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 *Шрамко Дарини Ігорівни*

академічної групи *125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Кручінін О.В.			
економічний	доц. Пілова Д.П.	95	відмінно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.	85	добре	

Дніпро
2022

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

«_____»_____2022 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Шрамко Дарині Ігорівна* **академічної групи** *125-18-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему ***Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»***

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

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження ІТС відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки», аналіз потенційних загроз*	18.04.2022-02.05.2022
Розділ 2	*Формування вимог захисту в ІТС, розробка профілю захищеності, політик безпеки та проектних рішень*	03.05.2022-27.05.2022
Розділ 3	*Економічне обґрунтування доцільності впровадження запропонованих рішень кваліфікаційної роботи*	30.05-2022-07.06.2022

Завдання видано _____ Корнієнко В. І.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 06.04.2022

Дата подання до екзаменаційної комісії: 10.06.2022

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

РЕФЕРАТ

Пояснювальна записка: 91с., 10 рис., 21 табл., 5 додатків, 9 джерел.

Об'єкт дослідження: ІТС відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

Метою кваліфікаційної роботи є забезпечення на заданому рівні захисту інформації, що обробляється в інформаційно-телекомунікаційній системи відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

Методи дослідження: спостереження, аналіз, опис.

Перший розділ містить основні відомості з нормативних документів, обґрунтування необхідності створення КСЗІ та результати обстеження середовища функціонування ІТС.

В другому розділі формуються вимоги щодо проектних рішень, аналізується стан виконання окремих послуг безпеки, пропонуються організаційні та технічні заходи та обґрунтовується вибір послуг захисту для реалізації необхідних послуг.

Третій розділ є економічною частиною кваліфікаційної роботи, що містить розрахунки фінансових витрат на впровадження комплексної системи захисту інформації. Метою третього розділу є доведення та обґрунтування економічної доцільності введення в експлуатацію комплексних системи захисту інформації.

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, ПРОФІЛЬ ЗАХИЩЕННОСТІ, НОРМАТИВНО-ПРАВОВА БАЗА, ПОСЛУГИ БЕЗПЕКИ ІНФОРМАЦІЇ.

ABSTRACT

Explanatory note: 91p., 10 fig., 21 table, 5 supplements, 9 sources.

The research object: ITS of the accounting department of the municipal higher educational institution “Dnipropetrovsk Academy of Music named after M. Glinka ».

The purpose of the qualification work is to ensure at a given level of protection of information processed in the information and telecommunications system of the accounting department of the municipal higher educational institution "Dnipropetrovsk Academy of Music. M. Glinka ».

Research methods: observation, analysis, description.

The first section contains basic information on normative documents, substantiation of the need to create a CCIS, and the results of the survey of the ITS environment.

The second section forms the requirements for design decisions, analyzes the status of individual security services, offers organizational and technical measures, and justifies the choice of security services to implement the necessary services.

The third section is the economic part of the qualification work, which contains calculations of financial costs for the implementation of a comprehensive information security system. The third section aims to prove and substantiate the economic feasibility of putting into operation a comprehensive information security system.

COMPREHENSIVE INFORMATION SECURITY SYSTEM, INFORMATION AND TELECOMMUNICATION SYSTEM, MODEL OF THREATS, MODEL OF THE OFFENDER, INFORMATION SAFETY, CYBERSECURITY, PROTECTION PROFILE, REGULATORY FRAMEWORK, AND INFORMATION SECURITY SERVICES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ІТС – інформаційно-телекомунікаційна система;

ІС – інформаційна система;

КСЗІ – комплексна система захисту інформації;

ДСТУ – державний стандарт України;

НДТЗІ – нормативний документ із технічного захисту інформації;

КЗЗ – комплекс захисту інформації;

ІзОД – інформація з обмеженим доступом;

НСД – несанкціонований доступ;

КЗ – контрольована зона;

ДТЗ – допоміжні технічні засоби;

ПК – персональний комп’ютер;

ОС – операційна система;

ЗУ – закон України;

РС – робоча станція;

ОІД – об’єкт інформаційної діяльності;

ІБ – інформаційна безпека;

ISO – international organization for standardization.

ЗМІСТ

ВСТУП

На сьогоднішній день більшість бюджетних установ, що працюють завдяки налагодженій комп'ютерній системі, мають багато проблем з рівнем безпеки оброблювальної інформації.

Так чи інакше, в кожній бюджетній установі циркулює інформація, витік якої призведе до серйозних наслідків, що вплинуть на репутацію установи та фінансові втрати. Саме тому розробка та впровадження заходів інформаційної безпеки є однією з головних задач сьогодення.

Якщо раніше засоби захисту інформації розроблялися переважно державними органами влади в Україні, то зараз ситуація принципово змінюється на користь приватних підприємств, що надають свої послуги. Тож, для запобігання несанкціонованого доступу, витоку інформації чи інших порушень захисту інформації в автоматизованій системі (далі – АС), доцільно використовувати комплексі засоби захисту інформації (далі – КЗСІ).

Комп'ютеризація державних установ України – невід'ємна частина технологічного прогресу. Проте, на жаль, керівники більшості державних установ так чи інакше нехтують правилами інформаційної безпеки, що призводить до відсутності налагодженої комплексної системи захисту інформації.

Як наслідок, такі бюджетні організації можуть стати небажаним об'єктом уваги зі сторони зловмисників. Саме тому тема даної кваліфікаційної роботи є актуальною, бо в разі недбалого ставлення до процесів захисту інформації під загрозою може опинитися конфіденційна інформація, що обробляється в ІТС, що в свою чергу може призвести до катастрофічних наслідків для репутації державної установи.

Метою кваліфікаційної роботи є розробка комплексної системи захисту інформації відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

РОЗДІЛ І. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ. ОБСТЕЖЕННЯ ІТС ТА АНАЛІЗ СТАНУ ЗАХИЩЕННОСТІ

1.1 Стан питання

За даними Національного координаційного центру кібербезпеки, у 2021 році в Україні було зафіксовано майже 14 мільйонів інцидентів у сфері кібербезпеки. Масштабних кібератак за минулий рік не було зафіксовано, втім, понад 75% атак були спрямовані на державний сектор. Найбільша кількість інцидентів пов'язана з комп'ютерними системами, решта – зі скануванням ресурсів та атаками типу brute-force. Цікаво, що на початку 2021 року спеціалісти з кібербезпеки виявили масову розсилку фішингових електронних листів нібито від Держспецзв'язку, що були, спрямовані на державний сектор [1].

Державний сектор завжди користувався значим «попитом» серед кіберзлочинців, тому з кожним роком масованість кібер-атак на бюджетні установи буде тільки зростати. Враховуючи воєнний стан в Україні, наразі усі державні установи знаходяться в зоні ризику та потребують впровадження комплексних заходів по забезпеченню цілісності та конфіденційності інформації.

За даними рейтингу «Цифрова якість життя» (Digital Quality of Life Index 2021, DQL) від Surfshark, Україна піднялася на 18 позицій вище, ніж у 2020 році. Так, Україна зайняла 47-му сходинку разом з Сербією та Філіппінами. Згідно рейтингу, Україна демонструє найвищі показними з доступності Інтернету (28-е місце) та кібербезпеки (25-е місце), проте має доволі низькі показники у сфері електронного урядування (61-е місце), електронної інфраструктури (42-е місце)) та якості Інтернету (68-е місце).

Проте, діджиталізація України не може не визивати захоплення, адже Дія – це, безумовно, серйозна заявка на світовій технологічній арені. За словами віце-прем'єр міністра цифрової економіки Михайла Федорова, білим хакерам допоки не вдалося знайти суттєвих вразливостей в «державі в смартфоні» [2].

Україна має не аби який технологічний потенціал, проте, питання кібербезпеки все же залишається одним з ключових на порядку денному.

Так, за словами заступника секретаря РНБО Сергія Демедюка, в Україні інфраструктура, що пов'язана з глобальною мережею Інтернет, дуже різнобарвна, оскільки в країні немає єдиної системи, як, наприклад, в Європі чи США. Тобто, це є великою перевагою для українського кіберпростору та головною біллю для зловмисників, бо це спонукає їх прикладати багато сил та часу, щоб охопити відразу декілька цілей для атак [2].

Сергій Демедюк підкреслив, що атаки в основному здійснюються на персонал державних установ з метою заволодіння інформацією з персонального комп'ютера (далі – ПК) співробітника задля потрапляння в мережу критичної інфраструктури установи. [2].

Очевидно, що задля досягнення своєї мети зловмисники не нехтують самими брудними способами заволодіння необхідною інформацією. Соціальна інженерія, фішинг, масовані DDoS-атаки тощо – це все інструменти чорних хакерів. Зрозуміло одне – державні установи цікавлять злочинців набагато сильніше, ніж приватні підприємства, бо ціна за конфіденційну інформацію бюджетних організацій набагато більша.

Крім того, державні установи в Україні – це ще й одна з найважливіших баз у сфері електронного документообігу. Згідно з рейтингом Digital Quality of Life Index 2021, DQL, нашій країні ще слід попрацювати над електронним урядуванням та інфраструктурою, що також робить сферу бюджетних послуг вразливою для кібер-атак.

Кожна бюджетна організація задля стабільного функціонування потребує велику кількість одиниць техніки, зокрема комп'ютерів, маршрутизаторів, принтерів, серверів, камер відео нагляду тощо. Зазвичай, кількість одиниць техніки становить від 10 до 100 в залежності від розміру підприємства.

Враховуючі підвищений інтерес зловмисників до бюджетних установ, а також специфіку роботи таких підприємств і наявність великої кількості одиниць техніки, виникає потреба у впровадженні комплексної системи захисту інформації.

Розробляючи комплексну систему захисту інформації підприємств, зазвичай враховуються такі чинники:

- фізичні розміри бюджетної установи;
- фінансовий стан;
- стан інформаційної безпеки;
- кількість одиниць техніки;
- діяльність бюджетної установи тощо.

При проектуванні комплексної системи захисту інформації слід дотримуватися головних критеріїв: адекватності, системності, комплексності, відкритості алгоритму та простоти реалізації.

Механізми КСЗІ повинні бути максимально простими та зрозумілими; вони не повинні вимагати від співробітників державних установ якихось особливих навичок та вмінь.

Тож, спеціаліст з кібербезпеки, аналізуючи запит на розробку КСЗІ для певної бюджетної організації, ставить перед собою такі задачі:

- захист персональних даних співробітників;
- захист конфіденційних даних підприємства;
- захист інформації з обмеженим доступом, що циркулює на підприємстві тощо.

Лише комплексний підхід до забезпечення інформаційної безпеки може в декілька разів зменшити ризик несанкціонованого доступу до системи, а також суттєво заощадити фінансові ресурси бюджетної установи.

1.2 Теоретичні відомості

1.2.1 Об’єкт інформаційної діяльності

Згідно Статті 1 Розділу І ЗУ «Про Державну службу спеціального зв’язку та захисту інформації України», об’єкт інформаційної діяльності – це інженерно-технічна споруда (приміщення), транспортний засіб, де провадиться діяльність, пов’язана з державними інформаційними ресурсами та інформацією, вимога щодо захисту якої встановлена законом.

Згідно Наказу Служби Безпеки України «Про затвердження Зводу відомостей, що становлять державну таємницю (Звід відомостей, п.7) 12.08.2005 N 440 (z0902-05), об’єкт інформаційної діяльності- це інженерно-технічна споруда (приміщення) з визначеною контрольованою зоною, де здійснюється діяльність, пов'язана з інформацією, що підлягає технічному захисту.

Згідно з наказом адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження нормативного документа системи технічного захисту інформації» НД ТЗІ 1.6-005-2013 (Нормативний документ, розд.3) 15.04.2013 № 215 (Об'єкт інформаційної діяльності (ОІД) - інженерно-технічна споруда (приміщення), де здійснюється діяльність, пов'язана з інформацією, що підлягає захисту.

1.2.2 Підстави для створення КСЗІ

Згідно з шостим пунктом створення КСЗІ, що описано в НД ТЗІ 3.7-003-2005, підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

- аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися 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 тощо) експлуатації ІТС у разі створення КСЗІ. На підставі проведеного аналізу приймається рішення про необхідність створення КСЗІ [3].

Крім того, підставою створення КСЗІ на підприємстві є забезпечення захисту персональних прав людини, що описано в ЗУ «Про захист персональних даних». Згідно з цим законом, кожна людина має право на невтручання в особисте життя через обробку її персональних даних.

Окрім зазначених обставин, що пов'язані з безпекою інформації, існує ще й економічна доцільність розробки та впровадження КСЗІ через те, що на підприємстві циркулює інформація, втрата чи розповсюдження якої може негативно вплинути на репутацію підприємства та додати суттєвих матеріальних збитків.

Розробка та впровадження КСЗІ є сферою інтересів усіх керівників підприємств (бюджетних чи приватних), що дбають про репутацію організації, розуміють ризики та можливі матеріальні збитки через недбалість та економію на засобах інформаційної безпеки.

1.3 Обстеження об'єкту інформаційної діяльності

1.3.1 Загальні відомості

«Дніпропетровська академія музики ім. М. Глінки» – це комунальний вищий навчальний заклад у м. Дніпро, що надає послуги освіти усім бажаючим оволодіти грою на музичних інструментах, вокалом тощо.

За формою власності «Дніпропетровська академія музики ім. М. Глінки» - це державний (комунальний) заклад освіти, що був заснований у 1898 році.

Основні види діяльності:

- надання освітніх послуг студентам за різними формами навчання;
- надання додаткових репетиторських послуг для усіх бажаючих оволодіти музичними інструментами;
- надання приміщень та залів для проведення тематичних заходів та музичних концертів.

Комунальний вищий навчальний заклад працює 7 днів на тиждень з 9:00 до 18:00. За попередньою домовленістю, передбачається проведення додаткових занять зі студентами з 18:00 до 21:00.

Штат працівників комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»: ректор (1), заступник ректора з АГР (1), викладачі (35), головний бухгалтер (1), бухгалтер (4), секретар (3), системний адміністратор (3), завідувач відділу кадрів (1), секретар відділу кадрів (2), співробітник відділу кадрів (4), електрик (4), сантехник (4), слюсар (4), прибиральниця (3).

Штат відділ бухгалтерського обліку: головний бухгалтер (1), секретар головного бухгалтера (1), бухгалтер (4).

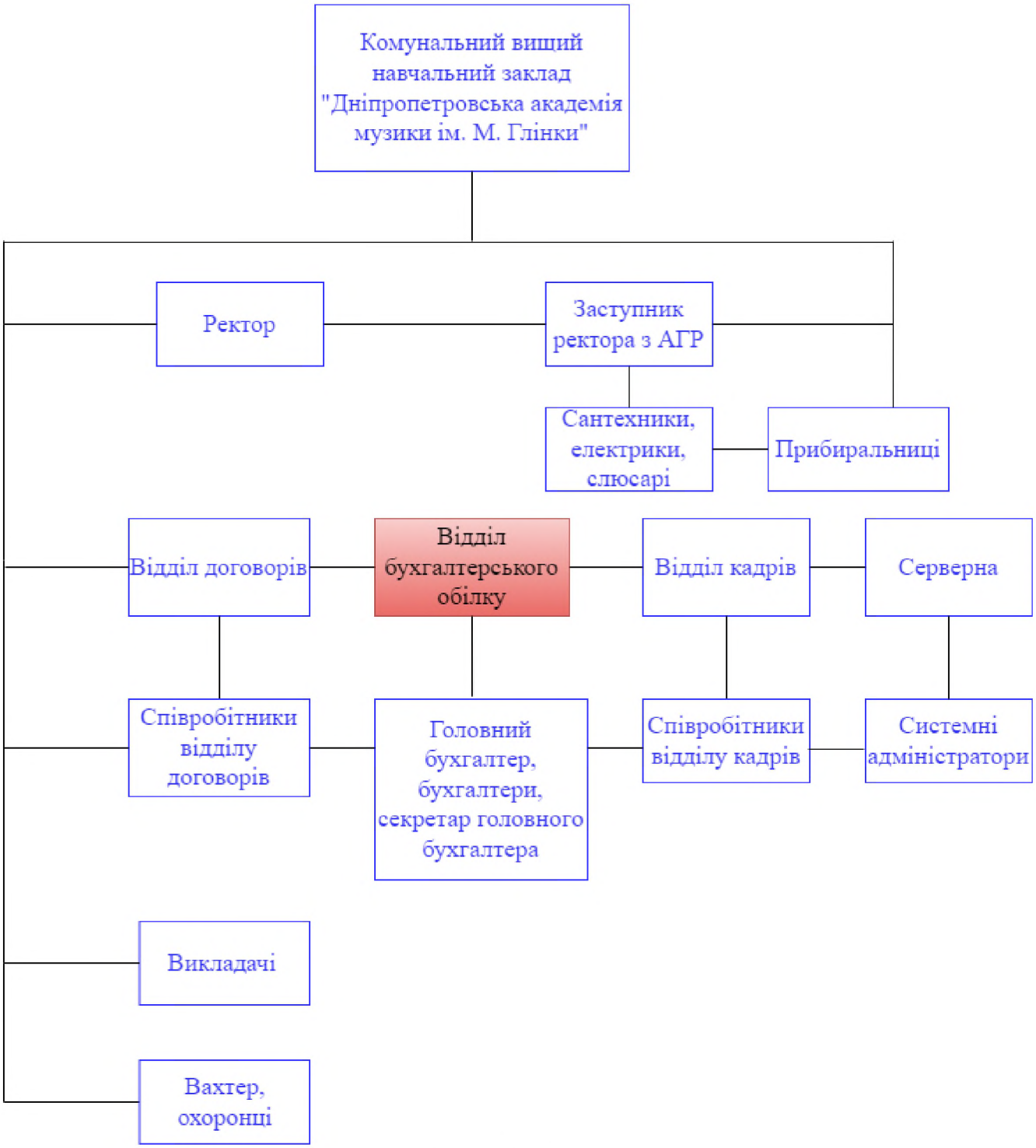

Рис. 1.1 – Організаційна структура

ОІД складається з однієї кімнати площею 25 м².

Згідно з НД ТЗІ 1.6-005-2013, було проведено категоріювання приміщення, на якому здійснюється обробка технічними засобами ІзОД, що не становить державної таємниці. Акт категоріювання розміщено у Додатку Г.

1.3.2 Фізичне середовище

Опис ситуаційного плану:

Об’єкт інформаційної діяльності (ОІД) знаходиться на четвертому поверсі у чотирьох поверховому комунальному приміщенні за адресою 49044, м. Дніпро, вул. Ливарна 10.

Ліворуч, через проїзну дорогу від будівлі, де розташований ОІД, знаходяться 6- та 9-типоверхові житлові будинки. В одному з корпусів житлового будинку за адресою Ливарна, 17 на першому поверсі розташоване відділення «Нової Пошти» № 93, в іншому корпусі на першому поверсі – кондитерський магазин «Болгарія». Біла житлового будинку за адресою Ливарна, 15 в кооперативній триповерховій будівлі на першому поверсі знаходиться продуктовий магазин « На Ливарній» за адресою Ливарна, 13.

Позаду будівлі розташований семиповерховий бізнес-центр «Pixel Plaza» за адресою Ливарна, 4. Праворуч від бізнес-центру розміщується десятиповерховий житловий будинок за адресою Ливарна, 3.

З півночі від ОІД на відстані 300м. знаходиться Січеславська набережна з виходом до річки Дніпро. З півдня на відстані 50м – бізнес-центр «Pixel-Plaza». З північного заходу – житлові будинки. Біля входу до закладу освіти розміщений паркінг для працівників та здобувачів освіти.

Територія навколо будівлі вкрита асфальтом. Поверхня даху – плоска, вкрита руберойдом. Заклад освіти має окремий вхід для осіб з обмеженими можливостями.

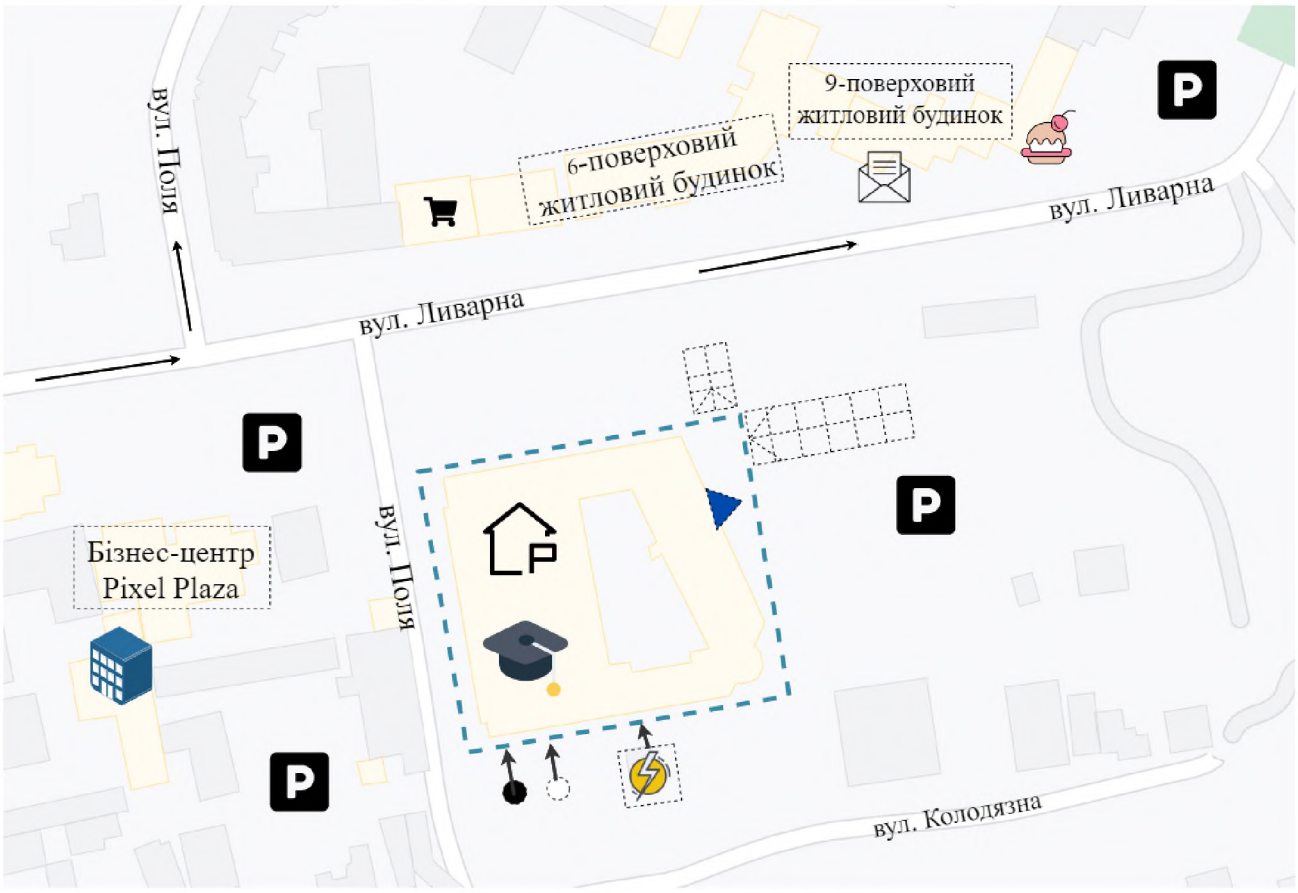

Рис. 1.2 – Ситуаційний план

Рис. 1.3 – Умовні позначення ситуаційного плану

Дані про споруду та прилеглі до неї об’єкти зазначені у таблицях №1.1 та №1.2 відповідно.

Таблиця 1.1. Характеристика прилеглих будівель та споруд

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
1	Житловий будинок	9	вул. Ливарна, 17	100м
2	Житловий будинок	6	вул. Ливарна, 15	60м
3	Кондитерський магазин «Болгарія»	1	вул. Ливарна, 17	150м
4	Бізнес-центр «Pixel Plaza»	7	вул. Ливарна, 4	50м
5	Магазин «На Ливарній»	1	вул. Ливарна, 13	45м

Продовження таблиці 1.1

№	Найменування	Кількість поверхів	Адреса	Відстань від ОІД
6	Поштове відділення «Нової пошти» №93	1	вул. Ливарна, 17	100м
7	Житловий будинок	10	вул. Ливарна, 3	250м
8	Паркінг для співробітників та студентів комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»	–	вул. Ливарна, 10	125м
9	Паркінг для гостей та працівників Бізнес-центру «Pixel Plaza»	–	вул. Ливарна, 4	45м
10	Паркінг для жильців житлових будинків	–	вул. Ливарна 15-17	50м

Таблиця 1.2 – Характеристика прилеглих доріг

№	Найменування	Ширина проїзної частини	Інтенсивність руху	Відстань від ОІД	Паркування
1	Під'їзна дорога до будівлі ОІД	5м	Інтенсивний	30м	Ні

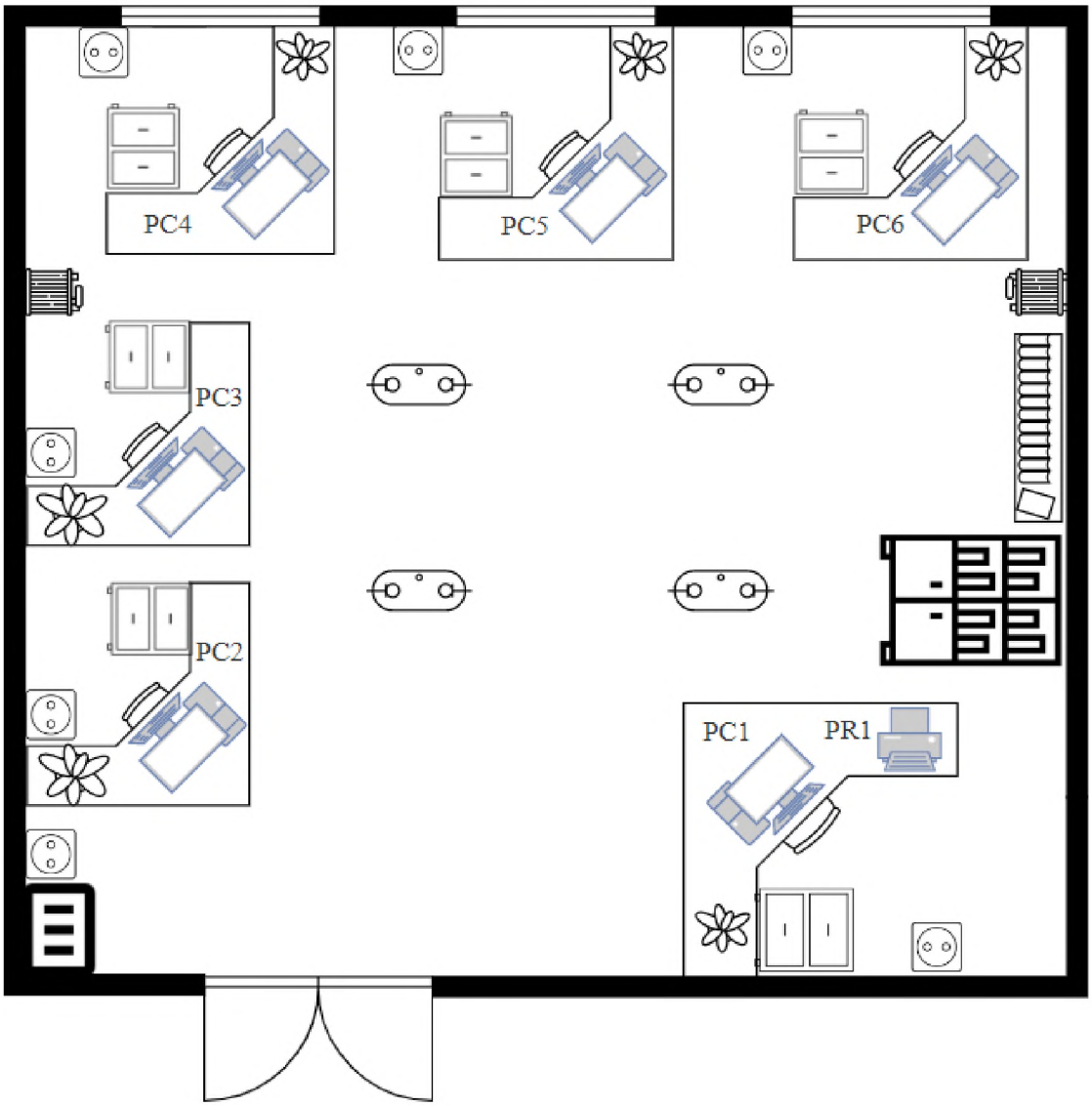

Рис. 1.4 – Генеральний план ОІД

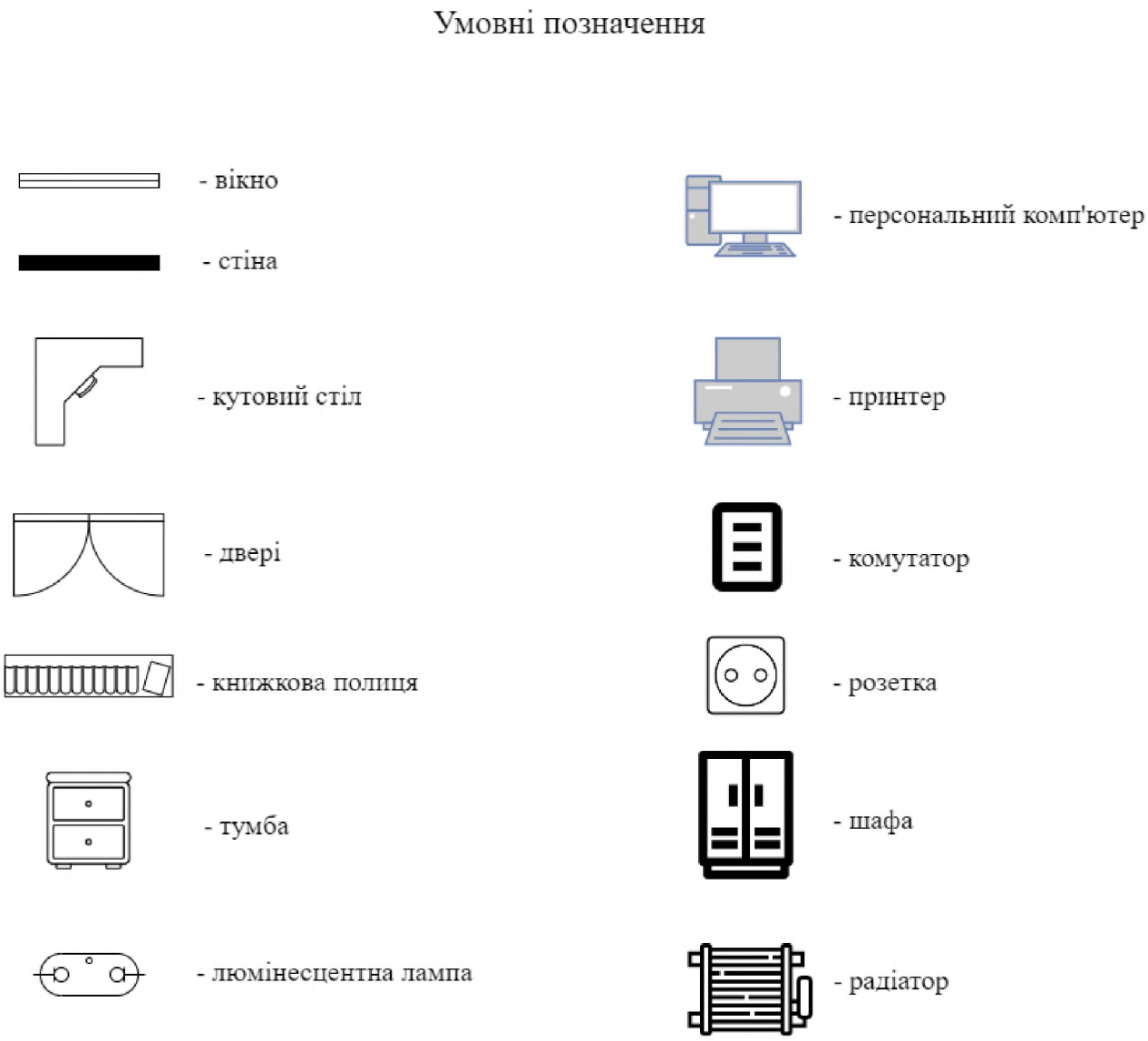

Рис. 1.5 – Умовні позначення генерального плану ОІД

КЗ обмежена стінами, стелею (дахом), підлогою, вікнами та дверми.

У робочий час режим КЗ забезпечується персоналом комунального закладу на підставі інструкції з режиму роботи.

У неробочій час режим КЗ забезпечується охороною у складі двох охоронців, один з яких виконує робочі обов’язки на вахті, що знаходиться на першому поверсі будівлі; другий – здійснює обхід території будівлі кожні три години. Системи сигналізації та відеоспостереження відсутні.

Доступ до ОІД мають усі співробітники відділу бухгалтерського обліку.

До будівлі, де знаходиться ОІД, підведені такі зовнішні комунікації:

- система електропостачання, що підключена до трансформаторної підстанції (ТП -1);
- система глобальної мережі Інтернет, яка забезпечується провайдером ТОВ «Воля-Кабель» (кручена пара);
- система опалення – централізована, постачальник послуг – КП «Теплоенерго». Подача теплоносія відбувається від районної котельні. Температура – 90°С-70°С. Опалювальні прибори – чавунний радіатор М140-А0.

Комунікації споруди – підземні та подаються до будівлі через підвальне технічне приміщення.

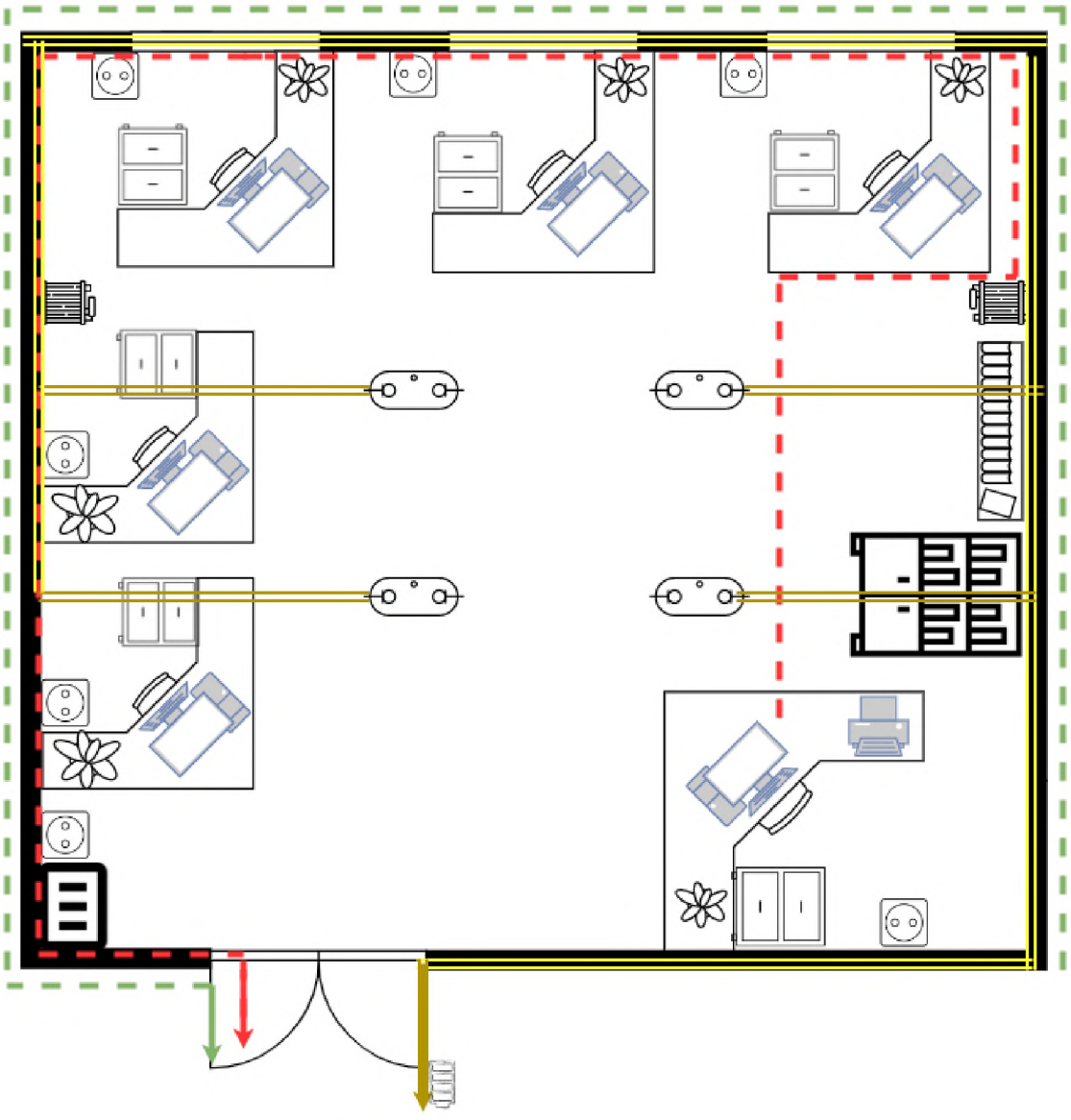

Рис. 1.6 – Схема комунікацій ОІД

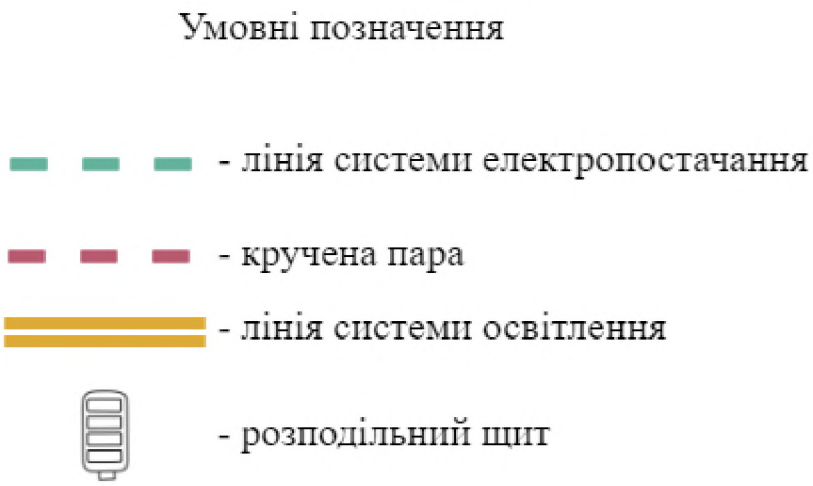

Рис. 1.7 – Умовні позначення схеми комунікацій ОІД

Площа ОІД – 25м².

Зовнішні стіни будівлі, в якій розташований ОІД, зроблені з повнотілої цегли та бетонних конструкцій (товщина – 400 м), внутрішні – з повнотілої цегли (товщина – 250мм).

Вікна будівлі – металопластикові з одинарним склопакетом (800мм х 1200 мм). Частина вікон має горизонтальні металеві жалюзі (переважно в кабінеті ректору, відділу кадрів, відділу бухгалтерського обліку тощо).

Вхідні двері – металопластикові двох-стулчасті з врізним металевим замком, міжкімнатні – дерев'яні з врізним металевим замком.

Підлога і стелі будівлі – з залізобетону. Висота стелі – 3 м (на першому поверсі – 5м). Підлога на всіх поверхах вкрита ламінатом.

Організаційний порядок закладу освіти встановлює обмеження щодо доступу до деяких кімнат.

Доступ до серверної має системний адміністратор (3) та заступник ректора з АГР (1). Ключі від серверної знаходяться на вахті, що розташована на першому поверсі. Отримання ключів здійснюється після запису в журнал активності, що зберігається в вахтера.

Прибирання та ремонт серверної здійснюється прибиральницею, сантехником, електриком тощо під наглядом системного адміністратора чи заступника ректора з АГР у спеціально відведений для цього час.

Доступ до ОІД мають усі співробітники відділу бухгалтерського обліку. Залучення системного адміністратора, сантехників, електриків, прибиральниць тощо до виконання службових обов'язків здійснюється під наглядом головного бухгалтера у відведений для цього час. Інший персонал закладу доступу до ОІД не має.

Комп'ютери розташовані на столах працівників відділу бухгалтерського обліку. На столі головного бухгалтера, порчу із комп'ютером, знаходиться БФП, яким можуть користуватися усі працівники відділу бухгалтерії.

Комутатор розташований на стелі біля входу. Сервери знаходяться в серверній, на підлозі.

Під час обідньої перерви співробітникам дозволено користуватися власними смартфонами за призначенням. У робочий час працівники можуть скористатися розетками для зарядження власних мобільних пристроїв, навушників тощо.

Бухгалтерські звіти та інші документи зберігаються в дерев'яній шафі. Паперові носії інформації зберігаються в тумбочці біля робочого столу секретаря. Запасні ключі до відділу бухгалтерського обліку зберігаються в тумбочці біля робочого столу головного бухгалтера, яка закривається на ключ. Ключ від тумби знаходиться в головного бухгалтера.

На столах і шафах використання замків не передбачене. Регламентовані місця для зберігання зовнішніх носіїв інформації (флеш-накопичувачі тощо) відсутні. Як правило, зовнішні носії інформації зберігаються на робочих столах працівників відділу бухгалтерського обліку.

Лінії електроживлення та освітлення виходять за межі ОІД до поверхового щитка. Поверховий щиток через нижчі поверхи підключений до розподільчого щитку, який підключений до трансформаторної підстанції ТП-1 та системи міського електроживлення.

Освітлення на ОІД здійснюється за допомогою люмінесцентних ламп, що розміщенні на стелі.

Опалення централізоване. Подача гарячої води в труби здійснюється КП «Теплоенерго».

Труби системи опалення виходять за межі КЗ.

ОІД обладнаний одним вогнегасником, що розташований праворуч від вхідних дверей.

Комп'ютерна мережа – дротова (кручена пара), що працює за допомогою комутатора. В свою чергу, комутатор підключено до технічного підземного поверху, де відбувається з'єднання з мережевим обладнанням провайдера ТОВ «Воля-Кабель». Сторонні споживачі мережевого обладнання відсутні.

1.3.3 Обчислювальна система:

ІТС відділу бухгалтерського обліку – це багатомашинний та багатокористувацький комплекс, що обробляє інформацію різного ступеня доступу.

Обчислювальна система взаємодіє з поштовими серверами Google та Outlook задля здійснювання листування з колегами з інших відділів, керівництвом, а також вирішення фінансових проблем та питань з представниками банків тощо. Листування захищене безпечним підключенням через протоколи HTTP та TLS.

Локальна АС складається з 6 комп'ютерів, одного БФП та додаткових технічних засобів. В робочу групу чи домен пристрої не об'єднані.

Комп'ютери підключені до комутатора крученою парою, що проходить над стелею. В свою чергу, комутатор підключений до локальної мережі через мережеве обладнання провайдера ТОВ «Воля-Кабель», що генерує динамічні IP-адреса та виконує маршрутизацію даних. Сторонні споживачі до локальної мережі не під'єднані.

Кожен користувач має свій унікальний пароль для входу в систему, який видає системний адміністратор. Логін користувача – це його прізвище та ініціали, прописані англійською без пробілів. Усі паролі зберігаються у системного адміністратора у файлі на його комп'ютері, що розташованій у серверній. Якщо користувач забуває чи втрачає свій пароль – системний адміністратор має сформувати та видати користувачу новий.

Кожний користувач ІТС має на своєму ПК встановлені драйвера для друку документів за допомогою бездротового мережевого БФП. Друк здійснюється за допомогою прикладних програм для дистанційного друку та функції спільного доступу.

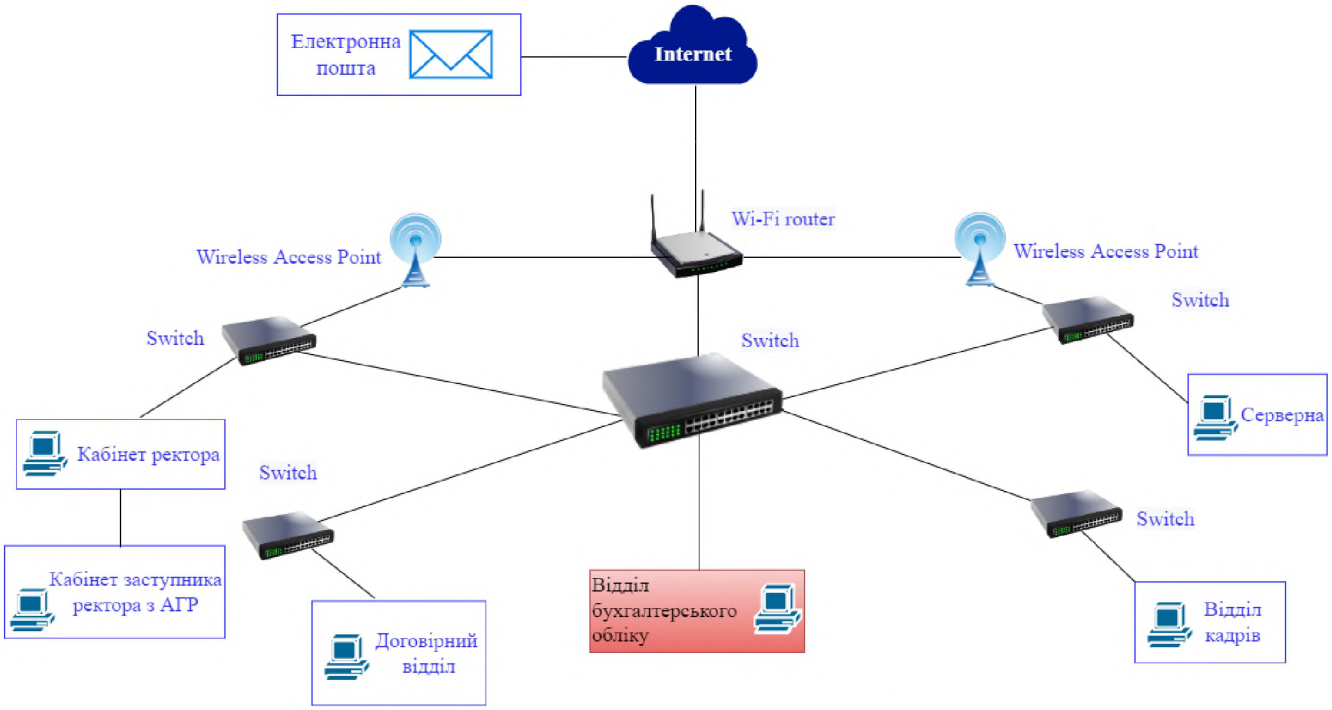

Рис. 1.8 – Загальна схема ІТС

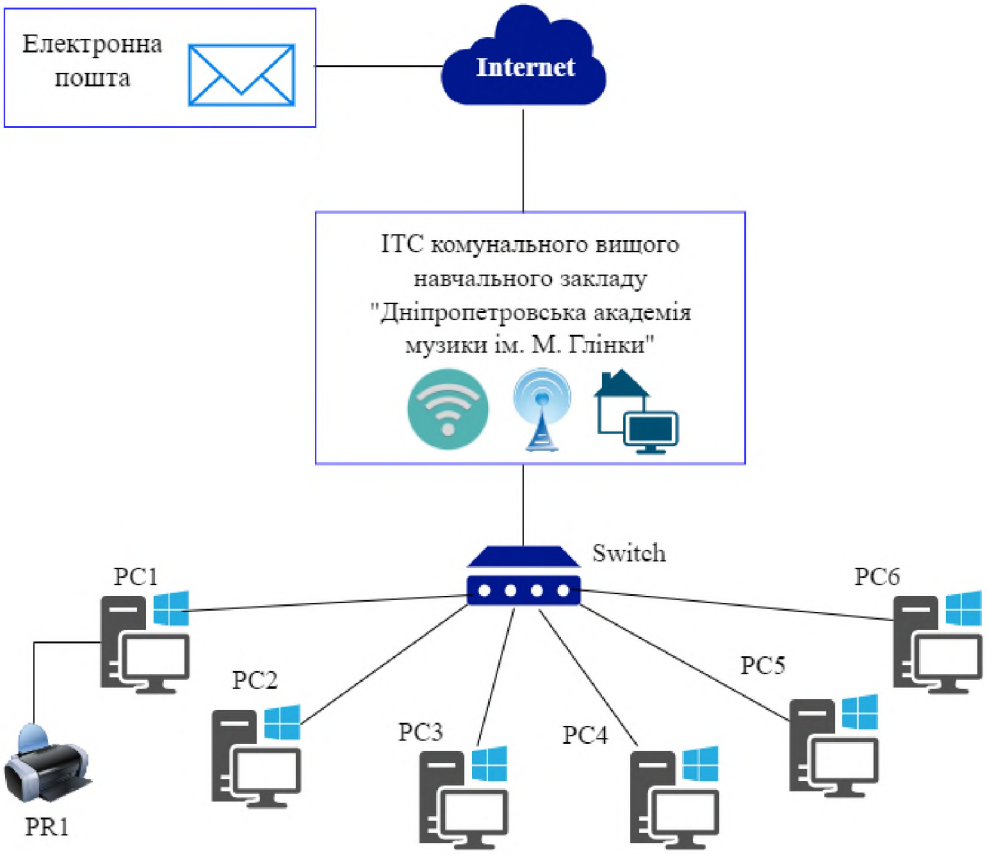

Рис. 1.9 – Схема інформаційно-обчислювальної системи відділу бухгалтерського обліку

Таблиця 1.3 демонструє перелік та характеристику основних та додаткових технічних засобів ІТС.

Таблиця 1.3 – Основні технічні засоби ІТС

№	Тип	Модель	Характеристики	Серійний та інвентаризаційний номери	Відстань до КЗ
1	Персональний комп'ютер (ім'я в системі PC1)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ 4GB, монітор Dell E2216HV 22.1	Системний блок PC12345-1, монітор 210-210	1м
2	Персональний комп'ютер (ім'я в системі PC2)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ 4GB, монітор Dell E2216HV 22.1	Системний блок PC12345-2, монітор 210-211	1м
3	Персональний комп'ютер (ім'я в системі PC3)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ	Системний блок PC12345-3, монітор 210-212	1м

			4GB, монітор Dell E2216HV 22.1		

Продовження таблиці 1.3

№	Тип	Модель	Характеристика	Серійний та інвентаризаційний номери	Відстань до КС
4	Персональний комп'ютер (ім'я в системі PC4)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ 4GB, монітор Dell E2216HV 22.1	Системний блок PC12345-4, монітор 210-213	1,5м
5	Персональний комп'ютер (ім'я в системі PC5)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ 4GB, монітор Dell E2216HV 22.1	Системний блок PC12345-5, монітор 210-214	1,5м
6	Персональний комп'ютер (ім'я в системі PC6)	ZEVS PC M540	Процесор Intel i5, Жорсткий диск 240GB SSD, відеокарта Intel HD Graphic 4600, ОЗУ 4GB,	Системний блок PC12345-6, монітор 210-215	1, 6м

			монітор Dell E2216HV 22.1		

Продовження таблиці 1.3

№	Тип	Модель	Характеристика	Серійний номер	Відстань до КС
7	Багатофункціональний пристрій (PR1)	Epson L3110	Друк - струменевий, кількість кольорів – 4, сфера застосування – офіс, формат друку – A4.	C11CG87405	1м
8	Комутатор	TP-Link TL-SG1008	Буферна пам'ять – 2 МБ, споживання – 4, 3 Вт,8 портів, пропускна спроможність – 16 Гбіт/с.	SG1008-1	1м
9	Бездротова точка доступу	Cisco Aironet 3600i	Тип антени – внутрішня, максимальна швидкість з’єднання – 450 Мбіт/с, кількість антен – 4, харчування – PoE/адаптер	AIR-CAP36021-R-1	5м
10	Бездротова точка доступу	Cisco Aironet 3600i	Тип антени – внутрішня, максимальна	AIR-CAP36021-R-2	2м

			швидкість з’єднання – 450 Мбіт/с, кількість антен – 4, харчування – PoE/адаптер		

Таблиця 1.4 Додаткові технічні засоби ІТС

№	Пристрій	Модель	Характеристика	Серійний номер	Відстань до КЗ
1	Миша комп’ютерна бездротова (6 шт.)	HP Wireless Mouse 220 (3FV66AA)	Тип підключення – радіо, тип сенсора – оптичний, підключення – бездротове, роздільна здатність сенсора – 1300, частота опросу – 2,4 Гц, кількість кнопок – 3, ергономіка – для обох рук (симетрична)	3FV66-1	1м
				3FV66-2	1м
				3FV66-3	1м
				3FV66-4	1,5м
				3FV66-5	2м
				3FV66-6	2м
2	Клавіатура бездротова (6 шт.)	Trust Nado BT White (23746_TRUST)	Тип підключення – бездротове, конструкція клавіатури – мембранна, кількість клавіш – 85, інтерфейс підключення – Bluetooth	123746A	1м
				223746B	1м
				323746C	1м
				423746D	1,5м
				523746E	2м
				623746F	2м

3	Електричний чайник	Liberton LEK-1803 Black	Ємність – 1.8 л, потужність – 1500 Вт, автоматичне відключення, синій колір підсвічування, матеріал корпусу – пластик та скло	1853321	2,5м

Таблиця 1.5 – Програмне забезпечення

Тип	Назва	Опис	Ліцензія	Встановлено на пристрій
Системне ПЗ	Операційна система Windows 10 Pro 21H	Операційна система	Корпоративна ліцензія (OLP)	ПК №1-6
	Драйвери	Набір драйверів для прикладних пристроїв (клавіатура, мишка, принтер тощо)	Власницьке програмне забезпечення (пропрієтарна ліцензія)	ПК №1-6
Прикладне	Microsoft Office 365 for Business (базовий)	Пакет офісних програм для бізнесу	Корпоративна ліцензія (OLP)	ПК №1-6
	7-Zip	Архіватор	GNU Lesser General Public License	ПК №1-6

Продовження таблиці 1.5

Тип	Назва	Опис	Ліцензія	Де встановлено
Спеціалізоване	Google Chrome	Веб-браузер	Google Chrome executable, ліцензія BSD	ПК №1-6
	Brave	Веб-браузер	Mozilla Public License, version 2.0	ПК №1-6
	TeamViewer	Пакет ПЗ для віддаленого контролю комп'ютерів	Власницьке програмне забезпечення (пропрієтарна ліцензія)	ПК №1-6
	1С:Бухгалтерія 8.	Бухгалтерський програмний продукт	Власницьке програмне забезпечення (пропрієтарна ліцензія)	ПК №1-6
	360 Total Security Premium	Антивірусне ПЗ	Власницьке програмне забезпечення (пропрієтарна ліцензія)	ПК №1-6

Дистанційне адміністрування системи та вирішення питань, пов'язаних з оновленням ПЗ, відновленням паролів тощо виконує системний адміністратор за допомого ПЗ для віддаленого доступу TeamViewer.

Системний адміністратор не має власного акаунту в АС. Усі питання, що виникають, вирішуються з системним адміністратором через комп'ютер співробітника відділу бухгалтерського обліку завдяки ПЗ TeamViewer.

1.3.4 Інформаційне середовище

Таблиця 1.6 – Інформація, що циркулює на досліджуваному об'єкті

№	Інформація	Режим доступу	Правовий режим	Представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
1	Довідкові матеріали	Відкрита	Відкрита	Паперові носії	1	1	1
2	Відомості про інвентаризацію та вартість музичних інструментів	ІзОД	Конфіденційна	Паперові носії	2	1	1
3	Аналітичні дані	ІзОД	Конфіденційна	Електронні, паперові носії	3	3	1
4	Щорічна звітність про фінансову діяльність	ІзОД	Конфіденційна	Електронні, паперові носії	4	3	1
5	Фінансова звітність за надання репетиторських послуг	ІзОД	Конфіденційна	Електронні, паперові носії	3	2	1

Продовження таблиці 1.6

№	Інформація	Режим доступу	Правовий режим	Представлення в ІТС	Вимоги до захисту		
					К	Ц	Д
6	Технологічна інформація	ІзОД	Конфіденційна	Електронні носії	4	4	2

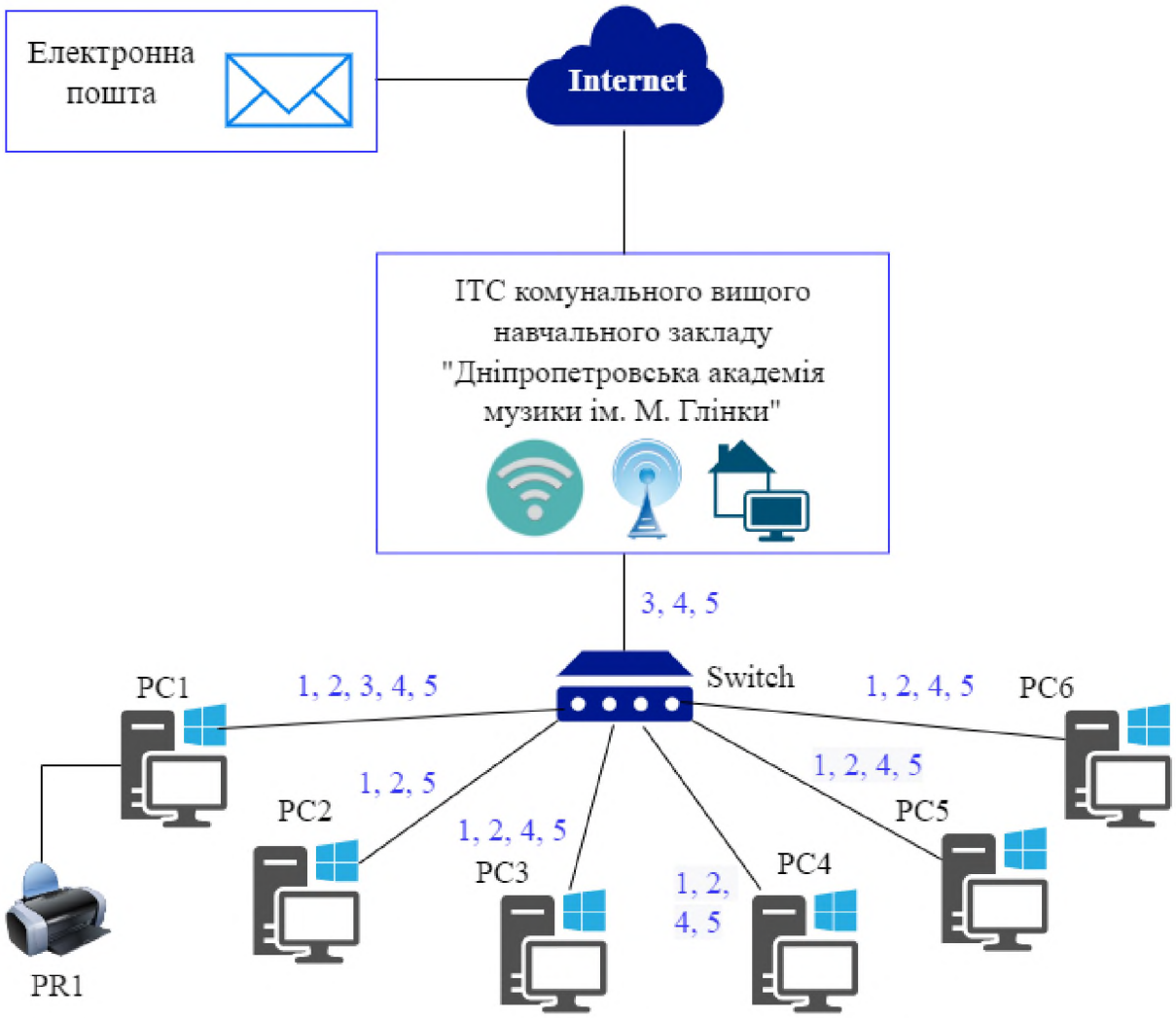

Рис.1.10 – Схема інформаційних потоків

Уся інформація, що знаходиться в АС (окрім зазначеного виду), представлена у вигляді електронних та електромагнітних полів, а також видової інформації на екранах моніторів комп'ютерів.

Класифікація інформація здійснювалася з використанням рівнів властивостей інформації.

Рівні конфіденційності інформації:

- К1 –інформація не є конфіденційною, або збитки не є суттєвими у випадку розкриття цієї інформації особам, що не мають доступу до неї;
- К2 –заклад зазнає несуттєвих збитків у випадку розкриття цієї інформації особам, яким не передбачається доступ;
- К3 –заклад зазнає суттєвих збитків у випадку розкриття цієї інформації особам, яким не передбачено доступ;
- К4 – значні фінансові втрати у випадку розкриття інформації особам, яким не передбачений доступ;
- К5 – критичний рівень конфіденційності, що може призвести до краху закладу у випадку розкриття конфіденційної інформації.

Рівні цілісності інформації:

- Ц1 – збитки відсутні, втратою цілісності можна знехтувати;
- Ц2 – заклад зазнає невагомих збитків;
- Ц3 – заклад зазнає вагомих збитків;
- Ц4 – втрата цілісності інформації може призвести до значних матеріальних чи репутаційних втрат;
- Ц5 – втрата цілісності інформації може призвести до краху закладу.

Рівні доступу інформації:

- Д1 – збитки відсутні, втратою доступу можна знехтувати;
- Д2 – заклад зазнає невагомих збитків;
- Д3 –заклад зазнає вагомих збитків;
- Д4 –втрата доступу до інформації може призвести до значних матеріальних чи репутаційних втрат;
- Д5 – втрата доступу до інформації може призвести до краху закладу.

Технологія обробки інформації:

Довідкові матеріали зберігаються на паперових носіях. Довідкові матеріали розробляться головним бухгалтером та співробітниками відділу бухгалтерії та

інших відділів комунального вищого навчального закладу. За режимом доступу та правовим режимом дана інформація є відкритою. Усі працівники відділу бухгалтерського обліку мають доступ до довідкових матеріалів. Інформація може змінюватися та редагуватися головним бухгалтером, секретарем та іншими співробітниками відділів комунального вищого навчального закладу.

Відомості про інвентаризацію та вартість музичних інструментів представлені на паперових носіях. Після взяття на облік нового музичного інструменту, відомості про нього заносяться на паперові носії секретарем та перевіряються бухгалтером. Інформація може редагуватися бухгалтером чи секретарем.

Аналітичні дані створюються головним бухгалтером щороку і містять дані про фінансові витрати на надання освітніх послуг, ефективність впровадження та використання різних систем та продуктів тощо. Доступ до інформації має тільки головний бухгалтер.

Щорічна звітність про фінансову діяльність зберігається на ПК головного бухгалтера та бухгалтерів, а також на паперових носіях. Створюється бухгалтерами, підлягає редагуванню та видаленню головним бухгалтером. Секретар не має доступу до щорічної звітності про фінансову діяльність.

Фінансова звітність за надання репетиторських послуг зберігається на ПК головного бухгалтера, бухгалтерів та на паперових носіях. Створюється бухгалтерами, підлягає редагуванню видаленню та головним бухгалтером. Секретар може редагувати інформацію.

Технологічна інформація створюється, змінюється та підлягає видаленню системним адміністратором. Системний адміністратор генерує та видає паролі усім користувачам. Паролі користувачів конфігурацію систем розташовується та зберігаються на ПК системного адміністратора, що знаходиться у серверній.

Будь-яка інформація (окрім технологічної) при запиті може бути переглянута співробітниками відділу кадрів.

Автоматичне резервне копіювання інформації (окрім 6) не проводиться.

Резервне копіювання інформації 6 проводиться автоматично наприкінці робочого дня системним адміністратором на сервер.

1.3.5 Середовище користувачів

Позаштатними співробітниками є електрик, сантехник, персонал провайдеру ТОВ «Воля-Кабель», охоронець закладу освіти та прибиральниця. Прибиральник має доступ до кімнати наприкінці робочого дня під наглядом головного бухгалтера. Перед входом до кімнати прибиральниця ставить свій підпис і час прибирання в журналі активності на вахті, що знаходиться на першому поверсі закладу освіти.

Таблиця 1.7 – Характеристика користувачів відділу бухгалтерського обліку

№	Посада	Кількість	Роль в ІТС	Рівень кваліфікації
1	Головний бухгалтер	1	Група користувачів 1	Високий
2	Бухгалтер	4	Група користувачів 2	Високий
3	Секретар	1	Група користувачів 3	Високий
4	Системний адміністратор	3	Системний адміністратор,	Високий

Обов’язки головного бухгалтера:

- ведення бухгалтерського обліку;
- підготовка даних для складання звітності;
- стеження за збереженням бухгалтерських документів, їх оформлення; прийом і контроль первинної документації;
- підготовка звітів до рахункової обробки тощо.

Обов’язки бухгалтера:

- ведення фінансових розрахунків;

- облік коштів;
- розрахування затрати на надання освітніх та інших послуг;
- оформлення платежів за комунальні, матеріальні та інші послуги тощо.

Обов'язки секретаря головного бухгалтера:

- прийом та обробка електронних листів;
- оформлення документації та звітності;
- прийом громадян щодо подальшого вирішення їх питань та запитів.

Обов'язки системного адміністратора:

- підготовка та збереження резервних копій даних;
- контроль за станом технічного обладнання;
- встановлення та оновлення налаштувань операційної системи та прикладного програмного забезпечення;
- усунення неполадок при користуванні ПК;
- звітування своєї діяльності тощо.

Сантехник, електрик, прибиральниця тощо – співробітники інших відділів закладу освіти, яких викликають до відділу бухгалтерського обліку за запитом і можуть перебувати у кімнаті тільки при наявності хоча б одного працівника відділу бухгалтерського обліку.

Інформація, що циркулює на ОІД (табл.1.8) пронумерована в таблиці від 1 до 6.

Таблиця 1.8 – Матриця розмежування доступу

Посада	1	2	3	4	5	6
Головний бухгалтер	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	–
Бухгалтер	ЧСРЗДВ	ЧСРЗД	–	ЧСРЗД	ЧСРЗВД	–
Секретар	ЧСРЗДВ	ЧСЗД	–	–	ЧСР	–

Системний адміністратор	ЧСРЗДВ	–	–	–	–	ЧСРЗДВ

Умовні позначення розмежування доступу:

- Ч – читання;
- С – створення;
- Р – редагування;
- З – зберігання;
- В – видалення;
- Д – друк.

1.3.6 Модель порушника

Порушник – це користувач, що здійснює несанкціонований доступ до інформації.

Специфікація середовища ІТС допускає дві групи потенційних порушників:

- внутрішні порушники, що мають доступ до технічних засобів, які обробляють інформацію з обмеженим доступом;
- зовнішні порушники, що знаходяться за межами КЗ

Таблиця 1.9. – Модель порушника

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Сума загроз
Внутрішні порушники						
Головний бухгалтер	М3	К3	З2	Ч3	Д2	13
Бухгалтер	М3	К3	З2	Ч2	Д2	12
Секретар	М3	К3	З1	Ч2	Д2	11
Системний адміністратор	М3	К4	З2	Ч3	Д3	15
Зовнішні порушники						
Хакери	М3	К4	З4	Ч1	Д3	15

Персонал, що обслуговує технічне обладнання та приміщення	М2	К1	З1	Ч1	Д1	6

Продовження таблиці 1.9

Посада	Мотив	Кваліфікація	Можливості	Час дії	Місце дії	Сума загроз
Сторонні особи, що знаходяться за межами КЗ	М2	К1	З1	Ч1	Д1	6

Специфікація моделі порушника за мотивами здійснення порушень:

- М1 – безвідповідальність (недбалість);
- М2 – самоствердження;
- М3 – корислива цілеспрямованість [8].

Специфікація моделі порушника за рівнем кваліфікації та обізнаності щодо ІТС:

- К1 – не володіє знаннями та інформацією про порядок функціонування ІТС, не має навичок щодо користування штатними засобами системи;
- К2 – має навички щодо користування ПК на рівні користувача;
- К3 – володіє базовими знаннями щодо функціонування програмного забезпечення й операційних системі практичними навичками роботи із засобами, що реалізовані в ІТС;
- К4 – володіє знаннями щодо функціонування засобів і механізмів захисту, що використовуються в ІТС, та їх недоліками [8].

Специфікація моделі порушника за показником можливостей використання засобів ІТС для реалізації загроз:

- З1 – має фізичний доступ до автоматизованого робочого місця ІТС, але не є авторизованим користувачем ІТС;
- З2 – має можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- З3 – має можливість керування функціонуванням елементів ІТС, тобто конфігурує програмне забезпечення та комплекс засобів захисту ІТС;
- З4 – не має фізичного доступу до ресурсів ІТС [8].

Специфікація моделі порушника за часом дії:

- Ч1 – під час бездіяльності компонентів системи (під час планових перерв у роботі, у неробочій час);
- Ч2 – під час функціонування ІТС;
- Ч3 – під час перерви у роботі для обслуговування та ремонту [8].

Специфікація моделі порушника за місцем дії:

- Д1 – усередині будівлі та приміщень, але без доступу до технічних засобів ІТС;
- Д2 – з робочих місць користувачів;
- Д3 – з інших об'єктів ІТС, в тому числі каналів зв'язку [8].

Аналізуючи модель порушника, можна зробити висновок, що найбільшу загрозу безпеці ІТС становлять хакери та системний адміністратор, що володіє паролями користувачів та іншою технічною інформацією про АС..

Однак, окрім зовнішніх порушників, загрозу становлять також і працівники відділу бухгалтерського обліку. Вони можуть зчинити злочин через корисливі або особисті мотиви через конфлікт з керівництвом, сварку в колективі тощо.

Висновок: ІТС повинна бути більш контрольованою, а доступ до конфіденційної інформації – розділений.

1.3.7 Аналіз загроз для інформації в ІТС

Існуючі джерела, що загрожують безпеці інформації в ІТС, можна розділити на наступні підгрупи:

- стихійні (природні);
- антропогенні (внаслідок дій людини);

- техногенні (збої в роботі технічних та програмних засобів).

Загрози за природою виникнення: природні, штучні, навмисні, ненавмисні.

Загрози за відношенням до об'єкту захисту: внутрішні, зовнішні.

Загрози за спрямованістю до властивостей інформації: порушення конфіденційності, цілісності та доступності.

Антропогенні загрози

Таблиця 1.10 – Характеристика антропогенних загроз

№	Джерело загрози	Загроза	Вразливість	Наслідки
1	Системний адміністратор	Несанкціонований вхід до АС	Відсутність керування обліковими записами користувачів	Несанкціоноване копіювання ІзОД
2	Користувач системи	Завантаження та встановлення несанкціонованого ПЗ	Відсутність розмежування дій користувачів в системі	Порушення цілісності, конфіденційності та доступності інформації
3	Внутрішні користувачі системи	Несанкціоноване копіювання ІзОД	Відсутність протоколів подій та відстеження операцій з ІзОД	Порушення конфіденційності ІзОД
4	Зовнішні порушники	Ознайомлення з ІзОД внаслідок підглядання або випадкового ознайомлення з ІзОД	Відсутність режиму доступу стороннім особам до технічних засобів	Порушення конфіденційності ІзОД

5	Системний адміністратор	Неконтрольоване призначення повноважень та/або атрибутів доступу користувачам	Відсутність розмежування функцій системного адміністратора	Порушення конфіденційності, цілісності та доступності інформації

Техногенні загрози

Таблиця 1.11 – Характеристика техногенних загроз

№	Джерело загрози	Загроза	Вразливість	Наслідки
1	Єдиний канал зв'язку з мережею Інтернет	Унеможливлювано виконання деяких посадових обов'язків на невизначений час через необхідність доступу до Інтернет	Збій в роботі глобальної мережі Інтернет	Порушення темпу виконання професійних обов'язків
2	Стрибки напруги	Припинення роботи технічних засобів	Збій в системи електропостачання та відсутність стабілізаторів напруги, засобів безперебійного живлення	Уповільнення темпу виконання професійних обов'язків, порушення цілісності та доступності інформації

Загрози, що не є актуальними для даної ІТС

Таблиця 1.12 – Перелік загроз, що не становлять небезпеки для даної ІТС

№	Джерело загрози	Загроза	Вразливість	Наслідки

2	Внутрішні користувачі	Свідомі чи несвідомі помилки користувачів	Низька комп'ютерна грамотність та кваліфікація користувачів	Порушення конфіденційності та цілісності інформації. Загроза не є актуальною через достатню кваліфікацію користувачів (найнижча кваліфікація у секретаря – середня)

Продовження таблиці 1.12

№	Джерело загрози	Загроза	Вразливість	Наслідки
3	Зовнішні порушники	Використання технічних засобів розвідки для збору видової інформації.	Розташування ПК №3-5 біля вікон	Порушення конфіденційності інформації. Загроза не є актуальною через наявність горизонтальних жалюзі на вікнах та малі обороти закладу освіти, що не становлять інтересу для зловмисників
4	Зовнішні порушники	Перехоплення ПЕМВН	ПЕМВН від засобів обробки інформації з	Витік ІзОД. Загроза не є актуальною через малі обороти закладу

			обмеженим доступом	освіти.

Для виявлення найбільш актуальних загроз необхідно провести розподілення загроз за ступенем небезпеки.

Таблиця 1.13 – Розподілення рівня загроз за ступенем небезпеки

Загроза	Рівень загрози				Ступінь небезпеки
	Ймовірність	Збитки			
		К	Ц	Д	
Можливість несанкціонованого входу системним адміністратором до АС за допомогою облікового запису іншого користувача	3	4	3	3	40
Встановлення користувачами несанкціонованого ПЗ	3	4	4	4	48
Несанкціоноване копіювання ІзОД	4	4	1	1	32
Підглядання або ознайомлення з інформацією з обмеженим доступом	2	2	1	1	11
Неконтрольоване призначення системним адміністратором повноважень доступу користувачам	4	4	3	3	53
Відсутність доступу до мережі Інтернет через збої у роботі провайдера	3	1	4	3	32
Стрибки напруги	3	1	4	3	32

Класифікація загроз:

1 – ймовірність мала або відсутня (0-10%);

2 – невірогідна (10-20%);

3 – можлива (20-40%);

4 – достатня вірогідність загрози (40-60%);

5 – висока вірогідність загрози (60-100%).

Ступінь небезпеки можна розрахувати за формулою:

$$Кн = \frac{І*(К+Ц+Д)}{75} * 100$$

ВИСНОВКИ ДО І РОЗДІЛУ

Мною був проаналізований стан інформаційної безпеки бюджетних установ України станом на сьогодні та перспективи на майбутнє. Було з'ясовано, що найбільша кількість кібератак спрямовується саме на бюджетний сектор через його інформаційну цінність та відсутність достатнього рівня захисту інформації.

Розділ містить дані про обстеження об'єкту інформаційної діяльності, а саме: відомості про фізичне середовище, обчислювальну систему, інформаційне середовище, середовище користувачів, аналіз моделі порушника та актуальних загроз.

РОЗДІЛ ІІ. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Формування вимог захисту інформації в ІТС

2.1.1 Визначення вимог до захисту КЗЗ

Автоматизована система, що аналізується, є організаційно-технічною системою, яка включає в себе фізичне середовище, робочий персонал та оброблювальну інформацію.

Проаналізувавши джерела загроз, вразливості й и актуальні загрози, а також ймовірних порушників, можна обґрунтувати вимоги до механізмів захисту.

Усі об’єкти у відділу бухгалтерського обліку, що потребують захисту, умовно можна поділити на три множини:

1) дані на дисковому просторі серверу (паролі від акаунтів користувачів тощо);

2) програмне забезпечення та дані, що зберігаються на жорстких дисках робочих станцій персоналу;

3) фінансові звіти, аналітичні звіти, довідкові матеріали тощо.

Опис послуг і умов представлені в НД ТЗІ 2.5-004-99.

Умова: КД-2 – Базова довірча конфіденційність

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.

Необхідні умови: НИ-1 [4].

Умова: КА-2 – Базова адміністративна конфіденційність

Множина об’єктів, до яких відноситься умова: множина 2.

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

Необхідні умови: НО-1, НИ-1 [4].

Умова: КО-1 – Повторне використання об’єктів.

Множина об’єктів, до яких відноситься умова: оперативна пам'ять комп’ютерів.

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 [4].

Умова: КВ-2 – Базова конфіденційність при обміні.

Множина об’єктив, до яких відноситься умова: множина 3.

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

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

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

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

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

Необхідні умови: НО-1 [4].

Умова: ЦД-1 – Мінімальна довірча цілісність

Множина об’єктів, до яких відноситься умова: 1, 2.

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.

Необхідні умови: НИ-1 [4].

Умова: ЦО-1 –Обмежений відкат

Множина об’єктів, до яких відноситься умова: множина 1

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

Необхідні умови: НИ-1 [4].

Умова: ЦВ-1 – Мінімальна цілісність при обміні

Множина об’єктив, до яких відноситься умова: множина 3.

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

Необхідні умови: НИ-1 [4].

Умова: ДР-1 –Квоти

Множина об’єктів, до яких відноситься умова: системний простір жорстких дисків.

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

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

Необхідна умова: НО-1 [4].

Умова: ДВ-1 – Ручне відновлення

Множина об’єктив, до яких відноситься умова: 1, 2, 3.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Необхідна умова: НО-1.

Умова: НР-2 – Захищений журнал.

Множина об’єктів, до яких відноситься умова: 1, 2 [4].

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.

Необхідні умови: НИ-1, НО-1 [4].

Умова: НИ-2 – Одиночна ідентифікація та автентифікація.

Множина об’єктив, до яких відноситься умова: 2.

Атрибути користувачів: інсталяція та запуск ПЗ, зміна системних файлів, перегляд журнал подій, а також дозвіл на перегляд, редагування, видалення та виконання.

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

Необхідні умови: НК-1 [4].

Умова: НК-1 – Однонаправлений достовірний канал

Множина об’єктів, до яких відноситься умова: 2.

Достовірний зв'язок повинен реалізуватися автентифікацією користувачів (складний пароль) і наданням доступу до АС тим користувачам, які мають для цього необхідні повноваження.

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

Необхідні умови: немає [4].

Умова: НО-2 – Розподіл обов’язків адміністратора

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.

Необхідні умови: НИ-1 [4].

Умова: НЦ-2 – КЗЗ з контролем цілісності.

Множина об’єктів, до яких відноситься умова: 2.

КЗЗ повинно забезпечити перевірку цілісності ПЗ за допомогою засобів автоматичної перевірки і оновлення.

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

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

Необхідні умови: НР-1, НО-1 [4].

Умова: НВ-1 –Автентифікація вузла.

Множина об’єктів, до яких відноситься умова: 2.

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.

Необхідні умови: немає [4].

{КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НВ-1}, Г-2.

Таблиця 2.1 – Вимоги до критеріїв захисту інформації

Критерії	Послуги безпеки	Вимоги до рівня послуг безпеки
Конфіденційність	Довірча конфіденційність	КД-2 –Базова довірча конфіденційність
	Адміністративна конфіденційність	КА-2 – Базова адміністративна конфіденційність
	Повторне використання об’єктів	КО-1 – Повторне використання об’єктів
	Конфіденційність при обміні	КВ-2 –Базова конфіденційність при обміні
Цілісність	Довірча цілісність	ЦД-1 – Мінімальна довірча цілісність
	Відкат	ЦО-1 – Обмежений відкат
	Цілісність при обміні	ЦВ-1 – Мінімальна цілісність при обміні
Доступність	Використання ресурсів	ДР-1 – Квоти
	Відновлення після збою	ДВ-1 – Ручне відмовлення
Спостереження	Реєстрація	НР-2 – Захищений журнал
	Ідентифікація і автентифікація	НИ-2 – Одиночна ідентифікація і автентифікація

Продовження таблиці 2.1

Критерій	Послуги безпеки	Вимоги до послуги безпеки
	Достовірний канал	НК-1 – Однонаправлений достовірний канал
	Розподіл обов'язків	НО-2 – Розподіл обов'язків адміністраторів
	Цілісність комплексу засобів захисту	НЦ-2 – КЗЗ з гарантованою цілісністю
	Ідентифікація та автентифікація при обміні	НВ-1 – Автентифікація вузла)
Гарантії	Рівень гарантій	Г-2

2.1.2 Профіль захищеності

Враховуючи перелік засобів ТЗІ від 01.03.2021 (8) та висновку №1027 (9), операційна система Microsoft Windows 10 Pro, що використовується у відділу бухгалтерського обліку, відповідає вимогам нормативних документів в обсязі умов КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦА-1, ЦВ-1, ДР-1, ДЗ-2, ДВ-2, НР-1, НР-2, НИ-1, НИ-2, НК-1, НО-3, НЦ-2, НТ-2, НВ-1 з гарантією Г-2 згідно НД ТЗІ 2.5-004-99.

Дана операційна система від американської компанії «Microsoft Corporation» містить можливості щодо реалізації вимог до функції безпеки.

Таблиця 2.2 – Профіль захищеності

Вимога до рівня послуг безпеки	Реалізована	Частково реалізована	Не реалізована
КД-2 – Мінімальна довірча конфіденційність	Управління доступом до об'єктів здійснюється завдяки спискам контролю доступу.		

Продовження таблиці 2.2

Вимоги до рівня послуг безпеки	Реалізована	Частково реалізована	Не реалізована
КА-2 – Базова адміністративна конфіденційність			Розмежування об’єктів захисту, що містять ІзОД, за атрибутами доступу
КО-1 – Повторне використання об’єктів			Не реалізовано очищення пам’яті після використання ПЗ, які обробляють ІзОД
КВ-2 –Базова конфіденційність при обміні	Протоколи HTTPS, TLS		
ЦД-1 – Мінімальна довірча цілісність	Облікові записи користувачів з унікальними паролями, розмежування доступу до ІзОД		
ЦО-1 – Обмежений відкат	Вбудовані функції ПЗ, які дозволяють зробити відкат нещодавніх дій, та		

	тимчасові копії файлів ІзОД		

Продовження таблиці 2.2

Вимоги до рівня послуг безпеки	Реалізована	Частково реалізована	Не реалізована
ЦВ-1 – Мінімальна цілісність при обміні	Наявність протоколу захисту транспортного рівня (TLS) під час користування електронною поштою Google (Gmail)		
ДР-1 – Квоти	Організаційні методи захисту		
ДВ-1 – Ручне відмовлення	Інтерфейс КС має можливість виконання ручного відновлення (параметри задаються вручну)		
НР-2 – Захищений журнал	В системі є можливість вибору фізичного носія для зберігання даних реєстрації		
НИ-2 – Одиночна ідентифікація і автентифікація	Вбудовані функції ОС Windows Pro 10. Користувачі проходять автентифікацію за допомогою введення логіну і паролю під час		

	входу в систему		

Продовження таблиці 2.2

Вимога до рівня послуги безпеки	Реалізована	Частково реалізована	Не реалізована
НК-1 – Однонаправлений достовірний канал	Вбудовані функції ідентифікації та автентифікації після запуску ОС		
НО-2 - Розподіл обов’язків адміністраторів		Локальна політика безпеки Windows передбачає функції розподілу адміністратора та користувача. Відсутня реалізація ранжування ролей системного адміністратора та адміністратора безпеки.	
НЦ-2 – КЗЗ з гарантованою цілісністю	Вбудовані функції перевірки цілісності Windows Pro 10 в процесі ініціалізації системи		

Продовження таблиці 2.2

Вимога до рівня послуги безпеки	Реалізована	Частково реалізована	Не реалізована
НВ-1 – Автентифікація вузла	Протокол HTTPS під час з'єднання через веб-браузер Google Chrome		

Загрози витоку інформації через технічні канали зв'язку не становлять небезпеку через специфіку АС та співвідношення технічної реалізації витоку та потенційного прибутку від отриманої інформації.

Рівень визначається переліком вимог до рівня послуг безпеки.

На основі аналізу необхідних послуг було зроблено висновок, що зазначені вище послуги відповідають переліку стандартних вимогу класу «3» рівня «2».

Відповідно до методичного забезпечення, для даної АС обрано клас «3». АС тобто являє собою багатомашинний комплекс, що обробляє інформацію різного ступеня обмеження доступу.

Профіль захищеності: 3.КДЦ.2: {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НВ-1}, Г-2.

В результаті аналізу КС було виявлено:

- послуги, що реалізовано: КД-2, КВ-2, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НЦ-2, НВ-1;
- послуги, що реалізовано частково: НО-2;
- послуги, що не реалізовано: КА-2, КО-1.

2.2 Технічні проектні рішення щодо реалізації вимог безпеки

2.2.1 Елементи політики безпеки

Елементи політики безпеки умовно можна розділити на дві категорії: організаційні заходи політики безпеки та положення.

Розглянемо детальніше усі рішення.

Антивірусний захист

Метою даної політики безпеки є створення таких вимог, виконання яких є обов'язковими усіма робочими станціями, що входять до складу досліджуваної ІТС. Правил політики безпеки повинні дотримуватися усі працівники закладу.

Зміст:

- перевіряйте оновлення антивірусного ПЗ та своєчасно встановлюйте їх;
- ні в якому разі не відкривайте, не завантажуйте та не розсилайте підозрілі файли. Перед тим, як відкрити підозрілий файл, перевірте його за допомогою антивірусного ПЗ або зверніться за допомогою до системного адміністратора;
- ніколи не відкривайте повідомлення, що надходять на електрону пошту від незнайомих відправників;
- завантажте та встановіть модифікацію антивірусного ПЗ;
- за можливістю уникайте прямого дискового доступу (читання та запис), за винятком того, що відповідає необхідним критеріям;
- регулярно чистіть вашу електрону пошту від спаму та інших повідомлень, що не мають відношення до робочих процесів;
- використовуйте тільки ліцензійне ПЗ;
- перевіряйте на вміст шкідливого програмного забезпечення та комп'ютерних вірусів усі зовнішні носії інформації (флеш-накопичувачі тощо).

Так як ОС Windows 10 Pro передбачає наявність вбудованого антивірусного рішення Microsoft Defender, використання наявного антивірусного ПЗ 360 Total Security не є доцільним і повинно бути видалено з робочих станцій працівників відділу бухгалтерського обліку.

Резервне копіювання

Поки катастрофа чи стихійне лихо не торкнулося конкретну організацію, керівництво, як правило, не буде розробляти додатковий захист та дбати про план аварійного відновлення інформації.

Це помилка, адже стихійні лиха та несподівані обставини можуть нагрянути зненацька та призвести до суттєвих матеріальних втрат, а на відновлення даних

доведеться виділити багато часу та коштів. Варто зазначити, що під несподіваними обставинами розуміється не тільки стихійні погодні умови, а й будь-яку ситуацію, що здатна нанести серйозні репутаційні та фінансові втрати.

Дана політика безпеки визначає вимоги до базового плану аварійного відновлення, що повинен бути впроваджений у відділу бухгалтерського обліку комунального вищого навчального закладу та описує процес відновлення технічних систем та інформації, що може бути пошкоджена.

Зміст:

- розробити план реагування на надзвичайні ситуації та стихійні лиха, а саме: назначити відповідального та перші дії, які потрібно виконати в разі аварійного відключення систем;
- розробити план поступових дій, що включає в себе передачу відповідальності на іншого працівника в разі відсутності зв'язку з відповідальним за відновлення інформації в критичних ситуаціях;
- дослідити усю інформацію, що циркулює та обробляється в АС. Описати критичність та конфіденційність інформації;
- розробити список критичних послуг;
- розробити порядок відновлення інформації в короткостроковій та довгостроковій перспективі;
- розробити план резервного копіювання та відновлення пошкодженої інформації. Це надзвичайно важливий пункт, що включає в себе необхідність опису даних, які необхідно резервувати, носії збереження цієї інформації і частоту створення резервних копій;
- розробити порядок заміни пошкодженого чи непрацездатного обладнання. Порядок повинен містити опис існуючого обладнання, його орієнтовану вартість та ряд торгових точок, де цей товар можна придбати чи замінити.

Створення плану аварійного відновлення інформації – це лише теорія, яка буде працювати лише в купі з практикою, тому керівництво повинно виділити певний час для перевірки виконання цього плану. Необхідно раз на рік проводити

профілактичні заходи щодо перевірки ефективності цього плану у штучно створених умовах аварійного відключення.

Режим «чистого столу»

Так як у відділі бухгалтерського обліку щоденно здійснюється прийом великої кількості відвідувачів, режим «чистого столу» є актуальним через блокування загрози витоку видової інформації.

Режим «чистого столу» – це дієвий захід захисту інформації у ситуаціях, коли співробітник звільняється або робочі станції не використовуються. Цей метод необхідний, щоб забезпечити видалення усіх конфіденційних даних в разі потреби.

Метою даного режиму є встановлення мінімальних вимог для підтримки «чистого столу». Така політика відповідає стандартам безпеки ISO 27001/17799 та є невід'ємною частиною заходів контролю конфіденційності.

Зміст:

- співробітники повинні слідкувати, щоб у кінці робочого дня усі ПК повинні бути вимкнені;
- інформація з обмеженим доступом, що міститься на паперових носіях, повинна бути прибрана з робочих місць та знаходитися у ящиках чи шафах, що зачиняються на замок;
- ключі, що використовуються для доступу до інформації з обмеженим доступом, не повинні залишатися без нагляду; повинен бути назначений відповідальний за ключами та визначено місце їхнього перебування;
- паролі від систем, що записані на липких записках чи папері, після закінчення робочого дня повинні бути сховані у ящик, що зачиняється на ключ;
- друкована інформація з обмеженим доступом повинна негайно вилучатися з принтера;
- зовнішні носії збереження чутливої інформації повинні зберігатися у спеціально відведених для цього місцях, що зачинаються на замок;
- знищення документів з обмеженим доступом повинно відбуватися в офіційних захищених контейнерах для шредерів;

- усі друкувальні пристрої повинні очищатися від паперів після друку. Не можна залишати документи без нагляду після завершення друкувального процесу;
- усі працівники повинні забезпечити належний захист інформації з обмеженим доступом на паперових та зовнішніх носіях після закінчення робочого дня. Кожен співробітник несе особисту відповідальність за місцеперебування чутливої інформації в неробочий час.

Положення про використання мережі Інтернет

Мета: Підвищення рівня інформаційної безпеки та захисту інформації з обмеженим доступом за допомогою впровадження правил для співробітників, що використовують Інтернет при виконанні своїх прямих обов'язків

Область дії: Положення поширюється на усіх працівників відділу бухгалтерського обліку комунального вищого навчального закладу, які при виконані своїх прямих обов'язків так чи інакше використовують глобальну мережу Інтернет.

Відповідальні особи: Системний адміністратор.

Положення: Доступ до мережі Інтернет виконується тільки через системи комунального вищого навчального закладу. Використання глобальної мережі можливе у таких випадках:

- отримання та обробки електронних листів;
- робочого листування з партнерами та іншими співробітниками;
- складання фінансових, аналітичних та інших звітів;
- збору інформації в разі потреби додаткової обізнаності у сферах, що впливають на порядок роботи та виконання посадових обов'язків.

Співробітникам забороняється:

- користуватися сторонніми додатками та месенджерами у робочий час;
- листуватися у робочій час на вільні теми з членами сім'ї, друзями та іншими людьми, що не мають відношення до робочого процесу;
- грати в комп'ютерні ігри у робочий час та використовувати інші програми, що відволікають від робочого процесу;

- передавати конфіденційну та чутливу інформацію третім особам.

Використання технічного обладнання для листування та телефонного спілкування з членами сім'ї, друзями тощо у робочий час розглядається експлуатація ресурсів комунального вищого навчального закладу, що суворо заборонено статутом ділової етики, а також законодавствам, політикам і процедурам комунального вищого навчального закладу. Виключення неможливі. В обідню перерву співробітники можуть проводити листування та телефонні розмови з третіми особами виключно за допомогою особистих засобів зв'язку.

Відповідальність: У разі порушення норм і правил, до працівника будуть застосовані дисциплінарні міри та санкції у вигляді позбавлення премій, посад тощо (в залежності від ступеня порушення норм і правил комунального вищого навчального закладу).

Раз на рік дане положення переглядається ректором комунального вищого навчального закладу, заступником ректора, секретарем ректора та системним адміністратором. В разі виникнення надзвичайних ситуацій та непередбачуваних обставин, дане положення може бути переглянуто та редаговано раніше зазначеного терміну перевірки.

Положення про резервне копіювання

Мета: Відновлення інформації з обмеженим доступом внаслідок надзвичайних ситуацій, стихійних лих тощо. Впровадження заходів щодо забезпечення цілісності інформації через аварійне відключення системи. Запобігання втрати інформації через помилки користувачів, комп'ютерні віруси, стихійні лиха, злам системи та витік інформації тощо.

Область дії: Положення поширюється на усіх працівників відділу бухгалтерського обліку комунального вищого навчального закладу. Дане положення застосовується до фінансової та аналітичної звітності, технічної документації, інформації про співробітників та студентів, партнерів тощо.

Відповідальні особи: Системний адміністратор.

Положення:

- впровадження повного резервного копіювання інформації з обмеженим доступом;
- призначення відповідального за збереження та відновлення цілісності інформації в разі стихійного лиха, надзвичайних ситуацій тощо;
- встановлення життєвих циклів та календарних заходів резервного копіювання;
- встановлення груп інформації, що підлягають плановому резервному копіюванню;
- створення звітів про резервне копіювання;
- вимагання дотримування правил резервного копіювання від усіх співробітників відділу бухгалтерського обліку комунального вищого навчального закладу;
- перевірка актуальності інформації, що підлягає плановому резервному копіюванню.

Відповідальність: Порушення правил резервного копіювання може коштувати закладу серйозних наслідків, тому до працівників, що порушують встановленні правила, будуть застосовані суворі міри від штрафів, що будуть стягуватися з заробітної плати, до звільнення з закладу.

Положення про резервне копіювання перевіряється кожні півроку системним адміністратором. Дане положення не може бути змінено чи редаговано навіть у разі виникнення надзвичайних ситуацій.

КА-2 – Базова довірча конфіденційність.

Задля ранжування доступу системний адміністратор повинен розмежувати об’єкти захисту, що містять ІзОД, за атрибутами доступу користувачів в локальній політиці безпеки ОС Windows 10 Pro.

КО-1 – Повторне використання об’єктів.

Системний адміністратор повинен автоматизувати роботу програми звільнення оперативної пам’яті Mem Reduct задля запуску після користувача або процесу ІзОД. Для цього необхідно використати «Планувальник задач», що є вбудованою функцією ОС Windows 10 Pro.

Для звільнення місця для збереження інформації доцільно завантажити безкоштовне ПЗ для автоматизації Automize 12, Системний адміністратор повинен, використовуючи Automize 12, налаштувати програму Mem Reduct 3.3.5.

НО-2 – Розподіл обов'язків адміністратора

Так як системний адміністратор має наднормові обов'язки, що може вплинути на якість виконання його професійних обов'язків, є потреба в розподілі обов'язків системного адміністратора. Задля цього необхідно перекласти частину задач на іншого працівника – секретаря чи іншу довірену особу з числа співробітників, але варто враховувати компетентність та комп'ютерну грамотність співробітників.

Кращим рішенням буде залучити адміністратора з безпеки.

Враховуючи наймання нового співробітника, необхідно обмежити деякі обов'язки системного адміністратора, а саме:

- заборонити інсталяцію і оновлення нового ПЗ без нагляду адміністратора безпеки;
- заборонити змінювати журнал безпеки без дозволу адміністратора безпеки.

Системному адміністратору необхідно впровадити:

- встановити блокування сеансу, якщо активність відсутня впродовж 3-х хвилин;
- -перекласти обов'язки щодо генерації паролів на адміністратора безпеки.

Обов'язки адміністратора з безпеки:

- введення аудиту безпеки КС;
- контроль журналу безпеки;
- генерація надійних паролів для користувачів КС.

Адміністратору з безпеки заборонений вхід в облікові записи користувачів; власного облікового запису в АС не має.

У зв'язку з появою нового співробітника, необхідно внести зміни до матриці розмежування доступу. Адміністратор з безпеки має ряд повноважень, що зазначено в матриці розмежування.

Таблиця 2.3 – Матриця розмежування доступу

Посада	1	2	3	4	5	6.1	6.2
Головний бухгалтер	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	ЧСРЗВД	–	–
Бухгалтер	ЧСРЗДВ	ЧСРЗД	–	ЧСРЗД	ЧСРЗВД	–	–
Секретар*	ЧСРЗДВ	ЧСЗД	–	–	ЧСР	–	–
Адміністратор з безпеки	ЧЗ	–	–	–	–	ЧР	ЧСРЗВД

*виконує обов'язки адміністратора з безпеки

Умовні позначення розмежування доступу:

- Ч – читання;
- С – створення;
- Р – редагування;
- З – зберігання;
- В – видалення;
- Д – друк.

2.2.2 Обґрунтування вибору додаткового КЗЗ

Для виконання професійних обов'язків у відділу бухгалтерського обліку використовується бухгалтерська програма від російської компанії 1С. Це становить ряд загроз і може призвести до втрати даних, передачі конфіденційної інформації, що циркулює на АС, країні-агресору та суттєво збільшує загрозу кібератак.

Ризики користування бухгалтерською програмою від компанії 1С:

- загроза витоку інформації. ПЗ, яке належить країні-агресору, може передавати інформацію третім особам. Так як сервер програми 1С розміщений в РФ, подальше використання даної бухгалтерської програми неможливе;
- репутаційні ризики. Використання програмного забезпечення країни-агресора негативно вплине на репутацію закладу та понесе за собою втрату довіри колег, партнерів та співробітників МОН.
- фінансові збитки. Витрати на користування даною бухгалтерською утилітою можуть бути направлені на фінансування армії країни-агресора.

Проектне рішення містить два шляхи реалізації:

1) Заміна утілити від компанії 1С аналогічної бухгалтерською програмою українського виробництва «BAS Бухгалтерія».

Даний програмний продукт призначений для автоматизації бухгалтерського і податкового обліку, зокрема й підготовки обов'язкової звітності, в організаціях, що здійснюють будь-які види комерційної діяльності: (оптова й роздрібна торгівля, надання послуг, виробництво продукції тощо).

Бухгалтерський та податковий облік у програмі «BAS Бухгалтерія». ведеться відповідно до чинного законодавства України.

ПЗ має дві версії: базова (2240 грн) та корпоративна (18000 грн).

Для виконання професійних обов’язків робітників відділу бухгалтерського обліку необхідно залучити корпоративну версію «BAS Бухгалтерія».

Недоліком даної бухгалтерської програми є відсутність вбудованого комплексу засобів захисту ПЗ, тому є необхідність додаткового впровадження КЗЗ «Гриф-Мережа» версії 4 виробництва ТОВ «Інститут комп’ютерних технологій».

КЗЗ призначений для захисту від несанкціонованого доступу до ІзОД.

Засіб технічного захисту інформації відповідає вимогам нормативних документів СТЗІ в Україні в повному обсязі функцій, зазначених в нормативному документі «Комплекс засобів захисту інформації в локальних обчислювальних мережах від несанкціонованого доступу «Гриф» версія 4. Призначений для захисту від несанкціонованого доступу до інформації з обмеженим доступом.

Технічне завдання UA21541987.00025-019001». Висновок №1034, строк дії – з 24.10.2019 до 24.10.2022 (3 роки).

Даний комплекс засобів захисту забезпечує захист від НСД до ІзОД та регулює правила розмежування доступом [6].

Вартість ПЗ для одного комп'ютера – 7000 грн.

Так як строк дії КЗЗ добігає кінця 24.10.2022, а впровадження КСЗІ потребує певних часових затрат, доцільним буде використання ПЗ для бухгалтерського обліку від українського виробника із вбудованим КЗЗ і строком дії до 2024 року.

2) Бухгалтерське ПЗ із вбудованим КЗЗ

Впровадження бухгалтерського ПЗ із наявним КЗЗ програмного забезпечення є більш доцільним рішенням через економію витрат.

Таблиця 2.4 – Характеристика бухгалтерського ПЗ із вбудованим КЗЗ

Назва	Розробник	Відповідність вимогам	Експертний висновок	Вартість
Комп'ютерна програма «Українська бухгалтерська система УБС» (версія 1.ХХ)	Ісаєв Віктор Миколайович	Відповідає вимогам НД ТЗІ в обсязі функцій, зазначених у документі «КЗЗ комп'ютерної програми «Українська бухгалтерська система УБС» (версія 1.ХХ). Технічні вимоги за критеріями ТЗІ» з рівнем гарантій Г-2	№1229, дійсний з 16.03.2021 до 16.03.2024	14540 грн/од
Програмне забезпечення «Дебет Плюс» версії	Марченко Ярослав Григорович	Відповідає вимогам НД ТЗІ в обсязі функцій, зазначених у документі «КЗЗ ПЗ «Дебет Плюс»	№1231, дійсний з 01.04.2021 до	4500 грн/од

12		версії 12. Технічні вимоги за критеріями технічного захисту інформації» з рівнем гарантій Г-2.	01.04.2024	

Переваги комп'ютерної програми «Українська бухгалтерська система УБС»:

- налаштування під вимоги клієнта та специфічні облікові завдання;
- в умовах критичної інфраструктури працює без доступу до мережі Інтернет.

Переваги програмного забезпечення «Дебет-Плюс»:

- автоматизація усіх ділянок обліку установи;
- відділ навчання та підтримки «Дебет-Плюс» надає консультації в очному та дистанційному форматах;
- ліцензія на користування ПЗ сплачується один раз.

Проаналізувавши усі наявні переваги, рекомендовано запровадити комп'ютерну програму «Українська бухгалтерська система УБС» через можливість функціонувати в умовах критичної інфраструктури без доступу до мережі Інтернет, що зменшує залежність від зовнішніх факторів, підвищує безпеку ІзОД та потребує мінімум потужності від комп'ютерів.

2.2.3 Деінсталяція ПЗ для віддаленого доступу «TeamViewer»

ПЗ для віддаленого доступу встановлене на робочих комп'ютерах усіх співробітників відділу бухгалтерського обліку задля вирішення технічних питань з системним адміністратором в режимі «онлайн». Так як користувачі окрім власного облікового запису мають обліковий запис адміністратора, що порушує умову НО-2, необхідно відмовитися від використання ПЗ для віддаленого доступу «TeamViewer».

Доцільним буде деінсталювати «TeamViewer» та залучити системного адміністратора до вирішення усіх технічних питань в очному форматі. Так як ІТС містить користувачів високого рівнів, що передбачає вирішення незначних

технічних проблем особисто (без залучення системного адміністратора), очні профілактичні заходи не спровокують додаткового навантаження на виконання професійних обов'язків системного адміністратора.

2.2.4 Забезпечення комп'ютерів джерелом безперебійного живлення

Так як існує загроза збоїв в електропостачанні, що може призвести до стрибків напруги та пошкодження жорстких дисків серверу, є необхідність в закупівлі джерела безперебійного живлення (ДБЖ).

Комп'ютер 300 Вт з забезпеченням напруги в 220В.

За час автономної роботи джерело безперебійного живлення повинно виконувати такі задачі:

- збереження інформації на твердо тільних накопичувачах;
- безпечне вимикання;
- безпечне завершення роботи програм і процесів;
- резервне копіювання;
- самостійне вимикання комп'ютера в разі відсутності системного адміністратора чи адміністратора безпеки.

В результаті аналізу часу, впродовж якого виконуються операції на сервері було з'ясовано, що 15 хвилин – оптимальний час для безпечного завершення роботи за допомогою джерела безперебійного живлення.

З'ясуємо значення інших показників:

Т (час, який повинно функціонувати ДЖБ)= 15 хв. = 0, 25 год.

Сумарне навантаження (См) (зазначено в документації прибору, що підключений до ДБЖ) = 200 Вт = 0,2 кВт.

ККД інвертора (за замовченням) = 0,8.

Робочі напруги: 230 В.

Типовий блок живлення – 12В.

$$Є = Т * І,$$

де Є – ємність АКБ;

І – струм.

Необхідний струм споживання:

$$I = \frac{Пс}{12} А$$

Пс – потужність споживання.

$$Пс = \frac{См}{ККД}$$

Пс = 200/0,9 = 250Вт.

I = 250/12=21А.

Є = 21 * 0,25 = 5 А * г.

Проаналізуємо існуючи варіанти ДБЖ:

Таблиця 2.5 – Перелік варіантів ДБЖ для закупівлі

Модель	АКБ	Потужність	Особливості	Гарантії	Вартість
APC Smart-UPS RT 1000VA (кількість виходів – 6)	12В/9А * г	1000Ва/700Вт	Захист від стрибків напруги	24 міс.	22221 грн
APC Smart-UPS X 750VA Rack/Tower LCD (кількість виходів – 8)	12В/9А * г	750Ва/600Вт	Захист від стрибків напруги, короткого замикання	24 міс. – ДБЖ, 12 міс. – АКБ	14999 грн

Порівнявши два пристрої у співвідношенні ціна/якість, доцільним буде закупівля ДЖБ APC Smart-UPS X 750VA Rack/Tower LCD для комп’ютера.

ВИСНОВКИ ІІ РОЗДІЛУ

Розділ ІІ – це спеціальна частина кваліфікаційної роботи, метою якого є формування вимог захисту інформації в ІТС відділу бухгалтерського обліку.

На основі результатів обстеження ІТС, аналізу загроз було обрано профіль захищеності 3КЦД-2: {КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НВ-1}, Г-2.

В результаті було виявлено:

- послуги, що реалізовані: КД-2, КВ-2, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НЦ-2, НВ-1;
- послуги, що реалізовані частково: НО-2;
- послуги, що не реалізовані: КА-2, КО-1.

Були запропоновані технічні проектні рішення щодо реалізації умов безпеки, серед яких організаційні методи політики безпеки та положення, а також обґрунтування впровадження додаткових КЗЗ, необхідність деінсталяції ПЗ для віддаленого доступу «TeamViewer» та аналіз вибору джерела безперебійного живлення для комп’ютерів в ІТС.

РОЗДІЛ ІІІ. ЕКОНОМІЧНИЙ РОЗДІЛ

Основна мета захисту інформації вибраного ОІД від внутрішніх загроз – це мінімізація матеріальних та репутаційних збитків при можливому порушенні інформаційної безпеки комунального закладу освіти.

Окрім безпеки інформації на підприємстві, потрібно подбати й про економічну доцільність. Це означає, що витрати на забезпечення достатнього рівня інформаційної безпеки підприємства не повинні бути більшими за збитки від реалізації загроз її порушення.

Економічний розділ даної кваліфікаційної роботи – це аналіз та перевірка економічної доцільності комунального закладу освіти, результатом чого є технічно-економічне обґрунтування доцільності запровадження запропонованих дій.

3.1 Визначення втрат на розробку КСЗІ

Аналіз економічної доцільності слід почати з підрахунку трудомісткості процесу створення.

Отже, трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

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

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

$tв$ – загальна трудомісткість розробки елементів політики безпеки. tв - тривалість розробки концепції безпеки інформації у організації; ta - тривалість процесу аналізу ризиків;

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

$tозб$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

товр – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

тд – тривалість документального оформлення політики безпеки.

Таким чином, трудомісткість розробки КСЗІ становить:

$$50+20+42+26+60+142=340$$

t=340 години.

Після цього необхідно розрахувати витрати на впровадження КСЗІ. Розрахунок здійснюється за формулою 3.2:

$$Крп = Ззп+Змч \text{ грн,} \quad (3.2)$$

де *Крп* – це витрати на формування проектних рішень;

Ззп – заробітна плата спеціаліста з інформаційної безпеки;

Змч – вартість витрат машинного часу, що необхідні для формування проектних рішень.

Витрати на заробітну плату спеціаліста ІБ розраховуються за формулою 3.3:

$$Ззп = t * Зіб, \text{ грн,} \quad (3.3)$$

де *t* - загальна тривалість розробки політики безпеки, годин;

Зіб – середньо годинна заробітна плата фахівця з інформаційної безпеки з нарахуваннями, грн/годину.

Середньо годинна заробітна плата фахівця з інформаційної безпеки, що може дозволити бюджет вищого навчального закладу, дорівнює 65 грн/год.

Відповідно до формули 3.3, витрати на утримання фахівця з інформаційної безпеки становлять:

$$Ззп = 340 год * 65 грн/год$$

$$Ззп = 22100 грн$$

Витрати машинного часу можна розрахувати за наступною формулою:

$$Змч = t * Смч \text{ грн.,} \quad (3.4)$$

де *t* – трудомісткість розробки на ПК, годин;

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

Вартість однієї години машинного часу ПК можна визначити за допомогою

формули 3.5:

$$Счм=P * tнал * Се+ \frac{Фзал * На}{Fp} + \frac{Клпз * Напз}{FP} грн$$

P – встановлена потужність ПК, кВт;

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

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

На – річна норма амортизації на ПК, частки одиниць;

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

Клпз – вартість ліцензійного програмного забезпечення, грн.;

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

Залишкова вартість ПК визначається на основі фактичного терміном його експлуатації як різниця між початковою вартістю та зносом під час користування пристроєм.

P = 0, 8 кВт;

Се = 1, 68 грн/кВт год;

Ліцензійне програмне забезпечення (для одного ПК):

- Windows 10 Pro – 1100 грн;
- Microsoft Office 365 (версія від 2018 року) – 700 грн;

Загалом: *1100 грн + 700 грн = 1800 грн* (для одного ПК)

Кількість ПК: 6

Вартість ліцензійного програмного забезпечення для 6 ПК: *1800 * 6 = 10800 грн.*

Вартість ПК = 24000 грн, строк корисної служби – 42 місяці.

Мінімальний строк корисної служби = 2 роки (24 місяці).

Накопичена амортизація = *(24000 * 42)/(5 * 12)=16800 грн*

Залишкова вартість: 24000-16800 = 7200 грн.

Розрахуючи, отримаємо:

$$Смч = 1,\ 68\ * 0,8 + \frac{7200 * 0,4}{1920} + \frac{10800 * 0,1}{1920} = 1,344 + 1,5 + 0,\ 57 = 3,\ 414\ грн$$

Тож, витрати на створення КСЗІ за формулою 3.2 становлять:

$$Змч = 340\ *\ 3,\ 414 = 1161\ грн.$$

Отримавши результат розрахунків, дізнаємося вартість розробки КСЗІ:

$$Крп = 22100\ грн + 1161\ грн = 23261\ \ грн.$$

Повна вартість капітальних витрат розраховуються за формулою 3.6:

$$К = Крп + Каз \quad \text{грн,} \tag{3.6}$$

де *Крп* – вартість розробки КСЗІ, тис. грн.;

Каз – вартість закупівлі апаратного забезпечення та додаткового обладнання, тис. грн.

Для впровадження КСЗІ у закладі необхідно придбати таке апаратне та додаткове забезпечення:

- Пристрій безперебійного живлення LP UL3500VA (1 шт., 15000 грн).
- Комп'ютерна програма «Українська бухгалтерська система УБС» (6 шт., 87240 грн).

Підсумовуючи, загальна вартість апаратного забезпечення становить:

$$Каз = 15000 + 87240 = 102240\ грн.$$

Таким чином, повна вартість капітальних витрат за формулою 3.6 дорівнює:

$$К = 23261\ грн + 102240\ грн = 125501\ грн.$$

3.2 Розрахунок експлуатаційних (поточних) витрат

Експлуатаційній витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (тиждень, рік тощо), що виражені у грошовому вигляді.

Поточні витрати можна розрахувати за формулою 3.7:

$$С = Са + Сз + Се + Сєв + Слиз \text{ грн,} \tag{3.7}$$

де *Са* – річний фонд амортизаційних відрахувань;

Сз – річний фонд заробітної плати інженерно-технічного персоналу;

Се – вартість електроенергії, що споживається апаратурою;

Слиц – річні витрати на оновлення та подовження ліцензій ПЗ.

Річний фонд амортизаційний відрахувань (*Са*) визначається за формулою 3.8:

$$Са = Фп/Т \text{ грн} \quad (3.8)$$

де *Фп* – первісна вартість придбаного обладнання;

Т – мінімальний термін корисного використання (дорівнює 5 років для апаратного забезпечення).

$$Са = \frac{15000}{5} = 3000 \text{ грн}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки, розраховується за формулою 3.9:

$$Сз = Зосн + Здод \quad (3.9)$$

Зосн – основна заробітна плата, що визначається, виходячи з місячного посадового окладу;

Здод – додаткова заробітна плата, що визначається в розмірі 8-10% від основної заробітної плати.

Застосовуючи цю формулу до комунального вищого навчального закладу, можна розрахувати витрати на заробітну плату інженерно-технічного персоналу:

$$Сз = Зосн + Здод1 + Здод2 \text{ грн},$$

де *Здод1* – додаткова заробітна плата інженерно-технічного персоналу за проведення річних семінарів та навчання персоналу щодо покращення навичок роботи з ІТС;

Здод2 – додаткова заробітна плата інженерно-технічного персоналу за оновлення існуючих нині положень (що описані у Розділі ІІ) щодо захисту інформації у закладі освіти.

Зосн = 6500 грн;

Здод1 = 1200грн;

Здод2 = 1000грн

Тож, можна провести такі розрахунки:

$$Сз= (6500+1200+1000) * 12 місяців$$

$$Сз = 104400 грн.$$

$Сз (1 місяць) = 8700 грн$

Також, до річного фонду заробітної плати додається єдиний внесок ($Сєв$) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати (за узгодженням з керівником економічної частини кваліфікаційної роботи було встановлено 22%):

$$Сєв = 0,22 * Сз$$

$Сєв = 0,22 *104400 =22,968$

Тепер можна підрахувати річні витрати на оновлення ліцензії ПЗ:

Таблиця 3.1 – Річні витрати на поновлення ліцензії ПЗ

№	Програмне забезпечення	Місячні витрати (1 користувач)	Місячні витрати (6 користувачів)	Річні витрати (6 користувачів)
1	Пакет офісних програм Microsoft Office 365	186,31 грн	1117,86 грн	13414,32 грн

$$Слиц = 13414, 32 грн$$

Тепер необхідно розрахувати вартість електроенергії.

Розмір електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($Сел$) визначається за формулою 3.10:

$$Сел = P * Fp * Це \text{ грн,} \quad (3.10)$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт (становить 0, 8 кВт)

Fp – річний фонд робочого часу системи інформаційної безпеки (за 40-

годинного робочого дня становить 1920)

Це – тариф на електроенергію, грн/кВт*годин (становить 1, 68 грн/кВт*годин)

Тож, вартість електроенергії, що споживається апаратурою, становить:

$$Се = 0{,}8\ кВт * 1920 * 1{,}68\ грн/кВт*годин$$

$$Се = 25804,8 \approx 25805\ грн.$$

Отже, повна вартість річних експлуатаційних витрат становить:

$$С = 3000\ грн + 104400\ грн + 22{,}968\ грн + 13414,32\ грн + 25805\ грн$$

$$С = 146642\ грн.$$

3.3 Оцінка величини збитку у разі реалізації загрози

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховуються, враховуючи ймовірність виникнення інциденту інформаційної безпеки і ймовірних економічних втрат. Ця величина – це та частка прибутку, що може бути втрачена.

Тож, для розрахунку збитків від реалізації загроз можна використати формулу 3.11:

$$U = Пп + Пв + V\ грн,$$

(3.11)

де *Пп* – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

Пв – вартість відновлення працездатності вузла (заміна конфігурацій, оновлення та переустановлення ПЗ тощо);

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

Для розрахунку показників Пп, Пв та V використовують формули 3.12, 3.13 та 3.14 відповідно.

$$Пп = \frac{\sum Зс * Чс}{F} * tn\ грн,$$

де F – місячний фонд робочого часу

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць

tn – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

Чс – чисельність співробітників атакованого вузла.

$Пв = Пві + Ппв + Пзч \; грн,$

де *Пві* – витрати на повторне введення інформації, грн;

Ппв – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

$$V = \frac{O}{F} * (tn + tв + tви) \; грн,$$

де F – місячний фонд робочого часу;

O – обсяг продажів атакованого вузла або сегмента корпоративної мережі грн на місяць;

tn – час простою вузла або сегмента корпоративної мережі внаслідок атаки, грн;

tв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

tви – час повторного введення пошкодженої або загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин.

В свою чергу, *Пви* та *Ппв* розраховуються за формулами 3.15 та 3.16 відповідно:

$$\text{Пви} = \frac{\sum \text{Зс} * \text{Чс}}{F} * t\text{ви грн},$$

де F – місячний фонд робочого часу

Зс – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн/місяць

tві – час повторного введення пошкодженої або загубленої інформації

працівниками атакованого вузла або сегмента корпоративної мережі, годин;

Чс – чисельність співробітників атакованого вузла.

$$\text{Ппв} = \frac{\sum \text{Зо} * \text{Чо}}{F} * tn \text{ грн},$$

де *F* – місячний фонд робочого часу

Зо – заробітна плата обслуговуючого персоналу, грн/місяць

тв – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

Чо – чисельність обслуговуючого персоналу.

Вихідні дані надані у таблиці 3.2.

Таблиця 3.2 – Вихідні дані для розрахунку збитків від реалізації загроз

Умовні позначення	Величина
tn (час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин)	7 годин
tв (час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин)	10 годин
tви (час повторного введення пошкодженої або загубленої інформації працівниками атакованого вузла або сегмента корпоративної мережі, годин)	8 годин
Зо (заробітна плата обслуговуючого персоналу, грн на місяць)	11000 грн
Зс (заробітна плата працівників атакованого вузла або сегмента корпоративної мережі, грн на місяць)	13000 грн/місяць
Чо (чисельність обслуговуючого персоналу, осіб)	1 особа
Чс (чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб)	3 особи

О (обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн на рік)	230000 грн
Пзч (вартість заміни встаткування або запасних частин, грн)	6500 грн
I (число атакованих вузлів або сегментів корпоративної мережі)	2 шт
N (середнє число атак на рік)	5 шт
F (місячний фонд робочого часу)	178 годин
Fr (річний фонд робочого часу)	1987 годин (за 2022 рік)

Таблиця 3.3 – Норми тривалості робочого часу в місяцях 2022 р. при 40-годинному тижні

Показник	Січень	Лютий	Березень	Квітень	Травень	Червень	Липень	Серпень	Вересень	Жовтень	Листопад	Грудень
П’ятиденний робочий день (за стандартних умов 8-годинного робочого дня)												
40 годин на тиждень	151	160	175	160	160	159	168	175	176	159	176	168

Загалом: 1987 годин на 2022 рік.

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

$$\text{Пп} = \frac{\sum \text{Зс} * \text{Чс}}{F} * tn = \frac{13000 * 3}{178} * 7 = 1534 \text{ грн}$$

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

$$Пв = Пви + Ппв + Пзч$$

$$Пви = \frac{\sum Зс * Чс}{F} * tви = \frac{13000 * 3}{178} * 8 = 1753 \text{ грн}$$

$$Ппв = \frac{\sum Зо * Чо}{F} * tn = \frac{11000 * 1}{178} * 7 = 432,5 \text{ грн}$$

Пзч становить 10000 грн (згідно таблиці 3.1)

Тож, *Пв* дорівнює: 1753 грн + 432, 5 грн + 6500 грн = 8686 грн.

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються, враховуючи середньо годинний обсяг продажів і сумарний час простою атакованого вузла або сегмента корпоративної мережі, і становлять:

$$V = \frac{O}{F} * (tn + tв + tви) \text{ грн} = \frac{230000}{178} * (7+10+8) = 32303 \text{ грн}$$

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

$$U = Пп + Пв + V \text{ грн} = 1534 \text{ грн} + 8686 \text{ грн} + 32303 \text{ грн} = 42523 \text{ грн}$$

Загальний збиток від атаки на вузол або сегмент корпоративної мережі закладу освіти розраховується за формулою:

$$B = \sum i \sum n U$$

$$B = 2*5*42523 = 425230 \text{ грн}$$

3.4 Визначення та аналіз показників економічної ефективності запропонованих в кваліфікаційній роботі проектних рішень

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

$$E = B * R - C \text{ грн}$$

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

R– очікування ймовірність атаки на вузол або сегмент корпоративної мережі, частки одиниць (55%);

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

Підрахувавши, можемо отримати загальний ефект:

Е = 425230 * 0,55 – 146642 = 87235 грн.

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу таких показників:

- Сукупна вартість володіння (ТСО);
- Коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);
- Термін окупності капітальних інвестицій *То*.

Показний сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент корпоративної мережі неможливо прорахувати у вартісній формі. В рамках даної кваліфікаційної роботи значення ТСО не використовується, бо було розраховано величину відверненого збитку.

Коефіцієнт ROSI показує, скільки коштів (у гривнях) додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки, то говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, отже:

$$ROSI = \frac{E}{K}$$

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

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

Таким чином, ROSI = 87235/3125501 = 0,695 ≈0,70.

ROSI = 0,70.

Якщо порівнюються два варіанти системи інформаційної безпеки, то обирається варіант з більшим значенням ROSI.

Проект системи інформаційної безпеки визнається доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину

річної депозитної ставки з урахуванням інфляції:

$$ROSI > \frac{(Nдеп - Nінф)}{100}$$

де *Nдеп* – річна депозитна ставка (20%)

Nінф – річний рівень інфляції (5%)

Оскільки 0,70 > 0,15, проект вважається економічно доцільним.

Термін окупності капітальний інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки, і розраховується за такою формулою:

То = К/Е = 125501/87235 =1,4 роки.

ВИСНОВКИ ІІІ РОЗДІЛУ

Мета економічного розділу даної кваліфікаційної роботи – перевірити, чи є проект системи інформаційної безпеки економічно доцільним.

Тож, в цьому розділі були проведені такі розрахунки:

- капітальні витрати на створення КСЗІ (К = 125501 грн);
- річні експлуатаційні витрати на підтримку заходів захисту (С = 146642 грн).

Отримані результати підтверджують вигідність введення в експлуатацію засобів захисту інформації:

- загальний ефект дорівнює 87235 грн;
- коефіцієнт ефективності, що перевищує річний рівень прибутковості альтернативного варіанта (0,70 > 0,15);
- термін окупності капітальних інвестицій – 1,4 роки.

Отже, розробка та впровадження обраних проектних рішень є економічно доцільним та вигідним.

Під час виконання даного розділу мною були засвоєні теоретичні та практичні навички щодо техніко-економічного обґрунтування доцільності запровадження запропонованих в проекті рішень відповідно до обраної теми.

ВИСНОВКИ

Актуальні проблеми в захисту інформації, що циркулює на бюджетних установах, є причиною для створення комплексної системи для захисту інформації вибраного об’єкту кваліфікаційної роботи.

Метою даної роботи є розробка комплексної системи захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

У першому розділі кваліфікаційної роботи був виконаний аналіз наявної обчислювальної системи, інформаційного середовища та середовища користувачів. На основі цих даних, була розроблена модель порушника та виявлені актуальні загрози для інформації в ІТС.

Другий розділ – це спеціальна частина, метою якої є формування вимог захисту інформації в ІТС задля розробки профілю захищеності та проектних рішень.

Третій розділ – економічна частина, метою якої є доведення економічної доцільності впровадження КСЗІ.

Для реалізації КСЗІ у відділу бухгалтерського обліку необхідно виконати впровадження усіх запропонованих рішень, а також провести профілактичні випробування та дослідну експлуатацію.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Відомості Ради національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Diialnist/4797.html?PRINT

2. «Кібербезпека в інформаційному суспільстві». Інформаційно-аналітичний дайджест. – Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Національна бібліотека України імені В.І. Вернадського. URL: http://ippi.org.ua/sites/default/files/2021-9.pdf

3. НД ТЗІ 3.7-003-2005 – Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системи. – ДСТСЗІ СБ України, Київ. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf

4. НД ТЗІ 2.5-004-99 – Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу – ДСТСЗІ СБ України – Київ. URL: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf

5. Методичні рекомендації до виконання кваліфікаційних робіт бакалаврів спеціальності 125 – Кібербезпека. – Національний технічний університет «Дніпровська Політехніка», Факультет інформаційних технологій, кафедра безпеки інформації і телекомунікацій. – Герасіна О.В., Тимофєєв Д.С., Кручінін О.В., Мілінчук Ю.А.

6. Опис комплексу засобів захисту інформації від НСД «Гриф-Мережа». Інститут комп'ютерних технологій. URL: https://www.ict.com.ua/?lng=1&sec=8&art=41

7. Експертний висновок КЗЗ «Гриф-Мережа» версії 3, виробництва ТОВ «Інститут комп'ютерних технологій» №1034 (з 24.10.2019 до 24.10.2022).

8. Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла Інтернет-доступу – Комаров М.Ю., Ониськова А.В., Гончар С.Ф.

9. Принципи та порядок розробки КСЗІ в ІТС – Землянко Ю.В., Замула О.А., Ткач О.О., Литвинова Н.І., Пересічанська Я.А. URL: https://openarchive.nure.ua/bitstream/document/861/1/460-469.pdf

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітки
Найменування				
1	А4	Реферат	2	–
2	А4	Список умовних скорочень	1	–
3	А4	Зміст	2	–
4	А4	Вступ	1	–
5	А4	Розділ І	37	–
6	А4	Розділ ІІ	25	–
7	А4	Розділ ІІІ	13	–
8	А4	Висновки	1	–
9	А4	Перелік використаних джерел	1	–
10	А4	ДОДАТОК А	1	–
11	А4	ДОДАТОК Б	1	–
12	А4	ДОДАТОК В	1	–
13	А4	ДОДАТОК Г	2	–
14	А4	ДОДТАОК Ґ	1	–

ДОДАТОК Б. ФОРМА ТА ЗМІСТ АКТУ КАТЕГОРІЮВАННЯ ОБЄКТУ

ЗАТВЕРДЖУЮ
Керівник установи-власника
(розпорядника, користувача) об'єкта
ректор Кришталь М.П.
(посада, підпис, ініціали, прізвище)
15.06. 2022

АКТ
категоріювання відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»
(найменування об'єкта категоріювання)

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

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

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

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

5. Встановлена категорія: 4 категорія

Голова комісії _____ Коваленко Р. О.
(підпис) (ініціали, прізвище)
Члени комісії: _____ Корнілєнко М.М.
(підпис) (ініціали, прізвище)
15.06.2022

ДОДАТОК В. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Шрамко_ДІ_125_18_1_ПЗ.docx
2. Шрамко_ДІ_125_18_1_ПЗ.pdf
3. Шрамко_ДІ_125_18_1_ДМ.pptx
4. Шрамко_ДІ_125_18_1_ПЗ.pdf.p7s

ДОДАТОК Г. ВІГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

В І Д Г У К
на кваліфікаційну роботу студентки групи 125-18-1
Шрамко Дарини Ігорівни

на тему: «Комплексна система захисту інформації інформаційно-телекомунікаційної системи відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки»»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, викладених на_____сторінках.

Метою кваліфікаційної роботи є забезпечення заданого рівня безпеки інформації, яка обробляється в ІТС відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності бакалавра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: обстеження середовищ функціонування ІТС, розробка моделі порушника, аналіз джерел загроз та вразливостей, визначення актуальних загроз, формування вимог до захисту інформації та розробка проектних рішень їх реалізації.

Запропоновано матрицю розмежування доступу, розроблені положення політики безпеки щодо: антивірусного захисту, резервного копіювання, режиму «чистого столу», використання глобальної мережі та резервного копіювання. Розроблені проектні рішення впровадження додаткового КЗЗ та забезпечення резервного електроживлення.

Практичне значення результатів кваліфікаційної роботи полягає у адаптації запропонованих рішень до особливостей відділу бухгалтерського обліку комунального вищого навчального закладу «Дніпропетровська академія музики ім. М. Глінки».

До недоліків відноситься недостатньо обґрунтована модель загроз та профіль захищеності.

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

За час дипломування Шрамко Д.І. проявила себе фахівцем, здатним достатньо самостійно вирішувати поставлені задачі та заслуговує присвоєння кваліфікації бакалавра за спеціальністю 125 Кібербезпека, освітньо-професійна програма «Кібербезпека» .

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

Кваліфікаційна робота заслуговує оцінки «добре».

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

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

ДОДАТОК Ґ . ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОЇ ЧАСТИНИ

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 95 б. («відмінно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)