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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Павлова Сергія Олексійовича*

академічної групи *125-17-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Pure glycerin»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Кагадій Т.С.			
розділів:				
спеціальний	ст.викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер				

Дніпро
2021

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

«____»_____2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Павлову Сергію Олексійовичу*** **академічної групи** ***125-17-1***

(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Pure glycerin»***

Затверджую наказом ректора НТУ «Дніпровська політехніка» від *07.06.2021р.* №*317-С*

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи ТОВ «Pure glycerin», аналіз потенційних загроз і визначення послуг безпеки, які реалізуються КСЗІ*	19.04.2021-30.04.2021
Розділ 2	*Аналіз існуючого стану послуг безпеки в ІТС, розробка проектних рішень*	03.05.2021-21.05.2021
Розділ 3	*Економічне обґрунтування доцільності впровадження запропонованих рішень кваліфікаційної роботи*	24.05.2021-09.06.2021

Завдання видано _____ *Кагадій Т.С.*
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: *11.01.2021р.*

Дата подання до екзаменаційної комісії: *10.06.2021р.*

Прийнято до виконання _____ *Павлов С.О.*
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 87 с., 5 рис., 22 табл., 7 додатків, 22 джерела.

Об’єкт дослідження: ІТС ТОВ «Pure glycerin».

Мета роботи: забезпечення заданого рівня захисту інформації в ІТС ТОВ «Pure glycerin».

Методи дослідження: спостереження, аналіз, опис.

У першому розділі викладені загальні відомості про підприємство, визначено необхідність захисту інформації в ІТС і створення КСЗІ, виконано обстеження середовищ функціонування ІТС, проаналізовані модель порушників і модель загроз, визначені основні вимоги до послуг захищеності інформації, які необхідно забезпечити КСЗІ.

У спеціальній частині проаналізований існуючий стан реалізації послуг захищеності в ІТС, прийняті організаційно-технічних проектні рішення у вигляді двох варіантів захисту.

В економічному розділі визначені витрати на розробку КСЗІ, оцінені можливі збитки від атаки (злому) на сегмент корпоративної мережі, визначені та проаналізовані показники економічної ефективності впровадження КСЗІ.

Результати рішень кваліфікаційної роботи можуть бути застосовані для реалізації інформаційної безпеки в ІТС ТОВ «Pure glycerin» шляхом побудування КСЗІ, що призведе до зниження фінансових втрат при інцидентах інформаційної безпеки.

ІНФОРМАЦІЙНА БЕЗПЕКА, ОБ’ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБСТЕЖЕННЯ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ПОСЛУГИ БЕЗПЕКИ, КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ

РЕФЕРАТ

Пояснительная записка: 87 с., 5 рис., 22 табл., 7 прилож., 22 источников.

Объект исследования: информационно-телекоммуникационная система ООО «Pure glycerin».

Цель квалификационной работы: обеспечение заданного уровня защиты информации в ИТС ООО «Pure glycerin».

Методы, используемые при разработке: наблюдение, анализ, описание.

В первом разделе изложены общие ведомости о предприятии, определена необходимость в защите информации в ИТС и в создании КСЗИ, произведено обследование сред функционирования ИТС, проанализированы модель нарушителя и модель угроз, определены основные требования к услугам защищенности информации, которые необходимо обеспечить КСЗИ.

В специальной части проанализировано существующее состояние реализации услуг защищенности в ИТС, приняты организационно-технические проектные решения в виде двух вариантов защиты.

В экономическом разделе определены затраты на разработку КСЗИ, оценены возможные убытки от атак (взлома) на сегмент корпоративной сети, определены и проанализированы показатели экономической эффективности внедрения КСЗИ.

Результаты решений квалификационной работы могут быть использованы для реализации информационной безопасности в ИТС ООО «Pure glycerin» путём построения КСЗИ, что приведёт к снижению финансовых потерь при инцидентах информационной безопасности.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ОБЪЕКТ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ, ИНФОРМАЦИОННО-ТЕЛЕКОМУНИКАЦИОННАЯ СИСТЕМА, ОБСЛЕДОВАНИЕ, МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, УСЛУГИ БЕЗОПАСНОСТИ, КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ЕКОНОМИЧЕСКАЯ ЦЕЛЕСООБРАЗНОСТЬ

ABSTRACT

Explanatory note: 87 p., 5 figures, 22 tables, 7 supplements, 22 sources.

Object of study: information and telecommunication system of «Pure glycerin» LLC.

The purpose of the qualification work: ensure the specified level of information protection in the ITS of «Pure glycerin» LLC.

Methods that were used: observation, analysis, description.

The first part of the study presents general information about the company, identifies the necessity of the information protection in the information and telecommunication system. A survey of the functioning environments was carried out. Were analyzed threat and intruder model. The main requirements to security services which need to be provided by comprehensive information protection system (CIPS) were identified.

In the second part of the study current state of security services implementation in the ITS were analyzed. Were determined organizational and technical design decisions in the form of two protection variants.

In the economic part the costs of developing CIPS were identified, possible losses from the attack (hacking) on a segment of the corporate network were estimated, indicators of economic efficiency by the implementation of CIPS were calculated and analyzed.

Results of the qualification work can be used to implement information security in the ITS “Pure glycerin” LLC, which will reduce financial losses at the time of information security incidents.

INFORMATION SECURITY, OBJECT OF INFORMATION ACTIVITY, INFORMATION AND TELECOMMUNICATION SYSTEM, SURVEY, THREAT MODEL, INTRUDER MODEL, SECURITY SERVICES, COMPREHENSIVE INFORMATION PROTECTION SYSTEM, ECONOMIC FEASIBILITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ДБЖ – джерело безперебійного живлення;

ДТЗС – допоміжні технічні засоби і системи;

ЗЕД – зовнішня економічна діяльність;

ЗУ – закон України;

ІТС – інформаційно-телекомунікаційна система;

КЗ – контрольована зона;

КЗЗ – комплекс засобів захисту;

КС – комп'ютерна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціоновані дії;

ОІД – об'єкт інформаційної діяльності;

ОТЗ – основні технічні засоби;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ТЗІ – технічний захист інформації.

ЗМІСТ

С.

ВСТУП

На сьогоднішній день повноцінне функціонування сучасних підприємств не можливо уявити без використання обчислювальної техніки та систем зв'язку. Кожне підприємство реалізує свої функції з використання інформаційно-телекомунікаційних систем, в яких може оброблюватись інформація з різним рівнем доступу – відкрита і з обмеженим доступом. В такому разі актуальною постає задача захисту інформації.

Практичні реалізації захисту інформації потребують постійного опрацювання.

В сучасних реаліях питання практичної реалізації захисту інформації потребують постійного опрацювання. Відсутність достатнього рівня захищеності пояснюється через необхідність вкладення капітальних затрат на систему безпеки інформації, відсутність ясності доказу своєї значимості та відсутності розуміння необхідних рішень і методів. Несвоєчасне вирішення таких питань може призвести до виникнення подій порушення властивостей інформації, що призведе до великих фінансових втрат або навіть до припинення функціонування підрозділів. Саме тому забезпечення інформаційної безпеки на підприємстві ТОВ «Pure glycerin» являється актуальним завданням.

Так як на підприємстві на сьогоднішній день відсутні рішення комплексного підходу до забезпечення безпеки інформації було вирішено впровадити комплексну систему захисту інформації. Це дозволить підприємству уникнути збитків внаслідок атак і забезпечить економічну вигоду.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості

Об’єктом інформаційної діяльності є СЕО підрозділ підприємства «Pure glycerin».

«Pure glycerin» - приватне підприємство, яке займається управлінням виробництва з очистки гліцерину після виробничих процесів.

Організаційна структура управління підприємством зображена на рисунку 1.1.

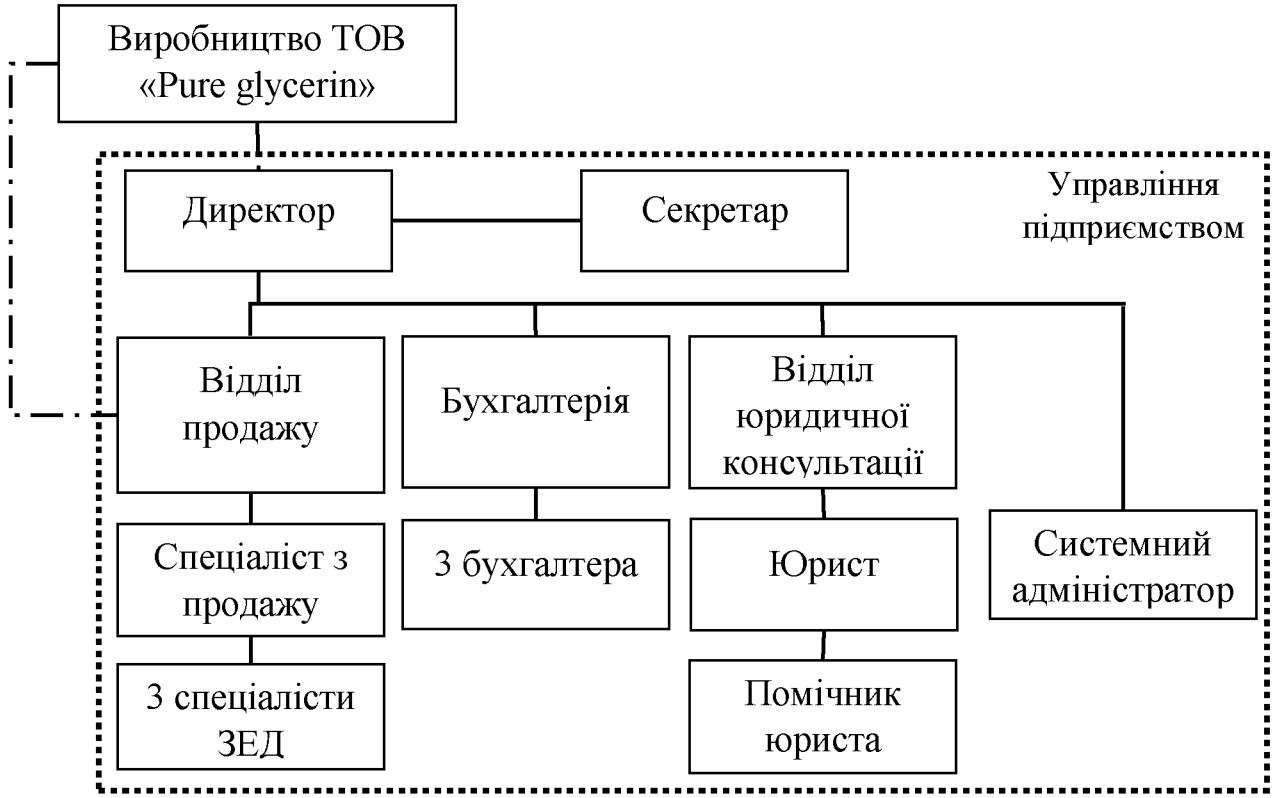


Рисунок 1.1 – Організаційна структура управління підприємством

Кімната підрозділу розташовується на 6 поверсі третьої вежі торгового центру «Вавилон».

Підрозділ працює з понеділка по п’ятницю з 8:30 до 17:30.

Кількість штатних співробітників – 11.

1.2 Обґрунтування необхідності створення КСЗІ в ІТС

Для розуміння причин необхідності захисту інформації на підприємстві, відношення суб'єктів і об'єктів захисту, потрібно виконати аналіз нормативно-правових актів, на підставі яких можуть формуватися вимоги захисту або встановлюватися обмеження доступу до певних видів інформації.

Згідно ЗУ «Про інформацію» статті 20 пункту 1: за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

Згідно статті 21 ЗУ «Про інформацію» [1] Інформація з обмеженим доступом:

1) Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація;

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

Згідно ЗУ «Про захист персональних даних» статті 5 пункту 1 об'єктами захисту є персональні дані.

Згідно ЗУ «Про захист персональних даних» [2] статті 10 пункту 2: використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

Згідно ЗУ «Про захист інформації в ІТС» [3] статті 5: власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Згідно Цивільного Кодексу України [4] статті 505: поняття комерційної таємниці.

1) Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

2) Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Так як в ІТС ТОВ «Pure glycerin» обробляється ІзОД, а саме – комерційна таємниця і персональні дані, її необхідно захистити.

Для полегшення формування вимог до КЗЗ ІТС, необхідно виконати її класифікацію згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [5]. АС на підприємстві відповідає ознакам класу 3.

Необхідно побудувати КСЗІ для виконання вимог захисту інформації.

Порядок проведення робіт і комплексу взаємоузгоджених заходів із впровадження КСЗІ в ІТС визначено у НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» [6]. Згідно НД ТЗІ 3.7-003-05 необхідно провести обстеження середовищ функціонування ІТС, а саме таких її складових:

- фізичного середовища;
- обчислювальної системи;
- інформаційного середовища;
- середовища користувачів.

На основі результаті обстеження необхідно:

- розробити модель загроз;
- виконати аналіз актуальних загроз;
- розробити політику безпеки;
- запропонувати проектні рішення щодо реалізації послуг безпеки.

Створення і впровадження КСЗІ гарантує зниження економічних втрат підприємства від реалізації потенційних загроз, визначених на етапі аналізу моделі загроз і модулі порушника.

1.3 Обстеження середовищ функціонування ІТС на ОІД

ОІД розташований за адресою: м.Дніпро, вул. Маршала Малиновського, 2, в торговому комплексі «Вавилон» на 6 поверсі 3 вежі. ОІД складається з кімнат: юриста, бухгалтерії, директора, серверної. Також з основного приміщення для спеціалістів(open space) і з кімнату для перемов.

Згідно НД ТЗІ 1.6-005-2013 [7] було проведено категоріювання приміщення, на якому здійснюється обробка технічними засобами ІзОД, що не становить державної таємниці. ОІД відноситься до 4 категорії. Акт категоріювання можна побачити у додатку Г.

1.3.1 Фізичне середовище

Проведемо опис ситуаційного плану ОІД

На рисунку Б.1 у додатку Б зображено ситуаційний план ОІД. Умовні позначення ситуаційного плану зображено на рисунку Б.2 в додатку Б.

З північного заходу від ОІД на відстані 150 м. знаходиться Слобожанський проспект і Центральний міст з інтенсивним транспортним потоком. З південного заходу знаходиться провул. Маршала Малиновського з парком і виходом до річки Дніпро. Поблизу торгового комплексу присутні місця для паркування транспортних засобів.

У таблиці 1.1 наведено сусідні будівлі відносно ОІД.

Територія навколо торгового комплексу впорядкована, асфальтована. Фундамент розташований на палях. Вся поверхня даху плоска і покрита

гідроізоляційним руберойдом. Торгівельний центр «Вавилон» відкритий з 7.00 до 23.00.

Таблиця 1.1 – Характеристика сусідніх будівель та споруд

Найменування	Кількість поверхів	Адреса	Відстань від ОІД, м
1. Житлова будівля	12	Пров. Любарського, 6	190
2. Житлова будівля	12	Пров. Любарського, 20	180
3. Житлова будівля	9	Пров. Любарського, 18	185
4. Житлова будівля	12	Пров. Любарського, 16	188
5. Житлова будівля	9	Пров. Любарського, 14	192
6. Житлова будівля	12	Пров. Любарського, 12	212
7. Житлова будівля	9	Пров. Любарського, 8	230
8. Житлова будівля	12	Пров. Любарського, 8	240
9. Житлова будівля	9	Пров. Любарського, 4а	275
10. Аквасфера	1	Пров. Любарського, 6а	170
10. Humana	2	Пров. Любарського, 20а	150
11. Анімалія	1	Пров. Любарського, 18	163
13. Ательє кераміки	1	Пров. Любарського, 16а	161
14. Укрпошта	1	Пров. Любарського, 14	170
15. Тріплекс	2	Пров. Любарського, 12а	180
16. Круазе	2	Пров. Любарського, 8	210
17. Кафе/бар Caramel	2	Пров. Любарського, 10	220
18. Автомийка	1	Пров. Любарського, 6а	240
19. 3 Державна пожежно-рятувальна частина	3	Пров. Любарського, 6	210
20. Шиномонтажна майстерня	1	Пров. Любарського, 4б/1	210
21. Автостоянка	1	Пров. Любарського,	220

		4б/2	

Продовження таблиці 1.1

Найменування	Кількість поверхів	Адреса	Відстань від ОІД, м
22. Магазин електроніки	1	Вул. Маршала Малиновського, 4	185
23. Адміністративна будівля	1	-	200
24. Адміністративна будівля	1	-	190
25. Адміністративна будівля	1	-	225
26. 7 вежа торгового комплексу «Вавилон»	7	Вул. Маршала Малиновського, 2	130
27. 6 вежа торгового комплексу «Вавилон»	7	Вул. Маршала Малиновського, 2	100
28. 5 вежа торгового комплексу «Вавилон»	7	Вул. Маршала Малиновського, 2	90
29. 4 вежа торгового комплексу «Вавилон»	7	Вул. Маршала Малиновського, 2	70
30. 2 вежа торгового комплексу «Вавилон»	7	Вул. Маршала Малиновського, 2	30

КЗ обмежена периметром поверху – стіни, стеля, підлога, вікна і двері.

Для описання режиму КЗ використаємо розподілення умов функціонування ОІД у час робочий час і в не робочий час.

У робочий час режим КЗ забезпечується співробітниками, які перебувають на території ОІД.

У не робочий час режим КЗ забезпечується силами групи швидкого реагування торгового комплексу з використанням системи сигналізації і відеоспостереження комплексу. Система сигналізації ОІД виконана на базі ПКП

«Лунь-9Р», до якого підключений індикатор зон «Линд-8». «Линд-8» налаштований на блокування і розблокування системи сигналізації за допомогою зчитування апаратних ключів, які видаються системним адміністратором. Журнал виданих ключів находиться у секретаря в столі.

Доступ до ОІД мають усі працівники, наймані працівники, обслуговуючий персонал, а також гості, які мають бути записані на відповідний час у секретаря.

До будівлі, в якій знаходиться ОІД, підключені наступні зовнішні комунікації:

– система електропостачання, яка підключена до трансформаторних підстанцій (ТП-1 і ТП-2) всередині торгового комплексу. Має підключення сторонніх споживачів;

– система заземлення, заземлювач якої розташовується під торговим комплексом «Вавилон» і під'єднується до розподільчих щитків вежі;

– система водопостачання, яка підключена до міської системи. Введення до будівлі виконано через підземні комунікації до підвального приміщення торгового комплексу;

– система каналізації, яка підключена до міської системи. Введення до будівлі виконано через підземні комунікації до підвального приміщення торгового комплексу;

– система газопостачання, яка підключена від міської системи від міської системи газопостачання підземними комунікаціями до газорозподільчого пункту, який під'єднується надземною трубою до торгового центру;

– система мережі Інтернет, яка забезпечується провайдерами «Київстар», «Forsage», «Фрегат», «Фринет», «Укртелеком» за допомогою підземних комунікацій до підвального приміщення торгового комплексу.

Окрім зовнішніх комунікацій, що під'єднуються до будівлі, в якій розташовується ОІД, підключені наступні внутрішні комунікації:

– автономна система вентиляції і кондиціювання , яка забезпечується за допомогою блоків автономного кондиціювання і труб;

– система опалення, яка входить в систему вентиляції і кондиціювання комплексу, яка забезпечується завдяки утепленим трубам опалення;

– система охорони комплексу, яка забезпечується системою відеоспостереження, пристроями контролю і управління доступом на дверях поверхів вище першого і групою швидкого реагування.

Проведемо опис генерального плану ОІД.

На рисунку Б.3 у додатку Б зображено генеральний план ОІД. Умовні позначення генерального плану зображено на рисунку Б.4 в додатку Б.

Площа ОІД – 140,1 м^2.

Зовнішні стіни будівлі, в якій розташований ОІД, цегляні (250 мм). Внутрішні стіни в офісі з скла (товщина 8 мм).

Металопластикові вікна з одинарним склопакетом (20 штук 800 мм·1200 мм, серед яких 4 одностулкових вікон що відкриваються, інші - глухі), мають горизонтальні металеві жалюзі.

Вхідні двері металеві (1 м·2.3 м, товщина – 40 мм) з врізним металевим замком.

Підлога і стеля з залізобетону. Стеля навісна «Армстронг», загальна висота стелі – 3 м, висота з навісною стелею – 2.7 м. Підлога вкрита ламінатом.

На рисунку Б.5 у додатку Б зображені технічні системи охоронної сигналізації, системи освітлення і системи пожежної сигналізації. Умовні позначення технічні системи генерального плану зображено на рисунку Б.6 в додатку Б.

За організаційним порядком на підприємстві до серверної кімнати може заходити тільки системний адміністратор за допомогою ключа від серверної, який знаходиться у директора в столі, і прибиральниця під наглядом. До інших кімнат на підприємстві немає обмежень щодо доступу.

В додатку В у таблиці В.1 наведено перелік і характеристики ОТЗ.

В додатку В у таблиці В.2 наведено перелік і характеристики ДТЗС.

Комп'ютери розташовані на столах працівників. Комутатор розташований на стіні біля секретаря. Сервери розташовані в серверній на підлозі.

В ОІД наявні мобільні пристрої співробітників, які використовуються для ведення перемов з клієнтами.

Папка з паперовими носіями інформації зберігається в столі секретаря. Бухгалтерські звіти зберігаються в дерев'яній шафі бухгалтерії. Запасні ключі до приміщення і ключі до панелі охорони Лунь зберігаються в столі директора. На столах і шафах замки та пристрої для опломбовування не використовуються. Регламентовані місця для зберігання зовнішні сторонніх носіїв на ОІД відсутні.

Лінія електроживлення ОТЗ і ДТЗС та освітлення виходить за межі ОІД до поверхового щитка перед вхідними дверима. Поверховий щиток через поверхи нижче підключений до розподільчого щитку вежі, який підключений до трансформаторних підстанцій (ТП) торгового комплексу ТП-1 і ТП-2 (рисунок Б.1) і системи міського електроживлення.

Освітлення на ОІД здійснюється за допомогою люмінесцентних ламп, які розташовані на стелі.

Система опалення і вентиляції проходять однаковим шляхом розповсюдження на ОІД і всередині торгового комплексу. Система опалення включає в себе нагнітаючі труби від автономної системи опалення торгового центру. Опалення здійснюється за допомогою потоків гарячого повітря, які мають виходи труб на ОІД під навісною стелею. Система вентиляції складається з труб і вентиляційних решіток, які виходять на ОІД під навісною стелею Труби системи опалення і вентиляції виходять за межі території КЗ.

Система пожежною сигналізації включає в себе датчики диму (9 штук), які являються частиною загальної системи пожежної безпеки торгового комплексу «Вавилон». ОІД обладнаний вогнегасниками.

Комп'ютерна мережа дротова (кручена пара), виконана на базі комутатора. Комутатор підключений до технічного поверху, де під'єднується до мережевого обладнання провайдера «Київстар». У мережевого обладнання провайдера присутні сторонні споживачі.

1.3.2 Обчислювальна система

На рисунку 1.2 зображена структурна схема обчислювальної системи підприємства.

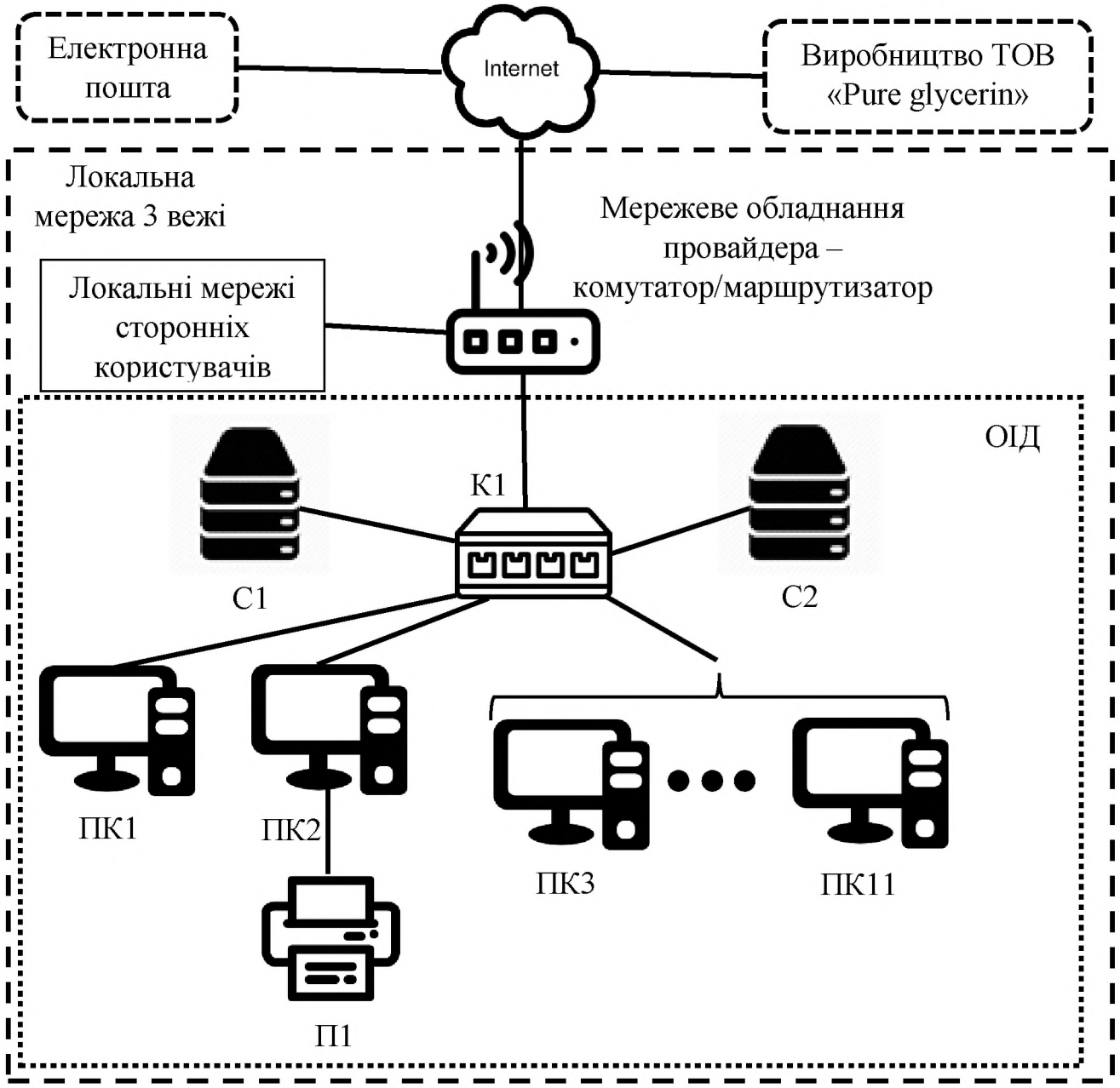


Рисунок 1.2 – Структурна схема обчислювального середовища

В додатку В у таблиці В.2 описані характеристики апаратних засобів ІТС.

На ОІД відсутні місця зберігання сторонніх зовнішніх носіїв. Обчислювальна система взаємодіє з стороннім поштовим сервером Google (електронна пошта з використанням безпечного підключення за допомогою протоколу HTTPS і TLS).

Локальна обчислювальна система складається з 11 комп'ютерів і 2 серверів (С1 сервер для роботи з 1С; С2 для зберігання файлів, резервних копій). Комп'ютерна система однорангова, усі комп'ютери і сервери підключені крученою парою, яка розташовується над навісною стелею, до комутатора К1. Комутатор підключений до локальної мережі 3 вежі через мережеве обладнання провайдера, яке видає динамічні IP-адреса і виконує маршрутизацію даних. До локальної мережі 3 вежі підключені сторонні споживачі (інші організації і підприємства).

Локальна комп'ютерна мережа взаємодіє через мережу Інтернет з заводом (виробництво) з очистки гліцерину за допомогою електронної пошти і телефонів.

Кожен користувач має доступ до свого комп'ютера за допомогою пароля, який формує і видає системний адміністратор. Усі паролі зберігаються у файлі системного адміністратора на ПК4.

Системний адміністратор виконує ручне оновлення ПЗ наприкінці робочого тижня (в п'ятницю).

У таблиці 1.2 наведено перелік та основні характеристики ПЗ, яке використовується на ОТЗ.

Таблиця 1.2 – Перелік ПЗ та характеристики в ІТС

Назва	Тип	Ліцензія	Де встановлено
Adobe Acrobat Reader DC 21.001.20142	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
CCleaner 5.77	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
Google Chrome 88.0.4324.190	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
IranView 4.53	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
Kaspersky Small Office Security 21.3.10.391	Спеціалізоване	Комерційна	ПК1, ПК2 …ПК11

Microsoft Edge 89.0.774.45	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11

Продовження таблиці 1.2

Windows 10 Professional 2004 19041.867	Системне	Комерційна, 29.03.22(дата закінчення)	ПК1, ПК2 …ПК11
Пакет програм Microsoft Office 2013 16.0.12430.20288	Прикладне	Комерційна, 13.08.21(дата закінчення)	ПК1, ПК2 …ПК11
Realtek Audio Console 29.11.2019	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
K-Lite Mega Codec Pack 15.3.5	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
VLC media player 3.0.7.1	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
WinRAR 5.80.0	Прикладне	Безкоштовно	ПК1, ПК2 …ПК11
Windows Server Essential 20H219042.508.200927-1902	Системне	Комерційна	С1, С2
Microsoft Dynamics NAV 2018	Прикладне	Комерційна	ПК5, ПК6, ПК7
Платформа 1С 8.3.18	Прикладне	Комерційна	ПК1, ПК2… ПК11, С1
Бухгалтерія 1С 2.0.23.1 (17.12.2020)	Прикладне	Комерційна	ПК2, ПК3
MS SQL Server 15.0.2000.5	Системне	Комерційна	С2
MS SQL Server Management Studio	Системне	Комерційна	С2

1.3.3 Інформаційне середовище ОІД

У таблиці 1.3 описана і класифікована інформація, яка циркулює на підприємстві.

Таблиця 1.3 – Класифікація інформації, яка циркулює в ІТС

Інформація	Вид представ-лення в ІТС	Режим доступу	Правовий режим	Вимоги до захисту		
				К	Ц	Д
1. Інформація про співробітників, копії персональних даних персоналу	Паперовий, електронний	ІзОД	Конфіден-ційна (персональні дані)	3	2	3
2. Інформація про закази	Електронний	ІзОД	Комерційна	3	3	3
3. Інформація о клієнтах	Електронний	ІзОД	Комерційна	3	3	3
4. Бухгалтерські звіти	Паперовий, електронний	ІзОД	Комерційна	4	4	3
5. Документи ЗЕД	Електронний	ІзОД	Комерційна	4	3	3
6. Інформація про послуги підприємства	Електронний	Відкрита	Відкрита	1	1	1
7. Інформація про імпорт/експорт продукції, матеріалів	Електронний	ІзОД	Комерційна	4	3	3

Продовження таблиці 1.3

Інформація	Вид представлення в ІТС	Режим доступу	Правовий режим	Вимоги до захисту		
				К	Ц	Д
8. Організаційно-розпорядчі документи	Паперовий, електронний	ІзОД	Конфіденційна інформація	1	2	1
9. Технологічна	Електронний	ІзОД	Конфіденційна	3	3	3

Примітка. Слід зазначити, що уся інформація в системі, окрім зазначеного виду, представлена у вигляді електронних полів, електромагнітних полів та у вигляді видової інформації на моніторах комп'ютерів.

Для класифікації інформації були використані переліки рівнів властивостей інформації.

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.

Визначимо технологію обробки інформації на підприємстві.

Інформація про співробітників, копії персональних даних персоналу: добавляються у систему під час найму нових працівників у електронному вигляді на ПК секретаря і в паперовому вигляді у папку, яка розташована у столі секретаря. Інформація може змінюватися, редагуватися, видалятися секретарем власноруч, або секретарем внаслідок звернення від співробітників.

Інформація про закази створюється і вноситься у систему секретарем після розмови з клієнтами у кімнаті для перемов або під час телефонного зв’язку до

бази даних на сервері С2 або за допомогою відсилання даних на корпоративну пошту з подальшою співбесідою. Інформація про закази може змінюватися, редагуватися і копіюватися секретарем, спеціалістами ЗЕД, спеціалістом з продажу, юристом, помічником юриста.

Інформація о клієнтах створюється і вноситься у систему секретарем після розмови з клієнтами у кімнаті для перемов або під час телефонного зв'язку до бази даних на сервері С2 або за допомогою відсилання даних на корпоративну пошту з подальшою співбесідою. Юрист і помічник юриста можуть отримати інформацію о клієнтах.

Бухгалтерські звіти створюються, змінюються і видаляються бухгалтерами щомісячно, щоквартально, а також включають в себе відрахування зарплат згідно відрядно-преміальної оплати праці.

Документи ЗЕД створюються, редагуються, видаляються спеціалістами ЗЕД і спеціалістом з продажу, передаються бухгалтерам для звітів. Юрист і помічник юриста можуть отримати інформацію о ЗЕД.

Інформація про послуги підприємства розташовується на сайті-візитці підприємства на сторонньому хостингу.

Інформація про імпорт/експорт продукції, матеріалів створюється, змінюється і видаляється спеціалістами ЗЕД та спеціалістом з продажу, передається бухгалтерам для звітів і юристам для надання юридичної консультації. Інформація про імпорт/експорт продукції включає в себе договори купівлі-продажу, які підписуються клієнтами після переведення коштів за заказ.

Інформація про організаційно-розпорядчі документи створюється секретарем і директором, підписується всіма працівниками підприємства, роздруковується на принтері П1, паперові документи або копії зберігаються у шафі директора.

Технологічна інформація створюється, змінюється і видаляється системним адміністратором. Паролі видаються всім користувачам і зберігаються у системного адміністратора. Інформація про розмежування доступу зберігається на

ПК4 і змінюється системним адміністратором. Інформація про реєстр, паролі, конфігурацію систем розташовується і зберігається на ПК1 – ПК11, С1, С2.

Будь-яка інформація може бути переглянута директором при запиті в бухгалтерію, до секретаря, до юристів або до спеціалісту з продаж, а також надається у вигляді звітів.

Резервне копіювання інформації 2, 3, 4, 5, 7 з таблиці 6 проводиться автоматично наприкінці робочого дня на сервер С2.

На рисунку 1.3 зображені інформаційні потоки підприємства.

1.3.4 Середовище користувачів

Позаштатними працівниками являються електрик, сантехник, персонал провайдеру Інтернет, охорона торгового комплексу і прибиральник. Прибиральник має доступ до кімнат наприкінці робочого дня і розписується у

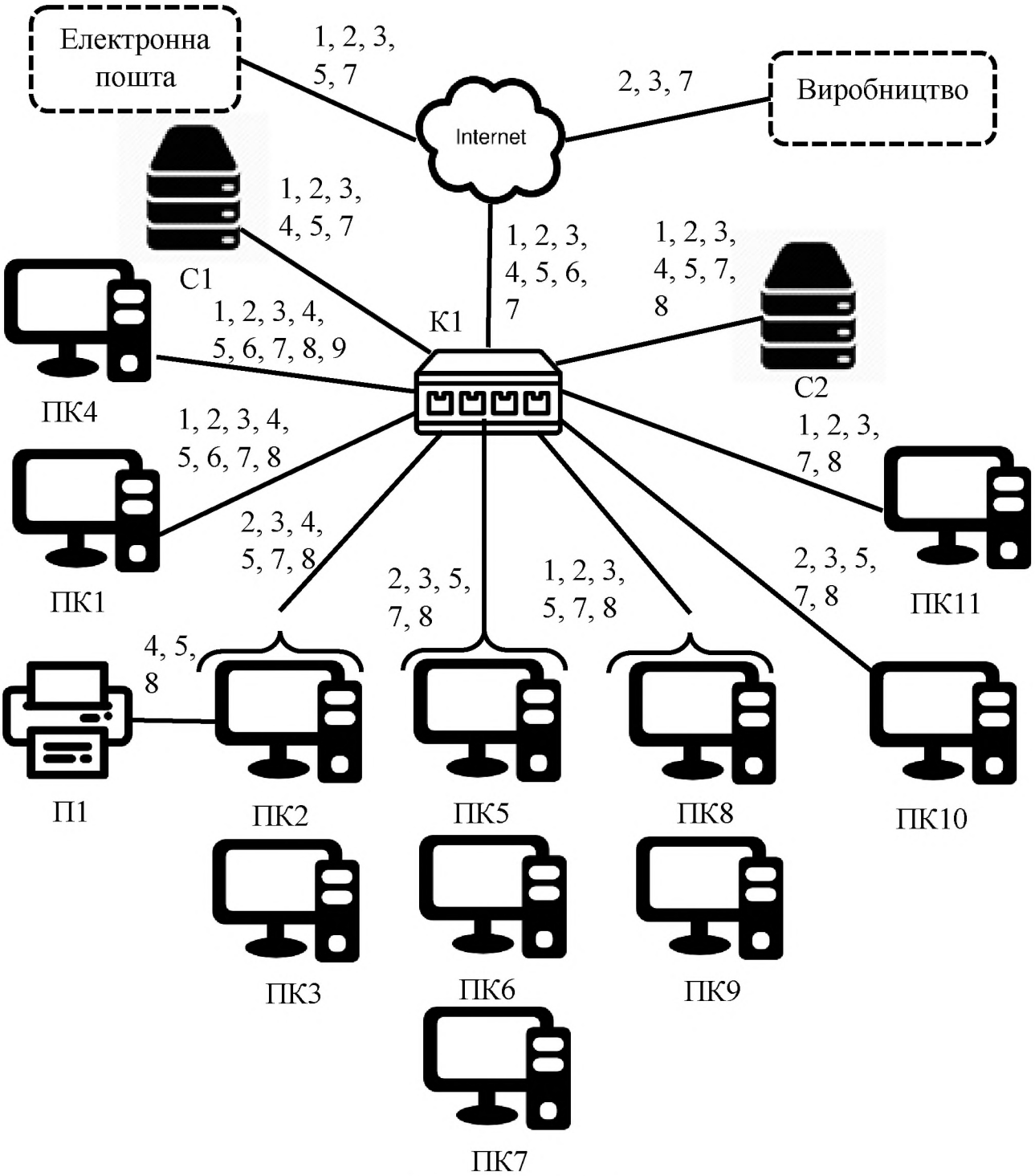


Рисунок 1.3 – Інформаційні потоки

журналі прибирання в кімнаті перед входом до ОІД.

У таблиці 1.4 описані штатні працівники підприємства.

Таблиця 1.4 – Характеристика працівників

Посада	Ідентифікація в системі за групою	Рівень кваліфікації	Кількість працівників
Директор	Група користувачів 4	Середній	1
Юрист	Група користувачів 2	Середній	1
Помічник юриста	Група користувачів 2	Середній	1
Спеціаліст з продажу	Група користувачів 1	Середній	1
Спеціаліст ЗЕД	Група користувачів 1	Середній	3
Секретар	Група користувачів 5	Середній	1
Бухгалтер	Група користувачів 3	Середній	2
Системний адміністратор	Системний адміністратор	Високий	1

Обов’язки директора:

– затвердження комерційних пропозицій від сторонніх організацій, що надають послуги по комунікаційнім, програмному й апаратному оснащенню підприємства;

– координувати всі види діяльності підприємства.

Обов’язки юриста:

– підтримання і оновлення існуючої документації, актів і політик на підприємстві;

– перевірка правильності складання юридичних документів;

– надання консультаційних змін у договорах і політиках підприємства;

– ведення ділових перемов із сторонніми організаціями;

– супроводження договорів із сторонніми організаціями;

– надання юридичних послуг стороннім організаціям, що оформили заказ.

Обов'язки помічника юриста:

– допомога юристу у веденні юридичних справ;

– ведення планування і звітності крайніх термінів виконання юридичних справ;

– допомога секретарю у разі найму працівників.

Обов'язки спеціаліста з продажу:

– ведення перемов (онлайн зустрічі, перемови на підприємстві, листування поштою) із клієнтами;

– супроводження договорів клієнтів;

– моніторинг тенденцій ринку;

– організація щомісячних, квартальних та річних звітів відділу продажу;

Обов'язки спеціаліста ЗЕД:

– імпорт і експорт необхідного матеріального забезпечення компанії;

– взаємодія із іноземними постачальниками;

– ведення обліку вартості імпортованої і експортованої продукції;

– підготовка документів митного оформлення вантажів;

– переклад технічної та внутрішньої документації.

Обов'язки бухгалтера:

– організація бухгалтерського обліку господарсько-фінансової діяльності підприємства, контроль за використанням матеріальних, трудових та фінансових ресурсів;

– забезпечення і контроль за обліком та звітністю на підприємстві;

– організовує та контролює складання розрахунків щодо використання прибутків, затрат на виробництво, платежів;

– контроль оформлення бухгалтерських звітів, документів, розрахунків та платіжних зобов'язань;

– організація щомісячного бухгалтерського обліку, квартальних та річних бухгалтерських звітів.

Обов'язки системного адміністратора:

– забезпечення належного функціонування та працездатності комп'ютерної мережі, програмного і апаратного забезпечення підприємства;

– підготовка та збереження резервних копій даних, їх періодичне знищення та оновлення;

– встановлення і конфігурування оновлень програмного забезпечення;

– встановлення, модифікація, конфігурування нового апаратного і програмного забезпечення;

– відповідальність за автоматизовані процеси програмного забезпечення;

– створення, облік і зміна облікових записів користувачів та їх доступу в комп'ютерній системі;

– забезпечення інформаційної безпеки організації;

– усунення нештатних ситуацій, неполадок в комп'ютерній системі;

– налаштування і підтримка працездатності серверів.

Обов'язки секретаря:

– ведення діловодства, в тому числі і в електронній формі;

– допомога директору у разі необхідності;

– приймання відвідувачів на підприємстві;

– оформлення заказів від відвідувачів.

Прибиральниця, сантехнік, електрик, персонал провайдера Інтернету – представники зовнішніх організацій, які залучаються за необхідністю і можуть перебувати в приміщенні лише при наявності внутрішніх працівників організації.

Розмежування повноважень доступу до інформації описано у таблиці 1.5 (інформація відповідає номерам інформації у таблиці 1.3).

Таблиця 1.5 – Матриця розмежування доступу

Об'єкт	Інформація									Повноваження інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9		
Директор	Ч	Ч	Ч	Ч	Ч	Ч	Ч	ЧС МВ ТД	Ч	Так	ПК1… ПК11, С1, С2
Юрист	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	-	ЧС МВ ТД	Ч	ЧС МВ ТД	ЧС МВ ТД	-	Так	ПК8
Помічник юриста	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	-	ЧС МВ ТД	Ч	ЧС МВ ТД	ЧС МВ ТД	-	Так	ПК9
Спеціаліст з продажу	-	ЧС МВ ТД	ЧС МВ ТД	-	ЧС МВ ТД	Ч	ЧС МВ ТД	ЧС МВ ТД	-	Так	ПК10
Спеціаліст и ЗЕД	-	ЧС МВ ТД	ЧС МВ ТД	-	ЧС МВ ТД	Ч	ЧС МВ ТД	ЧС МВ ТД	-	Так	ПК5, ПК6, ПК7
Секретар	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	-	-	Ч	-	ЧС МВ ТД	-	Так	ПК11
Бухгалтер	-	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	Ч	ЧС МВ ТД	ЧС МВ ТД	-	Так	ПК2, ПК3
Системний адміністратор	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	ЧС МВ ТД	Так	ПК1… ПК11, С1, С2

Умовні позначення доступу до інформації:

Ч – читання;

С – створення нових файлів;

М – редагування;

В – видалення.

Т – імпорт/експорт;

Д – друк.

1.4 Аналіз загроз інформації

Для складання моделі загроз для інформації, яка циркулює в ІТС необхідно визначити джерела реалізації загроз, вразливості, через які можлива реалізація загрози ІТС, і потенційні загрози інформації.

1.4.1 Аналіз порушників

Згідно НД ТЗІ 1.1-003-99 [8] порушник – це користувач, який здійснює несанкціонований доступ до інформації.

Враховуючи особливості середовища ІТС можна виділити наступні групи потенційних порушників:

– внутрішні особи, які мають безпосередній доступ до технічних засобів, на яких обробляється ІзОД, або обслуговують такі засоби;

– зовнішні особи, які знаходяться за межами КЗ, проте мають можливість фізичного підключення до каналів зв'язку або інших складових мережі передачі даних.

Із такого розподілу порушниками можуть бути як внутрішні співробітники ІТС так і внутрішні особи, які проникли шляхом НСД в її межи.

Для подальшої класифікації порушників використаємо наступні параметри:

– мета і мотив порушення;

– рівень знань про ІТС – його кваліфікація і освідомлення про структуру і механізми технічних засобів ІТС;

– рівень можливостей порушника – його можливі методи і засоби НСД та перехоплення інформації;

– час дії по відношенню до функціонування ІТС;

– місце дії – можливості щодо території доступу, в якій можуть знаходитись технічні засоби;

Для спрощення визначення рівня загроз від порушників і їх параметрів використаємо наступні таблиці: таблиці 1.6, таблиці 1.7, таблиці 1.8, таблиці 1.9, таблиці 1.10, таблиці 1.11.

Таблиця 1.6 – Категорії порушників

Позначення	Визначення категорії	Рівень загроз
Внутрішні по відношенню до ІТС		
ПВ1	Технічний персонал, який обслуговує будови та приміщення (прибиральники)	1
ПВ2	Група користувачів 1 в ІТС	2
ПВ3	Адміністратори ІТС, співробітники служби захисту інформації, група користувачів 2, 3, 4 в ІТС	3
ПВ4	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні по відношенню до ІТС		
ПЗ1	Відвідувачі (запрошені з будь-якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго-, водо-, теплопостачання і таке інше)	2
ПЗ3	Хакери, зовнішні організації, які підключені до провайдера	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 1.7 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення	Рівень загроз
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3

М4	Професійний обов'язок (ПЗ4)	4

Таблиця 1.8 – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

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

Таблиця 1.9 – Специфікація моделі порушника за показником можливостей використання засобів, методів подолання системи захисту

Позначення	Характеристика можливостей порушника	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів)	3

Продовження таблиці 1.9

Позначення	Характеристика можливостей порушника	Рівень загроз
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 1.10 – Специфікація моделі порушника за часом дії

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

Таблиця 1.11 – Специфікація моделі порушника за місцем дії

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

В таблиці 1.12 наведена класифікація порушників ІТС.

Найбільшу загрозу від внутрішніх працівників представляють директор і системний адміністратор.

З боку зовнішніх порушників найбільшу загрозу можуть мати представники обслуговуючого персоналу, хакери, зовнішні організації, які підключені до провайдера і агенти конкурентів під прикриттям.

Таблиця 1.12 – Модель порушника

Порушник	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	М2	К2	З1	Ч3	Д3	14
	3	2	2	1	3	3	
Юрист	ПВ3	М1	К2	З1	Ч1	Д2	10
	3	1	2	1	1	2	
Помічник юриста	ПВ3	М2	К1	З1	Ч1	Д2	10
	3	2	1	1	1	2	
Спеціаліст з продажу	ПВ2	М1	К2	З1	Ч1	Д2	9
	2	1	2	1	1	2	
Спеціаліст ЗЕД	ПВ2	М1	К2	З1	Ч1	Д2	9
	2	1	2	1	1	2	
Секретар	ПВ2	М1	К2	З1	Ч2	Д2	10
	2	1	2	1	2	2	
Бухгалтер	ПВ3	М1	К2	З1	Ч1	Д2	9
	3	1	2	1	1	2	

Продовження таблиці 1.12

Порушник	Категорія порушника	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання системи захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Системний адміністратор	ПВ3	М1	К4	З1	Ч4	Д4	17
	3	1	4	1	4	4	
Прибиральник	ПВ1	М1	К1	З2	Ч1	Д1	7
	1	1	1	2	1	1	
Відвідувач, замовник	ПЗ1	М3	К1	З3	Ч1	Д1	10
	1	3	1	3	1	1	
Технічний персонал, що обслуговує будови і приміщення	ПЗ2	М3	К2	З3	Ч2	Д2	14
	2	3	2	3	2	2	
Хакери	ПЗ3	М3	К3	З3	Ч4	Д1	17
	3	3	3	3	4	1	
Зовнішні організації, які підключені до провайдера	ПЗ3	М3	К3	З3	Ч4	Д4	20
	3	3	3	3	4	4	
Агенти конкурентів під прикриттям	ПЗ4	М4	К3	З3	Ч1	Д1	16
	4	4	3	3	1	1	

1.4.2 Аналіз загроз для інформації в ІТС

Усі джерела загроз безпеки інформації можна поділити на наступні групи:

- стихійні(природні); списки
- антропогенні(спричинені людиною);
- техногенні(спричинені не ідеальністю технічних і програмних засобів).

За природою виникнення загрози поділяють на:

- природні;
- штучні;
  1) Навмисні(спричинені свідомо);
  2) Ненавмисні(спричинені випадково внаслідок помилок, збоїв).

За відношенням до об'єкту захисту:

- внутрішні;
- зовнішні.

За спрямованістю до властивостей інформації на:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності.

Антропогенні загрози:

1) Джерело загрози – системний адміністратор. Загроза – несанкціоновані дії за допомогою облікового запису іншого користувача. Вразливість – відсутність керування обліковими записами, відсутність протоколів подій. Наслідки – порушення конфіденційності, цілісності і доступності інформації, до яких має доступ обліковий запис користувача, порушення цілісності системи і нормальних умов функціонування, несанкціоноване копіювання ІзОД.

2) Джерело загрози – системний адміністратор. Загроза – несанкціоноване або неконтрольоване призначення повноважень або атрибутів доступу користувачам. Вразливість – відсутність розмежування функцій системного адміністратора і адміністратора безпеки, відсутність захищених протоколів подій. Наслідки – порушення конфіденційності, цілісності і доступності інформації

через новий або змінений існуючий обліковий запис, порушення цілісності системи і нормальних умов функціонування, несанкціоноване копіювання ІзОД.

3) Джерело загрози – користувачі системи. Загроза – встановлення несанкціонованого ПЗ. Вразливість – відсутність розмежування дій користувачів в системі, відсутність протоколів подій. Наслідки – порушення конфіденційності, цілісності і доступності інформації, через можливість будь-якому користувачу в системі встановлювати програмне забезпечення або запускати будь-який виконавчий файл.

4) Джерело загрози – користувачі системи. Загроза – несанкціоновані дії в системі від імені іншого користувача. Вразливість – відсутність режиму експлуатації засобів обробки ІзОД: відсутність блокування екрана у період довгої неактивності користувача за робочим місцем. Наслідки – порушення конфіденційності, цілісності і доступності інформації, внаслідок можливості будь-якому користувачу під обліковим записом іншого зробити будь-які дії: встановлення ПЗ, форматування диску, копіювання ІзОД.

5) Джерело загрози – внутрішні користувачі системи. Загроза – несанкціоноване копіювання ІзОД. Вразливість – відсутність регламенту використання зовнішніх сторонніх носіїв, відсутність відстеження операцій з ІзОД, відсутність протоколів подій. Наслідки – порушення конфіденційності інформації.

6) Джерело загрози – зовнішні порушники. Загроза – підглядання або ознайомлення з ІзОД. Вразливість – відсутність режиму доступу сторонніми особами до технічних засобів обробки інформації. Наслідки – порушення конфіденційності інформації.

7) Джерело загрози – сторонні організації, представники конкурентних організацій через підключення до мережевого обладнання провайдера. Загроза – DoS-атака. Вразливість – підключення комутатором до мережевого обладнання провайдера, який у своїй мережі містить підключення сторонніх організацій. Наслідки – порушення доступності інформації, порушення працездатності КС.

8) Джерело загрози – внутрішні користувачі системи. Загроза – перехоплення трафіку, сніфінг. Вразливість – відсутність розмежування підрозділів всередині підприємства. Наслідки – порушення конфіденційності інформації, яка передається в ІТС.

Техногенні:

1) Джерело загрози – єдиний канал зв'язку з мережею Інтернет. Загроза – зупинка виробництва на підприємстві. Вразливість – збої, технічні перерви мережі Інтернет. Наслідки – порушення нормальної роботи підприємства.

2) Джерело загрози – стрибок напруги. Загроза – зупинка виробництва на підприємстві. Вразливість – збої режимів роботи системи електроживлення та відсутність засобів безперебійного живлення для серверів С1 і С2. Наслідки – порушення нормальної роботи підприємства, порушення цілісності і доступності інформації на серверах С1 і С2 через пошкодження жорстких дисків на серверах С1 і С2.

Для того щоб виявити актуальні загрози виконаємо їх ранжування в таблиці 1.13.

Таблиця 1.13 – Ранжування загроз

Загроза	Рівень загрози				Ступінь небезпеки
	Ймовірність, І	Збитки			
		К	Ц	Д	
Несанкціоновані дії системного адміністратора під обліковим записом іншого користувача	5	4	3	3	0,67
Несанкціоноване або неконтрольоване призначення повноважень або атрибутів доступу користувачам від імені системного адміністратора	5	4	3	3	0,67
Встановлення несанкціонованого ПЗ	5	4	3	3	0,67
Несанкціоновані дії в системі від імені	5	4	3	3	0,67

іншого користувача					
Несанкціоноване копіювання ІзОД	5	4	1	1	0,40

Продовження таблиці 1.13

Загроза	Рівень загрози				Ступінь небезпеки
	Ймовірність, І	Збитки			
		К	Ц	Д	
Підглядання або ознайомлення з ІзОД	2	2	1	1	0,05
DoS-атака сторонніх організацій	3	1	1	4	0,16
Перехоплення трафіку	4	3	1	1	0,16
Зупинка виробництва на підприємстві через збої єдиного каналу мережі Інтернет	2	1	3	3	0,16
Зупинка виробництва на підприємстві через стрибок напруги	2	1	4	4	0,21

Ймовірність загрози визначається за наступною класифікацією:

1 – ймовірність загрози не значна або нульова (0-1%);

2 – малоймовірно (1-5%);

3 – імовірно (5-30%);

4 – велика імовірність загрози (30-50%);

5 – загрозі ніщо не заважає трапитися (більше 50%).

Збитки від загрози визначаються рівнями класифікації інформації.

Ступінь небезпеки Кн визначаємо за формулою (1.1).

$$Кн = \frac{І \cdot (К+Ц+Д)}{75}. \quad (1.1)$$

Для даної ІТС наступні загрози не є актуальними:

1) Джерело загрози – повінь від Дніпра. Загроза – знищення частин ІТС або порушення нормальної працездатності підприємства. Вразливість – розташування

ІТС біля річки, залежність функціонування системи від поверхів нижче. Наслідки – порушення нормальної роботи підприємства, зупинка нормальної працездатності підприємства. Загроза не актуальна через малу ймовірність реалізації загрози.

2) Джерело загрози – внутрішні користувачі системи. Загроза – помилки користувачів. Вразливість – низька кваліфікація користувачів. Наслідки – порушення конфіденційності і цілісності інформації. Загроза не актуальна через достатню кваліфікацію працівників.

3) Джерело загрози – зовнішні порушники. Загроза – перехоплення ПЕМВН. Вразливість – ПЕМВН від засобів обробки ІзОД. Наслідки – виток ІзОД. Загроза не актуальна через малі обороти підприємства.

4) Джерело загрози – зовнішні порушники. Загроза – використання ТЗР для перехоплення видової інформації. Вразливість – розташування екранів ПК4, ПК5 поблизу вікон. Наслідки порушення конфіденційності інформації на моніторах ПК4, ПК5. Загроза не актуальні через використання жалюзі на вікнах всередині ОІД.

5) Джерело загрози – зовнішні користувачі. Загроза – зміна або перехоплення трафіку. Вразливість – відсутність надійної системи автентифікації відправника і отримувача. Наслідки – порушення конфіденційності і цілісності інформації, яка передається в мережі Інтернет. Загроза не актуальна внаслідок використання надійних протоколів автентифікації відправника і отримувача.

Висновок: загрози зі ступенем небезпеки менше 0,1 можна проігнорувати. Необхідно забезпечити підвищені вимоги до конфіденційності інформації.

1.5 Визначення вимог до КЗЗ

На підставі проаналізованих джерел загроз, вразливостей і визначених актуальних загроз і можливих порушників ІТС можна визначити вимоги до КСЗІ.

Було вирішено ввести умовні позначення однакових множин КС, до яких можуть відноситись різні послуги.

Множина об’єктів КС 1: інформація на дисковому просторі серверів С1 і С2.

Множина об’єктів КС 2: ПЗ(прикладне, спеціальне і системне), технологічна інформація, інформація, яка міститься в файлах і базах даних, що зберігаються на просторі жорсткого диску сервера С2 і С1.

Множина об’єктів КС 3: інформація про співробітників, копії персональних даних персоналу, інформація про закази, інформація о клієнтах, бухгалтерські звіти, документи ЗЕД, інформація про послуги підприємства, інформація про імпорт/експорт продукції, матеріалів.

КА-2 – Базова адміністративна конфіденційність.

Множина об’єктів КС, до яких повинна відноситися політика: множина 2.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

При виведені ІзОД на паперовий носій КЗЗ необхідно забезпечувати роздрукування реквізитів про обмеження доступу, інформації про роздрукований файл, базу даних, з якої взята інформація, місце і дата роздрукування, ким роздруковано.

Необхідна умова: НО-1, НИ-1.

КО-1 – Повторне використання об'єктів.

Множина об’єктів КС, до яких повинна відноситися політика: оперативна пам’ять комп’ютерів.

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.

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.

КВ-2 – Базова конфіденційність при обміні.

Множина об’єктів КС, до яких відноситься політика: множина 3.

Інтерфейсні процеси: ПЗ: Браузер Google Chrome, Пакет програм Microsoft Office, командний рядок, внутрішній інтерфейс Microsoft Windows.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Необхідна умова: НО-1.

ЦА-1 – Мінімальна адміністративна цілісність.

Множина об’єктів КС, до яких відноситься політика: множина 2, системний простір жорсткого диску користувачів.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

Необхідна умова: НО-1, НИ-1.

ЦО-1 – Обмежений відкат.

Множина об’єктів КС, до яких відноситься політика: множина 1.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

Необхідна умова: НИ-1.

ЦВ-1 – Мінімальна цілісність при обміні.

Множина об’єктів КС, до яких відноситься політика: множина 3.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання.

Запити на експорт та імпорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

ДР-1 – Квоти.

Множина об’єктів КС, до яких відноситься політика: системний простір жорстких дисків, простір жорсткого диску файлового сервера С2.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

Необхідна умова: НО-1.

НР-2 – Захищений журнал.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки:

- автентифікація користувача в системі;
- зміна групи користувачів;
- використання сторонніх зовнішніх носіїв;
- зміна атрибутів доступу;
- зміна атрибутів файлів;
- запуск ПЗ;
- встановлення і оновлення ПЗ;
- зміна компонентів захисту КС;

– збої активації корпоративної ліцензії;

– збої перевірки сертифікату сайту;

– перегляд журналу безпеки;

– перевірка файлів і сайтів Kaspersky Small Office Security;

– виведення документу на друк.

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.

Необхідні умови: НИ-1, НО-1.

НИ-2 – Одиночна ідентифікація і автентифікація.

Атрибути користувачів: інсталяція ПЗ, запуск ПЗ, зміна системних файлів, перегляд журналів подій, дозвіл на перегляд, редагування, видалення, виконання.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1 – Однонаправлений достовірний канал.

Достовірний зв’язок повинен встановлюватись механізмом автентифікації користувачів(введення надійного паролю) і надавати доступ до системи тим користувачам, які мають відповідний доступ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2 – Розподіл обов'язків адміністраторів.

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та системного адміністратора. Функції, притаманні кожної із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

Необхідна умова: НИ-1.

НЦ-1 – КЗЗ з контролем цілісності.

КЗЗ повинно забезпечувати перевірку цілісності Kaspersky Small Office Security за допомогою засобів автоматичної перевірки і оновлення баз, та брандмауеру Windows 10.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і або автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Користувачам необхідно дотримуватись політики ідентифікації і автентифікації під час входу в систему; користувач повинен пам’ятати свій ідентифікатор і пароль в системі, щоб мати доступ до інформації.

Необхідна умова: НР-1, НО-1.

НВ-1 – Автентифікація вузла.

Для ідентифікації і автентифікації КЗЗ повинен перевірити на відповідність і достовірність сертифікати вузла, в якому зазначається версія, серія, алгоритм підпису, час дійсності сертифікату, ім’я вузла і ключів шифрування.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

НА-1 – Базова автентифікація відправника.

Множина властивостей і атрибутів об'єкта, що передається: ім'я об'єкту, тип об'єкта, розмір, дата створення, дата зміни, можливість читати або редагувати, користувач-володілець об'єкту.

Множина властивостей і атрибутів користувача-відправника: ім'я, пошта користувача-відправника.

Множина властивостей і атрибутів інтерфейсного процесу: операційна система, ім'я інтерфейсного процесу, ім'я користувача-отримувача, IP-адреса і порт користувача-отримувача.

Процедури підтвердження передачі об'єкта від користувача-відправника: протокол TLS, перевірка сертифіката сайту.

Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

Необхідна умова: НИ-1.

НП-1 – Базова автентифікація отримувача.

Множина властивостей і атрибутів об'єкта, що передається: ім'я об'єкту, тип об'єкта, розмір, дата створення, дата зміни, можливість читати або редагувати, користувач-володілець об'єкту.

Множина властивостей і атрибутів користувача-одержувача: ім'я, пошта користувача-одержувача.

Множина властивостей і атрибутів інтерфейсного процесу: операційна система, ім'я інтерфейсного процесу, ім'я користувача-одержувача, IP-адреса і порт користувача-одержувача.

Процедури підтвердження передачі об'єкта до користувача-одержувача: протокол TLS, перевірка сертифіката сайту.

Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації.

Необхідна умова: НИ-1.

{КА-2, КО-1, КВ-2, ЦА-1, ЦО-1, ЦВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-2, НЦ-1, НВ-1, НА-1, НП-1}, Г-2.

Сформовані вимоги до критеріїв захисту інформації надано в таблиці 1.14.

Таблиця 1.14 – Вимоги до критеріїв захищеності інформації

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
Конфіденційності	Адміністративна конфіденційність	КА-2 – Базова адміністративна конфіденційність
	Повторне використання об'єктів	КО-1 – Повторне використання об'єктів
	Конфіденційність при обміні	КВ-2 – Базова конфіденційність при обміні
Цілісності	Адміністративна цілісність	ЦА-1 – Мінімальна адміністративна цілісність
	Відкат	ЦО-1 – Обмежений відкат
	Цілісність при обміні	ЦВ-1 – Мінімальна цілісність при обміні
Доступності	Використання ресурсів	ДР-1 (Квоти)
Спостережності	Реєстрація	НР-2 – Захищений журнал
	Ідентифікація і автентифікація	НИ-2 – Одиночна ідентифікація і автентифікація
	Достовірний канал	НК-1 – Однонаправлений

		достовірний канал
	Розподіл обов’язків	НО-2 – Розподіл обов'язків адміністраторів
	Цілісність КЗЗ	НЦ-1 – КЗЗ з контролем цілісності

Продовження таблиці 1.14

Критерії	Послуги безпеки	Вимоги до рівнів послуг безпеки
	Ідентифікація і автентифікація при обміні	НВ-1 – Автентифікація вузла
	Автентифікація відправника	НА-1 – Базова автентифікація відправника
	Автентифікація отримувача	НП-1 – Базова автентифікація отримувача
Гарантій	Рівень гарантій до КЗЗ	Г-2

1.6 Висновок

За результатами передатестаційної практики був описаний ОІД:

– загальна інформація про підприємство;

– загальна інформація про будівлю, у якій розташований ОІД;

– відомості про програмне і апаратне забезпечення на ОІД;

– відомості про інформаційну систему і інформаційні потоки;

– відомості про користувачів системи та їх доступ до об’єктів і інформації всередині АС.

Був виконаний аналіз джерел загроз і вразливостей та на основі цього аналізу було створено матрицю актуальних загроз. Необхідно проаналізувати

існуючий стан послуг в ІТС та надати методи та засоби захисту інформації для реалізації цих послуг.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Визначення рівня реалізації послуг безпеки

Для забезпечення вимог послуг необхідно провести аналіз існуючої реалізації послуг – реалізованих, нереалізованих і частково реалізованих, методів та засобів захисту інформації, політики безпеки, організаційних обмежень і на основі цього аналізу створити перелік послуг, які необхідно забезпечити за допомогою створення КСЗІ.

Згідно переліку засобів ТЗІ від 01.03.2021 [9] і експертного висновку №1027 [10] операційна система Microsoft Windows 10 Professional виробництва компанії «Microsoft Corporation» (США) відповідає вимогам нормативних документів з ТЗІ в обсязі функцій КД-2, КВ-1, КО-1, ЦД-1, ЦА-1, ЦВ-1, ЦО-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з рівнем гарантій Г-2 оцінки коректності їх реалізації згідно НД ТЗІ 2.5-004-99. Операційна система Windows 10 Professional включає в себе можливості щодо реалізації вимог до функцій безпеки.

Проаналізуємо стан вимог захищеності згідно таблиці 1.14.

КА-2 – Базова адміністративна конфіденційність.

Реалізовані атрибути доступу користувача і захищеного об’єкта за допомогою політики безпеки Windows 10. Не реалізовано розмежування об'єктів захисту, які містять ІзОД, за атрибутами доступу.

КО-1 – Повторне використання об'єктів.

Не реалізовано очищення пам’яті після використання програмного забезпечення, яке працює з ІзОД.

КВ-2 – Базова конфіденційність при обміні.

Реалізовано за допомогою протоколів HTTPS, TLS, TCP/IP.

ЦА-1 – Мінімальна адміністративна цілісність.

Не реалізоване розмежування доступу на підставі атрибутів доступу користувачів і захищеного об’єкта.

ЦО-1 – Обмежений відкат.

Реалізовано за допомогою вбудованих функцій програмного забезпечення, які під час користування дозволяють зробити відкат нещодавніх дій і також роблять тимчасові копії документів або файлів з ІзОД. Сервер С1 має вбудовані включені функції відкату бази даних 1С, яка зберігає файл з конфігурацією і версії об'єктів. Сервер С2 забезпечується відкат за допомогою вбудованих функцій механізму InnoDB.

ЦВ-1 – Мінімальна цілісність при обміні.

Реалізовано за допомогою коду автентифікації повідомлення (MAC – message authentication code) в протоколі захисту транспортного рівня (TLS – transport layer security) виявлення порушення цілісності під час передачі інформації на поштовий сервер Google.

ДР-1 – Квоти.

Не реалізовано обмеження на обсяг ресурсів, що виділяються окремому користувачу.

НР-2 – Захищений журнал.

В КС не включені функції журналу подій безпеки в системі.

НИ-2 – Одиночна ідентифікація і автентифікація.

Реалізовано за допомогою вбудованих функцій Windows 10: в локальній політиці безпеки та в редакторі локальної групової політики. Користувачі проходять автентифікацію під час введення паролю при вході в систему.

НК-1 – Однонаправлений достовірний канал.

Реалізовано за допомогою вбудованих функцій ідентифікації і автентифікації користувача Windows 10 після загрузки операційної системи за групою користувачів або окремим записом користувача в КС. Зв'язок з використанням даного каналу ініціюється виключно користувачем.

НО-2 – Розподіл обов'язків адміністраторів.

Реалізовані функції розподілу адміністратора і звичайного користувача за допомогою сегрегації прав користувачів в локальній політиці безпеки Windows 10. Не реалізовано розмежування адміністративні ролей: системного адміністратора і адміністратора безпеки.

НЦ-1 – КЗЗ з контролем цілісності.

Реалізовано за допомогою вбудованих функцій перевірки цілісності Windows 10 під час ініціалізації системи і після ініціалізації системи Kaspersky Small Office Security за допомогою перевірки модулів і файлів програми шляхом порівняння контрольної суми з «файлом маніфесту», який включає в себе усі критично необхідні компоненти програми.

НВ-1 – Автентифікація вузла.

Реалізовано за допомогою протоколів TCP/IP і HTTPS під час з'єднання через інтерфейсний процес Google Chrome.

НА-1 – Базова автентифікація відправник.

Реалізовано за допомогою протоколів TCP/IP і HTTPS під час з'єднання через інтерфейсний процес Google Chrome.

НП-1 – Базова автентифікація отримувача.

Реалізовано за допомогою протоколів TCP/IP і HTTPS під час з'єднання через інтерфейсний процес Google Chrome.

Г-2 – рівень гарантій.

Реалізовано за допомогою операційної системи Windows 10 [9].

В результаті аналізу КС було виявлено:

– реалізовані послуги: КВ-2, ЦО-1, ЦВ-1, НИ-2, НК-1, НЦ-1, НВ-1 ,НА-1, НП-1;

– частково реалізовані: КА-2, ЦА-1, НР-2, НО-2;

– нереалізовані: КО-1, ДР-1.

2.2 Проектні рішення щодо реалізації вимог безпеки

2.2.1 Елементи політики безпеки

Проектні рішення будуть представлені у вигляді елементів техно-робочого проекту.

Було визначено положення про використання паролів.

Усі користувачі в системі зобов'язані використовувати власний пароль від облікового запису в обчислювальній системі для автентифікації.

Усі паролі повинні виконувати наступні параметри:

– паролі не повинні мати те саме значення що і логін користувача (ім'я облікового запису);

– паролі не повинні повторюватись;

– паролі повинні складатися з букв верхнього і нижнього регістрів, цифр від 0 до 9;

– паролі повинні включати в себе хоча б один спецсимвол (~!@#$%^&*_-+='|\() {} []:;"' <>,.? /).

Користувачам необхідно виконувати наступні правила:

– забороняється записувати паролі на папір;

– забороняється передавати паролі в будь-якому вигляді будь-кому, в тому числі керівникам і колегам;

– забороняється використовувати функцію «Запам'ятати пароль» в програмах;

– якщо користувач запідозрює, що його пароль скомпрометовано, необхідно негайно повідомити адміністратора безпеки чи іншу людину, яка відповідає за паролі в «Pure glycerin».

Було визначено положення про безпеку сервера.

Системному адміністратору необхідно задокументувати наступні відомості, що відносяться до будь-якого сервера:

– конфігурація серверу, операційна система, їх характеристика і версія;

– яке ПЗ і його версія використовується;

– обновляти відомості при будь-якій зміні.

На сервері необхідно:

– забезпечити відключення служб і прикладних програм, які не використовуються в процесі роботи підприємства;

– забезпечуватись реєстрація доступу до сервісів, служб і захищатися методами контролю доступу;

– забезпечуватись реєстрація подій безпеки, яка повинна зберігатися мінімум 1 тиждень;

– забезпечуватись зберігання недільних резервних копій не менше ніж один місяці;

– забезпечуватись останні оновлення безпеки;

– використовувати підключення за допомогою безпечних каналів і протоколів;

– забезпечити використання тільки необхідних мережевих портів і загальних мережевих ресурсів.

Забороняється перебування сторонніх осіб у приміщенні, де розташований сервер. Про події безпеки повідомляти адміністратора безпеки чи іншу людину, яка відповідає за безпеку в «Pure glycerin».

Була змінена матриця розмежування доступу.

В результаті аналізу середовищ функціонування ІТС і моделі загроз було встановлено, що матриця розмежування доступу надлишкова, а тому потребує перегляду. Нова матриця розмежування доступу надана у таблиці 2.1.

Таблиця 2.1 – Нова матриця розмежування доступу

Об’єкт	Інформація									Повноваження інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9		
Директор	Ч	Ч	Ч	Ч	Ч	Ч	Ч	ЧСМВТД	Ч	Ні	ПК1… ПК11, С1, С2
Юрист	ЧСМВТ	ЧСМВТ	ЧСМВТ	-	ЧСМВТ	Ч	ЧСМВТ	Ч	-	Ні	ПК8
Помічник юриста	ЧСМВТ	ЧСМВТ	ЧСМВТ	-	ЧСМВТ	Ч	ЧСМВТ	Ч	-	Ні	ПК9

Продовження таблиці 2.1

Об’єкт	Інформація									Повноваження інсталювання ПЗ	Доступ до ресурсів
Користувач	1	2	3	4	5	6	7	8	9		
Спеціаліст з продажу	-	ЧСМВТ	ЧСМВТ	-	ЧСМВТ	Ч	ЧСМВТ	Ч	-	Ні	ПК10
Спеціалісти ЗЕД	-	ЧСМВТ	ЧСМВТ	-	ЧСМВТ	Ч	ЧСМВТ	Ч	-	Ні	ПК5, ПК6, ПК7
Секретар	ЧСМВТ	ЧСМВТ	ЧСМВТ	-	-	Ч	-	ЧСМВТД	-	Ні	ПК11
Бухгалтер	-	ЧСМВТ	ЧСМВТ	ЧСМВТД	ЧСМВТ	Ч	ЧСМВТ	Ч	-	Ні	ПК2, ПК3
Системний адміністратор	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	ЧСМВТД	Так	ПК1… ПК11, С1, С2
Адміністратор безпеки	-	-	-	-	-	-	-	-	ЧСМВТД	Ні	ПК1… ПК11, С1, С2

Умовні позначення доступу до інформації:

Ч – читання;

С – створення нових файлів;

М – редагування;

В – видалення;

Т – імпорт/експорт;

Д – друк.

Інформація в таблиці 2.1 відповідає номерам інформації у таблиці 1.3.

2.2.2 Резервування мережі Інтернет

Для забезпечення стабільності і безперервності роботи підприємства необхідно забезпечити КС другим каналом до мережі Інтернет. Для цього проаналізуємо рішення щодо можливості підключення до інших провайдерів.

Для дротового підключення до нового провайдера необхідно купити нове мережеве обладнання, яке зможе підтримувати 2 мережі. Перевагами такого рішення можуть бути:

- збільшення і розширення каналу передачі;
- зниження рівня загрузки одного каналу передачі даних;
- переходити з однієї мережі на іншу в разі збоїв.

Були проаналізовані наявні підключення провайдерів до торгового комплексу «Вавилон» і підключення сторонніх провайдерів [11]. Результати аналізу підключень до мережі Інтернет описані у таблиці 2.2.

Таблиця 2.2 – Порівняння підключень до мережі Інтернет

Найменування	Вартість, грн.		Швидкість, Мбіт/с	Додаткові функції і можливості
	Щомісячно	Підключення		
«Київстар» 4G	300	995	42	Mobile ID, Office 365, віртуальна АТС
	250	4395	150	Mobile ID, Office 365, віртуальна АТС
«Forsage»	233	-	100	-
«Фрегат»	300	-	15	-
«fts»	300	2880	10	-
«Союзтелеком»	340	4145	20	-
«Інтертелеком» 3G	300	4195	14,7	Програма лояльності

В результаті аналізу цін та можливостей в таблиці 2.2, інформації щодо стабільності на сайті відгуків [12] було вирішено підключитися за допомогою другого варіанту «Київстар 4G» до модему з використанням 4G, який буде підключено до існуючого комутатора DGS-1100-16V2. Обраний саме другий варіант, так як для стабільної і швидкої роботи 12 користувачів в системі без урахувань зниження швидкості від завантаженості мережі 42 Мбіт/с буде не вистачати.

Для реалізації резервування мережі Інтернет було вирішено використовувати модем. Можливості модемів були проаналізовані в таблиці 2.3. Було вирішено використовувати модем Huawei B593s – 12. Слід зазначити, що для керівництва підприємства залишається можливим використання бездрової мережі Wi-Fi за допомогою закупівлі і встановлення Wi-Fi адаптерів на комп'ютери і сервери в ІТС. В такому разі необхідно забезпечити надійну передачу даних мережею Wi-Fi.

2.2.3 Розмежування внутрішнього трафіку

Комутатор DGS-1100-16V2 має вбудовані функції розмежування підключень до внутрішньої мережі підприємства за допомогою таблиці білих Mac-адрес. Системному адміністратору необхідно налаштувати віртуальні локальні мережі підрозділів (vlan) бухгалтерії, юристів, спеціалістів у відкритому офісі і за допомогою функції комутатора Static Mac налаштувати дозволені підключення за Mac адресами комп'ютерів внутрішньої мережі. Такий розподіл внутрішньої мережі підприємства забезпечить унеможливлення перехоплення пакетів між підрозділами підприємства.

Для зменшення ризику DoS-атак і небажаного трафіку з боку внутрішніх організацій внутрішньої локальної мережі вежі системному адміністратору необхідно налаштувати функції комутатора DGS-1100-16V2 згідно офіційних рекомендацій [13]. Для локальної мережі «pure» і портів 12-13:

config igmp_snooping querier pure state enable

config igmp_snooping pure state enable

enable igmp_snooping

config multicast port_filtering_mode 12-13 filter_unregistered_groups

Таблиця 2.3 – Порівняння модемів

Найменування	Вартість, грн.	Максимальна швидкість приймання, Мбіт/с	Стандарти зв'язку	Порти	Гарантія, місяці
Huawei E5186S-61A	4000	150	Wi-Fi 802.11 a/b/g/n/ac 2,4 і 5 ГГц	4 x RJ-45; 2 x RJ11; 2 x SMA USB	12
Huawei B593s - 12	2180	150	Wi-Fi 802.11 b/g/n 2,4 ГГц	4 x RJ-45; 1 x RJ11; 2 x SMA microUSB	12
Huawei B315-22	2499	150	Wi-Fi 802.11 b/g/n 2,4 ГГц	4 x RJ-45; 1 x RJ11; 2 x SMA USB	12
Netgear MR1100	7999	150	Wi-Fi 802.11 a/b/g/n/ac 2,4 і 5 ГГц	1 x RJ-45; 2 x SMA USB	12

Примітка. Усі модеми підтримують стандарти GSM GPRS/EDGE, UMTS, HSDPA, HSPA, HSPA+, DC-HSPA+ до 63.3 Мбіт/с і мають підключення для антени.

2.2.4 Забезпечення серверів джерелом безперебійного живлення

Для забезпечення захисту інформації серверів С1 і С2, і уникнення пошкодження жорстких дисків серверів від збоїв системи електропостачання необхідно забезпечити джерелом безперебійного живлення (ДЖБ).

ДБЖ – джерело безперебійного живлення

Дано 2 сервери по 650 Вт з необхідним забезпеченням напруги в 220В.

Обчислимо необхідні параметри ДЖБ за допомогою формули (2.1):

$$Є = T \cdot I, \text{ А·г}, \quad (2.1)$$

де Є – ємність;

Т – час;

І – струм.

Визначимо необхідний струм споживання у формулі (2.2).

$$I = \frac{\text{Пс}}{12}, \text{ А}, \quad (2.2)$$

де Пс – потужність споживання.

Потужність споживання визначимо у формулі (2.3).

$$\text{Пс} = \text{Пн}/\text{ККД}, \text{ Вт}, \quad (2.3)$$

де Пн – потужність навантаження;

ККД – коефіцієнт корисної дії ДЖБ.

Час автономної роботи ДБЖ повинен включати в себе такі операції:

– збереження інформації та гарячих даних на твердотільних накопичувачах серверів С1 і С2;

– забезпечення резервного копіювання;

– коректне закриття процесів і програм;

– коректне вимикання;

– самостійне вимикання серверів при відсутності людей.

В результаті аналізу часу, за який здійснюються необхідні операції на серверах, було виявлено, що 13 хвилин достатньо для коректного завершення роботи за допомогою ДБЖ.

Т = 15 хвилин = 0,25 годин,

Пн = 2·150 = 300 Вт = 0.3 кВт,

Пс = 300/0,9 = 333 Вт,

I = 333/12 = 28 А,

Є = 128·0.25 = 7 А·г.

Порівняємо доступні ДБЖ в таблиці 2.4.

В результаті аналізу характеристик ДБЖ було вирішено використовувати Logic Power LPM U1400VA-P, так як він має захист від короткого замикання, можливість підключення до комп'ютера через USB type B і програму для налаштування автономного завершення серверів. Для перегляду стану ДБЖ системному адміністратору необхідно використати ПЗ Network UPS Tools [14]. Для налаштування вимикання серверів при переході на ДЖБ встановлюється ПЗ Power Manager II, яке йде у комплектації з блоком або скачати з офіційного сайту LogicPower [15].

Таблиця 2.4 – Порівняння характеристик джерел безперебійного живлення

Найменування	Потужність	Батарея	Особливості	Гарантія, місяців	Ціна, грн.
SVC VP-1000-LCD 1000VA	1000 ВА / 600 Вт	12 В / 9 А·г	USB роз'єм, дисплей, холодний старт, захист від короткого замикання, захист від перевантажень.	24	1781
Logic Power LPM U1400VA-P	1400 ВА / 840 Вт	2·12 В / 7.5 А·г	Зворотній зв'язок з ПК, захист від короткого замикання, захист від перевантажень.	24	2882
LogicPower LPM U850VA-P (LP10397)	850 ВА / 510 Вт	12 В / 8.5 А·г	Пряме підключення.	24	1650

Vinga LCD 800VA Shuko Metal Case	800 ВА / 480 Вт	12 В / 8 А·г	Холодний старт.	12	1699

Продовження таблиці 2.4

Найменування	Потужність	Батарея	Особливості	Гарантія	Ціна, грн.
EAST EA-850 Schuko	850 ВА / 480 Вт	12 В / 8 А·г	Холодний старт.	24	1799

2.2.5 Розподіл обов’язків системного адміністратора

Так як системний адміністратор володіє надлишковими параметрами доступу необхідно змінити його права згідно нової матриці розмежування доступу таблиці 2.1. Для реалізації розподілу обов’язків адміністраторів необхідно перекласти обов’язки адміністратора безпеки на довірену людину серед працівників – секретаря або залучити стороннього спеціаліста. Права системного адміністратора обмежити у відповідності до його нових обов’язків:

– заборонити інсталяцію нового ПЗ без дозволу адміністратора безпеки;

– заборонити зміну журналів безпеки.

Системному адміністратору необхідно впровадити наступні зміни:

– заборонити адміністратору безпеки створювати облікові записи;

– встановити блокування сеансу після 5 хвилин відсутності активності;

– перекласти обов’язки створення і видачі паролів на адміністратора безпеки.

Адміністратору безпеки необхідно:

– вести аудит безпеки системи;

– перевіряти журнали безпеки;

– реєструвати надійні паролі для користувачів КС згідно положення про використання паролів;

– перевіряти журнал безпеки при критичних подіях та інцидентах спрямованих на подолання засобів захисту в системі.

2.2.6 Проектні рішення у вигляді елементів техно-робочого проекту

КА-2 – Базова адміністративна конфіденційність.

Для реалізації розмежування доступу системному адміністратору необхідно розмежувати об’єкти захисту, які містять ІзОД, за атрибутами доступу користувачів в локальній політиці безпеки операційної системи Windows 10 згідно нової матриці доступу користувачів в таблиці 2.1.

КО-1 – Повторне використання об'єктів.

Для забезпечення реалізації отримання розділювального об’єкта без доступу до інформації, яка містилася у ньому від іншого користувача або процесу, системному адміністратору необхідно автоматизувати роботу програми звільнення оперативної пам’яті Mem Reduct [15] для запуску після використання користувачем або процесом ІзОД. Необхідно використати «Планувальник задач» у вбудованих функціях операційної системи Windows 10 і встановити використання програми очистки оперативної пам’яті «при коді подій» на закриття прикладного або спеціалізованого ПЗ з таблиці 1.2, яке працює з ІзОД, в журналі подій.

Для реалізації звільнення інформації було запропоновано використання корпоративної програми для автоматизації Automize 12. Системному адміністратору необхідно, використовуючи Automize 12 [16], налаштувати використання програми Mem Reduct 3.3.5 для запуску при закритті системного або прикладного ПЗ.

ЦА-1 – Мінімальна адміністративна цілісність.

Для реалізації забезпечення цілісності об’єктів системному адміністратору необхідно за допомогою вбудованих функцій Windows 10, локальна політика безпеки, призначити права окремим користувачам і групам користувачів. Параметри доступу до інформації необхідно задати за допомогою призначення

доступу на читання, редагування або повний доступ до папки з інформацією, з доступом в автономному режиму, а також обмеження на доступ кількості одночасних користувачів за допомогою нової матриці розмежування доступу в таблиці 2.1.

ДР-1 – Квоти.

Для забезпечення вимог системному адміністратору необхідно виділити кожному користувачу по 200Гб місця на сервері С2. Для цього необхідно використати розмежування місця за допомогою вбудованих функцій «Квот» на сервері С2 (рисунок 2.1).

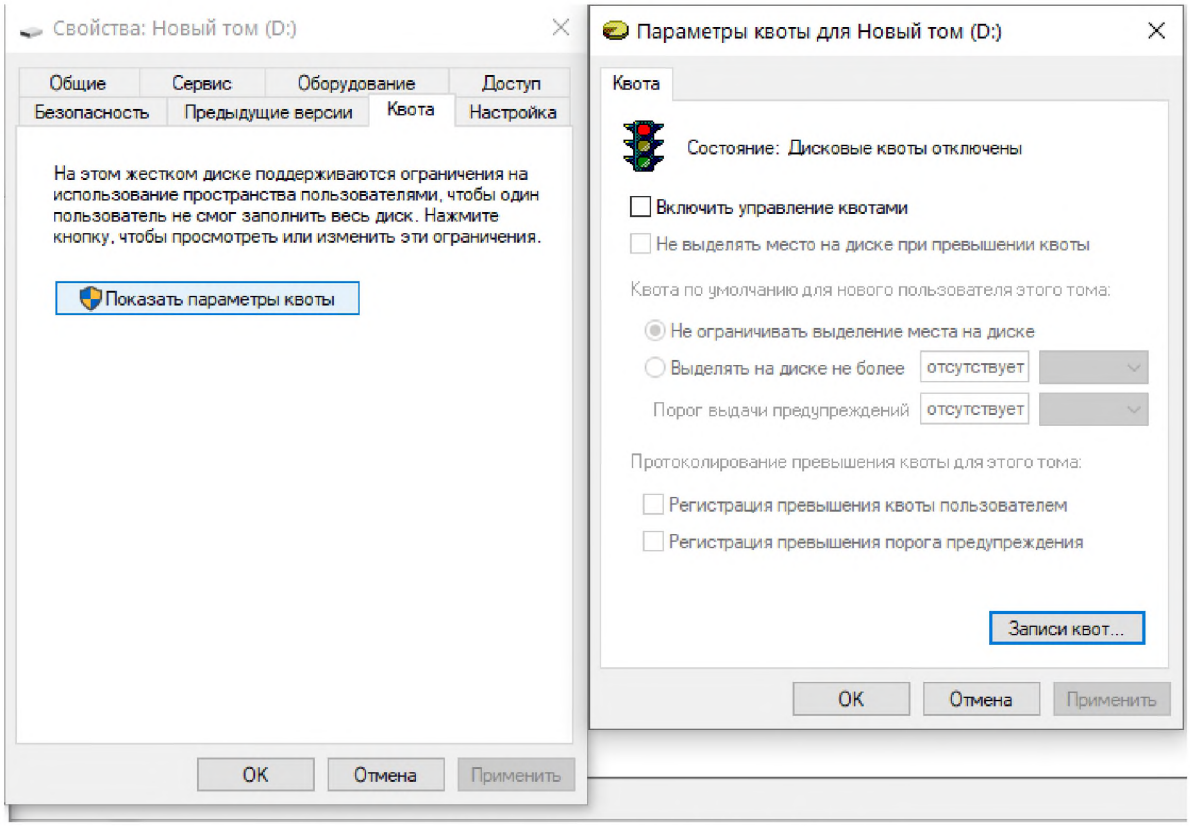


Рисунок 2.1 – Квоти Windows Server

НР-2 – Захищений журнал.

Для забезпечення ведення аудиту подій безпеки адміністратору безпеки необхідно включити аудит подій безпеки, який зображено на рисунку 2.2 і налаштувати події, які необхідно реєструвати:

– автентифікація користувача в системі;

– зміна групи користувачів;

– використання сторонніх зовнішніх носіїв;

– зміна атрибутів доступу;
– зміна атрибутів файлів;
– запуск ПЗ;
– встановлення і оновлення ПЗ;
– зміна компонентів захисту КС;
– збої активації корпоративної ліцензії;
– збої перевірки сертифікату сайту;
– перегляд журналу безпеки;
– перевірка файлів і сайтів Kaspersky Small Office Security;
– виведення документу на друк.

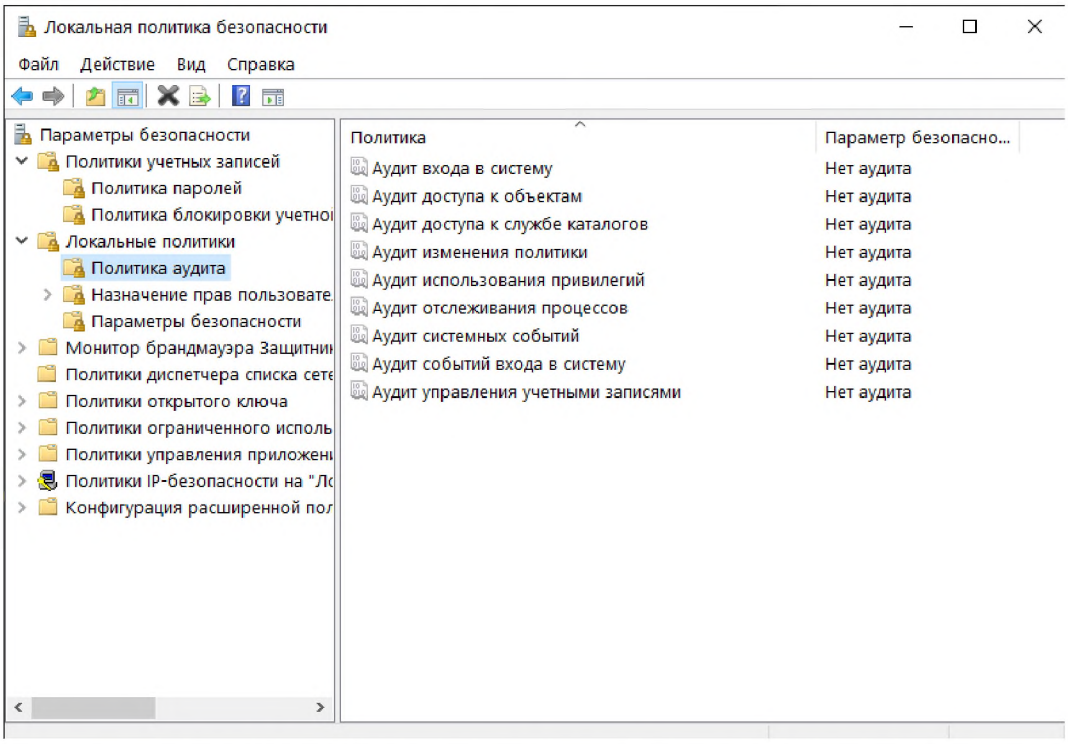


Рисунок 2.2 – Журнал політики безпеки Windows 10

2.2.7 Альтернативне рішення реалізації вимог безпеки

Альтернативним рішенням реалізації послуг безпеки може виступати використання КЗЗ «Гриф-Мережа», яким можна розгорнути як на комп'ютерах працівників, так і на серверах.

Згідно офіційного сайту Інституту комп'ютерних технологій [17] комплекс «Гриф-Мережа» версії 3.04 реалізує такі функції:

– ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), паролю та носія даних автентифікації (знімного файлового носія (пристрій Flash Drive, CD-RW, DVD-RW, дискета тощо)) при завантаженні ОС робочої станції до завантаження будь-яких програмних засобів з дисків;

– блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

– контроль цілісності та самотестування КЗЗ при старті та за запитом адміністратора;

– розподіл обов'язків користувачів та виділення кількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування;

– розмежування доступу користувачів до вибраних каталогів (папок), розміщених на робочих станціях та файлових серверах ЛОМ, та до файлів, які в них знаходяться;

– керування потоками інформації та блокування потоків інформації, що можуть призвести до зниження рівня її конфіденційності;

– контроль за виводом інформації на друк з можливістю маркування друкованих листів документів;

– контроль за експортом інформації на знімні носії з можливістю обмеження переліку знімних носіїв, які використовуються;

– контроль за імпортом інформації зі знімних носіїв;

– гарантоване видалення інформації шляхом затирання вмісту файлів, які містять ІзОД, при їх видаленні;

– розмежування доступу прикладних програм до вибраних каталогів та файлів, які в них знаходяться;

– контроль цілісності прикладного та системного програмного забезпечення (ПЗ) та ПЗ КЗЗ, а також блокування завантаження програм, цілісність яких порушена;

– контроль за використанням користувачами дискового простору файлових серверів (квоти);

– відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації з забезпеченням дотримання правил доступу до неї;

– безперервну реєстрацію, аналіз та обробку подій (входу користувачів в ОС, спроб несанкціонованого доступу, фактів запуску програм, роботи з ІзОД, виводу на друк і т.п.) в спеціальних протоколах аудита;

– негайне оповіщення адміністратора безпеки про всі виявлені порушення встановлених правил розмежування доступу;

– ведення архіву зареєстрованих даних аудита;

– взаємодію з прикладними програмними системами через визначений виробником КЗЗ інтерфейс.

Згідно офіційного сайту Інституту комп'ютерних технологій [17] і експертного висновку [18] функціональний профіль захищеності, який реалізує комплекс «Гриф-Мережа» в базовій конфігурації:

{КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДС-1, ДЗ-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-2, НТ-2}

Для аналізу доцільності можливості використання КЗЗ «Гриф-Мережа» проведемо порівняльну характеристику реалізації вимог захищеності в таблиці 2.5.

Таблиця 2.5 – Порівняльна характеристика вимог захищеності

Вимоги захищеності інформації	Гриф-Мережа
КА-2	КА-2
КО-1	КО-1
ЦА-1	ЦА-2
ДР-1	ДР-1
НР-2	НР-2
НИ-2	НИ-3
НО-2	НО-2

З таблиці 2.5 можна зробити висновок, що КЗЗ «Гриф-Мережа» реалізує необхідні вимоги захищеності.

2.3 Висновок

У другому розділі був проаналізований існуючий стан вимог захищеності інформації на підприємстві і визначені вимоги, які необхідно реалізувати за допомогою проектних рішень.

Для забезпечення захисту інформації від загроз, були реалізовані наступні рішення захисту інформації:

- нова матриця розмежування доступу;
- резервування мережі Інтернет;
- розмежування внутрішнього трафіку;
- оснащення ДЖБ серверів;
- розмежування прав системного адміністратора;
- реалізовані вимоги захищеності інформації: за допомогою вбудованих функцій Windows 10 і стороннього ПЗ або за допомогою КЗЗ "Гриф-Мережа".

Для визначення доцільності запровадження запропонованих рішень для підприємства необхідно проаналізувати їх економічні показники.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є економічне обґрунтування доцільності запровадження запропонованих організаційно-технічних рішень щодо побудування КСЗІ в ІТС підприємства ТОВ «Pure glycerin». Для визначення економічної ефективності необхідно:

– розрахувати капітальні витрати на програмні і апаратні засоби для впровадження КСЗІ;

– розрахувати річну вартість експлуатаційних витрат на утримання і обслуговування КСЗІ;

– визначити річний економічний ефект від впровадження КСЗІ в ІТС;

– визначити і проаналізувати показники економічної ефективності запропонованих рішень;

– зробити висновок щодо економічної доцільності.

Впроваджені проектні засоби і рішення наведені в таблиці 3.1.

Таблиця 3.1 – Проектні рішення кваліфікаційної роботи

Назва	Опис	Витрати, грн.
Елементи політики безпеки	Впровадження положень на підприємстві, оптимізація розмежування доступу користувачів	Безкоштовно
Резервування мережі Інтернет	Підключення до мережі «Київстар» 4G	250 щомісяця, 4395
	Закупівля модему Huawei B593s – 12	2749
Розмежування внутрішнього трафіку	Використання вбудованих функції комутатора D-Link DGS-1100-16V2	Безкоштовно

Продовження таблиці 3.1

Назва	Опис	Витрати, грн.
Оснащення ДБЖ серверів	Закупівля джерела безперебійного живлення SVC VP-1000-LCD 1000VA	2882
Розподіл обов'язків системного адміністратора	Розподіл обов'язків системного адміністратора і виділення адміністратора безпеки	Оплата праці
Реалізація вимог захищеності	Використання вбудованих функцій Windows 10 і стороннього ПЗ Mem Reduct, Automize 12	4370
	Використання КЗЗ "Гриф-Мережа"	7010

3.1 Розрахунок (фінансових) капітальних витрат

Так як для реалізації вимог захищеності надається два варіанти рішення капітальні витрати для першого і другого варіантів будуть відрізнятися.

3.1.1 Визначення трудомісткості розробки КСЗІ

Тривалість кожної робочої операції для розробки КСЗІ порахуємо згідно формули (3.1).

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

де $t_{\text{тз}}$ – тривалість складання технічного завдання КСЗІ, годин;

$t_{\text{тз}}$ = 13 годин;

$t_{\text{в}}$ – тривалість розробки концепції безпеки інформації у організації, годин;

$t_{\text{в}}$ =14 годин;

$t_{\text{а}}$ – тривалість процесу аналізу рисків, годин;

$t_а$ =18 годин;

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

$t_{вз}$ = 9 годин;

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

$t_{озб}$ = 23 години;

$t_{овр}$ – тривалість організації виконання відновлюваних робіт і забезпечення неперервного функціонування організації, годин;

$t_{овр}$ =15 годин;

$t_д$ – тривалість документального оформлення КСЗІ, годин;

$t_д$ = 10 годин.

t = 13 + 14 + 18 + 9 + 23 + 15 + 7 = 102 години.

3.1.2 Розрахунок витрат на створення КСЗІ

Визначимо витрати на створення КСЗІ за допомогою формули (3.2).

$$К_{рп} = З_{зп} + З_{мч}\text{ , грн.,} \tag{3.2}$$

де $К_{рп}$ – витрати на розробку КСЗІ, грн.;

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

$З_{мч}$ – вартість машинного часу, що необхідний для розробки політики безпеки, грн.

Витрати на розробку складаються з витрат на заробітну плату спеціаліста інформаційної безпеки, формула (3.3), і з вартості машинного часу під час розробки, формула (3.4).

$$З_{зп} = t + З_{іб}\text{ , грн.,} \tag{3.3}$$

де t – загальна тривалість розробки КСЗІ, годин;

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

Згідно статистики [18] заробітна плата спеціаліста з інформаційної безпеки 7047 грн. $З_{іб}$ = 7047/40 = 176 грн/годину.

$З_{зп} = 102 \cdot 176 = 17952$ грн.

$$З_{мч} = t \cdot С_{мч}\text{ , грн,} \qquad (3.4)$$

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

t = 102 години;

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

Вартість 1 години машинного часу ПК визначається за формулою (3.5).

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}\text{ , грн./година,} \qquad (3.5)$$

де P – встановлена потужність ПК, кВт;

P = 0,4 кВт;

$t_{нал}$ – кількість задіяних робочих станцій;

$t_{нал}$ = 1;

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

$С_е$ = 1.68 грн./(кВ·год);

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

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

$Н_а$ = 1/5 = 0.2;

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

$Н_{апз}$ = 1/2 = 0.5;

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

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

Для визначення залишкової вартості необхідно знайти накопичену амортизацію ПК. Вартість ПК – 19520 грн., мінімальний термін корисної служби – 60 місяців, термін використання ПК – 40 місяців.

$Ф_{зал} = 19520 – (19520 \cdot 40)/60 = 6507$ грн.

В таблиці 3.2 визначена вартість закупівлі ліцензійного програмного забезпечення.

Таблиця 3.2 Вартість закупівлі ліцензійного програмного забезпечення

Програмне забезпечення	Вартість, грн.
Варіант 1	
Mem Reduct	Безкоштовно
Automize 12	4370
Варіант 2	
«Гриф-Мережа»	7010

$К_{лпз1} = 4370$ грн.;

$К_{лпз2} = 7010$ грн.;

$$C_{мч1} = 0.4 \cdot 1 \cdot 1.68 + \frac{6507 \cdot 0.2}{1920} + \frac{4370 \cdot 0.5}{1920} = 2.49 \text{ грн./година;}$$

$$C_{мч2} = 0.4 \cdot 1 \cdot 1.68 + \frac{6507 \cdot 0.2}{1920} + \frac{7010 \cdot 0.5}{1920} = 3.17 \text{ грн./година;}$$

$З_{мч1} = 102 * 2.49 = 254$ грн. ;

$З_{мч2} = 102 * 3.17 = 323.3$ грн. ;

$К_{рп1} = 17952 + 254 = 18206$ грн. ;

$К_{рп2} = 17952 + 323.3 = 18275.3$ грн.

3.1.3 Капітальні (фіксовані) витрати на створення комплексу

На впровадження проектних рішень кваліфікаційної роботи вирахуємо капітальні витрати, формула (3.6).

$$К = К_{рп} + К_{зпз} + К_{рп} + К_{аз} + К_{навч} + К_{н}, \text{ грн.,} \quad (3.6)$$

де $К_{рп}$ – вартість розробки проекту КСЗІ та залучення для цього зовнішніх консультантів, грн.;

$К_{рп1}$ = 18206 грн.;

$К_{рп2}$ = 18275.3 грн.;

$К_{зпз}$ –вартість закупівлі ліцензійного основного та додаткового ПЗ, грн.;

$К_{зпз1}$ = 4370 грн.;

$К_{зпз2}$ = 7010 грн.;

$К_{рп}$ – вартість розробки КСЗІ, грн.;

$К_{рп}$ = 16000 грн.;

$К_{аз}$ –вартість закупівлі апаратного забезпечення та допоміжних матеріалів, грн.;

$К_{аз}$ = 10026 грн.;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, грн.;

$К_{навч}$ = 12000 грн.;

$К_{н}$ – витрати на встановлення обладнання та налагодження КСЗІ, грн;

$К_{н1}$ = 6750 грн.;

$К_{н2}$ = 14250 грн.;

$К_1$ = 18206 + 4370 + 16000 + 10026 + 12000 + 6750 = 67352 грн.;

$К_2$ = 18275.3 + 7010 + 16000 + 8925 + 12000 + 14250 = 77561.3 грн.

3.2 Розрахунок експлуатаційних витрат

Для визначення витрат на обслуговування КСЗІ, формула (3.7), порахуємо витрати на оновлення і модернізацію, витрати на керування КСЗІ, формула (3.8), та витрати від активності користувачів.

$$С = С_в + С_к + С_{ак}, \text{ грн.} \quad (3.7)$$

де С – витрати на функціонування КСЗІ, грн.;

$С_в$ – витрати на оновлення й модернізацію КСЗІ, грн.;

$С_к$ – витрати на керування КСЗІ, грн.;

$С_{ак}$– витрати викликані активністю користувачів системи, грн.

Так як в вартість ліцензії програмного забезпечення входить постійне підтримання і оновлення до нових версій – витрати на оновлення і модернізацію не виникають.

$С_в = 0$ грн.

Для використання КСЗІ в ІТС необхідно 3 рази за рік провести тренінги обслуговуючого персоналу за 4000 грн.

$С_{ак} = 12000$ грн.

$$С_к = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн.}, \quad (3.8)$$

де $С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$С_н = 12000$ грн.;

$С_а$ – річний фонд амортизаційних відрахувань;

$С_{а1} = 4370/2 = 2185$ грн.;

$С_{а2} = 7010/2 = 3505$ грн.;

$С_з$ – річний фонд заробітної плати інженерно-технічного персоналу, грн.;

$С_{єв}$ – витрати єдиного внеску на загальнообов’язкове соціальне страхування, грн.;

$С_{ел}$ – вартість електроенергії, що споживається апаратурою КСЗІ протягом року, грн.;

$С_о$ – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу, грн.;

$С_о = 0$ грн;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс КСЗІ, грн.;

$С_{тос1} = 67352 \cdot 0.03 = 1987.5$ грн.;

$С_{тос2}$ = 77561.3 · 0.03 = 2326.8 грн.

$$С_з = З_{осн} + З_{дод}, \text{ грн.}, \quad (3.9)$$

де $З_{осн}$ – основна заробітна плата, грн.;

$З_{дод}$ – додаткова заробітна плата, грн.

Так як виконання робіт вимагає залучення спеціаліста з інформаційної безпеки, в результаті співбесіди з керівниками було вирішено наймати стороннього.

$З_{осн}$ = 17000 · 0.25 · 12 = 51000 грн.;

$З_{дод}$ = 0,1·Зосн = 5100 грн.;

Порахуємо річний фонд заробітної плати інженерно-технічного персоналу згідно формули (3.9):

$С_з$ = 51000 + 5100 = 56100 грн.;

$С_{св}$ = 56100 · 0,22 = 12342 грн.

Вартість споживання електроенергії апаратурою КСЗІ визначається за формулою (3.11).

$$С_{ел} = P \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.10)$$

де Р – встановлена потужність апаратури КСЗІ, кВт;

Р = 0,4 кВт;

$F_р$ – річний фонд робочого часу КСЗІ, годин;

$F_р$ = 1920 годин;

$Ц_е$ – тариф на електроенергію, грн./кВт за годину;

$Ц_е$ = 1,68 грн./кВт за годину.

$С_{ел} = 0.65 \cdot 1920 \cdot 1.68 = 2096$ грн.;

$С_{к1} = 12000 + 2185 + 56100 + 12342 + 2096 + 0 + 1987.5 =$ 86710.5 грн.;

$C_{к2} = 12000 + 3505 + 56100 + 12342 + 2096 + 0 + 2326.8 =$ 88369.8 грн.;

$C_1 = 0 + 86710.5 + 12000 =$ 98710.5 грн.;

$C_2 = 0 + 88369.8 + 12000 =$ 100369.8 грн.

3.3 Оцінка величини збитку

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі визначається за формулою (3.11):

$$U = П_п + П_в + V, \text{ грн.}, \quad (3.11)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн.;

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

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

Втрати робочого часу і простою співробітників визначаються за формулою (3.12):

$$П_п = \frac{\sum З_c}{F} t_п, \text{ грн.}, \quad (3.12)$$

де $З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн. за місяць;

F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 годин), годин;

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

$t_п$ = 2 години.

Для визначення заробітної плати атакованого вузла визначимо заробітну плату співробітників у таблиці 3.3.

$\sum З_с = 192150$ грн.;

$П_п = \frac{192150}{176} \cdot 2 = 2183.5$ грн.

Таблиця 3.3 –Заробітна плата співробітників за місяць з нарахуванням ЄСВ

Посада	Кількість працівників, осіб	Місячна заробітна плата, грн.	Єдиний соціальний внесок, грн.	Витрати на заробітну плату з урахуванням ЄСВ, грн.
Директор	1	17000	3740	20740
Юрист	1	15000	3300	18300
Помічник юриста	1	10000	2200	12200
Спеціаліст з продажу	1	15000	3300	18300
Спеціаліст ЗЕД	3	13500	2970	49410
Секретар	1	10000	2200	12200
Бухгалтер	2	10000	2200	24400
Системний адміністратор	1	15000	3300	18300
Адміністратор безпеки	1	15000	3300	18300

Вартість відновлення вузла визначається за формулою (3.13):

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.}, \quad (3.13)$$

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.;

$П_{зч}$ = 5200 грн.

Знайдемо витрати на повторне уведення інформації за формулою (3.14):

$$П_{ви} = \frac{\sum З_c}{F} \cdot t_{ви}, \text{ грн.}, \quad (3.14)$$

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

$t_{ви}$ = 3 години.

$$П_{ви} = \frac{192150}{176} \cdot 3 = 3275.3 \text{ грн.}$$

Витрати на повторне введення інформації визначимо за формулою (3.15):

$$П_{пв} = \frac{\sum З_о}{F} \cdot t_в, \text{ грн.}, \quad (3.15)$$

де $t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, години;

$t_в$ = 3 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн.

Заробітна плата адміністраторів 15000 грн на місяць і 17000 грн. за 0.25 ставки.

$$П_{пв} = \frac{15000+4250}{176} \cdot 3 = 328.1 \text{ грн.};$$

$$П_в = 3275.3 + 328.1 + 5200 = 8803.4 \text{ грн.}$$

Знайдемо витрати від зниження обсягу продажів за час простою згідно формули (3.16):

(3.16)

$$V = \frac{О}{F_г} \cdot (t_п + t_в + t_{ви}), \text{ грн.},$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижнів, 5-ти денний робочий тиждень, 8-ми годинний робочий день);

$F_г = 2080$ годин;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн. у рік;

О = 5 млн. грн. у рік.

$V = \frac{5000000}{2080} \cdot (2 + 3 + 3) = 19230.7$ грн.;

$U = 2183.5 + 8803.4 + 19230.7 = 30217.6$ грн.

Таким чином загальний збиток від атаки на вузол визначимо за формулою (3.17):

$$B = \sum_i \sum_n U \qquad (3.17)$$

де I – число атакованих вузлів або сегментів корпоративної мережі;

I = 1;

N – середнє число атак на рік;

N = 5.

$B = \sum_1 \sum_5 30217.6 = 151088$ грн.

Величина загального збитку повинна бути скорегована на величину збитку, яка може бути завдана в результаті дій системного адміністратора. Для ТОВ «Pure glycerin» такий збиток може складати 100000 грн. та діями співробітників, величина збитку в такому випадку буде – 50000 грн.

$B = 151088 + 100000 + 50000 = 301088$ грн.

3.4 Загальний ефект від впровадження КСЗІ

З урахуванням ризиків порушення інформаційної безпеки можна визначити загальний ефект від впровадження КСЗІ за формулою (3.18).

$$E = B \cdot R - C, \text{ грн.}, \quad (3.18)$$

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

R – очікувана ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію КСЗІ, грн;

$E_1 = 301088 \cdot 0.57 - 98710.5 = 72909.6$ грн.;

$E_2 = 301088 \cdot 0.57 - 100369.8 = 71250.3$ грн.

3.5 Визначення та аналіз показників економічно ефективності системи

Коефіцієнт повернення інвестицій ROSI показує, скільки запобігає підприємство можливих втрат від атаки на сегмент корпоративної мережі від впровадження КСЗІ. Визначимо коефіцієнт ROSI за формулою (3.19):

$$ROSI = \frac{E}{K}, \text{ частки одиниць}, \quad (3.19)$$

де Е – загальний ефект від впровадження КСЗІ, грн.;

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

$ROSI_1 = \frac{72909.6}{67352} = 1.08;$

$ROSI_2 = \frac{71250.3}{77651.3} = 0.91.$

Проект побудови КСЗІ вважається доцільним за умови перевищення бажаного значення показника ефективності $E_н$, формула (3.20).

$$ROSI > E_н, \text{ частки одиниць}, \quad (3.20)$$

де Ен – бажане значення показника ефективності, частки одиниць.

Для підприємства «Pure glycerin» інформаційна безпека здійснюється за рахунок позикових коштів, тобто банківського кредиту. В такому разі показник ефективності визначається за формулою (3.21):

$$E_н = \frac{N_{кр}+N_{інф}}{100}, \text{ частки одиниць,} \quad (3.21)$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{кр}$ = 0.24 %;

$N_{інф}$ – річний рівень інфляції, %;

$N_{інф}$ = 100.7 %.

$E_н = \frac{0.24+100.7}{100} = 1;$

1) $1.08 > 1;$

2) $0.91 < 1.$

Визначимо термін окупності капітальних інвестицій за рахунок впровадження КСЗІ, формула (3.22).

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.22)$$

$T_{O1} = \frac{1}{1.08} = 0.93$ роки;

$T_{O1} = \frac{1}{0.91} = 1.1$ роки.

Термін окупності КСЗІ для першого варіанту T_{01} = 11.2 місяця, для другого – T_{02} = 13.2 місяців.

3.6 Висновок

В економічному розділі було проаналізовано основні економічні показники для впровадження КСЗІ і визначено, що перший варіант є економічно доцільним, а другий – ні. За результатами першого варіанту було визначено, що:

– капітальні витрати становлять 67352 грн.;

– експлуатаційні витрати становлять 98710.5 грн.;

– загальний збиток від атаки на сегмент корпоративної мережі складає 301088 грн.;

– ефект від впровадження КСЗІ становить 72909.6 грн;

– термін окупності капітальних інвестицій складає 11.2 місяця.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було проаналізовано необхідність забезпечення інформаційної безпеки на підприємстві ТОВ «Pure glycerin» і створення КСЗІ, виконано обстеження середовищ функціонування: фізичного середовища, обчислювальної системи, інформаційного середовища і середовища користувачів. Проведено аналіз та оцінку потенційних порушників і загроз інформації. На основі результатів аналізу було визначено вимоги до системи захисту інформації від НСД.

В рамках другого розділу був проведений аналіз сучасного стану реалізації послуг безпеки інформації і сформовані вимоги. Згідно з результатами проведеного аналізу з врахуванням актуальних загроз інформації були запропоновані проектні рішення: розроблені положення безпеки, змінені атрибути доступу користувачів, забезпечене резервування до мережі Інтернет, розмежований внутрішній трафік, забезпечення серверів ДБЖ, реалізовані послуги безпеки.

Під час виконання економічного розділу був розрахований більш доцільний варіант з впроваджених двох, економічні показники якого складали: капітальні витрати – 67352 грн., експлуатаційні витрати – 98710.5 грн. В результаті аналізу загроз загальний збиток внаслідок виникнення інциденту інформаційної безпеки може складати 301088 грн. Загальний ефект від впровадження КСЗІ становить 72909.6 грн з терміном окупності капітальних інвестицій в 11.2 місяця.

Для повної реалізації КСЗІ необхідні виконати впровадження запропонованих рішень, виконати попередні випробування, дослідну експлуатацію і виконання державної експертизи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про інформацію: Закон України від 01.07.2014 р. № 1556-VII. Дата оновлення 16.07.2020 р. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#Text

2. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення від 23.04.2021 р. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

3. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. Дата оновлення від 04.07.2020 р. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80

4. Цивільний кодекс України: Закон, Кодекс від 16.01.2003 р. № 435-IV. Дата оновлення від 27.05.2021 р. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/435-15#Text

5. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22). [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-005--99.pdf

6. НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (введено в дію Наказом ДСТСЗІ СБУ від 08.11.2005 р. № 125). [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/3.7-003-2005.pdf

7. НД ТЗІ 1.6-005-2013 «Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» (введено в дію

Наказом ДССЗЗІ від 15.04.2013 р. № 215). [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.6-005-2013.pdf

8. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (введено в дію Наказом ДСТСЗІ СБУ від 28.04.1999 р. № 22). [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf

9. Перелік засобів ТЗІ ДССЗЗІ від 29.04.2021 р. [Електронний ресурс] – Режим доступу до ресурсу: https://cip.gov.ua/services/cm/api/attachment/download?id=37706

10. Експертний висновок №1027 (дійсний з 26.09.2019 до 26.09.2022) «Державна експертиза за критеріями технічного захисту інформації операційної системи Microsoft Windows 10 Professional. Технічні вимоги». [Електронний ресурс] – Режим доступу до ресурсу: http://download.microsoft.com/documents/ukraine/certificates/MS/Windows.10.Pro.pdf

11. Підключення провайдерів мережі Інтернету за адресою в Дніпрі. [Електронний ресурс] – Режим доступу до ресурсу: http://www.multitest.ua/internet-v-kvartiru/dnepropetrovsk/marshala-malinovskogo-ul/2/#/v-ofis

12. Рейтинг Інтернет-провайдерів. [Електронний ресурс] – Режим доступу до ресурсу: https://2ip.ua/ru/services/providers-rating?act=2&city=%D0%94%D0%BD%D0%B5%D0%BF%D1%80%D0%BE%D0%BF%D0%B5%D1%82%D1%80%D0%BE%D0%B2%D1%81%D0%BA

13. Методичні вказівки налаштування функції «SGMP Snooping» комутаторів D-Link. [Електронний ресурс] – Режим доступу до ресурсу: https://www.dlink.ru/ru/faq/58/264.html

14. Методичні вказівки до програми перегляду стану джерела безперебійного живлення Network UPS Tools. [Електронний ресурс] – Режим доступу до ресурсу: https://networkupstools.org/docs/developer-guide.chunked/index.html

15. Методичні рекомендації до програмного забезпечення PowerManager II для джерела безперебійного живлення. [Електронний ресурс] – Режим доступу до ресурсу: https://logicfox.info/manuals/LP/UPS/0649/PowerManagerII.pdf

16. Опис комплексу засобів захисту інформації від несанкціонованого доступу «Гриф-Мережа». Інститут комп'ютерних технологій [Електронний ресурс] – Режим доступу до ресурсу: http://www.ict.com.ua/?lng=1&sec=10&art=41

17. Експертний висновок КЗЗ «Гриф-Мережа» версії 3, виробництва ТОВ «Інститут комп'ютерних технологій» №1034 (з 24.10.2019 до 24.10.2022). [Електронний ресурс] – Режим доступу до ресурсу: http://www.ict.com.ua/im/certif/exp_visn_GM.jpg

18. Програма для очистка оперативної пам'яті – Mem Reduct [Електронний ресурс] – Режим доступу до ресурсу: https://www.henrypp.org/product/memreduct

19. Методичні вказівки до програми автоматизації Automize 12 [Електронний ресурс] – Режим доступу до ресурсу: http://www.hiteksoftware.com/help/english/gui/basics.htm

20. Статистика заробітної плати спеціаліста з інформаційної безпеки в Україні. [Електронний ресурс] – Режим доступу до ресурсу: https://ua.trud.com/ua/salary/2/67683.html

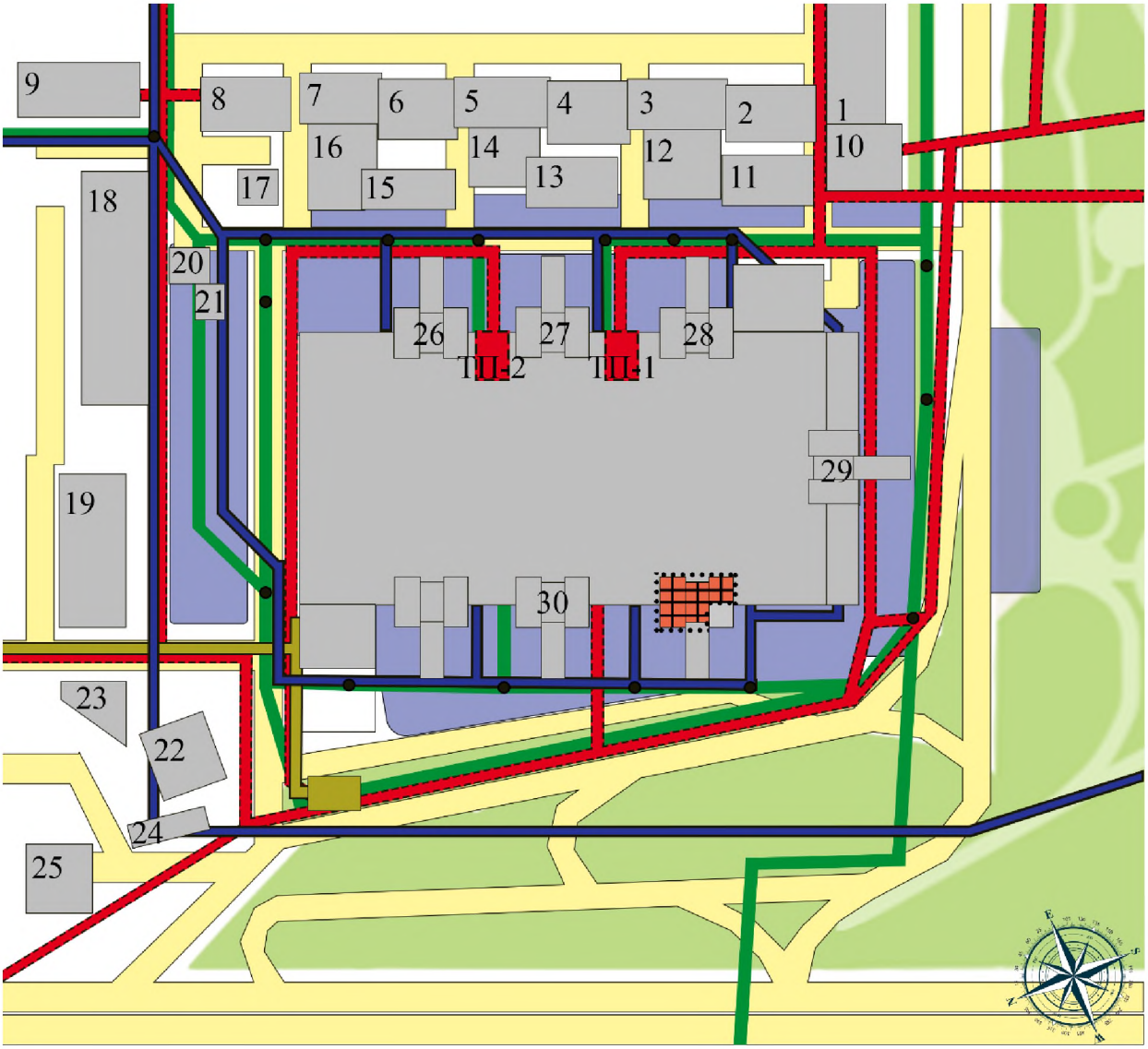
21. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП», 2020. – 47 с.

22. Методичні вказівки до виконання економічної частини дипломного проекту /Упоряд.: Д. П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	-
2	А4	Список умовних скорочень	1	-
3	А4	Зміст	2	-
4	А4	Вступ	1	-
5	А4	Стан питання. Постановка задачі	41	-
6	А4	Спеціальна частина	18	-
7	А4	Економічний розділ	15	-
8	А4	Висновки	1	-
9	А4	Перелік посилань	3	-
10	А4	Додаток А	1	-
11	А4	Додаток Б	6	-
12	А4	Додаток В	12	-
13	А4	Додаток Г	1	-
14	А4	Додаток Д	1	-
15	А4	Додаток Е	1	-
16	А4	Додаток Ж	1	-

ДОДАТОК Б. Плани та схеми систем ОІД



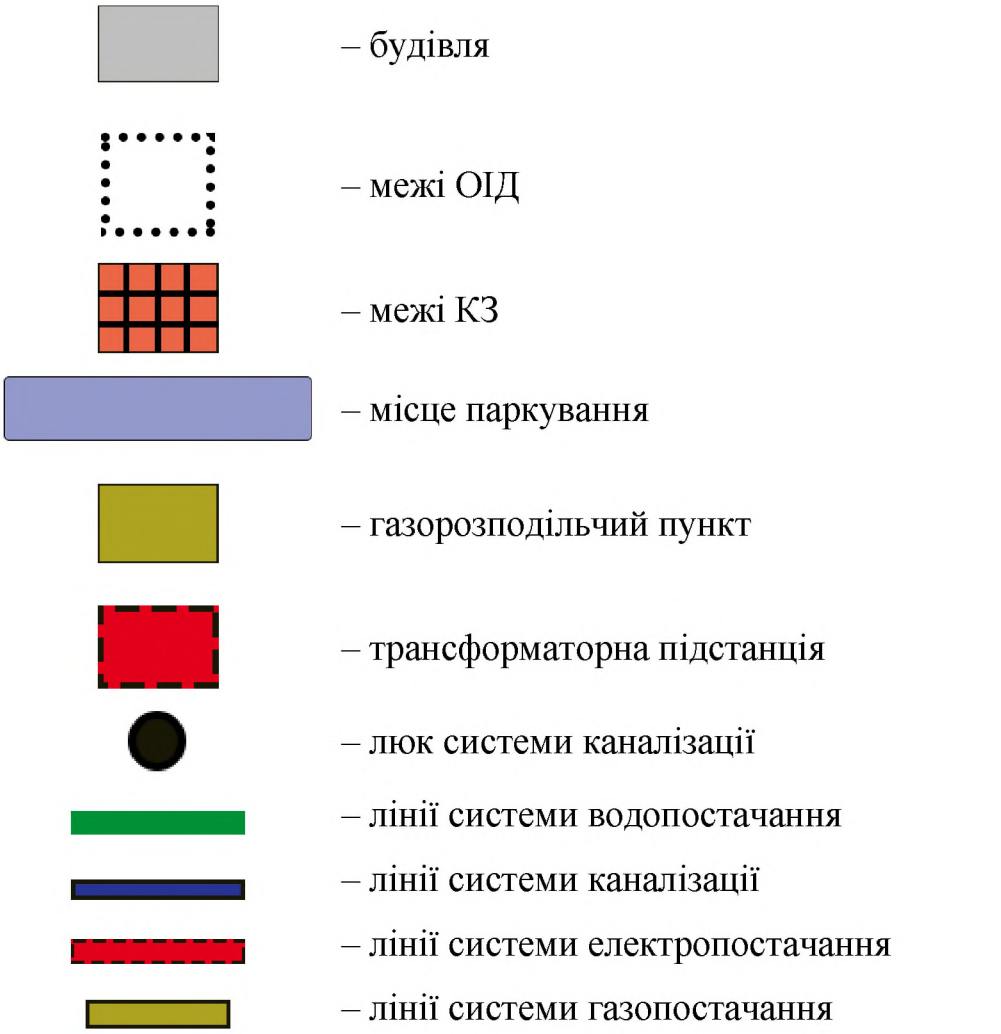
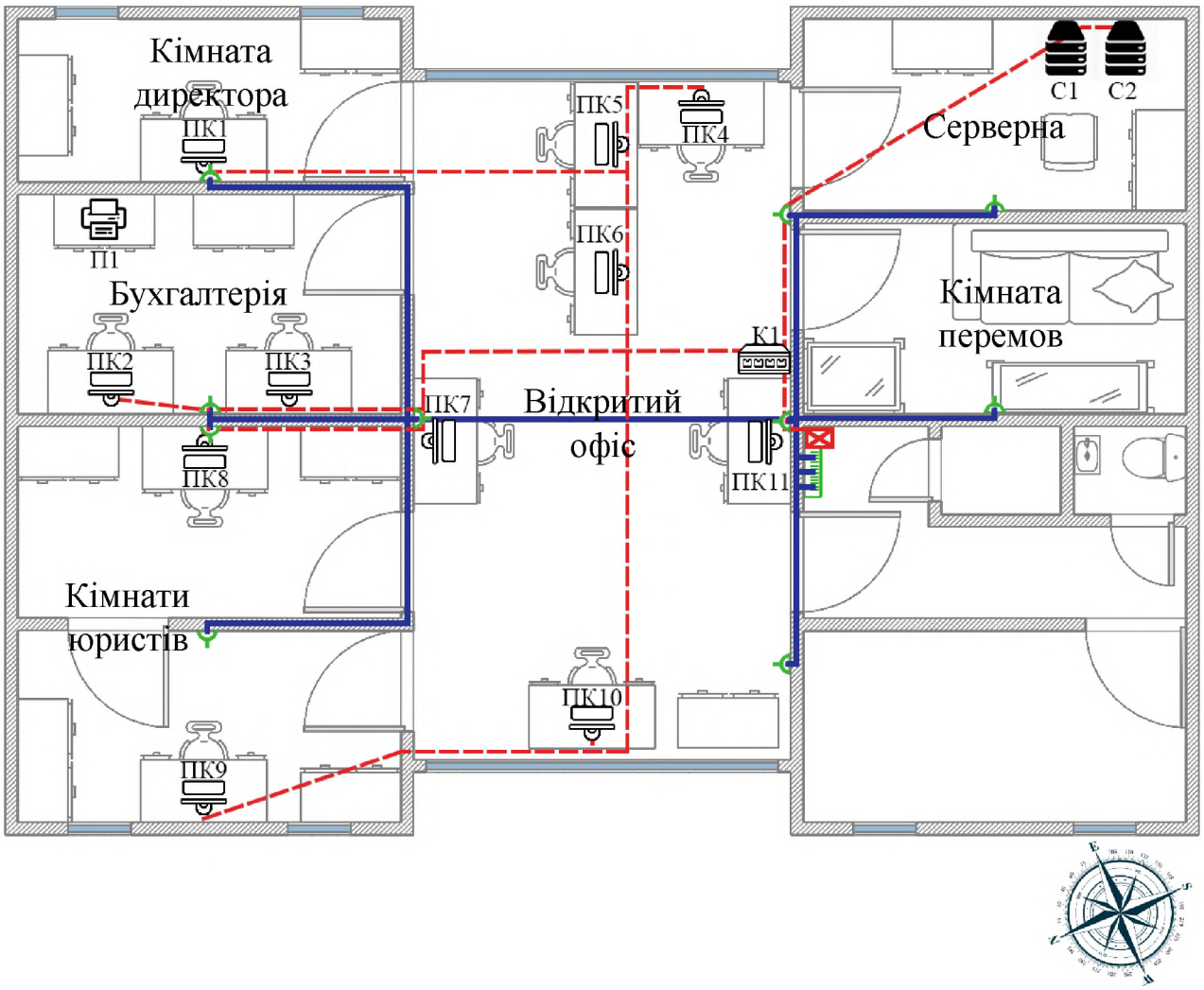
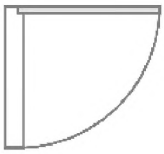
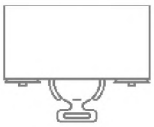


Рисунок Б.2 Умовні позначення ситуаційного плану


Кімната директора
ПК1
П1
Бухгалтерія
ПК2
ПК3
ПК8
Кімнати юристів
ПК9
ПК5
ПК4
ПК6
ПК7
Відкритий офіс
ПК10
К1
ПК11
C1
C2
Серверна
Кімната перемов


– двері


– робоче місце


– тумба


– персональний комп’ютер


– комутатор


– сервер


– розподільчий щиток поверху

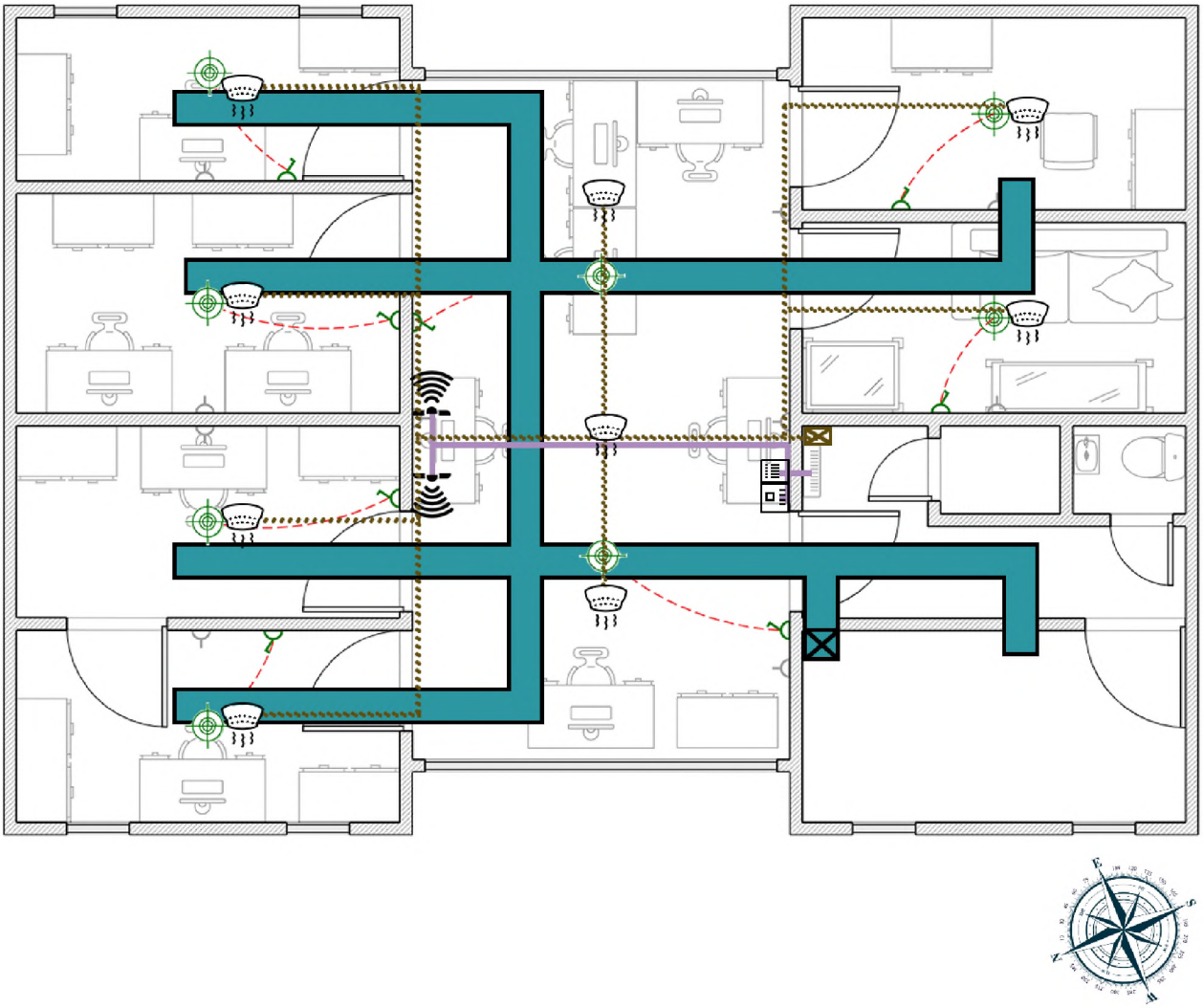

– розетка

– лінія системи комп’ютерної мережі


– лінія системи електропостачання


– лінія з’єднання системи комп’ютерної мережі з поверхами нижче

Рисунок Б.4 Умовні позначення генерального плану




– ПКП «Лунь 9»


– індикатор зон «Линд-8»


– вмикач/вимикач


– ІЧ датчик


– лампа системи освітлення


– лінія системи вентиляції і опалення

– лінія системи охоронної мережі


– датчик диму


– лінія системи пожежної системи


– лінія з’єднання пожежної системи з поверхами нижче


– лінія з’єднання системи вентиляції і опалення з поверхами нижче

Рисунок Б.6 Умовні позначення технічних систем генерального плану

ДОДАТОК В. Склад і характеристика ОТЗ і ДТЗС в ІТС

Таблиця В.1 – Перелік ОТЗ

Назва	Марка	Модель	Серійний номер	Розмі-щення	Відстань до границі КЗ, м
Системний блок ПК1	Vinga	Winston	UTA13UT76R	На столі	1
Системний блок ПК2	Vinga	Winston	TDBNN8IVWV	На столі	1
Системний блок ПК3	Vinga	Winston	LL6ZIGCPYV	На столі	1
Системний блок ПК4	Vinga	Winston	I5TUBDDDPW	На столі	0,3
Системний блок ПК5	Vinga	Winston	2RTX6U6R7K	На столі	1
Системний блок ПК6	Vinga	Winston	NLJW5SGKJU	На столі	1
Системний блок ПК7	Vinga	Winston	FERP2GAFG2	На столі	1
Системний блок ПК8	Vinga	Winston	D5O0JUI6IG	На столі	1
Системний блок ПК9	Vinga	Winston	L5E0A66ZNN	На столі	1
Системний блок ПК10	Vinga	Graphyte	9FCPGEBDJ3	На столі	0,3

Продовження таблиці В.1

Назва	Марка	Модель	Серійний номер	Розмі-щення	Відстань до границі КЗ, м
Системний блок ПК11	Vinga	Graphyte	3XZJDU8I78	На столі	1
Монітор ПК1	Dell	SE2219H Black	80106347273	На столі	1
Монітор ПК2	Dell	SE2219H Black	58388030128	На столі	1
Монітор ПК3	Dell	SE2219H Black	34259946454	На столі	1
Монітор ПК4	Dell	SE2219H Black	19031505802	На столі	0,3
Монітор ПК5	Dell	SE2219H Black	28345019125	На столі	0,6
Монітор ПК6	Dell	SE2219H Black	10955073408	На столі	1
Монітор ПК7	Dell	SE2219H Black	41346219495	На столі	1
Монітор ПК8	Dell	SE2219H Black	43001621757	На столі	1
Монітор ПК9	Dell	SE2219H Black	57441112900	На столі	1

Продовження таблиці В.1

Назва	Марка	Модель	Серійний номер	Розмі-щення	Відстань до границі КЗ, м
Монітор ПК10	Lenovo	ThinkVision T22i-10	29057912486	На столі	0,3
Монітор ПК11	Lenovo	ThinkVision T22i-10	44858582768	На столі	1
Клавіатура ПК1 USB	Vinga	KB110BK	927776087766	На столі	1
Клавіатура ПК2 USB	Vinga	KB110BK	743531175305	На столі	1
Клавіатура ПК3 USB	Vinga	KB110BK	337392297172	На столі	1
Клавіатура ПК4 USB	Vinga	KB110BK	485289773798	На столі	0,4
Клавіатура ПК5 USB	Vinga	KB110BK	244124093320	На столі	0,6
Клавіатура ПК6 USB	Vinga	KB110BK	602444732763	На столі	1
Клавіатура ПК7 USB	Vinga	KB110BK	579321767347	На столі	1
Клавіатура ПК8 USB	Vinga	KB110BK	036151984801	На столі	1

Продовження таблиці В.1

Назва	Марка	Модель	Серійний номер	Розмі-щення	Відстань до границі КЗ, м
Клавіатура ПК9 USB	Vinga	KB110BK	457239902024	На столі	1
Клавіатура ПК10 USB	Vinga	KB110BK	024122850456	На столі	0,6
Клавіатура ПК 11 USB	Vinga	KB110BK	352155894062	На столі	1
Сервер S1	Zalman	Z9 NEO Plus	ZWSTM13XLDIK	На підлозі	1
Сервер S2	Zalman	Z9 NEO Plus	W2XQBZT0N8T4	На підлозі	0,2
Комутатор К1	D-Link	DGS-1100-16V2	235447	На підлозі	0,2
Принтер П1	Canon	Pixma MG3640S	QJZXBFOVC031	На столі	1

Таблиця В.2 – Перелік ДТЗС

Назва	Марка	Модель	Серійний номер	Розміщення
Маніпулятор «миша»	Logitech	B100 Black	HFXPGLVEO8XDB	На столі біля ПК1
			G70JJKKD2FA4B	На столі біля ПК2
			HRO5XVK80951O	На столі біля ПК3
			EOG0MUBFQB8ZH	На столі біля ПК4
			SEYEP373EJUMF	На столі біля ПК5
			BDDC3UABBC91K	На столі біля ПК6
			2LNTJYF2QHZJI	На столі біля ПК7
			93OI9WQNJJQUC	На столі біля ПК8
			LHT1X17HLWGNQ	На столі біля ПК9
			VA28L1S7RZMAT	На столі біля ПК10
			0V07MT7LVW8WA	На столі біля ПК11
Датчик диму	Артон	СПД-3.10 Б3	61148270	На стелі
			73501207	
			90506591	

Продовження таблиці В.2

Назва	Марка	Модель	Серійний номер	Розміщення
			29364822	
			32673814	
			76492275	
			26465784	
			23098192	
ІЧ датчик	Сател	Topaz	8532103699	На стелі
			8531103030	
Приймально-контрольний прилад	Лунь	Лунь-9Р	36886256	Біля вхідних дверей
Панель охорони	Лунь	Линд-8	36840203	Біля вхідних дверей
Люмінесцентна лампочка – 32 штуки	PHILIPS	TLD58W/830	-	На стелі

Таблиця В.3 – Характеристика апаратних засобів ІТС

Назва	Характеристика	Марка, модель	Серійний номер
Монітор ПК1	Монітор	Dell SE2219H Black	80106347273
Монітор ПК2	Монітор	Dell SE2219H Black	58388030128
Монітор ПК3	Монітор	Dell SE2219H Black	34259946454
Монітор ПК4	Монітор	Dell SE2219H Black	19031505802
Монітор ПК5	Монітор	Dell SE2219H Black	28345019125
Монітор ПК6	Монітор	Dell SE2219H Black	10955073408
Монітор ПК7	Монітор	Dell SE2219H Black	41346219495
Монітор ПК8	Монітор	Dell SE2219H Black	43001621757
Монітор ПК9	Монітор	Dell SE2219H Black	57441112900
Монітор ПК10	Монітор	Lenovo ThinkVision T22i-10	29057912486
Монітор ПК11	Монітор	Lenovo ThinkVision T22i-10	44858582768
ПК1	Процесор	Ryzen 5 3600	13KTO6G7P73LK
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SB5AS7CIYZYZ
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	120790768893
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6OYQFH2F2
ПК2	Процесор	Ryzen 5 3600	B99D4OAU4NSJT
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBPF830IOT4K

Продовження таблиці В.3

Назва	Характеристика	Марка, модель	Серійний номер
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	685672439772
	Жорсткий диск	HDD WD Blue 1 Tb	WCC65NMR07BW
ПК3	Процесор	Ryzen 5 3600	93T07PDY8I8GS
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SB2OGC6LMZHA
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	015105835685
	Жорсткий диск	HDD WD Blue 1 Tb	WCC63SKP5KP5
ПК4	Процесор	Ryzen 5 3600	604HH1JG8O67G
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBEF5V7NNJYA
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	482099324588
	Жорсткий диск	HDD WD Blue 1 Tb	WCC63F3N3X33
ПК5	Процесор	Ryzen 5 3600	DGRIUJQLUHW74
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBBXFZNN8TO5
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	900468892793
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6ZD4FZE2E

Продовження таблиці В.3

Назва	Характеристика	Марка, модель	Серійний номер
ПК6	Процесор	Ryzen 5 3600	YHLA1XOFS69Q1
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBD0X5XOFB54
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	HS1584619844
	Жорсткий диск	HDD WD Blue 1 Tb	WCC61STU4NHW
ПК7	Процесор	Ryzen 5 3600	BC7Z0QS280EYO
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBCP9HW0MW0H
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	515052014422
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6S2F2G67S
ПК8	Процесор	Ryzen 5 3600	2WCMLF1AYSXCF
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SB1CYUABYFQ3
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	408603221297
	Жорсткий диск	HDD WD Blue 1 Tb	WCC61G7PX6O3
ПК9	Процесор	Ryzen 5 3600	S13HI029290SC
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBQOS86TAG13

Продовження таблиці В.3

Назва	Характеристика	Марка, модель	Серійний номер
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	517539821565
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6HCYW2CDW
ПК10	Процесор	Ryzen 5 3600	S8OG4SBUFHJF5
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SBP1O148BWE2
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	781972430979
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6Y2QG2W9J
ПК11	Процесор	Ryzen 5 3600	QP3TVIHBVT3TY
	Материнська плата	MSI B450-A PRO MAX	601-7B86-02SB6VGZ25GZU5
	Оперативна пам’ять	Samsung 8 GB DDR4 2666 MHz	546025860641
	Жорсткий диск	HDD WD Blue 1 Tb	WCC6LOBXRA08
Маніпулятор «миша» ПК1	Маніпулятор «миша»	Logitech B100 Black	HFXPGLVEO8XDB
Маніпулятор «миша» ПК2	Маніпулятор «миша»	Logitech B100 Black	G70JJKKD2FA4B
Маніпулятор «миша» ПК3	Маніпулятор «миша»	Logitech B100 Black	HRO5XVK80951O
Маніпулятор «миша» ПК4	Маніпулятор «миша»	Logitech B100 Black	EOG0MUBFQB8ZH

Продовження таблиці В.3

Назва	Характеристика	Марка, модель	Серійний номер
Маніпулятор «миша» ПК5	Маніпулятор «миша»	Logitech B100 Black	SEYEP373EJUMF
Маніпулятор «миша» ПК6	Маніпулятор «миша»	Logitech B100 Black	BDDC3UABBC91K
Маніпулятор «миша» ПК7	Маніпулятор «миша»	Logitech B100 Black	2LNTJYF2QHZJI
Маніпулятор «миша» ПК8	Маніпулятор «миша»	Logitech B100 Black	93OI9WQNJJQUC
Маніпулятор «миша» ПК9	Маніпулятор «миша»	Logitech B100 Black	LHT1X17HLWGNQ
Маніпулятор «миша» ПК10	Маніпулятор «миша»	Logitech B100 Black	VA28L1S7RZMAT
Маніпулятор «миша» ПК11	Маніпулятор «миша»	Logitech B100 Black	0V07MT7LVW8WA
Сервер С1	Процесор	Intel Xeon X5672	2WE36Y8PIFGRQ
	Материнська плата	Huananzhi X58 Deluxe (s1366, Intel X58, PCI-Ex16)	16LJA131
	Оперативна пам’ять – 2 штуки	Samsung 8 GB DDR3 1333 MHz	Y4NN5L0EB2HF 7VXBTMT798E0
	Жорсткий диск	SATA 4TB WD Raid Edition 5	WCC6FT7TL4K3
	Твердотільний накопичувач	Intel D3-S4510 Series 240GB	K4774QPH5P0Y
	RAID контролер	LSI 9211-8i HBA	1R2K761

Продовження таблиці В.3

Назва	Характеристика	Марка, модель	Серійний номер
Сервер С2	Процесор	Intel Xeon X5672	8K6T6QG1WMRZV
	Материнська плата	Huananzhi X58 Deluxe (s1366, Intel X58, PCI-Ex16)	F224AU33
	Оперативна пам’ять – 2 штуки	Samsung 8 GB DDR3 1333 MHz	1ALQ3I3FVLZC16WK152ZOHT5
	Жорсткий диск	SATA 4TB WD Raid Edition 5	WCC6FT7TL4K3
	Твердотільний накопичувач	Intel D3-S4510 Series 240GB	KBD251O57D5T
	RAID контролер	LSI 9211-8i HBA	1R653A2
Комутатор К1	Комутатор	D-Link DGS-1100-16V2	235447
Принтер П1	Принтер	Canon Pixma MG3640S	QJZXBFOVC031

ДОДАТОК Г. Форма та зміст акту категоріювання об’єкта

Прим. N ___

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
директор Шуліга А.М.
(посада, підпис, ініціали, прізвище)
16.05.2021

М. П.

АКТ
категоріювання приміщення ТОВ «Pure glycerin»
(найменування об'єкта категоріювання)

1. Підстава для категоріювання ___рішення про створення КСЗІ_____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,

_____
зміна ознаки, за якою була встановлена категорія об'єкта тощо;

_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

2. Вид категоріювання _____первинне_____
(первинне, чергове, позачергове)

_____
(у разі чергового або позачергового категоріювання вказується категорія, що була встановлена до цього категоріювання; посилання/реквізити на документ, яким було встановлено цю категорію)

3. На ОІД здійснюється обробка інформації технічними засобами
(обробка інформації технічними засобами та/або озвучування інформації)

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами та/або озвучується на об'єкті
_____конфіденційна інформація_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації"; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія _4 категорія _____

Голова комісії _____ Бойко Д.С
(підпис) (ініціали, прізвище)
Члени комісії: _____ Чемко Ю.А.
(підпис) (ініціали, прізвище)
16.05.2021

ДОДАТОК Д. Перелік документів на оптичному носії

1) Пояснювальна_записка_Павлов.docx
2) Пояснювальна_записка_Павлов.pdf
3) Презентація_Павлов.pptx

ДОДАТОК Е. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студента групи 125-17-1
Павлова Сергія Олексійовича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи ТОВ «Pure glycerin»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 87 сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС товариства з обмеженою відповідальністю «Pure glycerin» .

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, аналіз джерел загроз та вразливостей, виявлення актуальних загроз, формування вимог до рівня захищеності інформації від НСД, розробка проектних рішень та елементів політики безпеки.

Обґрунтовано рішення щодо резервування зовнішнього каналу та розмежування внутрішнього трафіку.

Практичне значення результатів кваліфікаційної роботи полягає у запропонованих правилах розмежування доступу.

До недоліків роботи можна віднести недостатньо обґрунтування методики аналізу загроз.

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

За час дипломування Павлов С.О. 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 «відмінно».

Керівник кваліфікаційної роботи, професор **Кагадій Т.С.**

Керівник спец. розділу, ст. викладач **Кручінін О.В.**

ДОДАТОК Ж. Відгук керівника економічної частини

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)