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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Коротуна Сергія Володимировича*

академічної групи *125-20-3*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-комунікаційної системи Новопавлівської сільської ради*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Коротуну С.В.*** **академічної групи** ***125-20-3***
(прізвище ім'я по-батькові) (шифр)

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

на тему ***Комплексна система захисту інформації інформаційно-комунікаційної системи Новопавлівської сільської ради***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Актуальність теми, обстеження ІКС, розробка моделі порушника та загроз. Вибір профіля захищеності.	30.05.2024
Розділ 2	Заходи програмно-організаційного рівня для підвищення безпеки інформації в КСЗІ	17.06.2024
Розділ 3	Техніко-економічне обґрунтування доцільності створення КСЗІ	23.06.2024

Завдання видано _____ *Валерій КОРНІЄНКО*
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ *Сергій КОРОТУН*
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 78 с., 19 рис., 23 табл., 4 додатка, 15 джерел.

Об'єкт розробки: інформаційно-комунікаційна система Новопавлівської сільської ради

Предмет розробки: комплексна система захисту інформації Новопавлівської сільської ради

Мета роботи: забезпечення достатнього рівня безпеки для Новопавлівської сільської ради.

У першому розділі було розглянуто актуальність теми кваліфікаційної роботи, обґрунтовано необхідність створення КСЗІ, проведено обстеження ІКС та проаналізовано організаційну структуру. Проаналізовані типи даних, які знаходяться на території ОІД, її місцезнаходження та захищеність. Визначено найактуальніші загрози та клас системи, після чого обрано необхідний профіль захищеності.

У другому розділі було розроблено рішення для подолання загроз, проаналізованих у першому розділі: впроваджено системи моніторингу, квоти та правильно налаштовано права розмежування доступом. Також застосовані вимоги, які зменшать загрозу витоку конфіденційної інформації.

У третьому розділі було обґрунтовано економічну доцільність створення КСЗІ, визначено, які можуть бути збитки при атаці на вузли корпоративної мережі. Розраховано капітальні та експлуатаційні витрати та коефіцієнт повернення інвестицій ROSI і термін окупності.

Практична цінність розробки полягає у захисті конфіденційності, цілісності та доступності важливих типів інформації в критичному ОІД.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ОБ'ЄКТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ПРАВИЛА РОЗМЕЖУВАННЯ ДОСТУПУ.

ABSTRACT

Explanatory note: 78 pp., 19 pic., 23 table, 4 app, 15 sources.

Development Object: Information and Communication System of Novopavlivska Village Council

Development Subject: Comprehensive Information Protection System of Novopavlivska Village Council

Purpose of the work: ensure a sufficient level of security for the Novopavlivka village council.

In the first section, the relevance of the topic of the qualification work was considered, the necessity for creating a CIPS was justified, an examination of the ICS was conducted, and the organizational structure was analyzed. The types of data located on the territory of the OIA, its location, and security were analyzed. The most relevant threats and the system class were determined, after which the necessary security profile was chosen.

In the second section, solutions were developed to overcome the threats analyzed in the first section: monitoring systems were implemented, quotas were set, and access rights were correctly configured. Additionally, requirements were applied to reduce the threat of confidential information leakage.

In the third section, the economic feasibility of creating the CIPS was substantiated, and potential losses from attacks on corporate network nodes were identified. Capital and operational expenses and the Return on Security Investment (ROSI) and payback period were calculated.

The practical value of the development lies in protecting the confidentiality, integrity, and availability of critical types of information within the critical IAO.

COMPREHENSIVE INFORMATION PROTECTION SYSTEM, INFORMATION ACTIVITY OBJECT, THREAT MODEL, INTRUDER MODEL, INFORMATION SYSTEM, CYBERSECURITY, ACCESS CONTROL RULES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АВПЗ – антивірусне програмне забезпечення;

АС – автоматизована система;

ДБЖ – джерело безперебійного живлення;

ДТЗ – допоміжні технічні засоби;

ІКС – інформаційно-комунікаційна система;

КСЗІ – комплексна системна захисту інформації;

КЗ – контрольована зона;

НД ТЗІ – нормативний документ технічного захисту інформації;

НСД – несанкціонований доступ;

ОС – операційна система;

ОІД – об’єкт інформаційної діяльності;

ОТЗ – основні технічні засоби;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ЦАЗІ – центр антивірусного захисту інформації.

ЗМІСТ

с.

ВСТУП

Інформація завжди була одним з найважливіших ресурсів для розвитку і прогресу людства. Інформаційне суспільство базується на інформації та розвиненій мережі послуг.

Завдяки цьому суспільству з'явився новий інформаційний-комунікаційний та економічний простір, і без залучення до нього в сучасному світі будь яка організація чи бізнес не зможуть вести конкурентноздатне існування. Це торкнулося усіх сфер суспільства: освіти, охорони здоров'я, культурних установ, члени яких або отримують, або надають інформацію, передаючи свої знання як послугу і швидке розповсюдження інформації, комунікацій та комп'ютерних технологій допомагає в цьому. Якщо раніше люди не сильно переймались кібербезпекою, то зараз, з розвитком технологій, потрібно все більше і більше звертати на це увагу, бо, окрім технологій, які допомагають людству, розвивається і шкідливе програмне забезпечення.

Реальність така, що наша залежність від технологій зростає, і ця залежність збережеться. Отже, постійний прогрес у методах і технологіях кібербезпеки є важливим для захисту нашого цифрового життя та активів.

Важливим завданням є навчати кібербезпеці та основам захисту інформації людей, які працюють в інформаційному середовищі для того, щоб зловмисники не досягали своїх цілей. Тому будь-яка організація має перш за все дбати про навченість працівників, який її обробляє.

Актуальність теми кваліфікаційної роботи пов'язана з великим спектром загроз для інформації та необхідності підвищення кваліфікації працівників у важливому об'єкті критичної інфраструктури.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про Новопавлівську сільську раду

Новопавлівська сільська рада є органом місцевого самоврядування, яка надає послуги громадянам територіальної громади; забезпечує реалізацію конституційних прав людини і громадянина; створює умови для забезпечення життєво важливих потреб та законних інтересів населення. Зареєстрована в 1997 році.

Організаційна структура Новопавлівської сільської ради представлена на рисунку 1.1.

Рисунок 1.1 – Організаційна структура

Рівень кваліфікації працівників Новопавлівської сільської ради представлений на таблиці 1.1.

Таблиця 1.1 – Характеристика працівників

№	Посада	Кількість працівників	Роль в системі	Рівень кваліфікації
1	Керівник	1	Системний адміністратор	Середній
2	Заступник керівника	1	Користувач	Середній
3	Секретар	1	Користувач	Високий
4	Бухгалтер	3	Користувачі	Низький
5	Системний адміністратор	1	Системний адміністратор	Високий
6	Прибиральниця	1	-	-

Обов’язки працівників:

– керівник – представляє громаду та сільську раду у відносинах з державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями різних форм власності. Організовує роботу сільської ради. Затверджує плани соціально-економічного розвитку громади та відповідає за управління комунальним майном та бюджетом громади. Забезпечує реалізацію соціальних програм, підтримку освіти, охорони здоров'я, культури, спорту та інших сфер соціальної політики на території громади;

– заступник керівника – виконує обов'язки сільського голови у випадку його відсутності (відпустка, відрядження, хвороба і т.д.) або в разі його відставки до обрання нового голови. Координує діяльність відділів, управлінь та інших виконавчих органів сільської ради. Допомагає в розробці бюджету громади та контролює його виконання. Працює над залученням інвестицій та фінансових

ресурсів для розвитку громади. Проводить прийоми громадян, розглядає їх звернення та скарги, допомагає вирішувати порушені питання;

– секретар – забезпечує підготовку матеріалів для розгляду на сесіях ради та веде протоколи засідань сільської ради та забезпечує їх зберігання. Веде облік звернень громадян, контролює їх розгляд та виконання. Забезпечує ділове листування сільської ради, підготовку та розсилку необхідних документів;

– бухгалтери – ведуть бухгалтерський облік, участь у підготовці проєкту бюджету громади, контроль за виконанням бюджету, аналіз відхилень та підготовка пропозицій щодо їх усунення. Аналіз фінансових операцій для виявлення можливих порушень чи недоліків. Розрахунок та нарахування заробітної плати працівникам сільської ради. Підготовка фінансових прогнозів та планів на майбутні періоди;

– системний адміністратор – моніторинг та обслуговування локальної мережі. Налаштування та управління маршрутизаторами, комутаторами, точками доступу та іншими мережевими пристроями. Забезпечення надійного та безперебійного доступу до Інтернету. Моніторинг безпеки мережі та систем, реагування на інциденти безпеки. Управління доступом користувачів до ресурсів мережі, налаштування прав доступу та політик безпеки;

– прибиральниця – здійснює прибирання приміщень у визначений час.

1.2 Обґрунтування необхідності створення комплексної системи захисту інформації

Закон України «Про інформацію» регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [1].

Згідно з Законом України «Про персональні дані» визначаються суб'єкти відносин, пов'язаних із персональними даними, об'єкти захисту, загальні/особливі вимоги до обробки персональних даних та контроль за додержанням законодавства про захист персональних даних [2].

Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» статті 8: інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю [3].

Підтвердження відповідності здійснюється за результатами державної експертизи порядком, встановленим законодавством.

Згідно з положенням "про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці" НД ТЗІ 1.6-005- 2013 об'єкти, на яких здійснюватиметься обробка технічними засобами та/або озвучуватиметься інформація з обмеженим доступом, що не становить державної таємниці, підлягають обов'язковому категоріюванню.

Категоріювання може бути первинним, черговим або позачерговим.

Категоріювання здійснюється для визначення необхідного (зі встановлених нормативно-правовими актами та норматив- ними документами системи технічного захисту інформації рівнів) рівня захисту інформації, що обробляється технічними засобами та/або озвучується на об'єкті [4].

В ОІД циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Новопавлівська сільська рада була визнана за результатами категоріювання, як об’єкт VI категорії, в той же час було прийняте рішення створити КСЗІ для забезпечення захисту ціннісних характеристик інформації та недопустимість її витоку.

1.3 Обстеження об’єкту інформаційної діяльності

1.3.1 Обстеження фізичного середовища

Адреса установи: Дніпропетровська область, Синельниківський район, с. Новопавлівка, вул. Карпінського, 19. Графік роботи: Понеділок-четвер: 8.00 - 17.00, п’ятниця 8.00 - 16.00. Перерва на обід: 12.00 - 13.00.

Будівля побудована з силікатної цегли. Стінні перегородки мають товщину 100 мм, а зовнішні стіни – 300 мм. Висота стелі – 3 м. ОІД має 7 трикамерних вікон з матеріалу – пластик і мають характеристики: висота – 1,43 м, ширина – 1,3 м, товщина – 24 мм. На усіх вікнах знаходяться сонцезахисні жалюзі. ОІД має 2 входи/виходи, обидві двері з матеріалу – метал і мають характеристики: висота – 2 м, ширина – 0,9 м, товщина – 70 мм. Всередині будівлі є 6 дверей з матеріалом – пластик і характеристиками: висота – 2м, ширини – 0,8 м, товщина – 70 мм.

Будівля не огороджена. З північної сторони від будівлі знаходиться закинутий гараж, зі східної сторони зелена зона, з південної сторони від будівлі пролягає проїжджа частина, із західної – місцева лікарня.

Система електроживлення централізована, підключена до електричного щитка, який з'єднаний з трансформаторною підстанцією. Система електроживлення та освітлення надана на рисунку 1.3. Система заземлення не виходить за межі ОІД.

Система комп'ютерної мережі проведена оптоволоконним кабелем. Вита пара підключена до комутатора, який утворює локальну мережу. Система комп'ютерної мережі надана на рисунку 1.4.

Система опалення централізована і має 7 радіаторів, по одному біля кожного вікна. Система водопостачання безе свій початок зі свердловини позаду будинку та йде через вбиральню. Система опалення та водопостачання надана на рисунку 1.5.

Система вентиляції працює за допомогою кондиціонерів з рекуператорами.

Система сигналізації централізована, з виходом на клавіатуру сигналізації.

Охоронця на ОІД немає.

ОІД складається з 7 приміщень:

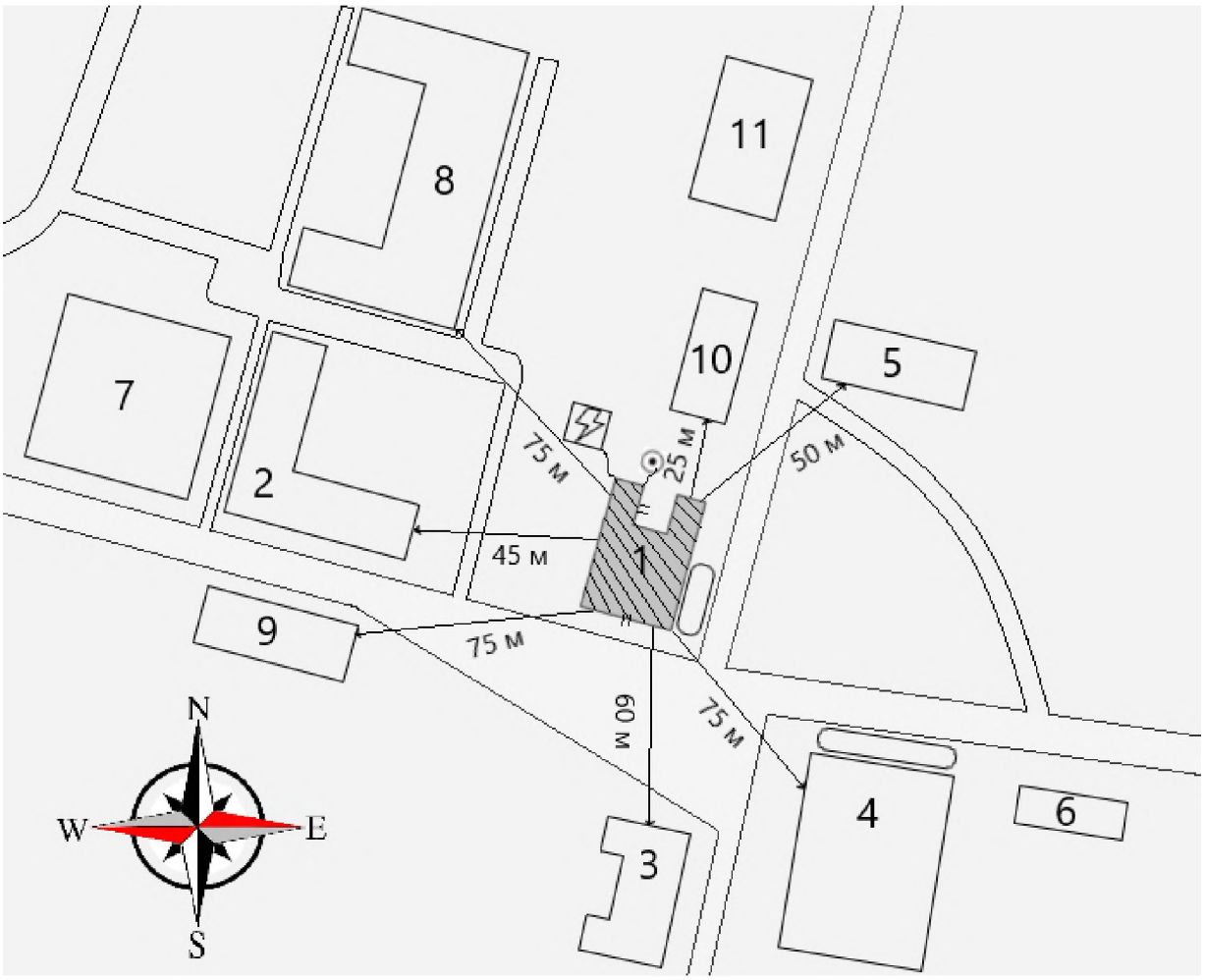
- кабінет керівника – 8 х 4 м;
- бухгалтерія – 8 х 4 м;
- системний Адміністратор – 5,5 х 3,5 м;
- котельня – 4 х 3,5 м;

– вбиральня – 1,5 х 3,5 м;
– вхідне приміщення – 2 х 2;
– загальний коридор.

Таблиця 1.2 – Характеристика будівель

№	Будівля	Адреса	Кількість поверхів	Відстань від ОІД, м
1	Сільська рада	Вул. Карпінського, 19	1	-
2	Лікарня	Вул. Карпінського, 17	1	45
3	Укрпошта	Вул. Карпінського, 18	2	60
4	Будинок культури	Вул. Карпінського, 24	2	75
5	Мельниця	Вул. Карпінського, 21	1	50
6	Церква	Вул. Карпінського, 26	1	130
7	Кафе «Будьмо»	Вул. Карпінського, 15	1	90
8	Закинута будівля	Вул. Поштова, 75	3	75
9	Закинута будівля	Вул. Карпінського, 14	1	75
10	Закинута будівля	Вул. Карпінського, 19а	1	25
11	Закинута будівля	Вул. Карпінського, 20	1	85

На таблиці 1.2 представлена характеристика будівель, які заходяться поруч. На півночі заходяться закинуті будівлі, що можуть бути використаними для спостереження за Новопавлівською сільською радою.Також така будівля є на південном заході.



Умовні позначення:

1 - Будівля;

- Парковка;

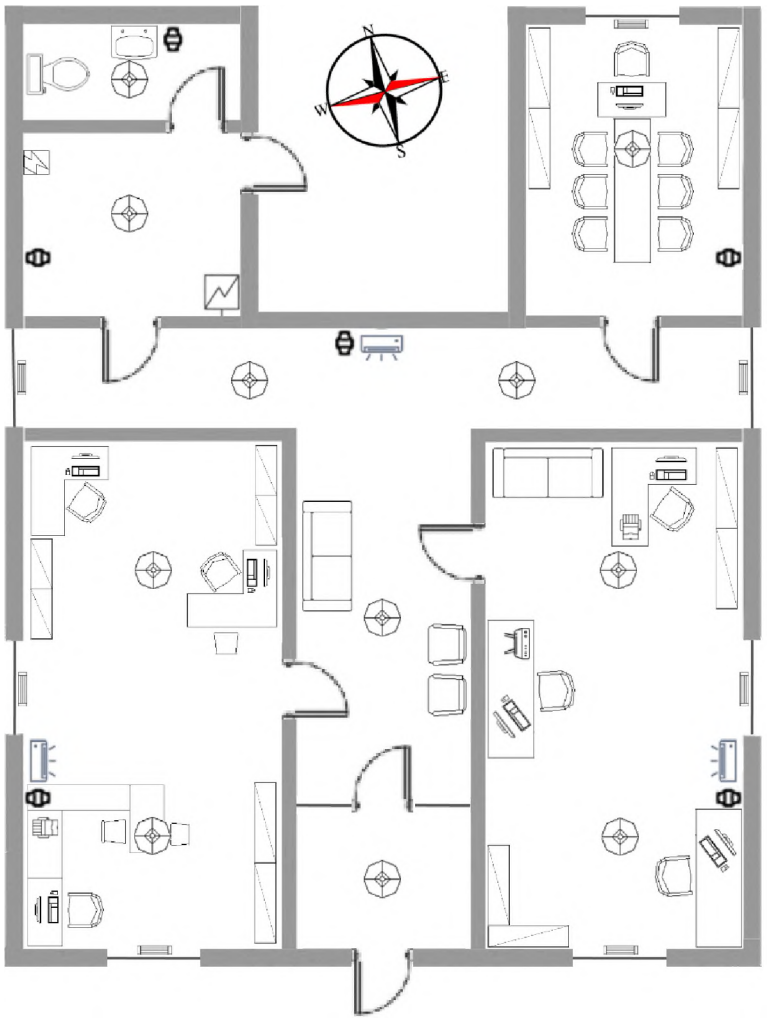
- свердловина;

- ОІД;

- Трансформаторна підстанція.

- КЗ

Рисунок 1.2 – Ситуаційний план



Умовні позначення:

- стіл; - радіатор; - шафа;

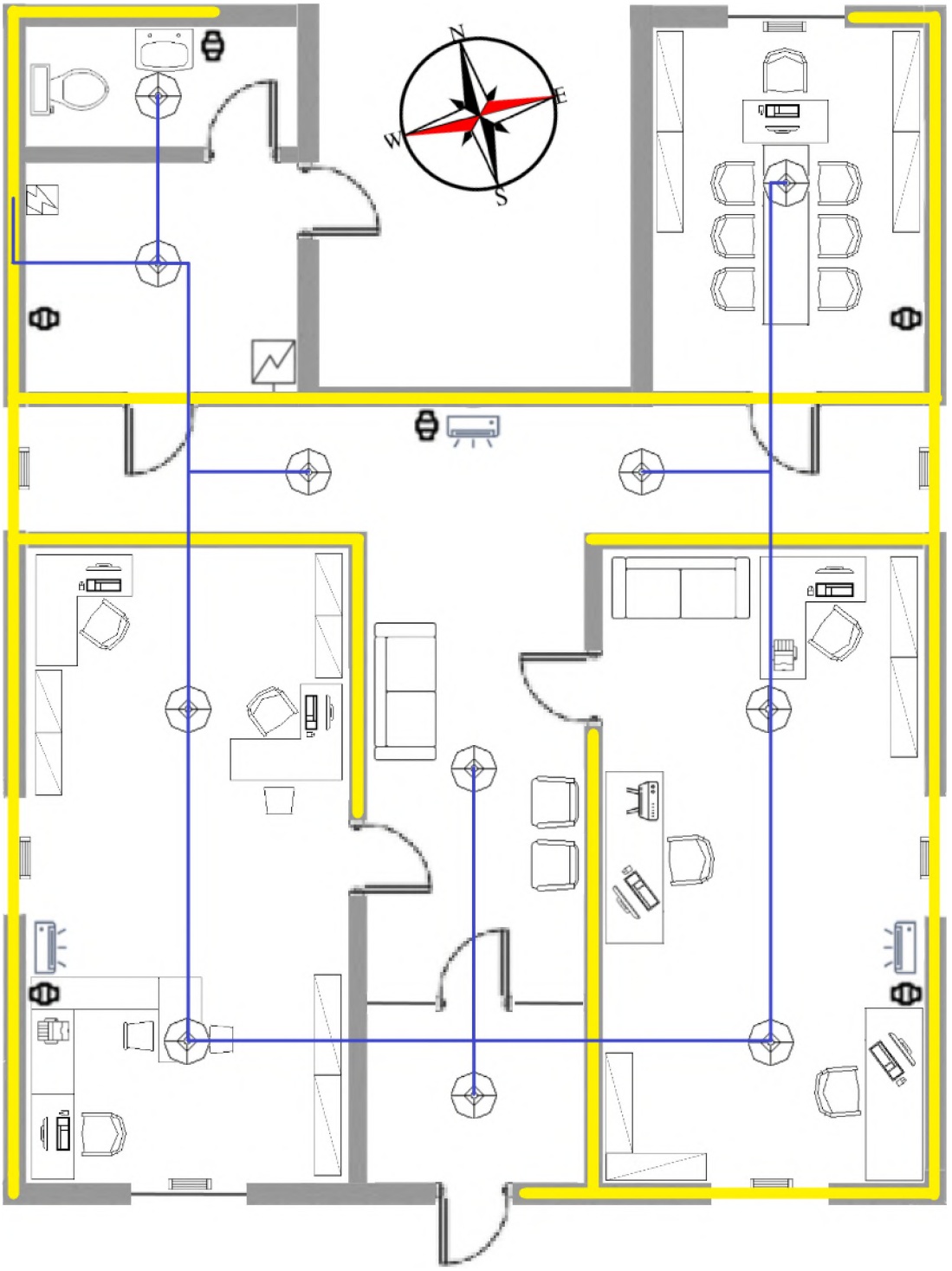
- ПК; - рекуператор; - комутатор;

- крісло; - кондиціонер; - диван;

- електричний щиток; - ксерокс/принтер; - світильник;

- унітаз; - умивальник; - електричний котел.

Рисунок 1.3 – Генеральний план

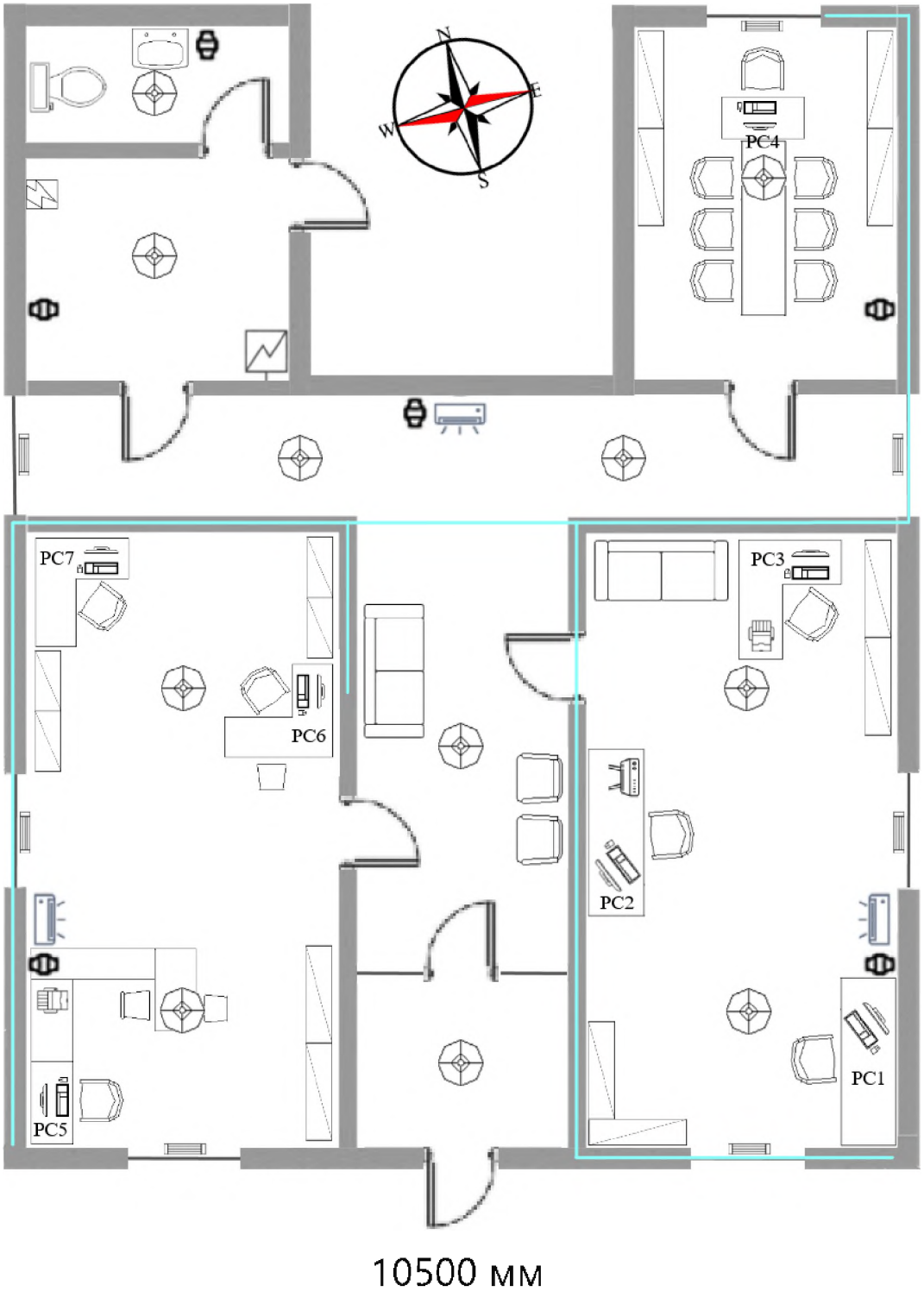


Умовні позначення:

- лінія електропостачання

- лінія світлопостачання

Рисунок 1.4 – Схема освітлення та електроживлення



Умовні позначення:

- лінія комп’ютерної мережі

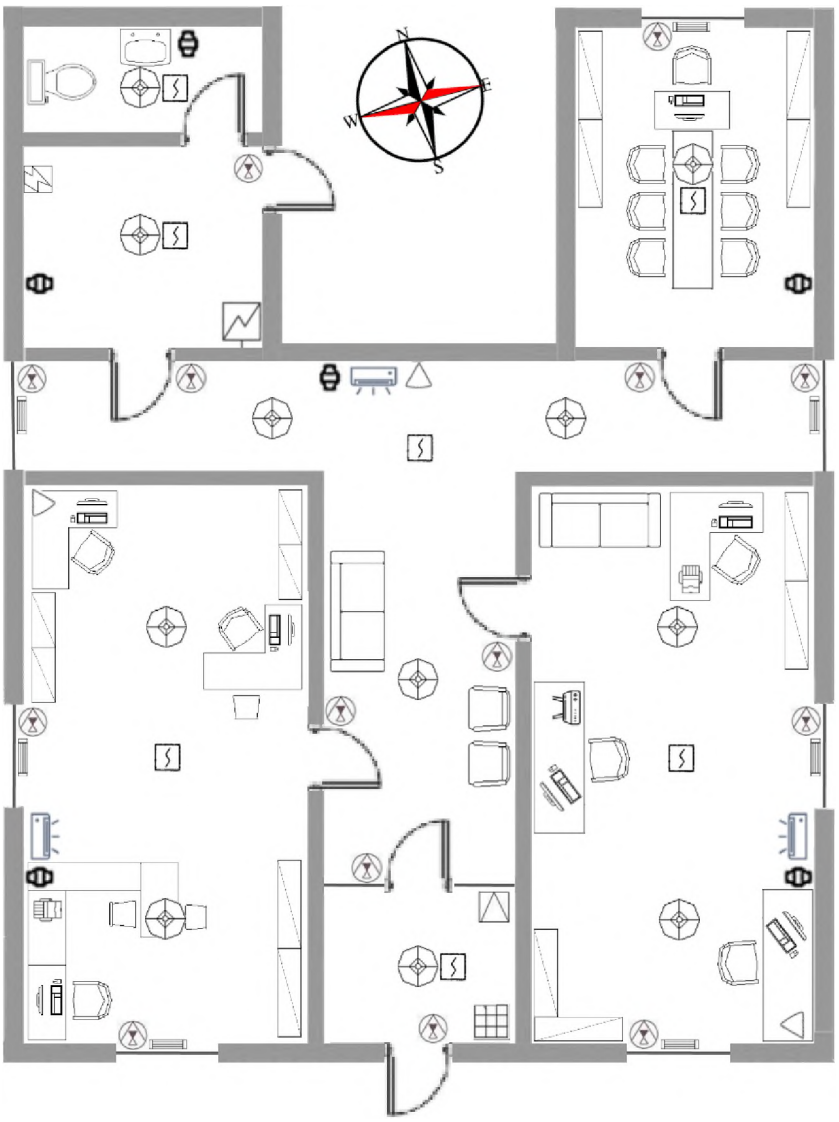
Рисунок 1.5 – Схема комп’ютерної мережі

Умовні позначення:

- лінія отоплення

- лінія водопостачання

Рисунок 1.6 – Схема опалення та отоплення



Умовні позначення:

- датчики диму;

- магнітноконтактний сповіщувач;

- камера відеоспостереження;

- клавіатура;

- пкп.

Рисунок 1.7 – Схема сигналізації

1.3.2 Обстеження обчислювального середовища

Таблиця 1.3 – Характеристика ОТЗ

Назва	Модель	Серійний номер	Відстань до межі ОІД, м
PC1. Монітор	Philips 223V7QHAB	TWOCRRRGP8O0YJSK	1
PC1. Системний блок	Dell OptiPlex 3080	W1KJIUW3RZWLFTLV	1
PC1. Клавіатура	Logitech K120	IC2X99OW0T1TF12G	1
PC1. Миша	Logitech B100	76IMB70J12V3T01C	1
PC2. Монітор	Philips 223V7QHAB	XJQBV7M8JW8UI764	4
PC2. Системний блок	Dell OptiPlex 3080	X8AVDPHMZ9S0OL5D	4
PC2. Клавіатура	Logitech K120	8WM37I7DBJ56VKUX	4
PC2. Миша	Logitech B100	OKVAEVOS8VIO1II6	4
PC3. Монітор	Philips 223V7QHAB	J0L7IIYRO42EII9Q	1,5
PC3. Системний блок	Dell OptiPlex 3080	SPVJ5PEWB4C9MQI3	1,5
PC3. Клавіатура	Logitech K120	CA0LKVMNS6M4KTWP	1,5
PC3. Миша	Logitech B100	6VGNM1DTYP55DM12	1,5
PC4. Монітор	Philips 223V7QHAB	I98XTH847RN4BM8P	1,5
PC4. Системний блок	Dell OptiPlex 3080	8ZV965HFW47D381E	1,5
PC4. Клавіатура	Logitech K120	YVBDOK9KYYNISVP3	1,5
PC4. Миша	Logitech B100	OPIE6U772KNSB8HA	1,5
PC5. Монітор	Philips 223V7QHAB	YE80ZPNZJBQRJFA8	1
PC5. Системний блок	Dell OptiPlex 3080	TUUE4F63BKIZLPHW	1

Продовження таблиці 1.3

Назва	Модель	Серійний номер	Відстань до межі ОІД, м
PC5. Клавіатура	Logitech K120	BSOX096G2LAV3541	1
PC5. Миша	Logitech B100	EIKN0RP67F8462MS	1
PC6. Монітор	Philips 223V7QHAB	Z2BH4S8KHCOI9NKO	4
PC6. Системний блок	Dell OptiPlex 3080	SO3RQ4KYMHXTKHFB	4
PC6. Клавіатура	Logitech K120	YV67GFKJ6ICT3AEP	4
PC6. Миша	Logitech B100	9N6WU23FKJUQ9M6L	4
PC7. Монітор	Philips 223V7QHAB	U0GZ8RC7DFPFBH9G	1
PC7. Системний блок	Dell OptiPlex 3080	0PDU3VCOQXAQSP18	1
PC7. Клавіатура	Logitech K120	3NWYWA7FLHCSOGOI	1
PC7. Миша	Logitech B100	7NQL8YZ4JKD1OP2H	1
Ксерокс/ Принтер	Brother DCP-L2550D	K3W8R9P1XT4FZ7YQ	1,5
Ксерокс/ Принтер	Brother DCP-L2550D	5P3Q7H1A9L6Z8G2J	1

Таблиця 1.3 показує технічні засоби, якими користуються працівники.

Характеристики системного блоку Dell OptiPlex 3080:

- процесор: Intel Core i3-10100 (4 ядра, 3.6 ГГц);
- оперативна пам'ять: 8 ГБ DDR4;
- жорсткий диск: 512 ГБ SSD;
- графіка: вбудована Intel UHD Graphics 630.

Характеристики Принтера/сканера Brother DCP-L2550D

- швидкість друку: до 34 сторінок на хвилину (ppm);
- роздільна здатність друку: до 1200 x 1200 dpi;
- сканування: роздільна здатність до 1200 x 1200 dpi;
- габарити (Ш x Г x В): приблизно 410 x 398.5 x 318.5 мм.

Таблиця 1.4 – Характеристика ДТЗ

Назва	Модель	Серійний номер	Відстань до межі ОІД, м
Камера відеоспостереження(3 шт.)	Hikvision DS-2CE76D0T-ITMFS	4UF782I6Y4QUQQRH 1BYQQJ37EGA7JB59 ZNRXTT4DYW63MJ00	0,5
Магнітоконтактний сповіщувач(14 шт.)	Satel B-1F	-	1-4
Пожежний сповіщувач(7 шт.)	ІПК-6	-	2
Клавіатура сигналізації	Satel VERSA-15	9H3Z4OHN6RH5KM03	0,5
ПКП	Satel VERSA-15	BA9QO5HX4HPFMKYU	1,5
Кондиціонер(3 шт.)	Midea MSAF-09HRN1	-	0,5
Рекуператор(6 шт.)	Prana 150	-	0
Комутатор	TP-Link TL-SG105	M9X6D4K2B8R1J7PF	4

Таблиця 1.5 – Характеристика ПЗ

Назва	Тип	Ліцензія	Розташування
Windows 10 (22H2)	Системне	Commercial	PC1-PC7
Microsoft Office	Прикладне	Corporative	PC1-PC7
Adobe Photoshop Elements 2023	Прикладне	Commercial	PC3
1С Бухгалтерія	Прикладне	Commercial	PC5-PC7
M.E.Doc	Прикладне	Commercial	PC5-PC7

Таблиці 1.4 та 1.5 показують інші ДТЗ та ПЗ, яким користуються працівники.

1.3.3 Обстеження інформаційного середовища

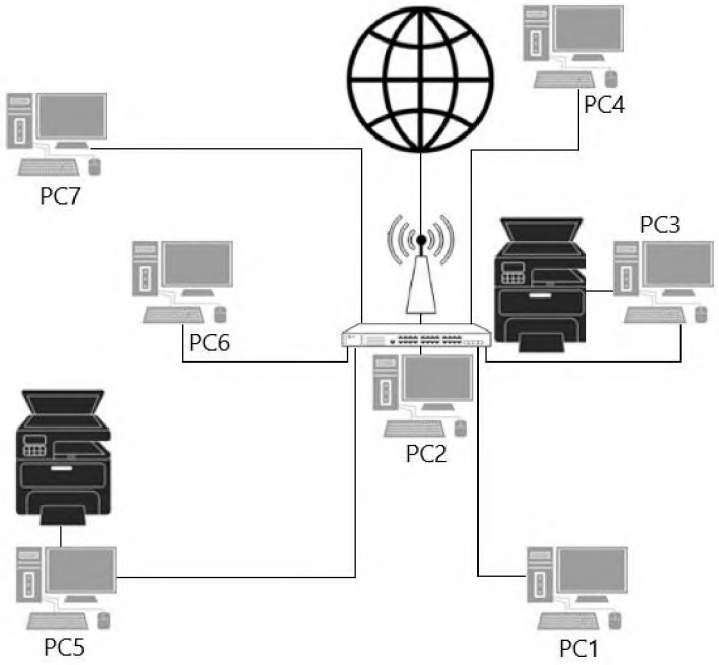


Рисунок 1.8 – Схема ІКС

Розміщення працівників, щодо комп'ютерної мережі:

- керівник – PC1;
- заступник керівника – PC2;
- секретар – PC3;
- системний адміністратор – PC4;
- бухгалтери – PC5, PC6, PC7.

Таблиця 1.6 – Характеристика інформаціїї, що обробляється

№	Інформація	Режим доступу	Правовий режим	Носій інформації	Приміщення зберігання	Вимоги до захисту інформації		
						К	Ц	Д
1	Фінансові дані	З обмеженим доступом	Конфіденційна інформація	Паперові документи, бухгалтерські програми.	PC5	К4	Ц4	Д4

Продовження таблиці 1.6

№	Інформація	Режим доступу	Правовий режим	Носій інформації	Приміщення зберігання	Вимоги до захисту інформації		
						К	Ц	Д
2	Документація сесій та засідань	Відкрита	Відкрита інформація	Паперові документи, офіційний веб-сайт	РС7, РС3	К1	Ц2	Д2
3	Громадські реєстри	З обмеженим доступом	Конфіденційна інформація	Паперові документи, електронні реєстри	РС2, РС3	К 4	Ц 4	Д 4
4	Правова документація	З обмеженим доступом	Конфіденційна інформація	Паперові, електронні документи	РС4	К3	Ц3	Д2
5	Проєкти та програми розвитку	Відкрита	Відкрита інформація	Паперові документи, офіційний веб-сайт	РС1, РС2, РС3	К1	Ц2	Д3
6	Технічна документація	З обмеженим доступом	Конфіденційна інформація	Паперові документи, електронні схеми.	РС4	К3	Ц3	Д2

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.

Фінансові дані:

Фінансові дані збираються та вводяться в програму 1С Бухгалтерія відповідно до встановлених процедур. Паперові дані зберігаються в архіві з обмеженим доступом (РС5). Електронні дані шифруються для забезпечення конфіденційності. Також створюються резервні копії для захисту від втрати інформації.

Документація сесій та засідань:

Паперові документи оцифровуються для подальшої публікації. Матеріали розміщуються на офіційному веб-сайті сільської ради (РС3) для відкритого доступу громадськості. Інформація регулярно оновлюється для забезпечення актуальності.

Громадські реєстри:

Інформація вводиться в електронні реєстри з дотриманням конфіденційності. Подання електронної звітності та шифрування даних відбувається за допомогою M.E.Doc. Архівування: Паперові документи архівуються в приміщеннях з обмеженим доступом (РС2, РС3).

Проєкти та програми розвитку:

Інформація на паперах оцифровується для подальшої публікації. Матеріали розміщуються на офіційному веб-сайті сільської ради (РС1, РС2, РС3) для відкритого доступу громадськості. Інформація регулярно оновлюється для забезпечення актуальності.

Паперові документи зберігаються в шафах, які зачиняються на ключ, за виключенням громадських реєстрів, які зберігаються у сейфі в кабінеті керівника.

Електронна інформація зберігається на флешках і ПК працівників, а також резервується у хмарних сховищах.

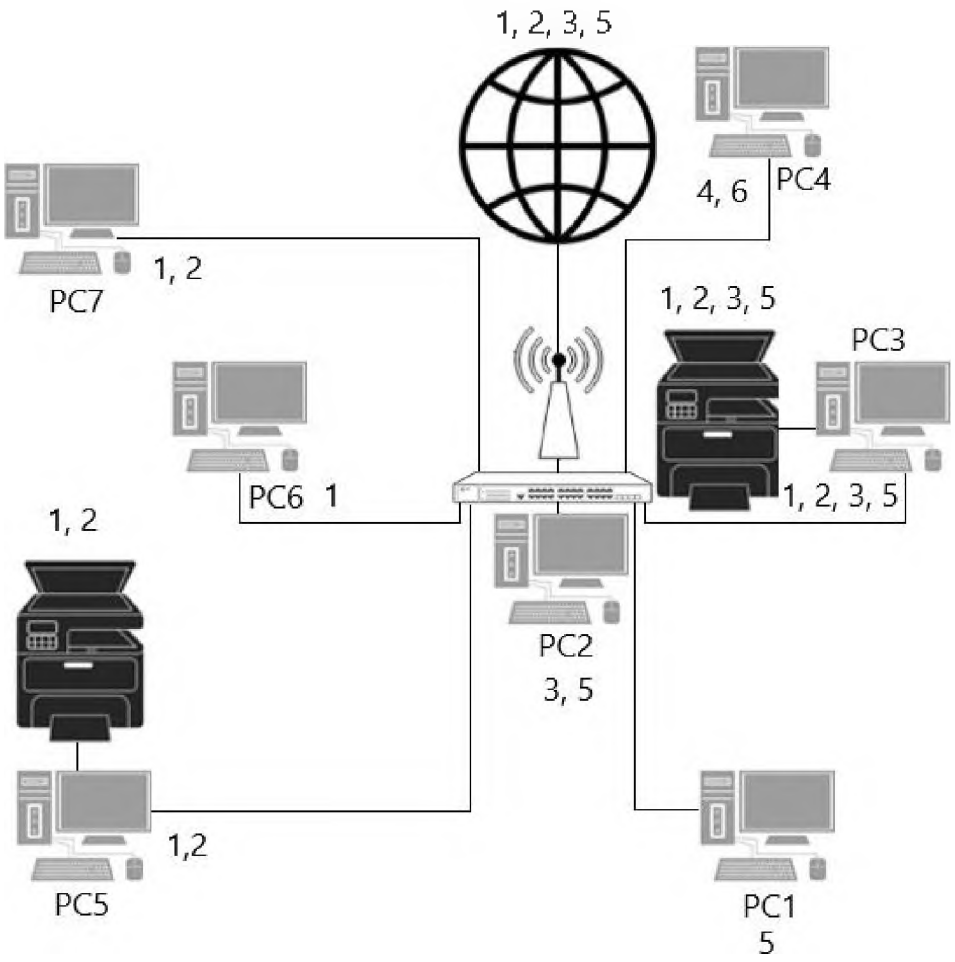


Рисунок 1.9 – Схема інформаційних потоків

Системний адміністратор розмежовує доступ, займається технічною підтримкою усіх технічних засобів, а також допомагає вирішувати помилки інших користувачів ІКС. Також допомагає вести офіційний сайт Новопавлівської ради.

Захищає та оновлює правову та технічну документацію. Якщо відбувається втрата даних, то допомагає відновити їх з резервних джерел та іншими способами.

Також забезпечує технічну підтримку під час проведення заходів (встановлює обладнання для презентацій, забезпечує доступ до мережі, тощо).

Таблиця 1.7 – Матриця правил розмежування доступу

№	Інформація	Керівник	Заступник керівника	Секретар	Системний адміністратор	Бухгалтери
1	Фінансові дані	R, P	R, P	R, P	R, W, M, D, P, C	R,W, M, D, P, C
2	Документація сесій та засідань	R, W, M, D, P, C	R, W, M, D, P, C	R, W, M, P, C	R, W, M, D, P, C	R, P
3	Громадські реєстри	R, W, M, D, P, C	R, W, M, P, C	R, W, M, P, C	R, W, M, D, P, C	-
4	Правова документація	R, P	R, P	-	R, W, M, D, P, C	-
5	Проєкти та програми розвитку	R, W, M, D, P, C	R, W, M, D, P, C	R, W, M, P, C	R, W, M, D, P, C	-
6	Технічна документація	R, P	R, P	-	R, W, M, D, P, C	-
Журнал подій		-	-	-	-	-
Встановлення ПЗ		+	+	+	+	+

– R – читання ;

– W – запис;

– M – модифікація;
– D – видалення;
– P – друк;
– C – створення.

1.4 Модель порушника

Модель порушника – це абстрактний опис потенційного зловмисника, його можливості, цілі, засоби та методи, які він може використовувати для реалізації загроз безпеці інформації.

Внутрішній порушник - це особа, яка має легальний доступ до інформаційних систем або ресурсів організації і може використовувати цей доступ з метою порушення безпеки інформації. Внутрішні порушники часто є співробітниками або підрядниками організації, які можуть мати різні мотиви для своїх дій.

Зовнішній порушник - це особа або група осіб, які не мають легального доступу до інформаційних систем або ресурсів організації і намагаються отримати доступ до цих ресурсів нелегально. Зовнішні порушники можуть діяти з різних мотивів і використовувати різні методи для досягнення своїх цілей.
Для створення таблиці моделі порушника, потрібно врахувати різні аспекти, які можуть вплинути на безпеку інформаційних систем.

Таблиця 1.8 – Категорії порушників

Умовне позначення	Категорія	Оцінка загроз
Внутрішні порушники		
ВП1	Користувачі	2
ВП2	Технічний персонал	1
ВП3	Системні адміністратор	4
ВП4	Керівні посади	3
Зовнішні порушники		
ЗП1	Відвідувачі	1
ЗП2	Хакери	4
ЗП3	Колишні працівники	3

Внутрішні загрози можуть бути такими ж небезпечними, як і зовнішні кібератаки. Недбалість співробітників, наприклад, неправильне поводження з даними або потрапляння на фішингові схеми, може призвести до витоку даних.

Внутрішні загрози, коли співробітники навмисно компрометують дані, також становлять значний ризик. Ключові проблеми включають:

- недостатнє навчання з питань безпеки даних;
- погано керовані системи доступу;
- відсутність моніторингу та аудиту;
- недостатні перевірки під час найму.

Таблиця 1.9 – Мотив порушників

Умовне позначення	Мотив	Оцінка загроз
M1	Безвідповідальність	2
M2	Самоствердження	3
M3	Корисливість	4

Таблиця 1.10 – Розуміння ІКС порушниками

Умовне позначення	Кваліфікація	Оцінка загроз
P1	Порушник не має знань та досвіду роботи з ІКС	1
P2	Порушник має базові знання та обмежений досвід роботи з ІКС.	2
P3	Порушник має значний досвід та знання в області ІКС	3
P4	Порушник має високий рівень знань та досвід, здатен впроваджувати атака різної складності	4

Таблиця 1.11 – Використання засобів ІКС порушниками

Умовне позначення	Кваліфікація	Оцінка загроз
В1	Використання розмов та документів на робочих місцях	1
В2	Використання архівів та програм, які обробляють інформацію	3
В3	Використання пасивних технічних засобів перехвату інформації	2
В4	Використання активних технічних засобів перехвату інформації	4

Таблиця 1.12 – Час дії порушників

Умовне позначення	Мотив	Оцінка загроз
Ч1	Під час призупинення функціонування ІКС	1
Ч2	Під час функціонування ІКС	2
Ч3	Під час відновлення, чи ремонту ІКС	3

Таблиця 1.13 – Місце дії порушників

Умовне позначення	Мотив	Оцінка загроз
Л1	Ззовні об’єкта	1
Л2	Всередині об’єкта без доступу до робочих місць	2
Л3	Всередині об’єкта з доступом до робочих місць	3
Л4	Всередині об’єкта з повним доступом	4

Таблиця 1.14 – Модель внутрішнього порушника

Порушник	Категорія	Мотив	Розуміння	Використання	Час дії	Місце дії	Сума загроз
Бухгалтери	ВП1	М1	Р2	В2	Ч2	Л3	
	2	2	2	2	2	3	13
Секретар	ВП1	М2	Р3	В2	Ч2	Л3	
	2	3	3	2	2	3	15
Системний адміністратор	ВП3	М3	Р4	В4	Ч3	Л4	
	4	4	4	4	3	4	23
Заступник керівника	ВП4	М2	Р2	В2	Ч2	Л3	
	3	3	2	2	2	3	15
Керівник	ВП4	М3	Р3	В2	Ч2	Л4	
	3	4	3	2	2	4	18
Керівник районної адміністрації	ВП4	М3	Р3	В3	Ч3	Л4	
	3	4	3	3	3	4	20
Прибиральниця	ВП2	М1	Р1	В1	Ч1	Л2	
	1	2	1	1	1	2	8

Таблиця 1.15 – Модель зовнішнього порушника

Порушник	Категорія	Мотив	Розуміння	Використання	Час дії	Місце дії	Сума загроз
Відвідувач	ЗП1	М1	Р1	В1	Ч2	Л2	9
	1	2	1	1	2	2	
Хакер	ЗП2	М3	Р4	В4	Ч2	Л1	19
	4	4	4	4	2	1	
Колишній керівник	ЗП3	М3	Р3	В3	Ч2	Л2	
	3	4	3	3	2	2	17

1.5 Модель загроз

Загрози можна розділити на:

- природні;
- техногенні;
- антропогенні.

Згідно НД ТЗІ 1.1-003-99 побудована модель загроз являє собою абстрактний опис засобів і методів можливих загроз. Після визначення ризиків модель загроз допомагає визначити пріоритетність виявлених ризиків і зважити витрати та вигоди від їх вирішення [10].

Таблиця 1.16 – Модель загроз

Загроза	Джерело загрози	Вразливість	Рівень ризику	Рівень загроз	К	Ц	Д
Пожежа	Система електропостачання	Збої в електропостачанні	1	2	-	+	+
Збої в електропостачанні	Відключення, штормова погода	Відсутність ДБЖ	3	1	-	-	+

Продовження таблиці 1.16

Загроза	Джерело загрози	Вразливість	Рівень ризику	Рівень загроз	К	Ц	Д
Збої обладнання	Система електропостачання	Збої в електропостачанні	1	3	-	+	+
Невірне налаштування обладнання	Системний адміністратор	Не кваліфікованість	1	1	-	+	+
Розголошення конфіденційної інформації	Колишні та теперішні працівники	Відсутність контролю за працівником	2	4	+	-	-
Використання стороннього ПЗ	Працівники	Відсутність квот та контролю за працівником	3	4	+	+	+
Помилка при введенні даних	Працівники	Людський фактор	4	2	-	+	-
Помилка при експлуатації технічних засобів та ПЗ	Працівники	Не кваліфікованість	3	2	-	+	+
Зловживання правами	Системний адміністратор	Неправильне розмежування прав доступу	4	4	+	+	+

Продовження таблиці 1.16

Загроза	Джерело загрози	Вразливість	Рівень ризику	Рівень загроз	К	Ц	Д
Зараження технічних засобів	Хакери	Відсутність оновлення антивірусного ПЗ, низька кваліфікація працівників в безпеці інформації	2	4	+	+	+
DDOS-атаки	Хакери	Недостатній моніторинг і реагування	3	3	-	-	+

Високий рівень - реалізація загрози спричиняє значні втрати (оцінка: 3 бали).

Середній рівень - реалізація загрози спричиняє помірні втрати (оцінка: 2 бали).

Низький рівень - реалізація загрози спричиняє незначні втрати або не спричиняє втрат (оцінка: 1 бал).

Основні загрози для інформаційної системи включають:

– збої в електропостачанні: переривання у постачанні електроенергії можуть призвести до вимкнення комп'ютерів і мережевих пристроїв, що може спричинити втрату даних, пошкодження апаратного забезпечення;

– розголошення конфіденційної інформації: Неконтрольований доступ до конфіденційних даних призводить до витоку інформації, що зашкодить репутації організації або спричинить юридичні наслідки;

– використання стороннього ПЗ: використання несанкціонованого чи піратського ПЗ може призвести до зараження шкідливими програмами, зазвичай спричиняє витік даних або збої в роботі;

– зловживання правами: надання користувачам надмірних прав доступу призводить до випадкових або навмисних дій, які шкодять системі;

– зараження технічних засобів: інфікування комп'ютерів або інших технічних засобів вірусами, троянами або іншими шкідливими ПЗ призводить до втрати даних, порушення роботи системи або витоку інформації;

– DDOS-атаки: атака, спрямована на перевантаження мережевої інфраструктури через надсилання великої кількості запитів, одночасно з багатьох джерел призводить до недоступності послуг для відвідувачів.

Об’єктами захисту є: персональні комп’ютери та громадський реєстр.

1.6 Аналіз та обрання профілю захищеності

Захист від шкідливого ПЗ базується на антивірусному ПЗ «Avast», але програма тривалий час не оновлювалась і не переглядалась. На ПК користувачів не встановлені квоти, які б забороняли завантажувати стороннє ПЗ та повний доступ до всього інтернету.

Системний адміністратор має повний доступ до системи і ніким не контролюється, що робить його небезпечним для ОІД та інформації, яка в ньому циркулює. Також фізичному захисту не вистачає центрального джерела безперебійного живлення до тих пір, поки не запрацює генератор, яке б запобігло випадками втрати даних під час стабілізаційних та екстренних відключень електроенергії.

АС належить до класу «3» (розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності).

Згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні профілі захищеності оброблювальної інформації від несанкціонованого доступу» [9], оберемо профіль:

3.КЦД.3 = (КД-2, КА-2, КО-1, КК-1, КВ-3, ЦД-1, ЦА-3, ЦО-2, ЦВ-2, ДР-2, ДС- 1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2}.

КД-2. Базова довірча конфіденційність.

Функції: здійснення розмежування доступу на підставі атрибутів користувачами до об'єктів у своїх облікових записах без втручання адміністратора. Захищає від НСД до інформації. Послуга впливає на облікові записи користувачів і захищені об'єкти в яких зберігаються фінансові дані, громадські реєстри, правова та технічна документація.

Механізм реалізації: встановленням атрибутів доступу до об'єктів свого облікового запису користуючись системними механізмами.

КА-2. Базова адміністративна конфіденційність.

Функції: здійснення розмежування доступу на підставі атрибутів адміністраторами, або користувачам з повноваженнями до об'єктів у облікових записах користувачів. Захищає від НСД до інформації. Послуга впливає на облікові записи користувачів і захищені об'єкти в яких зберігаються фінансові дані, громадські реєстри, правова та технічна документація.

Механізм реалізації: встановленням атрибутів доступу до об'єктів облікового записів користувачів користуючись системними механізмами.

КО-1. Повторне використання об'єктів.

Функції: перед повторним використанням об'єкта, дані цього об'єкта перезаписуються, а оперативна пам'ять, яка використовувалась – очищується. Захищає від НСД до інформації, якою користувався минулий користувач у об'єкті. Послуга впливає на усі типи інформації, якими користуються користувачі.

Механізм реалізації: ініціалізації вмісту поділюваних ресурсів, використовуваних для збереження пасивних об'єктів, а також ініціалізації (видалення) атрибутів доступу пасивних об'єктів, що видаляються.

КВ-3. Повна конфіденційність при обміні.

Функції: забезпечує безпечний обмін інформацією між КЗЗ та глобальними мережами, допомагає користувачам в захисті конфіденційної інформації при експорті та імпорті. Послуга впливає на конфіденційну інформацію, якою

діляться користувачі в глобальній мережі, тобто на передачу фінансових звітів та громадських реєстрів.

Механізм реалізації: VPN, TOR

ЦД-1. Мінімальна довірча цілісність.

Функції: здійснення розмежування доступу на підставі атрибутів користувачами до об'єктів у своїх облікових записах без втручання адміністратора. Захищає від несанкціонованої модифікації інформації. Послуга впливає на можливість модифікувати не заборонені файли у облікових записах користувачів і захищених об'єктах в яких зберігаються фінансові дані, документація сесій та засідань, громадські реєстри, проєкти та програми розвитку, правова та технічна документація.

Механізм реалізації: встановленням атрибутів доступу до об'єктів свого облікового запису користуючись системними механізмами.

ЦА-3. Повна адміністративна цілісність.

Функції: здійснення розмежування доступу на підставі атрибутів адміністраторами, або користувачам з повноваженнями до усіх об'єктів у облікових записах користувачів. Захищає від несанкціонованої модифікації інформації. Послуга впливає на можливість модифікувати не заборонені файли у облікових записах користувачів і захищених об'єктах в яких зберігаються фінансові дані, документація сесій та засідань, громадські реєстри, проєкти та програми розвитку, правова та технічна документація.

Механізм реалізації: встановленням атрибутів доступу до об'єктів облікового записів користувачів користуючись системними механізмами.

ЦО-2. Повний відкат.

Функції: відміна усіх операцій за вказаний проміжок часу. Допомагає відновлювати втрачені файли. Послуга впливає на усі типи інформації, якими користуються користувачі.

Механізм реалізації: Git та інші системи контролю версій.

ЦВ-2. Базова цілісність при обміні

Функції: забезпечує безпечний обмін інформацією між КЗЗ та глобальними мережами, допомагає користувачам в захисті цілісності інформації при експорті та імпорті. Послуга впливає на інформацію, якою діляться користувачі в глобальній мережі, тобто на передачу фінансових звітів, документації сесій та засідань, проєктів та програм розвитку і громадських реєстрів.

Механізм реалізації: хешування, завдяки якому можливе виявлення порушень цілісності шляхом звірення хеш-функцій оригінального та модифікованого файлів

ДР-2. Недопущення захоплення ресурсів.

Функції: дозволяє адміністраторам, або користувачам з повноваженнями керувати використанням усіх ресурсів. Послуга впливає на облікові записи та їх можливість розміщення інформації на дисковому просторі.

Механізм реалізації: вбудована функція квот.

ДС-1. Стійкість при обмежених відмовах.

Функції: зменшує вразливість систем до загроз, які змушують систему працювати без одного компонента. Послуга впливає на доступність інформації фінансових звітів та громадських реєстрів, правову та технічну документацію.

Механізм реалізації: GitLab для створення локального серверу.

ДЗ-1. Модернізація.

Функції: можливість провести модернізацію КС при умові, що це не призводить до необхідності ще раз проводити інсталяцію КС або до переривання виконання функцій захисту.

Механізм реалізації: автооновлення антивіруса та ОС

ДВ-2. Автоматизоване відновлення.

Функції: зменшує вразливість системи при відмові чи несправності компоненту системи Послуга впливає на доступність інформації фінансових звітів та громадських реєстрів, правову та технічну документацію.

Механізм реалізації: КС автоматично створює точки відновлення, за якими користувач може відновити все до робочого стану. Також точки відновлення можна створити вручну.

НР-3. Сигналізація про небезпеку.

Функції: Сповіщати користувача про події. Види сигналізації у системному застосунку Event Viewer:

– інформація – успішна дія
– попередження – подія, яка може спричинити проблеми
– помилка – виникнення значної проблеми
– критично – виникла серйозна проблема

Окрім цього застосунок фіксує входи та виходи, порушення прав доступу та намагання когось отримати доступ.

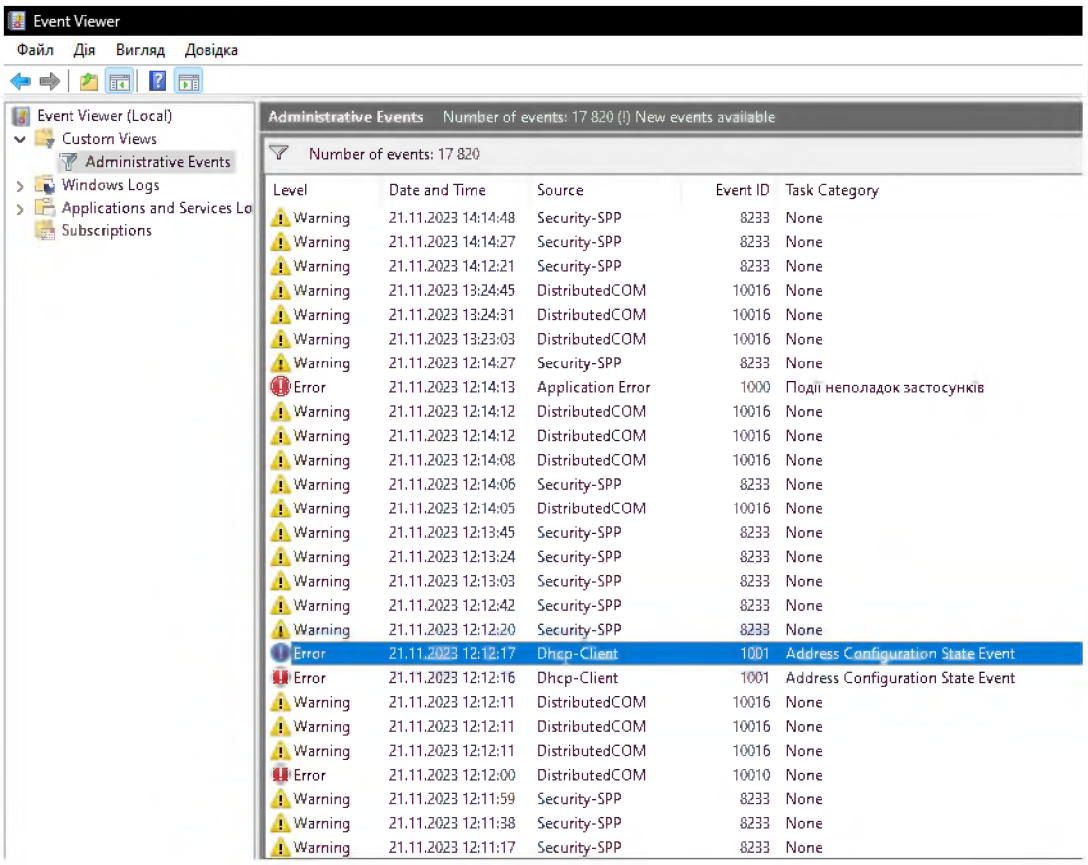


Рисунок 1.10 – Event Viewer

НИ-2. Одиночна ідентифікація і автентифікація.

Функції: перевірка особистості. Послуга впливає на захист інформації від людей, які перший раз прийшли та зловмисників.

Механізм реалізації: Послуга реалізовується за допомогою створених облікових записів, які потребують підтвердження паролем, при спробі доступу до системи.

НК-1. Однонаправлений достовірний канал.

Функції: Гарантує, що ідентифікацію і автентифікацію проходить людина та, що важлива інформація буде у руках людини, яка знає пароль.

Механізм реалізації: клавіатура за допомогою можна ввести пароль, інакше пароль ввести не вийде, так як зв'язок буде недостовірний.

НО-2. Розподіл обов'язків адміністраторів.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора.

Функції: мінімізує ролі, щоб включати тільки ті функції, які необхідні для виконання даних їй завдань.

Механізм реалізації: встановленням атрибутів доступу до об'єктів облікового записів користувачів користуючись системними механізмами.

НЦ-3. КЗЗ з функціями диспетчера доступу.

Функції: підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації або втрати керування. Послуги безпеки мають бути доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ [8].

Механізм реалізації: Avast Business Hub дозволяє займатись централізованим управлінням, зберігати паролі, керувати пристроями та налаштовувати заходи безпеки на усіх комп'ютерах, що знаходяться в мережі.

НТ-2. Самотестування при старті.

Функції: оцінює правильність функціонування КЗЗ при старті системи.

Механізм реалізації: КС використовує набір BIOS для перевірки даних та цілісність компонентів КС, а також драйверів і інших складових ОС. POST, який забезпечує захист і конфіденційність даних комп'ютера зберігається на мікросхемі BIOS ROM.

НВ-2. Автентифікація джерела даних.

Функції: вузли мережі ідентифікують інші вузли за допомогою шифрування трафіку. SSL/TLS сертифікат дозволяє зашифрувати з'єднання, в якому всі дані, що передаються між клієнтом та сервером кодуються таким чином, що тільки уповноважена сторона може їх прочитати. Ця послуга захищає персональні дані і конфіденційну інформацію, якими обмінюються обидві сторони Послуга впливає на конфіденційність інформації фінансових звітів та громадських реєстрів.

Механізм реалізації: SSL/TLS сертифікат

1.7 Постановка задачі

Під час обстеження було визначено, який профіль захищеності найбільше підходить для Новопавлівської сільської ради. виявлено певну кількість проблем, які створюються загрози для конфіденційності, цілісності та доступності інформації, що циркулює в ІКС.

Серед них:

- збої в електропостачанні;
- розголошення конфіденційної інформації;
- використання стороннього ПЗ;
- зловживання правами;
- зараження технічних засобів;
- DDOS-атаки.

Потрібно розробити заходи програмно-організаційного рівня для подолання вищевказаних проблем та підвищення безпеки інформації.

1.8 Висновки до першого розділу

Проведено аналіз актуальності теми, обстеження фізичного та інформаційного середовища Новопавлівської сільської ради, визначено види інформації, що циркулює в ОІД, та кількість персоналу та їх обов'язки.

Складено ситуаційний, генеральний та інші інфраструктурні плани, модель порушника, модель загроз. Також проаналізовано існуючий стан захищеності, клас системи та на основні нього обрано профіль захищенності.

Закінчивши збір та систематизацію інформації про загрози і можливих порушників були прийняті рішення про запровадження заходів програмно-організаційного рівня для підвищення безпеки інформації, які стосуються загроз описаних виявлених в першому розділі.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Заходи програмно-організаційного рівня для підвищення безпеки інформації

2.1.1 Заходи з регулювання антивірусного програмного забезпечення

Відповідно до ПОРЯДКУ оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації:

Оновлення АВПЗ здійснюється шляхом організації та забезпечення процесу отримання та впровадження в АВПЗ антивірусних оновлень.

Оновлення АВПЗ, який пройшов державну експертизу та має позитивний експертний висновок Адміністрації Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація Держспецзв'язку), здійснюється з використанням антивірусних оновлень, які розміщуються на веб-сайті ЦАЗІ (www.cazi.dsszzi.gov.ua).

На веб-сайті ЦАЗІ (www.cazi.dsszzi.gov.ua) розміщуються тільки антивірусні оновлення АВПЗ, які пройшли експрес-експертизу [5].

Антивірус обраний відповідно до переліку засобів ТЗІ, розміщеного на сторінці «Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації» Державної служби спеціального зв’язку та захисту інформації України [6]. Обидва антивіруси, які представлені у таблиці 2.1 підходять для використання на основі експертних висновків.

Порівнявши АВПЗ можна зробити висновок, що обидва антивіруси мають гарний функціонал, але Avast одразу пропонує вигідну пропозицію з централізованим управлінням, гарним захистом від вірусів і брандмауером з автоматичним налаштуванням, чим керівники Новопавлівської сільської ради і скористались, вибравши Avast. ESET в свою ж чергу має достатній функціонал тільки з персональними пропозиціями, що розділяються на багато підвидів і мають свою високу ціну, яка набагато вище за Avast.

Таблиця 2.1 – Порівняння АВПЗ

Функція	Avast	ESET
Антивірусний захист	Виявляє більшість шкідливих програм, але сканує довше. Пропонує 6 різних типів сканування: Швидке сканування - сканує критичні ділянки системи. Повне сканування - перевіряє всю систему. Інтелектуальне сканування - виявляє застарілі програми, файли cookie та проблеми з продуктивністю. Спеціальне сканування - автоматизує тип і частоту сканування. Цільове сканування - перевіряє вибрані папки або файли.	Виявляє більшість шкідливих програм і сканує найбільш приховані області на ПК. Пропонує 3 типи сканерів: Повне сканування - проводить ретельну перевірку кожної області жорсткого диска. Спеціальне сканування - дозволяє вибирати та сканувати певні папки або файли. Сканування знімних носіїв - сканує зовнішні пристрої та диски, підключені до системи.
Брандмауер	Легкий в налаштуванні. Пропонує функцію інтелектуального брандмауера, який автоматично налаштовується залежно від мережі, до якої ви підключаєтеся. Також можливо налаштувати фільтри вручну, але Avast рекомендує змінювати правила застосування лише у разі крайньої необхідності. У більшості випадків АВПЗ формулює оптимальні правила без вашого втручання.	Легкий в налаштуванні. Має брандмауер, який блокує усі несанкціоновані з'єднання. Можливо встановити різні режими фільтрації, такі як: Автоматичний режим - дозволяє весь вихідний трафік і блокує більшість вхідного трафіку. Інтерактивний режим - пропонує заздалегідь визначені правила, які вимагають вашого схвалення або несхвалення для кожного запит. Режим на основі політик - включає правила, визначені користувачем, і блокує всі невизначені з'єднання. Режим навчання - автоматично створює та зберігає правила.
Менеджер паролів	Має стандартний менеджер паролів з базовими функціями.	Має стандартний менеджер паролів з базовими функціями.
Централізоване управління	Включає централізоване управління з преміум-планом Essential Business Security	Включає централізоване управління разом з хмарною консоллю, але тільки для персональних пропозицій.

Продовження таблиці 2.1

Функція	Avast	ESET
Продуктивність	Сильніше навантажує ПК. При запуску інших програм при скануванні продуктивність уповільнюється.	Не має впливу на ПК, навіть при повному скануванні диска.
Підтримка	24/5 швидка та дружня підтримка від наших висококваліфікованих технічних інженерів	Надає кілька каналів підтримки та відмінне обслуговування клієнтів.
Ціна	Пропонує 2 преміум-плани: Small Office Protection за 2086 грн та Essential Business Security за 4234 грн на рік, з дуже обмеженою кількістю функцій у базових підписках.	Має багато персональних пропозицій та 2 преміум-плани: Security Essential за 4608 грн та Security Premium за 6972 грн на рік, кожен з яких пропонує хороше якість та високу ціну, але без персональної пропозиції не має достатньо функціоналу для мережі комп'ютерів.

При обстеженні Avast було виявлено, що АВПЗ не оновлюється, що може викликати багато загроз для безпеки інформації та самого обладнання на якій вона циркулює. АВПЗ працює на основі розпізнавання шкідливого коду, використовуючи дані з антивірусних сигнатур, які зберігаються у вірусних базах.

У світі постійно з'являється велика кількість нових шкідливих програм. Якщо не оновлювати АВПЗ, існує велика можливість, що програма проігнорує шкідливе ПЗ, тож найкращим захистом комп'ютера користувача від цих загроз є робоча та оновлена антивірусна програма. Тому необхідним рішенням буде підключення автоматичного оновлення ПЗ в неробочі години.

Адміністратор безпеки має додатково перевіряти час від часу ПЗ на наявність останнього оновлення, це буде легше та комфортніше робити за допомогою Avast Business Hub, який дозволяє адміністратору керувати функціями Avast на усіх підключених до цього централізованого управління пристроях. На рисунку 2.1 представлений вигляд Avast Business Hub та вкладки «Devices» в якій можна керувати усіма пристроями.

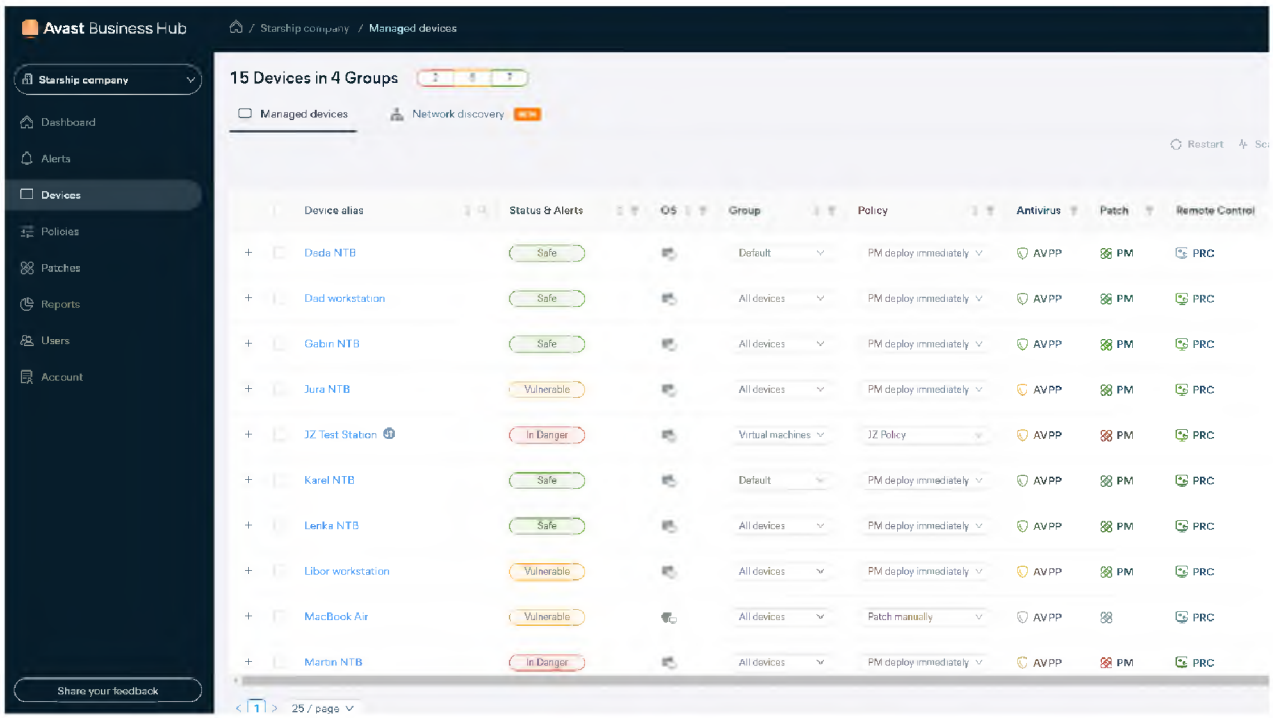


Рисунок 2.1 – Avast Business Hub

2.1.2 Заходи з регулювання використання стороннього ПЗ

При обстеженні було виявлено, що користувачі використовують сторонні зовнішні носії інформації. Відсутність обліку за сторонніми носіями інформації може спричинити зараження технічних засобів чи витік інформації. Для зменшення загрози необхідно сформувати перелік та розміщення носіїв. Створювати перелік та контролювати використання носіїв буде системний адміністратор, так як він відповідає за фізичний стан обладнання та мережі.

Важливою проблемою є можливість завантаження стороннього ПЗ з інтернету. Вирішенням проблеми може стати зміна прав доступу у користувачів адміністратором безпеки, задля заборони встановлення нових застосунків.

Також, задля недопущення зберігання на ПК користувачів зайвої інформації, наприклад: фільми, зображення, ігри – будуть введені квоти, які будуть обмежувати дисковий простір, що унеможливить зловживати ним, але диски постійно заповнюються новою інформацією, тому адміністратор безпеки повинен слідкувати за лімітом простору та збільшувати його у разі необхідності введення нової інформації.

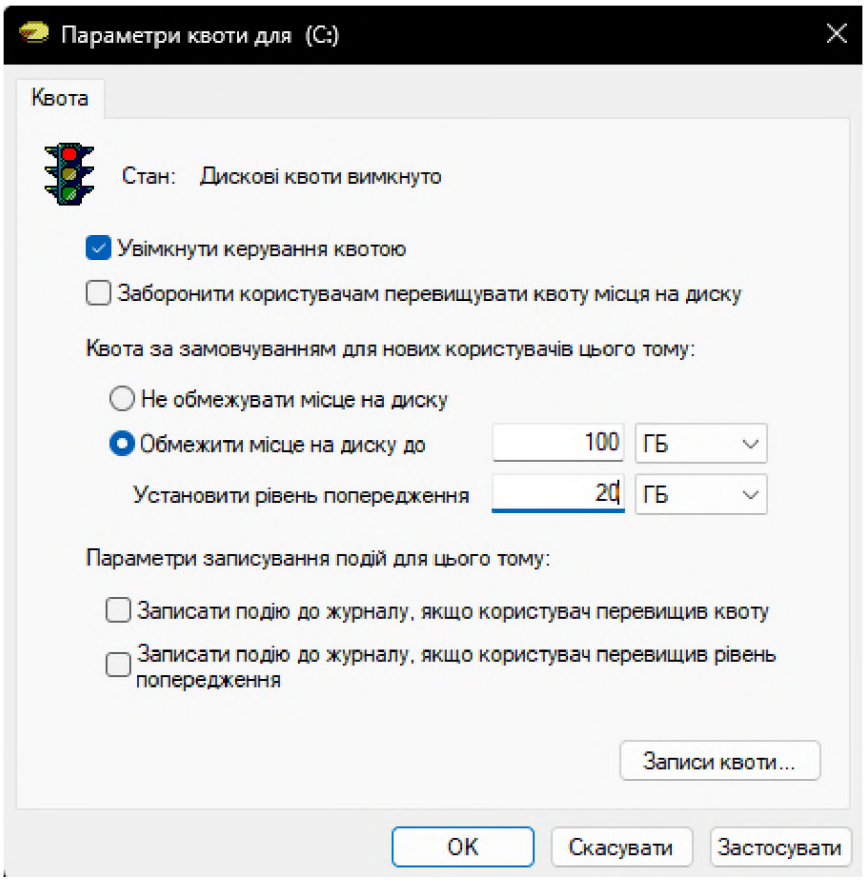


Рисунок 2.2 – Налаштування квот

2.1.3 Заходи для забезпечення захисту від атак на відмову в обслуговуванні

При обстеженні було виявлено, що в системі не використовується моніторинг функцій та вимкнені системні журнали подій. Відсутність спостереження за технічними засобами може погано позначитись на можливостях реагування на загрози, в тому числі і DDOS-атаки. Зменшити загрозу можна почавши використовувати «Windows Performance Monitor», створенням у ньому «Data Collector Sets» для моніторингу мережевих інтерфейсів. Створення Data Collector Sets наведено на рисунку 2.3.

Використовуючи дану системну програму можна збирати дані про компоненти обладнання, як наприклад, пам’ять, материнську плату, температуру, процесора, так і про інші події: вхід користувача у систему, брандмауер і т.д.

Приклад властивостей збору інформації про вхід користувача у систему показано на рисунку 2.4.

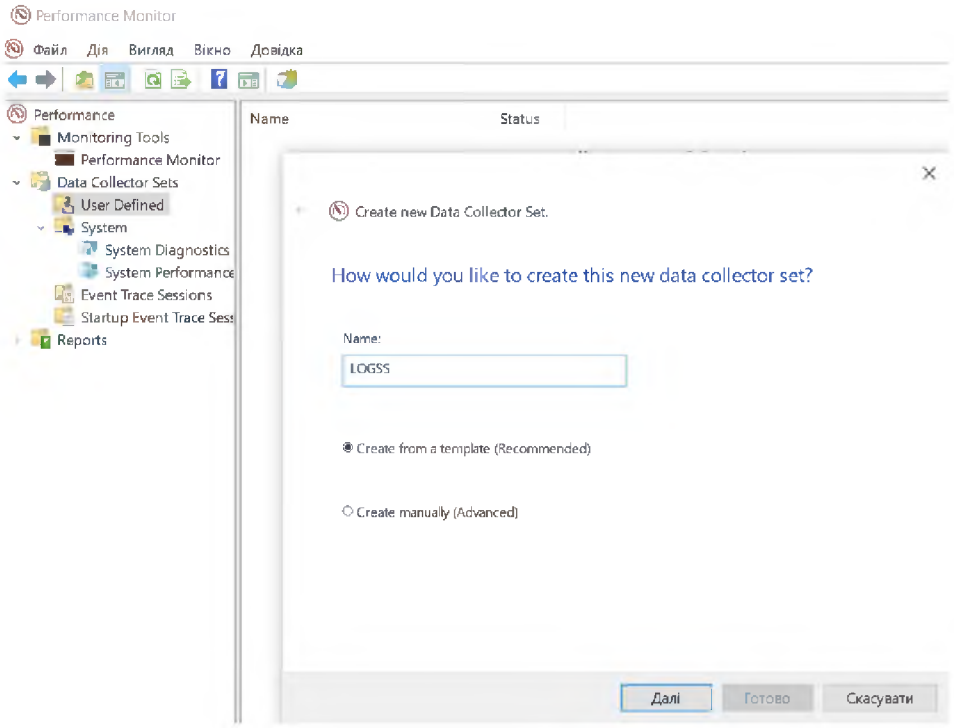


Рисунок 2.3 – Створення Data Collector Set

Створивши Data Collector Set потрібно натиснути на кнопку старт, щоб увімкнути збір інформації про систему.

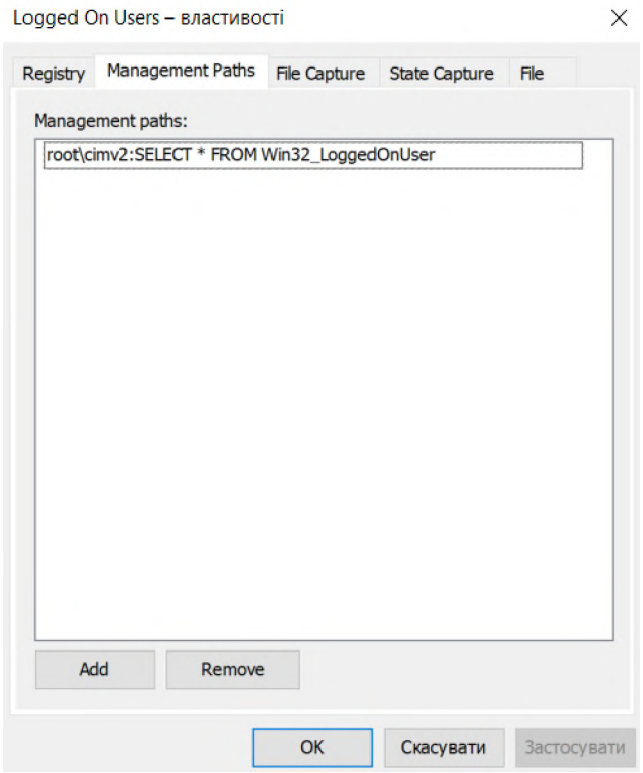
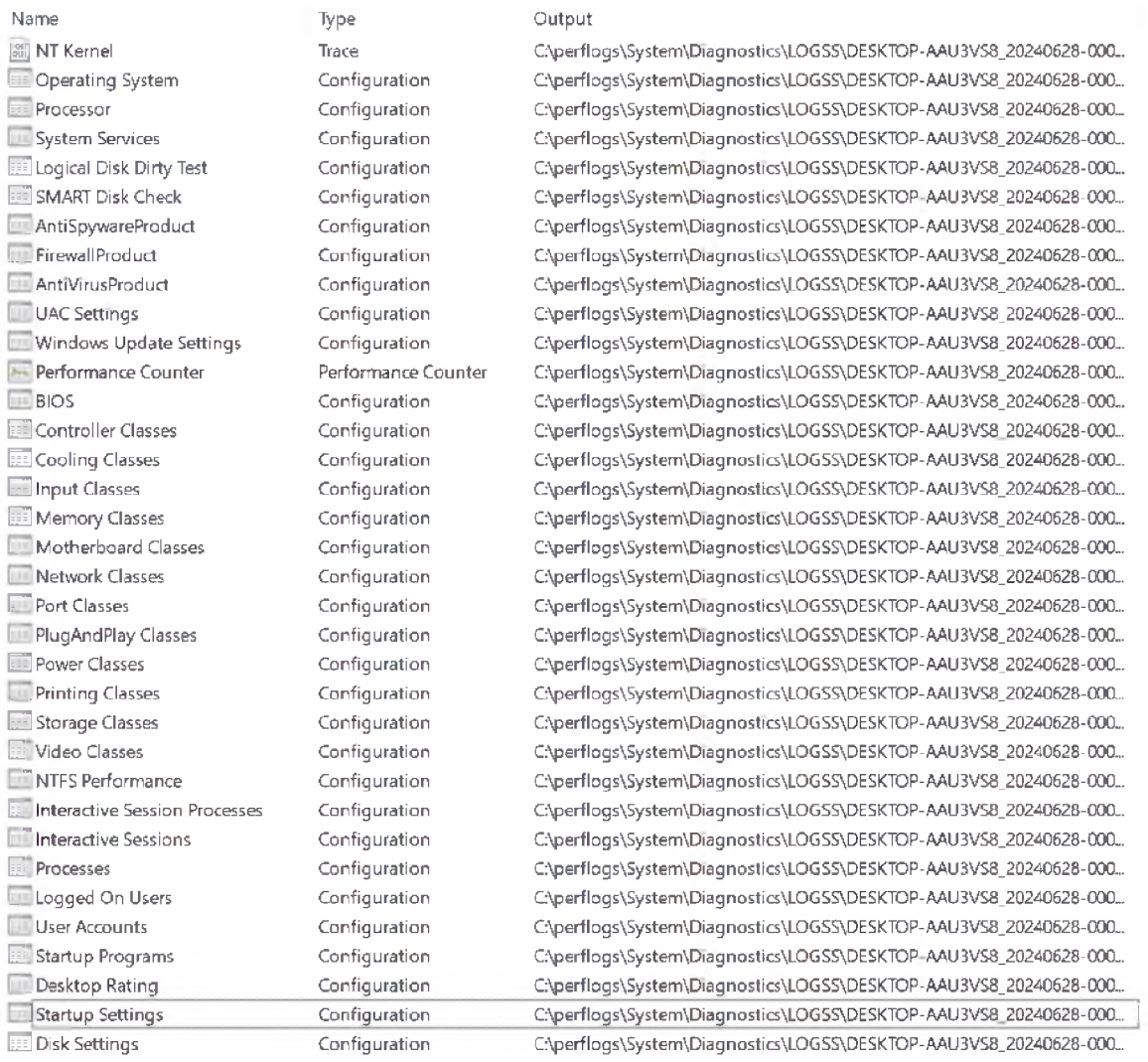


Рисунок 2.4 – Властивості входу користувача у систему



Name	Type	Output
NT Kernel	Trace	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Operating System	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Processor	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
System Services	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Logical Disk Dirty Test	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
SMART Disk Check	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
AntiSpywareProduct	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
FirewallProduct	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
AntiVirusProduct	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
UAC Settings	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Windows Update Settings	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Performance Counter	Performance Counter	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
BIOS	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Controller Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Cooling Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Input Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Memory Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Motherboard Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Network Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Port Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
PlugAndPlay Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Power Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Printing Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Storage Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Video Classes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
NTFS Performance	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Interactive Session Processes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Interactive Sessions	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Processes	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Logged On Users	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
User Accounts	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Startup Programs	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Desktop Rating	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Startup Settings	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...
Disk Settings	Configuration	C:\perflogs\System\Diagnostics\LOGSS\DESKTOP-AAU3VS8_20240628-000...

Рисунок 2.5 – Дані, які знаходяться в Data Collector Sets

Також потрібно встановити «Microsoft Network Monitor» та налаштувати фільтри для виявлення підозрілої активності з великої кількості запитів з одного IP-адреси. Цей інструмент дозволяє захоплювати, переглядати та аналізувати мережеві дані, а також розшифровувати мережеві протоколи. Його можна використовувати для визначення IP-адреси, з якої надходять запити для DDOS-атаки.

Для того, щоб розпочати потрібно вибрати мережевий адаптер, на який приходять запити і почати захоплення. DDOS-атаки відбуваються через велику кількість http запитів, які надсилаються до вас, тому у фільтрах потрібно виставити http, щоб побачити запити, які перенавантажують ресурс. Знайшовши сайт, все що потрібно, це заблокувати його через брандмауер.

Ось деякі приклади фільтрів які також можуть бути корисними:

– ipv4.address == "client ip" and ipv4.address == "server ip": цей фільтр призначений для відображення всіх пакетів, які включають як клієнтську, так і серверну IP-адреси.

– tcp.port ==: цей фільтр призначений для фільтрації пакетів за номером TCP-порту. Наприклад, tcp.port == 80 відобразить усі TCP-пакети, які використовують порт 80 (HTTP).

– udp.port ==: цей фільтр призначений для фільтрації пакетів за номером UDP-порту. Наприклад, udp.port == 53 відобразить усі UDP-пакети, які використовують порт 53 (DNS).

– icmp: цей фільтр відобразить усі ICMP-пакети, які зазвичай використовуються для діагностичних цілей, таких як команду ping.

– arp: цей фільтр відобразить усі ARP-пакети, які використовуються для перетворення IP-адрес в MAC-адреси в локальних мережах.

– property.tcpretransmits: цей фільтр відображає всі TCP-пакети, які були повторно передані. Це може бути корисно для діагностики проблем з мережею.

– property.tcprequestfastretransmits: цей фільтр відображає всі запити на швидке повторне передавання TCP-пакетів. Це відбувається, коли TCP-сегмент втрачений і отримувач надсилає повторний запит, щоб швидше отримати відсутній сегмент.

– tcp.flags.syn == 1: цей фільтр відображає всі TCP-пакети з встановленим прапором SYN. Цей прапор використовується при встановленні нового TCP-з'єднання (TCP handshake).

Ці фільтри дозволяють детально аналізувати мережевий трафік, визначати та усувати проблеми в мережі та забезпечувати безпеку.

На рисунку 2.6 зображено меню, яке захоплює пакети даних з мережевого адаптера.

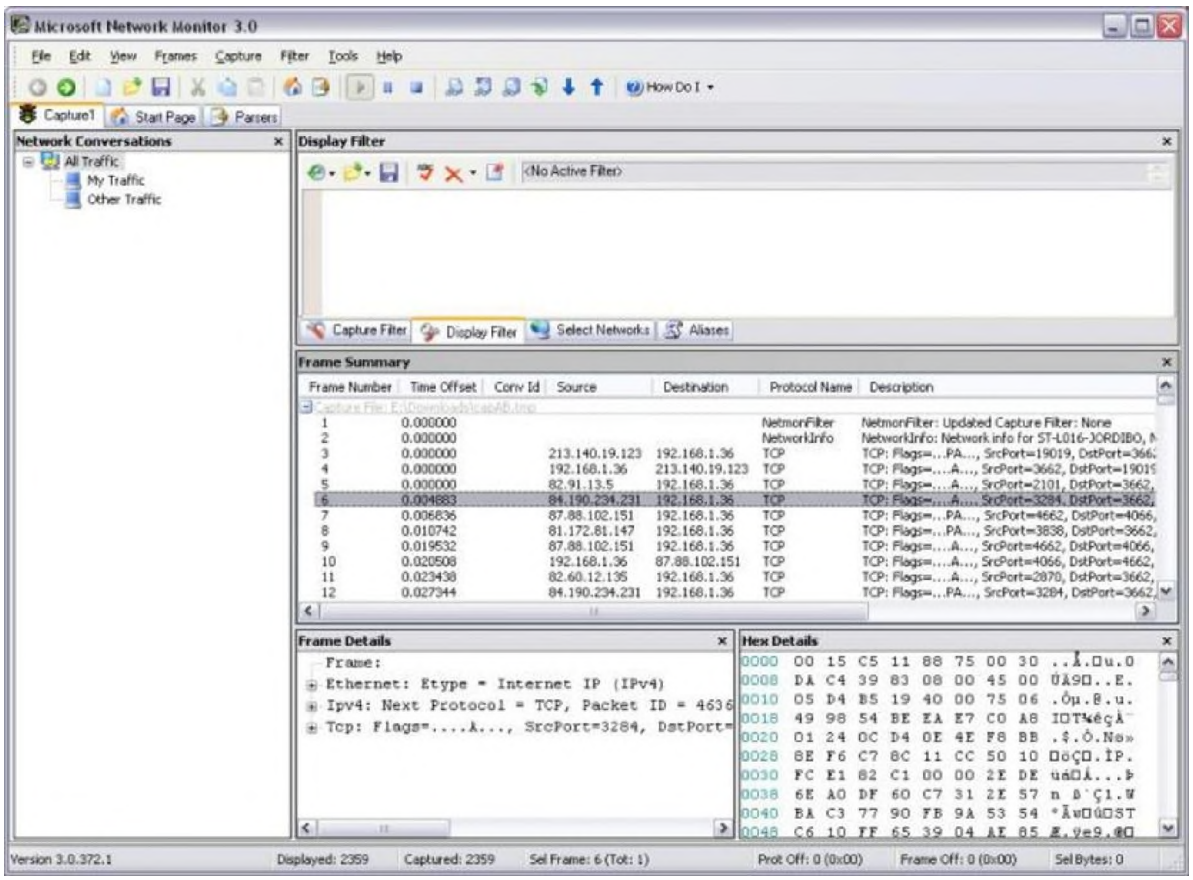


Рисунок 2.6 – Захоплення мережевого адаптеру

2.1.4 Заходи для розподілення адміністративних прав доступу

При обстеженні було виявлено, що системний адміністратор має найвищі повноваження у системі. За ним відсутній нагляд і якщо він стане порушником, цього або не помітять, або не зможуть зупинити. Рішенням цієї проблеми є створення додаткового облікового запису адміністратора безпеки іншому кваліфікованому працівнику для надання йому прав на спостереження за системними журналами подій. Найбільш кваліфікований працівник у Новопавлівській сільській раді – це секретар.

Також необхідно закрити доступ системному адміністратору до інформації, що обробляється, щоб він мав доступ лише до технічних речей для забезпечення ним ремонту та налаштування обладнання для успішної експлуатації користувачами. Враховуючи усі ці зміни була оновлена матриця розмежування прав доступу.

Таблиця 2.2 – Нова матриця розмежування прав доступу

№	Інформація	Керівник	Заступник керівника	Секретар	Адміністратор безпеки	Системний адміністратор	Бухгалтери
1	Фінансові дані	R, P	R, P	R, P	-	-	R,W, M, D, P, C
2	Документація сесій та засідань	R, W, M, D, P, C	R, W, M, D, P, C	R, W, M, P, C	-	-	R, P
3	Громадські реєстри	R, W, M, D, P, C	R, W, M, D, P, C	R, W, M, P, C	-	-	-
4	Правова документація	R, W, M, D, P, C	R, P	-	-	-	-
5	Проєкти та програми розвитку	R, W, M, D, P, C	R, W, M, D, P, C	R, W, M, P, C	-	-	-
6	Технічна документація	R, W, M, D, P, C	R, P	-	-	-	-
Журнал подій		-	-	-	+	+	-
Встановлення ПЗ		+	-	-	-	+	-

- R – читання;
- W – запис;
- M – модифікація;
- D – видалення;
- P – друк;
- C – створення.

2.1.5 Заходи для недопущення стороннього візуального контакту з інформацією

При обстеженні було виявлено, що існує можливість розголошення конфіденційної інформації, за рахунок утворення прямого візуального контакту з технічними засобами, які можуть містити конфіденційну інформацію. Щоб не допустити такого витоку інформації, потрібно встановити жалюзі, які б закривали вікна і ввести заборону на фото/відеозйомку ОІД.

2.1.6 Заходи для забезпечення безперебійного електропостачання

При обстеженні було виявлено, що Новопавлівська сільська рада має генератор, але не має джерела безперебійного живлення, яке б убезпечило роботу під час стабілізаційних чи екстренних відключень електропостачання до увімкнення генератора. Рішенням цієї проблеми може бути встановлення такого пристрою, а також встановлення автоматичного зберігання файлів на технічних засобах. Спершу потрібно вибрати ДБЖ.

Існує три основі типи архітектури:

Резервний (off-line), пристрій не має стабілізатору, тому підійде, якщо у будинку мінімальні коливання напруги. Через відключення часто бувають різкі коливання напруги, тому цей тип нам не підходить, до того ж має не найшвидше перемикання на акумуляторний режим роботи (приблизно 15-20мс). Зображений на фотографії 2.7 [14].

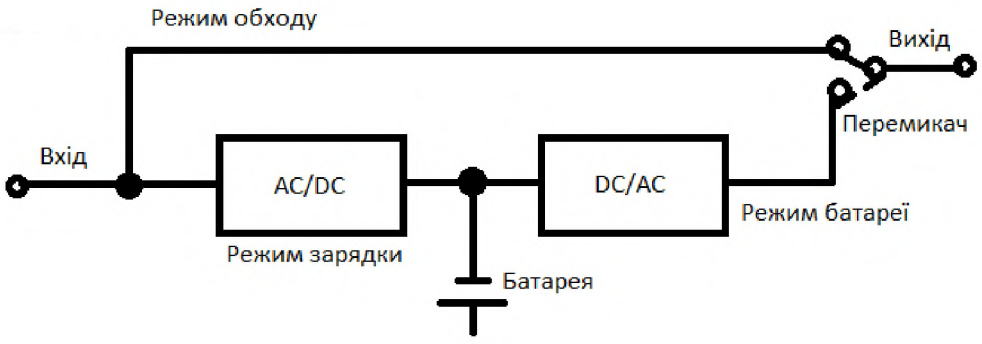


Рисунок 2.7 – Резервний (off-line)

Джерело безперебійного живлення з інтерактивною схемою має ті ж якості що і резервні, за винятком однієї особливості. У ланцюзі є стабілізатор напруги, реалізований на основі автотрансформатора. Це, в свою чергу, дозволяє підтримувати в системі рівномірне напругу в деякому діапазоні [14].

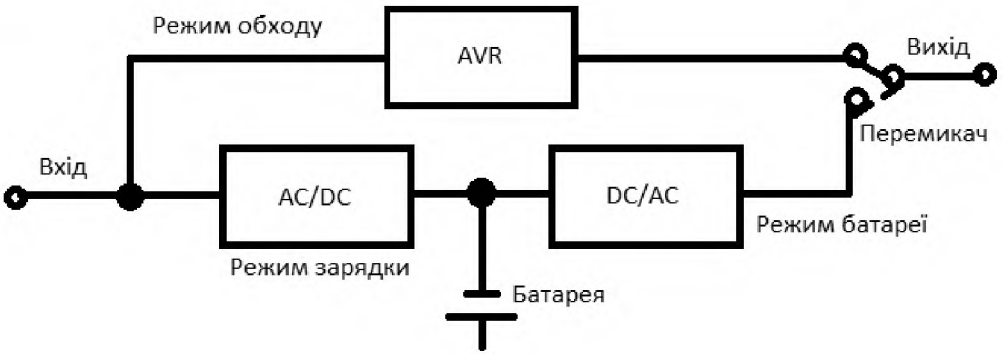


Рисунок 2.8 – Інтерактивний(Line-interactive)

У Online режимі, акумулятори працюють в режимі «буфера», а час зміни режиму електропостачання технічно дорівнює 0 мс. Таким чином, джерело безперебійного живлення типу on-line або подвійного перетворення гарантує захист навантаження, від будь-яких перешкод, які надходять з мережі [14].

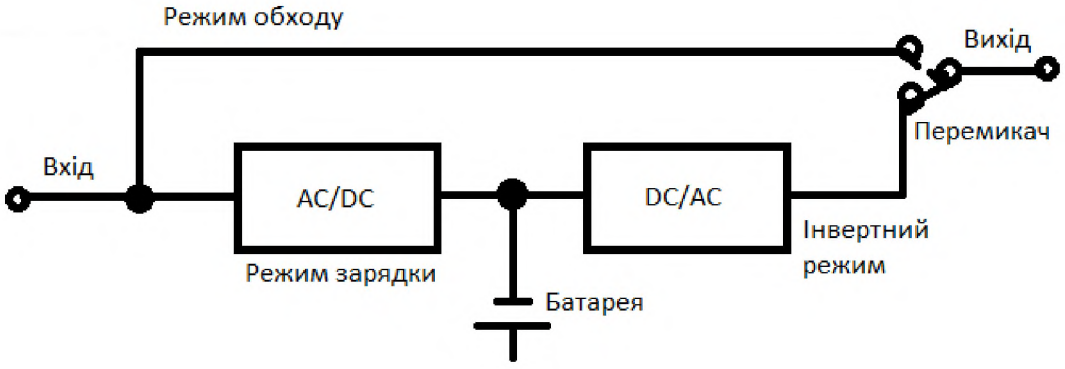


Рисунок 2.9 – Буферний(on-line)

Таблиця 2.3 – Порівняння типів архітектури ДБЖ

Характеристика	Off-line	Line-interactive	On-line
Потужність UPS	< 1,5кВА	< 4кВА	не обмежена
Стабілізація напруги	немає	ступінчата	повна
Стабілізація частоти	немає	немає	є
Фільтрація перешкод	слаба	середня	максимальна
Частота переходів	висока	середня	Не часто
Час переходу на батареї	4-16 мс	2-4 мс	0, немає
Час роботи від батареї	обмежений	обмежений	будь-який, визначається комплектацією АКБ
Форма синусоїди	часто трапеце-подібна/	трапеце-подібна /синусоїдальна	синусоїдальна
Режим by-pass	немає	немає	є
Гальванічна розв'язка	немає	немає	можлива

Таблиця 2.4 – Порівняння ДБЖ

Характеристика	APC Back-UPS BX700UI	CyberPower BR700ELCD	Powercom IMD-825AP	Eaton 5E 850iUS
Потужність (ВА)	700	700	825	850
Вихідна потужність (Вт)	390	420	495	480
Ємність батареї	7.2 А·год	7 А·год	9 А·год	9 А·год
Час зарядки	6 годин	8 годин	4-6 годин	USB, RS-232
Тип вихідної хвилі	Синусоїдальна	Синусоїдальна	Імітована Синусоїдальна	Синусоїдальна

Таблиця 2.5 – Таблиця використання електроенергії

№	Обладнання	Використання електроенергії, вт	Кількість	Загальне використання, вт
1	Монітор: Philips 223V7QHAB	18	7	126
2	Системний блок: Dell OptiPlex 3080	200	7	1400
3	Клавіатура: Logitech K120	0,5	7	3,5
4	Миша: Logitech B100	0,1	7	0,7
5	Принтер: Brother DCP-L2550D (в режимі друку)	480	2	960

Продовження таблиці 2.5

№	Обладнання	Використання електроенергії, вт	Кількість	Зашальне використання, вт
6	Джерело безперебійного живлення: Powercom IMD-825AP	10	2	20
	Сумарне використання			2510,2

Для нормальної роботи під час відключень Новопавлівська сільська рада має мати 2 ДБЖ, один в кабінеті керівника, інший в бухгалтерській. Найкраще для нашої ситуації буде інтерактивний тип, так як напруга постійно коливається і стабільне електропостачання є лише декілька годин.

Для забезпечення нормальної роботи під час відключень електроенергії, Новопавлівська сільська рада потребує два джерела безперебійного живлення (ДБЖ): один для кабінету керівника і один для бухгалтерії. Найбільш підходящим для нашої ситуації буде інтерактивний тип ДБЖ, оскільки напруга постійно коливається, і стабільне електропостачання є лише декілька годин. То ж я оберу ДБЖ Powercom IMD-825AP LCD IEC, враховуючи, що в нього більша ємність батареї і швидша зарядка – він кращий.

2.2 Висновки до спеціального розділу

В спеціальному розділі були представлені проєктні рішення для актуальних проблем, які визначені в першому розділі. Запропоновано ДБЖ, встановлені нові правила розмежування доступу та вимоги, щодо працівників.

Встановлені квоти щодо дискового простору та автоматичне оновлення АВПЗ. Секретар отримав вимоги, щодо створення переліку зовнішніх носіїв інформації та перевірки їх місцезнаходження та використання, а також була налаштована система моніторингу та журнали подій.

Впровадивши дані заходи програмно-організаційного рівня для підвищення безпеки інформації, обраний в першому розділі профіль захищеності буде реалізовано, а ІКС Новопавлівської сільської ради отримає необхідний рівень захисту інформації.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічної частини є техніко-економічне обґрунтування доцільності запровадження комплексної системи захисту. Для цього обумовлюється економічна ефективність застосування основних результатів, встановлених в процесі роботи. Економічна ефективність визначається:

– розрахуванням капітальних витрат, для розроблення КСЗІ;

– розрахуванням експлуатаційних витрат на утримання і обслуговування КСЗІ;

– визначенням річного економічного ефекту від впровадження КСЗІ;

– визначенням та аналізом показників економічної ефективності запропонованих рішень.

– висновком щодо економічної доцільності

3.1 Розрахунок капітальних витрат

3.1.1 Розрахунок трудомісткості розробки комплексної системи захисту інформації

Трудомісткість розробки КСЗІ:

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин,} \quad (3.1)$$

де $tmз$ – тривалість складання технічного завдання на розробку політики безпеки інформації, 16 годин;

$tв$ – тривалість розробки концепції безпеки інформації у організації, 14 годин;

ta – тривалість процесу аналізу ризиків, 19 годин;

$tвз$ – тривалість визначення вимог до заходів, методів та засобів захисту, 9 годин;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, 25 годин;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, 18 годин;

$t_{д}$ – тривалість документального оформлення політики безпеки, 5 годин.

$$t = 16 + 14 + 19 + 9 + 25 + 18 + 5 = 106 \text{ годин.}$$

3.1.2 Розрахунок витрат на створення політики безпеки інформації

$$K_{рп} = З_{зп} + З_{мч}, \quad (3.2)$$

де $K_{рп}$ - витрати на розробку політики безпеки інформації, 17164,26 грн;

$З_{зп}$ - витрати на заробітну плату спеціалісту з інформаційної безпеки, 16960 грн;

$З_{мч}$ - вартість витрат машинного часу, що необхідні для розробки політики, 204,26.

Витрати на заробітну плату спеціалісту з інформаційної безпеки:

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

де t – загальна тривалість розробки політики безпеки, 106 годин;

$З_{іб}$ – середньогодинна заробітна плата спеціаліста з інформаційної безпеки, 160 грн/година.

$$З_{зп} = 106 \cdot 160 = 16960 \text{ грн}$$

Витрати машинного часу:

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

де t – трудомісткість розробки політики безпеки інформації на ПК, 106 годин;

Смч – вартість 1 години машинного часу ПК, 1,927 грн/година.

Вартість 1 години машинного часу ПК, грн/година.

$$Смч = Р \cdot t_{нал} \cdot Се + \frac{Фзал \cdot На}{Fр} + \frac{К\,лпз \cdot На\,пз}{Fр}, \text{ грн,} \qquad (3.5)$$

де Р – встановлена потужність ПК, 0,25 кВт;

Се – тариф на електричну енергію, 4,32 грн/кВт·година;

Фзал – залишкова вартість ПК на поточний рік, 5130 грн;

На – річна норма амортизації на ПК, частки одиниці, 0,2;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці, 0,5;

Клпз – вартість ліцензійного програмного забезпечення, 7400 грн;

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

Залишкова вартість ПК:

$$Фзал = Впоч – (Впоч \cdot \ t_в) / t_{мін}, \text{ грн,} \qquad (3.6)$$

де Впоч – початкова вартість ПК, 22000 грн;

$t_в$ – термін використання ПК, 46 місяців;

$t_{мін}$ – мінімальний термін корисної служби, 60 місяців.

$$Фзал = 22000 – (22000 \cdot 46) / 60 = 5130 \text{ грн}$$

$$Смч = 0,25 \cdot 1 \cdot 4,32 + \frac{5130 \cdot 0,2}{1920} + \frac{7400 \cdot 0,5}{1920} = 1,927 \text{ грн/година}$$

$$З_{мч} = 106 \cdot 1,927 = 204,26 \text{ грн}$$

$$К_{рп} = 16960 + 204,26 = 17164,26 \text{ грн}$$

3.1.3 Розрахунок капітальних витрат на створення КСЗІ

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \quad (3.7)$$

де Кпр – вартість розробки проєкту інформаційної безпеки та залучення для цього зовнішніх консультантів, 17164,26 грн;

Кзпз – вартість закупівель ліцензійного основного й додаткового ПЗ, 0 грн;

Кпз – вартість створення основного й додаткового ПЗ, 0 грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 0 грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, 5000 + 1000 = 6000 грн;

На навчання працівників роботі з централізованим управлінням АВПЗ Avast Business Hub витратили 5000 грн, та ще 1000 грн витратили на проведення тренувальних заходів для злагодженої роботи в екстренних ситуаціях з ДБЖ та генератором.

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 3000 грн.

3.1.4 Розрахунок витрат на встановлення джерела безперебійного живлення

Вартість встановлення ДБЖ:

$$Кзс = Кзз + Кн + Кнавч, грн, \quad (3.8)$$

де Кзз – вартість закупівлі забезпечення та допоміжних матеріалів, 4,200 · 2 = 8400 грн;

Таблиця 3.1 – Опис ДБЖ

Характеристика	Powercom IMD-825AP
Потужність (ВА)	825
Вихідна потужність (Вт)	495
Ємність батареї	9 А·год
Час зарядки	4-6 годин
Тип вихідної хвилі	Імітована Синусоїдальна
Ціна, грн	4200

Кн – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 4 години · 400 грн = 1600 грн;

$$Кзс = 8400 + 1600 = 10000 грн$$

3.1.5 Розрахунок витрат на встановлення жалюзі на вікна

Вартість встановлення жалюзі:

$$Кзс = Кзз + Кн, грн, \quad (3.8)$$

де Кзз – вартість закупівлі забезпечення та допоміжних матеріалів, 800 · 5 = 4000 грн;

Кн – витрати на встановлення обладнання та налагодження системи

інформаційної безпеки, 2 години · 100 грн = 200 грн;

$$Кзс = 4000 + 200 = 4200 \text{ грн}$$

Отже, капітальні витрати:

$$К = 17164,26 + 10000 + 6000 + 4200 + 3000 = 40364,26 \text{ грн}$$

3.2 Розрахунок експлуатаційних витрат

3.2.1 Розрахунок річних поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \text{ тис. грн,} \quad (3.9)$$

де Св – вартість відновлення й модернізації системи, 0 грн;

Ск – витрати на керування системою в цілому, 89422,52 грн;

Сак – витрати, викликані активністю користувачів системи інформаційної безпеки, 0 грн.

Витрати на відновлення й модернізацію відсутні.

3.2.2 Розрахунок витрат на керування системою інформаційної безпеки

Витрати на керування системою інформаційної безпеки складають:

$$Ск = С_н + С_а + С_з + С_{єв} + С_{ел} + С_о + С_{тос}, \text{ грн,} \quad (3.10)$$

де Сн – витрати на навчання адміністративного працівника, 4500 грн;

При обстеженні стало зрозуміло, що системний адміністратор може зловживати правами, тому було прийняти рішення створити додатковий обліковий запис для секретаря і провести тренінги, щодо роботи з системними

журналами, моніторинговими сервісами та в цілому роллю адміністратора безпеки.

Са – річний фонд амортизаційних відрахувань; 8400/5 = 1680 грн;

Сєв – витрати єдиного внеску на загальнообов'язкове соціальне страхування, 61800 · 0,22 = 13596 грн;

Сел – вартість електроенергії, що споживається апаратурою КСЗІ протягом року, 4147,2 грн;

Со – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу, грн, 0 грн;

Стос – витрати на технічне й організаційне адміністрування та сервіс КСЗІ визначаються у відсотках від вартості капітальних витрат 3%, 1211 грн;

Річний фонд заробітної плати інжерно-технічного персоналу:

$$С_з = З_{осн} + З_{дод}, \text{ грн}, \quad (3.11)$$

де Зосн – основна заробітна плата, 15000 · 0,3 · 12 = 54000 грн;

Здод – додаткова заробітна плата, 650 · 12 = 7800 грн.

$$С_з = 54000 + 7800 = 61800 \text{ грн}$$

Вартість електроенергії, що споживається апаратурою КСЗІ протягом року:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн}, \quad (3.12)$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0,5 кВт;

Таблиця 3.2 – Таблиця використання електроенергії

№	Обладнання	Використання електроенергії, вт	Кількість	Загальне використання, вт
1	Монітор: Philips 223V7QHAB	18	7	126
2	Системний блок: Dell OptiPlex 3080	200	7	1400
3	Клавіатура: Logitech K120	0,5	7	3,5
4	Миша: Logitech B100	0,1	7	0,7
5	Принтер: Brother DCP-L2550D (в режимі друку)	480	2	960
6	Джерело безперебійного живлення: Powercom IMD-825AP	10	2	20
	Сумарне використання			2510,2

Fp – річний фонд робочого часу (за 40-годинного робочого тижня Fp = 1920);

$Ц_е$ – тариф на електроенергію, 4,32 грн/кВт·годин.

$$С_{ел} = 2,5 \cdot 1920 \cdot 4,32 = 20736 \text{ грн}$$

$$Ск = 4500 + 1680 + 61800 + 13596 + 20736 + 1211 = 103523 \text{ грн}$$

3.3 Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

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

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 7 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 17000 грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 22000 грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 6 осіб;

О – обсяг атакованого вузла або сегмента корпоративної мережі, 200000 грн у рік;

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

I – число атакованих вузлів або сегментів корпоративної мережі, 3;

N – середнє число атак на рік, 7.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.13)$$

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.

Заробітні плати працівників:

- керівник: кількість – 1, зарплата – 22000 грн;
- заступник керівника: кількість – 1, зарплата – 18000 грн;
- секретар: кількість – 1, зарплата – 17000 грн;
- бухгалтер: кількість – 3, зарплата – $15000 \cdot 3 = 45000$ грн

– системний адміністратор: кількість – 1, зарплата – 18000 грн;

– прибиральниця: кількість – 1, зарплата – 8000 грн.

Разом: 22000 + 18000 + 17000 + 45000 + 18000 + 8000 = 128000 грн

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$Пп = \frac{\sum Зс}{F} \cdot tп, \quad (3.14)$$

де Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 128000 грн за місяць;

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

П – час простою вузла або сегмента корпоративної мережі, 2 години;

$$Пп = \frac{128000}{176} \cdot 3 = 2181{,}81 \text{ грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \quad (3.15)$$

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, 0 грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$Пви = \frac{\sum Зс}{F} \cdot тви \quad (3.16)$$

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

$$Ппв = \frac{\sum Зо \cdot Чо}{F} \cdot тв \quad (3.17)$$

$$Пви = \frac{128000}{176} \cdot 4 = 2909{,}09 \text{ грн}$$

$$Ппв = \frac{17000}{176} \cdot 7 = 676{,}13 \text{ грн}$$

$$Пв = 2909{,}09 + 676{,}13 = 3585{,}22 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{F} \cdot (тп + тв + тви) \quad (3.18)$$

$$V = \frac{200000}{1920} \cdot (4 + 4 + 7) = 1562{,}5 \text{ грн}$$

$$U = 2181{,}81 + 3585{,}22 + 1562{,}5 = 7329{,}53 \text{ грн}$$

$$В = \sum i \cdot \sum n \cdot U \quad (3.19)$$

$$В = 3 \cdot 7 \cdot 7329{,}53 = 153920{,}13 \text{ грн}$$

Загальний збиток від атаки від атаки на сегмент чи вузол корпоративної мережі: 153920,13 грн

3.6 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \tag{3.20}$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, 153920,13 грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці 0,8;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 153920{,}13 \cdot 0{,}8 - 103523 = 19613{,}104 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

$$ROSI = \frac{E}{K}, \text{ частки одиниці}, \tag{3.21}$$

де E – загальний ефект від впровадження системи інформаційної безпеки, тис. грн;

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

$$ROSI = \frac{19613,104}{40364,26} = 0,48$$

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти розрахункове значення ROSI з бажаним значенням показника ефективності $E_н$. Проект системи інформаційної безпеки визнається доцільним за умови:

$$ROSI > E_н. \quad (3.22)$$

Але організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, то ж проєкт визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (Nдеп – Nінф) / 100 \quad (3.23)$$

де $N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 10%;

$N_{інф}$ – річний рівень інфляції, 7%.

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,2 > (10 – 7) / 100 = 0,2 > 0,03$$

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

$$To = \frac{1}{ROSI} \quad (3.23)$$

$$To = \frac{1}{0,48} = 2,08 \text{ роки, або } 25 \text{ місяців}$$

3.5 Висновки до економічного розділу

Було проведено розрахунки капітальних витрат на придбання і налагодження складових системи інформаційної безпеки, навчання працівників, щодо заходів програмно-організаційного рівня для підвищення безпеки інформації, впровадження ДБЖ та жалюзі. Було оцінено можливі збитки від атаки на вузли чи сегменти корпоративної мережі. Коефіцієнт повернення інвестицій ROSI показав, що одна гривня капітальних інвестицій дає 0,48 гривні додаткового прибутку.

Враховуючи, що об’єкт має критичне значення та має багато важливих даних, а також те, що проєкт окупиться через 2,08 роки, або 25 місяців можна зробити висновок, що прийняте рішення економічно доцільне.

ВИСНОВКИ

У першому розділі було визначено стан питання, проведено дослідження ОІД, створено організаційну структуру працівників, перелічено обчислювальну та допоміжну техніку. Обстежене інформаційне середовище, інформаційні потоки та проаналізовано розмежування прав доступу, визначено моделі загроз та порушника, проаналізовано найактуальніші проблеми і було обрано профіль захищеності на основі класу АС.

Перший розділ містить в собі визначення заходів, які необхідно провести для забезпечення достатнього рівня безпеки в Новопавлівській сільській раді.

У другому розділі проводились заходи програмно-організаційного рівня для підвищення безпеки інформації, які пропонували рішення для найактуальніших проблем визначених в першому розділі, таких як: можливе зловживання правами адміністратором, зараження технічних засобів шкідливим ПЗ, збої з електропостачанням і т.д.

Другий розділ містить в собі запровадження заходів, завдяки яким обраний профіль захищеності та достатній захист Новопавлівської сільської ради буде реалізовано.

У третьому розділі були проведені розрахунки показників, за допомогою яких можна обґрунтувати техніко-економічну доцільність впровадження КСЗІ та термін її окупності в майбутньому.

Третій розділ містить в собі розрахунки витрат на заходи програмно-організаційного рівня та їх економічна доцільність у вигляді показника ROSI, що становить 0,48 гривні додаткового прибутку та терміну окупності в 2,08 роки, або 25 місяців. Рішення є економічно доцільним для Новопавлівської сільської ради та, окрім того забезпечує її кращим захистом від витоку конфіденційної інформації та втрати даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України «Про інформацію» від 02.10.1992 No2657-XII // Відомості Верховної Ради України-1992-No 48. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

2. Закон України «Про захист персональних даних» від 01.06.2010 No 2297-VI // Відомості Верховної Ради України-2010-No 5. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 No80-VI // Відомості Верховної Ради України-1994-No 80. [Електронний ресурс] Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

4. НД ТЗІ 1.6-005 - Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. [Чинний від 15.04.2013] - К.: ДССЗЗІ, 2013-No125 (Нормативний документ системи технічного захисту інформації).

5. ПОРЯДОК оновлення антивірусних програмних засобів, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації від 26.03.2007 № 45. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0320-07#n12.

6. Перелік відповідно до п. 17 Положення про технічний захист інформації в Україні від 27 вересня 1999 р. № 1229. [Електронний ресурс] Режим доступу до ресурсу: https://cip.gov.ua/ua/news/zasobi-tzi-yaki-mayut-ekspertnii-visnovok-pro-vidpovidnist-do-vimog-tekhnichnogo-zakhistu-informaciyi.

7. НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. [Чинний від 08.11.2005] - К.: ДССЗЗІ, 2005- No125(Нормативний документ системи технічного захисту інформації).

8. НД ТЗІ 2.5-004-99 - Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999- No22 (Нормативний документ системи технічного захисту інформації).

9. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. [Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації).

10. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. [Чинний від 28.04.1999] - К.: ДСТСЗІ СБУ, 1999-No22 (Нормативний документ системи технічного захисту інформації).

11. ПОРЯДОК реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі затверджений ПКМУ від 04.04.2023 № 299. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#n12.

12. Методичні рекомендації до виконання дипломних робіт (проєктів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / О.Ю. Гусєв, О.В. Герасіна, О.М. Алексеев, О.В. Кручинін Дніпро: НГУ, 2018-52.

13. Методичні вказівки до виконання економічної частини дипломного проєкту /Упорядн. Д. П. Пілова. Дніпро: Національний технічний університет «Дніпровська політехніка», 2019.

14. Правильний підбір джерела безперебійного живлення. [Електронний ресурс] Режим доступу: http://www.esludger.com.ua/uk/yak-vybraty-dbzh-pidbir-dzherela-bezperebiinoho-zhyvlennia.html.

15. Умовні позначення основних типів меблів та сантехніки. [Електронний ресурс] Режим доступу: https://studfile.net/preview/5193683/page:24/.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	34	
6	А4	2 Розділ	13	
7	А4	3 Розділ	13	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	2	

ДОДАТОК Б. Перелік документів на оптичному носії

Пояснювальна_записка_Коротун.docx
Пояснювальна_записка_Коротун.pdf
Презентація_Коротун.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 90 б. («відмінно»).

Керівник розділу _____ Дар'я ПІЛОВА
(підпис) (ім'я, призвіще)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
«Комплексна система захисту інформації інформаційно-комунікаційної системи Новопавлівської сільської ради»
студента групи 125-20-3
Коротуна Сергія Володимировича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 78 сторінці та містить 19 рисунків, 23 таблиці, 15 джерел та 4 додатків.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІКС Новопавлівської сільської ради.

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 ІКС, розробка моделі порушника та моделі загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано матрицю розмежування доступу, розроблені елементи положення політики безпеки. Розроблені проектні рішення: регулювання використання стороннього програмного забезпечення, захисту від атак на відмову в обслуговуванні, впровадження антивірусного програмного забезпечення та реалізації резервного електроживлення.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей Новопавлівської сільської ради.

До недоліків відноситься недостатньо обґрунтовані модель загроз та профіль захищеності, а також окремі елементи запропонованих рішень.

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

За час дипломування Коротун С.В. проявив себе фахівцем, здатним достатньо самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

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

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи, професор Корнієнко В.І.

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