Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(освітній рівень)

на тему: "Впровадження системи управління інформаційною безпекою державної установи на основі результатів оцінки CSET "

Виконав: студент VI курсу, групи СБм-61

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Містерман Іван Михайлович
підпис (прізвище та ініціали)

Керівник Деркач М.В.
підпис (прізвище та ініціали)

Нормоконтроль Стадник М. А.
підпис (прізвище та ініціали)

Завідувач кафедри Загородна Н.В.
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Містерману Івану Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Впровадження системи управління інформаційною безпекою державної установи на основі результатів оцінки CSET

Керівник роботи Деркач Марина Володимирівна, кандидат технічних наук, доцент, викладач кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024

2. Термін подання студентом завершеної роботи 12.12.2025

3. Вихідні дані до роботи Результати оцінювання рівня кібербезпеки інформаційної інфраструктури державної установи, отримані за допомогою інструменту Cybersecurity Evaluation Tool (CSET).

4. Зміст роботи (перелік питань, які потрібно розробити)
Проаналізувати нормативно-правові та стандартні засади інформаційної безпеки.
Оцінити поточний стан кіберзахисту державної установи за допомогою CSET.
Розробити концептуальну модель і модуль системи управління інформаційною безпекою/
Обґрунтувати та апробувати практичні технічні й організаційні заходи з підвищення рівня кіберстійкості.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Мета: розроблення та практичне обґрунтування модуля системи управління інформаційною безпекою. Актуальність теми. Об'єкт та предмет дослідження. Методологія. Аналіз стану кібербезпеки державної установи. Мережева топологія CSET. Практичне впровадження: AdGuard Home. Практичне впровадження OpenVPN. Повторне оцінювання стану кібербезпеки державної установи. Висновки.

Висновки. У роботі розроблено та обґрунтовано впровадження ISMS державної установи на основі результатів оцінювання CSET. Отримані результати можуть бути використані як практичне підґрунтя для подальшого розвитку кібербезпеки державних установ.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Теслюк В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 22.09	Виконано
2.	Підбір джерел для впровадження системи управління інформаційною безпекою в державній установі	23.09 – 30.09	Виконано
3.	Опрацювання джерел в галузі дослідження	01.10 – 16.10	Виконано
4.	Оформлення розділу «Аналіз сучасного стану інформаційної безпеки в державних установах»	17.10 – 22.10	Виконано
5.	Проведення оцінки кібербезпеки за допомогою CSET	23.10 – 31.10	Виконано
6.	Оформлення розділу «Аналіз стану кібербезпеки державної установи»	01.11 – 03.11	Виконано
7.	Розробка модулю ISMS з урахуванням результатів CSET	04.11 – 10.11	Виконано
8.	Проведення повторної оцінки кібербезпеки за допомогою CSET	11.11 – 15.11	Виконано
9.	Оформлення розділу «Проєктування системи управління інформаційною безпекою (ISMS)»	16.11 – 21.11	Виконано
10.	Виконання завдання до розділу «Охорона праці та безпека в надзвичайних ситуаціях»	22.11 – 29.11	Виконано
11.	Оформлення кваліфікаційної роботи	30.11 – 07.12	Виконано
12.	Нормоконтроль	08.12 – 10.12	Виконано
13.	Перевірка на плагіат	12.12 – 14.12	Виконано
14.	Попередній захист кваліфікаційної роботи	15.12 – 20.12	Виконано
15.	Захист кваліфікаційної роботи	23.12.2025	

Студент _____ Містерман І.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Впровадження системи управління інформаційною безпекою державної установи на основі результатів оцінки CSET // Кваліфікаційна робота ОР «Магістр» // Містерман Іван Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // С. 83, рис. – 19, табл. – 3, кресл. – 0, додат. – 0.

Ключові слова: кіберінцидент, державна установа, система управління інформаційною безпекою, ISMS; CSET.

Магістерська кваліфікаційна робота присвячена дослідженню підходів до впровадження системи управління інформаційною безпекою в державній установі на основі результатів оцінювання, виконаного за допомогою інструменту CSET. Актуальність роботи зумовлена зростаючою кількістю кіберінцидентів, що спрямовані на інформаційні ресурси державного сектору, а також необхідністю приведення внутрішніх процесів безпеки у відповідність до сучасних міжнародних стандартів та національних регуляторних вимог. Формування ефективної системи управління інформаційною безпекою є одним із ключових чинників забезпечення стабільності функціонування державних установ та підвищення рівня їх кіберстійкості.

ABSTRACT

Implementation of an information security management system for a state institution based on the results of a CSET assessment // Thesis of educational level "Master"// Ivan Misterman // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБм-61 // Ternopil, 2025 // p. 83, figs. 19, tbls. 3, drws. 0, apps. 0.

Keywords: cyber incident, government agency, information security management system, ISMS; CSET.

The master's thesis is devoted to researching approaches to implementing an information security management system in a government agency based on the results of an assessment performed using the CSET tool. The relevance of the work is due to the growing number of cyber incidents targeting public sector information resources, as well as the need to bring internal security processes into line with current international standards and national regulatory requirements. The formation of an effective information security management system is one of the key factors in ensuring the stability of public institutions and increasing their cyber resilience.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CSET	–	інструмент оцінювання кібербезпеки
IT	–	інформаційні технології
CIS Controls	–	набір пріоритетних заходів кіберзахисту, розроблений Center for Internet Security
Актив	–	ресурс, що має цінність для організації (дані, обладнання, ПЗ, сервіси)
Загроза	–	потенційна подія, що може завдати шкоди активам
ISMS	–	система управління інформаційною безпекою
Вразливість	–	слабкість в системі, яка може бути використана загрозою
Ризик	–	можливість реалізації загрози з урахуванням впливу та ймовірності
Інцидент ІБ	–	подія, що порушує або може порушити безпеку інформації
NIST	–	Національний інститут стандартів і технологій США
NIST SP 800	–	серія рекомендацій і стандартів NIST у сфері кібербезпеки
ISO/IEC 27001	–	міжнародний стандарт систем управління інформаційною безпекою
IEC 62443	–	стандарт з кібербезпеки промислових та критичних систем
OpenVAS	–	система відкритого сканування вразливостей
Nessus	–	комерційний сканер вразливостей
SIEM	–	система управління подіями та інформацією безпеки
VPN	–	віртуальна приватна мережа
Політика безпеки	–	сукупність правил і вимог, що регламентують захист інформації в організації

MFA	–	багатофакторна автентифікація
DNS	–	система доменних імен

ВСТУП

Актуальність теми дослідження зумовлена потребою підвищення рівня кіберзахисту державних установ в умовах зростання кількості кібератак, спрямованих на системи державного управління. Порушення інформаційної безпеки в такому середовищі може мати наслідки, що виходять далеко за межі технічних проблем, оскільки ураження інформаційних систем державних органів впливає на національну безпеку, доступність публічних сервісів, стабільність інституцій та довіру громадян. Тому впровадження системи управління інформаційною безпекою, заснованої на результатах об’єктивного аудиту, є актуальним та стратегічно важливим завданням.

Метою роботи є розроблення та обґрунтування підходу до побудови та впровадження системи управління інформаційною безпекою державної установи з урахуванням результатів аудиту, виконаного за допомогою CSET.

Об’єктом дослідження є процес управління інформаційною безпекою в державній установі.

Предметом є методи, моделі та організаційно-технічні рішення щодо побудови системи управління інформаційною безпекою.

Наукова новизна полягає у формуванні цілісного підходу до побудови системи управління інформаційною безпекою, який інтегрує результати аудиту, технічний аналіз інфраструктури та організаційні чинники, що визначають ефективність захисту. Такий підхід дає змогу створити модель управління, яка не лише відповідає сучасним вимогам, але й може бути адаптована відповідно до змін зовнішнього середовища, нових загроз та розвитку цифрових технологій. Це має практичну цінність для будь-якої державної установи, яка прагне підвищити рівень кіберзахисту та забезпечити безперервність функціонування своїх сервісів.

Практичне значення роботи полягає у можливості використання запропонованих рішень для вдосконалення процесів управління інформаційною безпекою у реальних умовах державних установ. Розроблені рекомендації

можуть слугувати основою для створення або модернізації ISMS, оптимізації внутрішніх політик та процедур, підвищення рівня обізнаності персоналу та посилення контролю над критичними компонентами інформаційної інфраструктури. Крім того, модель впровадження, що ґрунтується на результатах CSET, може бути адаптована до різних організаційних структур і масштабів установ, що робить її універсальною та практично застосовною.

Основні результати проведених досліджень обговорювались на: XIII науково-технічній конференції «Інформаційні моделі, системи та технології» (м. Тернопіль, Україна).

Основні результати кваліфікаційної роботи опубліковано у працях конференції (див. Додаток А).

РОЗДІЛ 1 АНАЛІЗ СУЧАСНОГО СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДЕРЖАВНИХ УСТАНОВАХ

1.1 Обґрунтування обраної теми

У сучасних умовах цифрової трансформації державного сектору питання забезпечення інформаційної безпеки набуває особливої ваги. Широке впровадження електронних сервісів, зростання залежності від мережевої інфраструктури та активне використання інформаційно-комунікаційних технологій роблять державні установи вразливими до кіберзагроз, які за своїм характером стають дедалі складнішими, цілеспрямованішими та більш руйнівними. Цифрове середовище, яке покликане забезпечувати ефективність державного управління та доступність адміністративних послуг, водночас створює фундаментальні ризики функціонування, оскільки порушення інформаційної безпеки може призвести до збоїв у роботі критично важливих сервісів, компрометації службової інформації або втрати даних, що мають суттєве значення для громадян та державних процесів.

Високий рівень загроз вимагає від державних організацій системного підходу до управління безпекою, заснованого не лише на технічних засобах, а й на політиках, процедурах, механізмах контролю та безперервному моніторингу стану захищеності. У цьому контексті концепція системи управління інформаційною безпекою (Information Security Management System, ISMS) посідає центральне місце, оскільки передбачає не лише застосування засобів захисту, а й формування цілісної моделі управління ризиками, що охоплює організаційні, технічні та процесні аспекти діяльності установи. Впровадження ISMS дає змогу створити узгоджену систему правил та механізмів контролю, які забезпечують передбачуваність, прозорість та ефективність процесів інформаційної безпеки.

Однак побудова дієвої ISMS потребує достовірної оцінки поточного стану кіберзахисту. Лише на основі чітких аналітичних даних можливо визначити

реальні вразливості, проаналізувати ризики, оцінити рівень зрілості процесів і сформувати обґрунтовані рішення щодо підвищення рівня безпеки. У цьому контексті особливого значення набувають спеціалізовані інструменти аудиту, які дозволяють здійснити комплексну та структуровану оцінку інформаційної безпеки. Одним з таких інструментів є CSET – програмно-методичний комплекс, орієнтований на багатовимірне оцінювання відповідності практик безпеки вимогам сучасних стандартів. Його використання дає змогу перетворити неструктуровані дані про стан інфраструктури на систематизований аналітичний матеріал, необхідний для формування політик, процедур та технічних заходів захисту.

Досягнення мети кваліфікаційної роботи передбачає всебічний аналіз структури IT-інфраструктури, визначення суттєвих інформаційних активів, оцінювання загроз та вразливостей, а також дослідження стану процесів, які забезпечують безперебійну та захищену роботу систем установи. Особливе значення має інтерпретація результатів, отриманих у процесі оцінювання, оскільки саме вони стають основою для формування рекомендацій та практичних кроків щодо побудови або вдосконалення ISMS.

Логіка дослідження ґрунтується на поєднанні теоретичного аналізу сучасних підходів до управління інформаційною безпекою з практичним застосуванням методів аудиту. На початковому етапі важливо проаналізувати сучасний стан кіберзахисту в державних установах, окреслити основні проблеми, визначити системні недоліки та типові загрози, що впливають на функціонування державного сектору. Значну увагу необхідно приділити характеристиці базових стандартів і методів, які формують міжнародну практику побудови ISMS. Хоча сама робота не покладається на сторонні джерела, важливим є узагальнення загальних тенденцій, які склалися у сфері інформаційної безпеки на глобальному рівні, а також осмислення підходів, що застосовуються у державному секторі різних країн.

Другий етап передбачає детальне дослідження інформаційного середовища конкретної установи: її структури, характеру інформаційних потоків, категорій

даних, функцій та технологічних процесів. Аналіз інфраструктури дозволяє визначити ключові точки концентрації ризиків та оцінити залежність установи від цифрових компонентів, що є необхідним для формування обґрунтованої моделі загроз. У цьому контексті важливо дослідити, наскільки наявні засоби захисту відповідають реальним викликам та чи забезпечують вони достатній рівень стійкості до кіберінцидентів.

Особливе місце у дослідженні відведене застосуванню CSET як інструменту, який дозволяє здійснити комплексну оцінку зрілості процесів інформаційної безпеки та відповідності практик управління сучасним вимогам. Його використання надає можливість отримати структуровані дані про сильні та слабкі сторони системи безпеки, сформувати об'єктивне бачення стану захищеності та визначити напрями розвитку, які потребують додаткової уваги.

Таким чином, робота спрямована на розв’язання комплексного завдання – створення науково обґрунтованого, практично орієнтованого підходу до впровадження системи управління інформаційною безпекою державної установи на основі результатів оцінки CSET. Зростаюча складність кіберзагроз та важливість інформаційної інфраструктури для нормального функціонування держави зумовлюють потребу у таких дослідженнях, які поєднують аналітичну глибину, системність і практичну застосовність сформованих рішень.

1.2 Нормативно-правові засади кібербезпеки державного сектору України

Нормативно-правове забезпечення кібербезпеки державного сектору України формувалося як реакція на різке зростання кількості кібератак на критичну інфраструктуру, органи державної влади та державні інформаційні ресурси. Для державних установ воно відіграє роль комплексного регулятивного середовища, яке визначає правила, принципи, повноваження суб’єктів, механізми координації та відповідальність у сфері цифрової безпеки. В умовах тривалих гібридних загроз та необхідності інтеграції до європейського

кіберпростору нормативно-правова база України безперервно оновлюється, поступово наближаючись до моделей ЄС і НАТО.

Ключовим елементом нормативної основи є законодавче регулювання. Центральною ланкою є Закон України «Про основні засади забезпечення кібербезпеки України», який визначає поняття кібербезпеки, встановлює суб'єктів її забезпечення, визначає їхні функції та встановлює засади взаємодії між державними структурами. Особливу увагу в законі приділено державному сектору як об'єкту захисту, що пов'язано з високою цінністю державної інформації та її значенням для національної безпеки. Закон закладає також вимоги щодо розвитку системи моніторингу, обміну інформацією про інциденти та реагування на кібератаки [1].

У структурі державного сектору важливу роль відіграє нормативне регулювання захисту державних інформаційних ресурсів. Постанови Кабінету Міністрів України формують практичні вимоги щодо організації інформаційної безпеки у державних органах, включно з проведенням технічного захисту інформації, сертифікацією комплексів захисту, регламентацією доступу до інформаційних систем та порядком функціонування державних реєстрів. Ці документи забезпечують стандартизацію процедур і створюють уніфікований підхід до управління безпекою в різних установах [2].

Важливою частиною нормативної бази є вимоги з технічного та криптографічного захисту інформації. Положення та накази Адміністрації Державної служби спеціального зв'язку та захисту інформації України визначають процедури застосування засобів криптографічного захисту, вимоги до інформаційних систем, а також правила проведення аудиту та атестації комплексів захисту. Ці акти встановлюють технічні параметри безпеки й забезпечують практичний механізм впровадження державних стандартів у сфері кіберзахисту [3].

Окремий напрям нормативного забезпечення стосується критичної інформаційної інфраструктури. Після запровадження відповідних змін законодавство визначило категорії об'єктів критичної інфраструктури, порядок

їх ідентифікації, критерії оцінювання їх значущості та вимоги щодо забезпечення їхньої кіберстійкості. Для державного сектору це особливо актуально, оскільки значна частина критичної інфраструктури належить або контролюється державними органами. Нормативна база встановлює вимоги щодо безперервності діяльності, планів реагування на інциденти та протоколів взаємодії під час кризових ситуацій.

Важливою складовою у формуванні кібербезпеки державних установ є вимоги щодо захисту персональних даних. У цьому контексті застосовуються положення Закону «Про захист персональних даних», який встановлює порядок обробки, зберігання, використання та передачі персональної інформації. Державні органи несуть підвищену відповідальність за дотримання цих норм, оскільки оперують великими масивами конфіденційних даних громадян. Закон також визначає вимоги до організаційних і технічних засобів захисту, що мають бути впроваджені в державних інформаційних системах [4].

Важливе значення мають документи, спрямовані на узгодження українського законодавства з міжнародними практиками. Національна стратегія кібербезпеки визначає довгострокові пріоритети розвитку системи державного кіберзахисту, включно з адаптацією стандартів НАТО та ЄС. Стратегія встановлює необхідність впровадження систем управління інформаційною безпекою, розвитку інституційної спроможності державних органів, покращення підготовки спеціалістів, а також забезпечення належного рівня фінансування кіберзахисту [5].

Важливу роль у нормативному регулюванні відіграють міжвідомчі документи, які визначають порядок обміну інформацією та координацію дій під час кіберінцидентів. Такі документи містять вимоги до взаємодії між Національним координаційним центром кібербезпеки, Держспецзв’язку, правоохоронними органами та іншими інституціями. Координаційна модель, закріплена у НПА, створює основу для єдиного національного механізму реагування та мінімізації наслідків кібератак.

Окремі нормативні акти регламентують питання аудиту, моніторингу та оцінювання рівня кібербезпеки в державних установах. Вони визначають періодичність проведення оцінок, вимоги до звітності, а також критерії, за якими аналізуються технічні та організаційні заходи захисту. Саме такі акти створюють умови для системного та регулярного контролю за дотриманням вимог безпеки в органах влади, що забезпечує якісну основу для подальшого впровадження систем управління інформаційною безпекою.

Таким чином, нормативно-правові засади кібербезпеки державного сектору України формують багаторівневу систему, що охоплює законодавчу, технічну, організаційну та інституційну складові. Їхнє значення полягає у створенні єдиного регулятивного простору, який забезпечує можливість ефективного функціонування сучасних систем захисту інформації, сприяє підвищенню стійкості державних інституцій до кіберзагроз та підтримує прагнення України до інтеграції у світову систему кібербезпеки.

1.3 Міжнародні стандарти управління інформаційною безпекою

Управління інформаційною безпекою у сучасних державах і організаціях спирається на комплекс міжнародних стандартів, що визначають принципи, методології та вимоги до захисту інформаційних ресурсів. Їхня роль є ключовою, оскільки вони забезпечують глобальну уніфікацію підходів до кіберзахисту, сприяють підвищенню рівня довіри між державними установами, партнерами й громадянами, а також створюють основу для ефективного впровадження систем управління безпекою на практиці. Для державного сектору України ці стандарти є орієнтиром у створенні систем управління інформаційною безпекою, які відповідають вимогам ЄС та НАТО [6].

Серед найбільш впливових міжнародних нормативів у цій сфері виділяються три групи стандартів: ISO/IEC 27001, сімейство NIST SP 800, а також галузеві стандарти IEC 62443, орієнтовані на промислову та критичну інфраструктуру. Кожен із них має власну специфіку, однак разом вони формують

універсальну методологічну базу, яку державні органи можуть використовувати для побудови комплексного захисту своїх інформаційних активів.

1.3.1 ISO/IES 27001 як універсальний міжнародний стандарт управління інформаційною безпекою

Стандарт ISO/IEC 27001 є міжнародним еталоном у сфері організації процесів управління інформаційною безпекою. Він описує вимоги до створення, впровадження, підтримання та постійного вдосконалення системи управління інформаційною безпекою (ISMS). Його головна особливість полягає в тому, що він поєднує організаційні, технічні та управлінські інструменти, завдяки чому забезпечує структурований і вимірюваний підхід до захисту інформації.

Сутність стандарту базується на процесній моделі управління, яка передбачає циклічність дій: планування**,** реалізацію**,** перевірку та удосконалення. Такий механізм дозволяє організаціям адаптувати систему до змін зовнішніх та внутрішніх умов, що особливо актуально у сфері кібербезпеки, де загрози швидко еволюціонують.

Однією з ключових вимог ISO/IEC 27001 є системний підхід до оцінювання ризиків. Стандарт не обмежується технічними параметрами захисту, а формує модель, у якій саме ризик є основним критерієм вибору методів захисту. Державні установи, застосовуючи ці положення, отримують змогу визначати пріоритети захисту, враховуючи критичність активів, ймовірність інцидентів та потенційні наслідки.

Стандарт також містить комплекс заходів безпеки, згрупованих у відповідні категорії (політики, персонал, фізична безпека, операційний контроль, криптографія тощо). Хоча текст стандарту не містить обов’язкових технічних рішень, він формує універсальну рамку для побудови повноцінної системи безпеки в державних органах.

Для державного сектору України ISO/IEC 27001 є важливим ще й у контексті інтеграції до європейського цифрового простору. Багато країн ЄС

використовують цей стандарт як нормативний мінімум для державних установ, тому його впровадження в Україні сприяє поступовому наближенню до європейських практик управління інформаційною безпекою.

1.3.2 NIST SP 800: ризик-орієнтований підхід США до організації кіберзахисту

Сімейство документів NIST SP 800, розроблених Національним інститутом стандартів і технологій США, визначає одну з найдетальніших методологій кібербезпеки у світі. На відміну від ISO/IEC 27001, який має універсальний характер, стандарти NIST орієнтовані насамперед на потреби державних структур США, але водночас мають глобальне визнання завдяки своїй практичності та глибині опрацювання [7].

Основою NIST SP 800 є концепція управління ризиками, згідно з якою інформаційні системи повинні бути класифіковані залежно від очікуваних наслідків кіберінцидентів. Розроблені NIST рекомендації містять детальні вимоги щодо:

- класифікації систем;
- вибору базових заходів безпеки;
- реалізації політик захисту;
- тестування безпеки;
- постійного моніторингу стану систем.

Ця структура дозволяє державним органам не лише формувати політики безпеки, але й здійснювати контроль за їх виконанням на кожному етапі життєвого циклу інформаційної системи.

Серед документів сімейства особливе значення мають:

- NIST SP 800-53, що містить каталог технічних і організаційних контролів безпеки;
- NIST SP 800-30, присвячений методології оцінювання ризиків;

- NIST Cybersecurity Framework, який формує універсальну модель управління кібербезпекою на основі функцій «виявлення», «захист», «виявлення», «реагування», «відновлення» [8].

Для державних установ України стандарти NIST можуть бути корисними як практичні методичні документи, що дозволяють деталізувати та розширити положення ISO/IEC 27001. Особливо це актуально у тих сферах, де потрібна висока деталізація технічних вимог – наприклад, у державних реєстрах або в інформаційних системах спеціального призначення.

1.3.3 IES 62443: стандарти для захисту промислових систем та критичної інфраструктури

Стандарти IEC 62443 орієнтовані на захист промислових систем керування (ICS) та об’єктів критичної інфраструктури. Вони набувають особливого значення у державному секторі, оскільки значна частина критичної інфраструктури України належить саме державним або комунальним підприємствам: енергетика, транспорт, водопостачання, медицина, оборонно-промисловий комплекс [9].

На відміну від загальних стандартів, IEC 62443 враховує специфіку промислових процесів, де пріоритетом є безперервність роботи та стійкість до фізичних наслідків кібератак. Стандарти серії визначають:

- вимоги до захисту промислових мереж;
- правила сегментації та зонування;
- моделі загроз для ICS;
- роль постачальників і виробників обладнання;
- процедури управління вразливостями;
- вимоги до життєвого циклу розробки промислових систем.

Однією з ключових концепцій IEC 62443 є визначення *рівнів безпеки* (Security Levels), що дозволяють класифікувати об’єкти критичної інфраструктури залежно від потенційних загроз і вимог до їхнього захисту.

Такий підхід забезпечує масштабованість та адаптивність системи безпеки, що є критично важливим для державних підприємств різного профілю.

Оскільки промислова інфраструктура часто зазнає кібератак із використанням спеціалізованих засобів, стандарт пропонує методи аналізу загроз, які враховують технічні, організаційні та фізичні аспекти. Це робить IEC 62443 незамінним при проектуванні заходів безпеки для державних систем, пов'язаних з технологічними процесами.

1.3.4 Співвідношення міжнародних стандартів та їх застосування в державному секторі України

Хоча ISO/IEC 27001, NIST SP 800 та IEC 62443 відрізняються за структурою та сферою застосування, між ними існує логічна взаємодоповнюваність. Стандарти ISO формують універсальну рамку управління безпекою, NIST – надає практичні методики та деталізовані вимоги, а IEC 62443 – адаптує механізми захисту до промислових та критично важливих систем.

Для державного сектору України така комбінована модель є оптимальною, оскільки вона дозволяє:

- формувати політики на основі ISO/IEC 27001;
- деталізувати технічні вимоги за допомогою NIST SP 800;
- захищати промислові системи згідно з IEC 62443;
- адаптувати модель ризиків до українських законодавчих вимог;
- забезпечити сумісність із міжнародними партнерами та програмами цифрової інтеграції.

Впровадження міжнародних стандартів у державних установах також створює підґрунтя для незалежної сертифікації систем управління безпекою, що є поширеною вимогою у міжнародних проєктах технічної допомоги, а також співпраці.

1.4 Аналіз інструментів аудиту кібербезпеки

Аудит кібербезпеки є одним із ключових процесів для забезпечення належного рівня захисту інформаційних систем, особливо у державному секторі, де надійність функціонування інформаційних ресурсів безпосередньо впливає на національну безпеку. Ефективний аудит передбачає як аналіз організаційних заходів, так і перевірку технічних параметрів інформаційної інфраструктури, що потребує використання спеціалізованих інструментів та методів. Серед найпоширеніших інструментів, що застосовуються державними установами та організаціями критичної інфраструктури у світі, виділяють CSET**,** CIS Controls**,** OpenVAS та Nessus. Вони охоплюють різні аспекти аудиту – від комплексної оцінки відповідності до міжнародних стандартів до виявлення технічних вразливостей у мережах та системах.

1.4.1 CSET як інструмент комплексної оцінки кібербезпеки

Інструмент CSET (Cybersecurity Evaluation Tool) розроблений Міністерством внутрішньої безпеки США для проведення структурованої оцінки рівня кіберзахисту організації на основі вимог міжнародних та галузевих стандартів. Основна мета CSET – забезпечити можливість системного аналізу політик, процедур, технічних заходів безпеки та рівня організаційної підготовки до кіберзагроз [10].

Особливість CSET полягає в тому, що він є методологічним інструментом, а не сканером вразливостей. Він побудований на принципах опитувальника та системного аналізу, де кожен пункт відповідає вимогам певного стандарту чи нормативного документа. Це дає можливість організації отримати оцінку не окремих систем, а всієї структури забезпечення кібербезпеки. Для державних установ це особливо важливо, оскільки їх діяльність регулюється великою кількістю вимог щодо захисту інформації.

CSET дозволяє інтегрувати норми ISO/IEC 27001, NIST SP 800, IEC 62443, CIS Controls та інших міжнародних документів. Така універсальність робить його ефективним інструментом для перевірки виконання державних вимог у сфері технічного та організаційного забезпечення інформаційної безпеки. Крім того, CSET містить модуль оцінювання промислових систем, що робить його корисним для аналізу критичної інфраструктури.

Однією з важливих можливостей CSET є автоматична генерація звітів, які включають графічні діаграми, оцінку ризиків, перелік невідповідностей та рекомендації щодо покращення системи безпеки. Це дає змогу планувати заходи безпеки більш обґрунтовано та систематично.

1.4.2 CIS Controls як стратегія організаційного та технічного аудиту

CIS Controls є набором пріоритетних заходів кібербезпеки, розроблених Center for Internet Security. На відміну від CSET, який виконує функцію всебічного аналізу відповідності, CIS Controls структуровано як практичний набір дій, що дозволяють організації підвищити рівень кіберзахисту через впровадження конкретних технічних і організаційних контролів [11].

Контролі CIS включають вимоги до: інвентаризації активів, контролю прав доступу, управління вразливостями, моніторингу подій, забезпечення безпеки конфігурацій, управління інцидентами, навчання персоналу.

Ці контролі згруповані за рівнями критичності та адаптовані під різні типи організацій. У державному секторі CIS Controls застосовуються переважно для операційного та технічного аудиту, оскільки дозволяють деталізувати вимоги ISO/IEC 27001 і визначити, які саме технічні заходи повинні бути впроваджені для забезпечення базового рівня захисту.

Перевагою CIS Controls є їхня практичність та орієнтація на сучасні типи кібератак. Вони регулярно оновлюються відповідно до змін у кіберзагрозах, що робить їх актуальним інструментом аудиту. У контексті державних установ CIS Controls дозволяють структурувати роботу IT-підрозділів та забезпечити

відповідність вимогам міжнародних партнерів, які часто використовують ці контролі як мінімальний стандарт безпеки.

1.4.3 OpenVAS як відкритий інструмент сканування вразливостей

OpenVAS (Open Vulnerability Assessment System) є одним із найпоширеніших інструментів з відкритим вихідним кодом для сканування вразливостей. Він забезпечує автоматичний аналіз інформаційних систем з метою виявлення відомих вразливостей у мережевих службах, операційних системах, вебсервісах та інших компонентах IT-інфраструктури [12].

OpenVAS проводить глибоке сканування мережі, використовуючи базу тестів безпеки, яка регулярно оновлюється спільнотою розробників. У процесі аудиту система надсилає запити до мережевих служб і визначає, чи відповідають ці служби характеристикам відомих вразливостей. Результати сканування містять:

- список знайдених вразливостей;
- їх критичність;
- опис потенційних ризиків;
- рекомендації щодо усунення.

OpenVAS часто застосовується державними установами завдяки його відкритій ліцензії, що не потребує значних фінансових витрат. Крім того, він може бути інтегрований у внутрішні системи моніторингу та використовуватися як частина регулярного аудиту мережевих ресурсів.

Однією з переваг OpenVAS є можливість налаштування сценаріїв сканування відповідно до потреб конкретної організації. Це дозволяє зосередитися на критично важливих сегментах мережі, що особливо важливо для державних систем, де конфіденційність даних має першочергове значення.

1.4.4 Nessus як комерційний інструмент професійного сканування вразливостей

Nessus – один із найпоширеніших комерційних інструментів для виявлення технічних вразливостей. Його розробником є компанія Tenable, яка забезпечує регулярні оновлення баз сигнатур, що дозволяє інструменту швидко реагувати на появу нових загроз [13].

Nessus використовується для: сканування мережевих портів, аналізу конфігурацій систем, виявлення помилок у налаштуванні мережевих сервісів, перевірки систем на відповідність політикам безпеки, оцінки рівня захищеності веб-додатків.

У порівнянні з OpenVAS Nessus має ширший функціонал, швидше отримує оновлення бази вразливостей і забезпечує більш детальний аналіз конфігурацій. Це робить його одним із інструментів, які часто застосовуються у системах критичної інфраструктури та державних центрах кіберзахисту.

Перевагою Nessus є наявність готових політик відповідності, які можуть бути використані для оцінки систем згідно з вимогами NIST, CIS Controls, PCI DSS та інших стандартів. Для державних органів це означає можливість швидко перевірити відповідність технічних систем регуляторним вимогам.

1.4.5 Порівняльний аналіз інструментів аудиту

Порівняльний аналіз показує, що CSET та CIS Controls виконують більше організаційно-методологічні функції, тоді як OpenVAS і Nessus призначені для технічного сканування. CSET забезпечує системний аудит відповідності стандартам і генерує рекомендації на рівні політик та процедур, CIS Controls конкретизує пріоритетні дії, а OpenVAS і Nessus дозволяють оцінити реальний стан технічної безпеки та знайти конкретні вразливості. Для державної установи оптимально використовувати комбіновану модель, де CSET і CIS Controls визначають стратегію та пріоритети заходів, а OpenVAS і Nessus забезпечують

детальну перевірку систем на технічному рівні. Такий підхід дозволяє не тільки відповідати нормативним вимогам, а й практично підвищувати рівень захищеності критичних систем, виявляючи слабкі місця на ранніх етапах.

Таким чином, комплексне використання цих інструментів створює повноцінну систему аудиту кібербезпеки, що поєднує організаційні, методологічні та технічні аспекти. Це особливо важливо для державних установ, де критична інформація має високий рівень конфіденційності, а помилки у забезпеченні безпеки можуть призвести до значних наслідків для національної безпеки.

1.5 Огляд існуючих підходів до побудови систем управління інформаційною безпекою

Питання побудови систем управління інформаційною безпекою (ISMS) є надзвичайно важливим для сучасних організацій, зокрема державних установ, які оперують критичними інформаційними активами. Існують різні підходи до створення та розвитку ISMS, і їх вибір залежить від багатьох факторів – масштабів організації, типу інформаційних систем, характеру загроз, наявних ресурсів та регуляторних вимог. Ідеї ризик-орієнтованого підходу, його методи і практична цінність для державних установ детально описані в низці праць та методичних матеріалів, які підкреслюють необхідність систематичної ідентифікації активів і регулярної переоцінки ризиків. Застосування такого підходу дозволяє концентрувати зусилля та ресурси на найбільш критичних активи й сценарії загроз, що особливо важливо в умовах обмеженого бюджету або застарілої інфраструктури.

Стандартизований підхід, орієнтований на впровадження ISO/IEC-подібних вимог, передбачає формалізацію політик, процедур і механізмів контролю та створення циклічного процесу «планування – реалізація – перевірка – вдосконалення», який є базовим для сертифікаційних процедур. Така модель дає змогу забезпечити прозорість і підзвітність процесів, що важливо при аудиті та

взаємодії з регуляторами й міжнародними партнерами; її практичні аспекти і складнощі імплементації розглядаються в аналітичних статтях і методичних вказівках, які наголошують на потребі в ресурсах та компетенціях для повноцінного впровадження стандартів. У державному середовищі стандартизація полегшує узгодження внутрішніх політик з національними вимогами та сприяє сумісності з міжнародними практиками.

Паралельно з цим формується підхід, що інтегрує питання корпоративного управління (governance) та ISMS, де безпека розглядається не лише як технічна чи оперативна функція, а як елемент стратегії управління організацією в цілому. Така інтеграція передбачає активну участь вищого керівництва, визначення відповідальності на рівні ради або дирекції, а також імплементацію навчальних програм та механізмів зміни поведінки працівників. Роботи, що аналізують взаємозв’язок COBIT та ISO/IEC підходів, показують, що інтеграція корпоративного управління з ISMS підвищує ефективність контролю і дозволяє поєднати управлінські цілі з практиками кібербезпеки [14].

Рамкові моделі зрілості (maturity frameworks) пропонують поступовий, етапний шлях розвитку ISMS: вони дозволяють організації оцінити початковий стан, визначити цілі та поступово підвищувати рівень зрілості процесів управління безпекою. Відомі моделі, що використовуються для цього (наприклад, NIST CSF чи підходи, вивчення яких представлено у наукових роботах), забезпечують структуру для встановлення цілей, метрик і плану дій, що робить розвиток ISMS прогнозованим і керованим. Дослідження з адаптивних стратегій зрілості підкреслюють важливість поетапного нарощування можливостей і доведення процедур до повторюваного та контрольованого стану, що є критично важливим для організацій з обмеженими ресурсами [15].

Технологічно-орієнтований підхід акцентує увагу на впровадженні конкретних технічних засобів – SIEM, системи виявлення вторгнень, рішення для управління вразливостями, засоби контролю налаштувань та управління ідентифікацією. Він ефективний тоді, коли стоїть завдання оперативно

підвищити технічну стійкість інфраструктури, однак без супутніх політик і процесів ризикує створити «купу інструментів» без системної координації. Методичні матеріали та практичні керівництва наголошують, що технології слід розглядати як складову ISMS, але не як повноцінну заміну організаційних заходів [16].

Комбінований підхід, що об’єднує елементи ризик-орієнтованого, стандартизованого, управлінського та технологічного підходів, сьогодні вважається найпрактичнішим для державних установ. Поєднання стандартів ISO/IEC з практичними контролями CIS чи NIST і з моделями зрілості дозволяє сформувати адаптивну ISMS, яка відповідає нормативним вимогам, враховує локальні ризики та одночасно використовує доступні технічні засоби. Публікації та методичні матеріали підтверджують, що поетапна інтеграція різних підходів допомагає мінімізувати початкові витрати та поступово підвищувати рівень захищеності.

При виборі конкретного підходу для державної установи важливо врахувати низку організаційних особливостей: структуру управління, наявність компетенцій, бюджетні обмеження, характер інформаційних активів та існуючі регуляторні вимоги. Практичні керівництва щодо управління конфігурацією та інші методичні джерела підкреслюють, що навіть при обмежених ресурсах можна досягти суттєвого підвищення безпеки шляхом правильної пріоритизації заходів та поступової імплементації елементів ISMS [17].

Нарешті, дослідження, присвячені адаптивним стратегіям і практикам, вказують на те, що успішна ISMS повинна бути «живою» системою: вона потребує постійного моніторингу, повторної оцінки ризиків, навчання персоналу та регулярного оновлення процедур у відповідь на зміну загрозового середовища та технологічного ландшафту. Ця теза підтверджується як академічними роботами, що аналізують стратегії підвищення зрілості, так і практичними матеріалами, що описують поетапні підходи до впровадження ISMS у складних організаційних середовищах [18].

1.6 Висновки до першого розділу

У результаті проведеного аналізу сучасного стану інформаційної безпеки в державних установах було встановлено, що система кіберзахисту державного сектору України перебуває у процесі активного розвитку та вдосконалення. Нормативно-правові акти, що регламентують діяльність у сфері кібербезпеки, формують комплексну багаторівневу основу, яка охоплює питання організації систем захисту, порядку реагування на інциденти, державної політики у сфері кіберзахисту та взаємодії між суб'єктами безпеки. Незважаючи на наявність значної кількості регуляторних документів, практика їх реалізації в державних установах часто стикається з проблемами недостатньої уніфікації підходів, різною зрілістю IT-процесів та обмеженими ресурсами, що вимагає розроблення ефективних моделей інтеграції нормативних вимог у реальні механізми управління безпекою.

Дослідження міжнародних стандартів ISO/IEC 27001, NIST SP 800 та IEC 62443 продемонструвало, що вони утворюють методологічну базу, яка дозволяє формувати цілісні системи управління інформаційною безпекою. ISO/IEC 27001 забезпечує універсальність і придатність до широкого спектра організацій, NIST SP 800 орієнтований на деталізацію технічних і процедурних механізмів, а IEC 62443 зосереджується на захисті промислових і критичних систем. Важливою характеристикою цих стандартів є їх взаємодоповнюваність: вони дозволяють створювати адаптивні моделі безпеки, що враховують специфіку державного сектору, рівень технічної зрілості установи та типи інформаційних активів.

Розгляд інструментів аудиту – CSET, CIS Controls, OpenVAS та Nessus – показав, що ефективна система оцінювання інформаційної безпеки потребує поєднання організаційного та технічного аналізу. CSET та CIS Controls дозволяють оцінити відповідність процесів безпеки вимогам стандартів і практик, тоді як OpenVAS і Nessus забезпечують глибоке технічне сканування вразливостей інформаційних систем. Такий підхід створює можливість для формування повноцінної картини стану кіберзахисту установи, включаючи як

стратегічні, так і операційні аспекти. Порівняльний аналіз цих інструментів продемонстрував доцільність їх комбінованого застосування. Організаційно-методичні рішення формують основу політик та процедур, тоді як технічні сканери надають інформацію щодо фактичного стану інфраструктури. Це дозволяє мінімізувати інформаційні прогалини, визначити реальні ризики та сформувати обґрунтований перелік першочергових заходів для підвищення рівня кіберзахисту державної установи. Саме така інтегрована модель створює підґрунтя для побудови ефективної системи управління інформаційною безпекою. Отримані висновки створюють концептуальний фундамент для подальших досліджень у другому розділі, присвяченому аналізу конкретної державної установи, її інфраструктури, інформаційних активів та результатів оцінки засобами CSET.

РОЗДІЛ 2 АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ ДЕРЖАВНОЇ УСТАНОВИ

2.1 ІТ-інфраструктура установи

Інформаційно-технологічна інфраструктура Тернопільської державної сільськогосподарської дослідної станції Інституту сільського господарства Карпатського регіону Національної академії аграрних наук України (далі ІСГ Карпатського регіону НААН) формується відповідно до функціональних потреб науково-дослідної діяльності, адміністративного управління та забезпечення інформаційного обміну між структурними підрозділами. Особливістю даної установи є поєднання класичних офісних ІТ-ресурсів із обладнанням, що використовується у польових і лабораторних аграрних дослідженнях. Це зумовлює нерівномірність технологічного оснащення, різний рівень ІТ-компетентностей персоналу та підвищені вимоги до безпеки даних, які збираються та опрацьовуються в рамках наукових експериментів.

Основний адміністративний будинок установи має локальну комп’ютерну мережу (LAN), побудовану на основі кабельної інфраструктури з використанням декількох комутаторів, що забезпечують підключення робочих станцій у кабінетах. Вся мережа функціонує в межах одного поверху, що характерно для невеликих державних установ, де централізоване серверне обладнання не передбачене ані штатним розписом, ані бюджетними можливостями. Прокладена кабельна інфраструктура забезпечує базову надійність і мінімізацію перешкод, проте її загальний технічний стан характерний для установ з обмеженим фінансуванням, що проявляється у відсутності резервних ліній, старих точках розгалуження та недостатній стандартизації маркування кабелів.

Доступ до Інтернету забезпечується через один центральний маршрутизатор провайдера. Також встановлено Wi-Fi роутер, який наразі знаходиться у вимкненому стані. У разі потреби роутер може бути ввімкнутий і налаштований для забезпечення доступу мобільних пристроїв або ноутбуків, зокрема під час підготовки звітів чи проведення нарад зі структурними

підрозділами. Проте на момент проведення дослідження бездротовий сегмент мережі відсутній, що значно знижує рівень потенційних кіберзагроз, пов’язаних із перехопленням трафіку, підробкою точок доступу чи неконтрольованим підключенням сторонніх пристроїв. Це нетипове рішення, однак воно відображає реальну ситуацію, коли керівництво установи тимчасово обмежує роботу бездротової мережі для зниження загроз несанкціонованого доступу або через відсутність потреби у Wi-Fi у більшості внутрішніх підрозділів.

Структурні підрозділи, розташовані в різних районах області, функціонують автономно та мають власні комп’ютери, що використовуються для польових досліджень, аграрних вимірювань та первинної фіксації даних. Кількість комп’ютерної техніки в усій установі, включаючи віддалені підрозділи, становить приблизно 30 одиниць. Окрім стаціонарних ПК, використовуються ноутбуки, що є необхідним інструментом під час виїздів до господарств і дослідних полігонів. Відсутність уніфікованого технічного обліку та централізованої служби IT-підтримки ускладнює координацію роботи обладнання, однак відповідає типовим умовам функціонування наукових підрозділів державного сектору.

Операційні системи, що використовуються на робочих станціях, належать переважно до поколінь Windows 7 та Windows 10. Частина комп’ютерів працює на застарілому програмному забезпеченні, оскільки оновлення ОС потребує додаткового фінансування, яке не завжди доступне, а також через те, що певне спеціалізоване обладнання або програмні модулі досліджень можуть бути сумісні лише з конкретними версіями Windows. Це створює додаткові ризики, оскільки саме Windows 7 з 2020 року не отримує оновлень безпеки, що підвищує загрозу експлуатації вразливостей при підключенні таких пристроїв до мережі або при роботі з зовнішніми носіями.

Зовнішні носії інформації широко використовуються у діяльності установи. Флеш-накопичувачі, SD-карти та зовнішні жорсткі диски застосовуються як для перенесення даних між комп’ютерами, так і для експорту результатів аграрних досліджень з лабораторного обладнання. Це зручно, але водночас збільшує ризик

потрапляння шкідливого програмного забезпечення, оскільки часто такі носії не проходять перевірку антивірусними засобами, а стандартизовані політики контролю використання зовнішніх пристроїв відсутні.

Суттєвою частиною ІТ-інфраструктури станції є спеціалізоване наукове обладнання, яке використовується для проведення аграрних вимірювань, збору статистичних даних, моніторингу стану ґрунтів, рослинності, погодних умов тощо. Частина обладнання підключається до комп'ютерів через USB-інтерфейси, інша – через COM-порти або спеціальні контролери. Наявність такого обладнання вимагає збереження можливості роботи на старих ОС, що знижує гнучкість модернізації ІТ-інфраструктури. Дані, отримані з цих пристроїв, обробляються у локальних програмах, а не в хмарних вебсервісах, оскільки установа не використовує хмарні технології для зберігання чи резервування інформації. Відсутність серверного обладнання та централізованого сховища ускладнює забезпечення цілісності та доступності дослідних даних, особливо в довгостроковій перспективі.

Важливим аспектом є відсутність серверного приміщення, файлового сервера або серверів додатків, що є типовою рисою державних наукових установ із невеликим ІТ-бюджетом. Усі дані зберігаються локально на робочих станціях співробітників, а документообіг забезпечується стандартними офісними програмами та електронною поштою. Це суттєво знижує рівень контрольованості інформаційних потоків та обмежує можливість впровадження сучасних методів захисту, таких як централізоване резервування, доменна політика безпеки або управління доступом на основі ролей.

Окрему увагу заслуговує взаємодія між центральним підрозділом і віддаленими структурними одиницями. Через відсутність VPN-каналів та захищених каналів зв'язку передача інформації здійснюється переважно через електронну пошту або за допомогою зовнішніх носіїв, що створює підвищений ризик втрати або компрометації даних. Водночас така модель роботи відображає реалії бюджетних наукових установ, де ІТ-інфраструктура виконує допоміжну роль і розбудовується за залишковим принципом.

Узагальнюючи, ІТ-інфраструктуру дослідної станції можна охарактеризувати як функціональну, але фрагментарну, з обмеженими можливостями масштабування та мінімальною кількістю сучасних засобів управління ІТ-ресурсами. Її стан потребує впровадження систематизованих заходів із забезпечення інформаційної безпеки, оскільки велика частина інформації є результатом багаторічних досліджень і має високу наукову та економічну цінність.

2.2 Аналіз інформаційних активів та категоризації даних

Аналіз інформаційних активів є ключовим етапом у формуванні цілісної системи кіберзахисту, оскільки дозволяє встановити, які ресурси є основою для виконання функцій державної установи та які саме компоненти ІТ-інфраструктури можуть бути критичними з точки зору конфіденційності, цілісності та доступності даних. Проведення цього аналізу створює підґрунтя для подальшого визначення загроз, оцінки ризиків і планування заходів з підвищення рівня кібербезпеки.

У межах цього пункту аналіз здійснюється з урахуванням фактичних характеристик інфраструктури Тернопільської державної сільськогосподарської дослідної станції ІСГ Карпатського регіону НААН, яка, згідно з описом у пункті 2.1, функціонує без серверного обладнання, без сегментації мережі, з використанням персональних комп’ютерів, центрального маршрутизатора провайдера та відключеного Wi-Fi маршрутизатора, а також містить розгалужену структуру підрозділів, що використовують ноутбуки для виїзної роботи.

2.2.1 Аналіз інформаційних активів

Інформаційні активи установи формуються з урахуванням того, як саме здійснюється обробка, передавання та зберігання інформації на робочих місцях.

Через відсутність виділених серверів персональні комп’ютери фактично виконують роль основних центрів зберігання та обробки даних. Це підсилює їх значення як ключових активів, оскільки будь-які порушення в їх роботі безпосередньо впливають на доступність та цілісність службових процесів.

До апаратної частини активів належать робочі станції співробітників та ноутбуки, які використовуються у структурних підрозділах і під час виїзних досліджень. Вони є базовою ланкою обробки даних, а тому містять широкий спектр інформації: від службових документів до результатів досліджень, що проводяться польовими групами. Окреме значення мають зовнішні носії, які активно застосовуються у роботі для перенесення файлів або резервування. Через мобільність та невисокий рівень контролю їх використання вони становлять додатковий актив із підвищеним ризиком.

Іншим компонентом фізичної інфраструктури є центральний маршрутизатор провайдера. Він забезпечує доступ усіх робочих станцій до Інтернету, тобто відіграє ключову роль у комунікаційних процесах. Хоча в установі присутній другий маршрутизатор, що може забезпечувати Wi-Fi доступ, його відключений стан означає, що на момент аналізу він не бере участі у мережевих процесах і не формує активного технічного активу. Проте за умови його включення він миттєво стане частиною критичних активів, що потребують захисту.

До програмних активів належить операційне середовище робочих станцій, а також прикладні програми, зокрема ті, що забезпечують комунікації та обробку службової інформації. Певне значення має також системне ПЗ, яке виконує мережеві, сервісні та захисні функції.

Мережеві активи охоплюють локальну мережу, що з’єднує робочі станції, та канал доступу до Інтернету. Їх значення визначається тим, що фактична взаємодія користувачів, обмін даними та оновлення програмного забезпечення відбуваються саме через ці елементи. У відсутності сегментації мережі будь-яка робоча станція стає одночасно і активом, і потенційною точкою доступу для загроз.

Також інформаційні активи включають дані, що циркулюють в установі. Це службові документи, персональні дані співробітників, робочі записи підрозділів, результати аграрних досліджень, технічні конфігурації пристроїв і програмного забезпечення, а також комунікаційні матеріали, що передаються через цифрові канали. Оскільки установою не використовуються хмарні сервіси, усі дані розміщуються локально, на фізичних носіях або робочих станціях, що підвищує залежність від надійності кінцевих пристроїв та дисципліни користувачів.

2.2.2 Категоризація даних

Категоризація даних здійснюється з метою визначення пріоритетності захисту різних типів інформації та оптимального розподілу засобів безпеки. Оцінювання проводиться на основі трьох ключових критеріїв: конфіденційності, цілісності та доступності. Через те, що установа не має централізованої серверної інфраструктури, інформація, що зберігається на робочих станціях, набуває особливо високого значення, оскільки втрата або пошкодження одного комп’ютера може спричинити втрату важливих даних.

Найвищий рівень критичності мають дані, що містять службову або персональну інформацію, зокрема результати досліджень, звіти, внутрішня документація та конфіденційні робочі матеріали. До цієї групи належать і дані, що передаються через електронну пошту та інші засоби комунікації, включаючи текстові та мультимедійні матеріали, адже саме через них відбувається значна частина службової взаємодії співробітників, особливо за умови роботи у структурних підрозділах або під час виїздів.

До даних середньої важливості належать технічні налаштування програм та операційних систем, системні журнали, локальні конфігурації мережевих інтерфейсів, а також внутрішні робочі файли, що не містять критично чутливої інформації. Компрометація таких даних може порушити працездатність робочих місць, однак зазвичай не призводить до прямих загроз для діяльності установи.

Найнижчий рівень критичності мають матеріали довідкового характеру, загальнодоступні документи, а також дані, що не мають службового значення.

2.3 Ідентифікація вразливостей і загроз безпеці

Ідентифікація вразливостей та загроз безпеці є ключовим етапом формування цілісної системи кіберзахисту, оскільки саме на цьому етапі визначаються потенційні слабкі місця IT-інфраструктури, які можуть бути використані зловмисниками, а також умови, за яких можуть виникати небажані інциденти. З огляду на те, що Тернопільська державна сільськогосподарська дослідна станція ІСГ Карпатського регіону НААН функціонує без серверного обладнання, з мінімальною сегментацією мережі, з використанням персональних комп’ютерів у різних підрозділах та з активним застосуванням зовнішніх носіїв, питання виявлення вразливостей набуває особливо важливого значення.

2.3.1 Вразливості, пов’язані з технічним станом робочих станцій

Одним із найбільш значущих джерел вразливостей є програмне та апаратне забезпечення персональних комп’ютерів, які використовуються як основні робочі інструменти. Через відсутність серверної архітектури саме робочі станції зберігають більшість даних та забезпечують доступ до службових матеріалів. Використання операційних систем Windows 7 і Windows 10, особливо у випадку їх несвоєчасного оновлення, створює ризики наявності відомих експлойтів, які можуть бути використані для несанкціонованого доступу або порушення роботи. Окремим фактором ризику є можливі апаратні збої, оскільки відсутність централізованих серверів означає, що кожна робоча станція є автономним центром даних, а її вихід з ладу може призвести до непоправних втрат інформації.

Недостатність засобів контролю над конфігураціями систем безпеки, антивірусним захистом та станом оновлень програмного забезпечення також

збільшує ймовірність компрометації. З огляду на мобільний характер роботи співробітників, які здійснюють виїзди до районних підрозділів, ноутбуки можуть підключатися до різних мереж, що підсилює ризики зараження шкідливими програмами або несанкціонованого доступу до даних.

2.3.2 Вразливості, пов’язані з мережею та комунікаційною інфраструктурою

Мережева інфраструктура установи складається з одного центрального маршрутизатора провайдера та дротової локальної мережі, що з’єднує робочі станції. За відсутності сегментації всі комп’ютери перебувають у спільному мережевому середовищі, що створює ризик внутрішнього поширення шкідливих програм або порушення роботи всієї мережі у разі компрометації одного пристрою.

Відключений Wi-Fi маршрутизатор на даний момент не є активною точкою ризику, однак його майбутнє використання без належного захисту може створити додатковий канал доступу для зловмисників. Наявність лише базового маршрутизатора провайдера означає, що мережевий трафік, ймовірно, проходить без використання складних механізмів фільтрації, що підвищує ймовірність проникнення небажаного трафіку.

Мобільність персоналу також сприяє тому, що ноутбуки ймовірно періодично підключаються до сторонніх мереж, де не завжди можна гарантувати належний рівень безпеки. Після підключення до внутрішньої мережі такі пристрої можуть переносити загрози, які будуть здатні поширюватися між іншими вузлами мережі.

2.3.3 Загрози, пов’язані з використанням зовнішніх носіїв

Оскільки зовнішні носії застосовуються активно і виконують роль інструментів обміну інформацією між підрозділами, вони є одним із потенційно

найризикованіших елементів в інфраструктурі. Використання флеш-накопичувачів без шифрування або без відповідної перевірки значно підвищує ймовірність занесення шкідливого коду на робочі станції. Особливо критичною є ситуація у разі, коли їх використовують у різних пристроях або під час роботи поза межами установи.

Відсутність централізованого контролю над тим, які носії підключаються до робочих місць, означає, що можливість несанкціонованого перенесення конфіденційної інформації також не можна виключати. Такі сценарії не завжди пов’язані зі зловмисністю, але можуть виникати внаслідок недбалості співробітників або ненавмисного копіювання даних.

2.3.4 Загрози, що випливають із діяльності підрозділів у районах

Оскільки установа має низку структурних підрозділів, розташованих у різних районах області, а співробітники здійснюють виїзну діяльність із використанням ноутбуків та польового обладнання, зростає ризик втрати або фізичної компрометації пристроїв. У таких умовах зловмисник може отримати доступ до конфіденційної інформації або змінити налаштування пристрою, що у майбутньому призведе до складніших інцидентів.

Додатковим фактором ризику є можливість підключення польового обладнання або датчиків до ноутбуків, оскільки навіть офіційне лабораторне обладнання може мати власні вразливості, які розглядаються значно рідше, ніж вразливості широко доступних комп’ютерних систем.

2.3.5 Загрози, пов’язані з людським фактором

Незалежно від технічного рівня захисту, людський фактор залишається одним із головних джерел ризику. Недостатня обізнаність користувачів щодо сучасних методів соціальної інженерії, фішингових атак і небезпеки відкриття

невідомих файлів може призводити до інцидентів, які важко попередити технічними засобами.

Крім того, відсутність формалізованих процедур роботи з інформацією і стандартизованих політик користування пристроями створює можливості для помилок, таких як встановлення ненадійного програмного забезпечення, несвоєчасне оновлення системи або передачу службових файлів через незахищені канали.

2.4 Проведення оцінки кібербезпеки за допомогою CSET

Оцінювання кібербезпеки установи проводилося із застосуванням програмного засобу CSET (Cybersecurity Evaluation Tool), який надає можливість комплексно аналізувати стан інформаційної безпеки, оцінювати відповідність вимогам стандартів і виявляти проблемні області. Робота з програмою розпочалася із завантаження основного меню, у якому зазначено ключові функціональні модулі інструмента. Цей етап дозволяє сформувати загальне бачення структури оцінювання та передбачених інструментів аналізу. Подальшим кроком стало налаштування метаданих оцінювання, зокрема визначення особи-фасилітатора, відповідальної за проведення аналізу системи кібербезпеки. Програма автоматично включає дані про того, хто здійснює оцінювання, що підвищує точність та документованість процесу. Відповідна інформаційна панель наведена на рисунку 2.1.

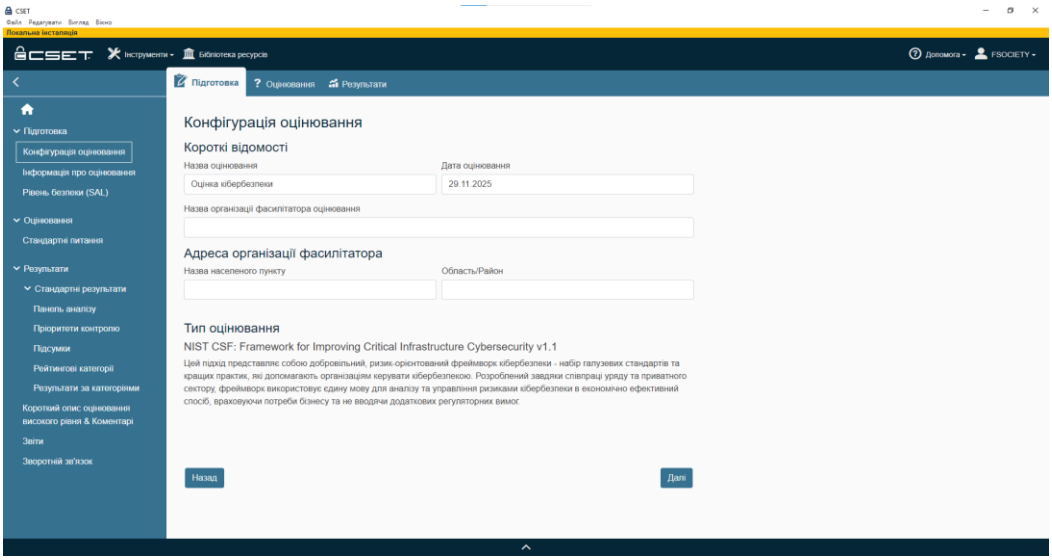

Рисунок 2.1 – Інформація про фасилітатора

Після цього було сформовано базову інформацію про сам процес оцінювання, включно з його метою, об’єктом і типовими параметрами оцінюваної системи, що відображено на рисунку 2.2. На цьому етапі закладаються основні критерії, які впливають на подальший алгоритм формування питань і вимог.

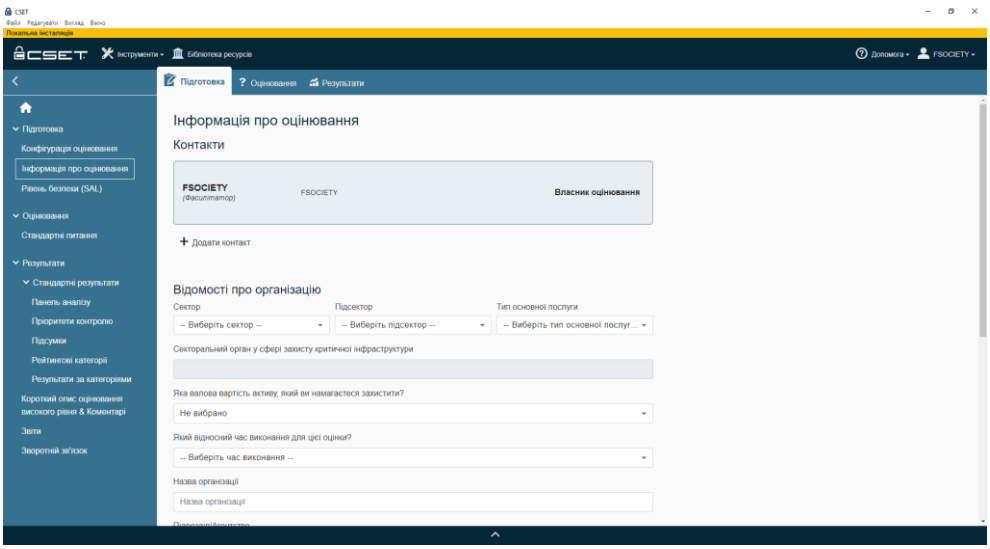

Рисунок 2.2 – Інформація про оцінювання

Наступним кроком стала процедура визначення рівня безпекового функціоналу SAL (Security Assurance Level). Програма CSET автоматично

пропонує оптимальний рівень захисту, виходячи з критичності системи та обраного профілю.

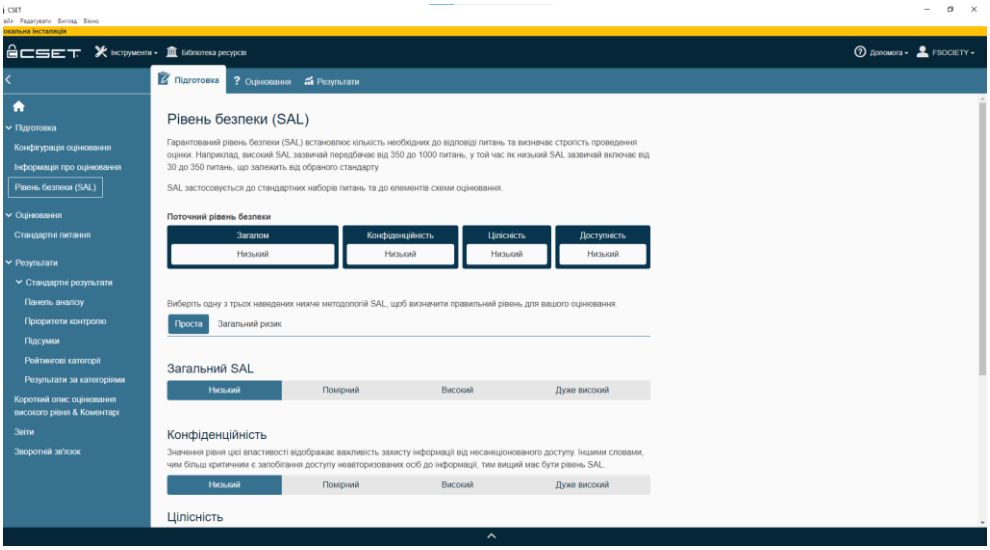

Рисунок 2.3 – Вибір рівня безпеки (SAL)

У випадку досліджуваної установи було застосовано базовий рівень SAL, що відповідає низькій складності IT-інфраструктури та обмеженому набору критичних активів. Вибір рівня SAL подано на рисунку 2.3.

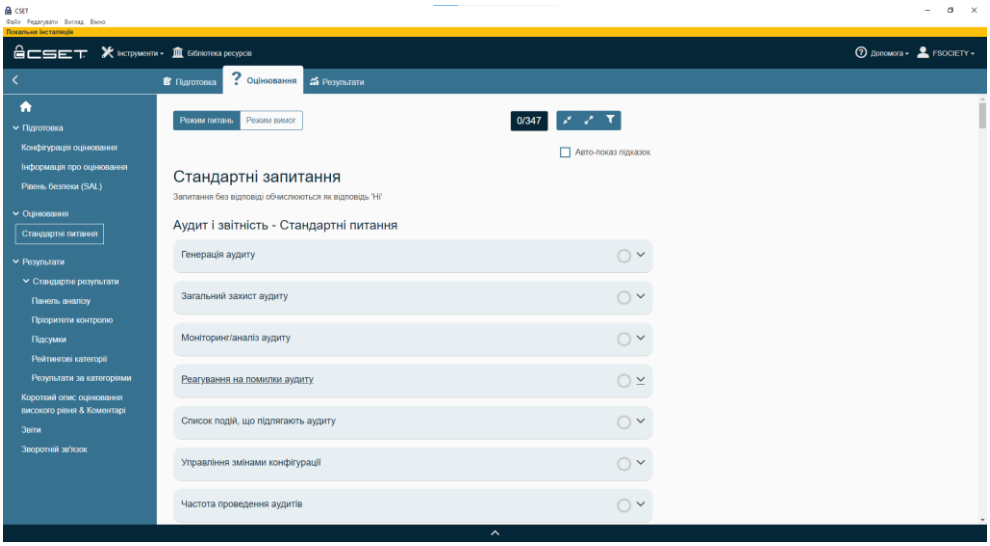

Рисунок 2.4 – Оцінювання в режимі питань

Після формування параметрів оцінювання програмне забезпечення переходить до основного етапу, який передбачає заповнення блоків із

запитаннями. Оцінювання може виконуватися у двох режимах. Перший режим передбачає послідовне надання відповідей на питання, що стосуються певних аспектів безпеки. Це дозволяє оцінювачеві точно відобразити фактичний стан окремих контролів. Вікно такого режиму подано на рисунку 2.4.

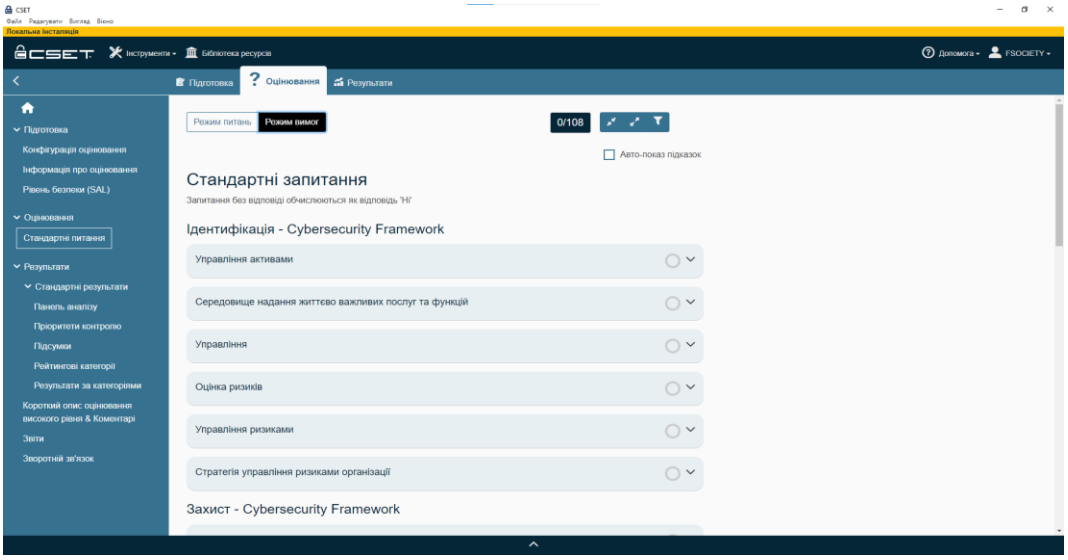

Рисунок 2.5 – Оцінювання в режимі вимог

Другий режим ґрунтується на оцінюванні вимог, де замість запитань пропонується перелік контрольних заходів, які потрібно підтвердити або спростувати відповідно до фактичного стану системи (рис. 2.5).

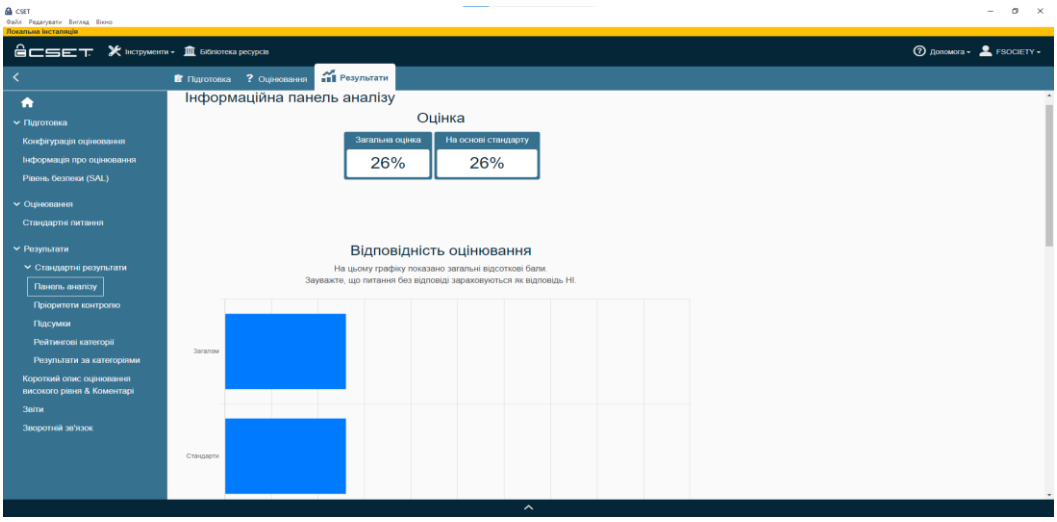

Рисунок 2.6 – Результати оцінювання

Після завершення опрацювання всіх тематичних блоків CSET формує підсумкові результати оцінювання. У загальному вигляді ці результати подані на рисунку 2.6. Вони демонструють рівень відповідності реалізованих заходів безпеки рекомендованим практикам.

Для того щоб підсумкові дані було легше інтерпретувати, CSET окремо виділяє найбільш проблемні сфери, у яких відповідність контролям є мінімальною.

Рисунок 2.7 – Найпоширеніші проблемні сфери

Візуалізацію таких сфер наведено на рисунку 2.7.

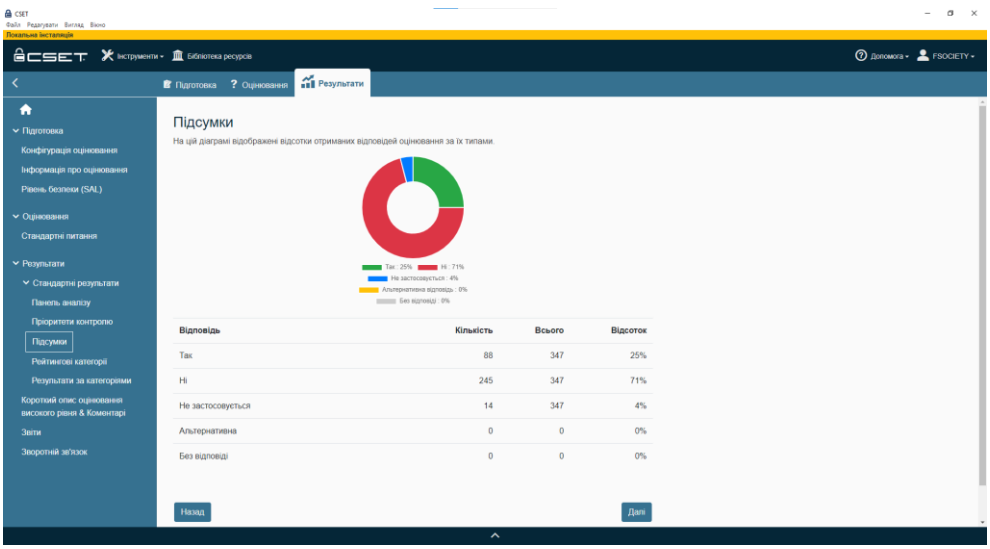

Рисунок 2.8 – Діаграма підсумку відповідей

Важливою частиною оцінювання є зведені діаграми, що демонструють розподіл відповідей за категоріями «так», «ні» та «не застосовується». Вони дають змогу оцінити загальний стан кіберзахисту установи зі структурної точки зору. Відповідний графічний підсумок наведено на рисунку 2.8.

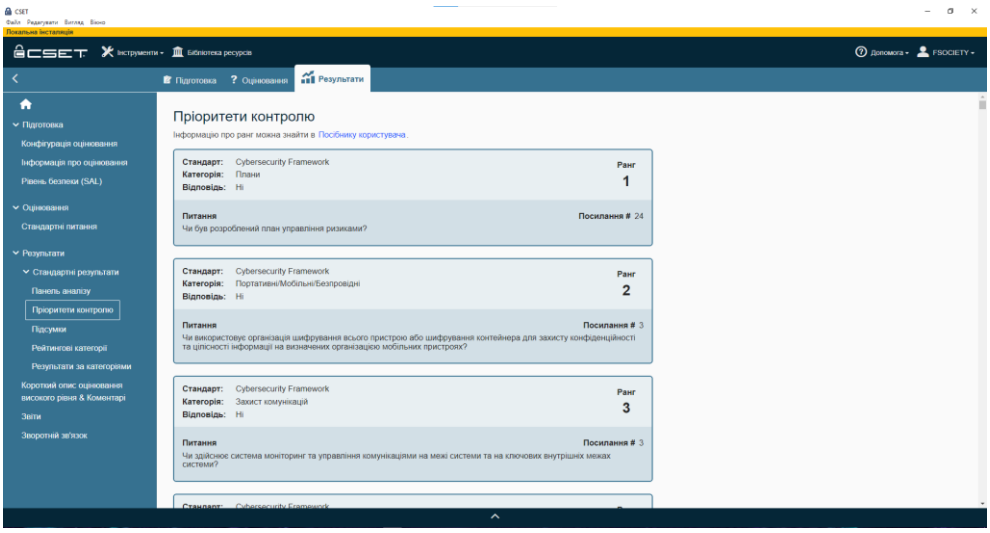

Рисунок 2.9 – Пріоритети контролю

Одним із ключових результатів CSET є визначення пріоритетів впровадження контролів, що дозволяє правильно вибудувати послідовність заходів для підвищення кіберзахисту. Відповідний фрагмент із рекомендованими пріоритетами контролю наведено на рисунку 2.9.

Рисунок 2.10 – Найпоширеніші проблеми сфери

Окремо формуємо перелік найпоширеніших проблемних сфер, які потребують першочергового вдосконалення. Цей перелік (рис. 2.10) представлений у таблиці 2.1, що деталізує сфери, на яких установі необхідно сконцентрувати ресурси та увагу.

Таблиця 2.1 – Найпоширеніші проблемні сфери

Категорія	**Ранг**	**Не виконано**	**Всього**	**Відсоток**
1	2	3	4	5
Безперервність	1	26	35	8%
Керування та оцінювання ризиків	2	28	28	8%
Моніторинг та шкідливе програмне забезпечення	3	18	21	6%
Плани	4	18	24	5%
Захист комунікацій	5	12	13	5%
Політики	6	11	14	4%
Керування конфігураціями	7	12	18	4%
Захист інформації	8	10	16	3%
Навчання	9	9	13	3%
Портативні/Мобільні/Безпровідні	10	8	9	3%
Захист систем	11	8	10	3%
Організаційне	12	8	8	3%
Реакція на інциденти	13	14	15	3%
Придбання систем та сервісів	14	6	8	2%
Політики та основні процедури	15	5	8	2%
Аудит і звітність	16	8	10	2%
Фізичний захист	17	6	13	2%
Захист оточення	18	7	11	2%

Продовження таблиці 2.1

1	2	3	4	5
Цілісність системи	19	8	10	2%
Контроль доступу	20	3	5	1%
Керування обліковими записами	21	3	13	1%
Обслуговування	22	3	7	1%
Процедури	23	2	4	1%
Програмне забезпечення	24	1	2	0%
Персонал	25	1	3	0%
Керування інформацією та документами	26	1	1	0%
Керування віддаленим доступом	27	1	3	0%
Ідентифікація	28	5	5	0%
Відповідь	29	1	1	0%
Захист	30	2	4	0%
Приватність	31	0	1	0%

З метою глибшої деталізації CSET формує індивідуальні бали для кожної категорії оцінювання. Вони відображають позитивні аспекти діяльності установи, тобто ті сфери, у яких рівень відповідності є достатнім або близьким до прийнятного (табл. 2.2).

Таблиця 2.2 – Індивідуальні бали для кожної категорії

Категорія	**Пройшов**	**Всього**	**Відсоток**
1	2	3	4
Аудит і звітність	2	10	20%
Безперервність	9	35	26%
Відповідь	0	1	0%
Захист	2	4	50%

Продовження таблиці 2.2

1	2	3	4
Захист інформації	6	16	38%
Захист комунікацій	1	13	8%
Захист оточення	4	11	36%
Захист систем	2	10	20%
Ідентифікація	0	5	0%
Керування віддаленим доступом	2	3	67%
Керування інформацією та документами	0	1	0%
Керування конфігураціями	6	18	33%
Керування обліковими записами	10	13	77%
Керування та оцінювання ризиків	0	28	0%
Контроль доступу	2	5	40%
Моніторинг та шкідливе програмне забезпечення	3	21	14%
Навчання	4	13	31%
Обслуговування	4	7	57%
Організаційне	0	8	0%
Персонал	2	3	67%
Плани	6	24	25%
Політики	3	14	21%
Політики та основні процедури	3	8	38%
Портативні/Мобільні/Безпровідні	1	9	11%
Приватність	1	1	100%
Придбання систем та сервісів	2	8	25%
Програмне забезпечення	1	2	50%
Процедури	2	4	50%

Продовження таблиці 2.2

1	2	3	4
Реакція на інциденти	1	15	7%
Фізичний захист	7	13	54%
Цілісність системи	2	10	20%

Ці результати важливі, оскільки дозволяють сформувати об’єктивну картину стану кібербезпеки не тільки з погляду недоліків, але й з погляду наявних сильних сторін (рис. 2.11).

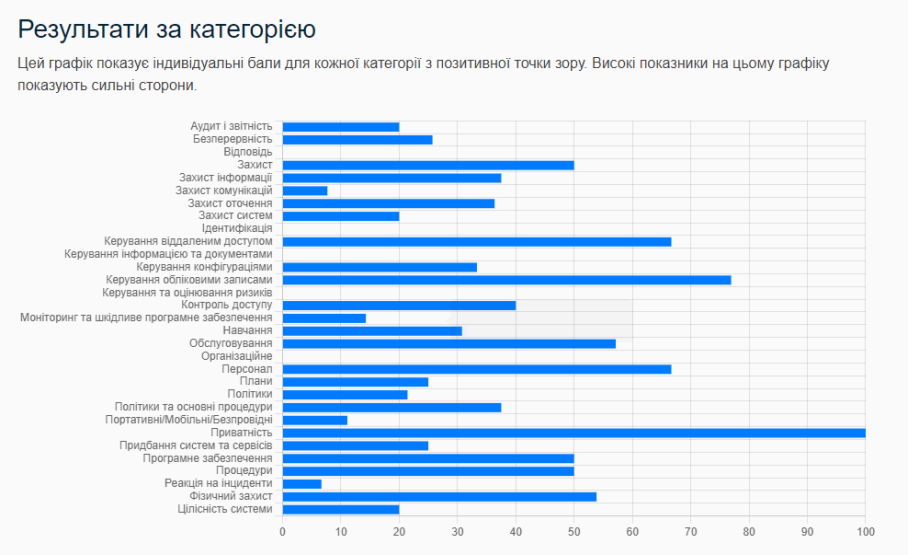

Рисунок 2.11 – Індивідуальні бали для кожної категорії

Після завершення оцінювання CSET дає змогу експортувати звіти, які можуть бути використані у подальшій роботі, зокрема під час підготовки моделей, політик і рекомендацій. Інтерфейс експорту результатів оцінювання зображений на рисунку 2.12.

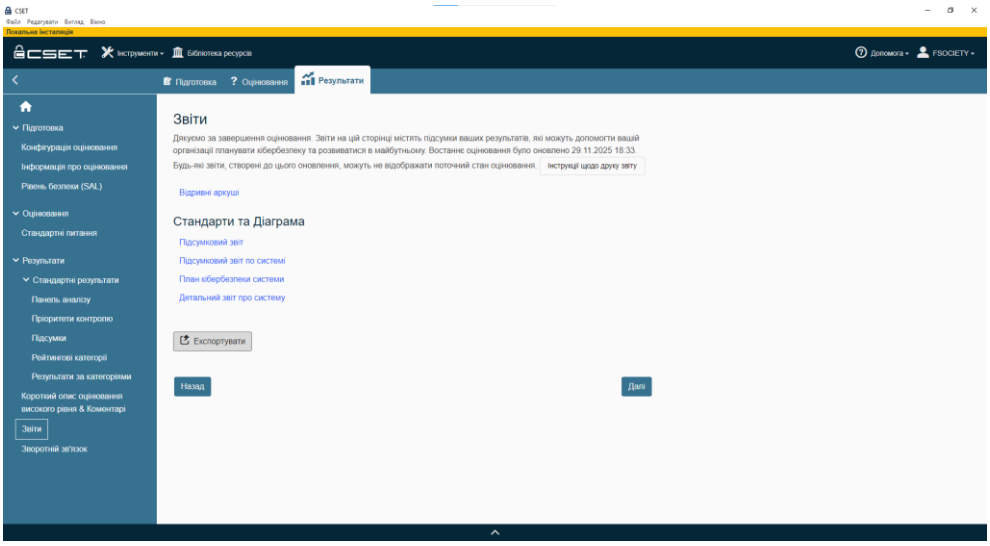

Рисунок 2.12 – Експорт звітів

Підсумовуючи результати, можна зазначити, що оцінювання за допомогою CSET дало змогу комплексно виявити ключові недоліки в системі кібербезпеки установи. Основними проблемами виявилися відсутність формалізованих політик безпеки, неструктурованість процесів управління конфігураціями, недостатня організація резервного копіювання та мінімальний рівень контролю доступу. Разом з тим інструмент показав наявність позитивних аспектів, які можуть стати основою для подальшого розвитку системи кіберзахисту. Отримані результати є базою для подальшого проєктування системи управління інформаційною безпекою, що детально розглядатиметься у розділі 3.

2.5 Висновки до другого розділу

У другому розділі було здійснено комплексний аналіз стану кібербезпеки Тернопільської державної сільськогосподарської дослідної станції Інституту сільського господарства Карпатського регіону НААН. На основі зібраної інформації, дослідження IT-інфраструктури, аналізу інформаційних активів та проведеної оцінки за допомогою інструменту CSET встановлено, що поточний рівень кіберзахисту установи відповідає базовим вимогам, проте характеризується низкою системних недоліків, які потребують усунення.

У межах дослідження ІТ-інфраструктури було визначено, що організація використовує відносно просту мережеву архітектуру, яка складається переважно з окремих робочих станцій, об’єднаних у локальну мережу за допомогою одного центрального маршрутизатора провайдера та декількох комутаторів. Відсутність серверного обладнання, хмарних сервісів, сегментації мережі та виділених серверних приміщень свідчить про те, що інформаційні потоки обробляються без централізованого контролю. Такі умови суттєво знижують загальну стійкість системи, а також збільшують залежність від конфігурації та безпечності кожного окремого кінцевого пристрою.

Аналіз інформаційних активів дав змогу класифікувати дані за рівнями критичності та визначити основні категорії інформації, що обробляється в установі. До найбільш значущих активів належать локальні дослідні дані, внутрішня службова інформація, документи фінансової звітності та інформація, що формується під час виїзних дослідних робіт. Водночас обробка інформації відбувається без впроваджених політик резервування, без складових системної підтримки цілісності даних та без формальних правил доступу, що створює ризики втрати, пошкодження або несанкціонованого розголошення інформації.

У процесі ідентифікації вразливостей встановлено, що найкритичнішими ризиками є використання операційних систем без гарантій регулярного оновлення, відсутність формалізованих вимог до захисту кінцевих пристроїв, застосування зовнішніх носіїв без контролю, а також мінімальний рівень журналювання подій у мережі. Враховуючи наявність розподілених структурних підрозділів і необхідність виїзної роботи співробітників, такі ризики стають ще більш значущими, оскільки рух інформації поза межами локальної мережі ускладнює забезпечення її конфіденційності та цілісності.

Окремо проведене оцінювання за допомогою CSET надало кількісну та структуровану картину стану кіберзахисту. Результати продемонстрували низький рівень відповідності ключовим контролям, особливо в доменах політик безпеки, управління конфігураціями, механізмів резервного копіювання, управління доступом та реагування на інциденти. Інструмент також визначив

найбільш проблемні сфери, сформував матрицю ризиків і надав рекомендації щодо першочергових заходів. Це дозволило встановити, що головні проблеми не є технологічними, а носять організаційно-процедурний характер, що є типовим для установ з обмеженим бюджетом та відсутністю спеціалізованих IT-підрозділів.

Загалом проведений аналіз показує, що кібербезпека установи перебуває на початковому рівні зрілості. Попри те, що сама структура мережі є відносно простою та не створює значної поверхні атаки, відсутність проєктного підходу до захисту, формалізованих політик та процедур, а також відсутність системної роботи з ризиками створює передумови для можливих інцидентів із безпеки. Отримані результати формують надійну основу для переходу до наступного етапу – проєктування системи управління інформаційною безпекою (ISMS), що буде розглянуто у розділі 3. Саме на основі висновків цього розділу буде здійснено розробку комплексу заходів, здатних суттєво покращити рівень кіберзахисту досліджуваної установи.

РОЗДІЛ 3 ПРОЄКТУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ (ISMS)

3.1 Концептуальна модель ISMS для установи

Розроблення концептуальної моделі системи управління інформаційною безпекою (ISMS) для державної установи потребує врахування її фактичного технічного стану, особливостей організації роботи, рівня кіберзагроз та результатів проведеного оцінювання за допомогою CSET. Враховуючи відсутність серверної інфраструктури, мінімальну мережеву складність, використання робочих станцій як основних обчислювальних вузлів та нестачу формалізованих політик і процедур, модель ISMS повинна бути адаптована до умов невеликої організаційної структури з обмеженими ресурсами. У такому середовищі ефективність системи управління безпекою досягається не за рахунок складних технологічних рішень, а завдяки чітко визначеним ролям, стандартизованим процесам, зрозумілій документації та уніфікованим правилам взаємодії користувачів із технічними засобами.

Концептуальна модель ISMS базується на циклі PDCA (Plan–Do–Check–Act), який дозволяє впроваджувати безперервне удосконалення практик кіберзахисту. Для установи з описаною інфраструктурою ця модель виступає основою для впорядкування управлінських процесів, підвищення відповідальності працівників за дотримання політик, а також формування зрозумілих вимог до безпеки. Планувальна фаза моделі передбачає визначення цілей, ризиків, політик і процедур. На цьому етапі закладається нормативна основа ISMS, яка включає політики щодо контролю доступу, використання зовнішніх носіїв, управління конфігураціями робочих станцій, ведення журналів подій, резервного копіювання та реагування на інциденти. Висновки CSET, що виявили відсутність документованих процесів, підтверджують нагальну потребу у формуванні цієї бази.

Наступним елементом концептуальної моделі виступає операційна частина, спрямована на практичне застосування визначених процедур. Оскільки установа не використовує серверні рішення, критично важливо зосередитися на захисті кінцевих пристроїв, через які відбувається оброблення та зберігання даних. Модель ISMS передбачає уніфікацію налаштувань операційних систем, установлення обов'язкових правил роботи зі змінними носіями, застосування антивірусного захисту, регулювання доступу до мережевих ресурсів та визначення порядку використання Wi-Fi, якщо його буде введено в експлуатацію. Операційний рівень також включає створення централізованого механізму резервування важливих даних, навіть якщо він здійснюватиметься на зовнішніх носіях або за допомогою локальних копій, враховуючи відсутність серверів чи хмарних рішень [19].

Контрольний компонент моделі зосереджений на моніторингу виконання політик і виявленні порушень, що є особливо важливим у середовищі з підвищеною залежністю від людського фактору. Через обмеженість інфраструктурних можливостей система контролю повинна бути організована таким чином, щоб її підтримка не потребувала складних інструментів. Найважливішими елементами контролю є регулярні внутрішні перевірки, огляди стану робочих станцій, аудит використання зовнішніх носіїв та перевірка відповідності конфігурацій затвердженим вимогам. Результати оцінювання CSET показали низький рівень впровадження механізмів контролю, що підкреслює необхідність систематизації цього процесу в ISMS.

Заключним компонентом концептуальної моделі ISMS є етап коригування, спрямований на удосконалення існуючих процесів і запобігання повторенню інцидентів. Модель передбачає аналіз виявлених порушень, розроблення коригувальних заходів, оновлення політик та навчання персоналу на основі реальних сценаріїв. З огляду на те, що установа має невеликий штат працівників, залучених до роботи з інформаційними системами, процес навчання та підвищення обізнаності може бути впроваджений у форматі регулярних інструктажів, роз'яснювальних матеріалів та коротких семінарів. Такий підхід

дозволяє зміцнити культуру інформаційної безпеки та компенсувати технічні обмеження інфраструктури.

Концептуальна модель ISMS відповідає вимогам, визначеним на основі оцінювання CSET, та створює основу для побудови цілісної системи кіберзахисту. Вона забезпечує інтеграцію управлінських, технічних і організаційних заходів у єдину структуру, що дозволить установі ефективно управляти інформаційними ризиками в умовах обмежених ресурсів. У подальших підрозділах ця модель буде трансформована в конкретні технічні рішення, процедури та засоби контролю, які становитимуть практичний каркас ISMS.

3.2 Програмні та організаційні засоби для впровадження ISMS

Ефективне впровадження системи управління інформаційною безпекою в державній установі потребує комплексного поєднання програмних інструментів, організаційних заходів та процедур, які разом створюють цілісну модель захисту. Враховуючи результати оцінювання CSET, а також особливості IT-інфраструктури установи, описаної у другому розділі, виникає необхідність у впровадженні такої сукупності засобів, яка буде оптимальною для малої установи без розвиненої серверної інфраструктури.

Одним із ключових напрямів є встановлення та використання програмних рішень, що забезпечують базовий і середній рівень захисту кінцевих пристроїв. З огляду на те, що робочі станції фактично виконують функції основних обчислювальних та вузлів збереження даних, особливе значення мають засоби антивірусного захисту, фаєрволи, системи контролю активності користувачів та управління оновленнями. Ефективність таких заходів підтверджується сучасними дослідженнями у сфері побудови систем кіберзахисту, де підкреслюється значення гнучких та багатошарових механізмів захисту навіть у невеликих інформаційних середовищах.

Суттєвим компонентом програмної частини ISMS є механізми журналювання та відстеження подій. У відсутності серверної інфраструктури доцільно використовувати локальні журнали систем Windows, а також додаткові програмні агенти, здатні дублювати критичні події до резервних носіїв або мережевих папок. Крім того, важливо впровадити централізовані правила обліку носіїв інформації, оскільки за результатами оцінювання CSET саме використання зовнішніх носіїв становить один із найвищих ризиків інфікування системи шкідливим програмним забезпеченням. Дослідження щодо методів аналізу мережевого трафіку та виявлення аномальних потоків підтверджують важливість впровадження хоча б мінімальних засобів контролю поведінкових відхилень [20,21].

З огляду на наявність мобільних робочих процесів та виїзної діяльності співробітників, необхідним є застосування інструментів захисту каналів зв’язку, зокрема VPN-рішень, які гарантують цілісність і конфіденційність даних при їх передачі. Використання таких інструментів відповідає сучасним підходам до структуризації безпечного мережевого доступу, описаним у працях з комп’ютерних мереж, де підкреслюється роль захищених тунелів і сегментації потоків у побудові безпечного інформаційного середовища [22].

Не менш важливою складовою є розроблення організаційних заходів, що встановлюють правила, регламенти та процедури інформаційної безпеки. До таких заходів належить створення політик безпеки, які регламентують доступ до ресурсів, порядок користування зовнішніми носіями, правила резервування, стандарти оновлення та реагування на інциденти. У контексті вимог ISO/IEC 27001 такі політики є основою формування культури безпеки, оскільки визначають межі відповідальності кожного працівника та забезпечують передбачуваність роботи системи.

Особливе місце серед організаційних заходів займає підготовка персоналу до роботи в умовах підвищених кіберризиків. Навчання співробітників, моделювання інцидентів, а також використання спеціальних навчальних платформ значно зменшують кількість успішних атак та помилок користувачів.

Подібні симуляційні середовища та кіберполігони активно розвиваються у сучасній системі освіти з кібербезпеки та демонструють високу ефективність при формуванні практичних навичок [23].

Важливим елементом розбудови ISMS є забезпечення захисту конфіденційності даних через використання сучасних криптографічних інструментів. У цьому контексті доцільним є впровадження клієнтських засобів шифрування даних під час обміну файлами, а також систем одноразових або тимчасових ключів для внутрішнього спілкування. Дослідження у сфері захищених систем передачі повідомлень підтверджують, що застосування криптографічних механізмів з нульовою персистентністю та локальним генеруванням ключів суттєво підвищує загальну стійкість інформаційного середовища [24].

Узагальнюючи, програмні та організаційні засоби ISMS мають формувати цілісну структуру, яка захищає інформацію на всіх рівнях: від технічних контролів на кінцевих пристроях до політик, що регламентують поведінку користувачів. Для установи з простою, невеликою та слабо сегментованою інфраструктурою саме поєднання таких засобів дозволяє досягти вимогливого, але реалістичного рівня кіберзахисту без потреби у дорогих або надлишкових рішеннях.

3.3 Формування процедур управління ризиками та інцидентами

Формування процедур управління ризиками та інцидентами в рамках системи управління інформаційною безпекою державної установи є необхідною умовою забезпечення стійкості інформаційної інфраструктури та здатності реагувати на загрози. Ці процедури повинні базуватися на міжнародних стандартах, вимогах законодавства України та враховувати специфіку функціонування установи, зокрема обмеженість технічних ресурсів, відсутність серверної інфраструктури, мобільність персоналу та наявність зовнішніх носіїв.

В основі побудови процесу управління ризиками доцільно використовувати підходи, визначені у стандарті ISO/IEC 27005 «Information Security Risk Management», який описує цілісний цикл роботи з ризиками: ідентифікацію активів, визначення загроз і вразливостей, оцінювання рівня ризику, вибір методів його мінімізації та документування результатів. Важливим елементом є можливість адаптації моделі до установи, де відсутні складні IT-компоненти, а ключові ризики пов’язані з людським фактором, неконтрольованим використанням зовнішніх носіїв, відсутністю резервування та базових політик. Додатково застосовними є методологічні рекомендації NIST SP 800-30 «Guide for Conducting Risk Assessments», які особливо корисні тим, що пропонують структурований підхід до встановлення ймовірності реалізації загрози та оцінювання її впливу.

При формуванні процедури реагування на інциденти використано принципи стандарту ISO/IEC 27035 «Information Security Incident Management», який визначає процеси реєстрації подій, класифікації інцидентів, аналізу першопричин, документування та відновлення нормального функціонування. У контексті досліджуваної установи інцидентами можуть бути не лише кібератаки, а й випадки втрати ноутбука, зараження зовнішнього носія, відмови робочої станції або неправомірного доступу до облікових записів.

Формування процедур управління ризиками також має спиратися на законодавство України, яке регламентує кіберзахист державного сектору. Основоположним документом є Закон України «Про основні засади забезпечення кібербезпеки України», який встановлює обов’язок державних установ забезпечувати організаційні та технічні заходи кіберзахисту. Важливими є й інші документи, такі як Стратегія кібербезпеки України (2021), рекомендації ДСТУ ISO/IEC 27001:2023, а також керівні матеріали Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ), включно з регламентами ведення журналів безпеки, забезпечення резервного копіювання та організації доступу до інформаційних ресурсів. Усі ці норми дозволяють формувати

цілісний підхід, який відповідає як міжнародним практикам, так і національній політиці.

Узгодження процедур управління інцидентами із нормативно-правовою базою забезпечує їх формальну коректність, а залучення сучасних наукових підходів робить систему максимально адаптивною до сучасних кіберзагроз. У результаті формується комплексний процес, який дозволяє не лише ідентифікувати ризики, а й ефективно контролювати їх розвиток, запобігати інцидентам і підвищувати загальний рівень кіберстійкості установи.

3.4 Розробка модулю ISMS з урахуванням результатів CSET

Розробка модуля системи управління інформаційною безпекою (ISMS) для Тернопільської державної сільськогосподарської дослідної станції здійснювалася на основі поглибленого аналізу фактичного стану кіберзахисту та комплексної інтерпретації результатів оцінювання, проведеного за допомогою інструмента Cybersecurity Evaluation Tool (CSET). Отримані результати засвідчили наявність системних прогалин в організаційному, процедурному та технічному забезпеченні інформаційної безпеки, що зумовило необхідність переходу від фрагментарних заходів захисту до формування цілісного, керованого та адаптованого модуля ISMS.

На відміну від суто теоретичного проєктування, у межах даної роботи розробка модуля ISMS розглядається як поєднання концептуальних підходів міжнародного стандарту ISO/IEC 27001, рекомендацій CSET та реальних технічних рішень, які можуть бути впроваджені в умовах обмежених ресурсів державної установи. Такий підхід дозволяє не лише формально описати систему управління, а й продемонструвати її практичну реалізованість і прикладну цінність.

Метою розробленого модуля ISMS є створення цілісної системи управління ризиками, захисту інформаційних активів, контролю доступу, реагування на інциденти, забезпечення безперервності діяльності, журналювання подій та

відповідності вимогам чинного законодавства України у сфері кібербезпеки. Модуль інтегрує пріоритети, визначені CSET, з вимогами стандарту ISO/IEC 27001 та національною нормативно-правовою базою, що забезпечує його юридичну коректність і практичну доцільність що показано в таблиці 3.1.

Таблиця 3.1 – Відповідність CSET → ISO/IEC 27001 → Модуль ISMS

Категорія CSET	**Контролі ISO 27001**	**Реалізація в модулі ISMS**
Управління ризиками	A.6.1, A.8.2, A.15	Реєстр ризиків, карта ризиків, процедура оцінки
Інцидент-менеджмент	A.16	План реагування, журнал інцидентів, IRT
Контроль доступу	A.9	Реєстр користувачів, MFA, політика доступу
Моніторинг і логування	A.12.4	Сервер логів, аналіз журналів, політика аудиту
Резервне копіювання	A.12.3	Графік копій, тестування відновлення
Мережевий захист	A.13	Сегментація, VPN, шифрування WPA3
Захист носіїв	A.8.3	Політика носіїв, шифрування USB
Безперервність	A.17	План аварійного відновлення, UPS

Концептуально модуль ISMS побудований на основі циклу PDCA (Plan–Do–Check–Act), який є фундаментом стандарту ISO/IEC 27001. На етапі планування здійснюється ідентифікація активів, аналіз загроз і вразливостей, оцінка ризиків та формування політик. Етап реалізації охоплює впровадження організаційних, процедурних і технічних заходів. Перевірка передбачає моніторинг, аудит, аналіз журналів подій і контроль ефективності. Етап удосконалення забезпечує коригування політик, процедур та технічних налаштувань з урахуванням нових загроз і результатів повторних оцінювань.

Результати оцінювання CSET показали, що більшість вимог у категоріях Risk Management, Incident Response, Monitoring, Access Control та Continuity Planning або не виконані, або виконані частково. Саме ці напрями були покладені в основу розробки модуля ISMS з урахуванням реального стану IT-інфраструктури установи, яка характеризується використанням операційних систем Windows 7 та Windows 10, відсутністю серверної інфраструктури, мінімальною сегментацією мережі та застосуванням простих мережевих рішень.

Організаційно-нормативна складова модуля ISMS передбачає формування структури управління інформаційною безпекою, яка раніше була відсутня. Запроваджується роль менеджера інформаційної безпеки, відповідального за координацію всіх заходів у сфері захисту інформації, а також створюється Комітет з інформаційної безпеки, до складу якого входять представники керівництва та ключових підрозділів. Формально визначаються власники інформаційних активів, а дані про активи, їх критичність і відповідальних осіб вносяться до Реєстру активів, що стає базовим елементом ISMS.

Нормативна частина модуля включає розроблення повного пакета політик, необхідність яких була підтверджена результатами CSET. До складу модуля входять політики інформаційної безпеки, управління активами, класифікації інформації, управління доступом, використання VPN, бездротових мереж, резервного копіювання, управління інцидентами, контролю зовнішніх носіїв, криптографічного захисту, журналювання та аудиту, а також регламент DNS-фільтрації. Сукупність цих документів формує єдине нормативне поле, у межах якого реалізуються всі технічні та процедурні заходи.

Процедурна частина модуля ISMS зосереджена на впровадженні циклічного управління ризиками відповідно до ISO/IEC 27005. Створюється реєстр ризиків, матриця оцінки ймовірності та наслідків, визначаються методи обробки ризиків і періодичність їх перегляду. Окрему увагу приділено формуванню процесу реагування на інциденти, який раніше в установі був відсутній. Модуль ISMS описує повний життєвий цикл інциденту – від виявлення та реєстрації до

усунення, відновлення та постінцидентного аналізу, що підвищує керованість та прогнозованість дій персоналу.

Ключовою відмінністю розробленого модуля ISMS є наявність практичної технічної складової, реалізованої на основі доступних інструментів. З метою підвищення контролю мережевого трафіку та зниження ризиків фішингових і шкідливих атак було впроваджено DNS-фільтрацію на основі AdGuard Home. Це рішення дозволяє централізовано аналізувати DNS-запити, блокувати шкідливі та небажані домени, вести журнал активності користувачів і виявляти аномальні звернення, що фактично формує базовий рівень мережевого моніторингу.

Для забезпечення захищеного віддаленого доступу співробітників і структурних підрозділів області в модуль ISMS інтегровано використання OpenVPN. Обране рішення підтримує Windows-клієнти та використовує сучасні криптографічні алгоритми, зокрема AES-256-GCM, що забезпечує конфіденційність і цілісність переданих даних. Проведене тестування підтвердило достатній рівень пропускної здатності для виконання службових завдань без суттєвого впливу на продуктивність.

Важливим елементом практичної реалізації ISMS стало впровадження централізованого журналювання подій Windows. Було налаштовано аудит входів і виходів користувачів, змін політик безпеки, доступу до файлів і використання зовнішніх носіїв. Журнали подій зберігаються протягом визначеного періоду та використовуються для аналізу інцидентів і контролю відповідності вимогам ISMS. Це безпосередньо усуває одну з ключових прогалин, зафіксованих у результатах CSET.

Окрему увагу приділено захисту даних шляхом шифрування. У межах модуля ISMS передбачено використання BitLocker для робочих станцій на базі Windows 10 та VeraCrypt для систем Windows 7. Таке рішення забезпечує захист інформації у разі втрати або компрометації носіїв і відповідає вимогам CSET щодо забезпечення конфіденційності.

Практичні зміни в технічній інфраструктурі відображені у схемі мережевої топології «до» та «після» впровадження ISMS показаної на рисунку 3.1.

Рисунок 3.1 – Схема мережевої топології «до» та «після» впровадження ISMS

Початковий стан характеризувався відсутністю сегментації, моніторингу та контролю доступу. Після впровадження модуля ISMS мережа доповнена VPN-

сервером, DNS-сервером із функціями фільтрації, сервером журналювання та логічною сегментацією, що суттєво підвищує керованість і рівень захищеності. Архітектура модуля ISMS, представлена на схемі, наочно демонструє взаємодію організаційно-нормативних, процедурних і технічних компонентів, а також потоки журналів подій між елементами системи.

Після впровадження розробленого модуля ISMS було проведено повторне оцінювання рівня кіберзахищеності за допомогою інструмента CSET, що показано на рисунках 3.2-3.3. В додатку Б наведені додаткові результати оцінювання.

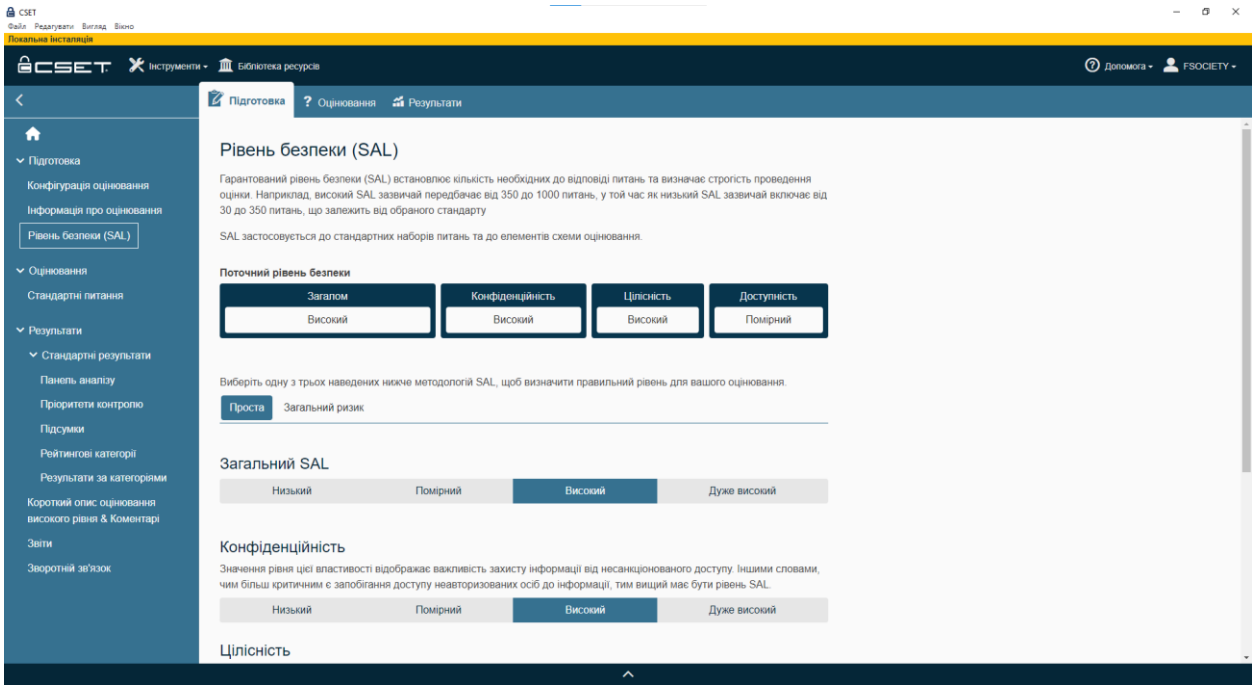

Рисунок 3.2 – Вибір рівня безпеки (SAL)

Повторна оцінка дозволила зафіксувати підвищення рівня відповідності вимогам у ключових категоріях, зокрема управління ризиками, моніторингу, контролю доступу та реагування на інциденти. Отримані результати підтверджують ефективність запропонованих рішень і доцільність використання CSET не лише як інструмента первинного аудиту, а й як засобу контролю результатів упровадження ISMS.

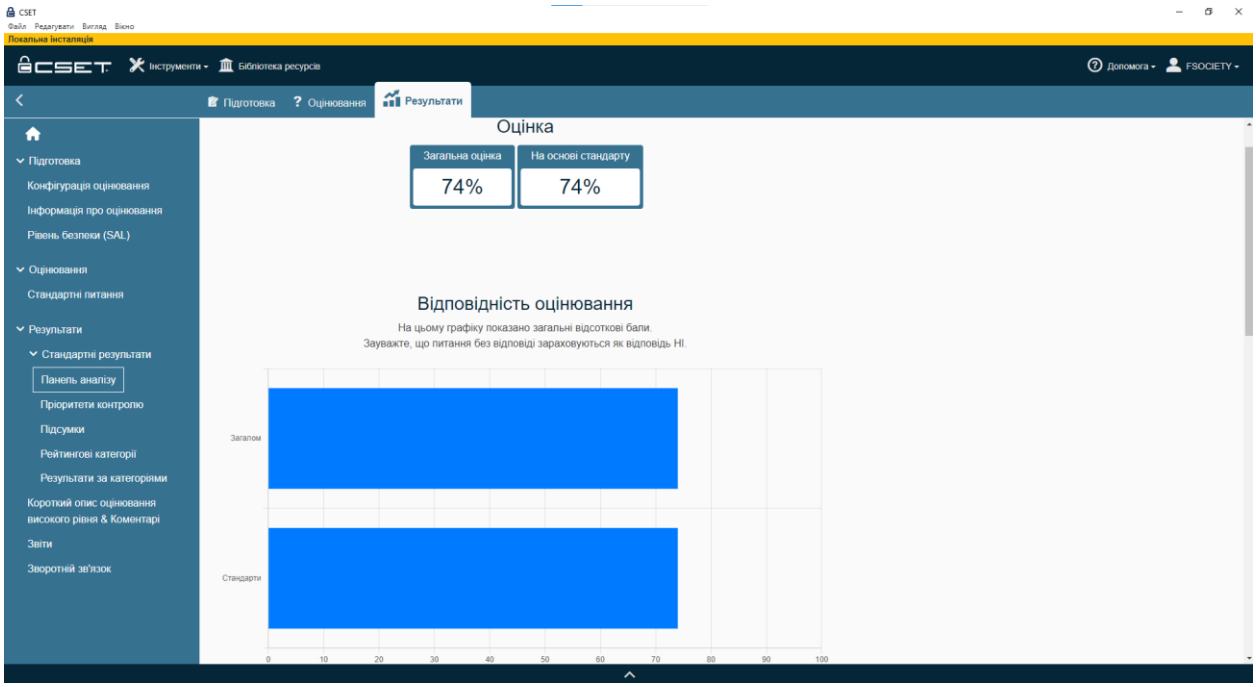

Рисунок 3.3 – Результати оцінювання

Розроблений модуль ISMS є комплексним документом, який інтегрує результати CSET, стандарти ISO/IEC 27001 та вимоги законодавства. Він містить організаційні, процедурні та технічні заходи, спрямовані на підвищення кіберстійкості установи та усунення критичних вразливостей.

Практичне впровадження технічних компонентів ISMS – OpenVPN, AdGuard Home, журналювання Windows, а також системи шифрування – дозволило суттєво посилити безпеку мережі установи навіть без інвестицій у складні серверні рішення.

Практичні тести підтвердили, що VPN забезпечує необхідну пропускну здатність та стійкість шифрування, а DNS-фільтрація значно знижує рівень небажаного та шкідливого трафіку.

Централізоване журналювання підвищило прозорість дій користувачів і створило основу для оперативного розслідування інцидентів.

Усе це дозволило провести повторне оцінювання CSET та отримати значне підвищення рівня відповідності стандартам кібербезпеки.

3.5 Висновки до третього розділу

У третьому розділі було здійснено комплексне проєктування системи управління інформаційною безпекою (ISMS) для Тернопільської державної сільськогосподарської дослідної станції з урахуванням сучасних вимог, міжнародних стандартів та результатів інструментального аудиту CSET. На основі детального аналізу реального стану IT-інфраструктури, виявлених загроз та оцінених ризиків сформовано концептуальну модель ISMS, яка визначає фундаментальні принципи, архітектуру та взаємозв'язки елементів системи. Вона стала основою для розроблення програмних, організаційних та технічних рішень, відповідних специфіці установи та рівня її цифрової зрілості.

У межах розділу було чітко визначено, що ключовими проблемами установи є відсутність нормативних документів у сфері інформаційної безпеки, недостатній рівень контролю доступу, відсутність системної роботи з ризиками, низький рівень моніторингу подій безпеки, застаріла інфраструктура та невпорядковані процедури щодо інцидентів. З урахуванням цих недоліків було сформовано комплекс організаційних засобів, включаючи створення ролей та відповідальностей, формування політик і процедур, налагодження документального забезпечення, а також визначення механізмів взаємодії між підрозділами та персоналом. Це забезпечує впровадження цілісної моделі управління, що охоплює і людей, і процеси, і технології.

Технічні заходи, запропоновані у межах ISMS, ґрунтувалися на даних CSET і передбачали модернізацію мережевої інфраструктури, впровадження механізмів антивірусного захисту та централізованого моніторингу, побудову сегментованої мережі, організацію захищених каналів передачі даних, підвищення рівня журналювання та впровадження базових засобів кіберзахисту. Ці рішення збалансовано поєднують можливості установи та вимоги міжнародних стандартів ISO/IEC 27001, ISO/IEC 27002 і ДСТУ.

Особлива увага була приділена формуванню процесів управління ризиками та інцидентами. На основі рекомендацій CSET та вимог ISO/IEC 27005 було

розроблено адаптовану модель оцінювання ризиків, визначено критерії, створено реєстр ризиків і запропоновано механізми їх регулярного перегляду. Так само було сформовано системну процедуру реагування на інциденти, включаючи порядок реєстрації, обробки, ескалації та відновлення, що забезпечує безперервність діяльності установи та знижує можливий вплив кіберінцидентів.

Ключовим результатом розділу стала розробка модуля ISMS – практично орієнтованої, структурованої та адаптованої моделі впровадження інформаційної безпеки в умовах державної установи з обмеженими ресурсами. Модуль об’єднує організаційні, процедурні та технічні елементи, описує їх взаємодію, містить механізми контролю, відповідності та вдосконалення, а також забезпечує можливість подальшої сертифікації та інтеграції з ширшими системами кіберзахисту. У модулі враховано всі ключові невідповідності, виявлені CSET, та сформовано конкретні шляхи їх усунення.

Отже, розроблена система ISMS створює цілісне середовище управління інформаційною безпекою, підвищує стійкість установи до сучасних кіберзагроз, мінімізує ризики порушення конфіденційності, цілісності та доступності інформації та забезпечує відповідність вимогам національного законодавства і міжнародних стандартів. Сформована архітектура ISMS не лише реагує на наявні проблеми, а й закладає основу для довгострокового розвитку установи в контексті цифрової трансформації та забезпечення її діяльності в умовах зростаючих кіберзагроз.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Під час розроблення та впровадження системи управління інформаційною безпекою державної установи на основі результатів оцінювання Cybersecurity Evaluation Tool (CSET) особлива увага приділяється питанням охорони праці та безпеки життєдіяльності персоналу. Це зумовлено тим, що ефективне функціонування системи інформаційної безпеки неможливе без забезпечення належних, безпечних і здорових умов праці для працівників, які безпосередньо експлуатують інформаційні системи, комп'ютерну техніку та мережеву інфраструктуру. У сучасних умовах людський фактор є одним із ключових елементів як інформаційної безпеки, так і безпеки життєдіяльності, що вимагає комплексного підходу до організації робочого середовища.

Нормативно-правовою основою забезпечення охорони праці в Україні є Закон України «Про охорону праці», який визначає загальні принципи державної політики у цій сфері. У статті 13 зазначеного закону встановлено, що *«роботодавець зобов'язаний створити належні, безпечні і здорові умови праці, забезпечити дотримання вимог законодавства про охорону праці та здійснювати контроль за станом охорони праці»* [25]. Це положення є обов'язковим для всіх підприємств, установ та організацій незалежно від форми власності, у тому числі для державних науково-дослідних установ, де значна частина працівників постійно працює з комп'ютерною технікою та інформаційними ресурсами.

Вимоги щодо створення безпечних умов праці також закріплені у Кодексі законів про працю України. Зокрема, стаття 153 КЗпП визначає, що *«на всіх підприємствах, в установах і організаціях повинні створюватися безпечні і нешкідливі умови праці»* [26]. З огляду на це, при впровадженні системи управління інформаційною безпекою необхідно враховувати не лише технічні

аспекти захисту інформації, але й ергономічні, психофізіологічні та організаційні умови праці персоналу.

Конкретні вимоги до безпеки та захисту здоров'я працівників, які використовують у своїй діяльності комп'ютери та інші екранні пристрої, на сьогодні визначаються нормативно-правовим актом з охорони праці НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я під час роботи з екранними пристроями», затвердженим Міністерством соціальної політики України. У цьому документі зазначено, що *«роботодавець зобов'язаний забезпечити організацію робочих місць з урахуванням ергономічних вимог, характеристик обладнання та умов праці, а також мінімізувати ризики для здоров'я працівників»* [27]. Саме цей нормативний акт є чинним і підлягає застосуванню в державних установах замість застарілих санітарних норм.

Згідно з вимогами НПАОП 0.00-7.15-18, робочі місця працівників, які працюють з комп'ютерною технікою, повинні бути організовані таким чином, щоб зменшувати навантаження на зоровий апарат, опорно-руховий апарат та нервову систему. Особлива увага приділяється розташуванню моніторів, клавіатур, робочих столів і крісел, рівню освітленості, параметрам мікроклімату приміщень, а також режиму праці та відпочинку. Виконання цих вимог є важливим не лише з точки зору охорони праці, але й з позицій інформаційної безпеки, оскільки перевтома та зниження концентрації уваги працівників підвищують імовірність помилок, інцидентів та порушень безпеки.

Закон України «Про забезпечення санітарного та епідеміологічного благополуччя населення» також покладає на роботодавця обов'язок контролювати вплив шкідливих і небезпечних факторів виробничого середовища. У документі визначено, що *«підприємства, установи і організації зобов'язані забезпечувати безпечні умови праці та здійснювати контроль за фізичними, хімічними і біологічними чинниками, які можуть впливати на здоров'я людини»* [28]. Для установ, де використовується значна кількість електронного обладнання, це означає необхідність контролю електромагнітних випромінювань, рівня шуму, температури та вологості повітря.

Важливим аспектом безпеки життєдіяльності є пожежна безпека. Відповідно до Правил пожежної безпеки для установ та організацій, у приміщеннях з комп'ютерною технікою повинні бути забезпечені належні умови експлуатації електромереж, заземлення обладнання, а також наявність первинних засобів пожежогасіння. У правилах зазначено, що *«електроустановки та електропроводка повинні експлуатуватися відповідно до вимог нормативних документів з пожежної безпеки, а персонал має бути проінструктований щодо дій у разі пожежі»* [29]. Дотримання цих вимог є особливо актуальним для державних установ, де зосереджені інформаційні ресурси та технічні засоби.

У міжнародному контексті питання охорони праці регламентуються стандартом ISO 45001:2018 «Occupational health and safety management systems», який встановлює вимоги до системи управління охороною праці та безпекою здоров'я. У стандарті підкреслюється, що *«організація повинна ідентифікувати ризики для здоров'я та безпеки працівників і впроваджувати заходи для їх усунення або мінімізації»* [30]. Положення цього стандарту узгоджуються з концепцією системного управління ризиками, яка використовується і в системах управління інформаційною безпекою.

Міжнародний стандарт ISO/IEC 27001:2022 також акцентує увагу на ролі персоналу в забезпеченні безпеки інформації. У ньому зазначено, що *«організація повинна враховувати людський фактор, компетентність персоналу та умови праці під час планування і впровадження заходів інформаційної безпеки»* [31]. Це підтверджує, що охорона праці та безпека життєдіяльності є невід'ємною складовою ефективної ISMS.

У контексті діяльності Тернопільської державної сільськогосподарської дослідної станції Інституту сільського господарства Карпатського регіону НААН України дотримання вимог охорони праці має особливе значення. Працівники установи виконують значний обсяг робіт з оброблення даних, підготовки звітної документації, аналізу результатів досліджень та взаємодії з інформаційними системами. Тому створення безпечних умов праці сприяє не

лише збереженню здоров’я персоналу, але й підвищенню надійності інформаційних процесів та зменшенню ризиків інформаційних інцидентів.

Отже, при розробленні системи управління інформаційною безпекою на основі результатів оцінки CSET вимоги охорони праці, технічної та пожежної безпеки інтегруються в єдину систему заходів. Такий підхід забезпечує комплексний захист як інформаційних ресурсів, так і працівників державної установи, а також гарантує відповідність діяльності чинному законодавству України та міжнародним стандартам у сфері безпеки.

4.2 Забезпечення безпеки життєдіяльності при роботі з персональним комп’ютером

Робота з персональним комп’ютером є невід’ємною складовою діяльності сучасних державних установ, зокрема науково-дослідних станцій аграрного профілю. Інформаційні технології застосовуються для обробки результатів досліджень, ведення електронної документації, комунікації з центральними органами управління, аналізу даних та підтримки управлінських рішень. Водночас тривале використання комп’ютерної техніки створює комплекс небезпечних і шкідливих факторів, які можуть негативно впливати на здоров’я працівників, що зумовлює необхідність системного підходу до забезпечення безпеки життєдіяльності.

Нормативно-правовою основою забезпечення безпечних умов праці в Україні є Закон України «Про охорону праці». У ньому зазначено, що *«роботодавець зобов’язаний створити належні, безпечні і здорові умови праці, забезпечити дотримання вимог законодавства про охорону праці та здійснювати контроль за їх виконанням»* [25]. Це положення безпосередньо поширюється на організацію робочих місць користувачів персональних комп’ютерів у державних установах.

Кодекс законів про працю України встановлює загальний обов’язок роботодавця щодо створення безпечних і нешкідливих умов праці. У статті 153

КЗпП України зазначено, що *«на всіх підприємствах, в установах і організаціях повинні бути створені безпечні і нешкідливі умови праці»* [26]. Таким чином, при експлуатації комп'ютерної техніки роботодавець зобов'язаний враховувати не лише технічну справність обладнання, але й умови, у яких перебуває працівник у процесі виконання службових обов'язків.

Основними небезпечними та шкідливими факторами при роботі з персональним комп'ютером є:

- напруження зору та зорове стомлення;
- статичні навантаження на опорно-руховий апарат;
- психоемоційні перевантаження;
- електрична небезпека;
- ризик виникнення пожеж через несправність електромереж або обладнання.

Регулювання безпечної експлуатації електрообладнання здійснюється відповідно до вимог НПАОП 40.1-1.21-98 «Правила безпечної експлуатації електроустановок споживачів». У документі наголошується, що *«електроустановки повинні експлуатуватися з дотриманням вимог електробезпеки, а персонал має бути проінструктований щодо дій у разі аварійних ситуацій»* [27]. Це означає необхідність використання справних розеток, заземлення комп'ютерної техніки, заборони самовільного втручання у електромережу та регулярного технічного контролю.

Важливою складовою безпеки життєдіяльності є ергономіка робочого місця. Інструкція з охорони праці при роботі з персональним комп'ютером передбачає, що *«робоче місце користувача ПК повинно бути організоване з урахуванням антропометричних даних працівника та забезпечувати зручну робочу позу»* [32]. Ергономічне робоче місце передбачає регульований стілець, правильне розташування клавіатури, миші та монітора, а також достатній простір для ніг.

Значну роль відіграють психофізіологічні фактори. Тривала робота з інформаційними системами, аналіз великих масивів даних та відповідальність за

результати діяльності можуть призводити до підвищеного рівня стресу. Методичні рекомендації з безпеки життєдіяльності наголошують, що *«організація праці з використанням комп'ютерної техніки повинна враховувати ризики розвитку професійної втоми та емоційного виснаження»* [33]. У зв'язку з цим доцільним є впровадження регламентованих перерв, чергування видів діяльності та оптимізація робочого навантаження.

Питання санітарного та гігієнічного забезпечення регламентуються Законом України «Про забезпечення санітарного та епідеміологічного благополуччя населення», у якому зазначено, що *«умови праці не повинні шкідливо впливати на здоров'я людини»* [28]. Це передбачає підтримання належного мікроклімату приміщень, достатнього рівня освітлення та регулярне провітрювання робочих зон.

Окрему увагу необхідно приділяти пожежній безпеці. Правила пожежної безпеки в Україні встановлюють, що *«у приміщеннях з електронним обладнанням повинні бути передбачені первинні засоби пожежогасіння, а електропроводка має відповідати вимогам нормативних документів»* [29]. Для державних установ це означає обов'язкову наявність вогнегасників, планів евакуації та проведення протипожежних інструктажів.

Важливим елементом забезпечення безпеки життєдіяльності є навчання та інструктаж персоналу. Закон України «Про охорону праці» визначає, що *«працівники повинні проходити інструктажі та навчання з питань охорони праці до початку виконання робіт»* [25]. У контексті роботи з персональним комп'ютером це включає ознайомлення з правилами електробезпеки, пожежної безпеки та правильної організації робочого місця.

У контексті впровадження системи управління інформаційною безпекою на основі результатів оцінки CSET забезпечення безпеки життєдіяльності набуває додаткового значення. Людський фактор є однією з ключових складових кібербезпеки, а фізичне та психічне перевантаження персоналу може призводити до помилок, які створюють загрози для інформаційних ресурсів. Таким чином, заходи з БЖД інтегруються у загальну систему управління ризиками ISMS.

Отже, забезпечення безпеки життєдіяльності при роботі з персональним комп’ютером у державній установі є комплексним завданням, що охоплює правові, організаційні, технічні та санітарно-гігієнічні заходи. Виконання вимог чинних нормативно-правових актів дозволяє мінімізувати ризики для здоров’я працівників та створити безпечні умови праці, що є необхідною передумовою ефективного функціонування системи управління інформаційною безпекою.

ВИСНОВКИ

У межах магістерської роботи виконано комплексне дослідження процесу впровадження системи управління інформаційною безпекою (ISMS) у державній установі на основі результатів оцінки, проведеної за допомогою інструмента CSET. Робота охопила аналіз нормативно-правових засад кібербезпеки, міжнародних стандартів інформаційної безпеки, методологій управління ризиками, а також особливостей функціонування IT-інфраструктури установи. Такий підхід дозволив сформувати цілісну модель підвищення кіберстійкості, що враховує як технічні, так і організаційні аспекти.

У першій частині дослідження систематизовано теоретичні основи побудови ISMS відповідно до ISO/IEC 27001, ISO/IEC 27005, NIST Cybersecurity Framework та інших міжнародних рекомендацій. Особливу увагу приділено ролі автоматизованих інструментів оцінювання, серед яких CSET є одним із найбільш репрезентативних для державного сектору. Обґрунтовано, що застосування CSET дає змогу отримати стандартизований аналіз стану кібербезпеки, визначити пріоритетні напрями підвищення захисту та забезпечити відповідність вимогам національного законодавства.

Другий розділ присвячено детальному аналізу поточного стану кібербезпеки досліджуваної установи. На основі звітів CSET ідентифіковано ключові інформаційні активи, виявлено критичні вразливості, класифіковано загрози та оцінено рівні конфіденційності, цілісності й доступності (SAL). Встановлено, що установа характеризується низьким рівнем формалізації процесів управління інформаційною безпекою, відсутністю політик, слабкою мережевою сегментацією, використанням застарілих операційних систем і недоліками в організації моніторингу, резервного копіювання та інцидент-менеджменту. Результати CSET стали фундаментальною основою для подальшого проєктування ISMS.

У третій частині роботи сформовано та розроблено модуль ISMS, що охоплює організаційний, технічний і процедурний рівні управління безпекою.

Модуль створений з урахуванням вимог міжнародних стандартів, положень національного законодавства та конкретних рекомендацій, сформованих інструментом CSET. Запропонований модуль включає структуру управління кібербезпекою, комплекс політик, процедури управління ризиками, інцидентами, резервним копіюванням, доступом, моніторингом, а також технічні заходи модернізації мережевої інфраструктури та засобів захисту. Особливістю даного модуля є адаптація заходів ISMS до умов малоресурсної державної установи, що дозволяє оптимізувати витрати та підвищити ефективність впровадження.

Результати дослідження свідчать, що інтеграція оцінювання за CSET у процес проєктування ISMS забезпечує високу точність визначення пріоритетів, скорочує час на проведення аудиту, покращує якість управлінських рішень та сприяє формуванню системного підходу до кіберзахисту. Запропонований у роботі модуль ISMS може бути використаний як типова модель для інших державних установ, які мають подібну структуру IT-інфраструктури та ресурсні обмеження.

Підсумовуючи, слід зазначити, що поставлена мета роботи досягнута: на основі результатів оцінювання CSET створено ґрунтовний, адаптований під потреби державної установи модуль ISMS, який забезпечує підвищення рівня інформаційної безпеки, формує передумови для подальшої сертифікації за ISO/IEC 27001 та сприяє розвитку культури кібербезпеки на рівні організації. Одержані результати мають практичну цінність та можуть бути використані для підготовки політик, внутрішніх регламентів, планування розвитку IT-інфраструктури та забезпечення кіберстійкості державного сектору в умовах зростання кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України». (2017).
2. Постанова Кабінету Міністрів України № 373 «Про затвердження Порядку забезпечення технічного захисту інформації». (2006).
3. Державна служба спеціального зв'язку та захисту інформації України. (2017). Наказ № 600 «Про затвердження вимог з технічного захисту інформації».
4. Закон України «Про захист персональних даних». (2010).
5. Стратегія кібербезпеки України. (2021).
6. International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems – Requirements.
7. National Institute of Standards and Technology. (2020). NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations.
8. National Institute of Standards and Technology. (2018). NIST Cybersecurity Framework (Version 1.1).
9. International Electrotechnical Commission. (2018). IEC 62443: Industrial communication networks – IT security for networks and systems.
10. U.S. Department of Homeland Security. (2023). Cybersecurity Evaluation Tool (CSET).
11. Center for Internet Security. (2021). CIS Controls v8.
12. Greenbone Networks. (2022). OpenVAS – Open Vulnerability Assessment System.
13. Tenable Network Security. (2023). Nessus Professional.
14. Mataracioglu, T., & Ozkan, S. (n.d.). Governing Information Security in Conjunction with COBIT and ISO 27001. arXiv.
15. Alencar, G. D., de Moura, H. P., et al. (2018). An adaptable maturity strategy for information security. arXiv.

16. Міністерство освіти і науки України. (n.d.). Навчальні матеріали щодо стандартів COBIT, ITIL, ISO/IEC.

17. DQS Global. Управління конфігурацією в інформаційній безпеці.

18. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S., et al. (2021). Synergy of building cybersecurity systems. PC Technology Center. https://doi.org/10.15587/978-617-7319-31-2

19. Malyuta Y., Derkach M., Lobur T. (2025). Modeling a Fog Computing Network Architecture for Secure IoT Data Processing. Security of Infocommunication Systems and Internet of Things, vol 3, no 2.

20. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., & Lechachenko, T. (2024). Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings, 3896, 1–11.

21. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. Комп'ютерні мережі. Книга 1 [навчальний посібник] - Львів, "Магнолія 2006", 2013. - 256 с.

22. Микитишин А. Г., Митник М. М., Стухляк П. Д., Пасічник В. В. Комп’ютерні мережі. Книга 2. [навчальний посібник]. Львів : "Магнолія 2006", 2014. 312 с.

23. Mishko, O., Matiuk, D., & Derkach, M. (2024). Security of remote IoT system management by integrating firewall configuration into tunneled traffic. Вісник Тернопільського національного технічного університету, 115(3), 122–129.

24. Tymoshchuk, D., & Yatskiv, V. (2024). Using hypervisors to create a cyber polygon. Measuring and Computing Devices in Technological Processes, (3), 52–56. https://doi.org/10.31891/2219-9365-2024-79-7

25. Derkach, M., Matiuk, D., Skarga-Bandurova, I., & Zagorodna, N. (2025). CrypticWave: A zero-persistence ephemeral messaging system with client-side encryption.

26. Lechachenko, T., Gancarczyk, T., Lobur, T., & Postoliuk, A. (2023). Cybersecurity Assessments Based on Combining TODIM Method and STRIDE Model for Learning Management Systems. In CITI (pp. 250-256).

27. Ревнюк, О. А., & Загородна, Н. В. (2024). МЕТОДОЛОГІЯ КІЛЬКІСНОЇ ОЦІНКИ ЗАХИЩЕНОСТІ ВЕБДОДАТКУ ЕЛЕКТРОННОЇ КОМЕРЦІЇ НА

ЕТАПІ ЕКСПЛУАТАЦІЇ. Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas, (2 (57)), 107-119.

28. Boltov, Y., Skarga-Bandurova, I., & Derkach, M. (2023, September). A Comparative Analysis of Deep Learning-Based Object Detectors for Embedded Systems. In 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (Vol. 1, pp. 1156-1160). IEEE.

29. Revniuk O.A., Zagorodna N.V., Kozak R.O., Karpinski M.P., Flud L.O. "The improvement of web-application SDL process to prevent Insecure Design vulnerabilities". Applied Aspects of Information Technology. 2024; Vol. 7, No. 2: 162–174.

30. Stadnyk, M., & Palamar, A. (2022). Project management features in the cybersecurity area. Вісник Тернопільського національного технічного університету, 106(2), 54-62.

31. Закон України «Про охорону праці» від 14.10.1992 № 2694-XII (зі змінами та доповненнями).

32. Кодекс законів про працю України (КЗпП), чинна редакція.

33. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я під час роботи з екранними пристроями».

34. Закон України «Про забезпечення санітарного та епідеміологічного благополуччя населення» від 24.02.1994 № 4004-XII.

35. Правила пожежної безпеки в Україні, чинна редакція.

36. ISO 45001:2018 Occupational health and safety management systems – Requirements with guidance for use.

37. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements.

38. Інструкція з охорони праці при роботі з персональним комп'ютером.

39. Магдисюк Л. Безпека життєдіяльності та охорона праці: методичні рекомендації.

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

XIII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

17-18 грудня 2025 року

ТЕРНОПІЛЬ
2025

Продовження додатку А

УДК 004.056
Іван Містерман, магістр
Тернопільський національний технічний університет імені Івана Пулюя

ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВНОЇ УСТАНОВИ НА ОСНОВІ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ CSET

Ivan Misterman, master

IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM IN A STATE INSTITUTION BASED ON CSET ASSESSMENT RESULTS

У роботі розглянуто науково-практичний підхід до формування та впровадження системи управління інформаційною безпекою (ISMS) у державній установі з використанням результатів інструментальної оцінки Cybersecurity Evaluation Tool (CSET). У сучасних умовах цифровізації, коли державні установи активно взаємодіють з інформаційними ресурсами та обробляють значні обсяги даних, питання забезпечення конфіденційності, цілісності та доступності інформації набуває стратегічного значення. Відповідно, застосування CSET дає змогу отримати структуровану й методично обґрунтовану оцінку кіберзахищеності, визначити ключові вразливості, а також співвідносити їх із вимогами міжнародних стандартів ISO/IEC 27001, NIST CSF та чинного законодавства України.

На основі аналізу звітів CSET ідентифіковано критичні розриви в управлінні ризиками, організації інцидент-менеджменту, контролі доступу, веденні журналів подій, захисті мережевої інфраструктури та у відсутності формальних політик інформаційної безпеки. Встановлено, що рівень конфіденційності, цілісності та доступності інформаційних активів установи відповідає низькому показнику SAL Low, що вимагає комплексної модернізації системи безпеки.

У межах роботи розроблено модуль ISMS, який включає організаційні, процедурні та технічні компоненти. Організаційна складова охоплює створення політик ІБ, визначення відповідальних осіб, формування Комітету інформаційної безпеки та розробку системи управління ризиками згідно з ISO/IEC 27005. Процедурний блок містить механізми управління інцидентами, регламенти резервного копіювання та відновлення, правила контролю доступу та моніторингу. Технічна складова модулю представлена заходами з модернізації мережевої інфраструктури, впровадженням захищених протоколів, централізованим антивірусним захистом, сегментацією мережі й побудовою системи збору та аналізу журналів безпеки.

Отримані результати мають практичну цінність для впровадження комплексної системи управління інформаційною безпекою в державних організаціях. Запропонований підхід може бути адаптований до інших установ подібного профілю та забезпечує підвищення рівня кіберстійкості, зменшення впливу ризиків кіберзагроз і формування відповідності вимогам національних та міжнародних нормативів інформаційної безпеки.

Література

1. CSET — Cybersecurity Evaluation Tool. U.S. Department of Homeland Security, 2023.
2. ISO/IEC 27001:2022 Information Security Management Systems — Requirements.
3. Закон України «Про основні засади забезпечення кібербезпеки України», 2017.

Додаток Б Детальні результати повторної оцінки

Рис Б.1 – Найпоширеніші проблемні сфери

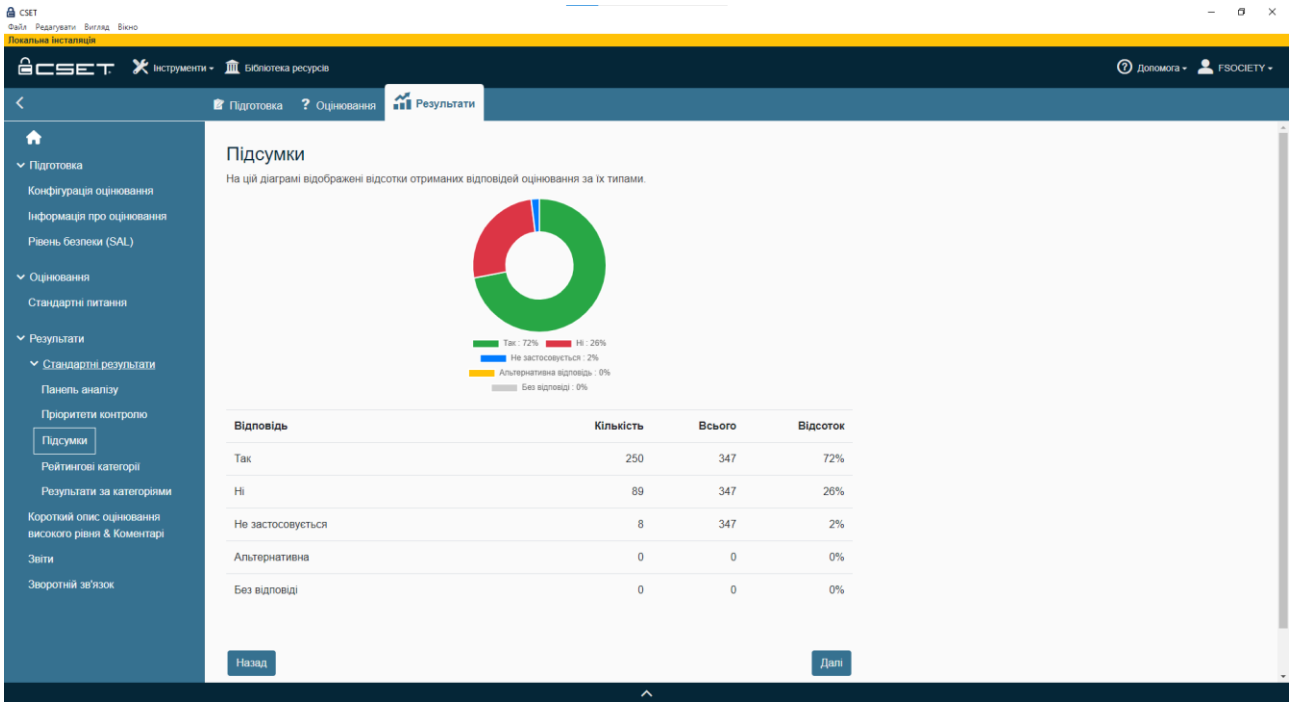

Рис Б.2 – діаграма підсумку відповідей

Продовження додатку Б

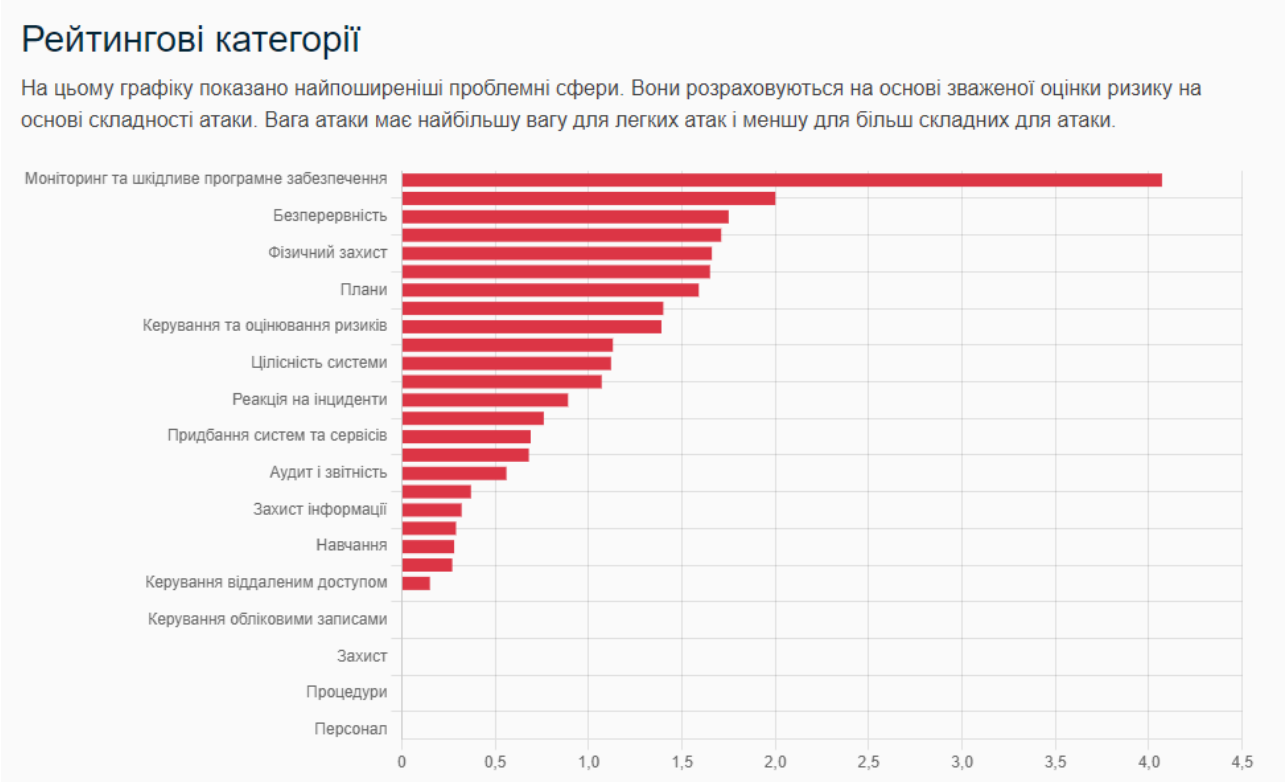

Рис Б.3 – Найпоширеніші проблеми сфери

Рис Б.4 – індивідуальні бали для кожної категорії з позитивної точки зору