Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

КОМПЛЕКСНА МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:
«Аудит інформаційної безпеки департаментів Вінницької міської ради. Частина 1. Методика проведення аудиту»

Виконав: студент 2 курсу групи 1БС-23м
спеціальності 125 Кібербезпека та захист інформації
_____ Ігор ПИЛЯВЕЦЬ
Керівник: к. т. н., доц., доцент каф. ЗІ
_____ Олеся ВОЙТОВИЧ
«13» 12 2024 р.
Опонент: к. т. н., доц., доц. каф. ПЗ
_____ Галина ЧЕРНОВОЛИК
«13» 12 2024 р.

Допущено до захисту
Завідувач кафедри ЗІ
д. т. н., проф.
_____ Лужецький В. А.
«13» 12 2024 р.

Вінниця ВНТУ – 2024 року

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти II (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека та захист інформації
Освітньо-професійна програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ,
д. т. н., проф.
Володимир ЛУЖЕЦЬКИЙ
«18» 09 2024 року

З А В Д А Н Н Я
НА КОМПЛЕКСНУ МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Пилявцю Ігорю Юрійовичу

1. Тема роботи: «Аудит інформаційної безпеки департаментів Вінницької міської ради. Частина 1. Методика проведення аудиту»
   керівник роботи: Войтович Олеся Петрівна, к. т. н., доцент кафедри ЗІ,
   затверджені наказом ректора ВНТУ від 17 вересня 2024 року №310.

2. Строк подання студентом роботи 20 грудня 2024 р.

3. Вихідні дані до роботи:
   - аналіз міжнародних стандартів;
   - аналіз державних вимог;
   - аналіз підприємства;
   - інформаційний аудит;
   - методика аудиту підрозділів Вінницької міської ради.

4. Зміст текстової частини: Вступ. 1 Аналіз джерел за напрямком аудиту інформаційної безпеки. 2 Аналіз об'єкту аудиту. 3 Розробка методики аудиту. 4 Економічна частина. Висновки. Перелік використаних джерел. Додатки.

5. Перелік ілюстративного матеріалу: Результати інформаційного аудиту департаментів вінницької міської ради. Послідовність дій при аудиті інформаційної безпеки за стандартами ISO 27000. Етапи процесу постійного вдосконалення. Співставлення вимог ISO 27001 та НДТЗІ 2.5-004-99. Співставлення вимог ISO 27002 та НДТЗІ 2.1-002-07.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Олеся ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	16.09.24	21.09.24
2	Олеся ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	28.09.24	04.11.24
3	Олеся ВОЙТОВИЧ, к.т.н., доц. каф.ЗІ	05.11.24	18.11.24
4	Ольга РАТУШНЯК, к.т.н., доц., доц. каф. ЕПВМ	19.11.24	21.11.24

7. Дата видачі завдання: 1 вересня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів комплексної магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз завдання. Вступ	1.09.2024 –15.09.2024	
2	Аналіз інформаційних джерел за напрямком комплексної магістерської кваліфікаційної роботи	16.09.2024-20.09.2024	
3	Науково-технічне обґрунтування	21.09.2024-28.09.2024	
4	Аналіз стандартів для проведення аудиту	28.09.2024-10.10.2024	
5	Аналіз та формування вимог до методики	11.10.2024-27.10.2024	
6	Проведення інформаційного аудиту	28.10.2024-04.11.2024	
7	Розробка методики аудиту	05.11.2024-18.11.2024	
8	Розробка розділу економічного обґрунтування	19.11.2024-21.11.2024	
9	Оформлення пояснювальної записки	22.11.2024-24.11.2024	
10	Попередній захист та доопрацювання МКР	25.11.2024-26.11.2024	
11	Виправлення зауважень, підготовка ілюстративного матеріалу	27.11.2024-08.12.2024	
12	Перевірка комплексної магістерської кваліфікаційної роботи на наявність текстових запозичень	09.12.2024-10.12.2024	
13	Предетавлення МКР до захисту, рецензування	11.12.2024-16.12.2024	
14	Захист МКР	17.12.2024-20.12.2024	

Студент _____ Ігор ПИЛЯВЕЦЬ

Керівник роботи _____ Олеся ВОЙТОВИЧ

АНОТАЦІЯ

УДК 004.81

Пилявець І. Ю. Аудит інформаційної безпеки департаментів Вінницької міської ради. Частина 1. Методика проведення аудиту. Комплексна магістерська кваліфікаційна робота зі спеціальності 125 – Кібербезпека, освітня програма – Безпека інформаційних і комунікаційних систем. Вінниця: ВНТУ, 2024. 84 с.

Укр. мовою. Бібліогр.: 29 назв; рис.: 16; табл.: 12.

Комплексна магістерська кваліфікаційна робота зосереджена на створенні методики аудиту інформаційної безпеки для Вінницької міської ради. У процесі виконання дослідження було здійснено ґрунтовний аналіз міжнародних і державних стандартів, які можуть бути застосовані під час проведення аудиту інформаційної безпеки. На основі цього аналізу розроблено методику комплексного аудиту, адаптовану до потреб міської ради та вимог сучасної інформаційної безпеки.

Ілюстративна частина роботи представлена 12 плакатами, які демонструють результати моделювання та проведених досліджень. Вони наочно відображають ключові етапи та висновки роботи, що дозволяє краще зрозуміти впроваджену методику та її ефективність.

Економічна частина роботи присвячена оцінці науково-технічного потенціалу та економічної ефективності розробки.

Ключові слова: аудит, інформаційна безпека, кібербезпека, моніторинг, аналіз ризиків.

ABSTRACT

Pyliavets I. Y. Audit of information security of departments of Vinnytsia City Council. Part 1. Audit methodology. Comprehensive master's qualification work in specialty 125 - Cybersecurity, educational program - Security of information and communication systems. Vinnytsia: VNTU, 2024. 84 p.

In Ukrainian. Bibliography: 29 titles; fig.: 16; tab.: 12.

The comprehensive master's qualification work focuses on creating an information security audit methodology for Vinnytsia City Council. In the process of conducting the study, a thorough analysis of international and state standards that can be applied during an information security audit was carried out. Based on this analysis, a comprehensive audit methodology was developed, adapted to the needs of the city council and the requirements of modern information security.

The illustrative part of the work is presented by 12 posters that demonstrate the results of modeling and research. They clearly reflect the key stages and conclusions of the work, which allows you to better understand the implemented methodology and its effectiveness.

The economic part of the work is devoted to assessing the scientific and technical potential and economic efficiency of the development.

Keywords: audit, information security, cybersecurity, monitoring, risk analysis.

ЗМІСТ

ВСТУП

У сучасному світі стрімкий розвиток технологій і зростання залежності бізнесу від цифрових систем та інформації висувають питання інформаційної безпеки на передній план. Забезпечення цілісності, конфіденційності та доступності даних стає критично важливим завданням для організацій будь-якого масштабу та галузі. Інформаційна безпека перетворилася на ключовий елемент успішного функціонування підприємств у цифровому середовищі. Постійні загрози, пов’язані з кібератаками, витоками конфіденційної інформації та технологічними ризиками, підкреслюють необхідність впровадження ефективних систем управління безпекою інформації.

Міжнародні стандарти, такі як ISO 27001 та NIST Cybersecurity Framework, пропонують чіткі орієнтири для організації процесів захисту інформації. Вони сприяють створенню системного підходу до управління ризиками та забезпечення безпеки даних, враховуючи як технічні, так і організаційні аспекти.

Актуальність проведення дослідження у межах комплексної магістерської кваліфікаційної роботи визначається необхідністю розробки ефективних підходів до забезпечення інформаційної безпеки в умовах активної цифровізації. Недостатній рівень захисту інформації може мати серйозні наслідки для організацій, зокрема фінансові втрати, погіршення репутації та зниження довіри клієнтів і партнерів. У сучасному середовищі, де цифрові платформи впроваджуються швидкими темпами, а обсяги даних постійно зростають, частота кібератак і витоків конфіденційної інформації неухильно збільшується. Зловмисники активно шукають уразливості в системах безпеки, що створює значні ризики для діяльності організацій.

Міжнародна серія стандартів ISO 27000 є визнаним еталоном у сфері інформаційної безпеки. Вона забезпечує структурований підхід до управління ризиками та захисту інформації. Разом із тим, спеціалізовані стандарти, які охоплюють конкретні аспекти інформаційної безпеки, можуть виявитися більш ефективними залежно від потреб конкретної організації. Для підвищення рівня захисту інформації необхідно розробити комплексну методику аудиту

інформаційної безпеки, що базуватиметься на найкращих світових практиках та підходах.

Об’єктом дослідження в межах цієї роботи є процес аудиту інформаційної безпеки.

Предметом дослідження виступає методика проведення такого аудиту.

Метою вдосконалення методики аудиту інформаційної безпеки державних установ за рахунок врахування та поєднання вимог міжнародних та державних стандартів, що дозволяє скоротити витрати під час підготовчих етапів.

Для досягнення мети необхідно виконати наступні завдання:

- аналіз міжнародних стандартів аудиту інформаційної безпеки;
- аналіз державних вимог інформаційної безпеки;
- інформаційний аудит підрозділів Вінницької міської ради;
- побудова методики аудиту.

Наукова новизна. Вдосконалення методики аудиту інформаційної безпеки державних установ за рахунок врахування та поєднання вимог міжнародних та державних стандартів, що дозволяє скоротити витрати під час підготовчих етапів.

Практична цінність полягає у тому, що розроблена комплексна методика аудиту підрозділів Вінницької міської ради дозволяє використовувати найкращі світові практики з забезпечення інформаційної безпеки враховуючи державні вимоги.

Результати комплексної магістерської роботи доповідалися на таких конференціях:

- Міжнародна науково-практична інтернет-конференція студентів, аспірантів та молодих науковців «МОЛОДЬ В НАУЦІ: ДОСЛІДЖЕННЯ, ПРОБЛЕМИ, ПЕРСПЕКТИВИ» (МН-2024) [1];
- Міжнародній науково-практичній Інтернет-конференція студентів, аспірантів та молодих науковців «МОЛОДЬ В НАУЦІ: ДОСЛІДЖЕННЯ, ПРОБЛЕМИ, ПЕРСПЕКТИВИ (МН-2025) [2-3].

За результатами комплексної магістерської кваліфікаційної роботи **опубліковано троє** тез.

1 АНАЛІЗ ДЖЕРЕЛ ЗА НАПРЯМКОМ АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Актуальність

Аудит інформаційної безпеки Вінницької міської ради (далі ВМР) є актуальним через постійне зростання кіберзагроз та необхідність захисту значних обсягів конфіденційної інформації громадян. ВМР зберігає персональні дані, фінансову інформацію та інші важливі дані, стають привабливими мішенями для кіберзлочинців, що зумовлює потребу у регулярному аудиті для виявлення загроз.

Дотримання законодавчих вимог і національних стандартів, зокрема Закону України «Про захист персональних даних», є ще одним критично важливим аспектом. Крім того, вплив європейських стандартів, як-от GDPR, вимагає дотримання правил захисту даних навіть на рівні органів місцевої влади. Аудит допомагає забезпечити відповідність цим вимогам, що знижує ризик санкцій та позовів.

Успішне проведення аудиту також підвищенню рівня довіри громадян до органів місцевої влади. Захищені дані сприяють впевненості громадян у безпеці їхніх персональних відомостей, що покращує взаємовідносини з ВМР. Окрім цього, забезпечення належного захисту даних є важливою умовою для безперервності надання міських послуг. Інциденти в кібербезпеці можуть паралізувати доступ до критично важливих сервісів, що негативно позначається на життєдіяльності міста.

Аудит також дозволяє оцінити відповідність ВМР міжнародним стандартам кібербезпеки, таким як ISO 27001, NIST, PCI DSS, GDPR та COBIT. Це сприяє оптимізації процесів захисту інформації, що підвищує ефективність заходів безпеки. Оскільки державні установи часто стають мішенями атак, зокрема в умовах війни, аудит забезпечує готовність до новітніх загроз і дозволяє оперативно адаптуватися до змін у кіберсередовищі.

Таким чином, аудит інформаційної безпеки є необхідним для захисту конфіденційних даних, зниження ризиків і забезпечення безперервності міських сервісів, що робить його актуальним і важливим для сталого розвитку цифрової інфраструктури міської ради в умовах сучасних викликів.

1.2 Аналіз міжнародних стандартів

1.2.1 ISO 27000

Стандарти серії ISO 27000 формують цілісну екосистему для управління інформаційною безпекою, яка охоплює створення, впровадження, підтримку та постійне вдосконалення системи управління інформаційною безпекою (ISMS). Вони взаємодіють між собою, забезпечуючи організаціям чіткий, послідовний і масштабований підхід до захисту інформації та управління ризиками.

У центрі цієї екосистеми знаходиться стандарт ISO 27001, який визначає основні вимоги до побудови ISMS (рис. 1.1)[4].

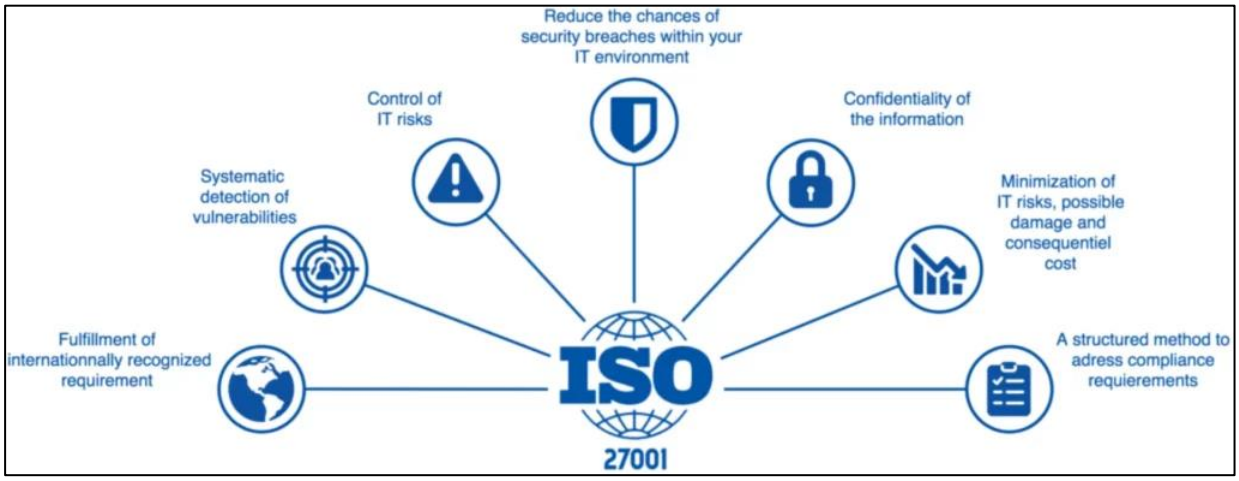


Рисунок 1.1 – Основні завдання ISO 27001

Його ключова мета полягає в захисті конфіденційності, цілісності та доступності інформації через аналіз ризиків і впровадження заходів контролю. Методологія PDCA (Plan-Do-Check-Act) забезпечує постійне вдосконалення системи. Цей підхід дозволяє організаціям систематично ідентифікувати загрози

та ризики, впроваджувати відповідні заходи безпеки, моніторити їхню ефективність і здійснювати коригувальні дії.

Для ефективного впровадження заходів безпеки стандарт ISO 27002 надає детальні рекомендації щодо конкретних практик і контролів [5]. Наприклад, він описує, як управляти доступом до інформаційних активів, використовувати криптографічні засоби або забезпечувати фізичну безпеку приміщень. Таким чином, ISO 27002 виступає як практичний довідник для впровадження вимог ISO 27001.

Оскільки управління ризиками є центральним елементом ISMS, стандарт ISO 27005 забезпечує структуру для їх оцінки та мінімізації [6]. Він деталізує процеси ідентифікації активів, аналізу загроз і вразливостей, оцінки впливу ризиків і розробки стратегій їхнього зниження. Це створює міцну основу для прийняття рішень на основі розуміння загроз і вразливостей.

Для забезпечення прозорості та ефективності функціонування ISMS важливим є аудит. Стандарти ISO 19011 та ISO 27007 забезпечують керівництво для проведення внутрішніх і зовнішніх аудитів[7-8]. ISO 19011 описує загальні принципи аудиту систем управління, а ISO 27007 зосереджується на специфіці перевірки ISMS. Аудитори аналізують відповідність політик і процедур вимогам ISO 27001, перевіряють виконання заходів безпеки та надають рекомендації щодо покращення системи.

Подальшим етапом є сертифікація, яка підтверджує, що ISMS відповідає вимогам ISO 27001. У цьому контексті стандарти ISO 27006 та ISO 17021-1 визначають вимоги до сертифікаційних органів [9-10]. Вони гарантують, що процес сертифікації є об'єктивним, прозорим і базується на високих професійних стандартах. Це забезпечує довіру до сертифікатів і їхнього впливу на репутацію організації.

Роль стандарту ISO 31000 у цій екосистемі полягає в забезпеченні загальної методології управління ризиками [11]. Цей стандарт розглядає управління ризиками не лише як частину інформаційної безпеки, а й як інтегрований підхід до управління всіма аспектами діяльності організації. Він

сприяє створенню культури ризик-менеджменту, яка пронизує всі рівні прийняття рішень.

Таким чином, серія ISO 27000 працює як єдиний механізм, де кожен стандарт виконує свою роль: ISO 27001 задає основну структуру ISMS, ISO 27002 деталізує заходи безпеки, ISO 27005 забезпечує управління ризиками, ISO 19011 і ISO 27007 допомагають у проведенні аудитів, а ISO 27006 та ISO 17021-1 гарантують якість сертифікаційних процесів. Разом ці стандарти утворюють цілісну систему для захисту інформаційних активів, яка є адаптивною до будь-якої організації, незалежно від її розміру чи галузі.

1.2.2 NIST Cybersecurity Framework (CSF)

У сучасному світі, де кіберзагрози змінюються надзвичайно швидко, забезпечення надійної кібербезпеки є особливо актуальним. Для надання організаціям надійного інструменту для захисту від кіберзагроз було створено NIST CSF – універсальний фреймворк для управління ризиками у сфері кібербезпеки. Згідно з дослідженням Gartner у 2022 році, NIST CSF став одним із найкращих фреймворків для управління кіберризиками [12]. У лютому 2024 року його оновили до версії 2.0, і ця стаття розглядає всі основні зміни.

Фреймворк NIST CSF розроблений Національним інститутом стандартів і технологій США, щоб допомогти організаціям керувати ризиками кібербезпеки. Хоча його впровадження не є обов'язковим, компанії, які прагнуть підвищити рівень інформаційної безпеки та продемонструвати це, можуть скористатися аудитом для оцінки відповідності вимогам. Це дозволяє чітко визначити, спланувати та пріоритезувати необхідні кроки для забезпечення надійного захисту.

Одним із прикладів застосування NIST CSF є Програма діагностики стану кібербезпеки, яку реалізує USAID Cybersecurity Activity для операторів критичної інфраструктури. З часу своєї появи у 2014 році і до оновлення до версії 1.1 у 2018 році фреймворк зазнав значних змін. Версія 2.0, представлена у 2024 році, стала першим масштабним оновленням за останнє десятиліття та внесла суттєві доповнення.

NIST CSF 2.0 розширює функціональність для зручності використання в різних галузях і компаніях різного розміру. Оновлений фреймворк додав нову функцію «Управління», що підкреслює важливість управлінських аспектів у кібербезпеці. Ця функція підтримує організації в управлінні ризиками, допомагаючи визначити пріоритети та досягати цілей, що ставлять інші функції, зокрема «Ідентифікація», «Захист», «Виявлення», «Реагування» та «Відновлення»(рис. 1.2). Зміщення акценту на управління дозволяє організаціям отримати більш цілісне уявлення про вплив загроз на їхню IT-інфраструктуру, дані та бізнес у цілому.

Рисунок 1.2 – Функції NIST Cybersecurity Framework

Для впровадження функції «Управління» у версії 2.0 фреймворк містить нові категорії. Серед них: організаційний контекст, що стосується управління ризиками, нагляд для постійного вдосконалення стратегії ризик-менеджменту, стратегія управління ризиками, яка підтримує оперативні рішення з ризик-менеджменту, а також чітко визначені ролі та обов'язки для постійного вдосконалення та послідовної оцінки ефективності.

Крім того, нова версія включає останні рекомендації щодо новітніх загроз і технологій, таких як штучний інтелект, і може застосовуватися разом із Фреймворком управління ризиками ШІ від NIST, опублікованим у січні 2023 року. Оновлення до NIST CSF 2.0 також передбачає набір допоміжних

інструментів і ресурсів, зокрема інструкцію зі швидкого впровадження (QSG), щоб забезпечити легкість використання стандарту для організацій різного масштабу.

Директор NIST Лорі Е. Локасіо зазначила, що CSF 2.0 є комплексним набором ресурсів, адаптованим для використання на кожному етапі розвитку організації. Нова редакція також пропонує приклади впровадження та інформаційний каталог, який регулярно оновлюється онлайн, а введення профілів організацій у фреймворку дозволяє організаціям швидше визначити свій поточний і цільовий профіль кібербезпеки.

1.2.3 PCI DSS (Payment Card Industry Data Security Standard)

PCI DSS (Payment Card Industry Data Security Standard) – це комплексний стандарт безпеки, який встановлює вимоги для захисту даних платіжних карток під час їх обробки, зберігання та передачі [13]. Він регулюється Радою стандартів безпеки платіжних карт, створеною провідними платіжними системами: Visa, MasterCard, American Express, Discover і JCB. Метою PCI DSS є допомога організаціям у забезпеченні надійного захисту даних платіжних карток, зокрема через впровадження необхідних заходів безпеки, що мінімізують ризики крадіжки та несанкціонованого доступу.

Цей стандарт містить 12 основних вимог, розділених на шість категорій, які охоплюють ключові аспекти кібербезпеки(рис. 1.3). Серед них є вимоги щодо створення та підтримки безпечної мережі, включаючи налаштування конфігурацій файрволів та уникнення стандартних паролів і заводських налаштувань для систем. PCI DSS також вимагає захисту збережених даних платіжних карток, забезпечення їх шифрування як під час зберігання, так і під час передачі через публічні мережі.

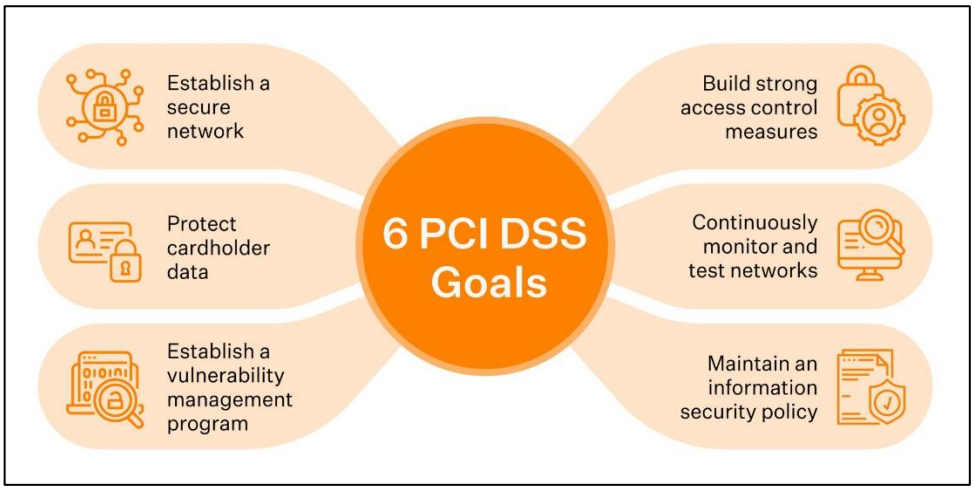


Рисунок 1.3 – Шість категорій PCI DSS

Стандарт також зобов'язує організації до регулярного управління вразливостями, яке включає використання антивірусного програмного забезпечення, а також оновлення систем і додатків для захисту від загроз. Контроль доступу є ще одним важливим аспектом PCI DSS: доступ до даних платіжних карток надається лише тим співробітникам, для яких це необхідно, а кожному користувачеві присвоюється унікальний ідентифікатор. Фізичний доступ до карткових даних обмежений, щоб запобігти випадковим чи зловмисним витокам інформації.

Моніторинг і тестування мереж також є невід'ємною частиною стандарту. Організації зобов'язані регулярно відстежувати активність у своїх системах і проводити тестування, щоб своєчасно виявляти та усувати потенційні вразливості. Усі ці заходи підкріплені інформаційною політикою безпеки, яка охоплює всіх співробітників та сприяє підтриманню високого рівня обізнаності про загрози та важливість захисту даних.

Виконання вимог PCI DSS є обов'язковим для всіх організацій, що зберігають, обробляють або передають дані платіжних карток. Це стосується як великих ритейлерів, так і невеликих онлайн-магазинів, а також провайдерів платіжних послуг. Завдяки впровадженню стандарту організації не лише підвищують рівень безпеки, а й демонструють свою прихильність до захисту

платіжних даних своїх клієнтів, що є важливим для збереження довіри і репутації на ринку.

1.2.4 GDPR (General Data Protection Regulation)

GDPR, або Загальний регламент захисту даних, прийнятий Європейським Союзом, з 25 травня 2018 року діє як основоположний закон для захисту прав і конфіденційності особистих даних громадян ЄС [14]. Його головне завдання – забезпечити безпеку і захист персональної інформації незалежно від місця її обробки (рис. 1.4).

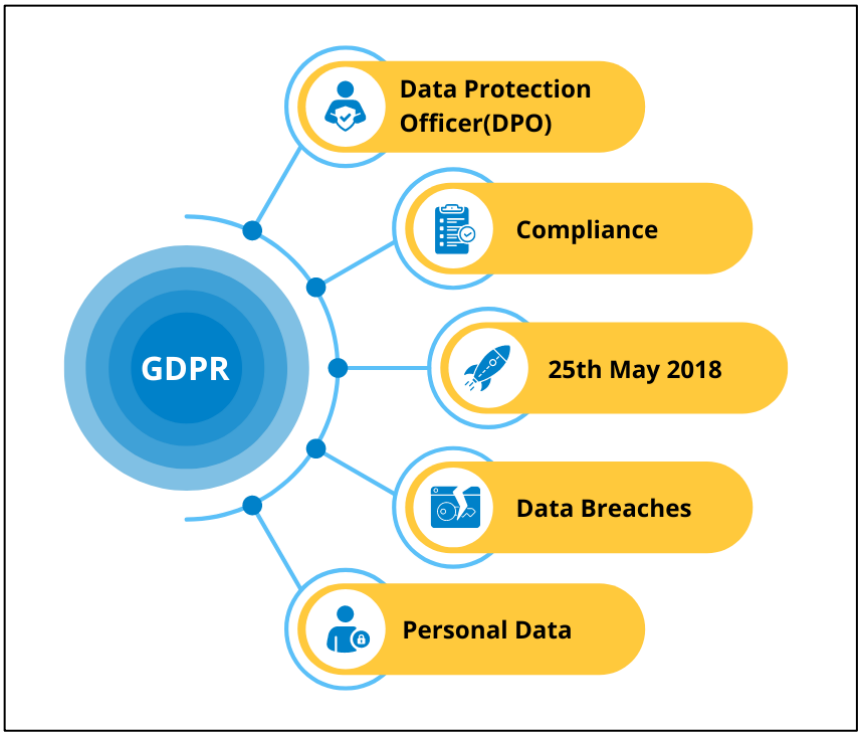


Рисунок 1.4 – Завдання General Data Protection Regulation

Для цього регламент передбачає жорсткі вимоги до компаній та організацій щодо збору, обробки, зберігання і передачі персональних даних, базуючись на принципах законності, прозорості та безпеки.

GDPR зобов'язує організації збирати тільки ті дані, що потрібні для конкретних і законних цілей, і зберігати їх лише на визначений термін, забезпечуючи точність і актуальність. Він також гарантує конфіденційність, цілісність та захист даних від несанкціонованого доступу або втрат. Це передбачає надання фізичним особам (суб'єктам даних) низки важливих прав,

таких як право на доступ до власних даних, право на їх виправлення, видалення або обмеження обробки. Суб’єкти даних також можуть переносити свої дані до іншого контролера та заперечувати проти обробки для маркетингу чи профілювання. Також передбачено можливість уникати рішень, які приймаються виключно автоматизованими засобами і можуть мати юридичні наслідки для особи.

Ключовим принципом GDPR є прозорість, що зобов'язує організації інформувати користувачів про обробку їхніх даних. Крім того, регламент вимагає отримання чіткої і добровільної згоди на обробку персональних даних та застосування надійних заходів захисту для запобігання витокам. У разі порушення захисту даних компанії зобов'язані повідомляти про це регуляторні органи протягом 72 годин. Також передбачено призначення відповідальної особи із захисту даних (Data Protection Officer, DPO) для організацій, які обробляють великий обсяг інформації.

GDPR змінив підхід до конфіденційності даних не лише в Європі, а й у всьому світі, ставши еталоном для встановлення нових стандартів обробки персональної інформації. Регламент вимагає від компаній прозорості, відповідальності та надає громадянам більше контролю над своїми даними, підвищуючи рівень захисту конфіденційності у цифровому середовищі.

1.2.5 COBIT (Control Objectives for Information and Related Technologies)

COBIT (Control Objectives for Information and Related Technology) — це фреймворк для управління IT-ресурсами, розроблений ISACA, який надає організаціям засоби для узгодження IT-стратегії з бізнес-цілями, оптимізації ресурсів та зниження ризиків [15]. Він сприяє прозорості, ефективності й контролю у сфері інформаційних технологій, пропонуючи практичні інструменти та рекомендації, що дозволяють досягати стратегічних цілей і відповідати вимогам регуляторів.

Основою COBIT є п’ять ключових принципів, які допомагають організаціям будувати ефективні процеси управління (рис. 1.5). Вони охоплюють потреби зацікавлених сторін, підтримують узгодженість управління IT з

бізнесом, забезпечують інтеграцію різних IT-фреймворків та чітко відрізняють управлінські функції від функцій менеджменту.

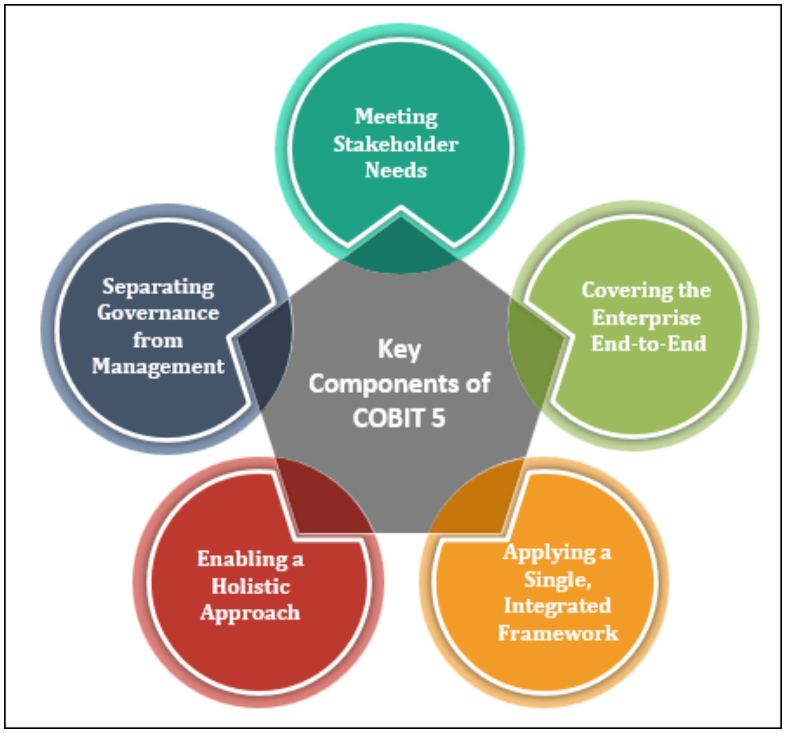


Рисунок 1.5 - П’ять компонентів COBIT

Фреймворк включає набір процесів, організованих у п’ять доменів, що відображають різні аспекти IT — від стратегічного планування до впровадження, підтримки й моніторингу. COBIT також пропонує модель зрілості для оцінки ефективності управління IT-процесами, що дозволяє організаціям оцінити свої практики, визначити сильні сторони та виявити області для поліпшення.

COBIT має важливе значення для організацій, оскільки допомагає зменшити IT-ризики, підвищити ефективність використання технологій і відповідати регуляторним стандартам. COBIT не є жорстким набором правил — це гнучка структура, що дозволяє інтегрувати управління IT у стратегічний розвиток бізнесу й успішно досягати поставлених бізнес-цілей.

1.2.6 КСЗІ (Комплексна система захисту інформації)

Комплексна система захисту інформації (КСЗІ) — це комплекс заходів, що включає правові, організаційні та технічні рішення, націлені на забезпечення захисту інформаційних систем від кібератак і несанкціонованого доступу [16]. В

Україні створення та функціонування КСЗІ є обов’язковим для всіх організацій, які обробляють державну інформацію або інформацію, критично важливу для національної безпеки. Державне законодавство, зокрема Закон "Про захист інформації в інформаційно-телекомунікаційних системах", визначає, що будь-яка інформаційна система, яка працює з конфіденційними даними, повинна пройти сертифікацію, яка підтверджує відповідність вимогам КСЗІ [17].

Сертифікація передбачає процедури, спрямовані на захист інформації: ідентифікація та автентифікація користувачів, керування доступом на основі ролей і прав, захист периметра інформаційної системи, шифрування даних, а також моніторинг і аудит усіх дій у системі. Ці заходи дозволяють мінімізувати ризик несанкціонованого доступу та втрату конфіденційності даних. Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ) контролює процес сертифікації, розробляє вимоги, перевіряє їхнє дотримання й видає сертифікати відповідності, що підтверджують захищеність інформаційних систем.

КСЗІ тісно пов’язана з національними стандартами кібербезпеки, спрямованими на побудову дієвої системи захисту даних. Вона ґрунтується на принципах міжнародних стандартів інформаційної безпеки, як-от ISO/IEC 27001, але адаптована до національних умов, що робить її ефективною у захисті державної інформації та сумісною з міжнародними системами безпеки [18]. Це особливо важливо в умовах глобалізації, де співпраця з іншими державами в питаннях кібербезпеки набуває критичного значення.

Однією з важливих складових КСЗІ є регулярний аудит інформаційної безпеки, що дозволяє аналізувати ефективність захисних заходів, виявляти нові загрози та своєчасно коригувати існуючі підходи. Такий підхід забезпечує актуальність системи і дозволяє підтримувати високий рівень захисту, адаптуючи його до змін у кіберпросторі. За рахунок регулярних перевірок, КСЗІ підвищує надійність інформаційних систем, що особливо важливо для державних установ і критично важливих підприємств, на які часто спрямовані кіберзагрози.

КСЗІ виконує ключову роль у забезпеченні національної безпеки України, гарантує цілісність, доступність та конфіденційність інформаційних ресурсів та знижує ймовірність успішних кібератак. Завдяки КСЗІ організації в Україні мають змогу більш ефективно захищати свої дані та пристосовуватися до нових викликів кібербезпеки, забезпечуючи стабільність і довіру до своїх інформаційних систем.

1.3 Постановка завдання

Для аудиту інформаційної безпеки міської ради, слід орієнтуватись на стандарти ISO 27001, NIST та КСЗІ оскільки ці стандарти найбільше відповідають специфічним потребам органів місцевого самоврядування, зокрема в аспектах державної безпеки, управління ризиками та забезпечення цілісності інформаційних систем. Застосування цих трьох стандартів дозволяє зосередитись на ключових аспектах управління інформаційною безпекою, що є необхідними для міської ради, без перевантаження додатковими вимогами.

ISO 27001 є міжнародно визнаним стандартом для побудови, впровадження, моніторингу та покращення системи управління інформаційною безпекою (ISMS). Він зосереджується на управлінні ризиками, що є критично важливим для організацій, які працюють з конфіденційною або чутливою інформацією, такою як дані громадян або адміністративні документи. ISO 27001 надає чітку структуру для визначення політик, процедур і технологій, які забезпечують безпеку інформаційних систем та дозволяє організувати ефективне управління ризиками. Це відповідає вимогам, які можуть бути актуальні для міської ради, де зберігаються різні види чутливої інформації, наприклад, дані про громадян, фінанси та інші важливі дані.

NIST, зокрема NIST Cybersecurity Framework (CSF), пропонує більш конкретний підхід до забезпечення кібербезпеки, охоплюючи ключові функції: ідентифікацію, захист, виявлення, реагування та відновлення. Для міської ради важливо мати систему, яка не лише забезпечує базовий захист, а й включає

ефективне реагування на кіберінциденти. Стандарт NIST також активно використовує концепцію управління ризиками і надає інструменти для оцінки та управління ризиками в умовах змінних кіберзагроз. Його можна безперешкодно застосовувати для різних рівнів організації, зокрема для місцевих органів влади, де швидкість реагування на загрози є критично важливою.

Комплексна система захисту інформації (КСЗІ) є нормативно-правовим актом, розробленим для забезпечення безпеки інформаційних систем в Україні. Для державних органів місцевого самоврядування важливо дотримуватися національних стандартів, які враховують специфіку законодавства, критичної інфраструктури та інших аспектів, що мають безпосереднє значення для національної безпеки. КСЗІ регулює безпеку інформаційних систем, що містять державну та критично важливу інформацію, а її впровадження дозволяє забезпечити відповідність вимогам, установленим на рівні держави.

Що стосується інших стандартів, таких як PCI DSS, GDPR та COBIT у контексті міської ради є обмеженою. PCI DSS орієнтований на безпеку платіжних карт і є критичним для підприємств, які займаються обробкою фінансових транзакцій, але не є пріоритетним для органів місцевого самоврядування, які в основному працюють з адміністративними даними та не обробляють великі обсяги платіжної інформації. GDPR, хоч і є важливим стандартом для захисту персональних даних, має специфіку для великих корпорацій і комерційних організацій, тому на місцевому рівні його застосування часто є надмірним, оскільки дані обробляються переважно в межах внутрішніх адміністративних процесів, а не в контексті комерційних відносин. COBIT зосереджується на управлінні IT-ресурсами та процесами на стратегічному рівні, але для органів місцевого самоврядування його застосування не є настільки критичним.

Таким чином, вибір ISO 27001, NIST і КСЗІ є обґрунтованим для органів місцевого самоврядування, оскільки ці стандарти забезпечують гнучке та комплексне управління інформаційною безпекою, відповідають як

національним, так і міжнародним вимогам, та дозволяють зосередитись на найбільш актуальних аспектах безпеки інформації в публічному секторі.

Висновки до розділу

У даному розділі було здійснено постановку задачі для проведення аудиту інформаційної безпеки міської ради, а також проведено огляд найбільш поширених міжнародних та національних стандартів, таких як ISO 27000, NIST, PCI DSS, GDPR, COBIT і КСЗІ. Кожен з цих стандартів має свої особливості та застосування в різних сферах інформаційної безпеки, однак для органів місцевого самоврядування, зокрема для міської ради, було визначено найбільш підходящі три підходи — ISO 27000, NIST і КСЗІ.

ISO 27000 був обраний завдяки своїй гнучкості та міжнародній визначності як стандарт, що забезпечує систематичний підхід до управління інформаційною безпекою через побудову та впровадження системи управління інформаційною безпекою (ISMS).

NIST був обраний через свою орієнтацію на практичні методи забезпечення кібербезпеки, зокрема через свою модель, яка включає ідентифікацію, захист, виявлення, реагування та відновлення. Цей стандарт дозволяє розробити конкретні стратегії і механізми для протидії кіберзагрозам, що є важливим для міської ради з огляду на постійну загрозу кібернападів та необхідність ефективного реагування на інциденти.

КСЗІ містить вимоги щодо захисту державної інформації та критичної інфраструктури, що особливо важливо для органів місцевого самоврядування, які мають справу з важливими даними громадян, бюджетними коштами та іншою адміністративною інформацією.

Таким чином, вибір ISO 27001, NIST і КСЗІ для аудиту інформаційної безпеки міської ради є обґрунтованим і спрямований на створення ефективної, комплексної і адаптивної системи захисту інформаційних активів органу місцевого самоврядування.

2 АНАЛІЗ ОБ'ЄКТУ АУДИТУ

Перед уточненням методики аудиту Вінницької міської ради слід приблизно охарактеризувати будову та ресурси якими користуються співробітники різних департаментів.

2.1 Структура Вінницької міської ради

Структура Вінницької міської ради включає кілька основних компонентів, зокрема органи міського самоврядування та виконавчі органи, що відповідають за реалізацію рішень ради [19]. ВМР складається з депутатів, що обираються громадянами, та виконавчого комітету, що включає міського голову і його заступників. Важливими елементами є також постійні комісії ради, які займаються попереднім розглядом питань, що виноситься на сесію.

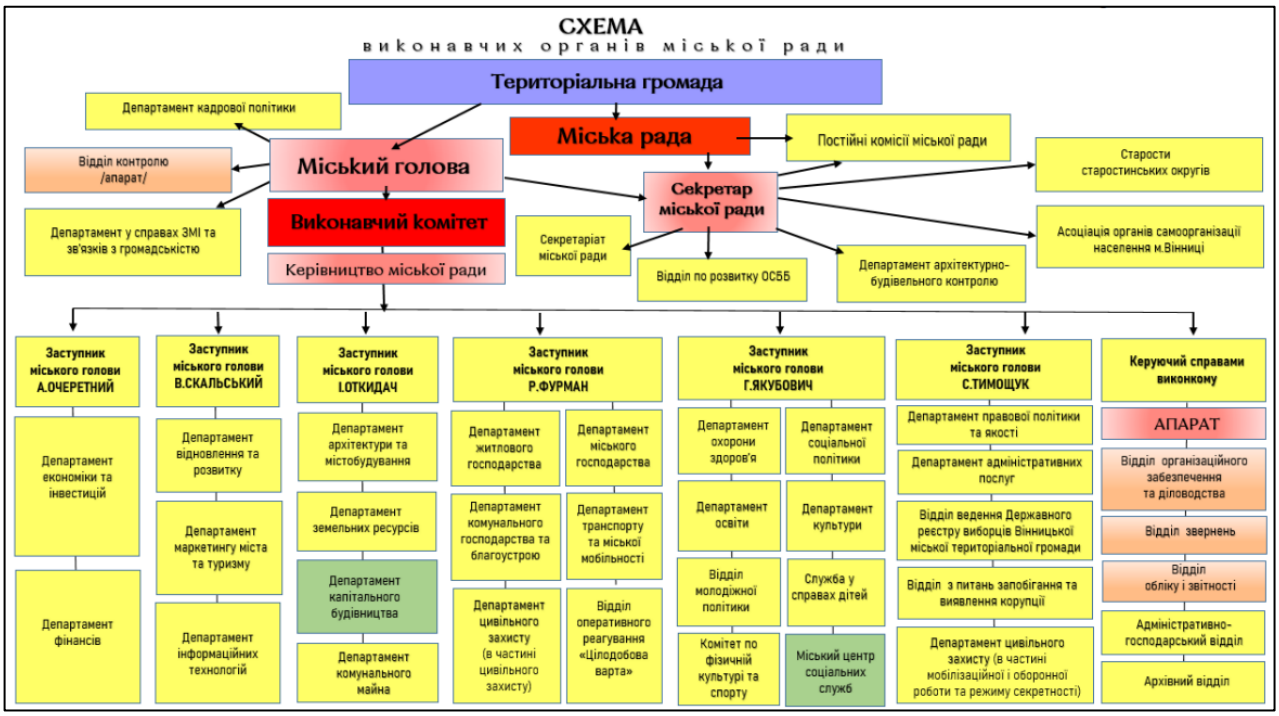


Рисунок 2.1 - Схема виконавчих органів Вінницької міської ради

Основні виконавчі органи ради організовані через департаменти, які відповідають за різні сфери, зокрема економіку, освіту, охорону здоров'я, соціальну політику, комунальне господарство, містобудування та архітектуру.

До них належать, зокрема, департамент житлового господарства, департамент освіти, департамент економіки, а також різні інші служби, що забезпечують діяльність громади на місцевому рівні.

Крім того, є структурні підрозділи для організаційного забезпечення діяльності ради, зокрема спеціалісти, що займаються обробкою документації та координацією роботи відділів.

Точна кількість співробітників Вінницької міської ради не наводиться в публічних джерелах, але можна отримати загальне уявлення про організаційну структуру та кількість персоналу на основі чисельності департаментів і підрозділів. За різними оцінками, міська рада має десятки відділів і департаментів, кожен з яких може включати від кількох до кількох десятків співробітників. Чим більша кількість співробітників тим важче проводити той чи інший вид аудиту.

2.2 Інформаційний аудит

Оскільки аудит інформаційної безпеки є багатоетапним процесом на момент проходження практики департамент Інформаційних технологій вже провів певні дії, зокрема інформаційний аудит певних департаментів та відділів. Його ціллю було дізнатись які сервіси використовують підрозділи Вінницької міської ради. Одним з результатів практики була систематизація та візуалізація даних інформаційного аудиту.

2.2.1 Департамент правової політики та якості міської ради

Основні функції департаменту правової політики та якості Вінницької міської ради охоплюють кілька ключових напрямків [20]. По-перше, департамент відповідає за реалізацію державної правової політики, організовуючи правову роботу міської ради та виконавчих органів для забезпечення належного застосування та дотримання законодавства і нормативних актів. Він також зосереджений на захисті інтересів територіальної

громади та органів влади в судах і інших правових інстанціях, а також на взаємодії з правоохоронними органами України.

Ще однією важливою функцією є впровадження та постійне вдосконалення системи управління якістю і протидії корупційним загрозам. Це включає відповідність європейським стандартам, таким як EN ISO 9001:2008, а також вимогам національного законодавства. Крім того, департамент здійснює аналітичне та інформаційно-довідкове забезпечення для міської ради, міського голови та виконавчих органів, сприяючи ефективності їх роботи в правовій сфері.

За для виконання поставлених завдань департамент використовує різноманітні сервіси та платформи на яких вони містяться (рис. 2.2)

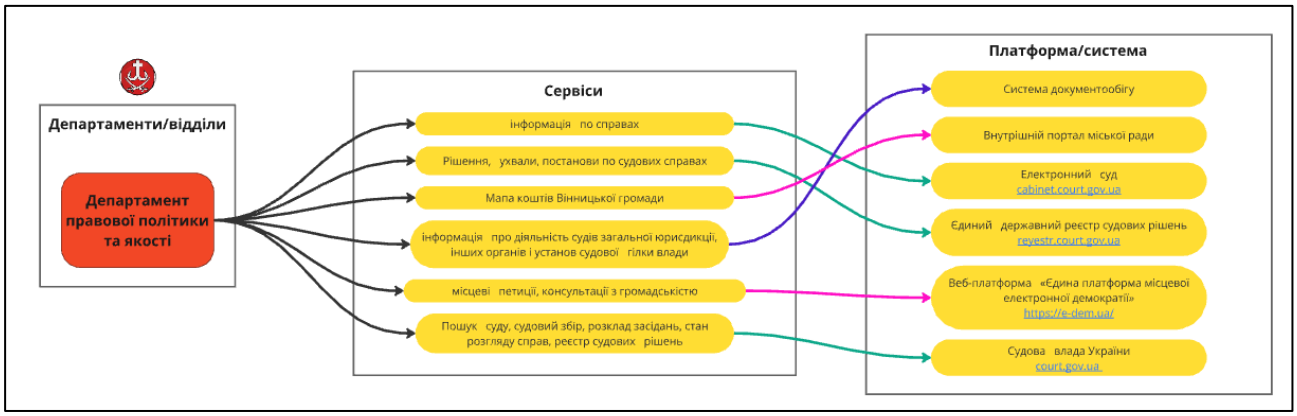


Рисунок 2.2 – Результат інформаційного аудиту департамент правової політики та якості міської ради

Департамент правової політики та якості міської ради, виконує розподіл інформації і надає послуги в юридичній сфері. Цей департамент взаємодіє з рядом сервісів, які зосереджені на підтримці доступу громадськості до судових рішень, фінансової інформації громади, даних про роботу судів, юридичних установ, а також забезпечує можливості для громадської участі через петиції та консультації. До таких сервісів належать інформація по справах, доступ до рішень та постанов суду, інформація про діяльність судів та інших органів судової влади, публічні консультації та петиції, а також пошукові інструменти

для перегляду судового збору, розкладу засідань, статусу розгляду справ та реєстру судових рішень.

Сервіси, які надає департамент, пов’язані з певними платформами та системами. Серед них система документообігу, яка забезпечує обробку документів, пов’язаних зі справами, та внутрішній портал міської ради, що використовується для комунікації та обміну інформацією всередині ради. Електронний суд надає можливість обробки справ онлайн, а Єдиний державний реєстр судових рішень забезпечує публічний доступ до судових рішень, сприяючи прозорості судової системи. Платформа «Єдина платформа місцевої електронної демократії» призначена для взаємодії з громадськістю, надаючи можливість подавати петиції та брати участь у консультаціях. Офіційний сайт «Судова влада України» забезпечує загальний доступ до інформації про судову систему України, включаючи дані про суди та справи.

Отже, департамент правової політики та якості виконує функцію посередника, що розподіляє юридичну та суспільно важливу інформацію через цифрові сервіси, спрямовані на підвищення прозорості, залучення громадськості та спрощення доступу до судових даних. Така структура відображає прагнення до електронного врядування і публічної підзвітності, що відповідає сучасним вимогам до відкритості влади та доступності інформації.

2.2.2 Департамент культури

Департамент культури міської ради відповідає за реалізацію державної політики та повноважень місцевого самоврядування в галузі культури та захисту суспільної моралі [21]. Він сприяє формуванню конкурентоспроможного мистецького середовища через створення власного мистецького продукту, визначає перспективи розвитку та зміст спеціальної освіти у сфері культури, а також співпрацює з міжнародними проектами та творчими організаціями. Департамент вживає заходів для підтримки культури української нації, збереження культурної самобутності корінних народів та національних меншин, розвитку всіх видів мистецтва, народної творчості, художніх промислів та ремесел. Він також здійснює повноваження у сфері збереження і використання

культурної спадщини. Окрім цього, департамент готує проєкти розпоряджень міської ради, її виконавчих органів та міського голови, включаючи нормативні акти. Департамент розглядає звернення громадян і проводить прийом громадян з питань, що належать до його компетенції, згідно з установленим графіком. Він також виконує інші завдання, передбачені чинним законодавством.

Департамент обробляє офіційні документи, такі як листи, звернення, рішення і протоколи, що забезпечують офіційне листування та обмін інформацією з іншими установами. Окрім цього, він використовує інформацію, яка потрібна для виконання посадових обов'язків працівників, а також дані, що стосуються конкретних завдань, які стоять перед департаментом (рис. 2.3).

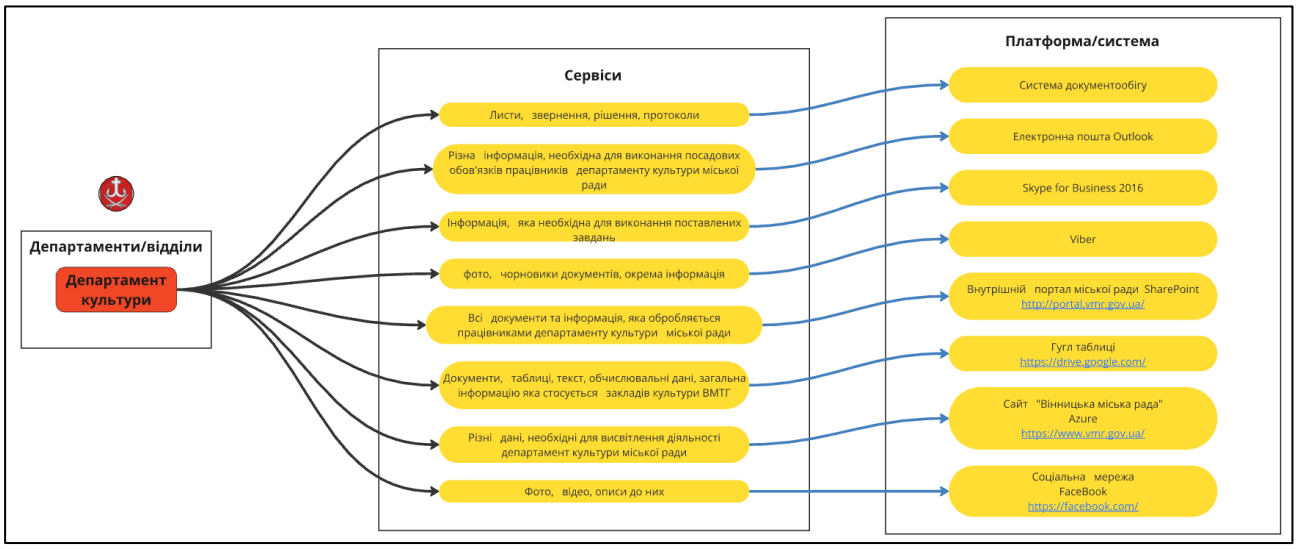


Рисунок 2.3 – Результат інформаційного аудиту департаменту культури

Для зберігання та обробки чернеток, фотографій та іншої інформації, необхідної для звітів або презентацій, також створені відповідні сервіси. Усі документи та інформація обробляються працівниками департаменту, зберігаються і використовуються для поточних або майбутніх потреб. Крім того, департамент створює та обробляє таблиці, загальні дані, що стосуються діяльності закладів культури, та інші дані, які необхідні для висвітлення діяльності департаменту в публічному просторі. Для цього готуються фото, відео та текстові описи, які публікуються у новинних ресурсах і соціальних мережах.

Для виконання цих завдань департамент культури використовує низку платформ. Основна платформа документообігу забезпечує зручний обмін і зберігання офіційної документації. Електронна пошта Outlook служить для офіційного листування, пересилання важливих документів та інформації. Для відеоконференцій і нарад департамент використовує Skype for Business 2016, а для швидкого обміну короткими повідомленнями та фотографіями – Viber. Внутрішній портал міської ради на базі SharePoint дозволяє працівникам обмінюватися документами в рамках організації. Для створення та обробки таблиць використовуються Google Таблиці, а сайт «Вінницька міська рада» на платформі Azure забезпечує публікацію новин, оголошень і важливих документів для громадськості. Окрім цього, соціальна мережа Facebook дозволяє департаменту інформувати громадськість про новини, події та заходи, які проводяться департаментом.

Ця структура платформ і сервісів сприяє ефективній організації роботи департаменту культури, підтримує внутрішній документообіг, забезпечує зручну комунікацію між працівниками, зберігання даних, а також дозволяє департаменту активно інформувати громадськість про свою діяльність через соціальні мережі та офіційні ресурси. Це сприяє реалізації завдань департаменту і забезпечує прозорість у його роботі.

2.2.3 Департамент охорони здоров’я

Департамент охорони здоров'я виконує широкий спектр функцій, спрямованих на розвиток і вдосконалення медичного обслуговування, а також на підтримку належного рівня якості медичної допомоги [22]. Згідно з Законом України "Про місцеве самоврядування в Україні", департамент працює над розвитком усіх видів медичних послуг, покращенням мережі лікувальних закладів різних форм власності, а також бере участь у визначенні потреби у кваліфікованих кадрах, сприяючи підвищенню їхньої кваліфікації. Він також активно підтримує право громадян на участь в управлінні охороною здоров'я, організовуючи діяльність громадських експертних, консультативних та

наглядових рад і залучаючи до співпраці громадські організації працівників медичної сфери.

Департамент здійснює контроль за якістю та обсягом медичної допомоги, що надається комунальними медичними підприємствами, використовуючи для цього галузеві медичні стандарти. Він готує пропозиції для впровадження реформ у галузі охорони здоров'я відповідно до чинних законодавчих актів і подає ці пропозиції на розгляд міській раді, її виконавчому комітету, міському голові, а також департаменту охорони здоров'я обласної державної адміністрації.

Крім цього, департамент забезпечує контроль за наданням пільговим категоріям населення необхідних лікарських засобів і медичних виробів, згідно з вимогами законодавства. Він аналізує стан охорони здоров'я в громаді, визначає тенденції та перспективи розвитку галузі. На основі науково обґрунтованих галузевих стандартів, департамент готує програми і прогнози, які сприяють охороні здоров'я населення, покращенню якості медичної допомоги та зміцненню матеріально-технічної бази галузі.

Як головний розпорядник коштів, департамент відповідає за ефективне використання фінансових, матеріальних та трудових ресурсів відповідно до бюджетного законодавства. Він також забезпечує медико-санітарне обслуговування під час ліквідації наслідків надзвичайних ситуацій, організовуючи заходи для захисту здоров'я населення в кризових умовах.

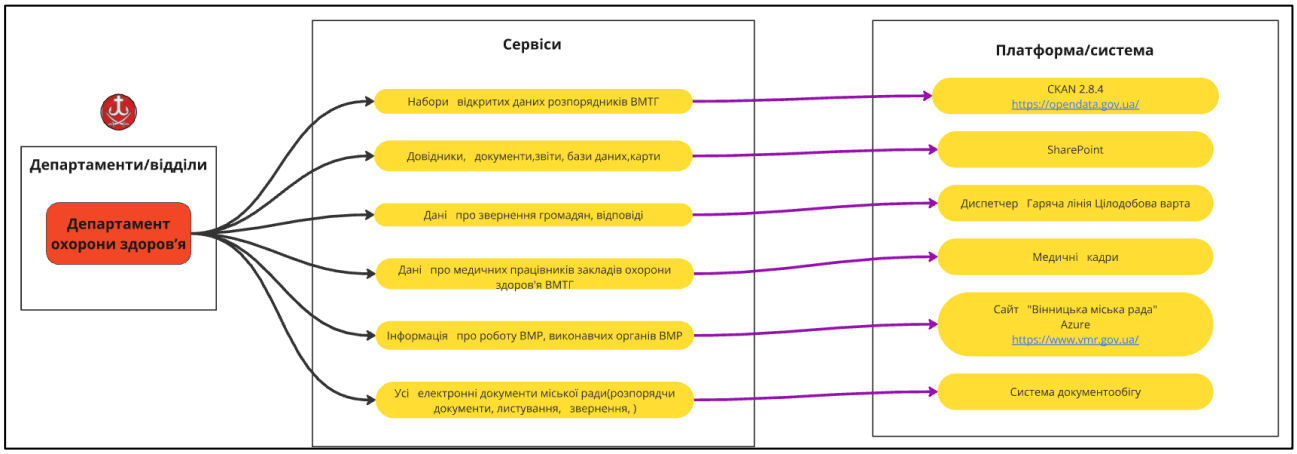


Рисунок 2.4 – Результат інформаційного аудиту департамент охорони здоров’я

Департамент охорони здоров'я використовує кілька сервісів та платформ для виконання своїх обов'язків. Зокрема, департамент має доступ до наборів відкритих даних, які керуються на платформі СКАН версії 2.8.4, що знаходиться за адресою opendata.gov.ua. Це дозволяє департаменту ефективно працювати з великим масивом відкритих даних, що може включати різні категорії інформації від урядових організацій.

Для зберігання, управління та обміну довідниками, документами, звітами, базами даних та картами департамент використовує платформу SharePoint. Це забезпечує зручний спосіб організації інформації та сприяє кращій координації в межах організації.

Дані щодо звернень громадян і відповідей на них надходять через диспетчерську службу Цілодобова варта. Цей сервіс допомагає оперативно реагувати на запити громадян і підтримувати зв’язок із суспільством.

Інформацію про медичних працівників закладів охорони здоров'я департамент отримує через платформу Медичні кадри. Це забезпечує доступ до інформації про кваліфікації та зайнятість медичних працівників, що є важливим для управління кадрами у сфері охорони здоров'я.

Також департамент використовує сайт ВМР на платформі Azure, де розміщена інформація про роботу органів виконавчої влади, їхню діяльність і досягнення. Цей ресурс надає широкий доступ до публічної інформації, яка може бути корисною для громадян і організацій.

Для роботи з усіма електронними документами міської ради, включно з розпорядженнями, листуванням та зверненнями, департамент використовує систему документообігу.

2.2.4 Архівний відділ

Відділ займається забезпеченням виконання вимог законодавства України щодо Національного архівного фонду та архівних установ [23]. Він відповідає за поповнення Національного архівного фонду документами місцевого значення, їх державну реєстрацію, облік, зберігання та використання інформації з цих документів. Також відділ забезпечує належне зберігання документів

Національного архівного фонду та документів з особового складу ліквідованих підприємств, установ і організацій на території міста, відповідно до вимог Держархівслужби України.

Крім того, відділ готує проекти розпорядчих актів для міської ради, її виконавчих органів і міського голови, включаючи нормативні акти, а також займається розглядом звернень та прийомом громадян. Він виконує інші повноваження, покладені на нього відповідно до чинного законодавства.

Важливим напрямком роботи відділу є забезпечення дотримання конституційних прав і свобод людини, захист конфіденційної інформації, а також виконання антикорупційних вимог.

Основні завдання відділу включають надання якісних послуг громадянам та організаціям міської ради в короткі терміни, за мінімальних процедур. Відділ також відповідає за облік, зберігання та охорону документів, що зібрались у результаті діяльності органів місцевого самоврядування, підприємств, установ, а також громадських організацій. Він приймає на зберігання архівні документи з особового складу та інші документи, що належать до Національного архівного фонду. Відділ здійснює контроль за веденням діловодства на підприємствах і в установах, надає методичну допомогу та видає архівні довідки, копії та витяги з документів, що зберігаються у відділі (рис.2.5).

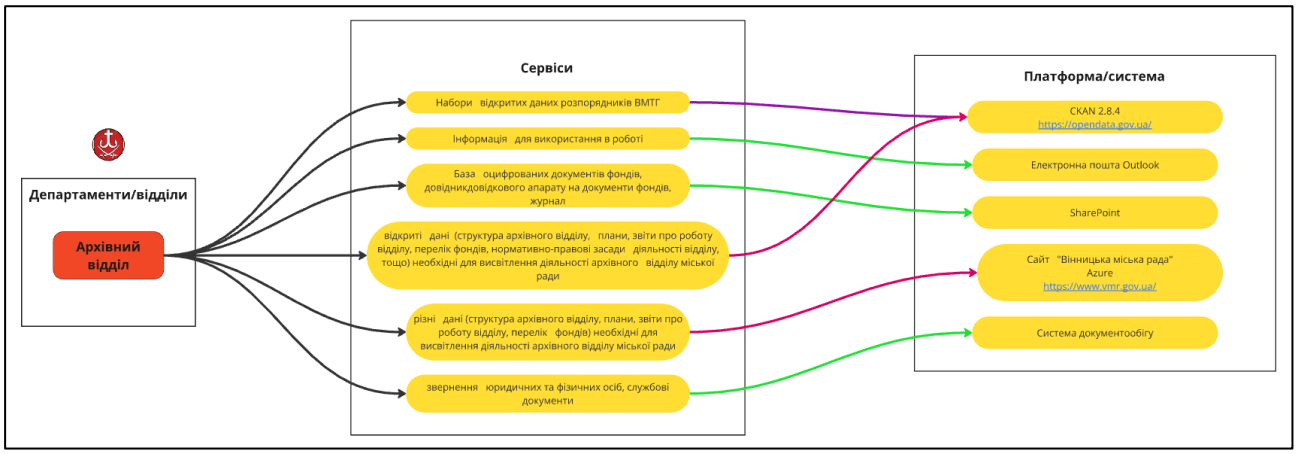


Рисунок 2.5 – Результат інформаційного аудиту архівного відділу

Архівний відділ використовує різноманітні сервіси та платформи для виконання своїх завдань, що забезпечують ефективну роботу з документами та

інформацією. Один із важливих сервісів – це набори відкритих даних розпорядників ВМТГ, які розміщуються на платформі CKAN версії 2.8.4, що доступна за посиланням opendata.gov.ua. Цей сервіс дозволяє зберігати та поширювати відкриті дані, які потрібні для звітності та взаємодії з громадськістю.

Для обміну інформацією, яка використовується в роботі відділу, застосовується електронна пошта Outlook. Вона забезпечує зручний спосіб комунікації між працівниками, обмін документами та зворотній зв’язок.

Важливу роль відіграє також база оцифрованих документів фондів, яка зберігається та керується через SharePoint. Тут архівний відділ може зберігати, організовувати та знаходити документи, журнали, та інші важливі архівні записи, що суттєво покращує доступ до інформації.

Для висвітлення структури відділу, планів, звітів про роботу, переліку фондів та нормативно-правових засад діяльності архівного відділу використовуються дані, що публікуються на сайті "Вінницька міська рада", який працює на платформі Azure і доступний за адресою vmr.gov.ua. Це дозволяє забезпечити доступ громадян до інформації про діяльність архівного відділу та відповідає вимогам прозорості.

Крім того, для зберігання та управління службовими документами, а також для звернень юридичних та фізичних осіб архівний відділ користується системою документообігу. Ця система оптимізує процеси документообігу та забезпечує швидкий доступ до необхідної інформації, що підвищує ефективність роботи відділу.

2.2.5 Департамент освіти

Департамент освіти виконує низку функцій, спрямованих на реалізацію державних та регіональних освітніх програм на території Вінницької міської територіальної громади [24]. Він проводить аналіз стану освіти в громаді, розробляє програми розвитку та забезпечує їх реалізацію. Департамент також відповідає за планування і координацію взаємодії між різними сферами при

реалізації Плану дій в рамках ініціативи «Громада, дружня до дітей та молоді», що включає врахування потреб дітей та молоді при формуванні міської політики.

У межах своїх повноважень департамент забезпечує виконання Конституції України, зокрема щодо функціонування української мови як державної в освітніх закладах та установах. Крім того, департамент здійснює управління діяльністю закладів освіти громади, керуючись чинним законодавством і рішеннями міської ради.

На рисунку 2.6 наведено результат проведення інформаційного аудиту у департаменті освіти.

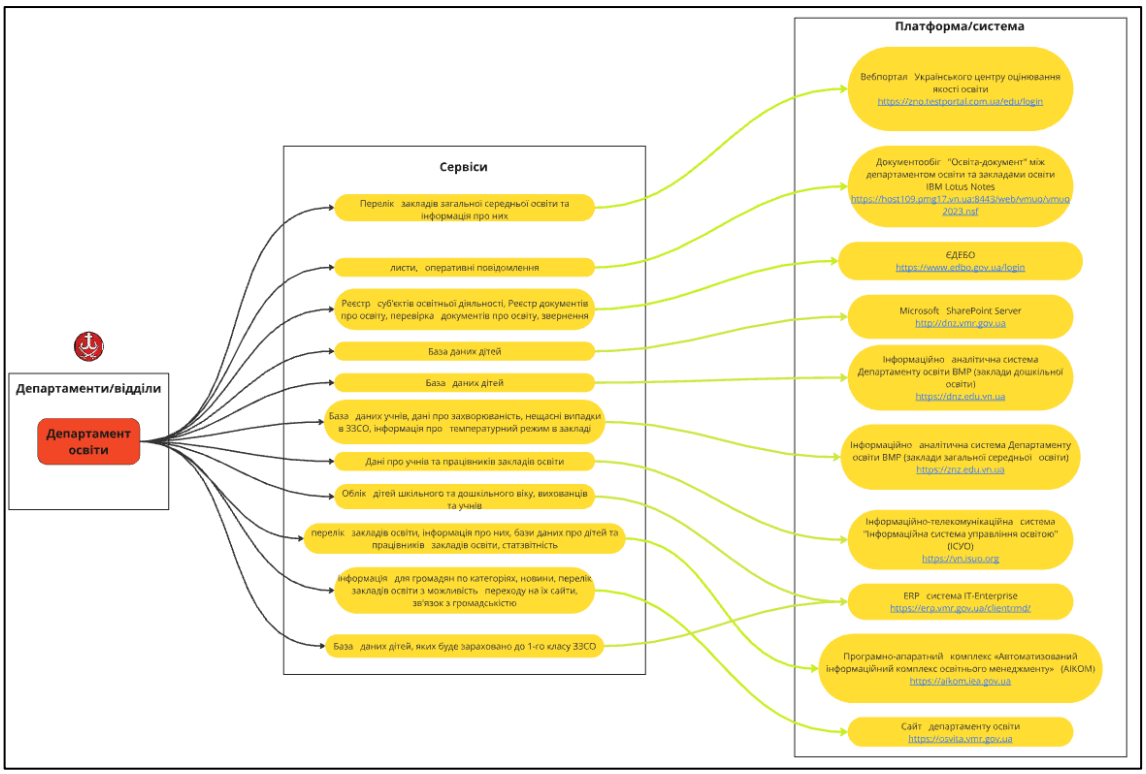


Рисунок 2.6 – Результат інформаційного аудиту департаменту освіти

Департамент освіти використовує різноманітні сервіси та платформи для організації роботи та управління інформацією, що дозволяє забезпечити ефективну діяльність у сфері освіти. Зокрема, для надання інформації про заклади загальної середньої освіти департамент застосовує вебпортал Українського центру оцінювання якості освіти, доступний за посиланням testportal.com.ua. Це допомагає інформувати громадськість про різні аспекти освітніх закладів.

Для управління документацією та оперативного обміну листами департамент використовує систему документообігу "Освіта-документ" на платформі IBM Lotus Notes, що функціонує для взаємодії між департаментом та освітніми закладами. Це забезпечує зручний процес обміну офіційними документами.

Реєстрація суб'єктів освітньої діяльності та перевірка освітніх документів здійснюється через платформу ЄДЕБО, що знаходиться на edbo.gov.ua. Це дозволяє забезпечити належний контроль та облік документів про освіту.

Для зберігання та організації даних про дітей департамент використовує Microsoft SharePoint Server за адресою vmr.gov.ua. Тут зберігаються бази даних дітей та інша важлива інформація.

Інформаційно-аналітичні системи департаменту забезпечують аналіз та управління даними як закладів дошкільної, так і загальної середньої освіти. Вони працюють на dnz.edu.vn.ua та zzo.edu.vn.ua відповідно. Це дозволяє департаменту отримувати необхідну аналітичну інформацію для управління освітніми процесами.

Інформаційно-телекомунікаційна система "Інформаційна система управління освітою" (ІСУО), доступна на isuo.org, забезпечує централізоване управління освітніми даними, що включає звітність і статистичні показники.

Для ефективного управління ресурсами департамент використовує ERP систему IT-Enterprise, що доступна на erp.vmr.gov.ua. Ця система допомагає в автоматизації адміністративних процесів та управлінні ресурсами.

Крім того, департамент застосовує програмно-апаратний комплекс "Автоматизований інформаційний комплекс освітнього менеджменту" (AIKOM) для управління освітніми процесами. Платформа AIKOM знаходиться за адресою aikom.ioc.gov.ua і допомагає оптимізувати управління освітніми закладами.

Офіційний сайт департаменту освіти, osvita.vmr.gov.ua, слугує для поширення інформації серед громадськості, включаючи новини, перелік закладів освіти та можливості зв’язку з департаментом.

2.2.6 Комітет по фізичній культурі та спорту

Комітет реалізує державну політику у сфері фізичної культури і спорту на місцевому рівні, підтримує розвиток спорту та фізичної культури, зокрема олімпійського та паралімпійського руху [25]. Він забезпечує, щоб спортивні та фізкультурні організації міста дотримувалися стандартів спортивної класифікації і нормативів. Комітет формує календарні плани спортивних і фізкультурних заходів, організовує та проводить спортивні події для всіх верств населення, включно з дітьми та молоддю, а також розробляє цільові програми для розвитку спорту і фізичної культури, подаючи їх на затвердження міському виконавчому комітету.

Крім того, комітет готує пропозиції для міської ради щодо фінансування і матеріально-технічного забезпечення програм у сфері спорту, працює над забезпеченням якості та доступності фізкультурно-спортивних послуг для громадян, а також здійснює міжнародну діяльність у цій сфері. Комітет сприяє залученню додаткових фінансових ресурсів, зокрема через підприємства, гранти міжнародних організацій і фондів. Він проводить інформаційно-роз'яснювальну роботу серед населення про важливість здорового способу життя та фізичної культури, підтримує публікацію актуальної інформації на порталі та сайті міської ради, а також вивчає ставлення мешканців міста до здорового способу життя.

На рисунку 2.7 наведено результат проведення інформаційного комітету по фізичній культурі та спорту.

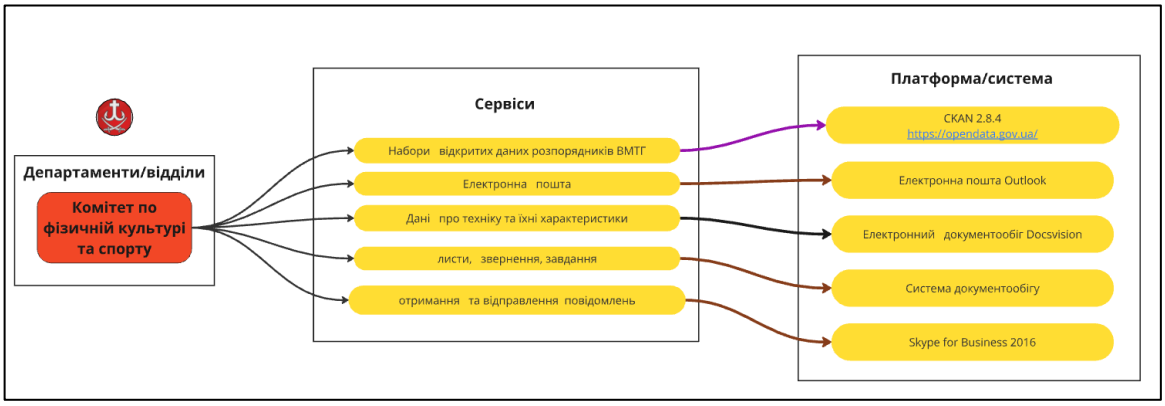


Рисунок 2.7 – Результат інформаційного аудиту департаменту фізичної культури та сорту

Комітет по фізичній культурі та спорту використовує кілька сервісів та платформ для виконання своїх завдань. Для роботи з відкритими даними розпорядників ВМТГ комітет користується платформою CKAN версії 2.8.4, що доступна на сайті opendata.gov.ua. Ця платформа дозволяє працювати з великими масивами даних, що є важливим для забезпечення прозорості та доступу громадськості до інформації.

Для обміну електронною поштою комітет використовує платформу Outlook, що забезпечує швидке та ефективне передавання повідомлень, зокрема для комунікації з іншими департаментами та зовнішніми організаціями.

Для управління даними про техніку та їхні характеристики застосовується система електронного документообігу Docsvision. Вона дозволяє зручно зберігати та керувати інформацією, що стосується інвентаризації та обліку обладнання, необхідного для спортивних заходів.

Для роботи з листами, зверненнями та завданнями комітет користується системою документообігу, яка забезпечує зберігання та організацію документації, що полегшує відстеження виконання завдань і обробку звернень громадян.

Також для швидкого обміну повідомленнями комітет використовує Skype for Business 2016, що дозволяє проводити онлайн-зустрічі та обговорення в режимі реального часу, забезпечуючи оперативний зв'язок між працівниками.

2.2.7 Департамент інформаційних технологій

Департамент інформаційних технологій забезпечує ефективну роботу виконавчих органів, комунальних підприємств та закладів міської ради, сприяючи покращенню якості життя мешканців Вінницької громади через впровадження сучасних цифрових технологій [26]. Основні функції департаменту включають визначення пріоритетних напрямків і завдань цифровізації на території громади, а також розробку, впровадження, організацію і контроль програм та проєктів цифрового розвитку.

Департамент відповідає за розвиток інформаційних технологій і технічного захисту інформації у підрозділах міської ради, бюджетних установах

і комунальних закладах громади. Він також забезпечує своєчасний ремонт, модернізацію і сервісне обслуговування обчислювальної та оргтехніки. Окрім того, департамент організовує роботу локальних мереж та інформаційних систем міської ради, забезпечуючи розподілений доступ до необхідних ресурсів.

Працівники даного департаменту мають найбільш тісний зв'язок з інформаційними техногіями, сервісами та платформами (рис. 2.8).

Департамент інформаційних технологій використовує широкий спектр сервісів та платформ для виконання своїх обов'язків, що охоплюють управління даними, комунікацію, документацію та підтримку безперебійної роботи систем. Основною платформою для управління відкритими даними є CKAN версії 2.8.4, яка дозволяє зберігати набори даних розпорядників ВМТГ та забезпечує доступ до них громадськості.

Для управління документацією департамент використовує систему документообігу BMP DocuVision та електронний документообіг Docsvision. Ці платформи дозволяють створювати, обробляти та зберігати документи, забезпечуючи оперативну роботу з файлами та звітами.

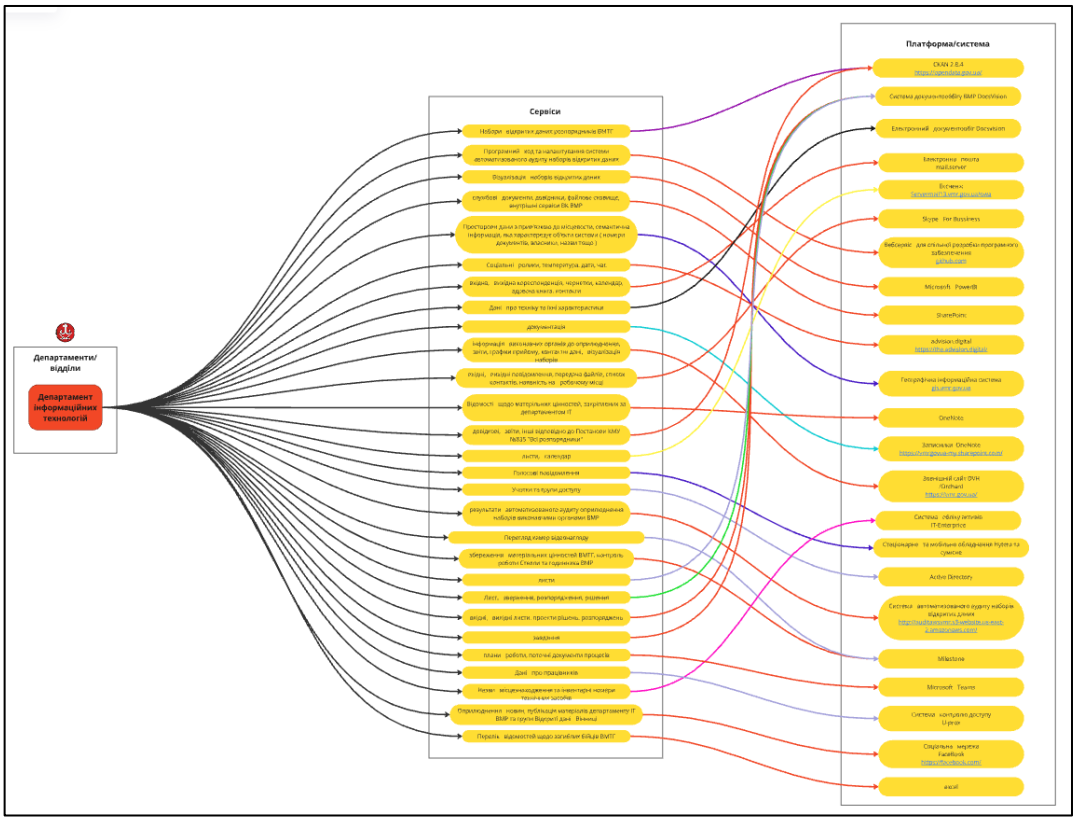


Рисунок 2.8 – Результат інформаційного аудиту департаменту інформаційних технологій

Для обміну електронною поштою використовується Outlook, а для швидкої комунікації між працівниками — Skype for Business, що забезпечує можливість проведення онлайн-зустрічей. Додатково департамент застосовує Webex для підтримки віддаленого доступу до різноманітного програмного забезпечення, що полегшує вирішення технічних завдань.

Microsoft Power BI є основним інструментом для створення аналітичних звітів, який дозволяє візуалізувати та аналізувати дані з різних джерел. Система SharePoint забезпечує спільне використання файлів і доступ до них для колег, що сприяє ефективному спільному виконанню проектів.

Для роботи з географічними даними застосовується геоінформаційна система, яка дозволяє відслідковувати розташування та особливості об'єктів у просторі. OneNote використовується для зберігання нотаток та оперативної інформації, що робить можливим швидкий доступ до потрібних записів.

Департамент також використовує записник OneNote для особистих та командних заміток, а інформаційний облік активів здійснюється за допомогою зовнішнього сайту DWH. Система обліку активів допомагає керувати матеріальними цінностями та контролювати їх використання.

Для забезпечення кібербезпеки та контролю доступу до мережевих ресурсів департамент застосовує Active Directory, що дозволяє обмежувати доступ до даних і ресурсів, а також контролювати користувачів та їхні права доступу.

Система автоматизованого аудиту автоматизує процес контролю наборів даних, що публікуються на зовнішніх ресурсах, забезпечуючи прозорість роботи департаменту. Важливу роль у моніторингу виконання завдань відіграє платформа Microsoft Teams, що забезпечує спільну роботу, планування та обмін інформацією.

Система відеоспостереження Milestone підтримує забезпечення безпеки, дозволяючи вести моніторинг активностей у приміщеннях та на території. Для комунікації з громадськістю та публікації важливих оголошень департамент використовує соціальні мережі, такі як Facebook.

Для аналітики та статистики використовується Excel, що дозволяє зручно обробляти числові дані та створювати графіки для звітності.

Висновки до розділу

У даному розділі було здійснено огляд структури Вінницької міської ради та завдань які покладені на різні департаменти. У кожному з них було проведено інформаційний аудит за яким можна зробити певні висновки.

Найбільш поширені платформи включають SharePoint, який використовується для управління документами та співпраці; систему документообігу для ведення офіційних документів; Azure, пов’язаний із сайтом міської ради для розповсюдження інформації для громадськості; Outlook, який застосовується для комунікацій; та CKAN (opendata.gov.ua) для роботи з відкритими даними, що особливо актуально для департаментів, які працюють з публічними даними.

Серед частих сервісів можна виділити використання наборів відкритих даних, що вказує на прагнення до прозорості та надання доступу громадськості до інформації; сервіси з управління документами для зберігання, пошуку та обміну документами; управління зверненнями громадян, зокрема в департаментах охорони здоров’я та освіти; і внутрішні засоби комунікації, як Skype for Business, Viber та Outlook, що підкреслює важливість зв’язку як всередині департаментів, так і назовні.

Загалом, основні платформи для роботи з документами та відкритими даними є важливими для різних департаментів, що свідчить про прагнення до прозорості, ефективної комунікації та раціонального обігу документів. Комунікаційні інструменти, як SharePoint і Outlook, мають значну цінність як для внутрішніх, так і для зовнішніх взаємодій.

3 РОЗРОБКА МЕТОДИКИ АУДИТУ

Згідно з результатом аналізу стандартів в першому розділі було обрано стандарти серії ISO 27000, NIST Cybersecurity Framework 2.0 та КСЗІ (конкретизувати). Даний розділ має на меті детально проаналізувати ці документи та вивести детальну методику аудиту підрозділів Вінницької міської ради.

3.1 Впровадження методики аудиту на основі стандартів ISO 27000

Як і було описано у першому розділі, на сьогоднішній день основними стандартами у аудиті інформаційної безпеки у всьому світі є стандарти серії ISO 27000. Проаналізувавши їх можна виділити послідовність дій при аудиті інформаційної безпеки міської ради які відображені у рисунку 4.1:

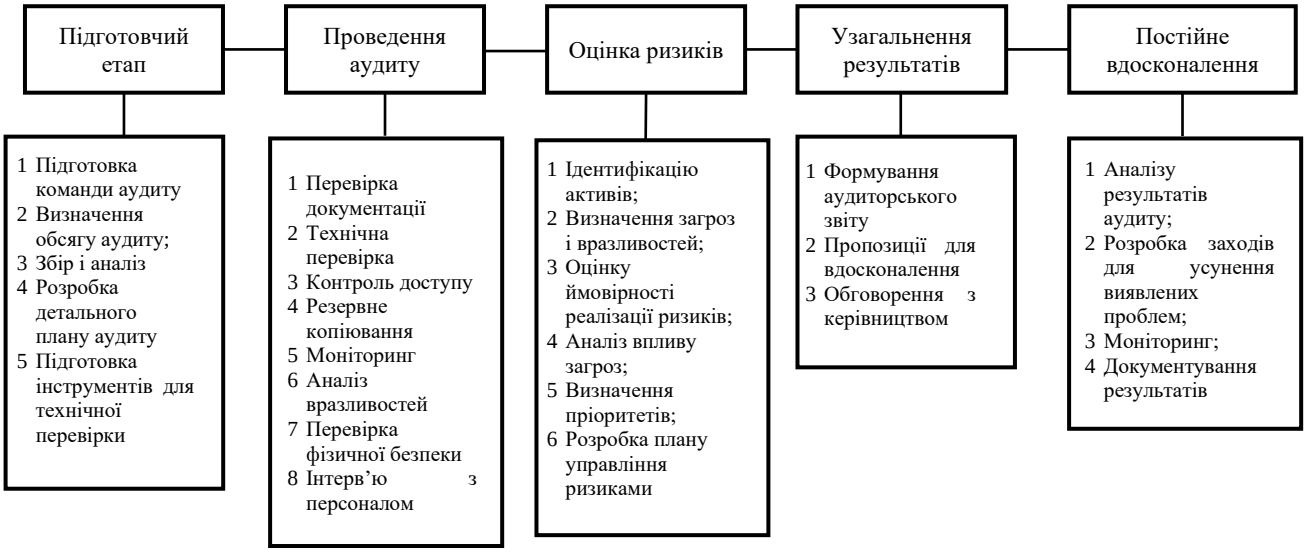


Рисунок 3.1 – Послідовність дій при аудиті інформаційної

3.1.1 Процедура підбору спеціалістів

На сьогоднішній день у процес аудиту активно проваджуються нові системи для автоматизації певних процесів та покращення якості аудиту, як більш тривіальні так і на основі штучного інтелекту. Тим не менше, в основі цих процесів завжди є людський персонал, серед етапів підготовки потрібно

виокремити етап з підбору персоналу. До всіх них слід висунути певні критерії по досвіду та знанням якими має володіти спеціаліст з аудиту інформаційної безпеки.

Підрозділ аудиту повинен мати критерії для перевірки базового досвіду, спеціального навчання або інструктажу членів аудиторської групи, які гарантують принаймні:

a) знання інформаційної безпеки;
b) технічні знання діяльності, що підлягають аудиту;
c) знання систем управління;
d) знання принципів аудиту;
e) знання моніторингу, вимірювання, аналізу та оцінки СУІБ.

Наведені вище вимоги мають застосовуватись до всіх аудиторів, які є частиною аудиторської групи, за винятком b), який можна поділити між аудиторами, які є частиною аудиторської групи.

Аудиторська група повинна мати відповідний досвід роботи з вищезазначених пунктів і практичного застосування цих пунктів. Тим не менше це не означає що аудитору потрібен повний спектр досвіду в усіх сферах інформаційної безпеки, але аудиторська група в цілому повинна мати достатньо оцінки і досвід для охоплення сфери СУІБ, що перевіряється.

Критерії відбору аудиторів гарантують, що кожен аудитор:

a) має професійну освіту або підготовку до еквівалентного рівня університетської освіти;
b) має принаймні чотири роки практичного досвіду роботи на з яких принаймні два роки на посаді або функції, пов’язаної з інформаційною безпекою;
c) успішно пройшов днів навчання, обсяг якого охоплює аудити СУІБ та управління аудитом;
d) набув досвіду в усьому процесі оцінки інформаційної безпеки до того, як взяти на себе відповідальність за виконання обов’язків аудитора. Цей досвід слід було отримати шляхом участі щонайменше в чотирьох

сертифікаційних аудитах СУІБ, включаючи повторну сертифікацію, загалом щонайменше 20 днів. Участь повинна включати перегляд документації та оцінку ризиків, оцінку впровадження та аудиторський звіт;

e) має відповідний і актуальний досвід;

f) підтримує поточні знання та навички з інформаційної безпеки та аудиту шляхом постійного професійного розвитку. Технічні експерти повинні відповідати критеріям a), b) і e).

В свою чергу голова комісії до вже переліченого має мати досвід активної участі у всіх етапах принаймні трьох аудитів СУІБ. Участь мала включати початкове визначення обсягу та планування, перегляд документації та оцінку ризиків, оцінку впровадження та офіційне звітування про аудит.

Підрозділ аудиту повинен переконатися, що володіє знаннями про технологічні, правові та нормативні розробки, що стосуються СУІБ, яку він оцінює. Для кращого розуміння даної області було проведено аналіз підприємства та інформаційний аудит у попередньому розділі.

Потрібно враховувати ризики, пов’язані з наданням компетентної, послідовної та неупередженого аудиту. Ризики можуть включати, але не обмежуватись ризиками, пов’язаними з:

— цілі аудиту;

— вибірка, що використовується в процесі аудиту;

— реальна та уявна неупередженість;

— правові, нормативні питання та питання відповідальності;

— клієнтську організацію, що перевіряється, та її робоче середовище;

— вплив аудиту на підрозділи та їх діяльність;

— здоров'я та безпека аудиторських груп;

— сприйняття зацікавлених сторін;

— оманливі заяви та дані підрозділів.

Важливо, щоб всі залучені усвідомлювали необхідність неупередженості.

3.1.2 Процес підготовки до аудиту

На етапі підготовки визначається мета аудиту, яка зазвичай включає перевірку ефективності Системи управління інформаційною безпекою (СУІБ) та її відповідність вимогам ISO 27001. Зокрема, уточнюються межі аудиту: які підрозділи, процеси чи активи будуть перевірятися. Наприклад, це можуть бути відділи інформаційних технологій, фінансовий департамент та залежно від мети та обсягу аудиту інші департаменти.

Збір попередньої інформації є важливим компонентом. Аудитори знайомляться з документами, такими як політика інформаційної безпеки, процедури управління ризиками, звіти про інциденти та план забезпечення безперервності діяльності. Цей аналіз дозволяє зрозуміти, як організація документує свою діяльність у сфері інформаційної безпеки та чи відповідає ця документація вимогам ISO 27001, зокрема розділам 5–10 стандарту.

На основі отриманих даних складається детальний план аудиту, що включає: графік перевірок, методи збору інформації (аналіз документів, інтерв'ю, технічні перевірки) та перелік питань, які будуть перевірятися.

3.1.3 Процес аудиту

Аудит розпочинається з аналізу документації. Аудитори оцінюють, чи відповідають політики, процедури та записи вимогам ISO 27001. Наприклад, розділ 6 стандарту встановлює вимоги до управління ризиками, включаючи аналіз та оцінку ризиків, а також плани з їхнього зниження. Аудитори перевіряють, чи ведеться реєстр ризиків, чи регулярно його оновлюють, та чи відображає він актуальні загрози.

Далі слідує технічна перевірка. Аудитори аналізують, як реалізовано технічні заходи безпеки, визначені у додатку А стандарту. Наприклад, вони перевіряють:

1) Як налаштовано контроль доступу до інформаційних систем. Чи використовуються багатофакторна автентифікація та розмежування прав доступу?

2) Як здійснюється резервне копіювання даних. Чи виконуються тести відновлення даних?

3) Чи ведеться моніторинг подій та виявлення аномалій у системах.

Крім того, проводиться аналіз процедур управління інцидентами. Аудитори перевіряють, чи існують регламенти реагування, чи ведуться записи про інциденти, та які заходи були вжиті для запобігання повторенню подібних подій.

Перевірка фізичної безпеки включає аналіз доступу до серверних приміщень, наявність систем відеоспостереження та сигналізації. Стандарт ISO 27001 вимагає захисту фізичних активів, тому аудитори оцінюють, чи реалізовано ці вимоги на практиці.

Після цього проводяться інтерв'ю з персоналом. Особлива увага приділяється обізнаності співробітників щодо політик інформаційної безпеки. Наприклад, відповідно до ISO 27001 (розділ 7.3), працівники повинні розуміти свою роль у захисті інформації, а також знати, як реагувати на інциденти. Важливо, щоб їхня діяльність відповідала задокументованим процедурам.

3.1.4 Процедура оцінки ризиків

Оцінка ризиків інформаційної безпеки відповідно до стандартів ISO 31000 і ISO 27005 є структурованим процесом який можна зобразити на рисунку 3.2.

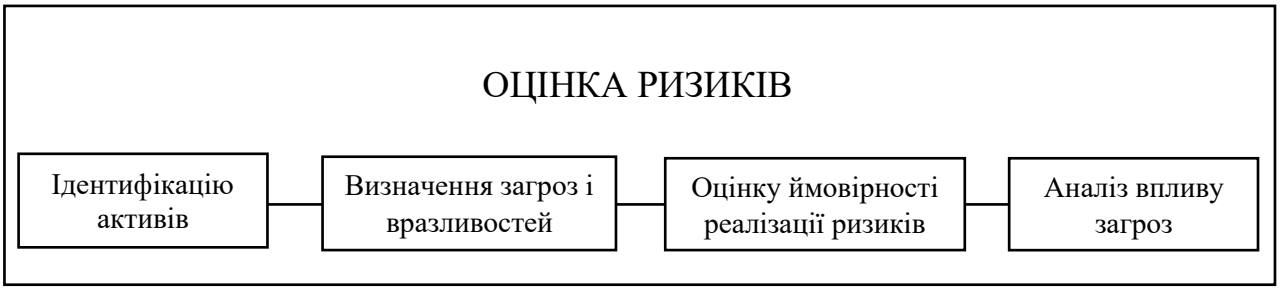


Рисунок 3.2 – Етапи процесу оцінки ризиків за стандартами ISO 31000 та ISO 27005

Процес починається з ідентифікації активів, як це передбачено в ISO 27005 (п. 7.2). Цей етап передбачає детальне виявлення всіх ресурсів організації, які потрібно захищати. До активів належать технічні (сервери, мережеве

обладнання), інформаційні (дані, документи) та фізичні (приміщення, пристрої) ресурси. Активи класифікуються за їхньою важливістю для організації відповідно до вимог ISO 27001 (дод. А). Наприклад, бази даних із персональними даними громадян отримують високий пріоритет через їхню критичність і чутливість. Важливим аспектом є також визначення власників активів, які відповідають за їхнє використання та захист.

Ідентифікація загроз (ISO 27005, п. 7.4.2) аналізує всі можливі загрози, які можуть вплинути на ці активи. Загрози включають різноманітні сценарії, наприклад, атаки зловмисників, технічні збої, фізичні небезпеки (пожежі, затоплення) або помилки співробітників. Для кожного активу визначаються можливі сценарії реалізації загроз, щоб оцінити їхню реальність та серйозність. Наприклад, для серверної кімнати загрозою є відсутність системи пожежогасіння, що створює ризик повного знищення даних у разі пожежі.

На етапі аналізу вразливостей (ISO 27005, п. 7.4.3) оцінюються слабкі місця системи, які можуть бути використані для реалізації загроз. Наприклад, використання застарілого програмного забезпечення без регулярних оновлень створює вразливість, що полегшує несанкціонований доступ. Аналіз включає технічні аспекти (вразливості систем), організаційні аспекти (недостатнє навчання співробітників) та фізичні аспекти (відсутність контролю доступу до критичних приміщень).

Оцінка ймовірності реалізації кожного ризику, яка описана в ISO 27005 (п. 7.4.4), може проводитися якісно (експертна оцінка) або кількісно (на основі даних про минулі інциденти). Ймовірність визначається за шкалою, наприклад, як низька, середня чи висока. Наприклад, якщо організація регулярно стикається з фішинговими атаками, ймовірність успішної атаки може бути оцінена як висока, особливо за відсутності навчання персоналу або технічних заходів захисту.

Далі оцінюється вплив реалізації кожного ризику (ISO 27005, п. 7.4.4). Аналіз включає оцінку наслідків реалізації ризику для конфіденційності, цілісності та доступності активів, а також фінансові втрати, репутаційний збиток

та можливі збої в роботі організації. Наприклад, витік персональних даних громадян може призвести до значних штрафів, судових позовів і втрати довіри громади. Для оцінки впливу використовується аналогічна шкала (низький, середній, високий).

Після цього визначається рівень ризиків шляхом комбінування ймовірності та впливу, що відповідає рекомендаціям ISO 27005 (п. 8). Це робиться за допомогою матриці ризиків, яка дозволяє чітко визначити, які ризики є критичними, а які можуть бути прийнятними без негайного втручання. Наприклад, якщо загроза є високоймовірною і має значний вплив, її оцінюють як критичний ризик. Це дозволяє організації зрозуміти, на які ризики потрібно звернути увагу в першу чергу.

На основі отриманих даних формується план управління ризиками (ISO 27005, п. 9). Він може включати заходи з уникнення ризиків (відмова від небезпечних процесів), зменшення ймовірності або впливу (наприклад, впровадження багатофакторної автентифікації), передачі ризиків (страхування) або прийняття ризиків (якщо вони мінімальні). План також передбачає конкретні строки виконання заходів, визначення відповідальних осіб та розподіл ресурсів для реалізації.

Результати оцінки документуються у вигляді звіту, який містить детальну інформацію про виявлені ризики, їхній рівень, рекомендовані заходи та пріоритетність. Документування є обов’язковим етапом, описаним в ISO 27005 (п. 10). Цей звіт надається керівництву організації для ухвалення стратегічних рішень.

Завершальний етап включає моніторинг і перегляд ризиків (ISO 27005, п. 11). В умовах динамічних змін у середовищі загроз важливо регулярно оновлювати оцінки ризиків, впроваджувати нові заходи та перевіряти ефективність існуючих. Це забезпечує постійне вдосконалення системи управління інформаційною безпекою.

3.1.5 Процес узагальнення результатів

Після завершення перевірок аудитори аналізують зібрані дані, включаючи записи інтерв'ю, результати технічних перевірок та документи. Цей аналіз спрямований на виявлення невідповідностей вимогам стандарту ISO 27001.

Узагальнення результатів проводиться у вигляді детального звіту. У ньому описуються всі виявлені невідповідності із зазначенням рівня їхньої критичності. Наприклад, якщо виявлено, що резервні копії не перевіряються на предмет можливості відновлення, це розглядається як серйозний ризик для безперервності бізнесу.

Звіт містить рекомендації для усунення недоліків. Ці рекомендації базуються на положеннях стандарту ISO 27002, який надає практичні вказівки щодо впровадження заходів безпеки.

Завершальний етап включає обговорення результатів з керівництвом міської ради. Аудитори пояснюють виявлені ризики, їхній потенційний вплив на організацію та пропонують план коригувальних дій. У цьому плані визначаються конкретні заходи, терміни їхнього виконання та відповідальні особи.

Остаточний звіт є не лише підсумком аудиту, а й дорожньою картою для вдосконалення системи управління інформаційною безпекою. У ньому зазначаються рекомендації щодо оновлення політик, процедур, технічних заходів і навчання персоналу.

Організація також повинна впровадити механізм моніторингу виконання коригувальних заходів, щоб забезпечити усунення недоліків. Наприклад, це може бути регулярний перегляд прогресу виконання або повторний аудит після завершення впровадження заходів.

Таким чином, детальний аудит, проведений за стандартами ISO 27000, дозволяє не лише виявити поточний стан інформаційної безпеки в підрозділах міської ради, а й створити базу для постійного вдосконалення та забезпечення відповідності найкращим практикам у цій сфері.

3.1.6 Процес постійного вдосконалення

Постійне вдосконалення є одним із ключових принципів стандарту ISO 27001 і частиною циклу PDCA (Plan-Do-Check-Act), який використовується для забезпечення динамічного розвитку системи управління інформаційною безпекою (СУІБ). Цей процес спрямований на адаптацію організації до змін у зовнішньому середовищі загроз, технологіях і законодавчих вимогах, а також на вдосконалення внутрішніх процесів. Процес постійного вдосконалення складається з етапів зображених на рисунку 3.3.

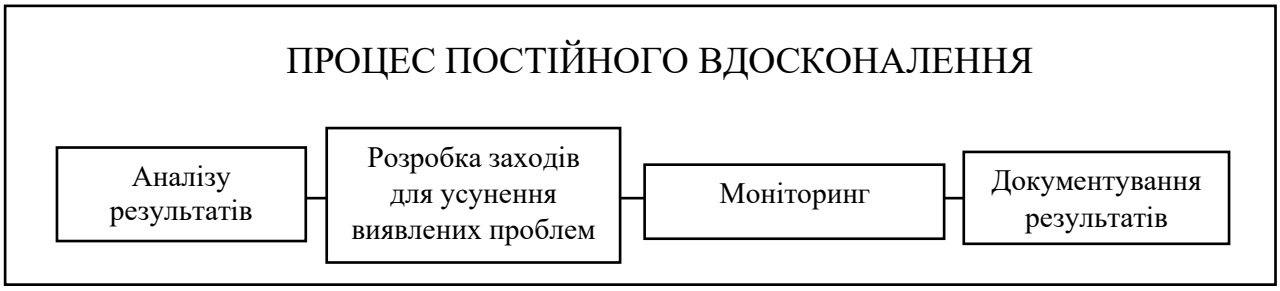


Рисунок 3.3 – Етапи процесу постійного вдосконалення

Аналізу результатів аудиту, який може бути проведений внутрішніми чи зовнішніми аудиторами відповідно до ISO 27007 (настанови для аудиту СУІБ). Аудит дозволяє виявити недоліки у функціонуванні СУІБ, включаючи невідповідності політик, недоліки технічного забезпечення чи недостатню обізнаність персоналу. На основі цього аналізу організація формулює коригувальні та запобіжні дії відповідно до вимог ISO 27001 (п. 10.1).

Наступним етапом є розробка заходів для усунення виявлених проблем. Коригувальні дії спрямовані на ліквідацію недоліків, наприклад, оновлення політик, впровадження нових технічних рішень або підвищення кваліфікації персоналу. Запобіжні дії зосереджуються на запобіганні повторному виникненню подібних проблем, наприклад, шляхом розробки нових процедур моніторингу чи автоматизації процесів.

Однією з важливих складових процесу вдосконалення є моніторинг та аналіз ефективності впроваджених змін. Відповідно до ISO 27001 (п. 9.1), організація повинна регулярно оцінювати, як зміни впливають на загальну

ефективність СУІБ. Для цього використовуються ключові показники ефективності (KPI), наприклад, зменшення кількості інцидентів безпеки, швидкість реагування на загрози або відповідність політик зовнішнім вимогам.

Окрім внутрішніх процесів, постійне вдосконалення включає адаптацію до змін у зовнішньому середовищі. Технологічні зміни, зокрема впровадження хмарних сервісів, також потребують оновлення політик безпеки, процедур і технічних заходів захисту.

Для підтримки безперервного вдосконалення важливо забезпечити регулярну комунікацію між усіма зацікавленими сторонами. Згідно з ISO 27001 (п. 7.4), організація повинна інформувати співробітників про зміни у СУІБ, навчати їх новим процедурам і залучати до обговорення шляхів вдосконалення. Регулярні тренінги та симуляції, наприклад, тестування готовності до фішингових атак, допомагають підвищити обізнаність і залученість персоналу.

Завершальним етапом процесу є документування результатів. Відповідно до ISO 27001 (п. 7.5), організація повинна вести записи про проведені аудити, впроваджені заходи та їхню ефективність. Це дозволяє створити базу знань, яка використовується для подальшого вдосконалення СУІБ.

Таким чином, постійне вдосконалення забезпечує динамічний розвиток системи управління інформаційною безпекою, адаптацію до нових викликів і зміцнення стійкості організації. Цей процес, відповідно до ISO 27001, не тільки усуває існуючі недоліки, але й запобігає їх повторному виникненню, забезпечуючи довгострокову ефективність та безпеку активів організації.

3.2 Впровадження NIST Cybersecurity Framework 2.0 в аудит ІБ на основі стандартів ISO

Впровадження NIST Cybersecurity Framework (CSF) у процес аудиту інформаційної безпеки ВМР потребує ретельного інтегрування з існуючими міжнародними стандартами, такими як ISO 31000 та ISO 27001. Це дозволяє забезпечити не лише дотримання найкращих практик кібербезпеки, але й

впровадити систематичний і стратегічний підхід до управління ризиками, який відповідає загальним цілям та обов'язкам міської ради.

Відповідно до ISO 31000, слід зосередитися на тому, як ризики можуть вплинути на здатність міської ради досягати своїх цілей, які включають забезпечення безперервного надання послуг громаді, захист конфіденційної інформації та дотримання регуляторних вимог. NIST CSF може бути впроваджений на цьому етапі через функцію GOVERN, яка акцентує увагу на визначенні стратегічних завдань, ролей і відповідальності у сфері кібербезпеки. Цей процес починається з аналізу політик інформаційної безпеки, щоб переконатися, що вони відповідають як стратегічним, так і операційним завданням міської ради.

На етапі планування аудиту важливо забезпечити узгодженість із принципами ISO 31000, які передбачають чітке визначення сфери аудиту, критеріїв оцінки ризиків та методів збору даних. Застосування NIST CSF на цьому етапі дозволяє створити ефективну структуру аудиту, використовуючи функцію IDENTIFY для визначення активів міської ради, таких як інформаційні системи, мережі, програмне забезпечення та дані. У процесі ідентифікації слід також враховувати загрози, що можуть впливати на ці активи, а також визначати вразливості, пов’язані з недостатнім захистом. Застосування NIST CSF дозволяє структурувати ці процеси, що забезпечує більш деталізовану та орієнтовану на практику оцінку.

Під час виконання аудиту важливо вимоги ISO 27001 встановлюють критерії перевірки процедур доступу, резервного копіювання, навчання персоналу та управління інцидентами. Однак NIST CSF забезпечує глибший технічний рівень аналізу. У рамках функції PROTECT слід оцінити, наскільки ефективно впроваджені заходи контролю доступу до інформаційних систем, шифрування даних та навчання персоналу. У функції DETECT, чи організація використовує сучасні інструменти моніторингу подій та аналізу аномалій для своєчасного виявлення кіберзагроз.

NIST CSF також забезпечує структурований підхід до перевірки процедур реагування на інциденти. RESPOND оцінює , чи документуються інциденти, чи є чітко визначені процеси комунікації із зацікавленими сторонами під час інцидентів, та наскільки швидко і ефективно впроваджуються коригувальні заходи. Функція RECOVER дозволяє оцінити здатність міської ради відновлювати свої операції після інцидентів, зокрема через тестування планів відновлення та аналіз ефективності резервного копіювання.

Після завершення перевірок слід перейти до глибокого аналізу ризиків, що є основою ISO 31000. У цьому процесі необхідно не лише оцінити ймовірність та вплив ризиків, але й розробити пріоритети для їх усунення. NIST CSF пропонує створення профілів організації, які допомагають виявляти прогалини між поточним станом кібербезпеки та бажаним. Наприклад, профіль може показати, що існуючі процедури моніторингу не дозволяють своєчасно виявляти загрози, що потребує вдосконалення систем моніторингу.

Завершальний звіт, який об’єднує підходи ISO та NIST, має включати конкретні рекомендації для усунення виявлених недоліків. Наприклад, якщо функція IDENTIFY показала недостатню обізнаність персоналу про ризики, слід рекомендувати впровадження регулярних тренінгів. Якщо функція PROTECT виявила проблеми із захистом конфіденційних даних, звіт має включати рекомендації щодо впровадження шифрування або покращення управління доступом.

Інтеграція NIST CSF дозволяє забезпечити безперервне вдосконалення кібербезпеки міської ради. На основі функції GOVERN слід розробити механізми моніторингу виконання рекомендацій, щоб забезпечити відповідність досягнутих змін загальній стратегії кіберзахисту ради. Таким чином, впровадження NIST CSF у процес аудиту інформаційної безпеки міської ради у поєднанні з ISO 31000 та ISO 27001 створює комплексний і надійний підхід до управління ризиками.

3.3 Впровадження КСЗІ в аудит ІБ на основі стандартів ISO

Аудит інформаційної безпеки міській раді що ґрунтується на міжнародних стандартах ISO 27000 і NIST Cybersecurity Framework має включати інтеграцію нормативних документів комплексної системи захисту інформації (КСЗІ).

Цей підхід дозволяє поєднати вимоги України з кращими світовими практиками для побудови ефективної та відповідної нормативам системи захисту. Розглянемо ключові етапи проведення аудиту та впровадження заходів із залученням з стандартів НДТЗІ.

ISO 27001 накладає подібну вимогу: необхідно визначити контекст системи, зацікавлені сторони та межі системи управління інформаційною безпекою (СУІБ). Порівняно з НДТЗІ, ISO 27001 передбачає ширший підхід до визначення бізнес-контексту та цілей організації. Однак у рамках українського регулювання на першому етапі критично важливо узгодити ІКС із вимогами законодавства.

Згідно з НДТЗІ 2.5-004-99, політики захисту інформації повинні враховувати класифікацію інформації за рівнем конфіденційності та передбачати технічні, криптографічні й організаційні заходи захисту [27]. У контексті міської ради це означає необхідність розробки політик для забезпечення конфіденційності персональних даних, доступу до них та їхньої цілісності(табл. 3.1).

Таблиця 3.1 Результат співставлення вимог ISO 27001 та НДТЗІ 2.5-004-99

Аспект	ISO 27001	НДТЗІ 2.5-004-99
Призначення	Стандарт для побудови системи управління інформаційною безпекою (СУІБ).	Вимоги до побудови систем захисту інформації в Україні.
Схожість	Обидва визначають вимоги до впровадження систем захисту інформації.	Спільний акцент на політиках безпеки та управлінні ризиками.
Відмінності	Глобальний підхід, більше уваги до менеджменту.	Фокус на технічних заходах і локальних вимогах.
Сфера застосування	Управління ризиками, політики захисту, сертифікація.	Реалізація державних вимог до інформаційної безпеки.

ISO 27001 пропонує загальний підхід до розробки політик, наголошуючи на їх узгодженні з цілями організації та забезпеченні розуміння політик усіма зацікавленими сторонами. Водночас НДТЗІ 2.1-002-07 вимагає створення

специфічних процедур контролю доступу, зокрема диференційованих прав доступу для користувачів (табл. 3.2)[28].

Таблиця 3.2 Результат співставлення вимог ISO 27002 та НДТЗІ 2.1-002-07

Аспект	ISO 27002	НДТЗІ 2.1-002-07
Призначення	Рекомендації щодо впровадження заходів інформаційної безпеки.	Загальні вимоги до захисту інформації в автоматизованих системах.
Схожість	Обидва описують технічні та організаційні заходи безпеки.	Спільний акцент на контролі доступу, моніторингу.
Відмінності	Гнучкі рекомендації, застосовні до різних організацій.	Жорсткі локальні вимоги до державних систем.

Ці вимоги співзвучні з рекомендаціями NIST CSF, які акцентують увагу на важливості визначення чітких правил і механізмів ідентифікації та автентифікації. У рамках КСЗІ особливу увагу приділяють формалізації процедур, що є ключовим аспектом для подальшої сертифікації.

Крім того, НДТЗІ вимагає забезпечення фізичного захисту інформаційних систем. Зокрема, у межах міської ради повинні бути впроваджені системи контролю доступу до приміщень із обробкою конфіденційної інформації. Це відповідає пунктам NIST CSF, які рекомендують використання фізичних бар’єрів.

Згідно з НДТЗІ 2.1-002-07, аудит КСЗІ охоплює перевірку технічних і організаційних заходів на відповідність визначеним критеріям [29]. У процесі аудиту проводиться аналіз журналів подій, перевірка конфігурації засобів захисту та тестування ефективності контролів.

ISO 27001 пропонує систематичний підхід до аудиту, що передбачає перевірку як відповідності політик, так і ефективності їх реалізації. Порівняно з ISO, НДТЗІ зосереджується на формальному дотриманні вимог, тоді як міжнародні стандарти акцентують увагу на досягненні цілей ІБ.

Особливістю НДТЗІ є обов’язковість переперевірки сертифікатів засобів захисту та їх відповідності новим вимогам, що забезпечує актуальність системи в умовах змінного середовища. NIST CSF додає до цього акцент на моніторингу нових загроз і реагуванні на інциденти.

Аудит КСЗІ міської ради на основі ISO 27000, доповнений стандартами НДТЗІ і NIST CSF, поєднує регламентовану відповідність із міжнародними

практиками управління інформаційною безпекою. Використання НДТЗІ дозволяє забезпечити сувору відповідність українському законодавству, а ISO та NIST додають гнучкості та орієнтованості на бізнес-процеси, створюючи ефективну систему захисту (табл. 3.3).

Таблиця 3.3 - Результат співставлення вимог НДТЗІ 2.1-002-07, НДТЗ 2.6-001-11, ISO 27006/27007

Аспект	НДТЗІ 2.1-002-07	ISO 27006	НДТЗІ 2.6-001-11	ISO 27007
Призначення	Захист інформації в автоматизованих системах	Сертифікація органів із СУІБ	Аудит систем технічного захисту інформації	Рекомендації для аудиту СУІБ
Масштаб	Локальний, Україна	Глобальний	Локальний, Україна	Глобальний
Цільова аудиторія	Держустанови, критична інфраструктура	Органи сертифікації	Організації, що проводять аудити	Аудитори СУІБ
Фокус	Вимоги до захисту інформації	Вимоги до сертифікації	Оцінка ефективності захисту	Організація, планування і звітність аудиту
Ризик-орієнтований підхід	Присутній	Присутній	Присутній	Присутній
Деталізація аудиту	Загальні вимоги	Чіткі вимоги до органів сертифікації	Загальні положення	Детальні рекомендації
Юридична основа	Відповідність законодавству України	Незалежний від юрисдикції	Відповідність законодавству України	Незалежний від юрисдикції
Адаптивність	Фіксовані вимоги	Гнучкий, адаптується до різних органів	Фіксовані вимоги	Гнучкий, адаптується до будь-якої організації
Ціль сертифікації	Сертифікація автоматизованих систем	Сертифікація органів із СУІБ	Перевірка відповідності систем захисту	Підтвердження якості управління СУІБ
Методологія аудиту	Загальна, без чітких методик	Конкретна для оцінки органів сертифікації	Загальна	Чітко структурована, включає рекомендації
Універсальність застосування	Вузьке, обмежене національними вимогами	Широке, для будь-якої організації	Локалізоване на український контекст	Глобальне, враховує різні юрисдикції
Роль аудиторів	Встановлює основні вимоги	Встановлює кваліфікацію для сертифікаційних органів	Регламентує базові обов'язки аудиторів	Описує вимоги до компетентності та поведінки аудиторів
Інтеграція з іншими стандартами	Інтегрується з іншими НДТЗІ	Враховує ISO 17021 (вимоги до сертифікацій)	Інтегрується з НДТЗІ	Сумісний з ISO 27001, 19011
Періодичність аудиту	Регламентується національними нормативами	Залежить від органів сертифікації	Визначено локальними нормами	Рекомендована регулярність

Інтеграція стандартів НДТЗІ до аудиту інформаційної безпеки на основі ISO 27000 дозволяє забезпечити відповідність державним вимогам.

3.4 Розробка методики аудиту

Як було зазначено вище, для впровадження ефективної системи інформаційної безпеки міської ради, аудит слід будувати на поєднанні міжнародних стандартів (ISO, NIST) і українських нормативних документів, які регламентують Комплексну систему захисту інформації (КСЗІ). Такий підхід дозволяє дотриматися локальних вимог, враховуючи закони та постанови

Кабінету Міністрів України, і водночас використовувати кращі практики світового рівня для управління інформаційними ризиками.

3.4.1 Процес попереднього аналізу та підготовки

Попередній аналіз та підготовка відіграють ключову роль на етапі організації аудиту інформаційної безпеки міської ради. Ця стадія спрямований на створення чіткої структури аудиту, визначення його обсягу, ресурсів, ключових показників ефективності та забезпечення взаєморозуміння між командою аудиторів і керівництвом міської ради. Для успішного виконання цього етапу слід врахувати вимоги міжнародних стандартів ISO, NIST CSF 2.0 та нормативних актів КСЗІ.

Розпочинається етап із визначення обсягу аудиту. У контексті міської ради з 40 відділами і близько 400 співробітниками необхідно встановити, які саме аспекти інформаційної безпеки будуть перевірені: технічна інфраструктура, політики та процедури, фізичний захист, навчання персоналу, відповідність законодавству чи всі ці компоненти разом. Відповідно до стандарту ISO 27001 (п. 4.3), визначення меж і обсягу системи менеджменту інформаційної безпеки є ключовим елементом на початковому етапі. Аналогічно, NIST CSF 2.0 (Identify) пропонує почати з інвентаризації активів, щоб зрозуміти, які ресурси критичні для роботи організації.

Наступним кроком є аналіз ризиків, пов’язаних із проведенням аудиту. Наприклад, якщо певні системи міської ради працюють у режимі 24/7, будь-яке втручання може вплинути на їхню працездатність. Відповідно до ISO 31000, аналіз ризиків допомагає виявити потенційні проблеми та розробити план їх мінімізації. Відповідність цьому підходу доповнюється методологією NIST SP 800-30, яка детально описує процес оцінки ризиків, включаючи їхню ідентифікацію, аналіз і визначення пріоритетності.

Одночасно з цим проводиться ідентифікація зацікавлених сторін. У межах міської ради це можуть бути керівники відділів, IT-служба, служба безпеки, юридичний відділ та інші. ISO 27001 (п. 5.2) підкреслює важливість залучення вищого керівництва до процесу аудиту для забезпечення його підтримки. У той

же час, NIST CSF 2.0 (Govern) наголошує на важливості інтеграції процесів кібербезпеки з загальним управлінням організацією. Спільна робота із зацікавленими сторонами дозволяє встановити реалістичні очікування, розподілити ролі та відповідальність, а також уникнути конфліктів під час аудиту.

Для ефективної підготовки важливо провести огляд існуючої документації міської ради. До такої документації належать політики безпеки, правила доступу, процедури управління ризиками, інструкції з реагування на інциденти, плани аварійного відновлення тощо. ISO 27002 (розділ 8) надає чіткі рекомендації щодо того, якою має бути структура документів, тоді як NIST CSF 2.0 (Protect) підкреслює важливість документування політик як частини управління кібербезпекою.

Ще одним важливим завданням є підготовка технічного інструментарію для проведення аудиту. Це може включати програмні засоби для аналізу логів, сканування вразливостей, перевірки мережевого трафіку та інші рішення. ISO 27001 та NIST акцентують увагу на необхідності використання спеціалізованих інструментів для моніторингу й аналізу даних. Вибір конкретних рішень залежить від технічних можливостей міської ради та типу перевірок, які заплановані.

Останнім, але не менш важливим елементом підготовки, є розробка плану комунікації. Важливо заздалегідь визначити, як команда аудиторів буде взаємодіяти з представниками міської ради, як інформуватиме про проміжні результати та як буде передаватися остаточний звіт. ISO 27001 (п. 7.4) вимагає, щоб комунікації були чіткими, зрозумілими та забезпечували ефективний обмін інформацією. NIST CSF 2.0 (Govern) також наголошує на важливості регулярних обговорень між командами безпеки та керівництвом.

3.4.2 Процес проведення аудиту

Проведення аудиту інформаційної безпеки міської ради є основним етапом, що забезпечує оцінку ефективності існуючих заходів безпеки, відповідність стандартам та виявлення можливих вразливостей. Цей етап

включає комплексну перевірку політик, процедур, технічних рішень і організаційних заходів. Під час аудиту особлива увага приділяється як виявленню проблем, так і оцінці поточної ефективності системи безпеки в контексті стандартів ISO 27001, ISO 27002, NIST Cybersecurity Framework (CSF) 2.0 та вимогам КСЗІ.

На етапі проведення аудиту перевіряються документи, що описують політики та процедури інформаційної безпеки в міській раді. Це включає аналіз усіх внутрішніх нормативних актів, регламентуючих питання доступу до інформаційних систем, управління інцидентами, резервного копіювання, зберігання даних та безпеки мереж. Згідно з ISO 27001 (п. 5.1–5.2), такі політики мають бути переглянуті та оновлені відповідно до змін у внутрішніх процесах та зовнішніх вимогах.

У ВМР це означає перевірку таких документів, як:

- політика безпеки інформаційних систем;
- процедури реагування на інциденти;
- правила управління доступом та ідентифікацією користувачів;
- стандарти резервного копіювання та відновлення даних.

Аудитор перевіряє, чи відповідають ці документи вимогам ISO 27001, чи вони актуальні, чи покривають всі аспекти інформаційної безпеки, а також чи відповідають новим законодавчим вимогам, таким як Закон України "Про захист персональних даних" або нормативним актам, що регулюють інформаційно-комунікаційні системи (КСЗІ).

Аудитори проводять оцінку ризиків та вразливостей з використанням методів, що відповідають стандартам NIST Cybersecurity Framework (CSF) 2.0 та ISO 31000. Це включає ідентифікацію можливих загроз для інформаційних систем міської ради, оцінку рівня їх ймовірності, а також впливу на організацію у разі реалізації таких загроз. Основною метою є визначення, які критичні активи та системи потребують додаткової уваги та посилення захисту.

Аудитори використовують інструменти для автоматизованого збору інформації, наприклад, програмне забезпечення для сканування вразливостей,

яке перевіряє мережеву інфраструктуру на наявність відомих вразливостей (наприклад, CVE-бази). Також проводиться огляд результатів попередніх інцидентів для визначення слабких місць у системі реагування на інциденти.

Крім того, важливим етапом є оцінка рівня захищеності персоналу від соціальної інженерії та фішингових атак. Для цього можуть бути проведені тестові фішингові атаки або тренінги з підвищення обізнаності.

Цей етап аудиту передбачає перевірку технічних засобів захисту, які забезпечують безпеку інформаційних систем міської ради. Аудитори перевіряють налаштування міжмережевих екранів (фаєрволів), систем виявлення та запобігання вторгненням (IDS/IPS), системи моніторингу безпеки (SIEM), а також верифікацію використання криптографічних засобів для захисту передавання та зберігання даних.

Згідно з ISO 27001 (дод. A), критичні інформаційні системи повинні бути захищені відповідними технічними засобами, а їх налаштування повинні регулярно перевірятися на відповідність найкращим практикам безпеки. Аудитори перевіряють, чи є належна конфігурація мережевого обладнання, чи застосовуються актуальні патчі безпеки для програмного забезпечення, та чи використовується надійна аутентифікація і контроль доступу.

Особлива увага приділяється тестуванню на проникнення (penetration testing), яке дозволяє виявити слабкі місця у безпеці системи. Це може включати як зовнішнє тестування з використанням публічно доступних інструментів, так і внутрішні перевірки з метою оцінки ефективності політики безпеки.

Оцінка фізичної безпеки є невід'ємною частиною аудиту, особливо в контексті ISO 27001 (дод. A), де йдеться про управління доступом до інформаційних систем. Вона включає перевірку наявності фізичних бар'єрів для доступу до серверних кімнат, контроль за вхідними дверима, наявність камер спостереження, а також верифікацію, чи встановлено необхідне обладнання для контролю доступу до обмежених приміщень (наприклад, карткові системи доступу).

Важливо також перевірити організацію захисту від стихійних лих (пожежі, підтоплення тощо). Відповідно до ISO 27001, для збереження інформаційних активів необхідно забезпечити захист не лише на рівні програмних та технічних засобів, але й фізично обмежити доступ до критичних систем.

Аудит також включає оцінку дотримання політик безпеки з боку співробітників міської ради. Це включає перевірку наявності тренінгів з інформаційної безпеки, оцінку рівня обізнаності працівників щодо ризиків і методів захисту, а також виявлення можливих порушень політики доступу.

Цей етап передбачає також перевірку управління привілеями користувачів: чи встановлено належний контроль доступу до критичних інформаційних ресурсів, чи проводиться регулярний перегляд прав доступу. ISO 27001 акцентує увагу на управлінні доступом, тому важливо перевірити, чи є політика регулярного перегляду прав доступу і чи правильно розмежовані права співробітників залежно від їх посад.

Завершальний етап аудиту — це формулювання висновків на основі отриманих результатів перевірки. Аудитор складає звіт, в якому зазначає виявлені слабкі місця, порушення та потенційні загрози. Крім того, надаються рекомендації щодо усунення виявлених недоліків та покращення існуючої системи безпеки. Це може включати рекомендації по оновленню політик, удосконаленню технічних засобів захисту або підвищенню рівня обізнаності персоналу.

У результаті аудиту міська рада отримує чітке розуміння, які аспекти системи безпеки потребують покращення, а також рекомендації для подальших дій.

3.4.3 Процедура оцінки ризиків

Цей етап базується на принципах управління ризиками, визначених у міжнародних стандартах, таких як ISO 31000, ISO 27005, а також у рекомендаціях NIST SP 800-30 та NIST Cybersecurity Framework (CSF) 2.0. У контексті міської ради, що складається з 40 відділів і близько 400 співробітників, оцінка ризиків має враховувати як технічні, так і організаційні аспекти.

Процес оцінки ризиків починається з ідентифікації активів. У рамках цього завдання необхідно скласти детальний реєстр усіх інформаційних активів міської ради, таких як сервери, робочі станції, мережеве обладнання, програмне забезпечення, бази даних і навіть паперові архіви. ISO 27001 (дод. A) наголошує на важливості інвентаризації активів, включаючи їхню класифікацію за рівнем критичності. NIST CSF 2.0 (Identify) передбачає створення профілю активів, що допоможе зрозуміти, які з них є найбільш важливими для досягнення стратегічних цілей організації. Визначення активів також має враховувати фізичні ресурси, такі як серверні приміщення та обладнання для зберігання даних.

Після ідентифікації активів проводиться аналіз загроз, які можуть вплинути на ці активи. Це включає як зовнішні загрози, наприклад, кібератаки, природні катастрофи або збої в електропостачанні, так і внутрішні загрози, такі як несанкціонований доступ співробітників, недотримання політик безпеки або ненавмисні помилки. NIST SP 800-30 пропонує деталізований підхід до аналізу загроз, включаючи їхню класифікацію та опис механізмів реалізації. Одночасно з цим стандарт ISO 27005 (п. 7.4.3) рекомендує враховувати ймовірність виникнення загроз та їхній потенційний вплив на організацію.

Аналіз вразливостей є наступним етапом. У цьому контексті потрібно оцінити, наскільки інформаційні системи міської ради захищені від ідентифікованих загроз. Наприклад, це може включати перевірку оновлення програмного забезпечення, налаштувань мережевого обладнання, конфігурації серверів, а також фізичної безпеки серверних приміщень. ISO 27002 (п. 12.6) акцентує увагу на важливості регулярного сканування вразливостей і оцінки їхнього впливу. Водночас, NIST CSF 2.0 (Protect) рекомендує використовувати автоматизовані інструменти для виявлення вразливостей, щоб забезпечити повноту аналізу та швидкість реагування.

Одним із важливих аспектів оцінки ризиків є визначення впливу потенційних інцидентів на організацію. Наприклад, несанкціонований доступ до бази даних із персональними даними громадян може призвести до фінансових

штрафів, порушення довіри громади та юридичної відповідальності. ISO 31000 пропонує оцінювати вплив ризиків не лише з точки зору фінансових втрат, але й репутаційних наслідків та впливу на стратегічні цілі організації. Аналогічно, NIST SP 800-30 рекомендує створювати моделі впливу, які допоможуть візуалізувати наслідки реалізації ризиків.

На основі зібраних даних проводиться оцінка ймовірності виникнення ризиків і їхньої серйозності. У цьому контексті використовується матриця ризиків, яка дозволяє категоризувати ризики за рівнем пріоритетності. Наприклад, ризик фізичного пошкодження серверної кімнати через відсутність системи пожежогасіння може бути оцінений як високий, якщо ця кімната містить критичні дані. ISO 27005 (п. 7.6) надає рекомендації щодо визначення рівнів ризиків та їхнього аналізу в контексті ймовірності та впливу. У свою чергу, NIST CSF 2.0 (Identify) пропонує використовувати інструменти, такі як аналіз сценаріїв і статистичні моделі, для більш точного прогнозування ризиків.

Важливо зазначити, що результати оцінки ризиків повинні бути задокументовані та передані керівництву для ухвалення рішень. Це передбачає створення звіту, який включає опис ідентифікованих ризиків, їхній рівень та запропоновані заходи для зниження впливу. ISO 27001 (п. 10.1) наголошує на важливості документації як основи для подальших дій. NIST CSF 2.0 (Respond) рекомендує включати в такі звіти плани з реагування, які допоможуть керівництву зрозуміти, які кроки необхідно зробити для мінімізації ризиків.

Процес оцінки ризиків завершується розробкою плану управління ризиками, який визначає конкретні заходи для зменшення ймовірності або впливу ідентифікованих загроз. Наприклад, встановлення системи багатофакторної автентифікації може знизити ризик несанкціонованого доступу до інформаційних систем. ISO 27001 (дод. A) та NIST CSF 2.0 (Protect) рекомендують створювати чіткий план дій, який враховує як технічні, так і організаційні аспекти управління ризиками.

3.4.4 Розробка політик і процедур

Розробка політик і процедур є важливим етапом у забезпеченні ефективності інформаційної безпеки міської ради. Цей процес дозволяє створити чітку нормативну базу, яка регламентує всі аспекти управління кібербезпекою, від доступу до ресурсів до дій у разі інцидентів. Політики та процедури повинні відповідати міжнародним стандартам ISO та NIST CSF 2.0, а також локальним нормативним актам КСЗІ, що гарантує їхню релевантність як на міжнародному, так і на локальному рівні.

Розпочинається цей процес із визначення загальної стратегії інформаційної безпеки. Згідно з ISO 27001 (п. 5.1), організація має визначити свою політику інформаційної безпеки, яка буде враховувати специфіку її діяльності та ризики. У випадку міської ради така політика охоплює аспекти захисту персональних даних, управління доступом, моніторингу систем та реагування на інциденти. NIST CSF 2.0 (Govern) доповнює цю вимогу, підкреслюючи необхідність інтегрування політики кібербезпеки у загальне управління організацією. Відповідно до Постанови №373, політика також має враховувати специфічні вимоги захисту державної інформації.

Ключовим компонентом є розробка процедур управління доступом. Це включає визначення рівнів доступу для співробітників, запровадження багатофакторної автентифікації та управління правами доступу. ISO 27002 (п. 9) надає рекомендації щодо управління ідентифікацією користувачів та контролю доступу. NIST детально описує принципи управління обліковими записами, наголошуючи на важливості регулярного перегляду прав доступу. Впровадження цих процедур гарантує, що доступ до критичної інформації матимуть лише уповноважені особи, що мінімізує ризики внутрішніх загроз.

Окремою складовою є розробка політики збереження логів і моніторингу систем. Логи повинні містити дані про всі значущі події, такі як спроби входу в систему, зміни конфігурації чи запуск нових програм. ISO 27002 (п. 12.4) та NIST наголошують на необхідності регулярного зберігання й аналізу логів для

виявлення підозрілої активності. У міській раді ці дані допоможуть вчасно виявляти інциденти, зокрема атаки зловмисників або внутрішні зловживання.

Політика управління інцидентами є ще одним ключовим елементом. Вона передбачає визначення алгоритму дій у разі виявлення кіберзагроз або інцидентів безпеки. ISO 27001 (дод. A) рекомендує організаціям впроваджувати процеси ідентифікації, аналізу та реагування на інциденти. NIST CSF 2.0 (Respond) акцентує увагу на необхідності документування інцидентів, проведення розслідувань та впровадження заходів для запобігання їх повторенню. Українське законодавство, включаючи Закон України "Про захист інформації в інформаційно-комунікаційних системах", вимагає, щоб організації мали чіткий план реагування на інциденти, адаптований до місцевих умов.

Важливим аспектом є розробка процедур управління ризиками. ISO 31000 визначає ризик як ефект невизначеності на цілі організації, а NIST SP 800-30 пропонує чіткий підхід до ідентифікації, аналізу й оцінки ризиків. Для міської ради це означає, що всі потенційні загрози, такі як фішингові атаки, вразливості в програмному забезпеченні або фізичний доступ до серверів, мають бути ідентифіковані, оцінені та враховані в політиках безпеки.

Крім того, розробка політики навчання співробітників є обов’язковою. Співробітники повинні розуміти основи інформаційної безпеки, знати, як діяти у разі підозрілих ситуацій, та розуміти свою відповідальність за захист інформації. ISO 27001 (дод. A) і NIST CSF 2.0 (Protect) підкреслюють важливість регулярного навчання персоналу як ключового елемента захисту від людського фактора. У рамках КСЗІ, це також відповідає вимогам Постанови №373, яка наголошує на необхідності підвищення обізнаності персоналу.

Нарешті, усі розроблені політики та процедури мають бути документально оформлені, затверджені керівництвом і періодично переглядатися для актуалізації. ISO 27001 (п. 10.1) встановлює вимогу до циклічного перегляду політик, що забезпечує їх відповідність новим загрозам та вимогам. NIST CSF 2.0 (Govern) доповнює цей підхід, підкреслюючи важливість безперервного вдосконалення політик.

3.4.5 Процес впровадження технічних і організаційних заходів

На цьому етапі впроваджуються заходи, що забезпечують захист активів і мінімізують ризики. Наприклад, відповідно до NIST, у мережевій інфраструктурі можуть впроваджуватися фаєрволи, системи моніторингу трафіку (SIEM) і механізми багатофакторної автентифікації. Стандарти ISO 27002 пропонують впровадження процедур регулярного оновлення програмного забезпечення і контролю доступу.

КСЗІ вимагає, щоб усі технічні засоби захисту були сертифіковані. Це включає використання сертифікованих засобів шифрування для передачі конфіденційної інформації, резервування даних і захисту серверів. Постанова № 373 також уточнює порядок тестування систем захисту перед введенням їх в експлуатацію.

Організаційні заходи включають навчання персоналу, створення команди реагування на інциденти та проведення регулярних тестів на проникнення (пентестів). Це дозволяє не лише забезпечити відповідність систем нормативним вимогам, але й підготувати співробітників до реальних загроз.

3.4.6 Процес постійного вдосконалення

Постійне вдосконалення в аудиті інформаційної безпеки міської ради є складовою підтримки ефективності системи управління безпекою в умовах змін зовнішнього середовища, внутрішніх процесів та появи нових кіберзагроз. Ця частина процесу орієнтується на рекомендації ISO 27001 (дод. A), принципи NIST Cybersecurity Framework (CSF) 2.0 (Improve), а також враховує локальні вимоги КСЗІ щодо безперервного контролю та оновлення заходів безпеки.

Основою постійного вдосконалення є цикл PDCA (Plan-Do-Check-Act), рекомендований ISO 27001 для управління процесами інформаційної безпеки. У міській раді цей підхід дозволяє не лише підтримувати належний рівень безпеки, але й адаптуватися до змін у законодавстві, технологіях або організаційних потребах. Наприклад, у разі оновлення законодавства про захист персональних

даних або змін у структурі міської ради система інформаційної безпеки може бути переглянута та модифікована відповідно до нових вимог.

Першим важливим елементом постійного вдосконалення є регулярне проведення повторних аудитів. Відповідно до ISO 27001 (п. 9.2), це передбачає оцінку ефективності вже впроваджених заходів і виявлення нових ризиків. У міській раді повторний аудит можна проводити раз на пів року або рік залежно від критичності захищеної інформації. При цьому увага приділяється не лише технічним системам, але й організаційним аспектам, таким як виконання співробітниками розроблених політик.

Для забезпечення актуальності системи управління безпекою важливо впровадити процес моніторингу нових загроз та уразливостей. NIST CSF 2.0 (Identify) рекомендує використовувати автоматизовані засоби для моніторингу відкритих джерел інформації, звітів про вразливості та нових типів атак. Наприклад, у міській раді можна налаштувати систему отримання сповіщень про оновлення баз даних вразливостей або звітів національного центру кіберзахисту.

Не менш важливим є процес оновлення технічних засобів захисту. Відповідно до ISO 27002 (п. 12.6), оновлення повинні включати патчинг програмного забезпечення, перевірку налаштувань безпеки мережі та регулярне тестування системи на проникнення. У міській раді, з її великим обсягом інформаційних систем, автоматизація цього процесу (наприклад, через інструменти управління оновленнями) може значно підвищити ефективність.

Для вдосконалення організаційних заходів велике значення має навчання персоналу. ISO 27001 (дод. A) і NIST CSF 2.0 (Protect) підкреслюють важливість підвищення обізнаності співробітників щодо нових загроз. Регулярні тренінги для працівників міської ради повинні включати симуляції фішингових атак, ознайомлення з сучасними видами соціальної інженерії та практичні інструкції з безпечного використання ресурсів.

Ключовим напрямом вдосконалення є оновлення політик і процедур безпеки. Згідно з ISO 27001 (дод. A), політики мають переглядатися у разі змін у зовнішньому середовищі або організаційних процесах. У міській раді це може

означати створення нових правил роботи у віддаленому режимі чи оновлення політик щодо використання особистих пристроїв.

Додатково важливо розвивати систему управління інцидентами. NIST CSF 2.0 (Respond) рекомендує впроваджувати методи аналізу причин інцидентів та розробляти заходи для уникнення подібних випадків у майбутньому. Наприклад, якщо в мережі міської ради була виявлена спроба фішингу, після ліквідації загрози необхідно не лише навчити співробітників, як уникати подібних атак, але й посилити контроль за вхідними листами за допомогою фільтрів.

Таким чином, постійне вдосконалення системи інформаційної безпеки у міській раді базується на циклічному процесі оцінки, адаптації та оновлення. Завдяки інтеграції принципів ISO 27001, NIST CSF 2.0 і КСЗІ, цей процес гарантує актуальність та ефективність захисних заходів навіть у динамічному середовищі. Це дозволяє міській раді не лише відповідати сучасним стандартам безпеки, але й запобігати потенційним загрозам у майбутньому.

3.5 Підрахунок витраченого часу

Підрахунок витраченого часу на аудит інформаційної безпеки міської ради є важливим етапом, який забезпечує ефективне планування та оптимальне використання ресурсів. Для міської ради з 40 відділами та близько 400 працівниками визначення тривалості аудиту базується на обсязі робіт, кількості задіяних фахівців, складності системи інформаційної безпеки та глибини перевірок. В основі цього процесу лежать рекомендації стандартів ISO 27001, ISO 19011, NIST Cybersecurity Framework (CSF) 2.0, а також врахування локальних вимог КСЗІ.

Витрати часу розраховуються з урахуванням таких параметрів, як масштабність перевірки, кількість і типи інформаційних активів, рівень загроз та ризиків, а також складність впроваджених технічних і організаційних рішень. Наприклад, відповідно до ISO 27006, для організацій подібного масштабу рекомендований час аудиту для сертифікації складається з аналізу документації,

перевірки системи на місці та формування звіту. У випадку міської ради це може становити від 15 до 25 днів залежно від рівня підготовленості.

Етап попереднього аналізу та підготовки передбачає збір та оцінку інформації щодо існуючої системи управління інформаційною безпекою. Згідно з ISO 19011, це може займати від 3 до 5 днів. Час залежить від складності наявної документації, обсягу активів і доступності ключових даних. У міській раді це може включати оцінку всіх політик і процедур, вивчення внутрішніх звітів про інциденти, а також аналіз мережевої інфраструктури.

На етапі розробки політик і процедур час витрачається на створення або адаптацію необхідної документації відповідно до стандартів. ISO 27001 вимагає, щоб усі політики охоплювали управління доступом, захист даних, реагування на інциденти, резервне копіювання тощо. Для міської ради, з огляду на масштаби та кількість працівників, цей етап може тривати від 5 до 10 днів.

Оцінка ризиків за стандартами NIST CSF 2.0 та ISO 31000 є одним із найбільш трудомістких етапів, оскільки включає ідентифікацію ризиків, їхню класифікацію, оцінку й розробку плану управління. У міській раді це може тривати від 7 до 12 днів, залежно від кількості активів і складності їхньої взаємодії.

Впровадження технічних і організаційних заходів є найбільш тривалим етапом. Він охоплює встановлення технічних засобів, налаштування систем, навчання персоналу, тестування рішень і документування. За стандартами ISO 27001 цей процес може займати від 20 до 30 днів. У міській раді цей час залежить від кількості технічних рішень, які потребують впровадження або оновлення.

На етапі постійного вдосконалення витрати часу визначаються циклічністю цього процесу. Відповідно до ISO 27001 (п. 10.2), повторні аудити, моніторинг системи та вдосконалення процедур можуть виконуватися протягом кількох днів кожні пів року або рік. Для міської ради це може становити 5–10 днів щорічно.

Сумарно, загальний час проведення аудиту інформаційної безпеки у ВМР може варіюватися залежно від глибини перевірок та підготовленості організації.

Для повного аудиту, включаючи всі ключові етапи, необхідно закладати від 50 до 80 днів роботи, що забезпечить належний рівень перевірки всіх компонентів системи безпеки та їх відповідність вимогам ISO, NIST CSF 2.0 і КСЗІ.

Висновки до розділу

У цьому розділі детально описано процес впровадження методики аудиту інформаційної безпеки для підрозділів Вінницької міської ради, яка базується на сучасних міжнародних і національних стандартах. Основу методики становить стандарт ISO 27000, що забезпечує систематичний підхід до управління інформаційною безпекою. Він дозволяє ефективно ідентифікувати та мінімізувати ризики, а також постійно вдосконалювати процеси забезпечення безпеки.

Для підвищення ефективності методики було інтегровано елементи NIST Cybersecurity Framework 2.0, що зосереджує увагу на практичних аспектах кібербезпеки. Цей підхід включає розробку процесів ідентифікації активів, які потребують захисту, впровадження механізмів для запобігання інцидентам, а також механізмів своєчасного виявлення кіберзагроз. Окремий акцент зроблено на налаштуванні процедур швидкого реагування на інциденти та розробці планів відновлення після атак. У методику включено нормативні вимоги КСЗІ, які регламентують захист державної інформації та критичної інфраструктури. Це особливо важливо для місцевих органів влади, які працюють із персональними даними громадян, фінансовою інформацією та іншими критично важливими ресурсами.

Аналіз показав, що проведення такого аудиту за розробленою методикою вимагає від 50 до 80 днів роботи, що є оптимальним для забезпечення всебічного та ефективного дослідження стану інформаційної безпеки.

4 ЕКОНОМІЧНА ЧАСТИНА

В процесі наукових досліджень необхідно враховувати як потенційні витрати на проведення дослідницького процесу, так і безпосередні результати, які визначають доцільність проведення дослідження. Отримані результати характеризують отриманий кінцевий продукт а також наукові знання, які можуть бути застосовані для подальшого розвитку науки.

Комплексна магістерська кваліфікаційної робота на тему «Аудит інформаційної безпеки департаментів вінницької міської ради. Частина 1. Методика проведення аудиту». Відноситься до науково-технічних робіт, що впроваджується на підприємстві «Вінницька міська рада». Основною метою цієї роботи є покращення процесу проведення аудиту інформаційної безпеки шляхом розробки методики яка б поєднувала державні вимоги з міжнародними стандартами. Для розрахунку доцільності та ефективності інвестицій, вкладених в дану роботу, необхідно провести такі етапи робіт:

1) Проведення технологічного аудиту власної науково-технічної розробки, тобто встановлення її науково-технічного рівня (без комерціалізації);
2) Розрахунок витрат на здійснення науково-технічної розробки;
3) Розрахунок економічної ефективності науково-технічної розробки у випадку її впровадження у вінницькій міській раді. Власному підприємстві та обґрунтування економічної доцільності впровадження розробником (замовником) розробленого у комплексній магістерській кваліфікаційній науково-технічного проекту.

4.1 Технологічний аудит розробки

Для проведення оцінювання необхідно отримати оцінки експертів відповідно кожного критерія і обчислити середню арифметичну оцінку, яка визначатиме науково-технічний рівень та комерційний потенціал розробки.

Експертами виступають:

1) Войтович Олеся Петрівна, доцент кафедри Захисту інформації, ВНТУ;

2) Каплун Валентина Аполінаріївна, старший викладач кафедри ЗІ, ВНТУ.

3) Баришев Юрій Володимирович, доцент кафедри ЗІ, ВНТУ;

Оцінювання проведено за показниками, що наведені в Додатку. Результати оцінювання наведено в таблиці 4.1:

Таблиця 4.1 – Результати оцінювання науково-технічного рівня і комерційного потенціалу розробки

Критерії	Експерти		
	Войтович О.П.	Каплун В.А.	Баришев Ю.В.
	Бали		
1. Технічна здійсненність концепції;	4	4	4
2. Ринкові переваги (наявність аналогів);	4	3	2
3. Ринкові переваги (ціна продукту);	5	5	5
4. Ринкові переваги (технічні властивості);	4	3	3
5. Ринкові переваги (експлуатаційні витрати);	3	4	3
6. Ринкові перспективи (розмір ринку);	3	4	4
7. Ринкові перспективи (конкуренція);	4	3	4
8. Практична здійсненність (наявність фахівців);	5	4	4
9. Практична здійсненність (наявність фінансів);	5	5	5
10. Практична здійсненність (необхідність нових матеріалів);	4	4	5
11. Практична здійсненність (термін реалізації);	4	4	4
12. Практична здійсненність (розробка документів);	5	5	5
Сума балів:	50	46	48
Середньоарифметична сума балів:	48		

Середньоарифметична сума балів оцінюється за наступною формулою:

$$СБ_С = \frac{\sum_{i=1}^{3} СБ_i}{3} = \frac{50+46+48}{3} = 48 \quad (4.1)$$

де $СБ_С$ – середньоарифметична сума балів,

$СБ_i$ – сума балів і-го експерта.

За результатами оцінювання робиться висновок про науково-технічний рівень та комерційний потенціал розробки. Висновок ґрунтується на оцінках кожного рівня, що наведені в таблиці 4.2.

Таблиця 4.2 – Науково-технічні рівні та комерційні потенціали розробки

Середньоарифметична сума балів СБ, розрахована на основі висновків експертів	Науково-технічний рівень та комерційний потенціал розробки
41…48	Високий
31…40	Вищий середнього
21…30	Середній
11…20	Нижчий середнього
0…10	Низький

В результаті бачимо, що розробка має високий потенціал. З комерційної точки зору, така оцінка обумовлена набагато нижчою ціною розробки, порівняно з аналогами, малою кількістю аналогів на помірному ринку а також відносно швидким терміном реалізації. З точки зору ефективності практичного застосування, розробка має великий потенціал завдяки визначенні функціоналу відповідно до вимог підприємства. З точки зору технічної та практичної здійсненності, розробка має відносно високі експертні оцінки.

Проведемо також оцінку конкурентоспроможності розробки шляхом порівняння з аналогами. Для порівняння візьмемо стандартну процедуру аудиту інформаційної безпеки по стандарту ISO 27000. Оскільки параметри оцінювання не є жорсткими та не можуть бути виміряні кількісно, оцінка якісних показників проводиться на п’ятибальною шкалою. Оцінювання проведено головою департаменту Інформаційних Технологій Вінницької міської ради, Романенко Володимиром Борисовичем.

Для обчислення одиничних параметричних індексів застосовується формула, як показано на приклад оцінки індексу зміни значення параметра «Проведення аудиту»:

$$q_{\text{зд}} = \frac{P_{\text{баз зд}}}{P_{\text{зд}}} = \frac{4}{3} = 1{,}33 \qquad (4.2)$$

Результати порівняння науково-технічної розробки та аналогу на ринку наведено в таблиці 4.3:

Таблиця 4.3 – Оцінки якісних показників

Параметр	Одиниця виміру	Аналог	Нова розробка	Індекс зміни значення параметра	Коефіцієнт вагомості
Технічні					
Проведення аудиту	5-бальна шкала	3	4	1,33	0,4
Оцінка ризиків	5-бальна шкала	3	4	1,33	0,3
Формування звітності	5-бальна шкала	4	3	0,75	0,2
Рівень безпеки	5-бальна шкала	4	5	0,8	0,1
Економічні					
Ціна	грн	300000	400000	1,33	0,4
Вартість впровадження змін (рік)	грн	50000	50000	0,24	0,6

Для визначення групового параметричного індексу за технічними показниками конкурентоспроможності застосуємо наступну формулу:

$$I_{ТП} = \sum_{i=1}^{4} q_i * \alpha_i = 1.33 * 0.4 + 1{,}33 * 0.5 + 0{,}75 * 0.2 + 0{,}8 * 0.1 = 1.161 \quad (4.3)$$

Для визначення групового параметричного індексу за економічними показниками конкурентоспроможності застосуємо наступну формулу:

$$I_{ЕП} = \sum_{i=1}^{2} q_i * \beta_i = 1{,}33 * 0{,}4 + 0{,}24 * 0{,}6 = 0{,}676 \quad (4.4)$$

Інтегральний показник конкурентоспроможності обчислюється за формулою:

$$К_{ІНТ} = I_{НП} * \frac{I_{ТП}}{I_{ЕП}} = 1 * \frac{1.161}{0{,}676} = 1.717 \quad (4.5)$$

Отриманий інтегральний показник $К_{ІНТ} = 1.717$ свідчить про перспективність конкурентоспроможності даної розробки.

З огляду на оцінки експертів та оцінку конкурентоспроможності розробки, можна зробити висновок про високий науково-технічний рівень, комерційний потенціал та перспективу конкурентоспроможності. В такому випадку можна зробити висновок про потенційну користь від науково-технічної розробки.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Для обрахунку витрат на здійснення науково-дослідної роботи необхідно розглянути такі статті витрат:

- витрати на оплату праці
- відрахування на соціальні заходи
- програмне забезпечення для наукових та експериментальних робіт
- амортизація обладнання
- накладні (загальновиробничі) витрати

Перейдемо до обрахунку витрат на оплату праці.

4.2.1 Витрати на оплату праці

Витрати на оплату праці можна умовно поділити на 2 категорії. Це виплати дослідникам, що проводять науково-дослідну роботу, що є підґрунтям для

подальшої розробки програмного застосунку, що реалізує напрацьовану теорії. Витрати на заробітну плату дослідників розраховуються на основі формули:

$$З_{\text{р}} = \sum_{i=1}^{n} \frac{M_{ni} * t_i}{T_p} \quad (4.6)$$

де k – кількість посад дослідників, залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – кількість днів роботи конкретного дослідника, дн.;

T_p – середня кількість робочих днів в місяці, T_p=21…23 дні.

Розрахунки наведено в таблиці 4.3:

Таблиця 4.4 - Витрати на заробітну плату дослідників

Посада	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Кількість днів роботи	Витрати на заробітну плату, грн
Керівник проекту	25000	1136,36	4	4544
Провідний спеціаліст	19850	902,27	22	19850
Розробник	23000	1045,45	22	23000
Лаборант	10500	477,27	10	4772,7
Всього				52166,7

Для обчислення витрат на заробітну плату робітників необхідно врахувати наступні статті витрат:

- погодинну тарифну ставку за виконання роботи;
- час роботи робітника на виконання роботи

Для визначення погодинного тарифу необхідно використати наступну формулу:

$$С_{\text{і}} = \frac{М_{\text{м}} * К_{\text{і}} * К_{\text{с}}}{Т_{\text{р}} * t_{\text{зм}}} \quad (4.7)$$

де $М_{\text{м}}$ – розмір прожиткового мінімуму працездатної особи або мінімальної місячної заробітної плати (залежно від діючого законодавства), грн;

$К_{\text{і}}$ – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду (табл. Б.2, додаток Б);

$К_{\text{с}}$ – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих

об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати. (табл. Б.1, додаток Б)

$Т_р$ – середня кількість робочих днів в місяці, приблизно $Т_р$ = 21…23 дні, було вирішено взяти середнє значення 22 дні;

$t_{зм}$ – тривалість зміни, згідно стандартизованого робочого дня дорівнює 8 годин.

Проведемо розрахунок погодинної ставки. Для розрахунків візьмемо мінімальну заробітну плату $М_м = 8000{,}00$ грн. В результаті отримані погодинні тарифні ставки для кожного виду робіт наведено разом з розрахунками витрат в таблиці 4.4.

Таблиця 4.4 - Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна ставка, грн	Величина оплати на робітника, грн
Аналіз вимог	8	3	1,35	101,25	812
Аналіз стандартів	15	4	1,5	112,5	1687,5
Аналіз методик	12	4	1,5	112,5	1350
Розробка методики	25	5	1,7	127,5	3937,5
Всього:					7787

Після обчислення витрат на основну заробітну плату робітників необхідно також визначити величину витрат на додаткову заробітну плату дослідників та робітників, що складає 10 … 12% від суми витрат за основну заробітну плату дослідників та робітників. Візьмемо середнє значення 11%:

$$З_{дод} = (З_о + З_р) * \frac{н_{дод}}{100\%} = (52166{,}7 + 7787) * \frac{11}{100}\% = 6594{,}90 \qquad (4.8)$$

Таким чином, загальні витрати на оплату праці становлять 6594,90 грн.

4.2.2 Відрахування на соціальні заходи

Відрахування на соціальні заходи включає в себе відрахування внеску на загальнообов’язкове державне соціальне страхування та для здійснення заходів щодо соціального захисту населення. Цей внесок обраховується як 22% від суми основної та додаткової заробітної плати дослідників та робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) * \frac{н_{зп}}{100\%} = (52166{,}7 + 7787 + 6594{,}90) * \frac{22}{100}\% = 14640{,}6 \quad (4.9)$$

де $н_{зп}$ – норма нарахування на заробітну плату.

Таким чином, бачимо, що сума відрахувань на соціальні заходи становить 14640,6 грн.

4.2.3 Програмне забезпечення для науково-технічних робіт

До даної статті витрат належать витрати на розробку та/або придбання спеціального програмного забезпечення, що необхідно для проведення досліджень та розробку продукту, а також витрати на проектування, формування та встановлення. Витрати на інсталяцію зазвичай складають 10 … 12% від вартості програмного забезпечення.

Балансова вартість програмного забезпечення обчислюється за наступною формулою:

$$В_{прг} = \sum_{i=1}^{k} Ц_{iпрг} * С_{прг} * К_{i} \quad (4.10)$$

Де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу цього виду, грн;

$С_{прг}$– кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

$К_{i}$ – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, (К і = 1,10…1,12). Для обчислень візьмемо $К_{i} = 1.10$;

k – кількість найменувань програмних засобів.

Таким чином, результати обчислень наведені в таблиці 4.5:

Таблиця 4.5 – Вартість програмних застосунків

Найменування програмного засобу	Кількість, шт	Ціна за одиницю, грн	Коефіцієнт вартості інсталяції	Вартість з урахуванням інсталяції, грн
Microsoft 365 Professional	1	1 899	1,10	2088,9
Adobe Acrobat Pro	1	995	1,10	1094,5
Miro Starter	1	995	1,10	1094,5
Всього				4277,9

Таким чином, отримуємо вартість програмного забезпечення, що складає 4277,9 грн.

4.2.4 Амортизація обладнання, програмних засобів та приміщень

До статті «Амортизація обладнання, програмних засобів та приміщень» відносять амортизаційні відрахування по кожному виду обладнання, устаткування та інших приладів і пристроїв, а також програмного забезпечення для проведення науково-дослідної роботи, за його наявності в дослідній організації або на підприємстві. В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо можуть бути розраховані з використанням прямолінійного методу амортизації за формулою:

$$А_{обл} = \frac{Ц_б}{Т_в} * \frac{t_{вик}}{12} \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$Т_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

Проведені розрахунки наведено в таблиці 4.6:

Таблиця 4.6 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання, місяців	Амортизаційні відрахування
Ноутбук Acer	18000	2	1	750
Принтер Canon	6000	2	1	250
Всього				1000

Таким чином, отримуємо вартість амортизації обладнання, яка складає 1000 грн.

4.2.5 Сировина та матеріали

Майже всі процеси відбуваються електронно, але є деяка необхідність у папері для записів, моделювання та друку.

Витрати на матеріали (*M*), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

де Нj – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

Цj – вартість матеріалу j-го найменування, грн/кг;

Кj – коефіцієнт транспортних витрат, (Кj = 1,1 … 1,15);

Вj – маса відходів j-го найменування, кг;

Цвj – вартість відходів j-го найменування, грн/кг.

$$М1 = 2{,}0 \cdot 172{,}00 \cdot 1{,}1 = 378{,}4 \text{ грн.}$$

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг,шт/грн	Норма витрат, кг,шт	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (500шт)(А4)	172,00	2,0	378,4
Блокнот (А5)	150,00	1,0	165
Ручка	25,00	2,0	55
Картридж для принтера	800,00	1,0	880,00
Всього			1478,5

4.2.6 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (*Ве*) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{M_{yi} \cdot t_i \cdot Ц_е \cdot К_{впі}}{\eta_i}$$

де W_{yi}– встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

Це – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), $Ц_е$ = 10,5 грн;

$К_{впі}$ – коефіцієнт, що враховує використання потужності, $К_{впі} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

Таблиця 4.10 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук Acer	0,045	30	10,17
Принтер Canon	0,2	10	21
Всього			21,17

4.2.7 Накладні (загальновиробничі) витрати

Накладні витрати розраховуються виходячи з основної заробітної плати дослідників та робітників, становлячи 100 … 150% від суми цих витрат. Сюди входять витрати, пов'язані з управлінням організацією, витрати на винахідництво та раціоналізацію, витрати на підготовку (перепідготовку) та навчання кадрів, витрати, пов'язані з набором робочої сили, витрати на оплату послуг банків, витрати, пов'язані з освоєнням виробництва продукції, витрати на науково-технічну інформацію та рекламу та ін.

Ці витрати обчислюються за формулою:

$$В_{нзв} = (З_0 + З_р) * \frac{Н_{нзв}}{100\%} = (52166{,}7 + 7787) * \frac{125}{100\%} = 74942{,}12 \quad (4.12)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати».

Якщо припустити, що накладні витрати становлять середнє значення діапазону, тобто 125%, в результаті обчислень отримаємо 74942,12 грн.

Загальні витрати на проведення науково-технічної роботи розраховуються як сума всіх попередніх статей витрат. Таким чином, використавши значення, отримані при попередніх розрахунках, можемо визначити, що загальні витрати на проведення науково-технічної роботи становлять 167575,36 грн, як зазначено в формулі:

$$В_{нзв} = З_0 + З_р + З_{дод} + B_e + З_н + В_{прг} + А_{обл} + М + B_e + В_{нзв} = 52166{,}7 + 7787 + 6594{,}90 + 21{,}17$$

$$+14640{,}6 + 4277{,}9 + 1000 + 14{,}28 + 1478{,}5 + 79594{,}31 = 167575{,}36 \quad (4.13)$$

Для визначення кінцевої вартості завершення науково-технічної роботи необхідно визначити етап виконання науково-технічної роботи. Дана науково-технічна розробка знаходиться на останніх етапах стадії розробки промислового зразка, тому буде застосовано коефіцієнт η=0,9. Таким чином, застосовуючи формулу отримуємо:

$$ЗВ = \frac{В_{заг}}{\eta} = 167575{,}36/0{,}9 = 186194{,}84 \quad (4.14)$$

4.3 Розрахунок економічної ефективності науково-технічної розробки

Дана розробка може бути виведена на ринок для подальшої реалізації. Для оцінки економічної ефективності даної науково-технічної розробки необхідно врахувати такі показники як час впровадження розробки, очікуваний час отримання позитивних результатів для інвестора, величина попиту та суб'єкти цього попиту, ціна реалізації на ринку розробок з аналогічними функціями.

Для прикладу наведемо обчислення прибутку інвестора в першому році після реалізації:

$$\Delta П_1 = (\pm \Delta Ц_0 * N + Ц_0 * \Delta N)_i * \lambda * \rho * \left(1 - \frac{\vartheta}{100}\right) = (400000 * 6 + 300000 * 0) * 0{,}8333 * 0{,}35 * (1 - 0{,}18) = 573976{,}04 \quad (4.15)$$

$$\Delta П_2 = (\pm \Delta Ц_0 * N + Ц_0 * \Delta N)_i * \lambda * \rho * \left(1 - \frac{\vartheta}{100}\right) = (400000 * 6 + 400000 * 6) * 0{,}8333 * 0{,}35 * (1 - 0{,}18) = 1147954{,}08 \quad (4.16)$$

$$\Delta П_3 = (\pm \Delta Ц_0 * N + Ц_0 * \Delta N)_i * \lambda * \rho * \left(1 - \frac{\vartheta}{100}\right) = (400000 * 6 + 400000 * 12) * 0{,}8333 * 0{,}35 * (1 - 0{,}18) = 1721931{,}12 \quad (4.17)$$

$$\Delta П_4 = (\pm \Delta Ц_0 * N + Ц_0 * \Delta N)_i * \lambda * \rho * \left(1 - \frac{\vartheta}{100}\right) = (400000 * 6 + 400000 * 18) * 0{,}8333 * 0{,}35 * (1 - 0{,}18) = 2297908{,}16 \quad (4.18)$$

Далі необхідно розрахувати приведену вартість всіх чистих прибутків ПП за формулою:

$$ПП = \sum_{i=1}^{T} \frac{\Delta П_i}{(1+\tau)^t} = \frac{573976{,}04}{1{,}15^1} + \frac{1147954{,}08}{1{,}15^2} + \frac{1721931{,}12}{1{,}15^3} + \frac{2297908{,}16}{1{,}15^4} =$$

$$= 499113{,}08 + 949546{,}35 + 1132414{,}87 + 1313583{,}74 = 3894658{,}04 \quad (4.19)$$

Необхідно розрахувати також початкові інвестиції PV. Обчислення проводиться за формулою:

$$PV = k_{розр} * ЗВ = 4 * 186194{,}84 = 744779{,}37 \quad (4.20)$$

Також необхідно обчислити приведений дохід за формулою:

$$E_{\text{абс}} = \text{ПП} - PV = 3894658{,}04 \ - 744779{,}37 \ = \ 3149878{,}67 \quad (4.21)$$

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність $E_{\text{в}}$ або показник внутрішньої норми дохідності (IRR, Internal Rate of Return) вкладених інвестицій за формулою:

$$E_{\text{в}} = \sqrt[\text{Тж}]{1 + \frac{\text{E}_{\text{абс}}}{PV}} - 1 = \sqrt[4]{1 + \frac{3149878{,}67}{744779{,}37}} - 1 = 0.512 \quad (4.22)$$

Для визначення бар'єрної ставки, з якою необхідно порівняти внутрішню економічну дохідність, використовується формула:

$$\tau_{\text{мін}} = d + f = 0.15 + 0.3 = 0.45 \quad (4.23)$$

Оскільки внутрішня економічна дохідність перевищує мінімальну, потенційний інвестор можу бути зацікавлений в даній розробці.

Також обчислимо період окупності інвестицій за формулою:

$$\text{T}_{\text{ок}} = \frac{1}{E_{\text{в}}} = \frac{1}{0{,}512} = 1{,}95 \quad (4.24)$$

Оскільки $\text{T}_{\text{ок}} < 3$ років, можна зробити висновок, що впровадження науково-технічної розробки є економічно ефективним.

Висновки до розділу

Отже, після повного дослідження економічної ефективності було проведено оцінювання науково-технічного рівня і комерційного потенціалу розробки трьома експертами за визначеними критеріями. Результат розрахунку середнього балу становить 48, що означає, науково технічний рівень та комерційний потенціал розробки є високим. Також було проведено аналіз рівня конкурентоспроможності розробки, який дозволив роз'яснити переваги відповідних технічних показників та економічних характеристик. Проведений аналіз показав, що розробка є конкурентоспроможною та її можна виводити на ринок. Проведено розрахунок витрат на здійснення науково-дослідної роботи та розрахунок економічної ефективності науково-технічної розробки від її впровадження на підприємстві. Проведені розрахунки показали, що впровадження розробки є економічно ефективним.

ВИСНОВКИ

У комплексній магістерській кваліфікаційній роботі було створено методику комплексного аудиту інформаційної безпеки підрозділів Вінницької міської ради (ВМР).

Для цього сформульовано завдання щодо проведення аудиту інформаційної безпеки міської ради та здійснено огляд основних міжнародних і національних стандартів, серед яких ISO 27001, NIST, PCI DSS, GDPR, COBIT і КСЗІ. Хоча кожен із цих стандартів має свої особливості та застосування, для місцевих органів самоврядування, зокрема міської ради, було визначено три найбільш доцільні підходи: ISO 27001, NIST і КСЗІ. ISO 27001 обрано завдяки його гнучкості та міжнародному визнанню як стандарту, що забезпечує систематичний підхід до управління інформаційною безпекою через побудову й впровадження системи управління інформаційною безпекою (ISMS). Цей стандарт критично важливий для організацій, оскільки сприяє ефективному управлінню ризиками та постійному вдосконаленню процесів безпеки. NIST обрано через його орієнтацію на практичні методи забезпечення кібербезпеки, зокрема завдяки моделі, яка включає ідентифікацію, захист, виявлення, реагування та відновлення. Цей підхід допомагає розробити конкретні стратегії для протидії кіберзагрозам, що є актуальним для міської ради через постійні кіберзагрози. КСЗІ містить вимоги щодо захисту державної інформації та критичної інфраструктури, що є особливо важливим для місцевих органів влади, які працюють з даними громадян, бюджетними коштами та адміністративною інформацією.

Проведено аналіз структури ВМР та завдань різних департаментів. У кожному департаменті виконано інформаційний аудит, на основі якого зроблено відповідні висновки. Найпоширенішими платформами є SharePoint для управління документами та співпраці; система документообігу для офіційних документів; Azure для забезпечення функціонування сайту міської ради; Outlook для комунікації; CKAN (opendata.gov.ua) для роботи з відкритими даними, що є

важливим для департаментів, які працюють із публічною інформацією. Серед основних сервісів виділено роботу з наборами відкритих даних, управління документами, обробку звернень громадян (особливо в департаментах охорони здоров'я та освіти), а також внутрішню комунікацію через Skype for Business, Viber та Outlook, що підкреслює значення зв'язку як всередині департаментів, так і з громадськістю.

Розроблено методику аудиту на основі стандартів ISO 27000 для підрозділів ВМР. З урахуванням проведеного аналізу в першому розділі до методики було додано NIST Cybersecurity Framework 2.0 і нормативні документи КСЗІ. Розроблена методика враховує сучасні міжнародні підходи до аудиту інформаційної безпеки, оцінки ризиків і державних вимог. Комплексний аудит, що поєднує кращі аспекти кожного стандарту, спрямований на досягнення найкращих результатів. Тривалість комплексного аудиту за розробленою методикою становить від 50 до 80 днів.

На завершальному етапі роботи оцінено науково-технічний рівень і комерційний потенціал розробки. Отримано високі показники науково-технічного рівня, що свідчить про потенційну корисність розробки. Комерційний потенціал демонструє можливість окупності проєкту менш ніж за три роки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Войтович О. П., Пилявець І. Ю., Радченко Є. В. Використання штучного інтелекту в аудиті інформаційної безпеки. м. Вінниця. ВНТУ, 2025. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2025/paper/viewFile/22704/18743. (дата звернення: 13.12.2024)

2. Майданевич Л., Пилявець І., Радченко Є. Використання спеціальних технічних засобів отримання інформації: сутність та особливості унормування. м. Вінниця. ВНТУ, 2024. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2024/paper/viewFile/21640/17886 (дата звернення: 13.12.2024)

3. Радченко Є.В., Пилявець І.Ю. АКТУАЛЬНІСТЬ ВИКОРИСТАННЯ ЛОКАЛЬНИХ ІНСТРУМЕНТІВ ПІДТРИМКИ АУДИТУ/ Наук. керівник О.П. Войтович. Вінниця, ВНТУ 2024р

4. ISO/IEC 27001:2022. ISO. URL: https://www.iso.org/standard/27001(date of access: 07.11.2024).

5. ISO/IEC 27002:2022. ISO. URL:https://www.iso.org/standard/75652.html(дата звернення: 13.12.2024).

6. ISO/IEC 27005:2022. ISO. URL: https://www.iso.org/standard/80585.html (дата звернення: 13.12.2024).

7. ISO 19011:2018. ISO. URL: https://www.iso.org/standard/70017.html (дата звернення: 13.12.2024).

8. ISO/IEC 27007:2020. ISO. URL: https://www.iso.org/standard/77802.html (дата звернення: 13.12.2024).

9. ISO/IEC 27001:2022. ISO. URL: https://www.iso.org/standard/27001 (дата звернення: 13.12.2024).

10. ISO/IEC 17021-1:2015. ISO. URL: https://www.iso.org/standard/61651.html (дата звернення: 13.12.2024).

11. ISO 31000:2018. ISO. URL: https://www.iso.org/standard/65694.html (дата звернення: 13.12.2024).

12. NIST G. M. NIST Cybersecurity Framework 2.0:. Gaithersburg, MD : National Institute of Standards and Technology, 2024. URL: https://doi.org/10.6028/nist.sp.1301 (дата звернення: 05.11.2024).

13. Securing the Future of Payments: PCI SSC Publishes PCI Data Security Standard v4.0. *PCI Security Standards Council*. URL: https://www.pcisecuritystandards.org/about_us/press_releases/securing-the-future-of-payments-pci-ssc-publishes-pci-data-security-standard-v4-0/ (date of access: 07.11.2024).

14. General Data Protection Regulation (GDPR) – Legal Text. General Data Protection Regulation (GDPR). URL: https://gdpr-info.eu/ (date of access: 07.11.2024).

15. COBIT | Control Objectives for Information Technologies | ISACA. ISACA. URL: https://www.isaca.org/resources/cobit (date of access: 08.11.2024).

16. Поради (рекомендації) щодо створення КСЗІ в ІКС, які використовуються для надання послуг доступу до мережі Інтернет. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/poradi-rekomendaciyi-shodo-stvorennya-kszi-v-its-yaki-vikoristovuyutsya-dlya-nadannya-poslug-dostupu-do-merezhi-internet (дата звернення: 08.11.2024).

17. Про захист інформації в інформаційно-комунікаційних системах. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 08.11.2024).

18. ДСТУ ISO/IEC 27001:2023. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT). На заміну ДСТУ ISO/IEC 27001:2015 ; чинний від 2023-08-22. Вид. офіц. 2023.

19. Про розподіл обов’язків між міським головою, секретарем міської ради, заступниками міського голови, керуючим справами виконавчого комітету. Вінницька міська рада. URL: https://www.vmr.gov.ua/media/Виконавчі%20органи/Головна%20сторінка/Розпорядження%2028-10-2024%20№142р.pdf (дата звернення: 08.11.2024).

20. Департамент правової політики та якості. Вінницька міська рада. URL: https://www.vmr.gov.ua/departament-pravovoi-polityky-ta-iakosti (дата звернення: 08.11.2024).

21. Департамент культури. Вінницька міська рада. URL: https://www.vmr.gov.ua/departament-kultury (дата звернення: 08.11.2024).

22. Департамент охорони здоров'я. Вінницька міська рада. URL: https://www.vmr.gov.ua/departament-okhorony-zdorovia (дата звернення: 08.11.2024).

23. Архівний відділ. Вінницька міська рада. URL: https://www.vmr.gov.ua/arkhivnyi-viddil (дата звернення: 08.11.2024).

24. Департамент освіти. Вінницька міська рада. URL: https://www.vmr.gov.ua/departament-osvity (дата звернення: 08.11.2024).

25. Комітет по фізичній культурі і спорту. Вінницька міська рада. URL: https://www.vmr.gov.ua/komitet-po-fizychnii-kulturi-ta-sportu (дата звернення: 08.11.2024).

26. Департамент інформаційних технологій. Вінницька міська рада. URL: https://www.vmr.gov.ua/departament-informatsiinykh-tekhnolohii (дата звернення: 08.11.2024).

27. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу. ТЗІ - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/nd-tz-2.5-004-99.html (дата звернення: 13.12.2024).

28. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. ТЗІ - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/nd-tz-2.1-002-07.html (дата звернення: 13.12.2024).

29. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення. ТЗІ - інформаційна безпека та захист інформації. URL: https://tzi.com.ua/nd-tz-2.1-002-07.html (дата звернення: 13.12.2024).

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ НАВЧАЛЬНОЇ (КВАЛІФІКАЦІЙНОЇ) РОБОТИ

Назва роботи: Аудит інформаційної безпеки департаментів Вінницької міської ради. Частина 1. Методика проведення аудиту

Автор роботи: Пилявець Ігор Юрійович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ

Керівник Войтович Олеся Петрівна, к.т.н., доцент

Показники звіту подібності

Turnitin	
Оригінальність	96 %
Загальна схожість	4 %

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її автора. Роботу направити на доопрацювання.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Заявляю, що ознайомлений з повним звітом подібності, який був згенерований Системою щодо роботи.

Автор роботи _____ (підпис) Ігор ПИЛЯВЕЦЬ (прізвище, ініціали)

Особа, відповідальна за перевірку _____ (підпис) Валентина КАПЛУН (прізвище, ініціали)

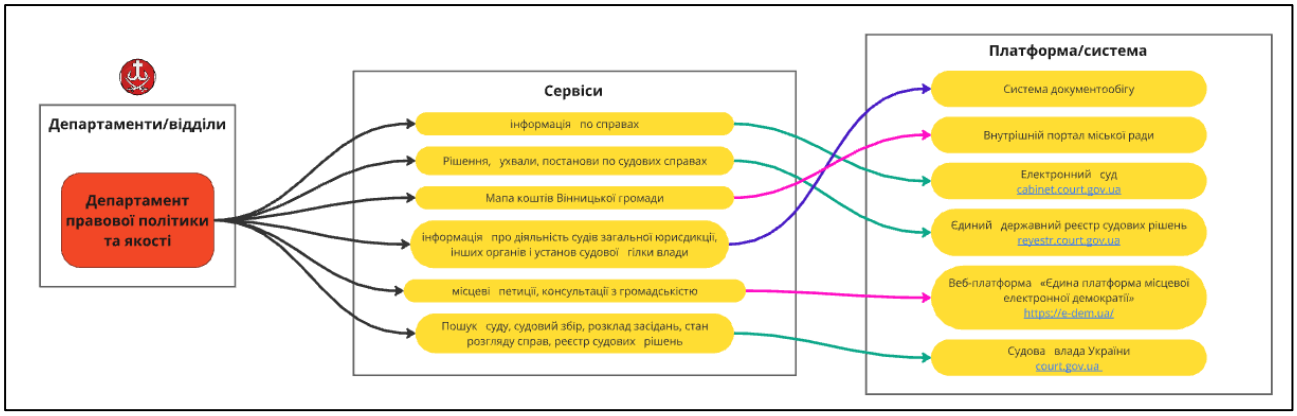
Керівник роботи _____ (підпис) Олеся ВОЙТОВИЧ (прізвище, ініціали)

ІЛЮСТРАТИВНА ЧАСТИНА

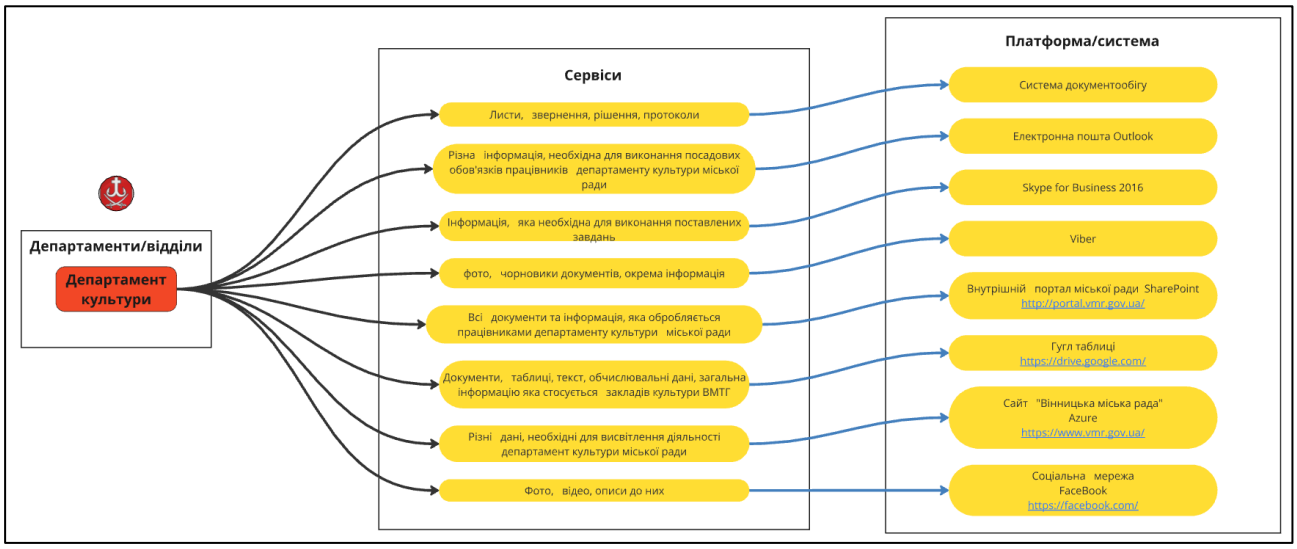
АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕПАРТАМЕНТІВ ВІННИЦЬКОЇ МІСЬКОЇ РАДИ.
ЧАСТИНА 1. МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ

Виконав: студент групи 1БС-23м
спеціальності 125 Кібербезпека
та захист інформації
_____ Ігор ПИЛЯВЕЦЬ
13.12 2024 р.
Керівник: к. т. н., доцент каф. ЗІ
_____ Олеся ВОЙТОВИЧ
13.12 2024 р.

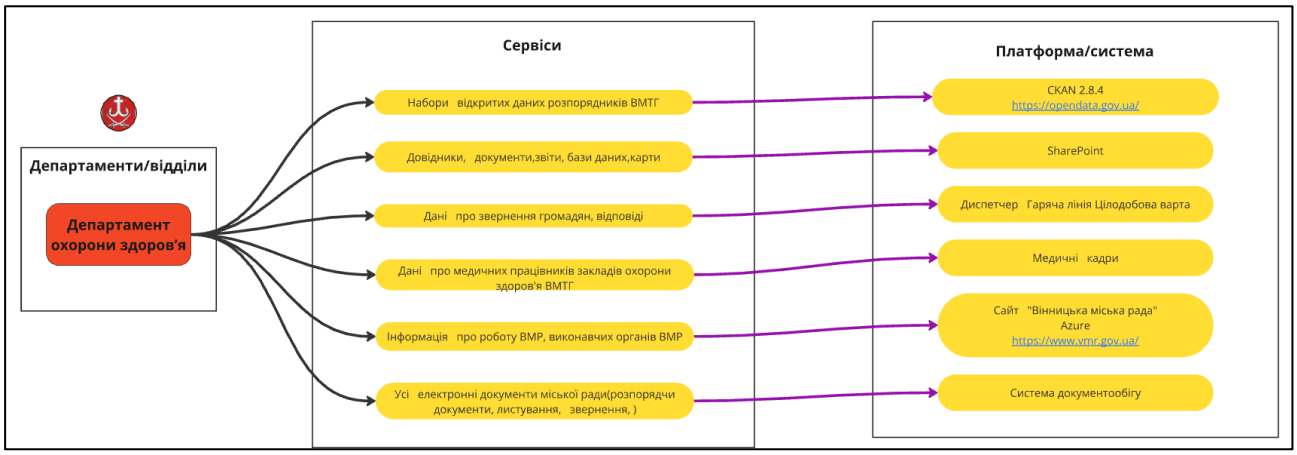
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТ ПРАВОВОЇ ПОЛІТИКИ ТА ЯКОСТІ МІСЬКОЇ РАДИ



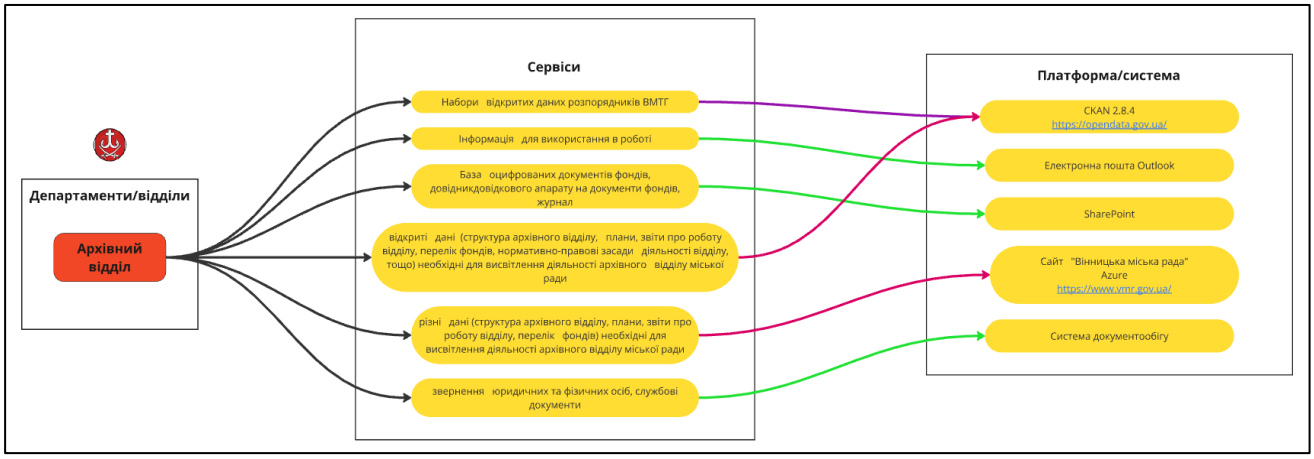
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТУ КУЛЬТУРИ



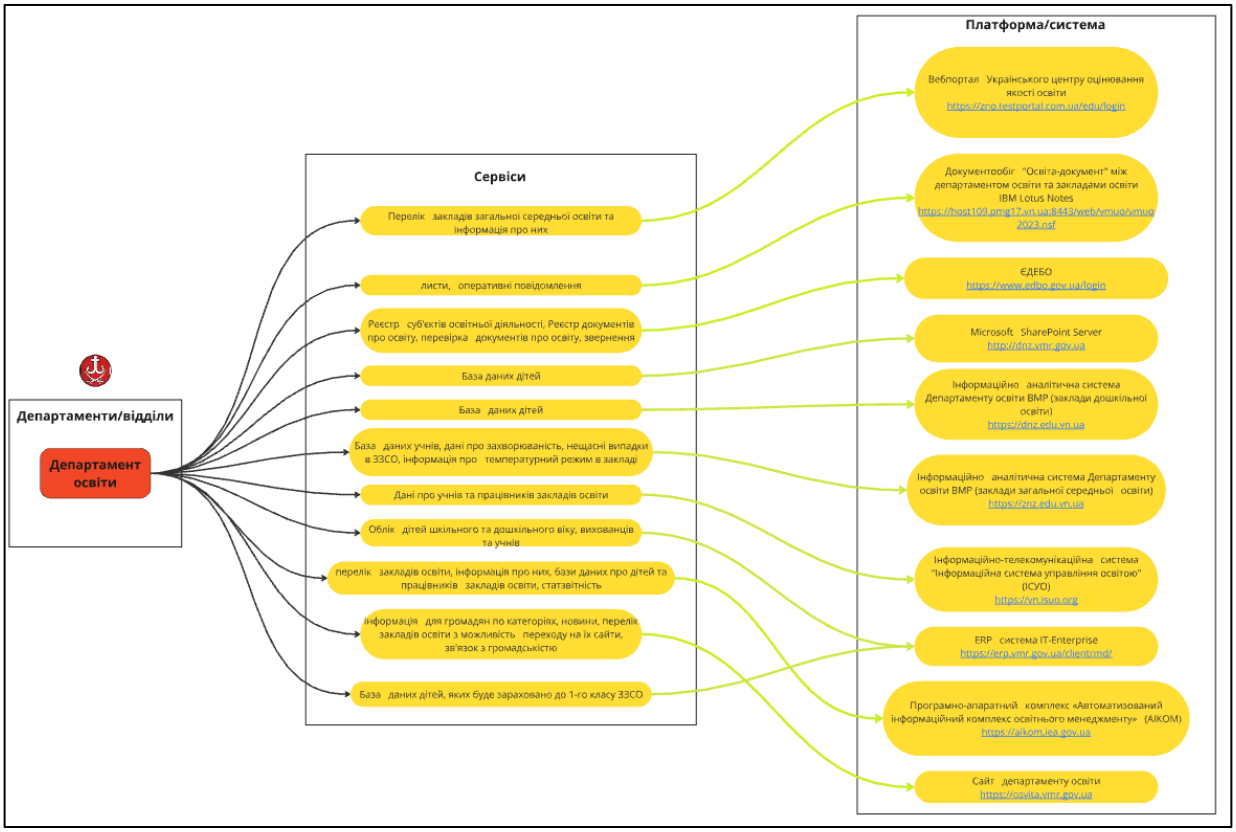
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТ ОХОРОНИ ЗДОРОВ’Я



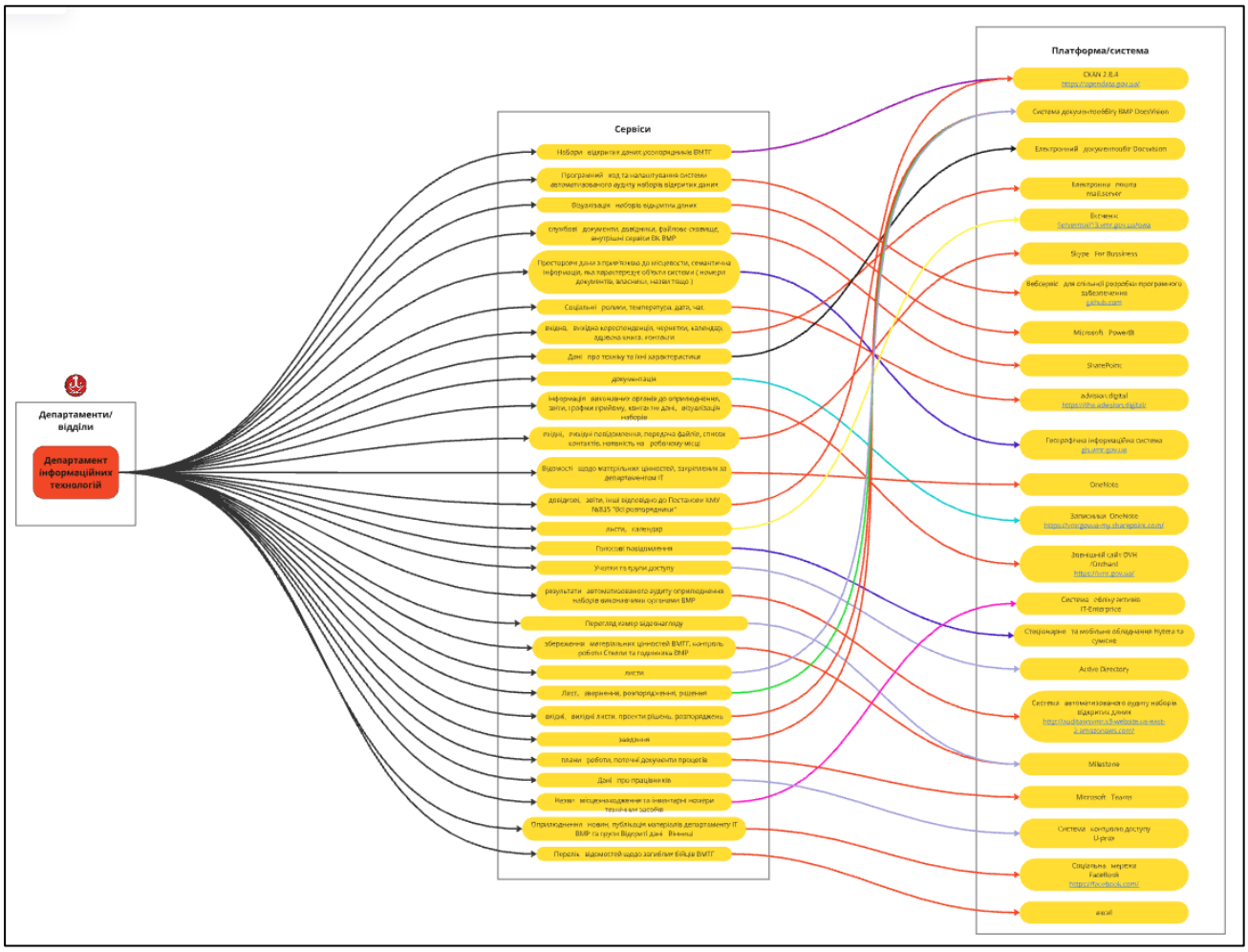
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ АРХІВНОГО ВІДДІЛУ



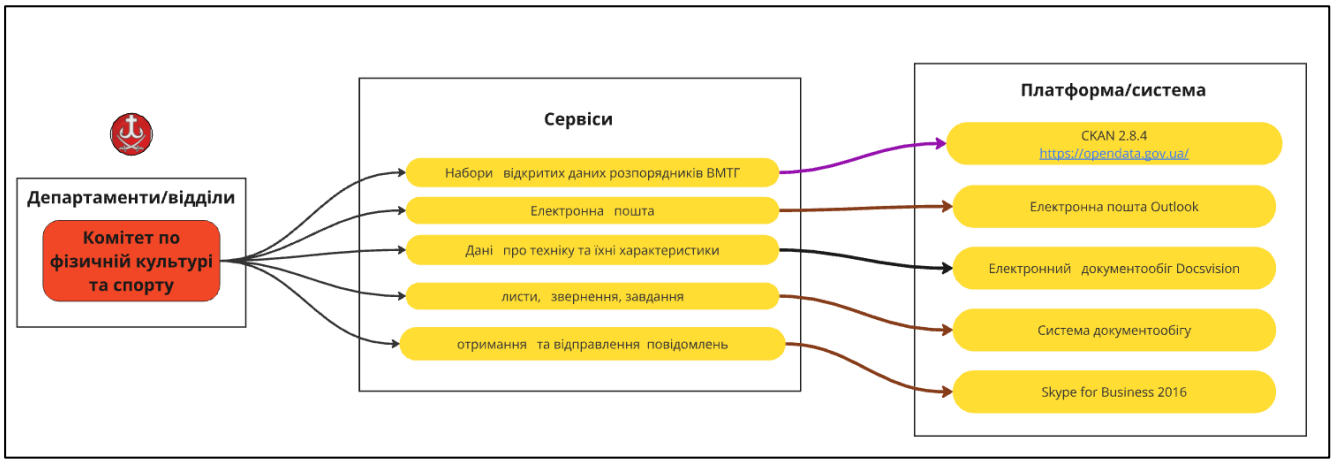
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТУ ОСВІТИ



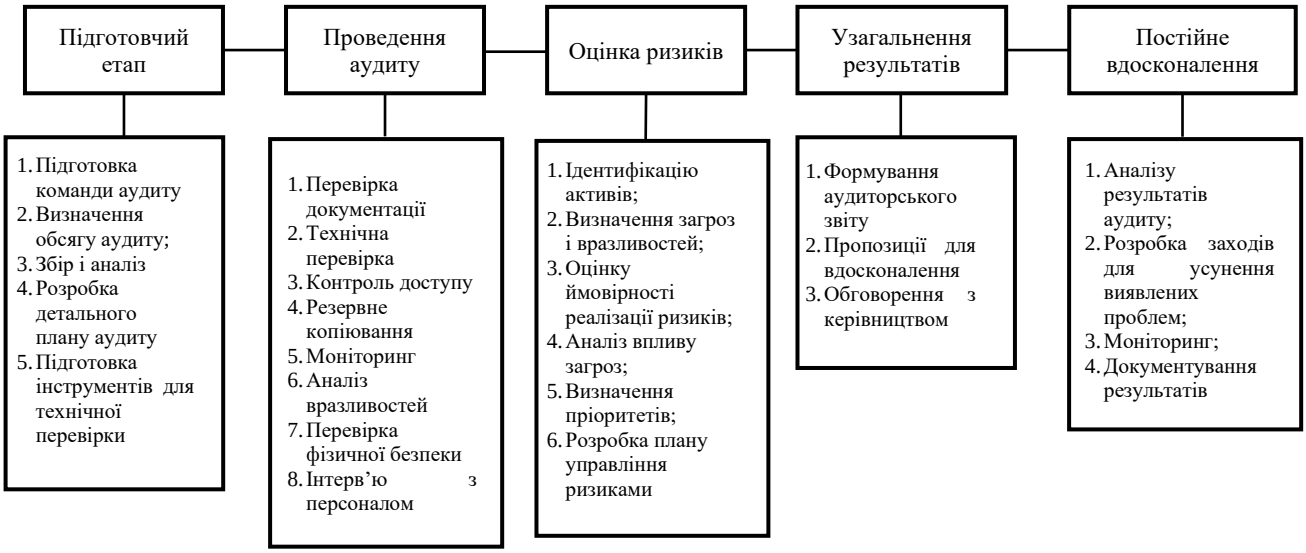
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ



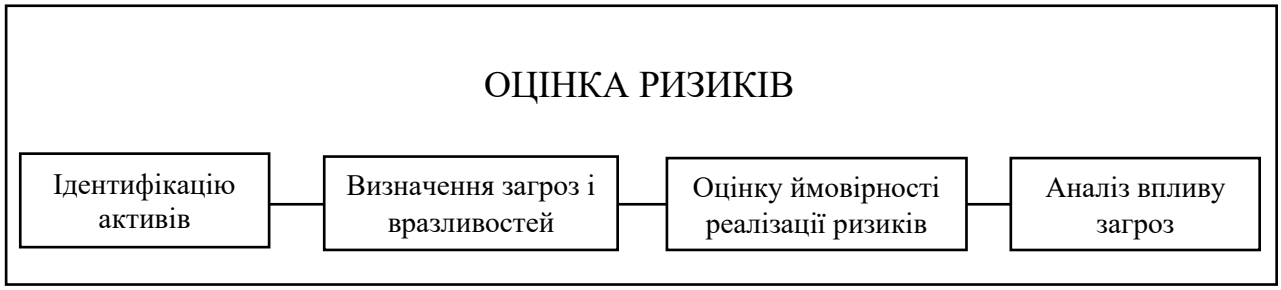
РЕЗУЛЬТАТ ІНФОРМАЦІЙНОГО АУДИТУ ДЕПАРТАМЕНТУ ФІЗИЧНОЇ КУЛЬТУРИ ТА СПОРТУ



ПОСЛІДОВНІСТЬ ДІЙ ПРИ АУДИТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА СТАНДАРТАМИ ISO 27000



ЕТАПИ ПРОЦЕСУ ПОСТІЙНОГО ВДОСКОНАЛЕННЯ



СПІВСТАВЛЕННЯ ВИМОГ ISO 27001 ТА НДТЗІ 2.5-004-99

Аспект	ISO 27001	НДТЗІ 2.5-004-99
Призначення	Стандарт для побудови системи управління інформаційною безпекою (СУІБ).	Вимоги до побудови систем захисту інформації в Україні.
Схожість	Обидва визначають вимоги до впровадження систем захисту інформації.	Спільний акцент на політиках безпеки та управлінні ризиками.
Відмінності	Глобальний підхід, більше уваги до менеджменту.	Фокус на технічних заходах і локальних вимогах.
Сфера застосування	Управління ризиками, політики захисту, сертифікація.	Реалізація державних вимог до інформаційної безпеки.

СПІВСТАВЛЕННЯ ВИМОГ ISO 27002 ТА НДТЗІ 2.1-002-07

Аспект	ISO 27002	НДТЗІ 2.1-002-07
Призначення	Рекомендації щодо впровадження заходів інформаційної безпеки.	Загальні вимоги до захисту інформації в автоматизованих системах.
Схожість	Обидва описують технічні та організаційні заходи безпеки.	Спільний акцент на контролі доступу, моніторингу.
Відмінності	Гнучкі рекомендації, застосовні до різних організацій.	Жорсткі локальні вимоги до державних систем.

СПІВСТАВЛЕННЯ ВИМОГ НДТЗІ 2.1-002-07, НДТЗ 2.6-001-11 З ISO 27006 ТА 27007

Аспект	НДТЗІ 2.1-002-07	ISO 27006	НДТЗІ 2.6-001-11	ISO 27007
Призначення	Захист інформації в автоматизованих системах	Сертифікація органів із СУІБ	Аудит систем технічного захисту інформації	Рекомендації для аудиту СУІБ
Масштаб	Локальний, Україна	Глобальний	Локальний, Україна	Глобальний
Цільова аудиторія	Держустанови, критична інфраструктура	Органи сертифікації	Організації, що проводять аудити	Аудитори СУІБ
Фокус	Вимоги до захисту інформації	Вимоги до сертифікації	Оцінка ефективності захисту	Організація, планування і звітність аудиту
Ризик-орієнтований підхід	Присутній	Присутній	Присутній	Присутній
Деталізація аудиту	Загальні вимоги	Чіткі вимоги до органів сертифікації	Загальні положення	Детальні рекомендації
Юридична основа	Відповідність законодавству України	Незалежний від юрисдикції	Відповідність законодавству України	Незалежний від юрисдикції
Адаптивність	Фіксовані вимоги	Гнучкий, адаптується до різних органів	Фіксовані вимоги	Гнучкий, адаптується до будь-якої організації
Ціль сертифікації	Сертифікація автоматизованих систем	Сертифікація органів із СУІБ	Перевірка відповідності систем захисту	Підтвердження якості управління СУІБ
Методологія аудиту	Загальна, без чітких методик	Конкретна для оцінки органів сертифікації	Загальна	Чітко структурована, включає рекомендації
Універсальність застосування	Вузьке, обмежене національними вимогами	Широке, для будь-якої організації	Локалізоване на український контекст	Глобальне, враховує різні юрисдикції
Роль аудиторів	Встановлює основні вимоги	Встановлює кваліфікацію для сертифікаційних органів	Регламентує базові обов’язки аудиторів	Описує вимоги до компетентності та поведінки аудиторів
Інтеграція з іншими стандартами	Інтегрується з іншими НДТЗІ	Враховує ISO 17021 (вимоги до сертифікацій)	Інтегрується з НДТЗІ	Сумісний з ISO 27001, 19011
Періодичність аудиту	Регламентується національними нормативами	Залежить від органів сертифікації	Визначено локальними нормами	Рекомендована регулярність

ДЕПАРТАМЕНТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ВІННИЦЬКОЇ МІСЬКОЇ РАДИ

АКТ
ВПРОВАДЖЕННЯ

Цим актом підтверджується, що результати магістерської кваліфікаційної роботи на тему «Аудит інформаційної безпеки департаментів Вінницької міської ради. Частина 1. Методика проведення аудиту», яку виконано Пилявцем Ігорем Юрійовичем за спеціальністю 125 «Кібербезпека та захист інформації» (Освітня програма «Безпека інформаційних і комунікаційних систем»), що виконувалася з 2 вересня 2024 р. по 9 листопада 2024 р., впроваджені у Департаменті інформаційних технологій Вінницької міської ради.

Цей документ не є підставою для фінансових розрахунків.

Директор департаменту
інформаційних технологій
Вінницької міської ради

Володимир РОМАНЕНКО