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 *Федоренко Дар'ї Ігорівни*

академічної групи *125-18-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно - телекомунікаційної системи Покровського міського центру зайнятості*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.	95	відмінно	
розділів:				
спеціальний	ст. викл. Тимофєєв Д.С.	95	відмінно	
економічний	к.е.н., доц. Пілова Д.П.	90	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.	90	відмінно	

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенці *Федоренко Дар'ї Ігорівні* **академічної групи** *125-18-2*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації _____

за освітньо-професійною програмою *Кібербезпека*

на тему **Комплексна система захисту інформації інформаційно-телекомунікаційної системи Покровського міського центру зайнятості**

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

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Визначення аналізу стану питання, актуальності та визначити основні етапи роботи	03.05.2022
Розділ 2	Виконати обстеження ІТС Покровського МЦЗ, розробити модель порушника та модель загроз, обрати профіль захищеності та пропозиції рішень щодо захисту ІТС	27.05.2022
Розділ 3	Обґрунтувати економічну доцільність впровадження КСЗІ, розрахувати витрати та ефект впровадження КСЗІ	07.06.2022

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

Дата видачі завдання: 10.01.2022

Дата подання до екзаменаційної комісії: 08.06.2022

Прийнято до виконання _____ Федоренко Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 95 сторінок, 7 рисунків, 19 таблиць, 6 додатків, 12 посилань.

Об’єктом розробки даної роботи є інформаційно-телекомунікаційна система Покровського міського центру зайнятості.

Предметом розробки даної роботи є комплексна система захисту інформації ІТС Покровського міського центру зайнятості.

Мета: забезпечення достатнього рівня захисту інформації ІТС Покровського міського центру зайнятості.

У першому розділі був проведений аналіз стану питання та розглянуте питання актуальності розробки і впровадження комплексної системи захисту інформації для підприємства. Наступним кроком були визначені основні етапи створення КСЗІ.

У спеціальній частині виконано обстеження середовищ функціонування інформаційно-телекомунікаційної системи, проаналізовано можливі загрози через наявні вразливості. Створено модель порушника та модель загроз. Наступним етапом обрано профіль захищеності та розроблено програмно-технічні методи захисту інформації.

В економічному розділі роботи розраховано капітальні та поточні витрати, проведено оцінку можливого збитку від атаки на вузол корпоративної мережі, визначено та проаналізовано показники економічної ефективності впровадження КСЗІ.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, ОБ’ЄКТ КОМП’ЮТЕРНОЇ СИСТЕМИ, ПРАВИЛА РОЗМЕЖУВАННЯ ДОСТУПУ, ІДЕНТИФІКАЦІЯ, КОМПЛЕКС ЗАСОБІВ ЗАХИСТУ, БЕЗПЕКА ІНФОРМАЦІЇ.

ABSTRACT

Explanatory note: 95 pages, 7 pictures, 19 tables, 6 annexes, 12 sources.

The object of development: information and telecommunication system of the Pokrovsk city employment center.

The subject of development: a comprehensive information protection system information and telecommunication system of the Pokrovsk city employment center.

The purpose of work: to ensure a sufficient level of information protection information and telecommunication system of the Pokrovsk city employment center.

In the first section the analysis of a status of an issue was carried out and the issue of urgency of development and introduction of complex system of protection of the information for the enterprise was considered. The next step was to identify the main stages of the creation of KSZI.

In the special part the survey of the environments of the information and telecommunication system operation is performed, the possible threats due to the existing vulnerabilities are analyzed. The model of the violator and the model of threats have been created. The next stage is the selected security profile and developed software and hardware methods of information protection.

In the economic section of the work, capital and operating costs were calculated, the possible damage from the attack on the node of the corporate network was assessed, and the indicators of economic efficiency of the comprehensive information protection system implementation were determined and analyzed.

INFORMATION AND TELECOMMUNICATION SYSTEM, PRODUCT OBJECT, ACCESS MIDITATION RULES, IDENTIFICATION, TRUSTED COMPUTING BASE, INFORMATION SECURITY.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце;

АС – автоматизована система;

АТС – автоматична телефонна станція;

ДСЗ – Державна служба зайнятості;

ЄДРПОУ – єдиний державний реєстр організацій та установ;

ЗІ – захист інформації;

ІБ – інформаційна база;

ІзОД – інформація з обмеженим доступом;

ІТС – інформаційно-телекомунікаційна система;

ОІД – об’єкт інформаційної діяльності;

ІЧ – інфрачервоний;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

МФП – мультифункціональний пристрій;

НСД – несанкціонований доступ;

ОЗП – оперативний запам’ятовуючий пристрій;

ОС – операційна система;

КЗ – контрольована зона;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПКП – приймально-контрольний прилад;

ЦЗ – центр зайнятості;

ЩК – щит квартирний.

ЗМІСТ

ВСТУП

Об’єктом розробки даної роботи є інформаційно-телекомунікаційна система Покровського міського центру зайнятості.

Предметом розробки даної роботи є комплексна система захисту інформації ІТС Покровського міського центру зайнятості.

Мета: забезпечення достатнього рівня захисту інформації ІТС Покровського міського центру зайнятості.

У XXI сторіччі розвиток технологій набирає обертів з кожним роком або, навіть можна підкреслити, з кожним сезоном. Відповідно до цього розвитку повинно розроблятися та впроваджуватися інноваційні технології щодо захисту, підтримки працездатного стану активів.

Нещодавно прочитала вираз, що нинішня молодь проживає нібито два життя: своє природнє/ істинне життя, та віртуальне. Питання безпеки завжди є актуальним у нашому житті. По-перше, усі люди спочатку згадують про особисту безпеку та нормальне співіснування у суспільстві, а з іншої сторони, живучи у постійному контакті з технологіями, намагаємось захистити свої дані та важливу інформацію на різноманітних носіях інформації.

Створюючи інформаційну систему, потрібно дбати перш за все про її безпеку. Тому створення комплексної системи захисту інформації є актуальним питанням сьогодення. Саме ця система поєднує в собі організаційні, технічні, а також програмні і апаратні засоби. У такій комбінації можливе безпечне функціонування систем: як автономних робочих станцій, так і комп’ютерних мереж.

Актуальність питання полягає у забезпеченні надійної та безперервної роботи підприємства. Під надійністю слід розуміти коректну працездатність системи, незалежно від зовнішніх впливів і ситуації в країні. Це важливо для підтримання володіння актуальними даними про стан кількості безробітних/ працюючих громадян, переліку наявних вакансій та інше.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

Комплексна система захисту інформації – це сукупність організаційних та інженерно- технічних заходів, які спрямовані на забезпечення захисту інформації від витоку, несанкціонованого доступу і оприлюднення. [1]

На сьогоднішній день існує думка, що інформацію необхідно захищати тільки під час оброблення комп'ю76тером. Так мислять ті, хто вважає комп'ютер центром зберігання інформації. Але хотілось би зауважити, що захист інформації спрямований на об'єкти інформатизації (наприклад, електронні інформаційні ресурси, інформаційні системи, програмне забезпечення). Це поняття охоплює більшу сферу захисту, ніж просто персональний комп'ютер.

У реальному житті окремі об'єкти інформатизації існують у межах одного підприємства і представляються у вигляді єдиного комплексу компонентів. Цей комплекс має спільні завдання та цілі, технологію інформаційної обробки даних, структурні відносини.

Сучасне підприємство – велика кількість різнорідних компонентів, об'єднаних в складну систему для виконання поставлених цілей, які в процесі функціонування підприємства можуть модифікуватися. Різноманіття та складність впливу внутрішніх та зовнішніх чинників, які часто не піддаються чіткому кількісному оцінюванню, призводять до того, що ця складна система може набувати нові якості, не властиві її складовим компонентів. Прийнято, що у кожній групі компонентів присутні люди. Людина як безпосередній працівник, людина може працювати у середовищі, використовуючи технічні системи, а також посередником між людиною і технікою є програмне забезпечення.

Якщо звернутися до історії цієї проблеми, то можна умовно виділити три періоди розвитку засобів захисту інформації:

- перший ми відносимо до того часу, коли обробка інформації здійснювалася за традиційними (ручними, паперовими) технологіями;
- другий – коли для обробки інформації на регулярній основі застосовувалися засоби електронної обчислювальної техніки перших поколінь;
- третій – коли використання засобів електронно-обчислювальної техніки набрав масового і повсюдний характер (поява персональних комп'ютерів).

У 60–70 рр. XX ст. проблема захисту інформації вирішувалася досить ефективно застосуванням в основному організаційних заходів. До них належали: режимні заходи, охорона, сигналізація і найпростіші програмні засоби захисту інформації. Ефективність використання цих коштів досягалася за рахунок концентрації інформації в певних місцях (спец. сховища, обчислювальні центри), що сприяло забезпеченню захисту відносно малими силами.

“Розподілення” інформації по місцях зберігання і обробки загострило ситуацію з її захистом. З'явилися дешеві персональні комп'ютери. Це дало можливість побудови мереж ЕОМ (локальних, глобальних, національних і транснаціональних), які можуть використовувати різні канали зв'язку. Ці чинники сприяють створенню високоефективних систем розвідки і отримання інформації. Вони знайшли відображення і на сучасних підприємствах [2].

Одним із основних законів України, який регламентує захист інформації є Закон України «Про захист інформації в автоматизованих системах», прийнятий постановою Верховної Ради України №81/94-ВР від 5 липня 1994 року. Основною метою являється забезпечення реалізації регулярного процесу на всіх етапах життєвого циклу систем обробки інформації. При цьому всі засоби, методи і заходи, які використовуються для ЗІ, найбільш раціональним чином об'єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

- з одного боку, забезпечення надійного захисту ідентифікації, що знаходиться в системі інформації: унеможливлення випадкового і навмисного отримання інформації сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації та обслуговуючого персоналу;
- з іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації досить складна, що вимагає для свого рішення не просто здійснення деякої сукупності наукових, науково-технічних і організаційних заходів і застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів і застосування комплексу спеціальних засобів і методів із ЗІ.

Якщо переглянути статистику з кібербезпеки, то можемо спостерігати зріст кількості інцидентів:

- у 2020 році було зафіксовано 1 120 витоків і кібератак. Про більшість цих інцидентів повідомляли провідні світові ЗМІ. В цілому 20 120 074 547 записів було зламано;
- кількість виявлених інцидентів, що сталися в другій половині 2020 року, свідчить про те, наскільки сильний вплив COVID-19 здійснив на організації. Більш того, кількість зламаних записів збільшилася на 50% у порівнянні з 2019 роком; [3]
- кількість витоків даних стабільна (зафіксовано 349), тоді як кількість кібератак сягнула позначки 771;
- 5.1 мільярдів записів персональних даних були скомпрометовані у 2021 році. Порушення даних, які були розкриті, становлять 1243 – збільшення на 11% порівняно з 2020 роком ;

Найбільш уразливі сектори, які зазнають порушення даних є охорона здоров'я (277 мільйонів порушень), персональні дані (263 мільйонів порушень), освіта (173 мільйонів порушень), технології та медіа сфера (157 мільйонів порушень). [4]

У сучасному становищі більшість працівників була вимушена перейти на дистанційну форму праці, учні/ студенти продовжували навчання в онлайн форматі. Спочатку на такі зміни вплинув COVID-19, а зараз воєнні дії на території України. Можемо підкреслити й той факт, що майже всі документи тепер зберігаються в додатку. Тобто, питання безпеки інформації є актуальним як ніколи.

1.2 Постановка задачі

На сьогоднішній день головною підставою для створення системи захисту інформації є забезпечення надійності ЗІ. Кожна система представлена у вигляді організованої сукупності об'єктів і суб'єктів, використовуваних методів і засобів захисту. Ці компоненти є складовою частиною системи, але їх також можна розглядати як окремі системи, що здійснюють захисні заходи.

СЗІ призначена для об'єднання всіх елементів у єдине ціле. Тобто функціонування кожного елементу захисту не повинно порушувати коректну роботу інших, зберігаючи логічний і технічний зв'язок. Розробка комплексної системи захисту, іншими словами системної, є найкращим рішенням цього питання.

Усі дії щодо КСЗІ регламентуються нормативно-правовими актами та нормативними документами із захисту інформації.

Далі наведені основні етапи створення КСЗІ:

1. Формування загальних вимог до КСЗІ в ІТС

На цьому етапі в загальному випадку виконується:

- аналіз нормативно-правових актів, на підставі яких можуть встановлюватися обмеження доступу до певних видів інформації або заборона такого обмеження, визначається необхідність забезпечення захисту інформації згідно з іншими критеріями;

- визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;
- оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.

При обстеженні ІТС розглядається як організаційно – технічна система, яка поєднує обчислювальну систему, фізичне середовище, середовище користувачів, оброблювану інформацію і технологію її обробки (далі – середовища функціонування ІТС)

Метою обстеження є опис кожного середовища функціонування ІТС та виявлення в них елементів, які безпосередньо або опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

2. Розробка політики безпеки інформації в ІТС

На цьому етапі розробник КСЗІ проводить детальне вивчення об'єкта, на якому створюється КСЗІ, уточнює моделі загроз, потенційного порушника та результати аналізу можливості керування ризиками, які виконані на попередніх етапах, а також виконує у разі необхідності додаткові науково-дослідні роботи, пов'язані з пошуком шляхів реалізації завдання на створення КСЗІ, оформлює і затверджує звіти з НДР, що виконувалися.

3. Розробка технічного завдання на створення КСЗІ

ТЗ на створення КСЗІ в ІТС є засадним організаційно-технічним документом, який визначає вимоги із захисту оброблюваної в ІТС інформації, порядок створення КСЗІ, порядок проведення всіх видів випробувань КСЗІ та введення її в експлуатацію в складі ІТС.

ТЗ на створення КСЗІ може розроблятися для вперше створюваних ІТС, а також під час модернізації вже існуючих ІТС.

4. Розробка проекту КСЗІ

Проект КСЗІ розробляється на підставі та у відповідності з Технічним завданням на створення ІТС і виконується на таких стадіях створення ІТС: ескізний проект, технічний проект, робоча документація.

Здійснюється розроблення, оформлення і затвердження завдань на проектування з суміжних питань, які пов’язані зі створенням КСЗІ або впливають на умови її функціонування (будівельні, електротехнічні, санітарно-технічні та інші підготовчі роботи).

5. Введення КСЗІ в дію та оцінка захищеності інформації в ІТС

6. Супроводження КСЗІ

Виконуються роботи з організаційного забезпечення функціонування КСЗІ та управління засобами захисту інформації відповідно до Плану захисту та експлуатаційної документації на компоненти КСЗІ, гарантійному і післягарантійному технічному обслуговуванню засобів захисту інформації. [5]

Не рекомендується приступати до створення системи за допомогою комплексного підходу до тих пір, поки не визначені такі її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. Як вхідні елементи виступають види загроз безпеки, можливі на даному об'єкті;
2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;
3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі сфер інших систем, які не підкоряються керівнику даного підприємства і не входять в сферу його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій із захисту інформації, переданої сигналами в кабельній лінії, що проходить територіями різних об'єктів. Як би не встановлювались межі системи, не можна ігнорувати її взаємодію з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися марними;

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати кращий варіант її побудови. Так, наприклад, мета, сформульована в найзагальнішому вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей. Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;
5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декілька варіантів побудови системи, що забезпечують задані цілі функціонування. Для того, щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісне оцінювання на всіх етапах створення системи [6].

Висновки за розділом 1

У даному розділі був описаний стан питання та поставлена задача роботи. Проаналізувавши вищевикладений матеріал, приходимо до важливості

застосовування системного підходу до побудови будь-якої системи. Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс протиріч вимог і характеристик.

Таким чином, з огляду на різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, цілі захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна інформація про об’єкт

Покровський міський центр зайнятості – установа, яка надає соціальні послуги громадянам України у місті Покровську.

Даний об’єкт є одним із відділів ДСЗ. Усі відділення ДСЗ працюють за єдиною схемою надання послуг. Клієнти можуть звернутися до будь-якого центру зайнятості та отримати всі передбачені законодавством соціальні послуги, пов’язані з працевлаштуванням. У ДСЗ створена уніфікована оперативна база вакансій, шукачів роботи та можливостей проходження професійного навчання по всій країні. Це дозволяє розширити зону пошуку роботи для безробітних не тільки в межах району чи області, а й держави в цілому.

Згідно НД ТЗІ 1.6-005-2013 «Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці» ОІД, який розглядається, встановлюється четверта (IV) категорія. Адже на об’єкті обробляється

технічними засобами та/або озвучується інформація з обмеженим доступом, яка не становить державну таємницю.

Керівником компанії була створена комісія для проведення обстеження в результаті якого був розроблений акт категоріювання, який наведений у Додатку Б. На підставі цього акту та з урахуванням проблем захисту інформації на об'єкті керівником було прийнято рішення по розробці КСЗІ. Наказ про створення КСЗІ наведений у Додатку В .

Середня кількість працівників у центрі зайнятості у Донецькій області складає 40 осіб. Середня кількість безробітних на одного працівника становить 58 осіб.

Водночас розподіл працівників на фронт-офіс (працівники, які безпосередньо контактують з клієнтом) та бек-офіс (менеджмент та адміністрація) у центрах зайнятості є відносно рівномірним. Так, кількість працівників фронт-офісу у трьох областях складає від 65% до 81% від загальної кількості персоналу. Це свідчить про те, у фокусі служби зайнятості — клієнт. Якщо говорити про навантаження персоналу у відділах сприяння працевлаштуванню, то в більшості випадків фахівці одночасно допомагають від 80 до 150 безробітним.

Досвід різних центрів зайнятості показує, що оптимальний показник для ефективної роботи — 100–120 безробітних осіб на одного фахівця. Розглядаючи відділи взаємодії з роботодавцями, простежується нерівномірний розподіл кількості підприємств для одного фахівця.

За спеціалістами можуть бути закріплені від 60 до 500+ роботодавців залежно від розміру міста та його економічної активності.

На рисунку 2.1 наведено організаційну структуру міського центру зайнятості.

2.2 Обстеження фізичного середовища

Об'єкт розташований у центрі міста у двоповерховій будівлі колишнього дитячого садку, яка має «Н» образну форму. Навпроти розташований військкомат, з одного боку межує з дитячим садком, а з іншого – з багатоповерховим будинком.

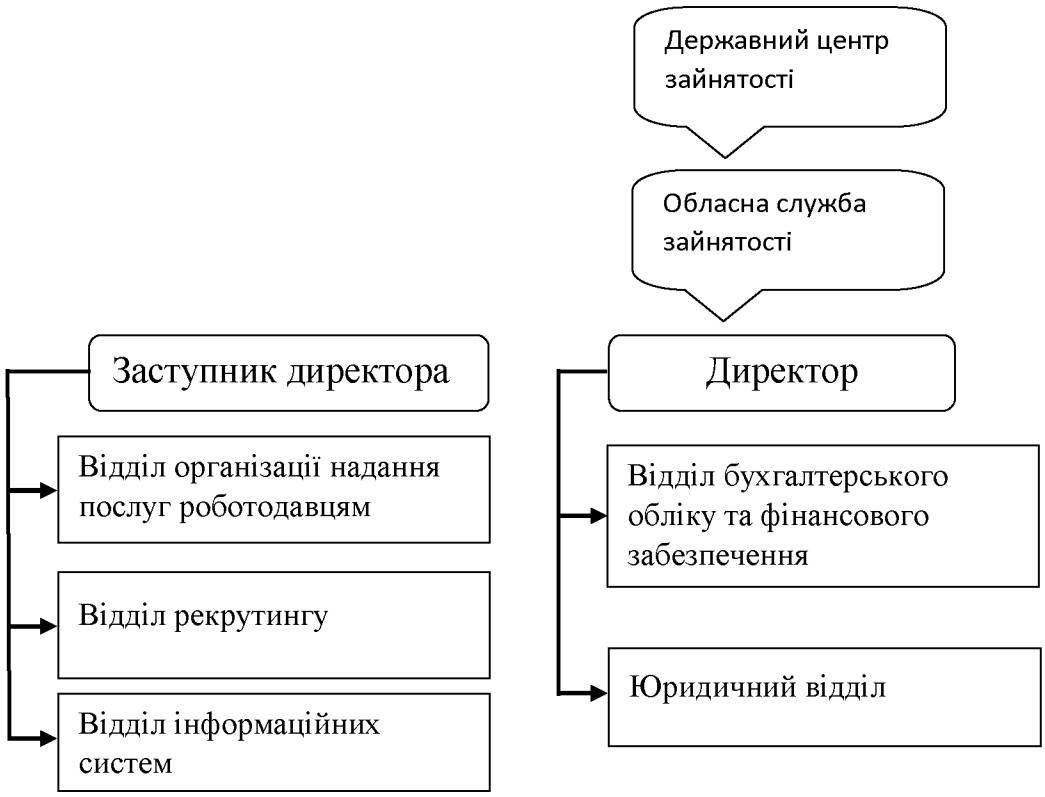


Рисунок 2.1. Структура міського центру зайнятості

Ситуаційний план зображено на рисунку 2.2.

Навколо будівлі наявний паркан, виконаний з металевих прутів заввишки 2 м. Прути розташовані на відстані 10 см один від одного. Територія навколо будівлі асфальтована і впорядкована. Передбачена парковка транспортних засобів уздовж суміжних/ прилеглих вулиць. По вулицях організований двонаправлений рух транспортних засобів середньої інтенсивності.

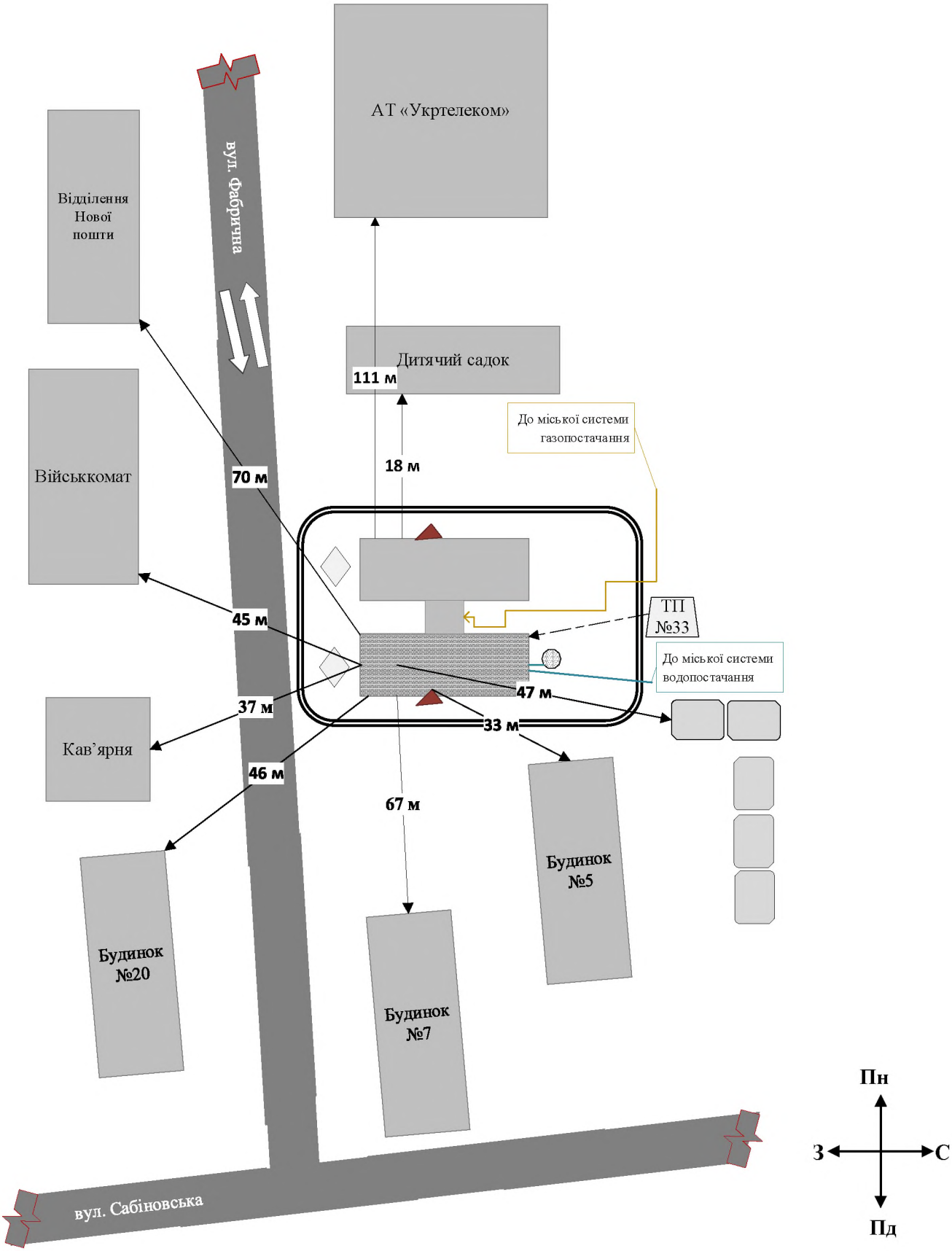
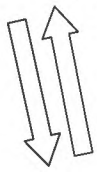


Рисунок 2.2. Ситуаційний план

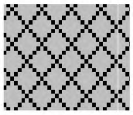
Умовні позначення ситуаційного плану:

дорога



напрямок руху транспортних засобів

будівля центру зайнятості



ОІД та межа КЗ

паркан

місце для паркування транспортного засобу

каналізаційний люк

трансформаторна підстанція (ТП)

споруда

гараж

Будівля виконана з силікатної цегли. Висота стель – 3 м, стінні перегородки товщиною 100 мм, стіни зовнішні – 300 мм.

На об’єкті встановлені металопластикові вікна з однокамерним склопакетом, який має два полотна скла. Полотна завтовшки 7 мм. Вікно поворотно-відкривного типу розміром 1400×1800 мм. Ззовні на вікнах встановлені металеві решітки: металеві прути у формі кіл діаметром 150 мм, які перетинаються між собою. Всередині на вікнах є вертикальні жалюзі, що виконують сонцезахисну роль.

Вхідні пластикові двері розміром 1200×2390мм з однією стулкою, що відкривається. Вхід у будівлю сконструйований з двох дверей, між ними утворюється маленький коридорчик довжиною 1500 мм, що відіграє термічну роль. Двері всередині будівлі виконані з металопластику та мають звичайні замки, що врізаються. Скло на дверях матове.

У будівлі є горище, вихід до якого обмежений інструкцією. Двері зачинені на навісний замок. Ключ, який відчиняє замок, знаходиться у охоронному пункті.

На об'єкті встановлена контрольована зона. Її межа проходить по контуру кабінетів. Будівля обладнана системами охоронної та пожежної сигналізацій. Центр уклав договір з охоронною фірмою. У робочий та неробочий час перепускний режим забезпечується централізованою охоронною сигналізацією. Після отримання сигналу на центральний пульт охоронна служба повинна зв'язатися з охоронником центру та дізнатися про деталі порушення. Після чого вирішується план наступних дій. Схема систем охоронної та пожежної сигналізації наведено на рисунку 2. 3.

Основні заходи контрольно-перепускного режиму розробляються фірмою та затверджуються керівником підприємства, оформлюються відповідним наказом та інструкцією про контрольно-перепускний режим. Фізичний доступ до апаратних засобів компонентів ІТС обмежено. Приміщення, в яких розміщуються відповідні засоби обладнані механічними замками.

У робочий час перепускний режим забезпечується фізичною охороною. Охоронці відпрацьовують добову зміну почергово. У кабінеті охорони знаходяться ключі від усіх кабінетів, які видаються під підпис працівникам. Об'єкт ставиться під охорону після того, коли останній працівник здасть ключ, тобто всі працівники залишать об'єкт.

Режим доступу до приміщень, у яких циркулює ІзОД, відповідає вимогам, які викладені у «Положенні про порядок користування носіями конфіденційної інформації». Дане Положення передбачає надання права безперешкодного доступу до таких приміщень лише персоналу ІТС, якому необхідно працювати із технічними

засобами, що розміщенні у цих приміщеннях. Доступ сторонніх осіб до цих приміщень здійснюється за умов присутності визначеного персоналу ІТС.

Унаслідок того що до об’єкту повинні мати доступ громадяни, тому турнікети та перепускні пункти відсутні. У інструкції прописані правила відвідування для громадян. Вони мають доступ до кабінетів, які розташовані на першому поверсі.

На ситуаційному плані зображено основні споруди, що розташовані поблизу, а також усі наявні комунікації.

Контур системи заземлення виконаний смугою від 40×4 із забиванням електродів із труб сталевих Ø32 мм. На підприємстві наявне захисне заземлення. Трипровідний провід підключений до щитка.

Лінії електропередачі (ЛЕП) системи електропостачання будівлі підключені до трансформаторної підстанції (ТП), яка виходить за межі КЗ. ЛЕП виконана кабелем АВВГ 3×95 + 1×70 – на підготовленому ліжку з піску та покритий кабель сигнальним листом. Щитова знаходиться у службовому приміщенні № 3, доступ до якого обмежений зачиненими дверями.

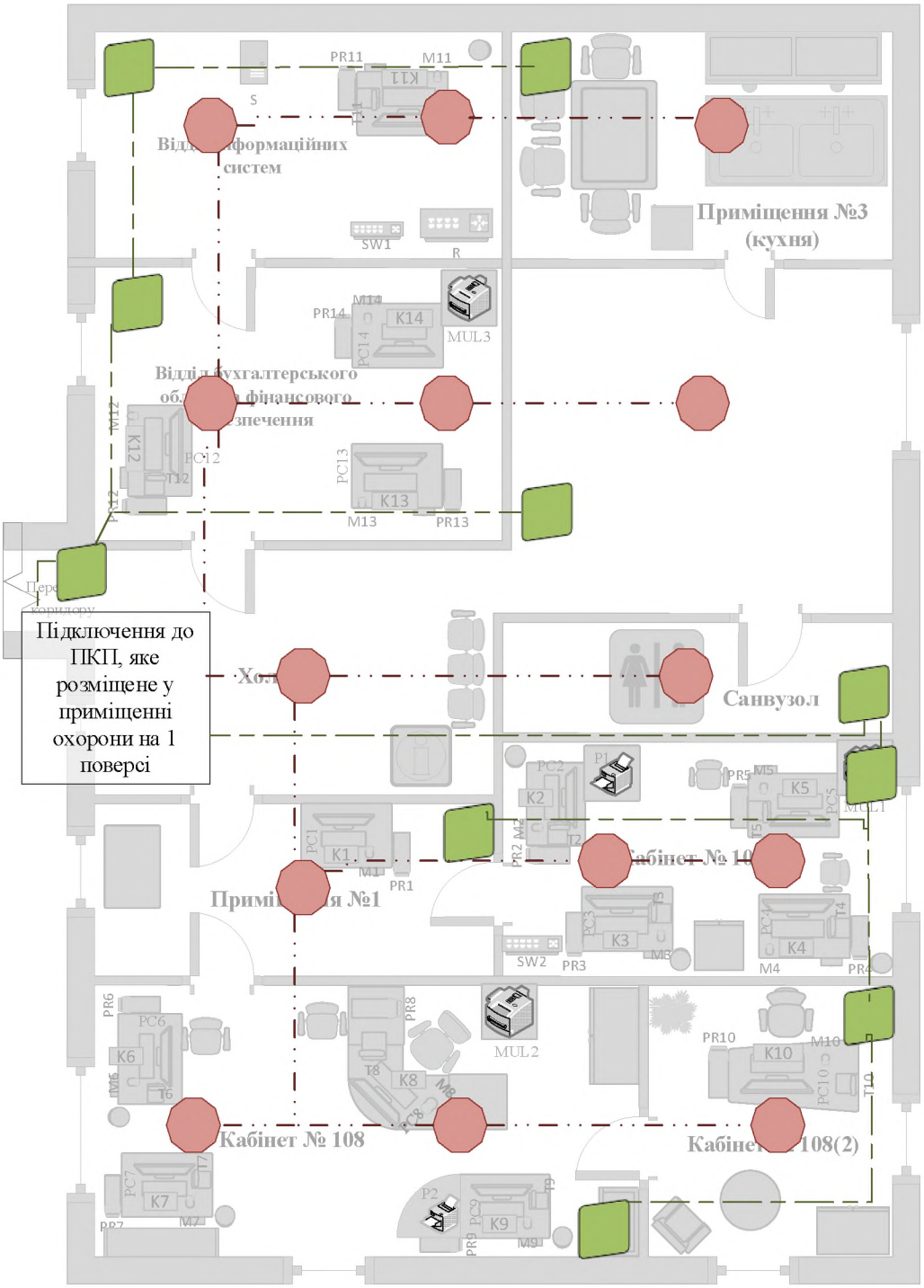


Рисунок 2.3. Схема систем охоронної та пожежної сигналізації

Умовні позначення схеми системи сигналізації:

пасивний ІЧ датчик руху системи охоронної сигналізації

димовий (пожежний) датчик системи пожежної сигналізації

Таблиця 2.1. – Найближчі об’єкти до ОІД

№	Призначення	Адреса	Кількість поверхів	Напрямок	Відстань до ОІД
1	Дитячий садок	вул. Фабрична, 3а	2	Північний	18 м
2	Житловий будинок №5	вул. Фабрична,5	10	Південно-східний	33 м
3	Кав’ярня «Feliz»	вул. Фабрична,18	1	Західний	37 м
4	Військкомат	вул. Фабрична,15	2	Західний	45 м
5	Житловий будинок №20	вул. Фабрична,20	10	Південно-західний	46 м
6	Гаражі мешканців будинків	вул. Чкалова	1	Східний	47 м
7	Житловий будинок №7	вул. Фабрична,7	10	Південний	67 м
8	Будівля відділення нової пошти	вул. Фабрична,13	1	Північно-західний	70 м
9	Будівля АТ «Укртелеком»	вул. Фабрична,1	4	Північний	111 м

Будівля підключена до міських систем водо- та газопостачання. Труби системи газопостачання проходять у повітрі із задньої сторони будівлі. Система водопостачання проведена під землею та має вихід труб на поверхню біля санвузлу. Відбувається подача тільки холодної води, але у будівлі присутні дві труби: для холодної та гарячої. Елементи систем водо- та газопостачання виходять за межі КЗ. Підведення системи газопостачання виконано для реалізації автономної системи опалення, яка має горизонтальну розводку. Батареї у кімнатах знаходяться під кожним вікном.

На генеральному плані вказано розташування основних та допоміжних технічних засобів і систем обробки інформації. Генеральний план ОІД наведений на рисунку 2.4.

Зовнішні стіни будівлі виконані із силікатної цегли, міжкімнатні стіні – з бетону. Металопластикові міжкімнатні двері встановлені на ОІД розміром 2050×950

мм. Двері одностворчасті та засклені. На дверях встановлені врізані одноточкові замки з роликовим засувом. У приміщеннях встановлені тристулкові металопластикові вікна, розміром 1700×1300 мм, з одним відкривним. Вікна мають однокамерний склопакет. Ззовні на вікнах встановлені металеві решітки. Вони виконані із кругів, які перетинаються, діаметром 300 мм. Усередині на вікнах наявні жалюзі з вертикальними планками шириною 127 мм. Карниз жалюзів виконаний із алюмінію, а планки – з тканини.

У приміщенні №1 розташоване робоче місце для відвідувачів, де вони мають змогу дізнатися актуальну інформацію щодо працевлаштування, написати або оформити власну заяву. У відділі інформаційних систем розташовані електричні щити системи електроживлення, яка наведена на рисунку 2.5.

Приміщення №2 є службовим, там розташована кухня для працівників центру зайнятості. Там розміщений холодильник, два рукомийника, підвісна шафа, стіл та стільці.

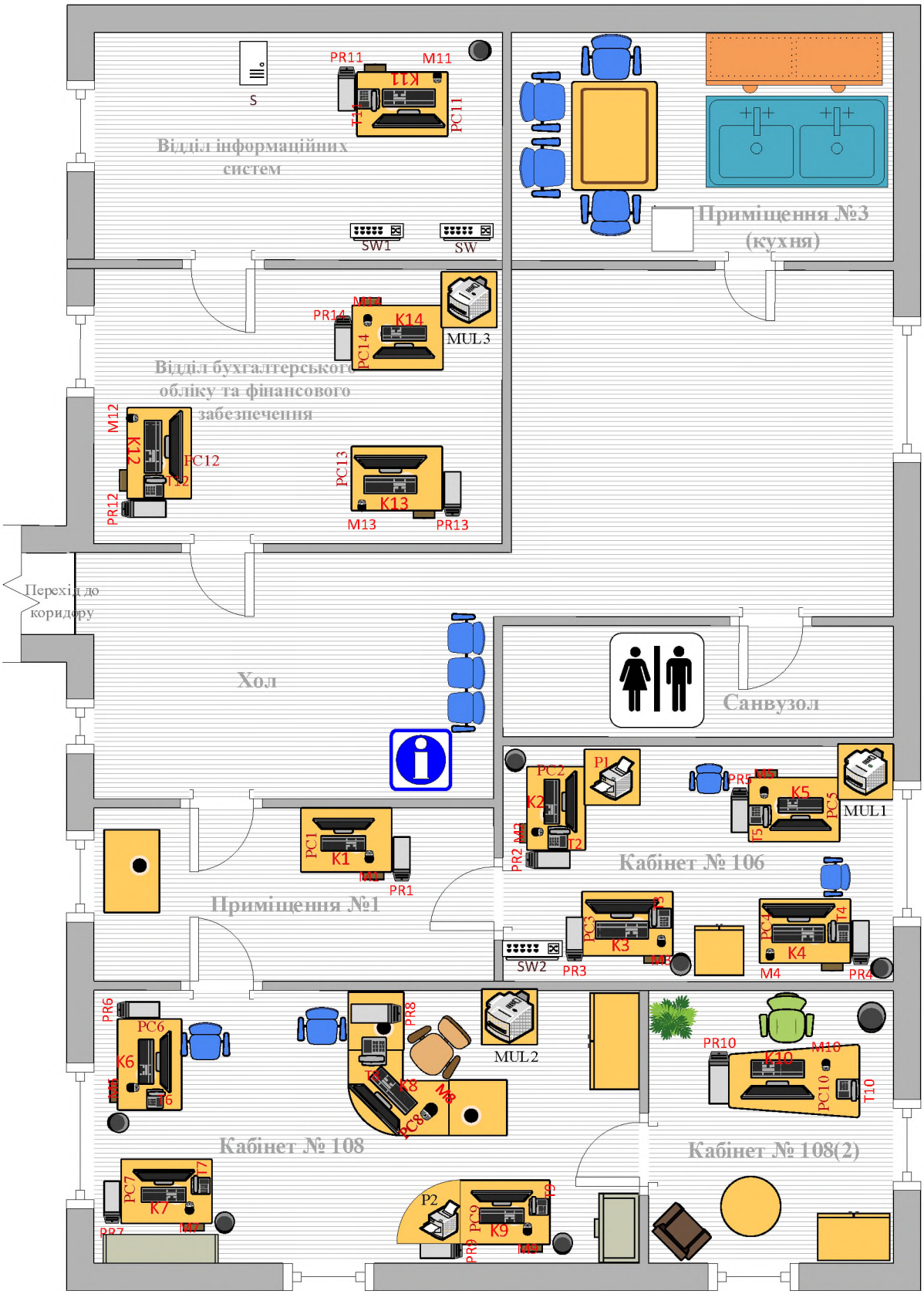


Рисунок 2.4. Генеральний план ОІД


офісний стіл


термінал (ПК)

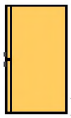

процесор

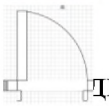

принтер


багатофункціональний пристрій


стаціонарний телефон


підвісна поличка

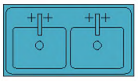

шафа


двері


вікно


інформаційний куточок для відвідувачів


холодильник


двосекційна мийка


місце розриву конструкції споруд


ОІД та межа КЗ


комутатор


сервер

Умовні позначення генерального плану ОІД:

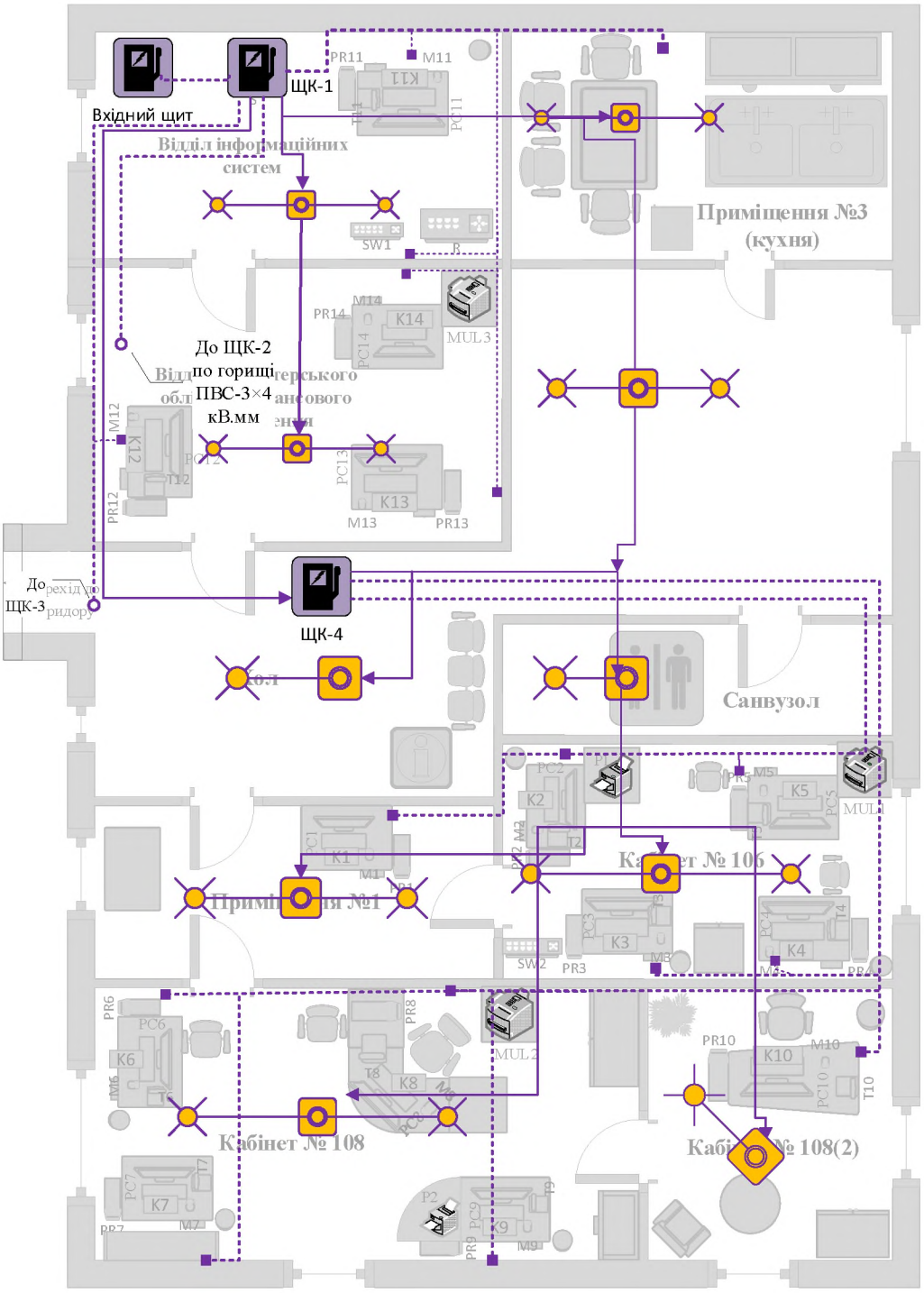
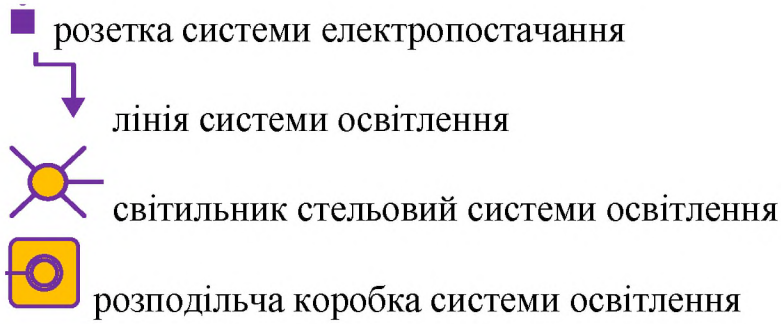


Рисунок 2.5. Схема систем електропостачання та освітлення ОІД

Умовні позначення схеми систем електропостачання та освітлення ОІД:

Електричний щит системи електроживлення

лінія електроживлення системи електропостачання



На рисунку зображено фрагмент системи освітлення об’єкту. Для розподілу електроенергії використано розподільні щити. Від вхідного електричного щитка проведено підключення до щитів 1 – 4. Щити 1 та 4 розташовані на першому поверсі та зображенні на рисунку 2.5. Щит №3 розташований на першому поверсі у протилежній стороні від щита №4. Щит №2 розташований на другому поверсі.

Для живлення ламп застосовується силовий провід з алюмінієвою струмопровідною жилою. Ізоляція виконана з ПВХ пластикату.

Світлодіодні світильники розміром 595×595×75 мм. Споживана потужність – 32 Вт, напруга мережі живлення – 170-264 В. У світильнику розміщено 4 світлодіодних лампи.

Таблиця 2.2. – Основні технічні засоби

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Монітор загального користування	Samsung E1920N	PC1	VOSP81GBC000056	На столі	5
Системний блок загального користування	Delux Dlc-mv860	PR1	CZCS3487BT	Під столом	5
Монітор штатного працівника	Samsung E1920N	PC2	AM67TB98700N58C	На столі	6
Системний блок	Delux Dlc-mv860	PR2	BVMN41748M	Під столом	6

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Монітор штатного працівника	Samsung E1920N	PC3	NT6373548GDY78I	На столі	5
Системний блок штатного працівника	Delux Dlc-mv860	PR3	54FG67BV23	Під столом	5
Монітор штатного працівника	Samsung E1920N	PC4	QA3THINF600053H	На столі	2
Системний блок штатного працівника	Delux Dlc-mv860	PR4	DGN244800M	Під столом	2
Монітор штатного працівника	Samsung E1920N	PC5	TR756HBV43795232	На столі	2
Системний блок штатного працівника	Delux Dlc-mv860	PR5	78TG5427J7	Під столом	2
Монітор штатного працівника	Samsung E1920N	PC6	RD42398JN0465H	На столі	1
Системний блок штатного працівника	Delux Dlc-mv860	PR6	54WS789N43	Під столом	1
Монітор штатного працівника	Samsung E1920N	PC7	AS457BT2356FD4	На столі	1
Системний блок штатного працівника	Delux Dlc-mv860	PR7	87AS6580VM	Під столом	1

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Монітор штатного працівника	Samsung E1920N	PC8	SK478972TG654398	На столі	4
Системний блок штатного працівника	Delux Dlc-mv860	PR8	23F568T5347	Під столом	4
Монітор штатного працівника	Samsung E1920N	PC9	AX467H74E3907765	На столі	2
Системний блок штатного працівника	Delux Dlc-mv860	PR9	23TR5684J9	Під столом	1
Монітор штатного працівника	Samsung E1920N	PC10	HT65Y34VB6532C78	На столі	3
Системний блок штатного працівника	Delux Dlc-mv860	PR10	98HN6348H6	Під столом	3
Монітор штатного працівника	Samsung E1920N	PC11	SD5677GH2248L09	На столі	2
Системний блок штатного	Delux Dlc-	PR11	32RF4679B6	Під столом	2

працівника	mv860				

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Монітор штатного працівника	Samsung E1920N	PC12	QW5428IB5637D65	На столі	2
Системний блок штатного працівника	Delux Dlc-mv860	PR12	78F535H65G	Під столом	2
Монітор штатного працівника	Samsung E1920N	PC13	KU764G4572F09Y	На столі	7
Системний блок штатного працівника	Delux Dlc-mv860	PR13	45FFH75330	Під столом	7
Монітор штатного працівника	Samsung E1920N	PC14	HY5459YC7563802	На столі	7
Системний блок штатного працівника	Delux Dlc-mv860	PR14	34F673B641	Під столом	7
Багатофункціональний пристрій	Canon i-SENSYS MF216N	MUL1	6B33GHM4968S69X	На окремому столі	1
Багатофункціональний пристрій	Canon i-SENSYS	MUL2	6B33GHM4968S69X	На окремому	5

	MF216N			столі	

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Багатофункціональний пристрій	Canon i-SENSYS MF216N	MUL3	6B33GHM4968S69X	На окремому столі	7
Принтер	HP LaserJet Pro M201dw	P1	54K8FCK945HFN4A	На окремому столі	6
Принтер	HP LaserJet Pro M201dw	P2	55K9GCK945HFN25	На окремому столі	1
Клавіатура загального користування	Delux DLK-3100	K1	79037F6748I6759B	На столі	5
Клавіатура штатного працівника	Delux DLK-6060UB	K2	394639B526749F5	На столі	7
Клавіатура штатного працівника	Delux DLK-6060UB	K3	2535869LD54800J	На столі	5
Клавіатура штатного працівника	Delux DLK-3100	K4	394639B526744H8	На столі	2

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Клавіатура штатного працівника	Delux DLK-6060UB	K5	394639B526745F1	На столі	2
Клавіатура штатного працівника	Delux DLK-6060UB	K6	394639B526742E5	На столі	1
Клавіатура штатного працівника	Delux DLK-3100	K7	2535869LD54845D	На столі	1
Клавіатура штатного працівника	Delux DLK-6060UB	K8	2535869LD5487YG	На столі	4
Клавіатура штатного працівника	Delux DLK-6060UB	K9	2535869LD5480LV	На столі	1
Клавіатура штатного працівника	Delux DLK-3100	K10	2535869LD54835D	На столі	3
Клавіатура штатного працівника	Delux DLK-6060UB	K11	2535869LD54827A	На столі	2
Клавіатура штатного	Delux DLK-	K12	394639B52674952	На столі	2

працівника	3100				

Продовження таблиці 2.2

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Клавіатура штатного працівника	Delux DLK-6060UB	K13	394639B526749J4	На столі	7
Клавіатура штатного працівника	Delux DLK-6060UB	K14	394639B52674L97	На столі	7
Сервер	ARTLINE Business T65	S	TR65HB34521	На підлозі	2
Комутатор	Hikvision DS-3E1105P-EI	SW	QXOY2DB606020	На стіні	5
Комутатор	D-link DES-1008D	SW1	12AC5600214	На стіні	5
Комутатор	D-link DES-1008D	SW2	15RG6389B46	На стіні	7

Відомості про системний блок:

- процесор: Intel® Celeron® CPU G1620 @2.70GHz;
- встановлена пам’ять (ОЗП): 4,00 ГБ;
- тип системи: 64-розрядна операційна система Windows, процесор x64;
- робоча група: CZ;
- наявні віртуальні носії інформації – це локальні диски C та D. На локальному диску C встановлено операційну систему і програми. На локальному диску D зберігаються створені текстові документи для особистого користування. Локальний диск D має розмір 368 Гб. Локальний диск C має розмір 6 Гб.

– У системі наявні мережеві пристрої. До них мають доступ усі члени мережі. Вони використовуються для швидкого обміну інформацією між працівниками.

Таблиця 2.3. – Допоміжні технічні засоби

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Комп'ютерна миша загального користування	A4tech N-70FX-1	M1	7GJ849502B57300	На столі	5
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M2	2WJ86548X065467	На столі	6
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M3	4FB47RCX6347452	На столі	5
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M4	5Y537C449NR572	На столі	2
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M5	6DHND4672892154	На столі	2
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M6	2F654268JN9977G7	На столі	1
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M7	8ST54378N5F6327	На столі	1
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M8	9IT64CD3562S357	На столі	4

Продовження таблиці 2.3

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M9	10TG54895R43N71	На столі	1
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M10	11TY68394VC32509	На столі	2
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M11	12WD458N5FR6432	На столі	1
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M12	13SVG568943G654	На столі	1
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M13	3EB6589IH654320	На столі	7
Комп'ютерна миша штатного працівника	A4tech G9-500FS	M14	5RG674328IK1234	На столі	7
Стаціонарний телефон	Panasonic KX-TS2350UAC	T2	4P85693JH5840ND	На столі	5
Стаціонарний телефон	Panasonic KX-TS2350UAC	T3	9B63840FYW389M5	На столі	4
Стаціонарний телефон	Panasonic KX-TS2350UAC	T4	8B6657F432D56M1	На столі	1
Стаціонарний телефон	Panasonic KX-TS2350UAC	T5	7B743DFG6123FD8	На столі	2

Продовження таблиці 2.3

Найменування	Модель	Позначення	Серійний номер	Розміщення	Відстань до межі ОІД, м
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т6	7BE321YH8749L09	На столі	1
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т7	8B436G789DE6587	На столі	2
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т8	8VRE58Y90431T54	На столі	5
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т9	8NH561278GH453S	На столі	1
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т10	8B54327F45DS890	На столі	1
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т11	8BG531F67854HJ7	На столі	1
Стаціонарний телефон	Panasonic KX-TS2350UAC	Т12	8B237L864F56730	На столі	1

2.3 Обстеження обчислювальної системи

Розмежування доступу до технічних засобів, на фізичному рівні, забезпечено організаційними заходами (відповідним обладнанням приміщень, в яких вони знаходяться).

ІТС відноситься до автоматизованих систем класу 3, згідно НД ТЗІ 2.5-005-99. Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

ІТС функціонує у режимі 24 години на добу, 7 днів на тиждень, за виключенням часу виконання технічних робіт з обслуговування компонентів ІТС.

На підприємстві наявні декілька каналів зв'язку. Підключення до мережі Інтернет виконано за допомогою оптоволоконного зв'язку, провайдером є АТ «Укртелеком». Також ця компанія надає послуги реалізації міні автоматичної телефонної станції (АТС). Міні – АТС забезпечує зв'язок між телефонами всередині підприємства, а також дає можливість виходу на комутовані телефонні мережі загального користування (ТМЗК). Для забезпечення швидкої, надійної та економічної передачі інформації в системі є виділений канал, провайдером якого є ПАТ «Доріс». Схема підключення до мережі наявна на рисунку 2.6.

Державний центр зайнятості є головним, тому від нього походить діяльність усіх підрозділів/ відділів. Центр зайнятості має єдину базу обміну інформацією. Усі дані мають бути синхронізованими та доступними для коректної роботи підрозділів/відділ.

У даній системі наявний сервер робочої групи. Сервер є окремим апаратно - програмним комплексом. У даній системі встановлено Windows Server 2003. Основними задачами сервера є забезпечення централізованого управління доступом до мережевих ресурсів і зберігання даних у локальній мережі на термін одного тижня (по вичерпанню терміну, усі дані повинні надсилатися до Державної єдиної бази).

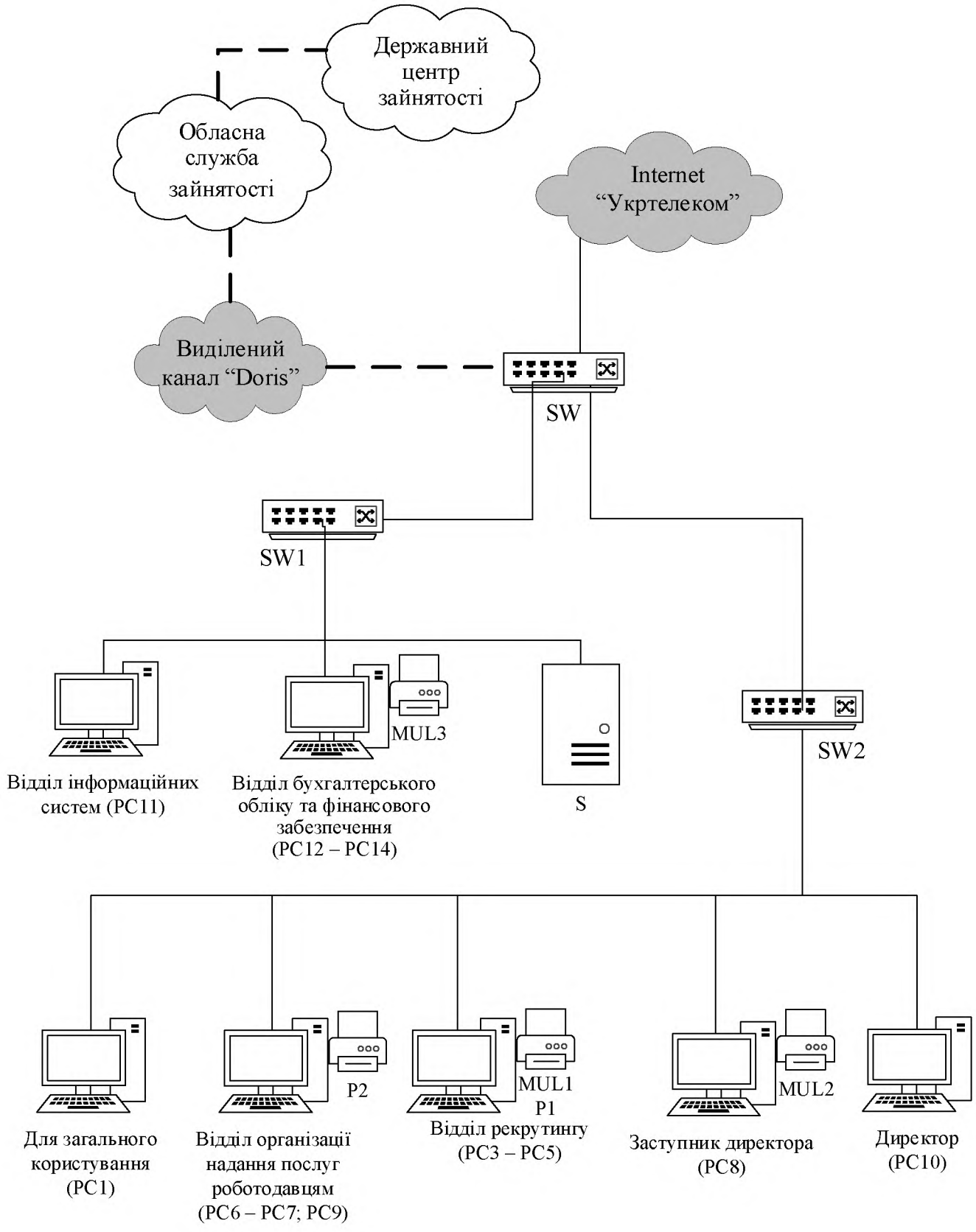


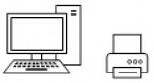
Рисунок 2.6. Схема підключення до мережі

Умовні позначення схеми системи підключення до мережі:

віддалена мережева структура підрозділу

інтернет/ виділений канал

мережевий комутатор



робоча станція

———— дротові лінії з’єднання локальної мережі

– – – – – лінії з’єднання мережі

За допомогою каналів зв’язку у рамках єдиної корпоративної мережі організовані наступні можливості:

- єдиний електронний документообіг;
- загальні архіви документів;
- дистанційний режим доступу до файлів, пристроїв друку, серверів з базами даних;
- сполучення обчислювальних мереж, у тому числі, що використовують різні мережеві протоколи;
- зв’язок для відеоконференцій;
- підключення до мережі Інтернет за виділеним каналом зв'язку;
- надання доступу до глобальних мереж даних, до фінансових торговельних та інформаційних систем;
- взаємодія між локальною обчислювальною мережею (ЛОМ) підрозділу та ЛОМ центрального офісу.

У службах зайнятості переважає індивідуальне використання ПЕОМ на робочому місті користувача для розв'язування локальних задач, що дає змогу реалізувати персональну технологію обробки даних. У той же час управління процесами зайнятості населення в районі/місті здійснюється шляхом оперативної взаємодії спеціалістів різних відділів центру зайнятості, у зв'язку з чим постає потреба колективного використання інформаційно-обчислювальних ресурсів. Наприклад, використання загальної бази облікових даних виключає дублювання, забезпечує оперативний пошук даних тощо. Тому для районних і міських (без районного поділу) центрів зайнятості доцільним є створення локальної мережі автоматизованих робочих місць їхніх фахівців з метою автоматизації розрахунків, пов'язаних з управлінням процесами зайнятості населення району. У такій мережі ефективно сполучаються можливості ПЕОМ для персональної обробки даних з перевагами розподіленої обробки даних, які забезпечують колективне використання загальних інформаційних ресурсів для управління процесами зайнятості населення.

У таблиці 2.4 наведені основні технічні засоби.

Таблиця 2.4. – Перелік основних технічних засобів

Найменування	Модель	Складова	Властивості
Монітор штатного працівника	Samsung E1920N	Діагональ	18.5”
		max роздільна здатність WXGA	1366x768
		Кут огляду горизонтальний	170°
		Споживна потужність у робочому режимі у режимі сну	20 Вт 0.3 Вт

Системний блок	Delux Dlc-mv860	Процесор	intel Core i5; 4 ядра; WD Caviar Blue 500 gb

Продовження таблиці 2.4

Найменування	Модель	Складова	Властивості
		Sockets	4 x 3,3 GHz 6MB;
		Материнська плата	lga Intel
		Оперативна пам'ять (RAM)	Data Technology;ddr3 2 x 2gb 1600 mhz
		Відеокарта	Intel igp 4500 series 128 up 1697 mb
		Жорсткий диск (HDD)	WD Caviar Blue 500 gb HDD sata 6 gb/s
Багатофункціональний пристрій	Canon i-SENSYS MF216N	Мережевий інтерфейс	Ethernet
		Інтерфейс USB	2.0
		max роздільна здатність друку	1200x1200 dpi
		Споживання потужності в робочому режимі	~ 500 Вт
Принтер	HP LaserJet Pro M201dw with Wi-Fi (CF456A)	Мережевий інтерфейс	Ethernet, Wi-Fi
		Інтерфейс	USB 2.0
		Мережева карта	Ethernet 10/100
		max роздільна здатність друку	600x600 dpi
		Споживання потужності в	~ 450 Вт

		робочому режимі	

Продовження таблиці 2.4

Найменування	Модель	Складова	Властивості
Комутатор	Hikvision DS-3E1105P-EI	Тип	Керований
		Тип портів Ethernet	4 x Fast Ethernet (10/100 Мбіт/с), 1 x SFP
		Метод комутації	Передача з проміжним зберіганням
		Протоколи PoE	IEEE 802. 3af, IEEE 802. 3at
		Пропускна здатність	1 Гб/с
Комутатор	D-link DES-1008D	Тип	Некерований
		Тип портів	8 x Fast Ethernet (10/100 Мбіт/с)
		Протокол	CSMA/CD
		Комутаційна матриця	1,6 Гбіт/с
		Швидкість фільтрації/передачі пакетів	Ethernet 14880 пакетів у с. на порт; Fast Ethernet 148 800 пакетів у сек. на порт
Сервер	ARTLINE Business	Процесор частота, GHz	AMD Ryzen 9 5900X 3,7

	T65	кількість ядер кількість процесорів встановлене/максимальне	12 1/1

Продовження таблиці 2.4

Найменування	Модель	Складова	Властивості
		Оперативна пам’ять Обсяг, ГБ Стандарт Максимальний обсяг, ГБ Тип слотів Кількість слотів	 64 DDR4-2666 ECC 128 UDIMM 4
		Жорсткий диск Обсяг, ГБ Інтерфейс	 2x2000 + 2x500 SATA
		Оснащення Вбудовані оптичні накопичувачі Зовнішні порти Кількість вільних PCI-Express слотів	 Немає 1 x UID Button/UID LED 2 x USB 3.2 Gen 1 1 x D-Sub 1 x COM port 2 x RJ-45 GbE LAN ports 1 x RJ-45 Mgmt LAN port 2 x PCI-E x16 1 x PCI-E x8 2xIntel I210AT + 1xMgmt

		Мережевий адаптер:	LAN
		Тип шасі	Tower

Таблиця 2.5. – Перелік програмного забезпечення

Найменування	Версія	Вид	Функціонування
Єдина інформаційно-аналітична система (ЄІАС) Державної служби зайнятості України «Інтегра-Флоу-16»	16	Прикладне спеціальне	PC2 - PC14
Мультимедійні мережеві пристрої	Windows Media Player Sharing; номер моделі 12.0	Прикладне загальне	PC2 - PC14
Операційна система Windows	Windows 8.1 Професійна ©Microsoft Corporation,2013. Усі права захищені	Системне	PC1 - PC14
Антивірус ESET Endpoint Security™	8.1.2037.9	Прикладне спеціальне	PC1 - PC14
Операційна система Windows	Microsoft Windows Server 2003	Системне	S
Офісний пакет додатків	Microsoft Office 2007	Прикладне загальне	PC1 - PC14
Драйвер для МФП та принтерів	3.6.290.1332	Прикладне загальне	PC2 - PC14

АРМ фахівця відділу працевлаштування, аналізу ринку праці та зайнятості створюється для автоматизації інформаційних процесів:

– обліку громадян, які шукають роботу, та безробітних громадян, які звертаються до центру зайнятості за консультаціями;

- обліку вакансій, тобто вільних робочих місць і вакантних посад;
- автоматизації процесів пошуку підходящої роботи, складання списків безробітних і формування наказів щодо надання їм відповідної матеріальної допомоги.

2.4 Обстеження інформаційного середовища

Порядок розповсюдження та використання програмних і технічних засобів визначаються ліцензійними умовами та дотримується.

Ідентифікація та автентифікація джерел отримання оновлень до програмного забезпечення, яке надходить до складу засобів захисту ІТС та встановлення цілісності таких оновлень здійснюється за умов підтвердження чинності сертифікату офіційного інформаційного ресурсу власника такого програмного забезпечення.

Інформація, яка обробляється в ІТС, являє собою сукупність інформаційних об'єктів у вигляді файлів та/або об'єктів баз даних, які обробляються і зберігаються в системі.

Інформаційне забезпечення АС з управління зайнятістю населення району/міста (як і будь-якої АС) складається з методичних та інструктивних матеріалів зі створення та функціонування АС, позамашинної та машинної інформаційних баз.

Під інформаційною базою системи при цьому розуміється сукупність певним чином упорядкованої інформації. Її організація ґрунтується на таких принципах:

- цілісності, тобто ІБ має задовольнити всі потреби користувачів;
- вірогідності (достовірності) — інформація, яка міститься в інформаційній базі має бути абсолютно точною і правдивою;
- захисту від несанкціонованого доступу до даних;
- стандартизації та уніфікації складових ІБ;
- мінімізації обсягів інформації, що вводиться і виводиться.

В якості інструктивних і методичних матеріалів при впровадженні автоматизації інформаційних процесів управління зайнятістю населення

використовуються Закон України «Про зайнятість населення», Кодекс законів про працю України, Інструкція про порядок реєстрації, перереєстрації і ведення обліку громадян, що шукають роботу, безробітних, Інструкція про порядок нарахування допомоги з безробіття тощо.

Зміст інформаційного забезпечення даної системи розглянемо на прикладі комплексу задач з обліку зайнятості населення району (розв'язується на АРМ фахівця та АРМ економіста відділу працевлаштування, аналізу ринку праці та статистики). Склад інформаційної бази комплексу задач з обліку зайнятості населення району/міста наведений на рисунку 2.7.

Позамашинна інформаційна база містить класифікатори техніко-економічної інформації, а також форми первинних і результатних документів з обліку безробітних району.

Автоматизоване розв'язування задач з обліку зайнятості населення передбачає використання таких первинних документів: паспорт, трудова книжка, звіт підприємства про наявність вільних робочих місць (вакантних посад), корінець направлення на роботу, звіт про звільнення робітників тощо.

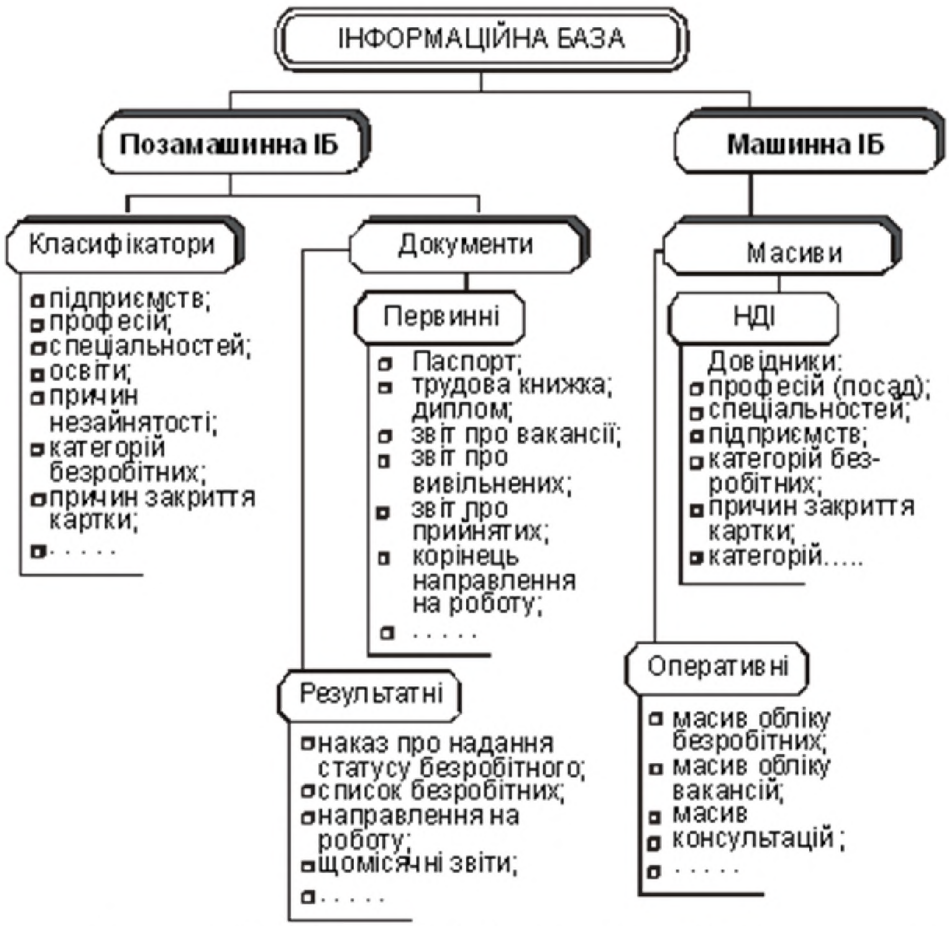


Рисунок 2.7. Складові інформаційної бази комплексу задач

Результатна інформація цього комплексу задач залежно від потреб користувачів подається у вигляді машинограм або відеокадрів. Це можуть бути: направлення на роботу; корінці направлень; накази: про присвоєння статусу безробітного і початку виплати допомоги з безробіття; про відстрочення виплати допомоги з обліку зайнятості населення; з безробіття, про припинення виплати допомоги з безробіття; список безробітних для нарахування допомоги тощо.

У процесі автоматизації розрахунків крім того використовуються класифікатори: загальнодержавні (підприємств, установ та організацій; професій і посад; спеціальностей; видів освіти; умов праці; систем оплати праці) та галузеві (причин закриття картки; причин незайнятості; характеру роботи; категорій безробітних; категорій квоти).

Машинна інформаційна база цього комплексу задач представлена масивами нормативно-довідкової, оперативної і результатної інформації, що зберігається.

Нормативно-довідкова інформація машинної інформаційної бази комплексу задач з обліку зайнятості населення району міститься в таких довідниках: професій, посад, спеціальностей, причин незайнятості, категорій квоти, видів освіти, причин закриття картки, підприємств, категорій безробітних, характерів роботи, умов роботи, оплати праці.

До оперативної інформації належать масиви обліку: безробітних, вакансій, консультацій, звільнених осіб, прийнятих осіб, направлень на роботу.

Основні види інформації, які циркулюють у відділах організації надання послуг роботодавцям та рекрутингу описані нижче.

Персональні дані про фізичну особу (INF_p): інформаційні об'єкти баз даних, що містять відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

До конфіденційної інформації про фізичну особу належать дані про:

- освіту;
- сімейний стан;
- стан здоров'я;
- адресу;
- дату і місце народження.

Дані про юридичну особу (INF_l) містяться у вигляді ЄДРПОУ і назви підприємства. Після внесення цих даних до бази Міністерства юстиції. У результаті запиту робітник отримує наступні дані:

- назва підприємства;
- директор;
- юридична та фактична адреса;
- контактні дані;
- сума уставного капіталу;
- дата заснування/відкриття/реєстрації;

- стан (діюче/ліквідоване/банкрут та інше);
- сфера діяльності.

Дані про трудову діяльність фізичних осіб (INF_w). Працівник вносить дані у базу даних з трудової книжки особи та її документів. Після робиться запит до Пенсійного фонду для підтвердження даних про трудову діяльність конкретної особи. До цих даних відносяться:

- дата працевлаштування та звільнення;
- назва підприємства працевлаштування та звільнення;
- посада працевлаштування та звільнення;
- номер приказу про прийняття на роботу;
- стаття звільнення.

Дані про організаційну діяльність підприємства (INF_o). Відносяться накази, розпорядження, оновлення/зміни законодавчої бази, оголошення про програми та заходи центрів зайнятості та державних установ міста.

До технологічної інформації відносяться (INF_t) дані про звітні дані щодо наявності працівників на робочих місцях і аудит робочих процесів за день, який підписується на початку робочого дня та по завершенню відповідальною особою відділу.

Таблиця 2.7. – Перелік інформації, яка циркулює в ІТС

Позначення виду	Режим доступу	Рівень доступу	Властивості захищеності інформації		
			К	Ц	Д
INF_p	Обмежений	Конфіденційна	+	+	+
INF_l	Обмежений	Конфіденційна	+	+	+
INF_w	Обмежений	Конфіденційна	+	+	
INF_o	Обмежений	Конфіденційна		+	+
INF_t	Обмежений	Конфіденційна		+	+

Інформація зберігається на паперових та електронних носіях (локальні диски, бази даних, мережеві віртуальні пристрої). Друкувати та копіювати документи можуть штатні працівники центру зайнятості. Кількість дозволених копій не нормована та не контролюється. Паперові носії зберігаються у теках на робочих місцях працівників і у шафах кабінетів. На підприємстві не передбачене використання персональних USB флеш-накопичувачів.

Для реєстрації вхідної та вихідної документації в системі електронного діловодства, роботи з роботодавцями та роботи з професійної підготовки, перепідготовки та підвищення кваліфікації використовується комп'ютерна програма «Інтегра-Флоу-2016». Цією системою обліку користуються відділи організації працевлаштування населення, відділ бухгалтерського обліку, відділ взаємодії з роботодавцями, відділи активної підтримки безробітних.

Система може повільніше функціонувати при завантаженні великої кількості документів та не розрахована на великі обсяги. Це одна із причин, чому у значній кількості центрів зайнятості документообіг дублюється в електронному та паперовому вигляді.

2.5 Обстеження середовища користувачів

Як структура, так і гранична чисельність працівників Державної служби зайнятості погоджуються міністерством, у підпорядкуванні якого перебуває служба зайнятості, та затверджуються директором Державного центру зайнятості.

У центрі зайнятості присутній відділ адміністрування. Тобто фізично відбувається контроль за встановленням, спостереженням, допомогою в обслуговуванні програмних і апаратних засобів. Адміністратор працює в окремому відділі та має рівень кваліфікації вище середнього.

У більшості центрів зайнятості плинність кадрів є невисокою, значна частина персоналу працює в центрах зайнятості понад 10 років. Кваліфікаційний рівень працівників центрів зайнятості є достатньо високим, оскільки ДСЗ вимагає володіння значною кількістю навичок для працевлаштування та подальшої роботи в

ДСЗ. Серед вимог працевлаштування в ДСЗ є наявність у кандидата повної вищої освіти відповідного до посадової інструкції напрямку підготовки за рівнями магістр та спеціаліст. Зазвичай це спеціальності в таких галузях, як соціальні та поведінкові науки, право, управління та адміністрування, соціальна робота. Від окремих працівників вимагається вища юридична або економічна освіта. Крім того, для працевлаштування на посаду галузевого фахівця із певною категорією є вимога конкретної кількості років професійного стажу. Для фахівців з питань зайнятості та фахівців вимогами є знання трудового законодавства України, основ організації праці та управління, основ психології, основ діловодства, основ етики, знання правил ділового етикету та спілкування, правил охорони праці та пожежної безпеки, володіння державною мовою, навички роботи на комп'ютері та знання відповідних програмних продуктів. Відбувається розвиток компетенцій персоналу, але чітка система та програма кар'єрного розвитку відсутня. Компетенції працівників ДСЗ наразі оцінити досить складно, адже в ДСЗ відсутня модель та системна програма оцінки компетенцій працівників різних рівнів, на основі яких можна було б зробити висновки.

Підвищення кваліфікації працівників ДСЗ здійснюється наступним чином: навчання за професійними програмами підвищення кваліфікації, короткострокове тематичне підвищення кваліфікації та стажування. Навчання для працівників центрів зайнятості різних рівнів компетенції відбувається регулярно, проте потребує покращення організації та структури програми навчання, а також створення системи вимірювання ефективності. Наразі підвищення кваліфікації персоналу відбувається один раз на п'ять років в Інституті підготовки кадрів Державної служби зайнятості України (але може і в інших навчальних закладах, відповідно до вимог законодавства України).

Також серед працівників присутні користувачі, які мають середній рівень користування програмними та апаратними засобами. Такі користувачі є слабкою ланкою ІТС.

Таблиця 2.8. – Розмежування доступу

Вид інформації / Користувачі	INF_p	INF_l	INF_w	INF_o	INF_t
Начальник відділу рекрутингу	R, W, E, P	R, W, E, P	R, W, P	R, W, P	R, P, E
Заступник начальника відділу рекрутингу	R, W, E, P	R, W, E, P	R, W, P	R, W, P	R, P
Фахівці відділу рекрутингу	R, W, E, P	R, W, E, P	R, W, P	R, P	R, P
Начальник відділу організації надання послуг роботодавцям	R, W, E, P	R, W, E, P	R, W, P	R, W, P	R, P
Заступник начальника відділу організації надання послуг роботодавцям	R, W, E, P	R, W, E, P	R, W, P	R, W, P	R, P, E
Фахівці відділу організації надання послуг роботодавцям	R, W, E, P	R, W, E, P	R, W, P	R, P	R, P

Позначення скорочень: R – читання, W – запис, E – редагування, P – друк.

2.6 Модель порушника

Модель порушника — це абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо [7]. Як порушник розглядається особа, яка може одержати несанкціонований доступ до роботи з включеними до складу ІТС засобами.

Перший критерій, за яким можна поділити усіх потенційних порушників, є відносно місця його перебування до ІТС: зовнішні та внутрішні.

Наведемо перелік потенційних порушників у таблиці, використовуючи оцінку рівня загрози за 4-бальною шкалою.

Таблиця 2.9. – Категорії порушників

Позначення	Категорія порушника	Оцінка загрози
Зовнішні порушники		
О1	Представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо)	1
О2	Відвідувачі центру зайнятості (представники організацій, громадяни, безробітні)	2
О3	Хакери	3
Внутрішні порушники		
І1	Технічний персонал, що обслуговує будівлю (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ до будівлі та приміщення, де розташовані компоненти ІТС)	1
І2	Користувачі (фахівці) системи	2
І3	Адміністратори системи (співробітники служби безпеки)	3
І4	Керівники різних рівнів та посадової ієрархії	4

Таблиця 2.10. – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушника	Оцінка загрози
М1	Безвідповідальність (цілеспрямовано або ненавмисно)	1
М2	Самоствердження	2
М3	Корисливий інтерес	3

Таблиця 2.11. – Специфікація моделі порушника за часом дії

Позначення	Характеристика часу	Оцінка загрози
Т1	До впровадження систем захисту інформації	1
Т2	У період неактивності системи (у неробочий час, під час планових перерв у її роботі, перерв для обслуговування та ремонтів і т.д.);	2
Т3	Під час функціонування системи	3
Т4	Під час як функціонування, так і не функціонування системи(окремих компонентів)	4

Таблиця 2.12. – Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії	Оцінка загрози
P1	Без доступу на контрольовану територію підприємства	1
P2	Усередині приміщень, але без доступу до технічних засобів	2
P3	З робочих місць користувачів (фахівців)	2
P4	З доступом до баз даних, архівів	3
P5	З доступом у зону керування засобами забезпечення безпеки	4

Таблиця 2.13. – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання системи захисту

Позначення	Характеристика можливостей	Оцінка загрози
C1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
C2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
C3	Використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які можуть бути приховано пронесені крізь охорону	3
C4	Використовує методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, перехоплення з каналів передачі даних, впровадження спеціальних програмних закладок)	4

Таблиця 2.14. – Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС

Позначення	Характеристика кваліфікації порушника	Оцінка загрози
K1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
K2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
K3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3

К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.15. – Модель порушника

Порушник	Мотив порушення	За часом дії	За місцем дії	Можливості порушника	Рівень кваліфікації	Сума загрози
О1	М1	Т2	Р2	С1	К1	8
1	1	2	2	1	1	
О2	М2 - М3	Т3	Р2	С1 - С2	К2	12-14
2	2 - 3	3	2	1 - 2	2	
О3	М2 - М3	Т4	Р1	С4	К3	17-18
3	2 - 3	4	1	4	3	
І1	М1	Т1-Т2	Р2	С1	К1	7-8
1	1	1 - 2	2	1	1	
І2	М1 - М3	Т3	Р3	С3	К2	13-15
2	1 - 3	3	2	3	2	
І3	М1 - М3	Т4	Р5	С3	К4	19-21
3	1 - 3	4	4	3	4	
І4	М1 - М2	Т3	Р4	С3	К2	16-17
4	1 - 2	3	3	3	2	

Проаналізувавши суми можливості виникнення загроз від певної категорії потенційних порушників, можна зробити наступні висновки:

1. найменш вірогідна категорія зовнішніх порушників – представники організацій, взаємодіючих з питань забезпечення систем життєдіяльності організації (енерго-, водо-, теплопостачання тощо). А найменш вірогідна категорія внутрішніх порушників – технічний персонал з обслуговування будівлі. Сума їх загроз становить ~ 8 балів.
2. найбільш вірогідна – адміністратори системи та співробітники служби безпеки. Це було очікувано, адже саме ці працівники мають привілейовані права в системі, тобто для цієї категорії мають бути застосовані додаткові контрольовані заходи.

2.7 Модель загроз

Моделювання загроз застосовується до широкого спектру систем організації, включаючи бізнес-процеси, інформаційні системи, мережеву інфраструктуру, розподілені підсистеми, додатки і сервіси, програмний код і т.д.

Процес моделювання загроз може виконуватися на будь-якій стадії розробки, але рекомендовано розпочинати на ранній стадії, щоб результати могли допомогти при розробці проекту і скоротити витрати.

Можемо означити моделювання загрози як метод, який використовується для розробки моделі шляхом ітеративної оцінки вразливостей. Зауважимо, що ця модель допомагає виявляти, повідомляти і розуміти загрози та заходи щодо їх зниження в контексті захисту критичних ресурсів.

Адекватні моделі загроз інформаційній безпеці дозволяють виявити існуючі загрози, розробити ефективні контрзаходи, підвищивши тим самим рівень інформаційної безпеки, і оптимізувати витрати на захист, сфокусувавши її на актуальних загрозах.

Інформація для свого існування завжди вимагає наявності носія. Носієм інформації може виступати поле або речовина. У деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

При аналізі проблеми захисту від НСД інформації, яка може циркулювати в КС, як правило, розглядаються лише інформаційні об'єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об'єктами) безвідносно до фізичних характеристик їх носіїв.

Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати:

– об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. і.) чи відмова елементів ОС;

– суб'єктивну природу, наприклад, помилки персоналу чи дії зловмисника. Загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними. [8]

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.

Навмисне походження загроз обумовлюється зловмисними діями людей.

Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації.

I. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.
II. Інформація зберігає цілісність, якщо дотримуються встановлені правила її модифікації (видалення).
III. Інформація зберігає доступність, якщо зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу.

Загрози, реалізація яких призводить до втрати інформацією якої-небудь з названих властивостей, відповідно є загрозами конфіденційності, цілісності або доступності інформації. [8]

На основі розробленої моделі порушника та класифікацію загроз можемо створити модель загроз ІТС Покровського МЦЗ, яка наведена в таблиці 2.16.

Таблиця 2.16. – Модель загроз

Вид загрози	Механізм реалізації загрози	Джерело загрози	Ризик для
Надзвичайна ситуація	Природне походження (пожежа, техногенні аварії)	Зовнішнє середовище	Ц, Д

Крадіжка	Викрадення носія ІзОД з метою несанкціонованого ознайомлення третіх осіб	Зловмисник	К, Ц, Д

Продовження таблиці 2.16

Вид загрози	Механізм реалізації загрози	Джерело загрози	Ризик для
Відмова в обслуговуванні	Пошкодження або виведення з ладу інформаційно-телекомунікаційної системи	Працівники, зловмисники, спеціальні програми	Д
Порушення нормального режиму роботи	Зараження системи комп'ютерними вірусами через відсутність контролю використання зовнішніх носіїв	Користувачі системи	Ц, Д
Відмова в доступі	Навмисне пошкодження парольних носіїв	Користувачі системи, зловмисники	Д
Недоліки	Помилки в роботі ПЗ системи	Розробник (постачальник), зловмисник	К, Ц, Д
Недоліки	Помилки під час конфігурації, використання та підключення засобів захисту (програми попередження атак, міжмережеві екрани)	Працівники, апаратно-програмні комплекси	К, Ц, Д
Недоліки	Виведення з ладу або порушення режиму роботи серверу робочої	ПЗ, зловмисник	Ц, Д

	групи		
Недолік своєчасного оновлення ПЗ	При відсутності останніх версій ОС та ПЗ неможливе протистояння сучасним загрозам	Зловмисник	Ц, Д

Продовження таблиці 2.16

Вид загрози	Механізм реалізації загрози	Джерело загрози	Ризик для
Підміна	Несанкціонована зміна інформації клієнтів у базах даних через недобросовісне виконання обов'язків або відсутності політики блокування клавіатури (облікового запису)	Працівники, зловмисники	Ц
Недостатня комп'ютерна грамотність	Помилкові дії персоналу через непоінформованість (неправильний запуск програм, некоректна модифікація даних у системі, виконання дій «за шаблоном»)	Працівники	К, Ц, Д
Помилки адміністраторів	Неправильне або ненавмисні помилки конфігурування системи захисту/ ОС	Адміністратори системи	К, Ц, Д
Шахрайство	Розголошення інформації клієнтів (копіювання ІзОД на зовнішні носії з метою несанкціонованого ознайомлення через нерегламентований доступ до	Працівники	К, Ц

	документів і їх друку), модифікація обладнання, підбір даних для аутентифікації в системі		

Аналіз можливих типових загроз в ІТС дає можливість визначити ключові ризики інформаційної безпеки, сформулювати подальшу методологію системи оцінки ризиків і визначення необхідних заходів щодо створення відповідної моделі захисту для системи.

2.8 Обрання профілю захищеності ІТС

У даній системі вразливими є всі властивості інформації: конфіденційність, цілісність і доступність. Тому слід приділити увагу на профілі захищеності, в яких підвищені критерії захищеності до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Згідно здійсненого обстеження ІТС відноситься до третього класу систем.

Пропонуємо обрати один із стандартних функціональних профілів захищеності оброблювальної інформації від несанкціонованого доступу, який буде задовольняти існуючі потреби. Згідно НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні профілі захищеності оброблювальної інформації від несанкціонованого доступу», оберемо профіль «3.КЦД.3».

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. Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об’єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта. КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену,

визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити — конкретних користувачів і/або групи користувачів, які мають право ініціювати процес.

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

НЕОБХІДНІ УМОВИ: НИ-1

КА-2. Базова адміністративна конфіденційність. Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

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

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

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

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

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

НЕОБХІДНІ УМОВИ: НО-1, НИ-1

КО-1. Повторне використання об'єктів. Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

НЕОБХІДНІ УМОВИ: НЕМАЄ

КК-1. Виявлення прихованих каналів. Повинен бути виконаний аналіз прихованих каналів. Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані.

Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів.

Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність.

НЕОБХІДНІ УМОВИ: КО-1, Г-3

КВ-3. Повна конфіденційність при обміні. Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів.

Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що

використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності.

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

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

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

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

Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника.

НЕОБХІДНІ УМОВИ: НО-1, НВ-1

ЦД-1. Мінімальна довірча цілісність. Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

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

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

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

НЕОБХІДНІ УМОВИ: НИ-1

ЦА-3. Повна адміністративна цілісність. Політика адміністративної цілісності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об’єкта.

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

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси (і групи процесів), які мають, а також тих, які не мають права модифікувати об'єкт.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес.

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

НЕОБХІДНІ УМОВИ: КО-1, НО-1, НИ-1

ЦО-2. Повний відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити всі операції, виконані над захищеним об'єктом за певний проміжок часу.

НЕОБХІДНІ УМОВИ: НИ-1

ЦВ-2. Базова цілісність при обміні. 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.

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

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

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

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

НЕОБХІДНІ УМОВИ: НО-1

ДР-2. Недопущення захоплення ресурсів. Політика використання ресурсів, що реалізується КЗЗ, повинна відноситися до всіх об’єктів КС.

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.

Повинна існувати можливість встановлювати обмеження таким чином, щоб КЗЗ мав можливість запобігти діям, які можуть призвести до неможливості доступу інших користувачів до функцій КЗЗ або захищених об'єктів. КЗЗ повинен контролювати такі дії, здійснювані з боку окремого користувача.

НЕОБХІДНІ УМОВИ: НО-1

ДС-1. Стійкість при обмежених відмовах. Розробник повинен провести аналіз відмов компонентів КС.

Політика стійкості до відмов, що реалізується КЗЗ, повинна визначати множину компонентів КС, до яких вона відноситься, і типи їх відмов, після яких КС в змозі продовжувати функціонування.

Повинні бути чітко вказані рівні відмов, при перевищенні яких відмови призводять до зниження характеристик обслуговування або недоступності послуги.

Відмова одного захищеного компонента не повинна призводити до недоступності всіх послуг, а має в гіршому випадку проявлятися в зниженні характеристик обслуговування.

КЗЗ повинен бути спроможний повідомити адміністратора про відмову будь-якого захищеного компонента.

НЕОБХІДНІ УМОВИ: НО-1

ДЗ-1. Модернізація. Політика гарячої заміни, що реалізується КЗЗ, повинна визначати політику проведення модернізації КС.

Адміністратор або користувачі, яким надані відповідні повноваження, повинні мати можливість провести модернізацію (upgrade) КС. Модернізація КС не повинна призводити до необхідності ще раз проводити інсталяцію КС або до переривання виконання КЗЗ функцій захисту.

НЕОБХІДНІ УМОВИ: НО-1

ДВ-2. Автоматизоване відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ має бути здатним визначити, чи можуть бути використані автоматизовані процедури для повернення

КС до нормального функціонування безпечним чином. Якщо такі процедури можуть бути використані, то КЗЗ має бути здатним виконати їх і повернути КС до нормального функціонування.

Якщо автоматизовані процедури не можуть бути використані, то КЗЗ повинен перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

НЕОБХІДНІ УМОВИ: НО-1

НР-3. Сигналізація про небезпеку. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

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

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

КЗЗ має бути здатним контролювати одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки КС. КЗЗ має бути здатним негайно інформувати адміністратора про перевищення порогів безпеки і, якщо реєстраційні небезпечні події повторюються, здійснити неруйнівні дії щодо припинення повторення цих подій.

НЕОБХІДНІ УМОВИ: НИ-1, НО-1

НИ-2. Одиночна ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

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

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

НЕОБХІДНІ УМОВИ: НК-1

НК-1. Однонаправлений достовірний канал. 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.

НЕОБХІДНІ УМОВИ: НЕМАЄ

НО-2. Розподіл обов’язків адміністраторів. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

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

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

НЕОБХІДНІ УМОВИ: НИ-1

НЦ-3. КЗЗ з функціями диспетчера доступу. 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.

КЗЗ повинен гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НЕОБХІДНІ УМОВИ: НЕМАЄ

НТ-2. Самотестування при старті. 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.

НЕОБХІДНІ УМОВИ: НО-1

НВ-2. Автентифікація джерела даних. 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.

КЗЗ повинен використовувати захищені механізми для встановлення джерела кожного об'єкта, що експортується та імпортується.

НЕОБХІДНІ УМОВИ: НЕМАЄ [9]

2.9 Розробка програмно-технічних методів захисту інформації

На першому кроці обираємо модель комутатору мережі призначеного для взаємодії пристроїв та керування трафіком у мережі. Він повинен забезпечувати надійні та якісні сервіси для постійно зростаючого трафіку. Керований комутатор повинен мати 2 оптичні порти (SFP) для підключення до мережі та 4 мідні порти (RJ45) для під'єднання комутаторів. Некеровані комутатори повинні мати 16 мідних порти (RJ-45). Швидкість передачі даних повинна становити 1000 Мбіт/с. Звертаючись до експертних висновків згідно переліку засобів ТЗІ від Держспецзв'язку розглянемо декілька варіантів комутаторів. У таблицях 2.17 та 2.18 наведемо порівняльні характеристики властивостей комутаторів.

Таблиця 2.17 – Порівняльна характеристика керованих комутаторів

	Cisco Catalyst Express 500-24TT	Edge-core ECS4120-28F	HUAWEI S5720-28P-SI-AC 02350DLN
Кількість портів Fast Ethernet (10/100)	24	немає	немає
Кількість портів Gigabit Ethernet (10/100/1000)	2	немає	24
Кількість портів SFP	немає	20	4
Інші порти	немає	4х комбо Gigabit Ethernet / SFP, 2х RJ-45 (консоль)	2х RJ-45 (консоль), 1х USB
Живлення	мережа	AC 100-240 В	AC 100-240 В

	Cisco Catalyst Express 500-24TT	Edge-core ECS4120-28F	HUAWEI S5720-28P-SI-AC 02350DLN
Моніторинг та конфігурування	DHCP-сервер	Web-інтерфейс	Web-інтерфейс, Telnet, Firewall, DHCP-сервер, DHCP-клієнт
Вартість	~13 800 грн	~ 21 350 грн	~ 32 400 грн

Таблиця 2.18– Порівняльна характеристика некерованих комутаторів

	HUAWEI S2700-9TP-PWR-EI	Cisco SG350-10-K9-EU	TP-Link SG1016PE
Кількість портів Fast Ethernet (10/100)	немає	8	немає
Кількість портів Gigabit Ethernet (10/100/1000)	8	Немає	16 портів з автопогодженням, авто-MDI / MDIX (роз'ємом RJ45)
Інші порти	1xSFP	2x GE combo, USB	немає
Живлення	AC 100-240 В, 50-60 Гц	AC 120-230 В, 50-60 Гц	AC 100-240 В, 50-60 Гц
Моніторинг та конфігурування	Web-інтерфейс, Telnet, SNMP	WEB-інтерфейс, SNMP Manager, IEEE 802.3	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.1q, IEEE 802.1p

	HUAWEI S2700-9TP-PWR-EI	Cisco SG350-10-K9-EU	TP-Link SG1016PE
		Ethernet MIB	
Додаткові функції	-	-	IGMP Snooping V1/V2/V3 Агрегування каналів Віддзеркалення порту Діагностика кабелю Виявлення петель
Вартість	~ 21 300 грн	~ 8 620 грн	~ 7 100 грн

За отриманими результатами можна виділити комутатори виробництва компанії Huawei Technologies Co.Ltd та TP-LINK Technologies CO., LTD. Це ідеальні рішення для малих і середніх підприємств. Обираючи серед великої кількості варіантів звернулися до експертних висновків згідно переліку засобів ТЗІ від Держспецзв'язку. Комутатор HUAWEI S5720-28P-SI-AC 02350DLN відповідає вимогам нормативних документів системи технічного захисту інформації в Україні, це підтверджує експертний висновок № 1011 (дійсний з 21.08.2019 до 21.08.2022). На жаль некеровані комутатори не затверджені експертними висновками, але порівнюючи характеристики моделей комутаторів, можна виділити більш надійні варіанти. Комутатор TP-Link SG1016PE є кращим рішенням для даної ІТС.

Впровадження у систему гігабітних комутаторів дозволить вирішити проблеми швидкості та надійності передачі даних. Дане рішення задовольнить наступні критерії профілю захищеності:

- КК-1. Можливий ефективний моніторинг мережі завдяки функції віддзеркаленню порту;
- КВ-3. Конфіденційність при обміні залежить від якості підключення як робочих станцій у локальній мережі, так і від якості підключення до глобальних мереж;

- НВ-2. Завдяки більш швидкому з'єднанню критерій автентифікації джерела даних виконується швидше, надійніше;
- ДС-1. Стійкість при відмові одного із захищених компонентів системи не призводить до повної відмови системи.

Для даної системи актуальні впровадження нових версій програмного забезпечення. Ці версії програм зможуть конкурувати з вразливостями з використанням останніх методик і технологій. Обираючи надійні рішення, звернемо увагу на експертні висновки №1027, №10190 та №1025 згідно переліку засобів ТЗІ від Держспецзв'язку. Пропозиція щодо оновлення ОС та програмного продукту Microsoft Office:

1. Операційна система Microsoft Windows 10 Professional виробництва компанії «Microsoft Corporation» (США);
2. Операційна система Microsoft Windows Server 2019 виробництва компанії «Microsoft Corporation» (США);
3. Програмний продукт Microsoft Office 2019 Standard виробництва компанії Microsoft Corporation» (США).

За допомогою новітніх програмних рішень Microsoft можливе виявлення нових вразливостей та запобігання загроз, які можливі через ці вразливості. З'являється можливість підтримки усіх нових послуг та забезпечення якісної роботи користувачів. Також задовольняє критерії ДЗ-1 (модернізації системи), КО-1 (за допомогою нових програмних рішень можливі перевірка та очищення об'єктів КС).

Зауважимо що в ІС використовується програмний продукт антивірусного захисту ESET Endpoint Antivirus для Windows однією з останніх версій. Це є вимогою до впровадження від головного підрозділу з захисту інформації. Із переваг можна виділити завчасне виявлення та очищення більшої кількості відомих і невідомих вірусів, черв'яків і т. ін; регулярне оновлення бази сигнатур вірусів, аналіз змісту мережевого трафіку та працює захист від мережевих атак. Задовольняє критеріям профілю захищеності ІТС:

- КК-1. Можливість моніторингу комп'ютера за допомогою монітора ресурсів, проведення аналізу системи;
- НР-3. Сигналізує про небезпеку та запобігає втраті даних, виявляє складні загрози та захищає від різного роду атак;
- НТ-2. Самотестування реалізоване система запобігання вторгненням (здійснюється моніторинг активності системи), наявний розширений сканер пам'яті (відстежує поведінку шкідливого процесу та сканує його.).

Втілення новітніх програмних продуктів буде малоефективним без забезпечення достатнім рівнем кваліфікації користувачів системи. Політики безпеки користувачів і адміністраторів повинні містити чіткі правила щодо можливостей у системі. Задля відповідності критерію НО-2 (Розподіл обов'язків адміністратора) пропонуємо виділити двох адміністраторів: системного та адміністратора безпеки. Обмеженими правами системного адміністратора є заборона інсталяції ПЗ без схвалення адміністратора безпеки, заборона зміни журналу безпеки. Адміністратор безпеки у свою чергу переймає на себе обов'язки створення паролів, ведення аудиту безпеки, перевіряти журнали безпеки на регулярній основі, а також під час незвичних подій у системі.

Заборона використання носіїв інформації є актуальною з приводу того, що вся інформація синхронізується з державною установою через мережу Інтернет, а користувачі системи працюють в єдиній локальній мережі. З цих причин користуватися носіями інформації є недоцільним, а також за таких умов зникне потенційне джерело загроз від витоку інформації.

У зв'язку зі специфікою оброблювальної інформації в ІТС, загрози наведені у таблиці 2.16 можливо мінімізувати завдяки застосуванню вище наведених засобів захисту.

Висновки за розділом 2

У даному розділі було проведено обстеження та опис кожного середовища функціонування ІТС. Завдяки повному аналізу ІТС з'явилась можливість для аналізу потенційних порушників, у результаті була створена модель порушника та модель загроз для ІТС підприємства.

У цьому розділі запропоновано програмні та апаратні засоби захисту інформації, які зможуть оптимізувати та покращити роботу системи в цілому.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Впровадження комплексної системи захисту інформації є не простим та іноді дорогим процесом. Після етапів обстеження середовищ функціонування інформації в ІТС, необхідно розглянути запропоновані методи і засоби захисту інформації з економічного аспекту.

Метою виконання економічного розділу є техніко-економічне обґрунтування доцільності впровадження запропонованих методів захисту інформації міського центру зайнятості. Для досягнення поставленої мети даної кваліфікаційної роботи та обґрунтування економічної доцільності впровадження КСЗІ, необхідно розрахувати наступні показники:

1. капітальні витрати;
2. експлуатаційні витрати;
3. річний економічний ефект.

Загальна інформація про об'єкт наведена у розділі 2.1. У таблиці 3.1 наведені проектні засоби і рішення, які були запропоновані.

Таблиця 3.1 – Проектні рішення кваліфікаційної роботи

Вид	Опис	Витрати
Модернізація комутаторів системи	Закупівля та налаштування комутаторів мережі HUAWEI S5720-28P-SI-AC 02350DLN, 2 × TP-Link SG1016PE	46 600 грн
Оновлення	Встановлення ОС Microsoft Windows 10	2 500 грн

операційних систем і програмних продуктів	Professional на робочих станціях системи.	
	Встановлення ОС Microsoft Windows Server 2019 на сервері системи.	3 770 грн
	Встановлення пакету програмного забезпечення Microsoft Office 2019 Standard на робочих станціях системи.	1 260 грн
Залучення адміністратора безпеки	Розподіл обов'язків між адміністраторами системи	Виплата заробітної плати

3.1 Розрахунок капітальних (фіксованих) витрат

– Визначення трудомісткості розробки КСЗІ

Тривалість кожної робочої операції для розробки КСЗІ розраховано за формулою (3.1).

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

де $t_{тз}$ – тривалість складання технічного завдання КСЗІ;

$t_{тз}$= 15 годин;

$t_{в}$ – тривалість розробки концепції безпеки інформації в організації;

$t_{в}$= 16 годин;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{а}$= 20 годин;

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

$t_{вз}$= 7 годин;

$t_{озб}$ – тривалість вибору основних рішень із забезпечення безпеки інформації;;

$t_{озб}$= 24 години;

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

$t_{овр}$= 17 годин;

$t_д$ – тривалість документального оформлення КСЗІ;

$t_д$= 10 годин.

$t = 15 + 16 + 20 + 7 + 24 + 17 + 10 = 109$ (годин)

– Розрахунок витрат на створення КСЗІ

Визначення витрат на створення КСЗІ за допомогою формули (3.2).

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

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

$З_{зп}$ – заробітна плата спеціаліста з інформаційної безпеки, яка розраховується за формулою (3.3);

$З_{мч}$ – вартість машинного часу, що необхідний для розробки КСЗІ.

Заробітна плата виконавця визначається за формулою:

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

де t – загальна тривалість розробки КСЗІ, годин;

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

За даними статистики [10] середня заробітна плата спеціаліста з інформаційної безпеки становить 2 780 грн. $З_{іб} = 2780 \div 40 = 69.5$ грн/годину.

$З_{зп} = 109 \cdot 69.5 = 7575.5$ грн.

Вартість машинного часу на ПК визначається за формулою:

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

де t – трудомісткість розробки КСЗІ на ПК, годин;

t= 109 годин;

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

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

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

де P – встановлена потужність ПК, кВт;

P= 0,45 кВт;

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

$t_{нал}$= 1;

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

$С_е$= 1,68 грн/кВт·година;

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

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

$Н_а = {}^{1}/_{5} = 0.2$;

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

$Н_а = {}^{1}/_{2} = 0.5$;

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

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

Для визначення залишкової вартості необхідно знайти накопичену амортизацію ПК. Вартість ПК становить 2600 грн., мінімальний термін корисної служби – 60 місяців, термін використання ПК – 50 місяців.

$Ф_{зал} = 2600 - (2600 \cdot 50) \div 60 = 433$ грн.

Вартість закупівлі ліцензійного програмного забезпечення $К_{лпз}$ наведено в таблиці 3.1.

$К_{лпз} = 2500 + 3770 + 1260 = 7530$ грн.;

$С_{мч} = 0.45 \cdot \ 1 \cdot 1.68 + \frac{433 \cdot 0.2}{1920} + \frac{7530 \cdot 0.5}{1920} = 2.75$ грн/година;

$З_{мч} = 109 \cdot 2.75 = 300$ грн.;

$К_{рп} = 7575.5 + 300 = 7875.5$ грн.

– Капітальні (фіксовані) витрати на створення комплексу

На впровадження проектних рішень кваліфікаційної роботи підрахуємо капітальні витрати за формулою (3.6).

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

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, грн;

$К_{пр}$ = 12000 грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення, грн;

$К_{зпз}$ = 7530 грн;

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

$К_{рп}$ = 10000 грн;

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

$К_{аз}$ = 46600 грн;

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

$К_{навч}$ = 5000 грн;

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

$К_{н}$ = 3000;

$К = 12000 + 7530 + 10000 + 46600 + 5000 + 3000 = 84130$ грн.

3.2 Розрахунок поточних (експлуатаційних) витрат

Визначення витрат на функціонування системи інформаційної безпеки здійснено за формулою (3.7)

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

$С_{в}$ – витрати на Upgrade-відновлення й модернізацію системи інформаційної безпеки;

$С_{в}$ = 0 грн. У вартість ліцензійного програмного забезпечення входить регулярне оновлення до нових версій.

$С_{к}$ – витрати на керування системою інформаційної безпеки розраховуються за формулою (3.8);

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{єв} + С_{ел} + С_{о} + С_{тос}, \text{ грн,} \quad (3.8)$$

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

У середньому 4 робітники відвідують тренінги з перекваліфікації та отримання нових навичок. Ціна для одного робітника складає 2000 грн.

$С_н$ = 8000 грн.

$С_а$ – річний фонд амортизаційних відрахувань;

Мережеві комутатори відносяться до групи 4 – машини та обладнання. Їх вартість складає більше 2500 грн., тому мінімально допустимий строк корисного використання становить 2 роки.

Строки амортизації нематеріальних активів групи 5 – програми для електронно- обчислювальних машин, у нашому випадку, становлять також 2 роки.

$С_а = 7530 \div 2 = 3765$ грн;

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

У систему залучається один адміністратор безпеки, який виконує інженерно-технічні завдання, на 0.3 ставки.

$С_з = (10000 \cdot 12) \cdot 0.3 = 36000$ грн.

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

$С_{єв} = 36000 \cdot 0.22 = 7920$ грн.

$С_е$ – вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року;

$$С_е = P \cdot F_p \cdot Ц_е, \text{ грн,} \quad (3.9)$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт;

F_p – річний фонд робочого часу системи;

$Ц_е$ – тариф на електроенергію, грн/кВт.

$С_е = 0.45 \cdot 1920 \cdot 1.68 = 1452$ грн.

$С_о$ – витрати на залучення сторонніх організацій;

$С_о$ = 0 грн;

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи;

$C_{тос} = 84130 \cdot 0.03 = 2523.5$ грн.

$C_к = 8000 + 3765 + 36000 + 7920 + 1452 + 0 + 2523.5 = 59660.5$ грн;

$C_{ак} = 1000$ грн;

$C = 0 + 59660.5 + 1000 = 60660.5$ грн.

3.3 Оцінка можливого збитку від атаки

Розрахунок упущеної вигоди від простою атакованого вузла або сегмента корпоративної мережі проведено за формулою (3.10).

$$U = П_п + П_в + V, \quad (3.10)$$

де $П_п$ – оплачувані витрати 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 – витрати від зниження обсягу оброблювальної інформації за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати робочого часу і простою співробітників визначаються за формулою (3.11):

$$П_п = \frac{\sum З_с}{F} t_п, \text{ грн}, \quad (3.11)$$

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

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

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

$t_п$ = 2 години.

Заробітна плата штатного працівника складає 8000 грн + єдиний соціальний внесок, тобто витрати на заробітну плату становлять 9760 грн. У даній системі є десять штатних працівників.

Заробітна плата директора, заступника директора та адміністратора системи становлять по 11000 + єдиний соціальний внесок, тобто витрати на заробітну плату становлять 13420 грн.

Розрахунок заробітної плати атакованого вузла:

$\sum З_с = 10 \cdot 9760 + 3 \cdot 13420 = 137860$ грн.

$П_п = \frac{137860}{176} \cdot 2 = 1567$ грн.

Вартість відновлення вузла визначається за формулою (3.12):

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

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

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

$П_{зч}$= 6000 грн.

Розрахунок витрат на повторне уведення інформації:

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

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

$t_{ви}$ = 3 години.

$П_{ви} = \frac{137860}{176} \cdot 3 = 2350$ грн.

Розрахунок витрат на відновлення вузла або сегмента корпоративної мережі:

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

де $З_о$ – заробітна плата обслуговуючого персоналу , грн;

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

$t_в$ = 3 години.

$П_{пв} = \frac{13420}{176} \cdot 3 = 229$ грн.

$П_в = 2350 + 229 + 6000 = 8579$ грн.

Розрахунок витрат від зниження очікуваного обсягу оброблювальної інформації за час простою атакованого вузла або сегмента корпоративної мережі за допомогою формули (3.16):

$$V = \frac{O}{Fr} \cdot (t_п + t_в + t_{ви}), \quad (3.16)$$

де Fr – річний фонд часу роботи організації (52 робочих тижня, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 годин.

O = 5 тис. запитів приблизно на 300000 грн;

$V = \frac{300000}{2080}(2 + 3 + 3) = 1153$ грн.

$U = 1567 + 8579 + 1153 = 11299$ грн.

Таким чином, загальний збиток від атаки на вузол або сегмента корпоративної мережі складає: $B = \sum_i \sum_n U$, (3.17)

де i – число атакованих вузлів або сегментів корпоративної мережі;

n – середнє число атак на рік;

$B = \sum_1 \sum_7 11299 = 11299 \cdot 1 \cdot 7 = 79093$ грн.

3.4 Загальний ефект від впровадження КСЗІ

Визначення загального ефекту від впровадження КСЗІ з урахуванням ризиків порушення інформаційної безпеки виконано за формулою (3.18):

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

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

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

C – щорічні витрати на експлуатацію КСЗІ, грн;

$E = 79093 \cdot 0.9 - 60660.5 = 10523.2$ грн.

3.5 Визначення та аналіз показників економічної ефективності

Для оцінки економічної ефективності системи захисту інформації, розглянутій у другому розділі кваліфікаційної роботи, розраховано коефіцієнт повернення інвестицій ROSI за формулою (3.19).

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

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

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

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

$$ROSI = \frac{10523.2}{84130} = 0.13$$

Для остаточної оцінки варіантів необхідно порівняти розрахункове значення ROSI із бажаним значенням показника ефективності $E_н$.

Проект системи інформаційної безпеки визначається доцільним за умови

$$ROSI > E_н \quad (3.20)$$

При $ROSI < E_н$ варіант є збитковим і більш економічним визнається відмова від його реалізації.

Для міського центру зайнятості впровадження системи захисту інформації реалізується фінансуванням капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань).

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (N_{деп} - N_{інф})/100, \quad (3.21)$$

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

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

$0.06 > (15 - 13.40)/100$ отримаємо $0.13 > 0.016$

Розрахунок терміну окупності капітальних інвестицій T_0 показує за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження КСЗІ:

$$T_o = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років.} \quad (3.22)$$

$$T_o = \frac{84130}{10523.2} = \frac{1}{0.13} = 8 \text{ років.}$$

Висновки за економічним розділом

У даному розділі розраховані та проаналізовані основні економічні показники для впровадження КСЗІ:

- капітальні витрати на створення КСЗІ, $К = 84130$ грн;
- поточні (експлуатаційні) витрати, $С = 60660.5$ грн;

загальний ефект від впровадження КСЗІ, $Е = 10523.2$ грн;

- коефіцієнт повернення інвестицій, $ROSI = \frac{10523.2}{84130} = 0.13$;
- термін окупності капітальних інвестицій, $T_o = \frac{84130}{10523.2} = \frac{1}{0.13} = 8$ років

За вищенаведеними результатами можна зробити висновок, що впровадження рішень щодо захисту інформації в ІТМ є економічно доцільним. Завдяки запропонованим впровадженням можливе становлення на шлях до модернізації системи та покращення умов праці.

ВИСНОВКИ

У першому розділі кваліфікаційної роботи детально наведений стан питання доцільності впровадження КСЗІ на підприємствах. Також визначено основні етапи розробки комплексної системи захисту інформації, за якими було проведено дослідження інформаційно-телекомунікаційної системи.

У другому розділі проведені основні етапи обстеження всіх середовищ функціонування ІТС: фізичного середовища, обчислювальної системи, інформаційного середовища та середовища користувачів. Після детального ознайомлення із системою, було виявлено слабкі місця системи – вразливості. Виходячи з цього були наведені можливі загрози системі. Наступним кроком було створення моделі загроз і моделі порушника у вигляді таблиць, що ілюструють

критичні компоненти системи. Також було підібрано профіль захищеності інформаційної системи відповідно до суттєвих критеріїв системи, які повинні бути реалізовані.

На вимогу керівника підприємства конфігурація ІТС та окремі моменти ситуаційного та генерального плану були змінені без впливу на результуючі рішення.

На основі досліджень і обробки інформації про об'єкт, було запропоновано втілення необхідних програмно-апаратних рішень задля надійної роботи системи.

У економічному розділі були проведені розрахунки основних показників, які допомагають обґрунтувати економічну ефективність основних і супутніх результатів впровадження запропонованих рішень.

ПЕРЕЛІК ПОСИЛАНЬ

1. UNIT. Побудова КСЗІ. URL: http://unit.com.ua/ua/postroenie-kszi (дата звернення 04.05.2022).
2. Логінова Н. І. правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с., іл
3. Статистика з кібербезпеки за 2020 рік.URL: https://10guards.com/ua/articles/2020-cybersecurity-statistics/ (дата звернення 15.05.2022).
4. Data breaches and cyber attacks report 2021. URL: www.itgovernance.co.uk (дата звернення 15.05.2022).

5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-2005
6. Остапов С. Е. технологія захисту інформації: навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2013. – 476 с.
7. Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000
8. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99
9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004.99
10. Огляд статистики зарплатні професії "Спеціаліст з інформаційної безпеки в Україні". URL: https://ua.trud.com/ua/salary/2/67683.html (дата звернення 09.06.2022)
11. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядн.: Д.П. Пілова. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2019. – 16 с.
12. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 Кібербезпека/ Упоряд.: О.В. Герасіна, Д.С. Тимофєєв, О.В. Кручінін, Ю.А. Мілінчук – Дніпро: НТУ «ДП»,2020. – 47с.
13. ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	

5	А4	Стан питання. Постановка задачі	7	
6	А4	Спеціальна частина	60	
7	А4	Економічний розділ	10	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	
15	А4	Додаток Е	1	

ДОДАТОК Б. Форма та зміст акта категоріювання об’єкта

Гриф обмеження доступу

Прим. № 1__

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об’єкта
Директор обласного ЦЗ
Адамов І. П. _____
(посада, підпис, ініціали, прізвище)
20.02. 2019
М.П.

АКТ
категоріювання Покровського міського центру зайнятості_____
(найменування об’єкта категоріювання)

1. Підстава для категоріювання закінчення терміну дії акта категоріювання від 15.01.2013 р.
_____
(рішення про створення КСЗІ, закінчення терміну дії акта категоріювання,
_____
зміна ознаки, за якою була встановлена категорія об’єкта, тощо;
_____
посилання/реквізити на розпорядчий документ про призначення комісії з категоріювання)

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

3. На ОІД здійснюється обробка інформації технічними засобами

4. Ступінь обмеження доступу до інформації, що обробляється технічними засобами на об’єкті конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”_____
(передбачена законом таємниця (крім державної); службова інформація; конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України “Про доступ до публічної інформації”; інша конфіденційна інформація, вимога щодо захисту якої встановлена законом)

5. Встановлена категорія_____третя «3»_____

Голова комісії _____ _____Попов Д.Г.___
(підпис) (ініціали, прізвище)
Члени комісії: _____ _____Сиротюк А. К.__
(підпис) (ініціали, прізвище)
27.01. 2019

ДОДАТОК В. Наказ про створення КСЗІ

Донецький обласний центр зайнятості

НАКАЗ

«03» березня 2019 м. Краматорськ № 247

Про створення комплексної системи захисту інформації в автоматизованій системі класу «3»

Відповідно до вимог Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР та на підставі акту категоріювання об'єкта від

НАКАЗУЮ:

1. Створити комплексну систему захисту інформації в АС класу «3» Покровського міського центру зайнятості, призначеній для обробки конфіденційної інформації громадян України;
2. Відповідним за створення КСЗІ та впровадження заходів захисту інформації призначити начальника відділу інформаційних систем Чижевського М. Ю.;
3. Закріпити за міським відділом організації матеріально-технічного забезпечення виконання таких обов'язків щодо створюваної АС
   - взаємодію з ліцензіатами у сферу технічного захисту інформації в процесі виконання робіт із створення комплексної системи захисту інформації та проведення державної експертизи;
   - адміністрування технічних засобів АС в процесі створення КСЗІ та штатної експлуатації АС;
   - взаємодію з відділом захисту інформації в процесі модернізації АС;
   - обслуговування технічних засобів АС (доналагодження, комутація, оновлення програмного та апаратного забезпечення).
4. Контроль за виконанням наказу залишаю за собою.

Директор Адамов І. П.

Додаток Г. Перелік документів на оптичному носії

1. Федоренко_ДІ_125_18_2_ПЗ.docx
2. Федоренко_ДІ_125_18_2_ПЗ.pdf
3. Федоренко_ДІ_125_18_2_ДМ.pptx
4. Федоренко_ДІ_125_18_2_ПЗ.pdf.p7s

Додаток Д. Відгук керівника економічного розділу

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

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

Додаток Е. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студентки групи 125-18-2

Федоренко Дар'ї Ігорівни

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи Покровського міського центру зайнятості»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на 95 сторінках.

Метою кваліфікаційної роботи є забезпечення деталізованої та актуалізованої ідентифікації інформаційних активів об`єктів захисту.

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 нормативно-правової бази у сфері забезпечення кібербезпеки; аналіз організаційно-документаційного забезпечення ідентифікації інформаційних активів; аналіз автоматизованих засобів збору інформації; визначення основних характеристик для класифікації інформаційних активів.

Розроблено рекомендації для проведення ідентифікації інформаційних активів.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності процесу ідентифікації інформаційних активів, за рахунок розробки рекомендацій для проведення ідентифікації.

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

За час дипломування Федоренко Д.І. проявила 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 95«відмінно».

Керівник кваліфікаційної роботи, д.ф.-м.н., проф. **Кагадій Т.С.**

Керівник спец. розділу, ст. викл. **Тимофєєв Д.С.**