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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Карякіна Євгена Андрійовича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи "Управління праці та соціального захисту населення міста Новомосковська"*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	професор Корнієнко В.І.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер				

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Карякіну Євгену Андрійовичу* **академічної групи** *125-17-2*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи "Управління праці та соціального захисту населення міста Новомоскоська"*

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-С

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання, постановка задачі, обстеження, модель загроз, модель порушника	03.05.2021-16.05.2021
Розділ 2	Вибір профілю захищеності, елементи політики безпеки, введення посади адміністратора безпеки, контроль друку на принтерах	17.05.2021-24.05.2021
Розділ 3	Техніко-економічне обґрунтування доцільності запровадження запропонованих рішень, впровадження джерела безперебійного живлення	25.05.2021-31.05.2021

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

Дата видачі: 08.01.2021 р.

Дата подання до екзаменаційної комісії: 11.06.2021

Прийнято до виконання _____ Карякін Є. А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 75 с., 6 рис., 11 табл., 6 додатків, 17 джерел.

Об’єкт розробки: інформаційно-телекомунікаційна система "Управління праці та соціального захисту населення міста Новомосковська".

Предмет розробки: комплексна система захисту інформації інформаційно-телекомунікаційної системи "Управління праці та соціального захисту населення міста Новомосковська".

Мета роботи: підвищення рівня захищеності інформації в ІТС державної установи "Управління праці та соціального захисту населення міста Новомосковська".

У першому розділі кваліфікаційної роботи наведено результати обстеження ОІД, в ході якого було проаналізовано фізичне середовище, обчислювальна система, середовище користувачів, інформація і технологія її обробки. Також було побудовано модель порушника і модель загроз.

У другому розділі обрано профіль захищеності. На основі моделей загроз та порушника було запропоновано елементи політики безпеки, програмне забезпечення для контролю друку та систему безперебійного живлення.

В третьому розділі було виконано розрахунки, щодо економічної доцільності використання запропонованих рішень з ІБ.

Результат проведених робіт може бути використаний для побудови комплексної системи захисту інформації "Управління праці та соціального захисту населення міста Новомосковська".

Практичне значення кваліфікаціної роботи полягає у створенні комплексу захисту інформації для «Управління праці та соціального захисту населення міста Новомосковська».

ІНФОРМАЦІЙНА БЕЗПЕКА, ПОЛІТИКА БЕЗПЕКИ, ПЕРСОНАЛЬНІ ДАНІ, ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕННОСТІ

РЕФЕРАТ

Пояснительная записка: 75 с., 6 рис., 11 табл., 6 приложений, 17 источников.

Объект разработки: информационно-телекоммуникационная система "Управление труда и социальной защиты населения города Новомосковска».

Предмет разработки: комплексная система защиты информации информационно-телекоммуникационной системы "Управление труда и социальной защиты населения города Новомосковска».

Цель работы: повышение уровня защищенности информации в ИТС государственного учреждения "Управление труда и социальной защиты населения города Новомосковска».

В первом разделе квалификационной работы приведены результаты обследования ОИД, в ходе которого были проанализированы физическая среда, вычислительная система, среда пользователей, информация и технология ее обработки. Также была построена модель нарушителя и модель угроз.

Во втором разделе избран профиль защищенности. На основе моделей угроз и нарушителя было предложено элементы политики безопасности, программное обеспечение для контроля печати и систему бесперебойного питания.

В третьем разделе были выполнены расчеты, экономической целесообразности использования предложенных решений по ИБ.

Результат проведенных работ может быть использован для построения комплексной системы защиты информации "Управление труда и социальной защиты населения города Новомосковска».

Практическое значение квалификацинои работы заключается в создании комплекса защиты информации для для «Управление труда и социальной защиты населения города Новомосковска».

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПОЛИТИКА БЕЗОПАСНОСТИ, ПЕРСОНАЛЬНІЕ ДАННЫЕ, ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ ЗАЩИЩЁННОСТИ

ABSTRACT

Explanatory note: 75 p., 6 drawins, 11 tables, 6 annexes, 17 sources.

Object of development: information and telecommunication system "Department of labor and social protection of the population of the city of Novomoskovsk".

Subject of development: a comprehensive information protection system of the information and telecommunication system "Department of Labor and Social Protection of the Population of the City of Novomoskovsk".

Purpose of work: increasing the level of information security in the ITS of the state institution "Office of Labor and Social Protection of the Population of the City of Novomoskovsk".

In the first section of the qualification work, the results of the OID survey are presented, during which the physical environment, the computing system, the user environment, information and the technology of its processing were analyzed. A model of the intruder and a model of threats were also built.

In the second section, a security profile is selected. Based on threat and intruder models, security policy elements, print control software, and an uninterruptible power system were proposed.

In the third section, calculations were made on the economic feasibility of using the proposed solutions for information security.

The result of the work carried out can be used to build an integrated information security system "Department of Labor and Social Protection of the Population of the City of Novomoskovsk".

The practical importance of qualification work is to create a complex of information protection for the "Department of Labor and Social Protection of the Population of the City of Novomoskovsk."

INFORMATION SECURITY, SECURITY POLICY, PERSONAL DATA, FUNCTIONAL SECURITY PROFILE

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІзОД – інформація з обмеженим доступом;

КСЗІ – комплексна система захисту інформації;

ОІД – об’єкт інформаційної діяльності;

НД ТЗІ – нормативний документ технічного захисту інформації;

АС – автоматизована система;

КЗ – контрольована зона;

КС – комп’ютерна система;

УПСЗН – управління праці та соціального захисту населення;

КЗЗ – комплекс засобів захисту;

ПК – програмний комплекс;

ЕЦП – електронно-цифровий підпис;

АБ – адміністратор безпеки;

ІБ – інформаційна безпека;

АКБ – акумуляторна батарея.

ЗМІСТ

ВСТУП

Способи обробки та зберігання інформації, на сьогоднішній день, направлені на швидкість роботи та простоту взаємодії користувача з обчислювальною системою. Проте підвищується складність реалізації таких інформаційно-обчислювальних систем. Окрім інформації з обмеженим доступом, яка належить державі, та комерційної таємниці, захисту від несанкціонованого доступу потребують персональні дані громадян.

Персональні дані кожної людини використовуються щодня. Для забезпечення захисту персональних даних в системі, необхідно проаналізувати особливості обробки та зберігання інформації. Після чого, потрібно розробити комплексну систему захисту інформацію для запобігання загрозам. Загроза – це множина умов і факторів, які створюють актуальну небезпеку несанкціонованого, в тому числі випадкового, доступу до персональних даних при їх обробці в інформаційній системі, результатом якого можуть бути знищення, модифікація, копіювання, розповсюдження цих даних, а також інші неправомірні дії.

Метою кваліфікаційної роботи є аналіз захищеності інформації з обмеженим доступом та розробка комплексної системи захисту інформації в «Управлінні праці та соціального захисту населення міста Новомосковськ», яка буде відповідати вимогам щодо захисту персональних даних відповідно до чинного законодавства.

Для вирішення поставлених проблем у кваліфікаційній роботі запропоновано наступні дії:

- провести обстеження об’єкта інформаційної діяльності;
- розробити модель порушника;
- виконати аналіз актуальних загроз для інформації з обмеженим доступом;
- сформувати вимоги до захисту ІзОД;

- проаналізувати існуючий стан захисту інформації з обмеженим доступом та розробити рекомендації для створення комплексної системи захисту інформації.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про об’єкт інформаційної діяльності

Назва об’єкта «Управління праці та соціального захисту населення міста Новомосковська».

Сфера діяльності включає управління здійснює керівництво у сфері соціального забезпечення населення та соціального захисту пенсіонерів, інвалідів, одиноких непрацездатних громадян, дітей-сиріт, одиноких матерів, багатодітних, а також малозабезпечених сімей з дітьми, інших соціально незахищених громадян, які потребують допомоги і соціальної підтримки з боку держави.

Форма власності державна власність.

Організаційно-правова форма орган виконавчої влади.

Адреса розташування 51200, Дніпропетровська область, місто Новомосковськ, вулиця Горького 2а.

Організаційна структура управління:

- Керівництво:
    1) Начальник управління.
    2) Заступник начальника управління.
- Системний адміністратор.
- Відділ планування, бухгалтерського обліку, звітності та фінансового забезпечення:
    1) Головний бухгалтер.
    2) Бухгалтери.
- Відділ обслуговування інвалідів та ветеранів:
    1) Головний консультант з питань соцзахисту недієздатних громадян.
    2) Консультант з питань соцзахисту недієздатних громадян.
- Відділ прийняття рішень:
    1) Провідний радник.

2) Консультант з фінансів.

- Відділ прийому громадян:

1) Консультанти громадян.

1.2 Обстеження ОІД

1.2.1 Фізичне середовище

Інформація щодо підприємства була змінена за вимогою власника інформаційно-телекомунікаційної системи, з метою забезпечення конфіденційності інформації.

ОІД розташований на першому поверсі жилої будівлі, яка має 9 поверхів. До будівлі примикає одноповерхове приміщення спортивного залу «Атлет». Границя контрольованої зони обмежена стінами приміщення ОІД. Північна стіна є внутрішньою, інші – зовнішні. Зі сходу від ОІД проходить вулиця Паланочна. Приміщення має 10 вікон, на вікнах встановлені залізні грати із зовнішньої сторони.

Єдиний вхід до «Управління праці та соціального захисту населення міста Новомосковська» (далі УПСЗН) знаходиться з західної сторони.

Охорону ОІД забезпечує охоронна служба «Гуард». Охоронця, який міг би бути присутній на об'єкті, немає. Сигналізація централізована. В якості лінії зв'язку виступає телефонна лінія, яка проходить на південь по стовпам вздовж вулиці Паланочна до пульту централізованого спостереження «Гуард».

Відкриває та закриває приміщення на початку та в кінці робочого дня начальник управління, він вмикає та вимикає сигналізацію.

Зі східної сторони по іншу сторону вулиці на відстані 25 м від ОІД знаходиться каналізаційний люк. Каналізаційна труба приходить в будинок під землею зі східної сторони та заходить у підвальне приміщення будівлі.

До будівлі підведено централізоване водопостачання підземним шляхом; оглядовий колодязь знаходиться на сході в 20 метрах від споруди. Труби водопостачання заходять у підвальне приміщення будівлі.

Електропостачання здійснюється підземною лінією передачі від трансформаторної підстанції № 232, яка знаходиться на півдні в 30 м від споруди. До трансформаторної підстанції також підключенні інші будівлі (будівля 2 і 3 на рисунку 1.1). Перелік усіх сусідніх будівель, що розташовані поблизу будівлі, в якій розташований ОІД, наведено у таблиці 1.1.

«Вита пара» від провайдера для виходу в мережу Інтернет входить у будівлю крізь отвір у стіні зі східної сторони. До будівлі кабель провайдера підходить по стовпам від щитка провайдера, який закріплений на стовпі на півдні від ОІД в 20 метрах. Живлення лінії зв'язку провайдера здійснюється від трансформаторної підстанції розташованої через одну паралельну вулицю на сході від ОІД, якщо там відсутнє електропостачання у зв'язку з технічними роботами, то інтернет на ОІД не працює.

Режим роботи УПСЗН :

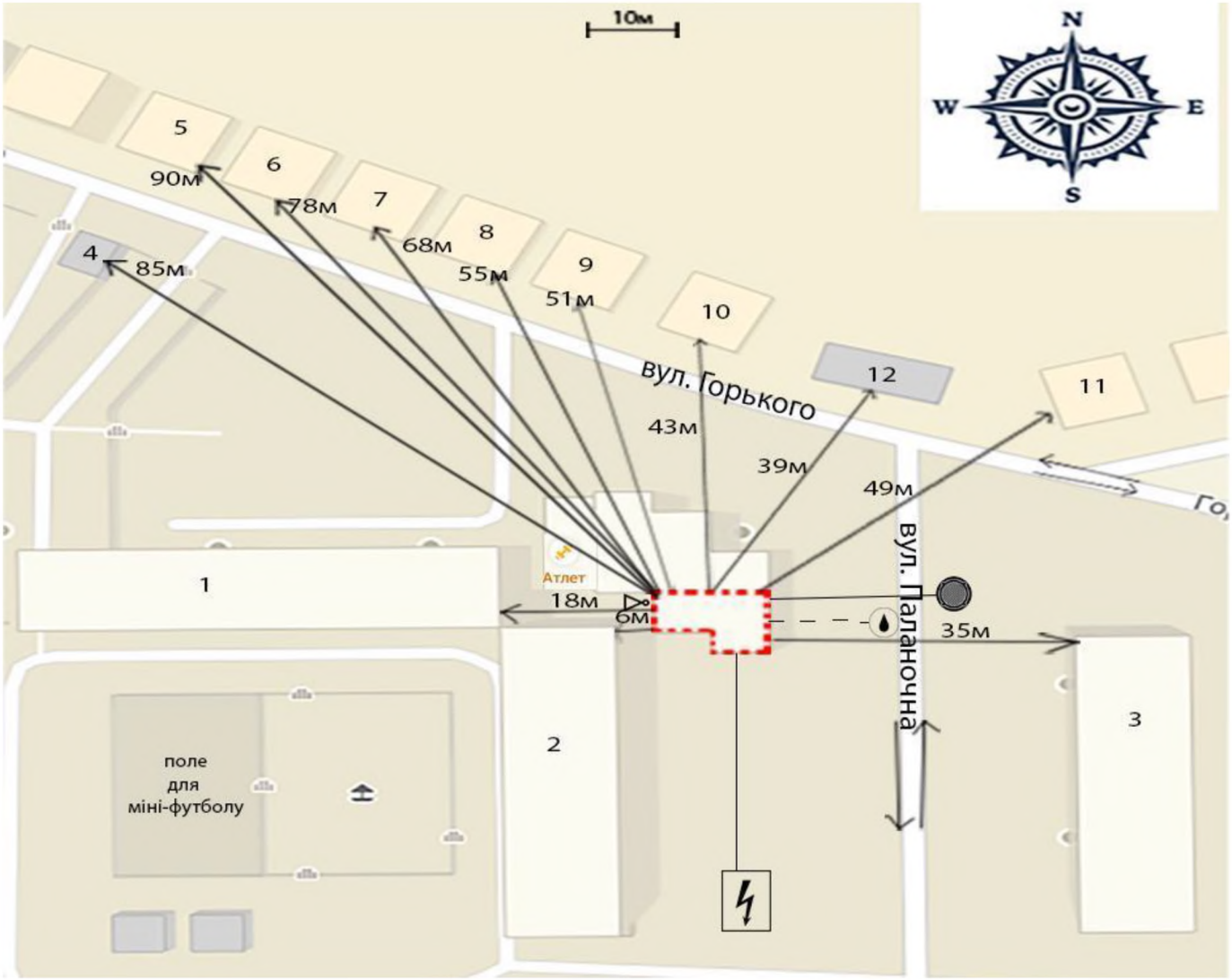
Субота	Зачинено
Неділя	Зачинено
Понеділок	08:00–17:00
Вівторок	08:00–17:00
Середа	08:00–17:00
Четверг	Зачинено
П'ятница	08:00–17:00

Таблиця 1.1 – Будівлі на ситуаційному плані

Найменування	Кількість поверхів	Адреса	Відстань до ОІД (м)
Житловий будинок 1	9	вулиця Горького буд. 2	18
Житловий будинок 2	9	вулиця Горького буд. 3	6
Житловий будинок 3	9	вулиця Горького буд. 4	35
Гараж 1	1	-	85
Приватний будинок 4	1	вулиця Горького буд. 5	90
Приватний будинок 5	1	вулиця Горького буд. 7	78
Приватний будинок 6	1	вулиця Горького буд. 9	68
Приватний будинок 7	1	вулиця Горького буд. 11	55
Приватний будинок 8	1	вулиця Горького буд. 13	51

Продовження таблиці 1.1

Найменування	Кількість поверхів	Адреса	Відстань до ОІД, м
Приватний будинок 9	1	Вулиця Горького буд. 15	43
Приватний будинок 10	1	вулиця Горького буд. 17	39
Гараж 2	1	-	49



Умовні позначення:

- границя контрольованої зони
- напрям руху
- оглядовий колодязь лінії канадізації
- головний вхід ОІД
- трансформаторна підстанція №232
- дитячий майданчик
- оглядовий колодязь лінії водопостачання

Рисунок 1.1 – Ситуаційний план

1.2.2 Обчислювальна система

В кабінеті начальника знаходиться сейф, у якому зберігаються паперові копії бухгалтерських висновків щодо надання компенсацій громадянам. До кабінету директора ніхто не може потрапити, крім самого директора, співробітники УПСЗН можуть увійти до кабінету тільки у присутності начальника. Контрольований режим доступу до кабінету начальника забезпечується залізними дверима із врізаним ригельним замком, ключ від якого є лише у начальника управління.

До кімнати, де знаходиться сервер, може потрапити лише системний адміністратор, начальник управління та його заступник. Доступ до кімнати з сервером обмежують двері з врізаним циліндричним замком, ключі від якого є у начальника та заступника начальника управління. Кімната постійно зачинена, робота з сервером здійснюється дистанційно. Для отримання фізичного доступу до сервера, системний адміністратор звертається до начальника або його заступника, вказує причину, чому йому необхідно потрапити до кімнати, у разі схвалення цього питання одного з керівників, отримує ключі від серверної.

Прилади безперебійного живлення відсутні на ОІД. Перелік усіх технічних засобів наведено у таблиці 1.2. Розташування технічних засобів на території ОІД зображено на рисунку 1.2.

У робочий час, доступ до всіх інших кімнат необмежений; громадяни можуть вільно звертатися зі своїми питаннями до спеціалістів усіх відділів.

Усі комп'ютери підключені до switch за допомогою розеток RJ45. Виходи усіх розеток ведуть у серверну кімнату, де розташований switch, загальна структурна схема з'єднання технічних засобів зображена на рисунку 1.3.

На поверху розміщена електрощитова до якої підключена зовнішня лінія енергопостачання, від якої в свою чергу використовується живлення розеток та системи освітлення.

Підключення зовнішніх носіїв до робочих ПК ніяк не контролюється. Правила друку щодо кількості копій не регламентуються.

Таблиця 1.2 – Технічні засоби обробки інформації

Найменування	Призначення	Де встановлено	Відстань до границі КЗ, м
Системний блок 1	Основне	Кабінет начальника	1
Монітор 1	Основне		1.3
Принтер 1	Основне		1
Клавіатура 1	Основне		1
Комп'ютерна миша 1	Допоміжне		1.5
Системний блок 2	Основне	Відділ прийняття рішень	1.5
Монітор 2	Основне		1.8
Принтер 2	Основне		1.5
Клавіатура 2	Основне		1.8
Системний блок 3	Основне		1.5
Монітор 3	Основне		1.8
Клавіатура 3	Основне		1.5
Комп'ютерна миша 3	Допоміжне		1.8

Продовження таблиці 1.2

Найменування	Призначення	Де встановлено	Відстань до границі КЗ
Системний блок 4	Основне	Бухгалтерія	3
Монітор 4	Основне		3.2
Клавіатура 4	Основне		3.2
Комп'ютерна миша 4	Допоміжне		3.2
Системний блок 5	Основне		1,5
Монітор 5	Основне		1,5
Клавіатура 5	Основне		1,5
Комп'ютерна миша 5	Допоміжне		1,5
Системний блок 6	Основне		1
Монітор 6	Основне		1,2
Клавіатура 6	Основне		1
Комп'ютерна миша 6	Допоміжне		1
Принтер 2	Основне		1,5

Продовження таблиці 1.2

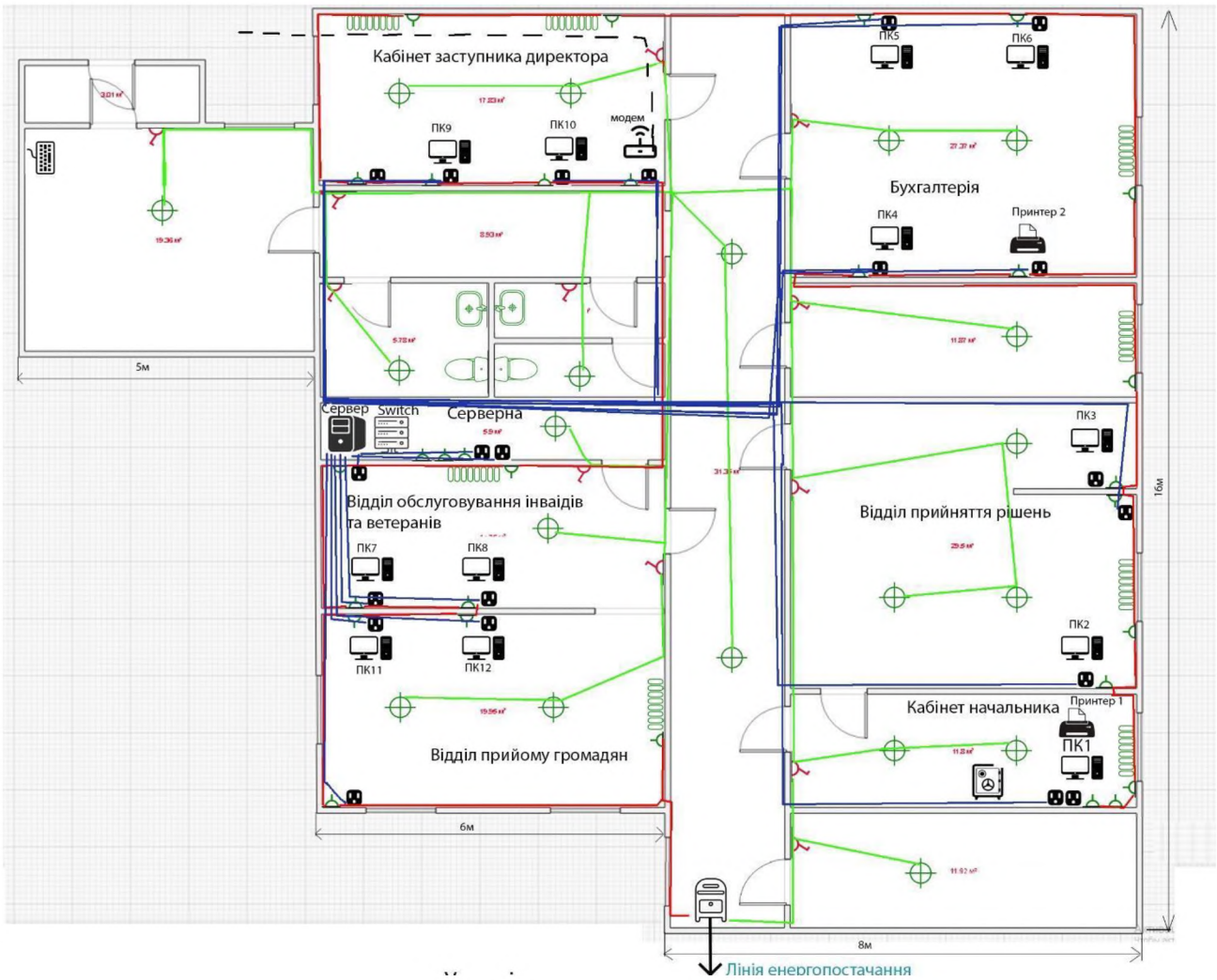
Найменування	Призначення	Де встановлено	Відстань до границі КЗ, м
Системний блок 7	Основне	Відділ обслуговування інвалідів та ветеранів	1
Монітор 7	Основне		1,2
Клавіатура 7	Основне		1
Комп'ютерна миша 7	Допоміжне		1,3
Системний блок 8	Основне		2,5
Монітор 8	Основне		2,5
Клавіатура 8	Основне		2,7
Комп'ютерна миша 8	Допоміжне		2,5
Системний блок 9	Основне	Кабінет заступника директора	1,5
Монітор 9	Основне		1,5
Клавіатура 9	Основне		1,7
Комп'ютерна миша 9	Допоміжне		1,7
Системний блок 10	Основне		2,5

Продовження таблиці 1.2

Найменування	Призначення	Де встановлено	Відстань до границі КЗ, м
Монітор 10	Основне	Кабінет заступника директора	2,5
Клавіатура 10	Основне		2,5
Комп'ютерна миша 10	Допоміжне		2,5
Модем	Основне		2,8
Системний блок 11	Основне	Відділ обслуговування інвалідів та ветеранів	1
Монітор 11	Основне	Відділ прийому громадян	1,2
Клавіатура 11	Основне		1
Комп'ютерна миша 11	Допоміжне		1,3
Системний блок 12	Основне		2,5
Монітор 12	Основне		2,5
Клавіатура 12	Основне		2,7

Продовження таблиці 1.2

Найменування	Призначення	Де встановлено	Відстань до границі КЗ, м
Комп'ютерна миша 12	Допоміжне		2,5
Сервер	Основне	Серверна кімната	0,5
Switch	Основне		0,5
Магніто-контакний датчик	Допоміжне	На всіх вікнах та вхідних дверях	0,04
ПКП	Допоміжне	коридор	0.4



Умовні позначення

- електрорадиатор
- раковина
-унитаз
- ПК
-принтер
- сервер
- switch
- модем
-розетка
- розетка RJ45
- світодиодна лампа
- вимикач совітлювальної системи
- сейф
- електропостачання розеток
- електрощитова
- «вита пара» від провайдера
- ПКП

Рисунок 1.2 – Генеральний план

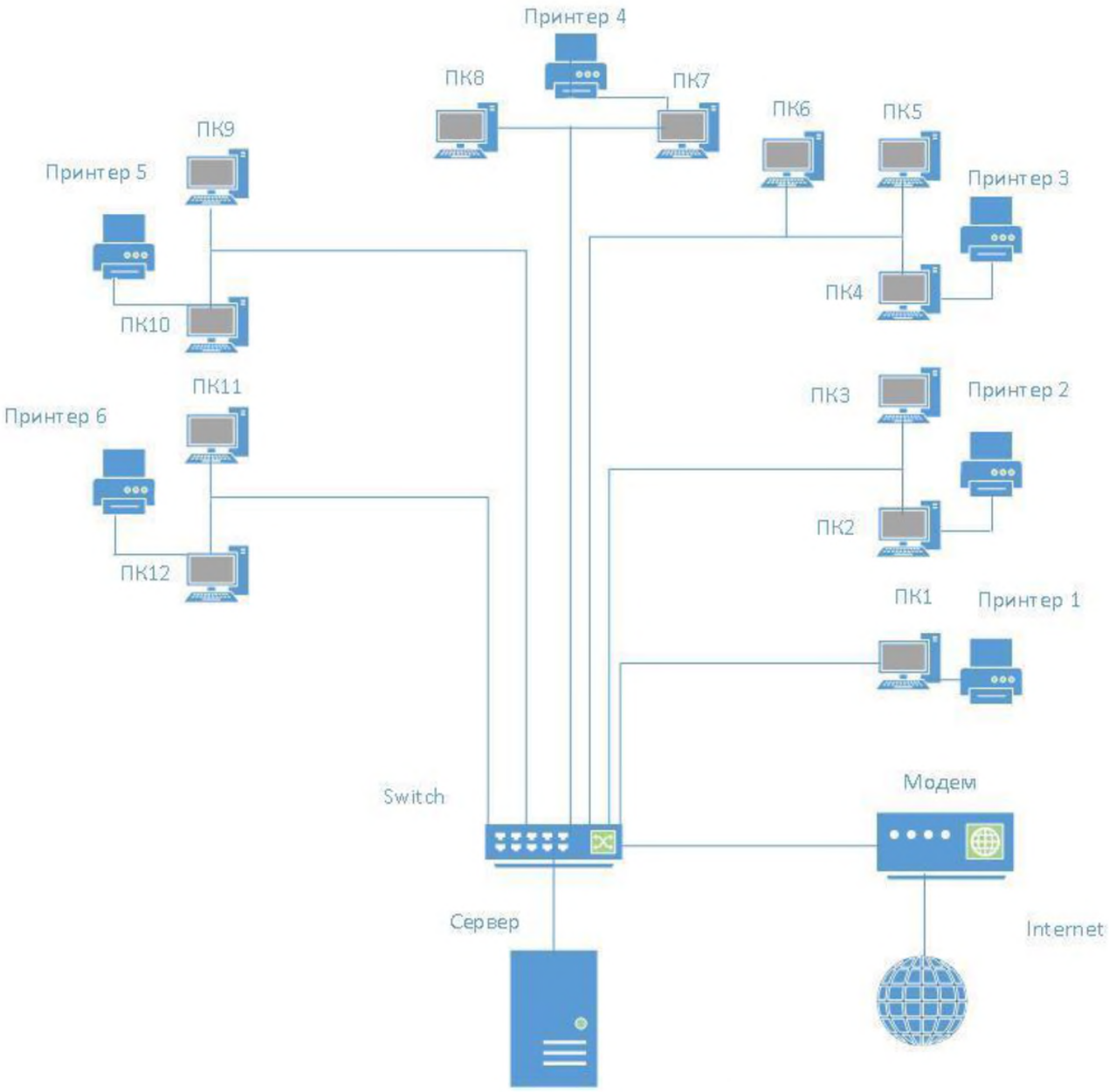


Рисунок 1.3 – Загальна структурна схема обчислювальної системи

Таблиця 1.3 – Основні технічні засоби

Ім'я в ІТС	Особливості конфігурації	Серійний номер	Відділ
ПК 1	AMD Ryzen 3 3200G 3.6 - 4GHz Samsung 8GB (4GBx2) DDR4 2666 MHz Asus PRIME A320M-K Western Digital Blue 1TB 5400rpm Seasonic SSP-300TBS 300W	L825D011 A321O454 FD123094 12R43524 RE439345	Кабінет начальника
Принтер 1	Модель HP DeskJet 2720 Швидкість чорно-білого друку 7.5 стр/хв Швидкість кольорового друку 5.5 стр./хв.	RT234232	

Продовження таблиці 1.3

Ім’я в ІТС	Особливості конфігурації	Серійний номер	Відділ
ПК 2	Intel 4-core Celeron J1900 2.0-2.42GHz SSD - Crucial BX500 240GB 2.5" AVIS PC3-12800 DDR3-1600 8Gb Seasonic SSP-300TBS 300W	SF125474 432654738 905434523 4584524FT	Відділ прийняття рішень
ПК 3	Intel 4-core Celeron J1900 2.0-2.42GHz SSD Crucial BX500 240GB 2.5" AVIS PC3-12800 DDR3-1600 4Gb Seasonic SSP-300TBS 300W	GR25F658 098475758 H325R234 098436574	
ПК 4	Intel 4-core Celeron J1900 2.0-2.42GHz Kingston SSD HyperX Fury 3D 120GB 2.5" ОЗУ Patriot DDR3 4GB 1600Mhz Seasonic SSP-300TBS 300W	L825D011 A321O454 FD123094 12R43524	Бухгалтерія

Продовження таблиці 1.3

Ім’я в ІТС	Особливості конфігурації	Серійний номер	Відділ
ПК 5	Intel 4-core Celeron J1900 2.0-2.42GHz Kingston SSD HyperX Fury 3D 120GB 2.5" ОЗУ Patriot DDR3 4GB 1600Mhz Seasonic SSP-300TBS 300W	RE439345 H325R234 098436574 KR232576	
ПК 6	Intel 4-core Celeron J1900 2.0-2.42GHz Kingston SSD HyperX Fury 3D 120GB 2.5" ОЗУ Patriot DDR3 4GB 1600Mhz Seasonic SSP-300TBS 300W	SF125474 432654738 905434523 4584524FT	
Принтер 2	Модель Canon i-Sensys MF3010 Швидкість друку 18стр/хв Колір друку тільки чорно-білий	YE43U324	

Продовження таблиці 1.3

Ім'я в ІТС	Особливості конфігурації	Серійний номер	Відділ
ПК 7	Intel Core 2 Extreme X6800 (LGA775, 2.93GHz, 4MB L2) ASUS P5W DH Deluxe (LGA775, Intel 975X Express) Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) PowerColor X1900 XTX 512MB (PCI-E x16) Maxtor MaXLine III 250GB (SATA150)	Hdu293847 Y4873972 892734092 23423489 AF4823422	Відділ обслуговування інвалідів та ветеранів
ПК 8	Intel Core 2 Extreme X6800 (LGA775, 2.93GHz, 4MB L2) ASUS P5W DH Deluxe (LGA775, Intel 975X Express) Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) PowerColor X1900 XTX 512MB (PCI-E x16) Maxtor MaXLine III 250GB (SATA150)	AB152353 OP-34052 IJ2342133 U8579234	

Продовження таблиці 1.3

Ім'я в ІТС	Особливості конфігурації	Серійний номер	Відділ
ПК 9	Intel Core 2 Extreme X6800 (LGA775, 2.93GHz, 4MB L2) ASUS P5W DH Deluxe (LGA775, Intel 975X Express) Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) PowerColor X1900 XTX 512MB (PCI-E x16) Maxtor MaXLine III 250GB (SATA150)	KJ239048 2342k234 234kjh234 234234234 KR541564	Кабінет заступника директора
ПК 10	Intel Core 2 Extreme X6800 (LGA775, 2.93GHz, 4MB L2) ASUS P5W DH Deluxe (LGA775, Intel 975X Express) Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) PowerColor X1900 XTX 512MB (PCI-E x16) Maxtor MaXLine III 250GB (SATA150)	82934dsf 982374982 9823749 9823741094 OP546123	

Продовження таблиці 1.3

Ім'я в ІТС	Особливості конфігурації	Серійний номер	Відділ
Модем	D-LINK DSL-500T	Uj0982384	
ПК 11	Intel Core 2 Duo E7300 2x2.66GHz HDD Seagate 3.5\ 500Gb 5400 rpm Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) Chieftec 300W (GPA-600S)	987234jk23 23489kj23 Kj324234 Sd23423424	Відділ прийому громадян
ПК 12	Intel Core 2 Duo E7300 2x2.66GHz HDD Seagate 3.5\ 500Gb 5400 rpm Corsair TWIN2X2048-8500C5 (DDR2-1067, 2 x 1024 MB, 5-5-5-15) Chieftec 300W (GPA-600S)	JF234234 SA1231235 O532234 RE123OP	
Модем	D-LINK DSL-500T	FD1023534	
Switch	PowerConnect 6248	KD213423	Серверна кімната

Продовження таблиці 1.3

Ім’я в ІТС	Особливості конфігурації	Серійний номер	Відділ
Сервер	Сервер Dell PowerEdge R510: - 2 x Intel Xeon 5506 сокет LGA1366; - Patriot DDR3 128GB 1600Mhz; - Western Digital Blue 500GB 5400rpm 16MB; - Western Digital Blue 500GB 5400rpm 16MB; - Western Digital Blue 500GB 5400rpm 16MB ; - Блок живлення: HP 300 Вт 830272-B21; Hp Tft7600 Kvm Console	PA12352398 VB234786P KD546221W KD561237L KD897456H PL54632514 KE4567841	

Таблиця 1.4 – Програмне забезпечення

Найменування	Тип програмного забезпечення	Де встановлена	Тип ліцензії	Дата дії ліценції
Док Проф 2.0	Спеціалізоване	ПК1 – ПК12, Сервер	Commercial	довічно
СОНАТА	Прикладне	ПК1 - ПК6, Сервер	Commercial	До 15.02.2022
1С:Бухгалтерия	Прикладне	ПК4-ПК6	Commercial	довічно
“Крипто Автограф”	спеціалізоване	ПК2-ПК12, сервер	Commercial	довічно
MS Word 2010	прикладне	ПК1-ПК12, сервер	Commercial	довічно
Windows 10 Home	системне	ПК1, ПК9	Commercial	довічно
Windows XP	системне	ПК2, ПК3, ПК4, ПК5, ПК6, ПК7, ПК8, ПК11, ПК12	Commercial	довічно
Windows Server 2008	системне	ПК10, сервер	Commercial	довічно

1.2.3 Інформація і технологія її обробки

На ОІД циркулює відкрита інформація та інформація з обмеженим доступом. В роботі розглянуто наступну інформацію з обмеженим доступом:

- декларація про доходи і витрати осіб – містить в собі персональні дані (ПІБ, номер та серія паспорта, місце проживання, ідентифікаційний номер фізичної особи, інформація про доходи);
- запит до податкової інспекції;
- довідка про доходи від податкової інспекції;
- бухгалтерський висновок.

Детальна класифікація інформації, яка обробляється в управлінні наведено в таблиці 1.4, а її кругообіг в АС наведено на рисунку 1.4.

Клієнти закладу заповнюють декларацію про доходи у паперовому вигляді. Завжди робиться копія декларації в електронному вигляді. Працівники у свою чергу формують запит до податкової інспекції, у якому використовують дані надані клієнтом. Запит здійснюється з використанням програмного комплексу Соната, дані вводяться з клавіатури. Також для здійснення запиту використовується електронно-цифровий підпис, який генерується у програмі «Крипто Автограф». Увесь документообіг здійснюється за допомогою Док Проф 2.0. Потім запит відправляється електронною поштою до податкової інспекції. Інспекція, в свою чергу, надсилає у відповідь на запит довідку про доходи громадянина. Ця довідка передається до бухгалтерського відділу, на її основі здійснюється розрахунок щодо доцільності та розміру нарахувань субсидії для громадянина. Паперові копії щодо нарахувань субсидій для громадян зберігаються у сейфі начальника управління, також він може переглядати їх в електронному вигляді.

Таблиця 1.4 – Інформація з обмеженим доступ, що циркулює на ОІД

Найменування	Вид представлення інформації в ІТС	Місце зберігання та/або обробки	Правовий режим	Вимоги до властивостей інформації		
				К	Ц	Д
Декларація про доходи і витрати осіб	Паперовий, електронний	ПК2-ПК12 Сервер Шухляди стола у відділі прийому громадян та відділі обслуговування інвалідів та ветеранів	Конфіденційна	3	2	2

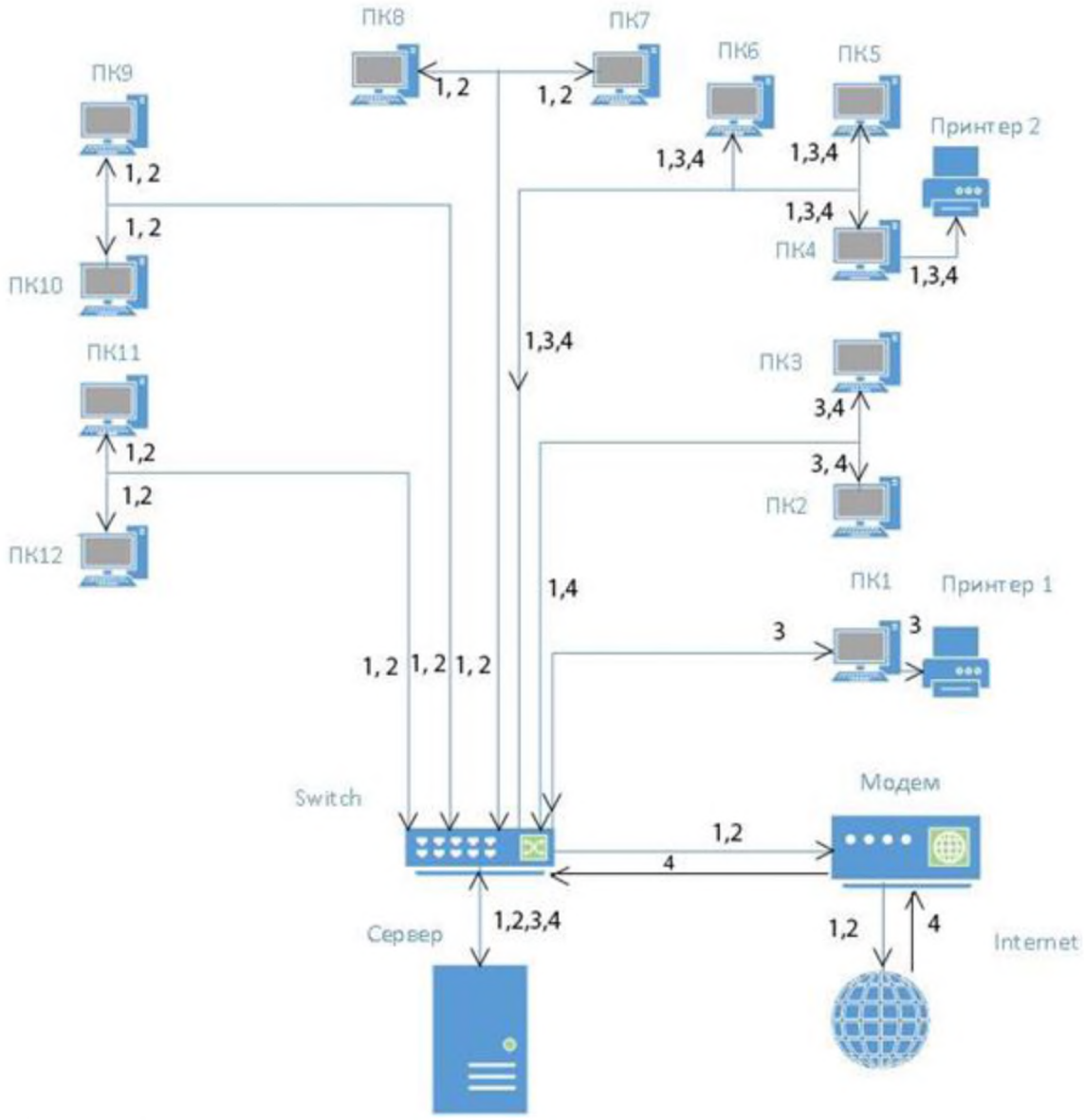
Продовження таблиці 1.4

Найменування	Вид представлення інформації в ІТС	Місце зберігання та/або обробки	Правовий режим	Вимоги до властивостей інформації		
				К	Ц	Д
Запит про доходи до податкової інспекції	електронний	ПК1, ПК4-ПК6, Принтер1, Принтер3, Сервер	Службова	2	2	1
Довідка про доходи від податкової інспекції	електронний	ПК4-ПК6, Принтер 3, сервер	Службова	2	2	1
Бухгалтерський висновок щодо надання субсидії	Електронний, паперовий	Сервер, ПК2-ПК6, Принтер1, Принтер2	Конфіденційна	2	2	2

К1/Ц1/Д1 – рівень властивостей, при якому організація не зазнає фінансових збитків та втрат відносно репутації, у разі їх порушення.

К2/Ц2/Д2 – рівень властивостей, при якому організація може понести незначні фінансові збитки.

К3/Ц3/Ц4 – рівень властивостей, при якому організація може понести суттєві матеріальні збитки та значне погіршення репутації.



Умовні позначення:

1– декларація про доходи і витрати осіб;

2 – запит про доході до податкової інспекції;

3 – бухгалтерський висновок щодо надання субсидій;

4 – довідка про доходи від податкової інспекції.

Рисунок 1.4 – Схема інформаційних потоків

Таблиця 1.5 - Користувачі комп'ютерної системи

Посада	Кваліфікація	Робоче місце	Роль в ІС
Начальник	Професійно володіє програмними комплексами	ПК1	користувач
Заступник начальника	Професійно володіє програмними комплексами	ПК9	користувач
Системний адміністратор	Має глибокі знання з інформаційних систем	ПК10	Системний адміністратор
Головний бухгалтер	Професійно володіє програмними комплексами	ПК4	користувач
Бухгалтер 1	Професійно володіє програмними комплексами	ПК5	користувач
Бухгалтер 2	Професійно володіє програмними комплексами	ПК6	користувач

Продовження таблиці 1.5

Посада	Кваліфікація	Робоче місце	Роль в ІС
Головний консультант з питань соцзахисту недієздатних громадян	Має низьку кваліфікацію	ПК7	користувач
Консультант з питань соцзахисту недієздатних громадян	Має низьку кваліфікацію	ПК8	користувач
Провідний радник	Має низьку кваліфікацію	ПК2	користувач
Консультант з фінансів	Впевнений користувач комп'ютера	ПК3	користувач
Консультант громадян 1	Має низьку кваліфікацію	ПК11	користувач
Консультант громадян 2	Має низьку кваліфікацію	ПК12	користувач

Таблиця 1.6 – Матриця розмежування доступом

Користувачі	Інформація з обмеженим доступом			
	Декларація про доходи і витрати осіб	Запит про доходи до податкової інспекції	Довідка про доходи від податкової інспекції	Бухгалтерський висновок щодо надання субсидії
Начальник	R	R	R	R, P
Заступник начальника	R	R	R	R, P
Системний адміністратор	R, D	R, D	R, D	R, D
Головний бухгалтер	R, P, D	R	R, P	R, W, M, D, P
Бухгалтер 1 Бухгалтер 2	R, W	R, W	R, D	R, W, M, P

Продовження таблиці 1.6

Користувачі	Інформація з обмеженим доступом			
	Декларація про доходи і витрати осіб	Запит про доходи до податкової інспекції	Довідка про доходи від податкової інспекції	Бухгалтерський висновок щодо надання субсидії
Головний консультант з питань соцзахисту недієздатних громадян	R, W, M, D, P	R, W, M	R	R
Консультант з питань соцзахисту недієздатних громадян, провідний радник, консультант з фінансів, консультант громадян 1, консультант громадян 2	R, W, M	R, W, M	R	R

Матриця розмежування доступу наведена в таблиці 1.6, де W – запис, M – модифікація, D – видалення, P – друк.

1.3 Аналіз загроз інформації

1.3.1 Модель порушника

З точки зору наявності права постійного чи разового доступу в контрольовану зону де розміщується ОІД усі фізичні особи можуть бути віднесені до однієї з наступних категорій:

- категорія І - особи, що не мають права доступу в КЗ;
- категорія ІІ - особи, що мають право доступу в КЗ.

Усі потенційні порушники розділяються на:

- зовнішніх порушників, що здійснюють атаки за межами КЗ;
- внутрішні порушники, які здійснюють атаки, знаходячись в межах КЗ.

В якості зовнішнього порушника крім осіб, що відносяться до категорії І повинні розглядатися особи категорії ІІ, що знаходяться за межами КЗ.

У відношенні до ОІД, в якості зовнішнього порушника із числа осіб категорії І можуть виступати:

- колишні співробітники;
- сторонні особи, які намагаються отримати доступ до ІзОД в ініціативному порядку;
- представники злочинних організацій.

Внутрішні порушники можуть поділятися на тих, хто не є зареєстрованими користувачами АС, проте має санкціонований доступ на територію КЗ, і на тих, хто є зареєстрованим користувачем. Останні поділяються за рівнем доступу до оброблюваної інформації.

Таблиця 1.7 - Модель порушника

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Внутрішні порушники						
Начальник управління	М3	К2	З2	Ч2	Д4	13
Заступник начальника управління	М3	К2	З2	Ч2	Д4	13
Системний адміністратор	М3	К3	З3	Ч4	Д4	17
Головний бухгалтер	М3	К2	З2	Ч3	Д2	13
Бухгалтер 1	М2	К2	З2	Ч2	Д2	10
Бухгалтер 2	М2	К2	З2	Ч2	Д2	10
Головний консультант з питань недієздатних громадян	М1	К1	З1	Ч2	Д2	7
Консультант з питань соцзахисту недієздатних громадян	М1	К1	З1	Ч2	Д2	7
Провідний радник	М2	К1	З1	Ч1	Д2	7

Продовження таблиці 1.7

Посада	Мотив порушень	Рівень обізнаності щодо ІТС	Можливості щодо подолання систем захисту	Можливості за часом дії	Можливості за місцем дії	Сума загроз
Консультант з фінансів	М3	К1	З1	Ч2	Д2	9
Консультант громадян 1	М1	К1	З1	Ч1	Д2	6
Консультант громадян 2	М1	К1	З1	Ч1	Д2	6
Зовнішні порушники						
Зловмисник	М3	К3	З3	Ч4	Д3	15

В таблиці 1.7 наведено модель порушника, де М1 – безвідповідальність, М2 – самоствердження, М3 – корисливий інтерес, К1 – володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС, К2 – володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування, К3 – знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості, З1 – може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях, З2 – використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації; З3 – використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації; Ч1 – під час повної бездіяльності ІТС з метою відновлення та ремонту; Ч2 – під час зупинки компонентів ІТС з метою технічного обслуговування та модернізації; Ч3 – під час функціонування ІТС (або

компонентів системи); Ч4 – як у процесі функціонування ІТС, так і під час призупинки компонентів системи; Д1 – усередині приміщень, але без доступу до технічних засобів ІТС; Д2 - з робочих місць користувачів (операторів) ІТС; Д3 – дистанційно; Д4 – з доступом у зону керування засобами забезпечення безпеки ІТС.

З побудованої таблиці 1.7 видно, що найбільшу загрозу становлять системний адміністратор та зовнішній зловмисник. Системний адміністратор має збиткові права в ІТС і його дії в системі ніким не контролюються. Вразливості, якими може скористатися зловмисник будуть розглянуті у моделі загроз.

1.3.2 Модель загроз

Згідно з НД ТЗІ 2.6-001-11, модель загроз має описувати методи та засоби реалізації загрози. Правильно реалізована модель загроз дозволяє виявити існуючі загрози, розробити ефективні контрзаходи, підвищивши тим самим рівень безпеки ІТС та оптимізувати витрати на забезпечення безпеки, сфокусувавшись на самих актуальних загрозах, які у разі їх реалізації, призведуть до найбільшого збитку.

В моделі загроз повинні враховуватися усі актуальні загрози на всіх стадіях їх життєвого циклу (рисунок 1.5).

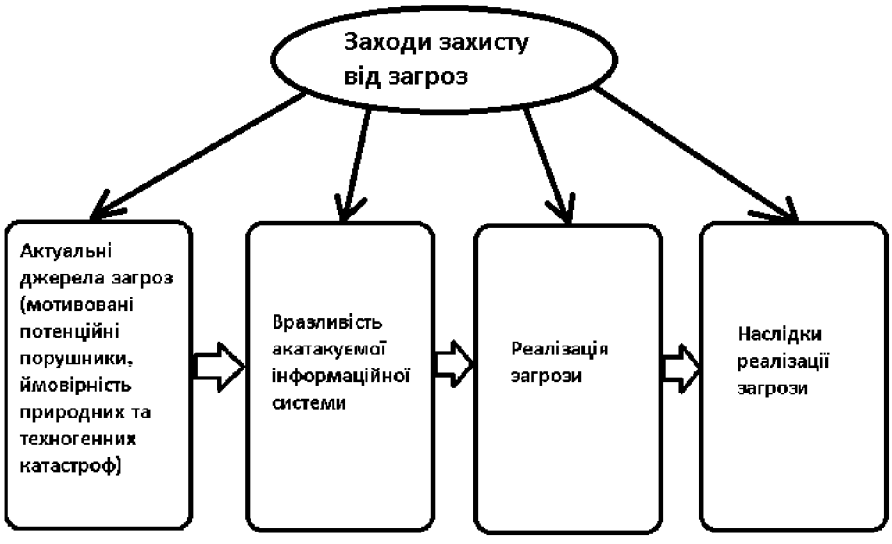


Рисунок 1.5 - Життєвий цикл загроз ІБ

Модель загроз необхідна, щоб керуватися нею на всіх етапах життєвого циклу системи (при проектуванні, в режимі експлуатації, при проведенні регламентних і ремонтно-профілактичних робіт, при модернізації та виводу її з експлуатації).

Модель загроз використовується при вирішенні наступних задач:

- аналіз захищеності від загроз безпеці в ході організації і проведенні робіт з питань інформаційної безпеки;
- проведенні заходів, направлених на запобігання НСД до інформації та блокування дій осіб, які не мають прав доступу до інформації;
- недопущення впливу на технічні засоби системи, в результаті якого може порушено їх функціонування;
- контроль над забезпеченням вимог до встановленого рівня захищеності.

Загрози, які внесені у діючу модель загроз, можуть уточнюватися і доповнюватися по мірі виявлення нових джерел загроз, розвитку способів та засобів реалізації загроз ІБ.

Таблиця 1.8 – Перелік загроз з визначенням порушень властивостей інформації

Джерело загрози	Вразливість	Загроза	Наслідки порушення			Ймовірність	Рівень загрози
Техногенні			К	Ц	Д		
Система електроживлення	Відсутність резервних копій жорстких дисків сервера, Не використовуються прилади безперебійного живлення	У разі реалізації загрози інформація пошкоджується і для її відновлення необхідно щоб громадяни повторно заповнили декларації. Це є суттєвий удар по репутації організації. Загроза втрати інформації	0	2	3	2	7

Продовження таблиці 1.8

Антропогенні							
Внутрішні							
Джерело загрози	Вразливість	Загроза	Наслідки порушення			Ймовірність	Рівень загрози
			К	Ц	Д		
Головний бухгалтер	Не контролюється кількість друкованих копій	Персональні дані лієнта що містяться в інформації 1 і 3 можуть покинути межі КЗ і бути передані третім особам. Загроза несанкціонованого доступу до друкованих копій інформації з обмеженим доступом	3	0	0	1	4
Системний адміністратор	Велика кількість повноважень для системного адміністратора в ІС	Загроза зловживання правами доступу.	3	2	1	1	7

Продовження таблиці 1.8

Джерело загрози	Вразливість	Загроза	Наслідки порушення			Ймовірність	Рівень загрози
			К	Ц	Д		
Користувачі з рівнем доступу R і W	Відсутність контролю зовнішнього трафіку (інформація що передається по електронній пошті)	Загроза несанкціонованого доступу до інформації шляхом передавання ІзОД через електронну пошту третім особам	2	0	0	2	4
Зовнішні							
Зловмисник	Низька компетентність працівників	Загроза порушення властивостей інформації шляхом зараження вірусним ПЗ.	2	2	2	2	8

Рівні загроз:

- низький – до 4 балів;
- середній – від 4 до 6 балів;
- високий – від 6 до 8 балів.

З моделі загроз, наведеній у вигляді таблиці 1.8, видно, що до найбільшого збитку репутації закладу, уразі реалізації загрози, призведуть наступні загрози:

- нестабільне електроживлення;
- використання службових обов'язків системним адміністратором у корисних цілях;
- зараження вірусом та передача співробітниками ІзОД третім особам через електронну пошту.

1.4 Висновок

В першому розділі кваліфікаційної роботи проведено обстеження ОІД, що належить «Управлінню праці та соціального захисту населення міста Новомосковська».

Було побудовано модель потенційного порушника та модель загроз ІБ, з яких можна зробити висновок щодо існуючого стану захисту інформації.

На основі отриманої інформації, в спеціальному розділі доцільно буде проаналізувати існуючі критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, які надані в НД ТЗІ 2.5-004-99 від 28.12.2012 № 806 та запропонувати організаційно-програмні рішення для забезпечення необхідного рівня захищеності інформації з обмеженим доступом.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз профілю захищеності

Згідно НД ТЗІ 2.5-005-99, автоматизована система, яка належить УПСЗН, являє собою АС класу "3" - розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу; передача інформації може здійснюватися через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

На основі обстеження ОІД і аналізу даних, які обробляються, було визначено стандартний функціональний профіль захищеності в КС, що входить до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:
3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1}.

Усі критерії захищеності детально описані в НД ТЗІ 2.5-004-99, нижче розглянемо ті, що актуальні для АС:

Базова довірча конфіденційність (КД-2). Реалізовано. В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів.

КС забезпечує послугу повторне використання об'єктів (КО-1). Реалізовано. Якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і скасовуються попередні права доступу до об'єкта. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття ". Критерії не встановлюють, коли саме має виконуватися очищення об'єкта. Залежно від реалізованих механізмів можна виконувати очищення об'єкта під час його звільнення користувачем або безпосередньо перед його наданням наступному користувачу. Повторне використання об'єкта може бути реалізовано також шляхом шифрування інформації, що міститься в об'єктах, і використання керування криптографічними ключами замість знищення інформації.

Конфіденційність при обміні (КВ-1). Реалізована. В розподіленому оточенні можуть взаємодіяти різні КЗЗ, які часто реалізують різні політики безпеки інформації. Послуги захисту інформації при обміні (конфіденційність при обміні, цілісність при обміні, ідентифікація і автентифікація при обміні, автентифікація відправника і автентифікація одержувача) дозволяють забезпечити безпеку обміну інформацією між такими КЗЗ через незахищене середовище. Так, реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. На АС використовується шифрування інформації за допомогою ПК «Крипто Автограф» для передачі її по незахищеним каналам.

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

Відкат (ЦО-1). Реалізована. Відкат є багатосторонньою послугою, що дозволяє відновлюватися після помилок користувача, збоїв програмного забезпечення або

апаратури і підтримувати цілісність баз даних, додатків, побудованих на транзакціях і т. ін. Дана послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат. Мається на увазі, що відкат — завжди доступна автоматизована послуга. Використання відкладеного резервування, що вимагає втручання користувача для завантаження резервного носія, не є реалізацією відкату. Якщо система реалізує дану послугу, то її використання має фіксуватись в журналі. Відміна операції не повинна приводити до видалення з журналу запису про операцію, яка пізніше була відмінена. Необхідною умовою для реалізації всіх рівнів даної послуги є реалізація рівня НИ-1 послуги ідентифікація і автентифікація

Мінімальна цілісність при обміні (ЦВ-1). Реалізована**.** Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів КС і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності. На АС перед передачею ІзОД до податковою інспекції усі файли підписуються ЕЦП.

Квоти (ДР-1). Реалізована**.** Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування доступністю послуг КС. Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу. Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або

від користувачів, яким надані відповідні повноваження. На АС кожен користувач має обмежений об'єм дискового простору.

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

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

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

Однонаправлений достовірний канал (НК-1). Реалізована. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал

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

Розподіл обов'язків адміністраторів (НО-2). Не реалізована. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

КЗЗ з гарантованою цілісністю (НЦ-2). Реалізована. Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування. Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Самотестування при старті (НТ-2). Реалізована. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

Автентифікація вузла (НВ-1). Реалізована. Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.2 Проектні рішення

2.2.1 Елементи політики безпеки

З моделі загроз видно, що суттєвою вразливістю є некомпетентні працівники УПСЗН. Зовнішні зловмисники можуть скористатися цією можливістю для здійснення НСД до ІзОД. На основі цього було запропоновано введення на підприємстві такі елементи політики безпеки: політика паролів, політика “чистого стола”, політика використання електронної пошти, які повинні бути доведені до відома співробітників керівництвом закладу.

Політика паролів

Мета політики встановити вимоги до створення та використання паролів для всіх користувачів АС. Забезпечити використання “сильних” паролів.

Область застосування політики зобов’язує всіх користувачів дотримуватися правил стосовно паролів, які наведені у цій політиці.

Політика безпеки:

- пароль має бути мінімум 12 символів, має містити в собі літери малого та високого регістру А-а, мінімум одну цифру та мінімум один спеціальний символ, наприклад #!@%*;
- заборонено використовувати послідовні паролі. Наприклад, “qwerty”, “123456”, “abcde”;
- заборонено використовувати в паролі персональні дані (наприклад, елементи ПІБ, дата народження своя чи родичів);
- пароль не повинен містити слова, які є в словниках українського, російського та англійського алфавітів;
- кожен користувач повинен змінювати пароль раз на місяць.

Політика “чистого стола”:

Мета політики встановити вимоги до робочого місця працівників де обробляється ІзОД.

Область застосування політики розповсюджуються на всіх користувачів інформаційної системи, які приймають участь в обробці ІзОД.

Політика безпеки:

- користувачам заборонено залишати на моніторі, у блокноті на столі або під клавіатурою записи логінів та паролів;
- персональний комп’ютер необхідно вимикати в кінці робочого дня;
- користувачу необхідно блокувати екран персонального комп’ютера, коли покидає робоче місце;
- не залишати друковані копії на столі або у принтері після закінчення роботи з ними.

Політика використання електронної пошти

Мета політики встановити вимоги до користування електронною поштою для забезпечення більшої захищеності системи та запобігання атакам фішингу та соціальної інженерії.

Область застосування політики розповсюджується на всіх користувачів інформаційної системи та на всю інформацію, що передається через електронну пошту.

Політика безпеки:

- інформація, що передається через електронну пошту, ОБОВ’ЯЗКОВО має бути підписана ЕЦП сформованим за допомогою ПК “Крипто Автограф”;
- користувачам забороняється переходити на будь-які посилання, що можуть надійти на пошту;
- забороняється використовувати електронну пошту для особистого листування, розсилки будь-яких провокуючих листів, рекламних

повідомлень, комерційних пропозицій тощо.

2.2.2 Введення посади адміністратора безпеки

З моделі загроз видно що найбільшу загрозу становить системний адміністратор. На основі проведеного обстеження ОІД було визначено що ІС належить до класу “3”. Згідно з НД ТЗІ 2.5-004-99 профіль захищеності в КС класу “3” з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації включає послугу безпеки НО-2 - розподіл обов'язків адміністраторів. Для реалізації послуги необхідно визначити мінімум дві адміністративні ролі: адміністратор безпеки та інший адміністратор, у випадку УПСЗН, це системний адміністратор.

Задачі і функції адміністратора безпеки (АБ).

Основними задачами АБ являються:

- супроводження засобів захисту інформації від НСД і основних технічних засобів та систем;
- створення резервних копій жорстких дисків сервера;
- організація розмежування доступу;
- контроль ефективності захисту інформації.

Для виконання поставлених задач на АБ покладаються наступні функції:

- допуск користувачів до технічних, програмних і інформаційних ресурсів;
- організація порядку обліку, зберігання і обробки ІзОД;
- підготовка інструкцій, що визначають задачі, функції та обов’язки користувачів ІзОД з питань захисту інформації;
- контроль виконання вимог діючих нормативних документів з питань захисту інформації при обробці її в КС;

Обов'язки адміністратора безпеки

Для реалізації поставлених задач і покладених функцій адміністратор безпеки зобов'язаний:

- вести журнал обліку експлуатаційної та технічної документації КСЗІ;
- здійснювати керування режимами роботи автоматизованих робочих місць;
- бути присутнім при внесенні змін в конфігурацію апаратно-програмних засобів, які функціонують в КС, здійснювати перевірку працездатності системи захисту після встановлення/оновлення технічних та/або програмних засобів;
- раз на 3 місяці перевіряти цілісність пломб на технічних засобах обробки інформації;
- вести журнал обліку нештатних ситуацій, фактів опечатування та зняття пломб, виконання профілактичних заходів, установки та модифікації технічних засобів обробки та захисту інформації;
- періодично проводити інструктаж користувачів по правилам роботи з використовуваними засоби обробки інформації;
- визначати інформаційні зв'язки між сегментами мережі;
- вести облік заявок користувачів на допуск до ІзОД.

Адміністратору безпеки забороняється:

- використовувати службове положення для створення облікових записів неіснуючих користувачів;
- використовувати ідентифікаційні дані користувачів, які стали доступними в ході виконання обов'язків, для маскування власних дій в системі;
- самостійно вносити зміни (без узгодження з системним адміністратором) до налаштувань КС;
- використовувати у власних або в чиїх-небудь інтересах ресурси інформаційної системи, надавати таку можливість іншим;

- вимикати КСЗІ без письмового погодження з керівництвом УПСЗН;
- передавати третім особам будь-яким способом мережеві адреси, імена, паролі, інформацію про рівень доступу користувачів, конфігураційні налаштування;
- проводити в робочий час дії, що призводять до збою, зупинки, уповільнення роботи КС, блокування доступу, втраті інформації без дозволу керівництва та попередження користувачів
- редагувати, видаляти, підмінювати журнали аудиту;
- порушувати правила експлуатації обладнання.

Адміністратор безпеки має право:

- переглядати права доступу користувачів до інформаційних ресурсів;
- вимагати у користувачів дотримуватися інструкцій з забезпечення захисту безпеки інформації;
- приймати участь у службових розслідуваннях по фактам порушення встановлених вимог до забезпечення захисту інформації, НСД, втрати ІзОД;
- здійснювати оперативне втручання в роботу користувача при явній загрозі інформаційній безпеці в результаті недотримання встановленої технології обробки інформації і невиконання вимог до інформаційної безпеки;
- вносити власні пропозиції по удосконаленню захисту інформаційної системи.

2.2.3 Контроль друку на принтерах

З моделі загроз видно, що суттєвою вразливістю є відсутність контролю друкованих копій документів, які містять інформацію з обмеженим доступом. Для зменшення ймовірності реалізації цієї загрози необхідно ввести в АС програмне забезпечення для контролю за друком.

PrintLimit Print Tracking - це ПО, яке може бути встановлено на одному з комп'ютерів автоматизованої системи; за допомогою чого можна здійснювати моніторинг і керувати друком, також можна підраховувати кількістю друкованих

копій, які були роздруковані на будь-якому принтері в системі. За допомогою PrintLimit Print Tracking можна керувати друком усіх користувачів системи в не залежності від комп'ютера та принтера за допомогою яких здійснювався друк.

Данна програма дозволяє направляти на друк документи в безпечну мережу і здійснювати ідентифікацію користувача шляхом вводу PIN-коду або сканованого пропуску. Основні функції, що зменшить ймовірність несанкціонованого друку:

- централізований менеджер друку;
- лічильник друку;
- контроль доступу до друку;
- підтримка принтерів будь-яких марок.

2.2.4 Впровадження джерела безперебійного живлення

Задачі які необхідно вирішити:

- забезпечити коректне завершення роботи серверу при відсутності електроживлення в неробочій час;
- у випадку не стабільного електропостачання в робочий час, продовжити час роботи АС для коректного завершення усіх процесів та збереження стану інформації на комп'ютерах всіх користувачів.

Необхідне обладнання:

- прилад розподільного живлення NetPing 4/PWR-220 v3/SMS - 3 шт;
- датчик наявності електроживлення - 1 шт;
- джерело безперебійного живлення Elim-Украина ПНК-12-300 - 1 шт (технічні характеристики наведено у таблиці 2.2);
- аккумуляторна батарея Challenger A12-55 - 1 шт(технічні характеристики наведено у таблиці 2.1);
- мікроконтролер Raspberry Pi - 1 шт;

Схема підключення обладнання зображена на рисунку 2.1.

На Raspberry Pi спершу треба встановити Linux Debian Raspberry Pi4. Для

реалізації програмної складової для керування електроживленням необхідно створити скрипт на скриптовій мові bash. Скрипт буде виконуватися в терміналі операційної системи Linux Debian Raspberry Pi4. Для коректної роботи скрипта необхідно встановити пакети Curl і Expect. Після чого створюється файл скрипту з розширенням name_script.sh. Запропонований скрипт наведено у додатку Б. Наступний крок це надання файлу скрипта права на виконання командою "sudo chmod +x name_script.sh", після чого необхідно запустити скрипт. Щоб скрипт запускався автоматично при старті Raspberry Pi потрібно додати скрипт в оточення локальних змінних.

Алгоритм роботи рішення:

1) Скрипт запущений на мікроконтролері Raspberry Pi кожні 5 хвилин опитує датчик наявності електропостачання, який підключено до NetPing 4/PWR-220 v3/SMS.
2) Якщо датчик "повідомляє" про наявність електропостачання - ніякі дії не виконуються.
3) Якщо датчик "повідомляє" про відсутність електропостачання і подія відбулася в неробочий час - пристрій керування електроживленням NetPing 4/PWR-220 v3/SMS надсилає СМС-повідомлення про подію, скрипт посилає серверу сигнал завершення роботи.
4) Якщо датчик "повідомляє" про відсутність електропостачання і подія відбулася в робочий час - пристрій керування електроживленням NetPing 4/PWR-220 v3/SMS надсилає СМС-повідомлення про подію. Усі комп'ютери продовжують працювати від джерела безперебійного живлення до повного розрядження акумуляторної батареї або відновлення електроживлення.

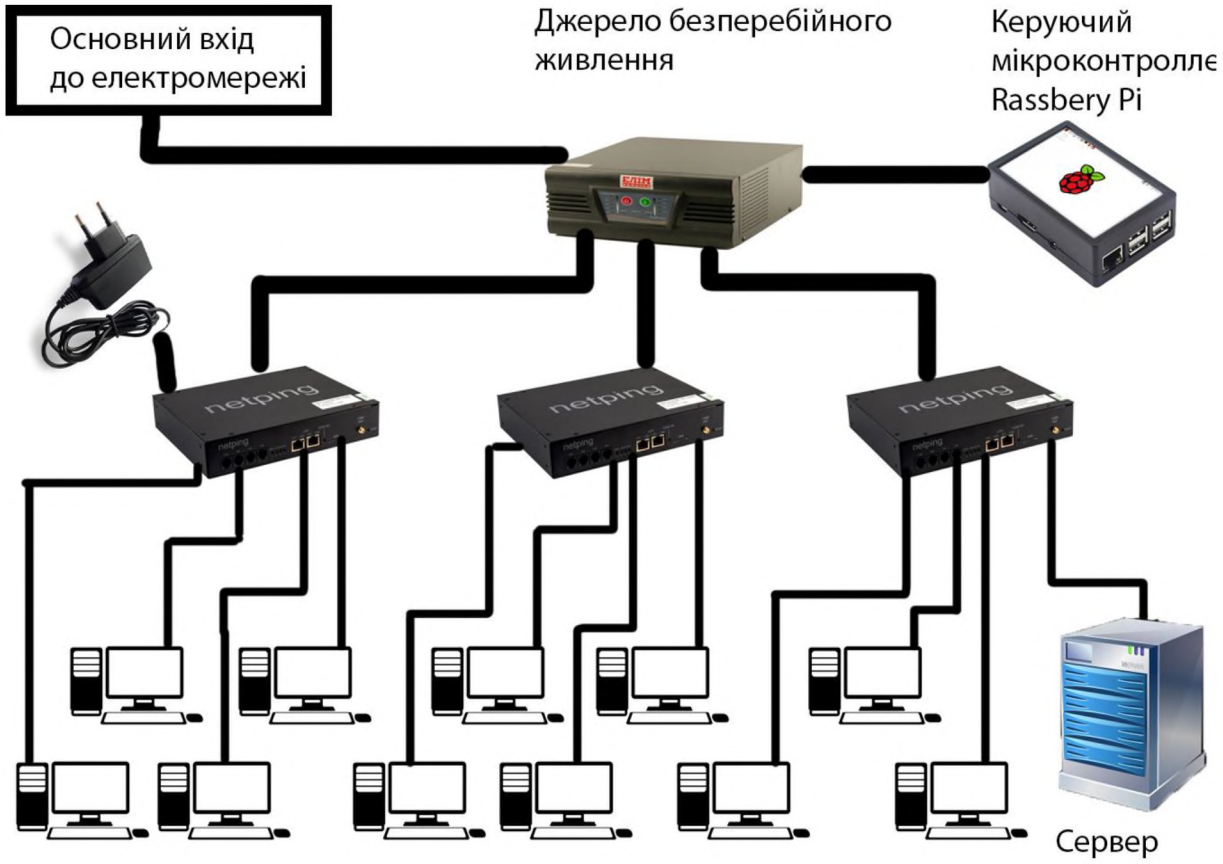


Рисунок 2.1 - Схема підключення джерела безперебійного живлення

Таблиця 2.1 - Технічні характеристики АКБ Challenger A12-55

Характеристика	Значення
Номінальна напруга, В	12
Ємність, А.г	55
Максимальний ток заряду, А	16,5
Максимальний струм розряду, А	550
Напруга заряду в циклічному режимі, В	14,6
Робоча температура, С	-20 … +60

Продовження таблиці 2.1

Характеристика	Значення
Термін експлуатації, років	12
Висота, мм	235
Ширина, мм	229
Маса, кг	18

Таблиця 2.2 - Технічні характеристики Elim-Украина ПНК-12-300

Технічні характеристики	Значення
Тип архітектури	лінійно-інтерактивний
Форма вихідної напруги	синусоїда
Тип виконання	зовнішня
Потужність, кВт	0,3
Напруга, В	12
Коефіцієнт потужності	0,99
Кількість фаз (вхід/вихід)	1/1
Нижні поріг вхідої напруги, В	145
Верхній поріг вхідної напруги, В	275
Вихідна напруга, В	220/230
Ток заряду батареї, А	15

Час автономної роботи розраховано за наступною формулою:

$$T = \frac{C \cdot U}{P \cdot N} = \frac{55 \cdot 12}{300 \cdot 13} \simeq 0.17 \text{ год } \simeq 10 \text{ хв.}, \quad (2.1)$$

де Т - час роботи від АКБ;

С – ємність;

U – напруга;

Р - потужність, N - кількість ПК.

Цей час, а саме 10 хвилин, розраховано з використанням показників потужності при максимальному навантаженні усіх технічних засобів системи, цього часу достатньо для завершення всіх необхідних процесів, наприклад, передача інформації або збереження її стану на робочий станції користувача. Також за цей час користувач має послати сигнал завершення роботи комп'ютера.

2.2.5 Аналіз загроз після впровадження заходів щодо ІБ

З таблиці 2.3, в якій наведено модель загроз після впровадження рішень з ІБ, видно, що усі показники відповідають низькому рівню загроз (до 4 балів). Можна спостерігати, як суттєво знизився ризик пошкодження, або втрати інформації в результаті нестабільного електроживлення. Також, було зменшено ймовірність НСД системним адміністратором, за допомогою введення посади адміністратора безпеки Отже можна зробити висновок, що впроваджені рішення надали суттєвого підвищення безпеки інформації в УПСЗН.

Таблиця 2.3 - Модель загроз після впровадження заходів щодо ІБ

Джерело загрози	Вразливість	Загроза	Наслідки порушення			Ймовірність	Рівень загрози
Техногенні			К	Ц	Д		
Система електроживлення	Відсутність резервних копій жорстких дисків сервера, не використовуються прилади безперебійного живлення	У разі реалізації загрози інформація пошкоджується і для її відновлення необхідно щоб громадяни повторно заповнили декларації. Це є суттєвий удар по репутації організації. Загроза втрати інформації	0	0	2	1	2
Антропогенні							
Внутрішні							
Головний бухгалтер	Не контролюється кількість друкованих копій	Персональні дані лієнта що містяться в інформації 1 і 3 можуть покинути межі КЗ і бути передані третім особам. Загроза Несанкціонованого доступу до друкованих копій інформації з обмеженим доступом	1	0	0	1	2

Продовження таблиці 2.3

Джерело загрози	Вразливість	Загроза	Наслідки порушення			Ймовірність	Рівень загрози
			К	Ц	Д		
Системний адміністратор	Велика кількість повноважень для системного адміністратора в ІС	Загроза зловживання правами доступу.	1	1	0	1	3
Користувачі з рівнем доступу R і W	Відсутність контролю зовнішнього трафіку (інформація що передається по електронній пошті)	Загроза несанкціонованого доступу до інформації шляхом передавання ІзОД через електронну пошту третім особам	1	0	0	1	2
Зовнішні							
Зловмисник	Низька компетентність працівників	Загроза порушення властивостей інформації шляхом зараження вірусним ПЗ.	1	1	1	1	4

2.3 Висновок

У другому розділі кваліфікаційної роботи було вибрано профіль захищеності, для реалізації якого необхідно було ввести посаду адміністратора безпеки.

На основі моделі порушника та загроз були визначені актуальні загрози ІБ підприємства УПСЗН. Виходячи з актуальних антропогенних загроз було

запропоновано елементи політики безпеки та встановлення системи контролю друку.

Для запобігання реалізації техногенної загрози та втрати інформації було рекомендовано створити систему безперебійного живлення. Було наведено необхідні технічні та програмні засоби для реалізації системи безперебійного живлення.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу дипломного проекту є техніко-економічне обґрунтування доцільності впровадження запропонованих політик безпеки та технічних засобів захисту інформації для "Управління праці та соціального захисту населення".

3.1 Розрахунок капітальних витрат

3.1.1 Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість складається з декількох видів робіт, щоб розрахувати трудомісткість розробки політики безпеки, необхідно врахувати трудомісткість кожної операції, що виконується.

$$t = t\text{тз} + t\text{в} + ta + t\text{вз} + t\text{озб} + t\text{овр} + t\sigma = 5{,}5 + 6{,}4 + 7{,}2 + 4 + 5{,}8 + 4{,}3 + +6 = 39{,}2 \text{ год.}, \quad (3.1)$$

де tтз – тривалість складання технічного завдання на розробку політики безпеки;

tв – розробки основних положень політики;

ta– тривалість аналізу ризиків;

tвз – тривалість формування вимог до рівня захищеності;

tозб – тривалість вибору рішень з забезпечення безпеки;

tовр– тривалість створення та оформлення технічної документації.

Витрати на розробку політики безпеки інформації складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки і вартості витрат машинного часу, що необхідний для розробки політики безпеки:

$$\text{Крп} = \text{Ззп} + \text{Змч} = 4356 + 3050{,}6 = 7406{,}6 \text{ грн.} \quad (3.2)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$\text{Ззп} = t \cdot \text{Зіб} = 39{,}2 \cdot 111{,}11 = 4356 \text{ грн.}, \quad (3.3)$$

де t – загальна тривалість створення політики безпеки, годин;

Зіб – середня часова оплата заробітна плата спеціаліста з інформаційної безпеки у Дніпровській області з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації визначається за формулою:

$$Змч = t \cdot Смч = 39{,}2 \cdot 77{,}82 = 3050{,}6 \text{ грн.}, \quad (3.4)$$

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

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

Вартість 1 години машинного часу персонального комп'ютера визначається за формулою:

$$С_{мч} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_p} + \frac{K_{лпз} \cdot Н_{апз}}{F_p} = 0{,}3 \cdot 39{,}2 \cdot 1{,}68 + \frac{2000 \cdot 0{,}5}{1920} + \frac{2300 \cdot 0{,}24}{1920} = 41{,}98 \frac{грн}{год}., \quad (3.5)$$

де Р – встановлена потужність персонального комп'ютера, кВт

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

Фзал– залишкова вартість персонального комп'ютера на кінець року, грн.;

На – річна норма амортизації на персональному комп'ютері, частки одиниці;

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

Клпз – вартість ліцензійного програмного забезпечення, грн.;

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

Для підрахунку капітальних витрат на проектування та впровадження рішень щодо захисту інформації розраховується за наступною формулою:

$$К = К_{пр} + К_{пз} + К_{тз} + К_{пб} = 7406{,}6 + 5368 + 28797 + 12034 + 3001 = 56606{,}6 \text{ грн.}, \quad (3.6)$$

де $К_{пз}$ – витрати на придбання ліцензійного програмного забезпечення;

$К_{тз}$ – витрати на придбання технічних засобів;

$К_{пб}$ – витрати на створення та впровадження політики безпеки.

3.1.2 Розрахунок поточних витрат

За методикою Gartner Group до поточних витрат відноситься:

- $С_в$ – вартість оновлення (модернізації) системи на протязі року, в нашому випадку оновлення використаних технічних засобів становить:
    1) комплект джерела безперебійного живлення та акумулятора - 6751 грн.;
    2) мікроконтролер Raspberry Pi – 2660 грн.;
    3) 3 шт. NetPing 4/PWR-220 v3/SMS – 19383 грн.;

  Таким чином маємо Св = 6751+2660 +19383 =28797 грн.

- $С_к$ – витрати на керування системою в цілому (заробітна платня адміністратора безпеки 12750грн. · 12 міс. = 153000грн, витрати).
- $С_{ак}$ – витрати викликані активністю користувача (амортизаційні відрахування від вартості обладнання 4235грн.).

Формула розрахунку амортизаційних відрахувань за умови, що залишкова вартість становитиме 0 грн. за прямолінійним методом має такий вигляд:

$$С_{ак} = \sum \frac{В_{тз}}{Т}, \quad (3.6)$$

де $С_{ак}$ – загальна сума амортизаційних відрахувань, грн;

$В_{тз}$ – вартість технічного засобу, грн;

Т – термін корисного використання, років.

$$С_{ак} = \sum \frac{В_{тз}}{Т} = \frac{6751}{12} + \frac{2660}{5} + \frac{19383}{6} = 4235 \text{ грн.}$$

Отже, річні поточні витрати складають:

$$С = С_в + С_к + С_{ак} = 28797 + 153000 + 4235 = 186032 \text{ грн.} \quad (3.6)$$

Вартість електроенергії, що споживається апаратурою системи інформаційного захисту безпеки протягом року, визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0,313 \cdot 1664 \cdot 1,68 = 874,99 \text{ грн.}, \quad (3.7)$$

де Р – потужність;

$F_р$ – річний фонд робочого часу системи;

$Ц_е$ – тариф на електроенергію.

3.2 Оцінка можливого збитку від атаки

Необхідні вихідні дані для розрахунку:

- tп – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;
- tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;
- tви – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;
- Зо – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;
- Зс – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць; Заробітна плата не повинна бути нижче мінімальної заробітної плати на 01 січня поточного року. Ставка єдиного соціального внеску 22% и більше згідно класу професійного ризику підприємства, на якому проводиться захист інформації.
- Чо – чисельність обслуговуючого персоналу (адміністраторів та програмних інженерів), осіб.;
- Чс – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;
- О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або

сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

- Пзч – вартість заміни встаткування або запасних частин, грн; I – число атакованих вузлів або сегментів корпоративної мережі; N – середнє число можливих атак на рік.

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

$$U = П_П + П_В = 14829{,}54 + 26684 = 41513{,}54 \text{ грн.}, \quad (3.8)$$

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 конфігурацій та ін.);

V - втрати від зниження обсягів продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн;

Втрати від простою роботи працівників через непрацездатність систему після атаки, являють собою втрати заробітної плати, які розраховуються за формулою:

$$Пп = \frac{\sum Зс}{F} \cdot t_П = \frac{10000 \cdot 6 + 12000 \cdot 4 + 15000 \cdot 2}{176} \cdot 8 = 14829{,}54 \text{ грн.}, \quad (3.9)$$

де F – місячний фонд робочого часу, год;

$t_П$ – час простою вузла, год;

$З_С$ – заробітна платня співробітників, грн/міс.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі:

$$П_В = П_{ВИ} + П_{ПВ} + П_{ЗЧ} = 11234 + 7000 + 8450 = 26684 \text{ грн.}, \quad (3.10)$$

де $П_{ви}$ - витрати на повторне введення інформації;

$П_{пв}$ – витрати на відновлення вузла;

$П_{зч}$ – вартість заміни устаткування.

Витрати на повторне введення інформації розраховується на основі зарплати співробітника, який буде вводити інформацію повторно, з урахуванням часу, який знадобиться для відновлення інформації:

$$П_{ви} = \frac{\sum З_с}{F} \cdot t_{ви} = \frac{10000 \cdot 2}{176} \cdot 98 = 11234 \text{ грн.}, \quad (3.11)$$

де $З_с$ – заробітна платня співробітників, грн/міс;

F – місячний фонд робочого часу, год;

$t_{ви}$ – час, затрачений на повторне введення інформації.

Витрати на відновлення вузла або сегмента корпоративної мережі визначаються часом відновлення після атаки і розміром середньогодинної заробітної плати обслуговуючого персоналу:

$$П_{пв} = \frac{\sum З_О}{F} \cdot t_в = \frac{12000+10000}{176} \cdot 56 = 7000 \text{ грн.} \quad (3.12)$$

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

$$B1 = \sum_i \sum_n U = 41513{,}54 * 2 * 1 = 83027{,}08 \text{ грн.} \quad (3.13)$$

Щоб розрахувати збитки у випадку витоку персональних даних про клієнтів потрібно враховувати штраф згідно чинного законодавства стосовно порушення правил захисту персональних даних, кількість постраждалих та ймовірність такої події:

$$B2 = S * N * K = 2473 * 53 = 131069 \text{ грн.}, \quad (3.14)$$

де S – сума штрафу за порушення правил захисту персональних даних;
N – кількість постраждалих клієнтів.

3.3 Загальний ефект від впроваджених засобів захисту інформації

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

$$E = (B1 \cdot R1 + B2 \cdot R2) - C = (83027{,}08 \cdot 0{,}9 + 131069 \cdot 0{,}9) - 186032 = \\ = 6654{,}42 \text{ грн.}, \quad (3.15)$$

де B1 – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;
R1 – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;
C – щорічні витрати на експлуатацію всіх заходів, грн;
B2 – загальний збиток від витоку персональних даних клієнтів, грн;
R2 – очікувана ймовірність витоку персональних даних за рік.

3.4 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Для оцінки економічної ефективності та доцільності введення системи захисту інформація, яка була запропонована в спеціальному розділі кваліфікаційної роботи. Оцінка здійснюється на основі таких показників:

- коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI;
- термін окупності капітальних інвестицій.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового

прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. З точки зору інформаційної безпеки, даний коефіцієнт можна розглядати як збереження коштів, які могли бути втрачені при реалізації атаки:

$$ROSI = \frac{E}{K} = \frac{6654{,}42}{56606{,}6} = 0{,}1, \quad (3.17)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки;
К – капітальні інвестиції

Щоб вирахувати за скільки років окупляться інвестиції, які були вкладені для впровадження системи захисту інформації, використовується формула:

$$T_O = \frac{К}{Е} = \frac{1}{ROSI} = \frac{1}{0{,}1} = 10 \text{ років}. \quad (3.18)$$

3.5 Висновок

В економічному розділі було проаналізовано витрати на впровадження політики безпеки і технічних засобів, які склали 56606,6 грн. Після впровадження політики безпеки та технічних засобів безперебійного живлення економічний ефект від запропонованих рішень склав 6654,42 грн. Також після підрахунку за формулою (3.18) було з'ясовано, що кошти затрачені на реалізацію механізмів захисту окупляться через 10 років. Виходячи з цих показників зроблено висновок, що запропоновані рішення захисту інформації є доцільними

ВИСНОВКИ

У першому розділі кваліфікаційної роботи було наведено результати обстеження ОІД, та побудовано моделі загроз та порушника. На основі цих даних було сформовано задачі, які необхідно було вирішити для забезпечення рівня захищеності, який відповідав би поставленим вимогам.

У спеціальній частині кваліфікаційної роботи було проаналізовано існуючий профіль захищеності. Спираючись на модель загроз та модель порушника було запропоновано наступні рішення:

- введення посади адміністратора безпеки, для реалізації послуги НО-2(Розподіл обов'язків адміністраторів);
- сформовано такі політики безпеки:
    1) політика паролів;
    2) політика «чистого стола»;
    3) політика використання електронної пошти;
- запропоновано технічну схему реалізації безперебійного живлення.

Розрахунки які були здійснені у третьому розділі, підтвердили доцільність реалізації запропонованих рішень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки. Методики виявлення закладних пристроїв. НД ТЗІ 2.7-011-2012 – Київ 2012 р.

2. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 2.6-001-11 – Київ 2011р.

3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступ. НД ТЗІ 2.5-005 -99 – Київ 1999 р.

4. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99 – Київ 1999 р.

5. Про захист персональних даних: закон України від 23.04.2021 р. № 2297-VI. Дата оновлення: 1.06.2010 [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1556-18#Text .

6. Пример интеллектуального управления питанием группы серверов при помощи NetPing [Електронний ресурс] Режим доступу до ресурсу: http://www.netping.ru/Blog/primer-intellektualnogo-upravleniya-pitaniem-gruppy-serverov-pri-pomoschi-netping .

7. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных [Електронний ресурс] Режим доступу до ресурсу: http://uralsudmed.ru/data/content/Image/5_%20%20%20%20%20%20%20.pdf .

8. Менеджер печати/счетчик печати/контроль печати [Електронний ресурс] Режим доступу до ресурсу: https://www.printlimit.com/russian/print-management/.

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

10. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Д. П. Пілова – Дніпро: НТУ «ДП», 2019 р.

11. Джерела безперебійного живлення (ДБЖ) [Електронний ресурс]. – Режим доступу до ресурсу: http://www.sven.fi/ua/press/publications/detail.php?id=6925 .

12. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 г.

13. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/ .

14. Про інформацію: Закон України: [Електронний ресурс] – Режим доступу до ресурсу: http://www.rada.gov.ua .

15. Класифікація інформаційних об'єктів [Електронний ресурс] – Режим доступу до ресурсу: http://www.razgovorodele.ru/security1/safety04/inf08.php .

16. Защита персональных данных: работа на опережение [Електронний ресурс] – Режим доступу до ресурсу: https://biz.ligazakon.net/ru/analitycs/195680_zashchita-personalnykh-dannykh-rabota-na-operezhenie .

17. Информационная безопасность и защита информации / Шаньгин В. Ф. – ДМК «Пресс», 2014 г.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Стан питання. Постановка задачі	37	
6	А4	2 Спеціальна частина	17	
7	А4	3 Економічний розділ	7	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток Г	1	
13	А4	Додаток Ґ	1	
14	А4	Додаток Д	2	

ДОДАТОК Б. НАКАЗ ПРО ПРИЗНАЧЕННЯ НА ПОСАДУ

УПРАВЛІННЯ ПРАЦІ ТА СОЦІАЛЬНОГО ЗАХИСТУ НАСЕЛЕННЯ МІСТА НОВОМОСКВСЬК

код ЄДРПОУ: 03192894, адреса місцезнаходження: Україна, 51200, Дніпропетровська обл., місто Новомосковськ, вулиця Горького, будинок 2А

НАКАЗ

№3/06-2021 від 17 червня 2021 року

1.Призначити на наступну посаду: Адміністратор безпеки особу: ІВАНОВ ІВАН ІВАНОВИЧ, починаючи з 21 червня 2021 року.

2. Встановити для Працівника щомісячний посадовий оклад в розмірі 12750 грн. (чотирнадцять тисяч двісті п’ятдесят гривень).

3. Працівника повідомлено, що виконувана робота є основною роботою.

_____

Від роботодавця: в особі Горбач Галина Миколаївна, яка діє на підставі наступного документа: Статуту редакція від 21.03.2018

З Наказом ознайомлений:

_____

ІВАНОВ ІВАН ІВАНОВИЧ (особистий підпис)

ДОДАТОК В. ЗМІСТ КЕРУЮЧОГО СКРИПТУ ДЛЯ ЕЛЕКТРОЖИВЛЕННЯ

```
#!/bin/bash
##### В этой секции вы можете указать свои значения #####
#IP адрес устройства NetPing8/PWR-220v3/SMS
NPip="192.168.1.208"
#учетные данные для устройства NetPing8/PWR-220v3/SMS
NPuser="visor"
NPpass="ping"
#Учетные данные для серверов
user="tester"
pass="12345"
#Список пк
serv="
192.168.1.180
192.168.1.181
192.168.1.182
192.168.1.183
192.168.1.184
192.168.1.185
192.168.1.186
192.168.1.187
192.168.1.188
192.168.1.189
192.168.1.190
192.168.1.191
192.168.1.192
"
############################################################
while true
do
#Запрашиваем информацию о состоянии датчика наличия 220V:
io1=$(curl --silent --user $NPuser:$NPpass http://$NPip/io.cgi?io1)
sensor_220=${io1:20:1}
if [ "$sensor_220" -eq 0 ] #Если питания нет
then
echo "Питания нет"
d=$(date +%H) #Получаем текущее время.
if [ "$d" -lt "09" ]||[ "$d" -gt "18" ] #Если текущее время раньше 9 утра и позже 18
часов
then
```

```
echo "Нерабочее время - выключаем сервера"
#Выключаем сервера:
for S in $serv
do
expect -c "
spawn ssh $user@$S
expect \"*(yes/no*)?*\" {send \"yes\r\"}
expect \"*password:\"
send \"$pass\r\"
expect \"*>\"
send \"shutdown -s\r\"
expect \"*shutdown:*\" {send \"sudo shutdown -h now\r\"}
expect \"*$user:*\" {send \"$pass\r\"}
expect eof " >> /dev/null
done
sleep 10m #Таймаут для завершения работы серверов.
#Отключаем розетки к которым подключены сервера:
for ((n=1; n<5; n++))
do
curl --silent --user $NPuser:$NPpass http://$NPip/relay.cgi?r$n=0 >> /dev/null
done
else
echo "Рабочее время - включаем сервера"
#Подаем питание на сервера:
for ((n=1; n<5; n++))
do
curl --silent --user $NPuser:$NPpass http://$NPip/relay.cgi?r$n=1 >>/dev/null
done
fi
else #Если питание есть
echo "Питание есть"
#Подаем питание на сервера:
for ((n=1; n<5; n++))
do
curl --silent --user $NPuser:$NPpass http://$NPip/relay.cgi?r$n=1 >>/dev/null
done
fi
sleep 5m
done
```

ДОДАТОК Г. Перелік документів на оптичному носії

1) Пояснювальна_записка_Карякін.doc

2) Пояснювальна_записка_Карякін.pdf

3) Презентація_Карякін.pptx

ДОДАТОК Ґ. Відгуки керівників розділів

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

ДОДАТОК Д. Відгук керівника кваліфікаційної роботи

ВІДГУК

на кваліфікаційну роботу студента групи 125-17-2

Карякіна Євгена Андрійовича

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи "Управління праці та соціального захисту населення міста Новомосковська"»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 74 сторінках.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз організаційної структури, аналіз потенційних загроз, складено акт обстеження, запропоновано організаційно-технічні рішення для запобігання реалізації актуальних загроз.

Розроблено рекомендації, щодо забезпечення інформаційної безпеки інформації з обмеженим доступом.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні рівня захищеності властивостей інформації з обмеженим доступом в інформаційно-телекомунікаційній системі "Управління праці та соціального захисту населення міста Новомоскоська".

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

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

Кваліфікаційна робота заслуговує оцінки «відмінно».

Керівник кваліфікаційної роботи: **професор Корнієнко В.І.**

Керівник спец. Розділу: **асистент Мілінчук Ю.А.**