studio (версія 16.0)	Спеціальне	Об'єктно-орієнтованімови програмування	Commercial	Lap#2, Lap#3, Lap#4

Опис структурної схеми

Структурна схема являє собою локальну систему з виходом в Інтернет. Усі працівники та клієнти мають вихід до Інтернету. В центрі мережу міститься комутатор. До нього під'єднанні інші комп'ютери та сервер, така структура називається «пасивною зіркою». Також ксерокс, підключений до комп'ютера бухгалтера. Структурна схема представлена на Рисунку 1.6.

Опис інформаційних потоків

На ОІД циркулює та обробляються інформаційні ресурси, такі як:

- інформація про клієнтів компанії;
- продукт роботи компанії;
- бухгалтерські звіти діяльності компанії

Вищеописані ресурси описані в таблиці 1.7. Оброблюється інформація робочим персоналом компанії, яка включає в себе директора, системного

адміністратора, 3 дизайнерів, 3 програмістів, бухгалтера та секретаря (Таблиця 1.8).

Інформація про клієнтів: дана інформація заповнюється на персональному комп'ютері або ноутбуку в спеціальному програмному продукту Excel директором або секретарем та зберігається на сервері. Секретар може копіювати та друкувати цю інформацію, директор зберігає усі папери у сейфі (Рисунок 1.7).

Бухгалтерські звіти діяльності компанії: ця інформація заповнюється на персональному комп'ютері в спеціальних програмних продуктах 1С та Excel бухгалтером та зберігається на сервері. Секретар може читати (використовувати) цю інформацію, бухгалтер та директор можуть копіювати та друкувати цю інформацію, директор зберігає усі папери у сейфі (Рисунок 1.7).

Продукт роботи компанії: ця інформація є підсумковим етапом роботи компанії та зберігається на сервер. Групи дизайнерів та програмістів використовуються цю інформацію у повному доступі з усіма правами. Секретар може читати, копіювати та друкувати цю інформацію, директор зберігає усі папери у сейфі (Рисунок 1.7).

На підприємстві використовуються засоби для створення резервних копії інформації на сервері. Резервне копіювання проводиться для усієї інформації на сервері.

Таблиця 1.7 - Інформація, яка циркулює на ОІД

Вид інформації	Режим доступу	Правовий режим	Вид представлення в ІТС	Вимоги до захисту		
				К	Ц	Д
Інформація про клієнтів компанії	Відкрита	—	Текстова, графічна	К1	Ц2	Д2
Продукт роботи компанії	Обмежений доступ	Конфіденційна	Текстова, графічна, звукова, відеоінформація	К4	Ц5	Д3

Бухгалтерські звіти діяльності компанії	Обмежений доступ	Службова	Текстова, графічна, числова	К3	Ц3	Д3

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;

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.

Опис середовища користувачів

Персонал підприємства включає: директора фірми, системного адміністратора, трьох дизайнерів, трьох програмістів, бухгалтера та секретаря.

Директор координує роботу підприємства, працює з клієнтами, перевіряє якість виконаної роботи, проводить закупівлю обладнання. Директор використовує персональний комп'ютер (PC#5).

Системний адміністратор займається технічною частиною компанії: забезпечують роботу усієї техніки (окрім охоронної та пожежної сигналізації), програмного забезпечення та комп'ютерної мережі. Виконує встановлення, оновлення та видалення ПЗ, ОС. Підтримує роботу та доступ до сервера, до Інтернету. Також у разі різної небезпеки інформації надає усі можливі заходи щодо усунення їх. Системний адміністратор використовує ноутбук (Lap#1), працює з сервером.

Дизайнери та програмісти займаються розробкою кінцевого продукту та мають повний доступ та повні права до нього. Дизайнери та програмісти використовують персональні комп'ютери (PC#1, 2, 3) та ноутбуки (Lap#2, 3, 4).

Бухгалтер контролює усі платежі, затрати та прибуток підприємства. Здійснює контроль з оплати праці, придбання нової техніки, канцелярії. Складає квартальні та річні звітності. Бухгалтер використовує персональний комп'ютер (PC#4) та підключений до нього ксерокс. Директор та секретар підтримують

зв'язок з замовниками та клієнтами. Секретар використовує персональний комп'ютер та ноутбук (Lap#5). Додається до опису персоналу компанії матриця розмежування доступу до інформації, КСЗІ та ресурсів у таблиці 1.8.

Таблиця 1.8 - Матриця розмежування

Користувач	Кількість працівників	Рівень кваліфікації	Інформація			Повноваження керувати КСЗІ	Ресурси
			Інф. про кл.	Продукт компанії	Бухгалт. звіти		
Директор	1	Високо-кваліфіковані робітники	R, W, C, D, M, S, P	R, C, D, P	R, C, D, S, P	+	PC#5
Системний адміністратор	1	Високо-кваліфіковані робітники	R	R	R	+	Lap#1, Commutator, Server
Дизайнер	3	Кваліфіковані робітники	R	R, W, D, M, S	—	—	PC#1, PC#2, PC#3
Програміст	3	Кваліфіковані робітники	R	R, W, D, M, S	—	—	Lap#2, Lap#3, Lap#4
Бухгалтер	1	Кваліфіковані робітники	R, W, C, P	R	R, W, C, D, M, S, P	—	PC#4, Ксерокс
Секретар	1	Некваліфіко-вані робітники	R, W, C, M, S, P	R	—	—	Lap#5

Умовні позначення:

R – читання
W – запис (створення)
C – копіювання
D – видалення
M – модифікація
S – зберігання
P – друкування

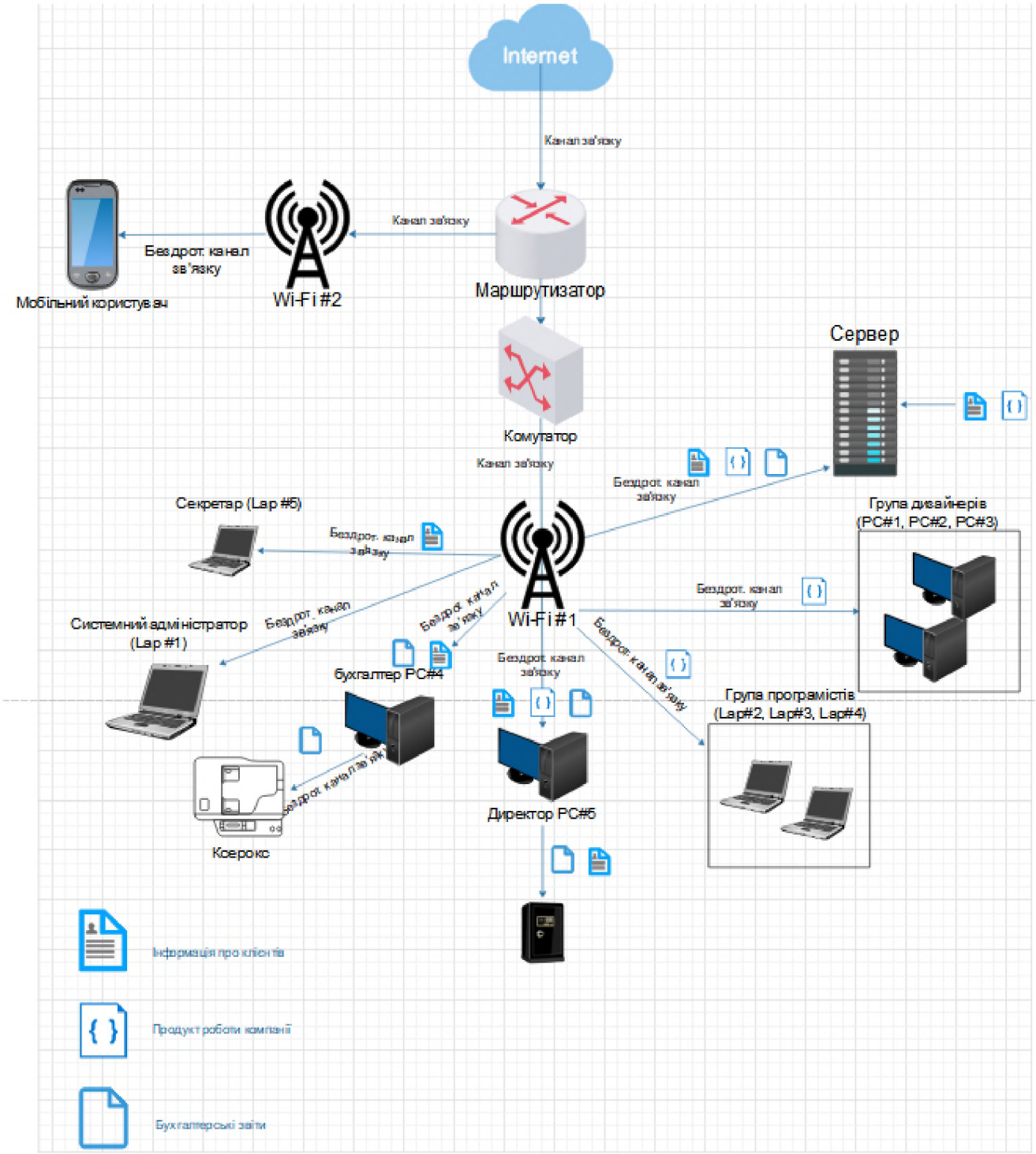


Рисунок 1.7 - Інформаційні потоки

1.4 Висновки до 1 розділу

Отже, можна сказати, що дана компанія має перелік нормативних документів, які становлять НПБ для даного підприємства. З точки зору безпеки інформації, у даних документах містяться такі види даних, як:

- Персональні дані працівників компанії;

- Інформація про діяльність підприємства;

- Підрозділи інформації підприємства, що становлять комерційну таємницю;

- Договори з клієнтами підприємства, бази даних клієнтів.

Згідно із 9 статті Законів України «Про захист інформації в ІТС»:

«Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.»

Виходячи із вищеописаного терміну можна сказати, що встановлення питання про реалізацію КСЗІ затверджено на законодавчому рівні і стосується всіх видів підприємств комерційного або державного плану. Оскільки в НПБ були присутні документи в яких може міститися ІЗоД, то для даного типу організації необхідно проаналізувати ІТС даної структури, створити акти обстеження і загроз, вразливостей, моделі порушника та виходячи із даних документів розробити КСЗІ для даної компанії.

Також у даному розділі було детально обстежено ІТС з точки зору безпеки інформації та досліджено організаційні, програмно-апаратні аспекти в сфері ІБ даної компанії.

У наступному розділі буде розроблено акти, які пов’язані з аналізом ІТС компанії та створено КСЗІ, яке буде забезпечувати мінімізацію можливого негативного впливу на компанію та її інформаційне середовище.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель загроз і порушника

Згідно із НД-ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації комп’ютерних систем від несанкціанованого доступу»:

«Модель загроз (model of threats) — абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз, таблиця 2.3.

Модель порушника (user violator model) — абстрактний формалізований або неформалізований опис порушника», таблиця 2.1.

Тобто, виходячи із даної термінології можна сказати що виходячи із акту обстеження виконуються роботи пов’язані із розслідуванням можливих інформаційних дір, які можуть привести до порушення конфіденційності, цілісності або доступності інформації та інших її властивостей. Далі буде проведено процедури, пов’язані з виявленням негативних факторів впливу на ІТС.

Модель порушника

Таблиця 2.1 - Категорії порушників

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ3	М3	К2	З2	Ч1	Д3	
	3	2	2	3	3	3	16
	П35	М4	К2	З4	Ч1	Д3	
	4	3	2	4	3	3	19
Системний адміністратор	ПВ2	М2	К3	З1	Ч4	Д4	
	2	2	4	1	4	4	17
	П35	М4	К3	З4	Ч4	Д4	
	4	3	4	4	4	4	23
Дизайнер	ПВ1	М2	К2	З1	Ч1	Д3	

	1	2	2	1	3	3	12
	ПЗ5	М4	К3	З2	Ч1	Д3	
	4	3	4	3	3	3	20

Продовження таблиці 2.1

Посада	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Програміст	ПВ1	М2	К2	З1	Ч1	Д3	12
	1	2	2	1	3	3	
	ПЗ5	М4	К3	З2	Ч1	Д3	20
	4	3	4	3	3	3	
Бухгалтер	ПВ1	М1	К2	З1	Ч4	Д3	10
	1	1	2	1	4	3	
	ПЗ5	М4	К3	З2	Ч4	Д3	21
	4	3	4	3	4	3	
Бухгалтер	ПВ1	М1	К1	З1	Ч1	Д2	9
	1	1	1	1	3	2	
	ПЗ5	М4	К3	З2	Ч1	Д2	19
	4	3	4	3	3	2	

Таблиця 2.2 - Модель внутрішнього порушника політики безпеки інформації

Категорія порушника «ПВ»	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Директор	ПВ3	М3	К2	З2	Ч1	Д3	16
Системний адміністратор	ПВ2	М2	К3	З1	Ч4	Д4	17
Дизайнер	ПВ1	М2	К2	З1	Ч1	Д3	12
Програміст	ПВ1	М2	К2	З1	Ч1	Д3	12

Бухгалтер	ПВ1	М1	К2	З1	Ч4	Д3	10
Секретар	ПВ1	М1	К1	З1	Ч1	Д2	9

Визначено, що найбільшу загрозу представляє співробітник ІТС, який виконує роль системного адміністратора. Дії особи на даній посаді мають відстежуватися, оскільки вона є основним потенційним порушником ІБ на ІТС даного підприємства.

Модель загроз

Таблиця 2.3 - Перелік загроз з визначенням порушень властивостей інформації та ІТС

№	Загроза	Вразливість	Збиток	Ризики властивостей інформації
Загрози, пов'язані з внутрішніми діями працівників				
1	Викрадення або знищення інформації	Недбале зберігання та облік документів, носіїв інформації, баз даних	Середній	К,Ц,Д
2	Несанкціоновані дії або помилки системних адміністраторів	Несанкціоновані або помилкові дії адміністраторів (неправильне встановлення або оновлення ПЗ, ОС, систем сигналізації, неправомірне відключення засобів захисту ІТС)	Високий	К,Ц,Д
3	Помилки користувачів	Помилки користувачів (встановлення та запуск піратського, шкідливого ПЗ, самостійне оновлення системи, використання Інтернету в інших цілях)	Середній	К,Ц
Загрози, пов'язані з зовнішніми діями сторонніх людей				
4	Викрадення інформації	Несанкціоноване копіювання інформації на сторонні носії людьми, що не є працівниками підприємства через недбалість самих робітників	Середній	К
5	Промисловий шпіонаж	Неправильний підбір співробітників. Викрадення	Середній	К

		інформації, працюючи на підприємство конкурент.		

Продовження таблиці 2.3

№	Загроза	Вразливість	Збиток	Ризики властивостей інформації
6	Перехоплення інформації (ПЕМВН)	Витік з переймання ПЕМВН, які створюються технічними засобами	Середній	К
7	Хакінг	Виконання несанкціонованих дій на кінцевому пристроєві клієнта	Високий	К,Ц
8	Перехоплення інформації (візуально-оптичне)	Несанкціонований перегляд інформації за рахунок візуально-оптичного каналу через недбалість працівника	Низький	К
Загрози, пов’язані з внутрішніми технічними проблемами				
9	Недолік охоронної сигналізації	Не якісне технічне обладнання або не правильно встановлена система охоронної сигналізації	Високий	Ц,Д
10	Недолік пожежної сигналізації	Не якісне технічне обладнання або не правильно встановлена система пожежної сигналізації	Високий	К,Ц,Д
11	Збої в каналах зв’язку	Перевищення порогу допустимого навантаження на канали зв’язку або ж розрахункові ресурси системи	Середній	Ц,Д
12	Зношення технічного обладнання	Збої та відмови системи електроживлення, часті скачки напруги	Низький	Ц,Д
13	Зношення носіїв інформації, серверу	Збої або пошкодження носіїв інформації, серверної частини підприємства	Високий	Ц
Загрози природного походження				
14	Катастрофа	Пожежа, повінь, землетрус, техногенні аварії	Високий	Ц,Д

*низький збиток - відсутній збиток/незначний збиток

Висновки дослідження моделі загроз і порушника

1. Порушення конфіденційності інформації (інформації про продукт виготовлення компанії, про клієнтів та бухгалтерські звіти) сторонніми людьми за рахунок несанкціонованого копіювання на сторонні носії. Причина - відсутність режиму КЗ на території підприємства або недбалість працівників. Можливі наслідки - виток інформації, незначні фінансові втрати, шкода репутації підприємства та клієнтів.

2. Порушення конфіденційності інформації сторонніми людьми за рахунок витоку її з ПЕМВН, які створюються технічними засобами. Причина - відсутність пасивних та активних засобів захисту від ПЕМВН. Можливі наслідки - виток інформації, незначні фінансові втрати, шкода репутації підприємства та клієнтів.

3. Порушення конфіденційності та цілісності інформації (інформації про продукт виготовлення компанії) співробітниками за рахунок людського фактору (встановлення та запуск піратського, шкідливого ПЗ, самостійне оновлення системи, використання Інтернету в інших цілях). Причина - недостатній контроль дій користувачів системним адміністратором. Можливі наслідки - виток інформації, фінансові втрати.

4. Порушення цілісності інформації на технічному обладнанні через поломку носіїв інформації або серверу. Причина - відсутність резервного копіювання. Можливі наслідки – часткова\повна втрата інформації, великі фінансові втрати.

5. Порушення конфіденційності, цілісності та доступності інформації системними адміністраторами за рахунок несанкціонованих або помилкових дій в ІТС (неправильне встановлення або оновлення ПЗ/систем сигналізації). Причина - корисливі дії персоналу, відсутність введення протоколів у журналі подій. Можливі наслідки – технічні збої.

З усіх наведених загроз, механізмів їх реалізації, імовірності, спрямованості, рівня шкоди та наслідків, можна зробити висновок, що помилки системних адміністраторів та користувачів, викрадення інформації, зношення носіїв інформації, серверу, перехоплення інформації є найнебезпечнішими та найактуальнішими загрозами для підприємства, що підлягають для негайної побудови нової політики ІБ. У наступних підрозділах буде розроблено КСЗІ і створено політику безпеки виходячи із зафіксованих загроз, вразливостей і порушень навмисного або ненавмисного характеру з боку осіб, які являються або не являються частиною ІТС.

2.2 Розробка КСЗІ

КД-4. Абсолютна довірча конфіденційність. **Не реалізовано**. ІТС не має достатню кількість ресурсів для розмежування через КЗЗ користувача, захищеного об’єкта і процесу

КД-3. Повна довірча конфіденційність. **Частково реалізовано.** У КЗЗ даної ІТС присутні апаратні та людські ресурси, які мають змогу визначати користувачу або групі користувачів процеси, які належать до його або їх домену конкретних користувачів або групи користувачів, які мають або не мають права ініціювати процес, але не мають можливості для розмежування через КЗЗ користувача, захищеного об’єкта і процесу.

КА-4, КА-3. Абсолютна, повна адміністративна конфіденційність. **Не реалізовано.** Дана політика не має можливості відноситись до всіх об’єктів КС.

КА-2. Базова адміністративна конфіденційність. **Реалізовано**. КЗЗ даної ІТС має програмно-апаратні механізми, які здатні надати можливість адміністратору або особі з відповідними повноваженнями через процедури керування доменами визначати конкретних користувачів або групи користувачів, які мають права ініціювати процеси (Механізм: Система розмежування доступу до ІР в ОС)

КО-1. Повторне використання об’єкта. **Частково реалізовано.** Через систему розмежування доступу облікових записів, користувачам може бути

доступна інформація, в залежності від рівня доступу користувача до IP на програмному рівні, але процеси механічного розмежування неможливо реалізувати (наприклад, при завершенні роботи система не має можливості автоматично форматувати жорсткий диск)

КК-3. Перекриття прихованих каналів. **Не реалізовано.** КЗЗ даної ІТС не має достатню кількість програмно-апаратних механізмів, які реалізують процедури ліквідації прихованих каналів.

КК-2. Контроль прихованих каналів. **Реалізовано.** В системі даної ІТС присутні програмно-апаратні ресурси та механізми, які забезпечують реєстрацію підмножини прихованих каналів (Механізм: Система перевірки завантажених ресурсів і виявлення прихованих каналів (SCDR and DPC))

КВ-4, КВ-3. Абсолютна, повна конфіденційність при обміні. **Не реалізовано.** КЗЗ даної ІТС не має максимально можливу кількість програмно-апаратних ресурсів для повної взаємодії із об'єктами і інтерфейсними процесами в КС.

КК-2. Базова конфіденційність при обміні. **Реалізовано**. КЗЗ має достатню кількість програмно-апартних ресурсів для забезпечення запитів імпортованих та експортованих ресурсів на підставі атрибутів доступу інтерфейсних процесів (Механізми: Віртуальна приватна мережа (VPN), механізми шифрування (PGP))

ЦД-4,3. Абсолютна, повна довірча цілісність. **Не реалізовано.** КЗЗ даної АС не має достатню кількість програмно-апаратних ресурсів для повної реалізації даної політики.

ЦД-2. Базова довірча цілісність. **Реалізовано.** В системі присутні механізми, які займаються даною політику. КЗЗ має можливість розмежовувати користувачів та їх групи які мають право ініціювати процеси.

ЦА-4,3. Абсолютна, повна адміністративна цілісність. **Не реалізовано** Система не має достатню кількість програмно-апаратних і людських ресурсів для повної реалізації даної політики.

ЦА-2. Базова адміністративна цілісність. **Реалізовано.** В системі присутні програмно-апаратні механізми і осіб, які можуть взаємодіяти з даними ресурсами,

керувати потоками інформації. КЗЗ має можливість призначати користувача та їх групи і розмежовувати даних осіб на підставах атрибутів доступу. Групи користувачів взаємодіють з потоками інформації в ІТС (Механізм: Програмні продукти запису файлів та їх пересування (Microsoft Office, програми відправки файлів по ОС))

ЦО-2. Повний відкат. **Частково реалізовано.** ІТС має програмно-апаратні ресурси для регулювання відкату за будь-який проміжок часу, але ІР можуть бути відновлені вибірково.

ЦВ-3. Повна цілісність при обміні. **Не реалізовано.** Під час імпорту\експорту ІР відсутні механізми КЗЗ які здатні забезпечувати повну реалізацію даної політики.

ЦВ-2. Базова цілісність при обміні. КЗЗ даної АС має програмно-апаратні механізми, які створюють умови імпорту\експорту. Адміністратори або користувачі з відповідними повноваженнями мають можливості створити умови на імпорт\експорт ІР та присвоєння чи зміни рівня захищенності (Механізм: Утиліта перевірки вагової частки завантажених файлів).

ДР-3, ДР-2. Приорітетність використання ресурсів, недопущення перехоплення ресурсів. **Не реалізовано**. Політика не відноситься до всіх об'єктів в КС.

ДР-1. Квоти. **Реалізовано.** В КЗЗ присутні програмно-апаратні механізми, які регулюють циркуляцію ІР в КС (Механізм: Програма обліку робочого часу користувачів).

ДС-3. Стійкість без погіршення обслуговування. **Не реалізовано.** КЗЗ даної АС не має достатню кількість програмно-апаратних ресурсів, для підтримки системи без погіршених умов у результаті відмови одного або декількох компонентів.

ДС-2. Стійкість з погіршенням характеристик обслуговування. **Реалізовано.** В системі присутні програмно-апаратні ресурси, які підтримують діяльність ІТС у погіршених умовах у результаті відмови одного або множини компонентів (Механізм: Звернений проксі, резервний сервер).

ДЗ-3, ДЗ-2. Заміна будь-якого компонента, обмежена гаряча заміна. **Не реалізовано.** КЗЗ не має можливості модернізації або заміни будь-якого компонента або конкретної множини компонентів без переривання обслуговування.

ДЗ-1. Модернізація. **Реалізовано**. КЗЗ даної ІТС має призначену особу з відповідними повноваженнями, яка має право переривати діяльність ІТС з метою виконання ремонтних робіт або модернізації компонетів в АС.

ДВ-3, ДВ-2. Вибіркове, автоматичне відновлення. **Не реалізовано.** КЗЗ не має програмно-апаратних ресурсів для відновлення і приведення до нормального стану КС у автоматичному режимі.

ДВ-1. Ручне відновлення. **Реалізовано**. У результаті збою КС в АС присутні особи з віповідними повноваженнями, які приводять КС до нормального стану або стану з обмеженими умовами у ручному режимі. У результаті виконання даної процедури КС тимчасово не доступний.

НР-5. Аналіз у реальному часі. **Не реалізовано.** КЗЗ не має функцій або програмно-апаратних механізмів для реєстрації НСД або інших подій у реальному часі.

НР-4. Детальна реєстрація. **Реалізовано.** В КЗЗ присутні програмно-апаратні ресурси, які забезпечують захист журналу подій від НСД або іншого негативного впливу на даний продукт. Адміністратори і користувачі з відповідними повноваженнями здатні аналізувати журнал подій використовуючи засоби для перегляду реєстраційних подій (Механізм: Журнал подій ОС, утиліта Anti-Red для журналу подій з системою блокування до редагування або іншого негативного впливу на реєстраційні події).

НИ-3. Множинна ідентифікація та автентифікація. **Частково реалізовано.** Система має 1 програмно-апаратний механізм для перевірки користувача в ІТС. Необхідність надання додактових програмно-апаратних механізмів встановлюється власником ІТС (Механізм: ПКП із налаштованим механізмом бази даних паролів, система ідентифікації ОС (даний механізм присутній, але не активний)).

НК-2. Двонаправлений достовірний канал. **Не реалізовано.** КЗЗ даної АС не надає користувачеві повного керування зв'язком. Зв'язок не може ініціюватися з боку КЗЗ.

НК-1. Однонаправлений достовірний канал. **Реалізовано.** В системі присутні механізми, які керують даною процедурою з боку користувача (Механізм: Програма передачі файлів ОС, Bluetooth).

НО-3. Розподіл обов'язків на підставі привілеїв. **Не реалізовано.** Політика розподілу в системі не визначає множину користувачів.

НО-2. Розподіл обов'язків адміністраторів. **Частково реалізовано.** В системі присутні механізми, які керують діяльністю обов'язків адміністраторів, але активувати дані програмно-апаратні ресурси та призначити відповідних осіб можливо за бажанням власника ІТС. АС має особу, яка виконує функцію адміністратора системи та адміністратора безпеки.

НЦ-3, НЦ-2. КЗЗ з функціями диспетчера доступу, гарантованою цілісністю. **Не реалізовано.** КЗЗ не має достатню кількість програмно-апаратних ресурсів для підтримки власних доменів від зовнішніх впливів, НСД та інших негативних випадків.

НЦ-1. КЗЗ з контролем цілісності. **Реалізовано.** Система має програмні ресурси, які спрямовані на оповіщення адміністратора системи і блокування КС від негативного втручання до тих пір, доки адміністратор не приведе ресурс до нормального стану власноруч (Механізми: Система оповіщення ОС, VirusChecker, OSLocker).

НТ-3. Самотестування у реальному часі. **Не реалізовано.** Система не має програмно-апаратних механізмів для тестування КС у реальному часі.

НТ-2. Самтоестування при старті. **Частково реалізовано.** В КЗЗ присутні механізми, які реалізують дану політику, проте активація даної функції можлива за наказом власника ІТС. (Механізм: Антивірусне ПЗ із механізмом пошуку вірусів, хробаків та ін. при старті ОС).

НВ-3, НВ-2. Автентифікація з підтвердженням, автентифікація джерела. **Не реалізовано.** В КЗЗ відсутні механізми захисту, які встановлюють джерело кожного об'єкта, що експортується або імпортується в КС.

НВ-1. Автентифікація вузла. **Реалізовано.** КЗЗ присутні механізми для реєстрації вузла або вузлів, які імпортують або експортують об'єкти в КС. (Механізм: Wireshark, Nmap).

НА-2. Автентифікація відправника з підтвердженням. **Не реалізовано.** Система не має департаментів, відділів або третіх осіб, які можуть однозначно підтвердити відправника завдяки протоколам автентифікації або інших механізмів.

НА-1. Базова автентифікація відправника. В КЗЗ присутній механізм, який фіксує множину властивостей і атрибутів об'єкта що передається користувачем-відправником (Механізм: Програма для створення та використання електронно-цифрового підпису (OpenSSL)).

НП-2. Автентифікація одержувача з підтвердженням. **Не реалізовано.** Система не має департаментів, відділів або третіх осіб, які можуть однозначно підтвердити одержувача завдяки протоколам автентифікації або інших механізмів.

НП-1. Базова автентифікація одержувача. КЗЗ наявний механізм, який здатний автентифікувати одержувача. Система визначає множину властивостей і атрибутів об'єкта що отримується користувачем-одержувачем (Механізм: Утиліта для перевірки електронно-цифрового підпису (OpenSSL)).

Рекомендаційними вирішеннями окрім реалізації КСЗІ з боку програмно-апаратних галузей буде налаштування організаційних аспектів, які налаштують циркуляцію інформації в ІТС. Наступним шляхом буде створено політики, які дозволять забезпечити порядок та послідовність інформаційних потоків в ІТС і мінімізують негативний вплив на ІТС.

2.3 Розробка політики безпеки

Згідно із НД-ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації комп'ютерних систем від несанкціанованого доступу»:

«Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації».

Тобто, можна сказати що політика безпеки представляє собою перелік нормативних документів, правил законів які забезпечують поведінку потоків інформації в ІТС. Нижче буде наведено декілька політик різнопланового характеру які встановлять стандарти для циркуляції інформації в АС.

Політика шифрування

Останній статус оновлення**:** оновлено травень 2020 року.

Метою цієї політики є надання вказівок, які обмежують використання шифрування для тих алгоритмів, які отримали істотне та публічне дослідженння і було доведено, що вони ефективно працюють. Крім того, ця політика створює напрямок для забезпечення і дотримання федеральних норм та надання законних повноважень щодо розповсюдження і використання технологій шифрування.

Сфера застосування

Ця політика поширюється на всіх співробітників компанії «Websofttonic» та їх філій.

Політика

Вимоги до алгоритму

Шифри, що використовуються, повинні відповідати або перевищувати набір, визначений як "AES-сумісний" або "частково сумісний з AES" відповідно до каталогу шифрів IETF / IRTF або набору, визначеного для використання в Державній службі спеціального зв'язку України. НД-ТЗІ, ДСТУ або будь-які замінені документи відповідно до дати впровадження. Для симетричного шифрування настійно рекомендується використовувати розширений стандарт шифрування (AES).

Використовувані алгоритми повинні відповідати стандартам, визначеними у Держспецзвязку або будь-якому заміненому документі, відповідно до дати впровадження. Для асиметричного шифрування настійно рекомендується використовувати алгоритми RSA та криптографії Еліптичної кривої (ECC).

Алгоритми підпису

Алгоритм довжини ключа

RSA 2048 Потрібно використовувати захищену схему прокладки. Рекомендується схема прокладки PKCS №7. Потрібне хешування повідомлень. LDWM SHA256 Зверніться до чернетки підписів на основі LDWM.

Вимоги до функції хешу

Загалом, «Websofttonic» дотримується політики охоронної служби «ГАРДА» щодо функцій хешу.

Ключова угода та автентифікація

- Обмін ключами повинен використовувати один з наступних криптографічних протоколів: Diffie-Hellman, IKE, або Еліптична крива Diffie-Hellman (ECDH).

- Кінцеві точки повинні бути аутентифіковані до обміну або виведення ключів сеансу.

- Публічні ключі, що використовуються для встановлення довіри, повинні бути аутентифіковані перед використанням. Приклади аутентифікації включають передачу через криптографічно підписане повідомлення або ручну перевірку хешу відкритого ключа.

- Усі сервери, що використовуються для аутентифікації (наприклад, RADIUS або TACACS), повинні мати встановлений дійсний сертифікат, підписаний відомим надійним постачальником.

- Усі сервери та програми, що використовують SSL або TLS, повинні мати сертифікати, підписані відомим надійним постачальником.

Генерація ключів

- Криптографічні ключі повинні бути створені та збережені безпечним чином, що запобігає втраті, крадіжці або компрометації.

- Генерування ключів повинно бути посіяне з галузевого стандартного генератора випадкових чисел (RNG).

Дотримання політики

Вимірювання відповідності

Охоронна служба «ГАРДА» перевірить відповідність цій політиці за допомогою різних методів, включаючи, але не обмежуючись ними, звіти про бізнес-інструменти, внутрішні та зовнішні аудити та зворотній зв'язок з власником політики.

Винятки

Будь-який виняток із політики повинен бути затверджений командою Infosec заздалегідь.

Недотримання

Працівник, який порушив умови цієї політики, може зазнати дисциплінарного стягнення, аж до припинення роботи.

Історія редагування

Дата	Опис
25.05.2020	Охоронна служба «ГАРДА» розробила дану політику
–	–

Політика зберігання інформації в ІТС

Останній статус оновлення: оновлено травень 2020 року

Опис

Дана політика може бути інструментом імпорту, щоб гарантувати, що всі чутливі / конфіденційні матеріали є видаляється з робочої області кінцевого користувача та блокується, коли елементи не використовуються або є працівник залишає свою робочу станцію. Це одна з найкращих стратегій, яку потрібно використовувати при спробі зменшити ризик порушення безпеки на робочому

місці. Така політика також може зростати обізнаність працівника щодо захисту конфіденційної інформації.

Призначення

Метою цієї політики є встановлення мінімальних вимог щодо підтримки «чистоти» де знаходиться ІЗоД, комерційна та конфіденційна інформація про працівників, інтелектуальну власність, клієнтів та постачальників захищені у замкнених місцях та поза сайтом. Дана політика є частиною стандартного базового контролю конфіденційності.

Сфера застосування:

Ця політика поширюється на всіх співробітників «WebSofttonic» та їх філій.

Політика:

- Співробітники зобов'язані забезпечити всю критичну інформацію на твердій копії або в електронній формі, яка захищена в робочій зоні, наприкінці дня та протягом тривалого періоду.

- Робочі станції комп'ютерів повинні бути заблоковані, коли робоча область незайнята.

- Робочі станції комп'ютерів повинні бути повністю вимкнені наприкінці робочого дня.

- Будь-яку критичну інформацію необхідно вийняти з письмового столу та зафіксувати у спеціально відведених місцях, зазначених власником ІТС в кінці робочого дня.

- Файлові шафи, що містять критичну інформацію, слід закрити та заблокувати, коли об'єкт не використовується або коли він не відвідується.

- Механізми та засоби, які використовуються для доступу до ІзОД або конфіденційної інформації, не повинні залишатися в полі без нагляду.

- Ноутбуки повинні бути або заблоковані замикаючим кабелем, або зафіксовані у шухляді.

- Паролі не можуть залишатися на клейких нотатках, розміщених на комп'ютері або під ними, а також не можуть бути записаними у доступних місцях.

- Роздруківки, що містять ІЗоД, мають бути негайно вилучені з принтера.

- Утилізацію критичних документів слід проводити у спеціально відведених місцях власником ІТС або довіреними особами з відповідними повноваженнями. Дана інформація повинна бути роздрібнена спеціальними механізмами або заблокована у файлових шафах або сейфах.

- Білі дошки, що містять критичну інформацію, слід стерти.

- Портативні обчислювальні пристрої, такі як ноутбуки та планшети повинно бути заблоковано.

- Фіксуйте в ІТС пристрої масового зберігання, такі як накопичувачі CDROM, DVD або USB які можуть містити критичну інформацію. Закріпіть їх у спеціально відведених місцях для їх зберігання (сейфи, шафи тощо)

- Усі принтери та факсимільні машини повинні бути очищені від паперів, як тільки вони надруковані. Це допомагає переконатися, що конфіденційні документи не залишаються на лотках для принтера, щоб порушник ІТС не вчинив негативний вплив на ІС підприємства.

Дотримання політики

Вимірювання відповідності

Охоронна служба «ГАРДА» перевірить відповідність цій політиці за допомогою різних методів, наприклад фізичним оглядом, відеомоніторингом, звітами про бізнес-інструменти, внутрішніми та зовнішніми ревізіями та відгуками власника політики.

Винятки

Будь-який виняток із політики повинен бути затверджений Охоронною службою «ГАРДА» заздалегідь.

Недотримання

Працівник, який спричинив порушення цієї політики, може бути підданий дисциплінарному стягненню аж до припинення роботи.

Історія редагування

Дата	Опис
29.05.2020	Охоронна служба «ГАРДА» розробила дану політику
–	–

2.4 Висновки до 2 розділу

Підводячи підсумки можна сказати, що у даному розділі було детально обстежено ІТС з точки зору безпеки інформації та досліджено організаційні, програмно-апаратні аспекти в сфері ІБ даної компанії. Зазначено дані фактори було за допомогою нормативних документів, затверджених із стандартами Держспецзвязку і розроблено методи боротьби із зафіксованими загрозами та вразливостями.

Проте на реалізацію даних політик, механізмів захисту тощо необхідні ресурси. У наступному розділі буде розглянуто економічні фактори, які впливають на економічне середовище компанії, розраховано витрати на реалізацію політик безпеки та КСЗІ, їх підтримку і надано рекомендації стосовно мінімізації витрат на реалізацію продуктів з галузі безпеки інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Основною метою цього розділу є розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення (далі об'єкт проектування), розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування, визначення річного економічного ефекту від впровадження об'єкта проектування, визначення та аналіз показників економічної ефективності реалізацію запропонованих рішень (КСЗІ та політик безпеки).

3.1 Капітальні витрати

На реалізацію даного проекту необхідні ресурси фізичного, організаційного і програмно-апаратного характеру. Нижче буде надано дані у табличній формі із можливими прорахунками і формулами. У випадках, коли ціна на певний продукт буде сильно варіюватися, то ціна буде прораховано завдяки наступній формулі. В інших випадках, наприклад, коли ціна за продукт незмінна (взята з джерела розробника), то формула не буде враховуватися.

$$\text{Середня ціна} = \frac{\text{Ціна 1} + \text{Ціна 2} + \cdots + \text{Ціна}N}{\text{Кількість джерел}} \quad (3.1)$$

Таблиця 3.1 – Витрати на закупівлю ресурсів та послуг

Назва	Опис	Ціна (грн, коп)	Примітки
Реєстрація засобів збереження інформації (флеш-карти, диски тощо)	Закупівля і фіксація засобів збереження інформації	Kingston Data Traveler (16 gb): 141,00 + 116,00 +179,00/3 = 145,30 (за 1 шт) 145,30 * 4 = 581,30	В АС компанії необхідно мінімум 4 флеш карти для керуючих осіб і осіб, які взаємодіють з документацією про діяльність ІТС (власник ІТС, головний директор, бухгалтер) та співробітників підтримки ІТС (системні адміністратори)
Пломбування роз'ємів на технічних пристроях	Закриття зайвих роз'ємів з метою зниження ризику витоку інформації через незареєстровані носії	Наліпка-пломба (1 рулон) : 0,56 + 0,68 + 1,11 \ 3 = 0,78 (за 1 шт) 0,78 * 20 = 15,66	Пломбування необхідно для всіх пристроїв, окрім технічних засобів керуючого персоналу, робітників, працюючих з документацією і співробітників підтримки ІТС (4 ноутбуки). Кількість пломб залежить від кількості портів на пристрої. 1 ноутбук має 5 портів (1 займає миша) . ПК – 6 портів (2 займають миша і клавіатура). 1 наліпка блокує доступ до 1 порта. Кількість портів: 4*5 = 20

Продоження таблиці 3.1

Назва	Опис	Ціна (грн, коп)	Примітки
Розробка політик безпеки	Дана процедура створить умови поведінки інформації в ІТС і розробить політики, які мінімізують інформаційні витоки.	Прорахунки не було зроблено (див. примітки)	Витрати залежать від часу, затраченого спеціалістом на розробку політики безпеки. Згідно прайсу сторонньої компанії, вартість розробки політики коштує 85 грн\год. Нижче буде прораховано витрати на реалізацію політики
Встановлення пасивних засобів захисту (Екранування приміщення)	Інсталяція механізмів захисту затверджених Держспецзвязком з метою зниження ризику витоку даних через ПЕВМН	Фарба YSHIELDHSF54 (ВЧ, НЧ, 5л) – 11200 Витрати 1 відра фарби: 6*5 = 30м2 Для 160м2: 160\5 =32л Для покриття всього приміщення необхідно:	Для зниження ризику реалізації даної загрози необхідно провести екранування приміщення. Вартість екрануючої фарби YSHIELDHSF54 (ВЧ, НЧ, 5 л) взята з сайту розробника. Для покриття всього приміщення площею 16*10 = 160 м2. Витрати 1л фарби на покриття: 6 м2\л

		32\5 = 6.4 = 7 відер 11200 * 7 = 78400	

Загальна сума на розробку КСЗІ: 581,30 + 15,66 + 78400 = 78996,96

Далі необхідно прорахувати, скільки грошових ресурсів втратить компанія на розробку політики безпеки інформації. Визначити можна за даною формулою:

$$К_{рп} = З_{зп} + З_{мч} \quad (3.3)$$

де Крп - витрати на розробку політики, Ззп - заробітна платня спеціаліста, Змч - витрачений час на розробку політики. Враховуючи такий фактор, що робітник отримує зарплатню в щомісячному еквіваленті, то можна розрахувати приблизні витрати на розробку політики. Спеціаліст працює 6 год\день 4 дн\тижд. Кількість годин за місяць можна розрахувати таким чином:

$$4\frac{\text{тижнів}}{\text{місяць}} \cdot 4\frac{\text{днів}}{\text{тиждень}} = 16\frac{\text{днів}}{\text{місяць}}$$

$$16\frac{\text{днів}}{\text{місяць}} \cdot 6\frac{\text{год}}{\text{день}} = 96\frac{\text{год}}{\text{місяць}}$$

Для знаходження витрат, необхідно прорахувати заробітню платню виконавця наступною формулою:

$$З_{зп} = t \cdot З_{іб} \quad (3.4(а))$$

$$З_{мч} = t \cdot С_{мч} \quad (3.4(б))$$

де, t - час, витрачений на розробку політики, Зіб - середня погодинна заробітна платня, Смч – вартість 1 години машинного часу ПК.

В свою чергу, для знаходження вартості години машинного часу необхідно залучити дану формулу:

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

де Р – встановлена потужність, Се – тариф на електричну енергію, Фзал – залишкова вартість ПК на поточний рік, На – річна норма амортизації, Напз – річна норма амортизації на ліцензійне ПЗ, Клпз – вартість ліцензійного ПЗ, Fр – річний фонд робочого часу.

Для визначення часу треба застосувати дану формулу, описану нижче:

$$t = t_{тз} + t_в + t_а + t_{вз} + t_{озб} + t_{овр} + t_д, годин, \quad (3.6)$$

де, ttз - час на оформлення технічного завдання, tв - час розробки концепції безпеки інформації організації, ta - тривалість процесу аналізу ризиків, tвз - тривалість визначення вимог, пов'язаних із забезпеченням заходів та засобів захисту, tозб - тривалість вибору основних рішень із забезпеченням безпеки інформації, tовр - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування підприємства, td - тривалість організації на оформлення документованого формату. Як приклад, буде розраховано вартість для політики, пов'язаної із забезпеченням антивірусного захисту в ІТС. Далі буде надано табличний формат часу, витраченого на розробку політики безпеки:

Таблиця 3.3 - Час, витрачений на розробку політики шифрування

Позначення	Пояснення і витрачений час

ttз	Огляд алгоритмів шифрування, зазначених Держспецзвязком - 6 год, оформлення технічного завдання - 3 год (Всього: 9 год)

Продовження таблиці 3.3

Позначення	Пояснення і витрачений час
tв	Огляд апаратно-технічних засобів, пов'язаних із циркуляцію інформації - 8 год, аналіз додаткових ресурсів організації - 4 год (Всього: 12 год)
ta	Аналіз алгоритмів шифрування в КС - 12 год, виявлення вразливостей в системі шифрування - 30 год (Всього: 42 год)
tозб	Інсталяція систем шифрування - 22 год, навчання співробітників ІТС в системі шифрування – 12 год (Всього: 34 год)
tовр	Тестування алгоритмів шифрування - 18 год, налаштування технічних ресурсів шифрування в КС - 12 год (Всього: 30 год)
tд	Розробка документу - 2 год

Сумарно витрачений час, формула (3.6):

$$t_1 = 9 + 12 + 42 + 34 + 30 + 2 = 129 \text{ годин}$$

Виходячи із вищеописаних даних, можемо знайти зарплатню виконавця, формула (3.4(а)):

$$З_{зп1} = 129 \text{ год} \cdot 85 \frac{\text{грн}}{\text{год}} = 10965 \text{ грн}$$

Далі за формулою 3.5 необхідно знайти вартість машинного часу. Потужність складає 4,22 кВт, тариф на електричну енергію – 1,87 $\frac{\text{грн}}{\text{кВт}} \cdot$ година, залишкова вартість ПК – 9400 грн, вартість ліцензійного антивірусного ПЗ –

347,50 грн, річна норма амортизації дорівнює 0,115 ч.о, норма амортизації антивірусного ПЗ – 0,092 ч.о, тобто:

$$С_{мч} = 4{,}22 \cdot 40 \cdot 1{,}87 + \frac{9400 \cdot 0{,}115}{1920} + \frac{0.092 \cdot 347{,}50}{1920} = 316{,}24 \text{ грн}$$

Можна провести наступні розрахунки згідно формули (3.4(б)):

$$129 \text{ год} \cdot 316{,}24 \text{грн} = 40794{,}44 \text{ грн}$$

Можемо зробити розрахунки за формулою (3.3):

$$К_{рп1} = 10965 \text{ грн} + 40794{,}44 = 51759{,}44 \text{ грн}$$

Далі необхідно розрахувати вартість для політики політики, пов'язаної із правилами поведінки з інформацією. У табличному форматі буде надано час, витрачений на розробку політики безпеки:

Таблиця 3.4 - Час на розробку політики зберігання інформації в ІТС

Позначення	Пояснення і витрачений час
ттз	Огляд ІС підприємства - 10 год, оформлення технічного завдання - 2 год (Всього: 12 год)
Тв	Аналіз організаційних аспектів підприємства – 12 год, аналіз засобів збереження інформації - 6 год (Всього: 13 год)
Та	Аналіз ризиків і загроз пов'язаних із захистом інформації в контексті реалізації людського фактору - 16 год, аналіз інформаційних витоків фізичного характеру – 8 год (Всього: 24 год)
тозб	Розробка аудитів і правил поведінки з інформацією для користувачів в ІТС – 25 год, встановлення засобів фізичного та електронного збереження інформації – 16 год (Всього: 41 год)
товр	Проведення стартових аудитів, пов'язаних із правилами поведінки з інформацією в ІТС - 8 год , тимчасовий контроль із засвоєнням матеріалу користувачами в ІТС - 40 год (Всього: 48 год)

tд	Розробка документу - 3 год (Всього: 3 год)

Сумарно витрачений час, формула (3.5):

$$t2 = 12 + 13 + 24 + 41 + 48 + 3 = 141 \text{ год}$$

Розрахуємо зарплатню виконавця і витрачений час на розробку політик, завдяки формулам (3.4) та (3.5):

$$З_{зп2} = 141 \text{ год} \cdot 85 \frac{\text{грн}}{\text{год}} = 11985 \text{ грн}$$

$$З_{мч2} = 141 \text{ год} \cdot 316{,}24 \text{ грн} = 44589{,}84 \text{ грн}$$

Далі знаходимо за формулою (3.3) витрати на розробку політики:

$$К_{рп2} = 11985 \text{ грн} + 44589{,}84 \text{ грн} = 56574{,}84 \text{ грн}$$

Посилаючись на таблицю 3.1, необхідно додати витрати розробки політик до суми, вказаної для розробки КСЗІ:

$$\text{Сума разових витрат: } С_{РВ} = К_{пр1} + К_{пр2} + \text{Сума для розробки КСЗІ}$$

$$С_{РВ} = 51759{,}44 \text{ грн} + 56574{,}84 \text{ грн} + 78996{,}96 \text{ грн} = 187331{,}24 \text{ грн}$$

Отже, капітальні витрати на реалізацію КСЗІ складають 187331,24 грн, враховуючи суми, прораховані на створення політик безпеки.

3.2 Поточні витрати

Наступним етапом розрахунків витрат підприємства буде прорахування поточних витрат на підтримку КСЗІ, таблиця 3.2.

Таблиця 3.2 – Поточні витрати на КСЗІ

Назва	Опис	Ціна (грн, коп)	Примітки
Щорічне поновлення ліцензії антивірусного ПЗ	Постійні витрати на поновлення ліцензії антивірусного ПЗ	Для 10 робочих станцій (5 комп'ютерів, 5 ноутбуків) із встановленим антивірусним ПЗ: 451.75 * 10 = 4517.50 Для 4 ноутбуків із ОС Linux Ubuntu: 451.75 * 4 = 1807 Загальна сума: 4517.50 + 1807 = 6324,50	Ціна була взята із сайту розробника. Вартість ліцензії для 1 ПК для ОС Windows на рік – 451.75 Так як в ІТС присутні пристрої з двома ОС, то необхідно поновлювати антивірусне ПЗ і на іншій ОС. В АС присутні 4 ноутбуки із ОС Linux Ubuntu. Вартість на поновлення антивірусного ПЗ на ОС Linux аналогічна (451.75)
Витрати на аудити з питань ІБ	Витрати спеціалістам з питань ІБ, що керують і розробляють аудити для співробітників компанії	85 * 4 = 340 (1 заняття) 4 * 4 = 16 занять\міс 16 * 12 = 192 занять\рік 340 * 192 = 65280	Ціна була взята із попередньої таблички. Розрахувати ціну можна в залежності від частоти проведення аудитів. Спеціалісти проводять аудити 4 рази на тиждень по 4 години.

Загальна сума на підтримку КСЗІ: 6324,50 + 65280 = 71604,50

Оскільки у даній організації присутні 2 особи, які забезпечують безпеку інформації і адміністрування систем в ІТС. заробітна платня працівників статична (без врахування премій). Заробітна платня адміністратора системи складає 20000 грн, генерального директора – 28000 грн. Витрати на підтримку КСЗІ буде розраховано за нижче описаною формулою:

$$С = С_н + С_а + С_з + С_{ел} + С_{тос}, \quad (3.7)$$

де Са - річний фонд амортизаційних витрат, Сз - річний фонд заробітної платні інженерно-технічного персоналу, Сн - витрати на навчання адміністративного персоналу і користувачів, Сел - вартість електроенергії, Стос - витрати на технічне й організаційне адміністрування.

Із вище описаного пункту, можна виразити формулу, для знаходження Сз наступним чином:

$$С_з = З_{осн1} + З_{осн2} + \ldots З_{осн n}, \quad (3.8)$$

де Зосн - основна заробітна платня робітника інженерно-технічного персоналу

Враховуючи вищеописану заробітну платню спеціалістів, можемо розрахувати Сз (Формула 3.8):

$$С_з = 20000 \text{ грн} + 28000 \text{ грн} = 48000 \text{ грн}$$

Витрати на навчання зазначено в таблиці 3.2, тобто, Сн = 65280 грн. Вартість електроенергії можна розрахувати за формулою:

$$С_{ел} = Р \cdot Fp \cdot Ц_е, \text{грн}, \quad (3.9)$$

де Р - встановлена потужність апаратури ІБ (кВт), Fр - річний фонд робочого часу системи ІБ, Це - тариф на електроенергію (грн\Квт · год).

Це дорівнює 1,87 грн\Квт · год. Даний показник встановлений із стандартами договору даного підприємства. За розрахунками даного року встановлена потужність апаратури ІБ складає 4,78 кВт. Аналізуючи режим роботи ІБ, можна сказати, що параметр річного фонду робочого часу системи ІБ складає 1920 годин. Отже, за формулою (3.9):

$$С_{ел} = 1{,}87 \cdot 1920 \cdot 4{,}78 = 17162{,}11 \text{ грн}$$

Згідно із таблиці 3.5, вагової частки витрат:

Витрати на технічне і адміністративне керування ІБ визначаються у відсотках від вартості капітальних витрат (Як правило 1-3%. Для даної задачі візьмемо 2%). Повертаючись до формули (3.7) можемо розрахувати поточні витрати. Дана сума призначена на місячні витрати:

$$С = 17162{,}11 + 48000 + 56574{,}84 + 187331{,}24 \cdot 2\% = 125483{,}57 \text{ грн}$$

Отже поточні витрати складають 125483,57 грн, враховуючи витрати на підтримку КСЗІ і заробітної платні спеціалістам інформаційної безпеки.

3.3 Оцінка можливого збитку

Враховуючи вищеописані поточні витрати, необхідно прорахувати можливі збитки в результаті реалізації загроз і упущеної вигоди. Умовно було зазначено множину елементів, які будуть враховані. Відповідь можна знайти завдяки наступним формулам:

$$U = П_п + П_в + V \quad (3.10)$$

$$П_п = \frac{\sum Зс}{F} \cdot t_п \quad (3.11)$$

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

де Пп – оплачувані втрати робочого часу, Пв – вартість відновлення працездатності вузла корпоративної мережі, Пви – витрати на повторне уведення інформації, Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, Пзч – вартість заміни устаткування або запасних частин, tп – час простою, F – місячний фонд робочого часу, V – втрати від зниження обсягу продажів.

В ІТС працюють 10 осіб, 1 з яких являється директором і власником ІТС (див. табл. 1.1), тобто дані параметри будуть розраховані для 9 робітників. Далі необхідно прорахувати погодинну заробітну платню працівників ІТС. Час простою складає 8 год. Всі працівники, умовно, працюють 23 дні/місяць, 40 год/тиждень, 176 год/місяць, тобто, погодинна заробітна платня працівника:

$$ПЗПП = \frac{\text{Фіксована місячна зарплата}}{\text{кільк. роб. год на місяць}} \quad (3.13)$$

Зарплата адміністратора системи складає 18000 грн. Отже згідно формули (3.13), ПЗПП адміністратора системи складає:

$$ПЗПП_1 = \frac{18000\ \text{грн}}{176\ \text{год}} = 102{,}27\frac{\text{грн}}{\text{год}}$$

Нижче буде прораховано погодинну зарплату інших співробітників ІТС. Зарплата програміста – 15000 грн, дизайнера – 13000 грн, бухгалтера і секретаря – 10000 грн:

$$ПЗПП_2 = \frac{15000\ \text{грн}}{176\ \text{год}} = 85{,}23\frac{\text{грн}}{\text{год}}$$

$$ПЗПП_3 = \frac{13000\ \text{грн}}{176\ \text{год}} = 73{,}87\frac{\text{грн}}{\text{год}}$$

$$ПЗПП_4 = \frac{10000\ грн}{176\ год} = 56{,}82\frac{грн}{год}$$

$$ПЗПП_5 = \frac{10000\ грн}{176\ год} = 56{,}82\frac{грн}{год}$$

Виходячи із отриманого результату, можемо розрахувати оплачувані витрати робочого часу за формулою (3.11):

$$\sum Зс = 122000\frac{грн}{місяць}$$

$$П_п = \frac{\sum Зс}{176\ год} \cdot 8\ год = 5545{,}45\ грн$$

Витрати на відновлення інформації і вузла можна знайти за формулами:

$$Пви = \frac{\sum Зви}{F} \cdot tви \quad (3.14)$$

$$Ппв = \frac{\sum Зпв}{F} \cdot tпв \quad (3.15)$$

де tпв – час, витрачений на повторне введення інформації, tпв – час, витрачений на відновлення вузла або сегмента мережі.

Умовно, для відновлення інформації і вузлів необхідно по 4 години на проведення кожної операції. Відновлення апаратних частин у даних формулах враховано не було, тобто, за формулами (3.14) та (3.15):

$$П_{ви} = \frac{\sum З_с}{176\ год} \cdot 4\ год = 2772{,}73\ грн$$

$$П_{пв} = П_{ви} = 2772{,}73\ грн$$

Витрати на зниження обсягу можемо найти за даною формулою:

$$V = \frac{O}{Fг} \cdot \text{час відновлення} \quad (3.16)$$

де Fг – річний фонд робочого часу роботи організації (стандарт: 2080 год), О - обсяг продажів атакованого вузла. Умовно було зазначено, що О = 450000 грн\рік.

Підставляючи дані можемо знайти даний елемент:

$$V = \frac{450000 \frac{\text{грн}}{\text{рік}}}{2080 \text{ год}} \cdot 8 \text{ год} = 1730{,}77 \text{ грн}$$

Знайдемо вартість відновлення працездатності вузла за формулою (3.12):

$$П_в = 2772{,}73 \text{ грн} + 2772{,}73 \text{ грн} = 5545{,}46 \text{ грн}$$

Можемо знайти упущену вигоду за формулою (3.10):

$$U = 5545{,}45 \text{ грн} + 5545{,}46 \text{ грн} + 1730{,}77 \text{ грн} = 12821{,}68 \text{ грн}$$

Отже, упущена вигода дорівнює 12821,68 грн. У описаних формулах не було взято до уваги витрати на апаратне відновлення.

Наступним етапом обґрунтування даної роботи буде розрахунок ефекту від впровадження системи інформаційної безпеки. Даний пункт можна знайти за наступною формулою:

$$E = B \cdot R - C \quad (3.17)$$

де В – загальний збиток від атаки, R – ймовірність реалізації атаки, С – поточні витрати на підтримку систем інформаційної безпеки. Знайти загальний збиток атаки необхідно за даною формулою:

$$B = \sum i \cdot \sum n \cdot U \quad (3.18)$$

де і – кількість атакованих вузлів, n – середнє число атак на рік.

За отриманими даними, на ІТС компанії за 2 роки було зроблено атаки на 6 вузлів. Було зроблено припущення, що за рік атака здійснюється на 3 вузли. За рік було зроблено 7 атак, тобто згідно формули (3.18):

$$B = 7 \text{ атак} \cdot 3 \text{ вузли} \cdot 12821{,}68 \text{ грн} = 269255{,}28 \text{ грн}$$

Ймовірність реалізації загрози складає 75%. Визначимо загальний ефект від систем інформаційної безпеки за формулою (3.17):

$$E = 269255{,}28 \text{ грн} \cdot 0{,}75 - 125483{,}57 \text{ грн} = 76457{,}89 \text{ грн}$$

Далі розрахуємо ефективність систем інформаційної безпеки за даною формулою:

$$ROSI = \frac{E}{K} \quad (3.20)$$

де Е – загальний ефект від впровадження систем інформаційної безпеки, К – капітальні інвестиції за варіантами, що забезпечили цей ефект. За умовою таблиці 3.1 і нижче описаних формул загальна сума на розробку КСЗІ складає 78996,96 грн. Отже можемо знайти даний елемент за формулою (3.20):

$$ROSI = \frac{76457{,}89 \text{ грн}}{78996{,}96 \text{ грн}} = 0{,}968$$

Останнім пунктом розрахування витрат на реалізацію КСЗІ буде прорахунок терміну окупності, який представляє собою час, необхідний для окуплення встановленних систем інформаційної безпеки і впроваджених політик. Даний елемент, можна розрахувати за даною формулою (3.20):

$$To = \frac{1}{ROSI} = \frac{1}{0,968} = 1,033 = 1 \text{ рік} \quad (3.21)$$

Тобто організації для окуплення систем інформаційної безпеки потрібен 1 рік.

Можна сказати, що так як дана компанія являє собою велику комерційну структуру, то можна надати певні рекомендації стосовно мінімізації витрат на розробку КСЗІ. Головними економічними чинниками даного підприємства будуть:

- Оптова закупівля ресурсів для реалізації КСЗІ;
- Проведення аудитів з питань безпеки інформації власноруч у простій та доступній формі;
- Залучення перевіреного та безкоштовного ПЗ для підтримки потоків інформації в ІТС (наприклад, безкоштовні програми резервного копіювання)

3.3 Висновки до розділу 3

Отже, у цьому розділі було проведено розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення (далі об'єкт проектування), розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування, визначення річного економічного ефекту від впровадження об'єкта проектування, визначення та аналіз показників економічної ефективності реалізацію запропонованих рішень (КСЗІ та політик безпеки).

Для реалізації КСЗІ і політик безпеки капітальні витрати компанії будуть складати 78996,96 грн. Експлуатаційні витрати дорівнюють 125483,57 грн на підтримку КСЗІ, політик безпеки та механізмів захисту.

У результаті реалізації даної системи інформаційної безпеки ефект від її реалізації буде складати 76457,89 грн. Збитки від реалізації атак на сегменти мережі та вузли складають 269255,28 грн. Порівнюючи ефект від реалізації систем захисту та упущених витрат від реалізації негативного впливу на ІТС можна сказати, що результат від впровадження КСЗІ буде максимально ефективним. Систем захисту компанії окупиться за 1 рік.

ВИСНОВКИ

Підводячи підсумки даної роботи можна сказати, що підприємства складають найважливішу інфраструктуру для підтримки економічного рівня будь-якої держави. Дані структури являються посередниками між суспільством і державою, надаючи велику кількість привілей: надання робочих міст, створення продукції, проектів, послуг тощо.

Проте дані організації будуть одними із перших, хто буде являтися жертвою нещасних випадків в сфері ІБ та інцидентів. Задля створення безпечних умов для існування даних компаній, держава повинна залучати органи, які займаються питаннями безпеки інформації.

В свою чергу органи повинні розробляти певні законопроекти, стандарти, правила та інші функції, які будуть забезпечувати безпечні умови для діяльності будь-якої організації.

На прикладі даної структури було розроблено стандарти ІБ підприємства, затверджених спеціалізованим органом з питань захисту інформації та телекомунікації. У роботі було створено нормативні документи і акти, які виявляють слабкі місця даного підприємства і запропоновано міри захисту, які знизять ризики реалізації зафіксованих загроз та вразливостей.

ПЕРЕЛІК ПОСИЛАНЬ

1. Нормативний документ СТЗІ. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. НД ТЗІ 1.1-005-07. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1 &art_id=102265&cat_id=46556&ctime=1344504841243

2. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.

3. Шаблоны политики безпеки. URL: https://www.sans.org/information-security-policy/

4. ПОСТАНОВА від 29 березня 2006 р. N 373. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. URL: https://zakon.rada.gov.ua/ laws/show/373-2006-%D0%BF

5. НД ТЗІ 1.3-001-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»

6. ДСТУ 2392-94 «Інформація та документація. Базові поняття. Терміни та визначення.»

7. ДСТУ 2732:2004 «Діловодство і архівна справа. Терміни та визначення»

8. Аудит інформаційної безпеки: підручник / В. А. Ромака, А. Е. Лагун, Ю. Р. Гарасим та ін. ; Держ. служба України з надзвич. ситуацій, Львів. держ. ун-т безпеки життєдіяльності, НАН України, Ін-т приклад. проблем механіки і

математики ім. Я. С. Підстригача. — Львів: Сполом, 2015. — 363 с. : іл. — Бібліогр.: с. 280—281 (37 назв). — ISBN 978-966-919-123-6

9. Антонюк А.О. Політика безпеки в захищених автоматизованих системах Наукові записки НаУКМА.-Київ: НаУКМА, 2003, т. 21, с.19-22.

10. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека. URL: http://bit.nmu.org.ua/ua/student/diplom/Метод_КРБ_125_2020.pdf

11. Державний стандарт України. ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання») / [На заміну ДСТУ 3008-95; чинний від 2017-07-01].- Київ: ДП «УкрНДНЦ», 2016. 31 с. URL: http://www.knmu.kharkov.ua/attachments/3659_3008-2015.PDF

12. Державний стандарт України. ДСТУ 8302:2015 “Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання” URL: http://lib.npu.edu.ua/files/dstu-8302-2015.pdf

13. Стандарти з інформації, бібліотечної і видавничої справи. URL: http://wwvv.library.univ.kiev.ua/ukr/about/dstu.html

14. ДСТУ ISO 5807:2016 Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів (ISO 5807:1985, IDT).

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	2	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	1 Розділ	27	
6	А4	2 Розділ	17	
7	А4	3 Розділ	16	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1. Пояснювальна записка Шайдулов Євгеній Сергійович.docx
2. Пояснювальна записка Шайдулов Євгеній Сергійович.pdf
3. Презентація Шайдулов Євгеній Сергійович.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

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

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Комплексна система захисту інформації інформаційно-телекомунікаційної системи приватного підриємства "Websofttonic"
Шайдулова Євгенія Сергійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 72 сторінках та містить 7 рисунків, 16 таблиць, 14 джерел та 4 додатка.

Мета роботи: визначення необхідності реалізації комплексу систем захисту інформації для підприємства, аналіз інформаційного поля компанії і розробка механізмів захисту в сфері інформаційної безпеки організації, розрахунок витрат на реалізацію проекту.

У кваліфікаційній роботі на прикладі даної структури було розроблено стандарти ІБ підприємства, затверджених спеціалізованим органом з питань захисту інформації та телекомунікації. У роботі було створено нормативні документи і акти, які виявляють слабкі місця даного підприємства і запропоновано міри захисту, які знизять ризики реалізації зафіксованих загроз та вразливостей.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

За час дипломування Шайдулов Є.С. проявив себе фахівцем, здатним

самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник Корнієнко Валерій Іванович