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: "Удосконалення системи кіберзахисту освітнього центру із використанням відкритих інструментів"

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека та захист інформації»
(шифр і назва напряму підготовки, спеціальності)
Ластівка Галина Іванівна
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 Яцишин В.В.
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 Ластівці Галині Іванівні
(прізвище, ім'я, по батькові)

1. Тема роботи Удосконалення системи кіберзахисту освітнього центру із використанням відкритих інструментів

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

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1025

2. Термін подання студентом завершеної роботи 12.12.2025

3. Вихідні дані до роботи ІКТ Центру цифрової трансформації ЧНУ, вразливості та методи їх усунення.

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ
Розділ 1. ІКС-інфраструктура Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича
Розділ 2. Оцінка поточного рівня захищеності Центру цифрової трансформації
Розділ 3. Удосконалення системи кіберзахисту освітнього центру
Розділ 4. Охорона праці та техніка безпеки в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Актуальність дослідження. Мета, обєкт, предмет . Завдання, наукова та практична новизна. Архітектура та топологія мережі ІКС. Сегментація VLAN в ІКС. Характеристика основних серверів Центру. Нормативно-правова база для аудиту інформаційної безпеки вебресурсів. Методи і підходи до проведення аудиту безпеки. Аналіз сучасних інструментів аудиту безпеки. Результати первинного аудиту безпеки Центру. Оцінка відповідності ІКС Центру міжнародним стандартам безпеки. Аналіз організаційних і технічних заходів забезпечення кібербезпеки ІКС. Оцінка ефективності після удосконалення системи кіберзахисту. Результати повторного тестування ІКС та їх аналіз. Висновки.

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.	Визначення основних характеристик ІКС Центру	23.09 – 1.10	Виконано
3.	Проведення аналізу архітектури ІКТ-системи та оцінювання її захищеності	2.10 – 12.10	Виконано
4.	Проведення аналізу інструментів для сканування та тестування	13.10 – 24.10	Виконано
5.	Проведення первинного аудиту вразливостей ІКС Центру	25.10 – 2.11	Виконано
6.	Проведення аналізу організаційних і технічних заходів забезпечення кібербезпеки ІКС	3.11 – 10.11	Виконано
7.	Впровадження багаторівневий захист відповідно до моделі Defense in Depth в ІКС	11.11 – 20.11	Виконано
8.	Розробка автоматизованого агрегатора вразливостей	21.11 – 27.11	Виконано
9.	Проведення оцінки ефективності захисту після удосконалення системи кіберзахисту ІКС	28.11 – 1.12	Виконано
10.	Аналіз результатів аудиту безпеки та підведення підсумків	2.12 – 7.12	Виконано
11.	Розгляд питань з охорони праці та техніки безпеки в надзвичайних ситуаціях	08.12 – 10.12	Виконано
12.	Перевірка на плагіат	12.12 – 14.12	Виконано
13.	Попередній захист кваліфікаційної роботи	15.12 – 19.12	Виконано
14.	Захист кваліфікаційної роботи	24.12.2025	

Студент _____ Ластівка Г.І.
(підпис) (прізвище та ініціали)

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

АНОТАЦІЯ

Удосконалення системи кіберзахисту освітнього центру із використанням відкритих інструментів // ОР «Магістр» // Ластівка Галина Іванівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБмз-61 // Тернопіль, 2025 // С. 84, рис. – 19, табл. – 24, кресл. – 18, додат. – 1.

Ключові слова: кібербезпека, інформаційно-комунікаційні системи, кіберзахист, агрегатор вразливостей, відкриті інструменти аудиту, Python.

У кваліфікаційній роботі магістра розроблено рішення багаторівневого захисту, на основі інтеграції сучасних методів аналізу вразливостей, систем управління подіями безпеки та хмарних рішень, застосування якого підвищило загальний рівень кіберстійкості ІКС Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича, що відповідає міжнародним стандартам ENISA 2024 та ISO/IEC 27001:2022.

У першому розділі роботи розглянута багаторівнева архітектура ІКС Центру. Досліджено механізми шифрування, моніторингу й контролю доступу до локальних серверних потужностей та хмарних сервісів Google Workspace.

У другому розділі проведений аналіз сучасних відкритих інструментів аудиту інформаційної безпеки та виконаний первинний аудит безпеки ІКС Центру, виявлені вразливості та визначені шляхи їх усунення.

У третьому розділі за допомогою розробленого агрегатора вразливостей було проведено повторне фінальне сканування та моніторинг безпеки ІКС Центру після впровадження методів захисту, результати якого підтверджують значне покращення стану кіберзахисту.

Результати використання відкритих систем (Wazuh, ELK Stack) у поєднанні з хмарними сервісами Google Workspace, також підтвердили й економічну доцільність застосування таких рішень.

ABSTRACT

Improvement of the Cybersecurity System of the Educational Center Using Open Tools // Thesis of educational level "Master"// Halyna Lastivka // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cybersecurity, group СБмз-61 // Ternopil, 2025 // p. 84, figs. 19, tbls 24, drws. 18, apps. – 1.

Keywords: cybersecurity, information and communication systems, cyber defense, vulnerability aggregator, open audit tools, Python.

The master's thesis develops a multi-level protection solution based on the integration of modern vulnerability analysis methods, security event management systems, and cloud solutions. Implementation of this solution has increased the overall level of cyber resilience of the ICS of the Digital Transformation Center at Yuriy Fedkovych Chernivtsi National University, which complies with international standards ENISA 2024 and ISO/IEC 27001:2022.

The first section of the work provides an overview of the multi-level architecture of the Center's ICS. The implemented mechanisms for encryption, monitoring, and control of access to local server capacities and Google Workspace cloud services are examined.

In the second section, an analysis of modern open information security audit tools is conducted, and an initial security audit of the Center's ICS is performed, vulnerabilities are identified, and ways to eliminate them are determined.

In the third section, using the developed vulnerability aggregator, a final rescan and security monitoring of the Center's ICS was performed after the implementation of protection methods, the results of which confirm a significant improvement in the state of cyber protection.

In addition, the results of using open systems (Wazuh, ELK Stack) in combination with Google Workspace cloud services also confirmed the economic feasibility of such solutions.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACL — Access Control List

BCP — Business Continuity Planning

CSIRT — Computer Security Incident Response Team

DLP — Data Loss Prevention

DMZ — Demilitarized Zone

DPI — Deep Packet Inspection

DWDM — Dense Wavelength Division Multiplexing

ENISA — European Union Agency for Network and Information Security

GCDS — Google Cloud Directory Sync

GDPR — General Data Protection Regulation

IDS/IPS — Intrusion Detection System/ Intrusion Prevention System

IRP — Incident Response Plan

ISMS — Information Security Management System

KSI — Key Security Indicators

MFA — Multi-Factor Authentication

NGFW — Next-Generation Firewall

NIST — National Institute of Standards and Technology

OWASP — Open Web Application Security Project

RBAC — Role-Based Access Control

SIEM — Security Information and Event Management

SSO — Single Sign-On

VLAN — Virtual Local Area Network

ZAP — Zed Attack Proxy

ІКС — Інформаційно-комунікаційні системи

ОС — Операційна система

ПЗ — Програмне забезпечення

ПК — Персональний комп’ютер

СМІБ — Система менеджменту інформаційної безпеки

СУБД — Система управління базами даних

ВСТУП

Актуальність. У сучасних умовах цифрової трансформації суспільства інформаційна безпека набуває стратегічного значення для стабільного функціонування освітніх, наукових та адміністративних структур. Зростання обсягів даних, поширення хмарних сервісів і віддаленого доступу створюють нові виклики для кіберзахисту інформаційно-комунікаційних систем (ІКС). Особливої актуальності питання безпеки набувають у закладах вищої освіти, де одночасно функціонує велика кількість користувачів, серверів, баз даних та мережевих вузлів.

Згідно з дослідженнями Європейського агентства з кібербезпеки (ENISA) [1], понад 80% інцидентів у сфері освіти пов’язані з людським фактором, неправильним налаштуванням доступів або використанням застарілих версій програмного забезпечення. Додатково, за даними звіту Cybersecurity Education Sector Threat Landscape 2024, заклади освіти дедалі частіше стають об’єктом атак типу ransomware, phishing та DDoS [2-4]. Це вимагає системного підходу до аналізу вразливостей і розроблення методів їх усунення.

Одним із ключових об’єктів дослідження у цій сфері є ІКС-інфраструктура Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича, яка забезпечує реалізацію освітніх, наукових і адміністративних процесів на базі цифрових сервісів.

Актуальність теми кваліфікаційної роботи зумовлена необхідністю підвищення рівня кіберзахисту освітніх інформаційних систем, удосконалення механізмів моніторингу загроз, а також впровадження адаптивних методів виявлення та нейтралізації вразливостей. Дослідження базується на практичному аналізі структури та технічних компонентів ІКС Центру цифрової трансформації, що дає можливість виявити реальні проблеми безпеки й обґрунтувати ефективні шляхи їх усунення.

Мета роботи – удосконалити рівень захисту інформаційно-комунікаційної системи Центру цифрової трансформації Чернівецького національного

університету імені Юрія Федьковича, тобто розробити практичні методи усунення вразливостей з урахуванням сучасних тенденцій у сфері кіберзахисту.

Завдання дослідження:

1. Здійснити аналіз структури та архітектури ІКС Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича.
2. Провести оцінку поточного рівня захищеності ІКС Центру цифрової трансформації.
3. Удосконалити систему кіберзахисту освітнього центру.
4. Провести оцінку рівня захищеності ІКС після удосконалення.

Об’єкт дослідження – інформаційно-комунікаційна система Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича.

Предмет дослідження – вразливості, загрози та методи захисту компонентів ІКС-інфраструктури освітньої установи.

Методи дослідження включають аналіз нормативно-правової бази, порівняльний аналіз архітектури мережевих систем, методи етичного хакінгу, сканування вразливостей (Nmap, Nessus, Burp Suite, Metasploit), аналітичне моделювання ризиків, а також методи оцінювання відповідності вимогам міжнародних стандартів ISO/IEC 27001, ISO/IEC 27005 та NIST SP 800-53.

Наукова новизна полягає у реалізації інтегрованого підходу щодо усунення вразливостей освітніх ІКС шляхом поєднання технічних, організаційних і криптографічних методів захисту.

Практичне значення полягає у можливості застосування результатів роботи для вдосконалення політики інформаційної безпеки в ІКС-інфраструктурі Центру цифрової трансформації та аналогічних освітніх закладів України. Практичні результати даної кваліфікаційної роботи будуть спрямовані на підвищення рівня безпеки освітнього цифрового середовища, зменшення ризиків несанкціонованого доступу до даних, а також формування рекомендацій щодо оптимізації механізмів кіберзахисту відповідно до сучасних

світових стандартів ІКС Черновецького національного університету імені Юрія Федьковича.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: IV міжнародній конференції з кібергігієни та управління конфліктами в глобальних інформаційних мережах (м.Київ, Україна).

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

РОЗДІЛ 1 ІКС-ІНФРАСТРУКТУРА ЦЕНТРУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЧЕРНІВЕЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

1.1 Характеристика інформаційно-комунікаційної системи Центру цифрової трансформації

Інформаційно-комунікаційна система Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича є ключовою складовою цифрової інфраструктури університету, що забезпечує функціонування інформаційних сервісів навчального, наукового та адміністративного призначення. Її архітектура побудована з урахуванням принципів масштабованості, надійності та безпеки, що дозволяє підтримувати безперервність освітніх процесів та інтеграцію з національними і міжнародними цифровими платформами [5-7].

Центр цифрової трансформації виступає структурним підрозділом університету, який виконує функції управління ІКС-інфраструктурою, адміністрування інформаційних ресурсів, забезпечення кібербезпеки, розроблення і впровадження новітніх цифрових технологій у навчальний процес. Основними напрямами діяльності Центру є підтримка корпоративних мережевих сервісів, адміністрування локальних мереж факультетів і кафедр, забезпечення безпечного підключення до Інтернету, управління системами електронного документообігу, дистанційного навчання та комунікації між підрозділами університету.

ІКС Центру складається з трьох основних рівнів: інфраструктурного (апаратного), програмного та організаційно-нормативного.

На інфраструктурному рівні реалізовано комплекс серверних і мережевих рішень, що забезпечують обробку, зберігання та передавання даних. Основу становить трирівнева Cisco-подібна архітектура (Core-Distribution-Access) [8], що гарантує відмовостійкість і балансування навантаження. Рівень ядра (Core) представлений високопродуктивними комутаторами Cisco Catalyst 9500 та

Arista 7050X, які об’єднують усі корпуси університету в єдину оптоволоконну магістраль зі швидкістю передавання даних до 25 Gbps. Канали резервовані за протоколом Rapid-PVST+, що забезпечує час конвергенції менше однієї секунди при зміні топології. Рівень розподілу (Distribution) формує сегментацію VLAN для ізоляції трафіку між адміністративними, навчальними та дослідницькими мережами. На рівні доступу (Access) функціонують комутатори Cisco Catalyst 9200 та HPE Aruba 2930F із підтримкою PoE+, які забезпечують живлення для точок доступу Wi-Fi, IP-телефонів та камер відеоспостереження.

Серверна інфраструктура Центру базується на фізичних серверах Dell PowerEdge R740 та HP ProLiant DL380 Gen10, що підтримують віртуалізацію на платформах VMware ESXi та Hyper-V. Сервери об’єднані у кластерну систему з підтримкою резервування та балансування навантаження. На них функціонують критичні сервіси – корпоративна електронна пошта (Exchange 2019), файлові сховища (Windows Server 2019 DFS), база даних (PostgreSQL, MySQL), а також вебпортали університету, реалізовані на Nginx і Apache. Для управління даними використовується SAN-сховище з реалізацією політики багаторівневого резервування [10, 11]. Резервне копіювання здійснюється засобами Veeam Backup та Acronis із дотриманням принципу “3-2-1”: три копії даних, дві на різних носіях, одна – поза основною локацією.

Мережеве підключення Центру організовано через два незалежні провайдери – «Уарнет» (науково-освітня мережа NREN України) та «Укртелеком», що забезпечує BGP-маршрутизацію та відмовостійкий доступ до Інтернету. Для підвищення рівня безпеки на периметрі встановлено NGFW-брандмауери FortiGate та Cisco ASA у кластері Active-Active, які виконують функції глибокого аналізу трафіку (DPI), SSL-інспекції, виявлення вторгнень (IDS/IPS) та фільтрації запитів. Контроль автентифікації адміністраторів здійснюється за протоколами RADIUS та TACACS+, що дозволяє вести централізований облік дій користувачів [12-13].

Програмне забезпечення ІКС включає як комерційні, так і open-source рішення. Основними операційними системами є Windows Server 2019, Ubuntu

22.04 LTS та Kali Linux. Серед основних платформ і сервісів використовуються Moodle для електронного навчання, Nextcloud для спільної роботи, Microsoft 365 Education, Google Workspace for Education та системи керування базами даних PostgreSQL і MS SQL. Для контролю стану мережі та системного журналювання використовується Splunk Enterprise, Zabbix, а також SIEM-модулі, інтегровані з антивірусними рішеннями ESET Protect і CrowdStrike Falcon.

Безпекова складова ІКС реалізована з урахуванням принципу глибокоешелонованого захисту (Defense-in-Depth). Вона включає комбінацію організаційних, технічних і криптографічних засобів забезпечення конфіденційності, цілісності та доступності даних. Захист інформаційних активів здійснюється на всіх рівнях: від фізичного захисту серверних приміщень до контролю трафіку, автентифікації користувачів, журналювання подій і резервування систем. Для шифрування даних у транспортному середовищі використовується TLS 1.3, для захисту збережених даних – AES-256. Впроваджено двофакторну автентифікацію (2FA) через апаратні токени та мобільні додатки, а також централізовану політику складних паролів.

Організаційна модель інформаційної безпеки Центру цифрової трансформації ґрунтується на нормативно-правових актах України, зокрема Законі України «Про основні засади забезпечення кібербезпеки України» (2017), Національній стратегії кібербезпеки на 2023-2027 роки [9], а також внутрішніх регламентах університету. Документаційна база включає політику управління ризиками, політику контролю доступу, порядок реагування на інциденти (IRP), регламент резервного копіювання та план безперервності діяльності (BCP). Працівники Центру проходять щорічне навчання з кібергігієни, а також участь у тренінгах з виявлення соціальної інженерії та фішингових атак.

Окрему увагу приділено забезпеченню безпеки веб-застосунків. Центр впровадив практики безпечної розробки програмного забезпечення згідно з рекомендаціями OWASP Secure Coding Practices [2]. Сайти університету функціонують на основі CMS WordPress та Joomla, які регулярно оновлюються,

проходять тестування на наявність XSS-, CSRF- та SQL-ін’єкцій. Зовнішні сервіси ізольовано у демілітаризованій зоні (DMZ), що мінімізує ризик проникнення до внутрішніх ресурсів у разі компрометації публічних серверів.

Організаційна структура управління ІКС передбачає розмежування повноважень між адміністраторами мереж, системними інженерами, фахівцями з інформаційної безпеки та аналітиками. Кожна категорія користувачів має обмежений набір привілеїв відповідно до принципу найменших прав (Least Privilege). Централізована система управління доступом на базі Active Directory дозволяє відстежувати дії користувачів, аналізувати аномальну активність і запобігати несанкціонованим спробам входу.

Для підвищення ефективності адміністрування ІКС використовується система моніторингу Zabbix, яка контролює стан обладнання, навантаження серверів, трафік мережі та інциденти безпеки. Система SIEM Splunk здійснює аналіз подій у реальному часі, кореляцію даних із мережевих пристроїв, серверів і систем автентифікації. Це дозволяє своєчасно виявляти спроби вторгнень, DDoS-атаки або внутрішні порушення безпеки.

Таким чином, інформаційно-комунікаційна система Центру цифрової трансформації є комплексним технологічним середовищем, що об’єднує сучасні апаратно-програмні засоби та методи кіберзахисту. Вона відповідає вимогам міжнародних стандартів безпеки, підтримує високий рівень надійності та адаптивності, а її організаційна модель забезпечує ефективне управління цифровими ризиками. Завдяки багаторівневій архітектурі, впровадженню автоматизованих засобів моніторингу та нормативній підтримці ІКС Центр створює передумови для безпечного функціонування університетського цифрового середовища та стійкості до сучасних кіберзагроз.

1.2 Архітектура та топологія мережі ІКС

Архітектура інформаційно-комунікаційної системи (ІКС) Центру цифрової трансформації побудована на принципах модульності, масштабованості та відмовостійкості. Вона забезпечує безперервне функціонування цифрових

сервісів університету, доступ до освітніх ресурсів, хмарних платформ, навчальних систем і внутрішніх баз даних. Основне завдання архітектури полягає у забезпеченні стабільної взаємодії між користувачами, серверами й мережевими компонентами з одночасним дотриманням високого рівня інформаційної безпеки.

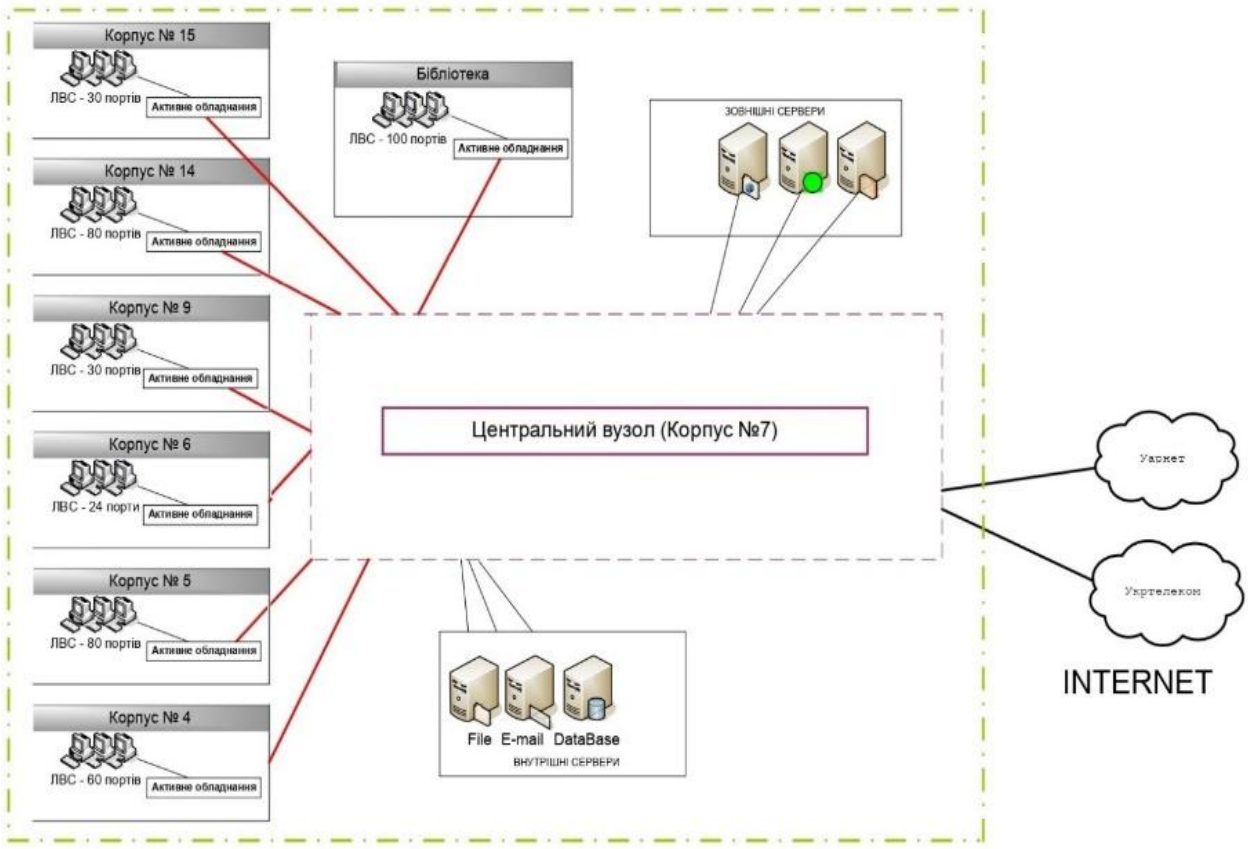

Рисунок 1.1 – Топологія мережі Центру

ІКС-інфраструктура Центру складається з трьох основних рівнів – ядра (Core Layer), рівня розподілу (Distribution Layer) та рівня доступу (Access Layer). Така модель відповідає рекомендаціям Cisco Enterprise Network Design Guide і забезпечує логічний поділ функцій маршрутизації, комутації та управління трафіком [8, 14].

Мережа Центру має гібридну топологію типу *зірка + кільце* (Hybrid Star-Ring) (рисунок 1.1), де центральний вузол управління розташований у корпусі №7 університету. Основу магістралі становлять комутатори Cisco Catalyst 9500, об’єднані в кластер StackWise Virtual, що гарантує високу пропускну здатність (до 6 Tbps) і відмовостійкість.

Між корпусами університету розгорнуто оптичну магістраль на базі технології DWDM із пропускною здатністю 10-25 Gbps.

Для резервування каналів використовується протокол Rapid PVST+, який автоматично створює альтернативний маршрут і відновлює зв’язок за час менше 1 секунди.

На рівні Distribution Layer функціонують комутатори Cisco Catalyst 9300 та MikroTik CRS326, які реалізують VLAN-сегментацію, маршрутизацію між підмережами та застосування списків контролю доступу (ACL).

Таблиця 1.1 – Сегментація VLAN в ІКС Центру цифрової трансформації

VLAN ID	Призначення сегменту	Користувачі/системи	Рівень доступу
VLAN 10	Адміністративна мережа	Керівництво, бухгалтерія, відділи кадрів	Обмежений, із доступом до ERP
VLAN 20	Сервери баз даних	PostgreSQL, MS SQL, Backup SAN	Локальний доступ через VPN
VLAN 30	Демілітаризована зона (DMZ)	Web-портали, DNS, VPN-шлюзи	Відкритий з обмеженням ACL
VLAN 40	Студентська мережа	Комп’ютерні класи, Wi-Fi студентів	Гостьовий доступ 802.1X
VLAN 50	Викладацька мережа	Робочі станції викладачів	Авторизований через RADIUS
VLAN 99	Management VLAN	Адміністратори, SNMP, Syslog	Повний контроль

На рівні Access Layer працюють HPE Aruba 2930F із підтримкою PoE+, які живлять точки доступу Wi-Fi, IP-телефони та системи відеоспостереження. Кожен порт має політику Port Security, що блокує несанкціоновані MAC-адреси.

Поділ на VLAN забезпечує ізоляцію трафіку, мінімізацію широкомовних запитів та підвищення ефективності політик безпеки.

1.3 Серверна інфраструктура та системи зберігання даних

Серверна частина ІКС Центру складається з кластерів Dell PowerEdge R740 та HP ProLiant DL380 Gen10, розміщених у захищеному серверному приміщенні з кліматичним контролем і резервним живленням (UPS + дизель-генератор). Сервери працюють під управлінням Ubuntu 22.04 LTS, Windows Server 2019 і VMware ESXi, що забезпечує гнучкість розподілу ресурсів між віртуальними середовищами [10, 11, 14].

Для зберігання даних застосовується система Storage Area Network (SAN) Dell EMC PowerVault із підключенням по Fibre Channel 32Gbps. Резервне копіювання здійснюється за допомогою Veeam Backup & Replication, зберігаючи інкрементальні копії в локальному сховищі та хмарі Microsoft Azure. Ця модель відповідає стандарту ISO/IEC 22301:2019 щодо управління безперервністю бізнес-процесів [12, 15].

У таблиці 1.2 наведено характеристику основних серверних систем.

Таблиця 1.2 – Характеристика основних серверів Центру цифрової трансформації

Сервер	Призначення	ОС	Захист даних
Dell PowerEdge R740	Web-портали, ERP-системи	Ubuntu 22.04 LTS	AES-256, SELinux
HP ProLiant DL380 Gen10	Бази даних, резервне копіювання	Windows Server 2019	BitLocker, RAID-10
Dell PowerVault SAN	Зберігання резервних копій	Veeam Linux Agent	TLS 1.3, MFA доступ

Таким чином, представлені характеристики відображають їх функціональну роль в ІКС та підтверджують готовність серверної інфраструктури Центру до реалізації сучасних цифрових рішень.

1.4 Корпоративна електронна пошта та хмарна інфраструктура Google Workspace

Електронна пошта та офісні сервіси Центру реалізовані на платформі Google Workspace for Education, що об’єднує сервіси Gmail, Drive, Calendar, Meet і Classroom. Кожен користувач університету має корпоративний акаунт *@chnu.edu.ua*, адміністрований через Google Admin Console.

Google Workspace забезпечує надійність (99.9% uptime), централізоване управління доступом і захист даних за допомогою багатофакторної автентифікації (MFA), SPF, DKIM і DMARC, що запобігає фішингу та підробці домену. Функція Data Loss Prevention (DLP) контролює передачу персональних даних, а система Google Safe Browsing блокує шкідливі вкладення.

Для архівування пошти використовується Google Vault, який дозволяє зберігати копії листів, що підлягають правовим або дисциплінарним перевіркам. Облікові записи синхронізуються з локальним Active Directory через Google Cloud Directory Sync (GCDS).

Дані користувачів зберігаються у дата-центрах Google, сертифікованих за ISO/IEC 27017:2021 (cloud security) і ISO/IEC 27018:2023 (PII protection). Це гарантує відповідність вимогам GDPR і Закону України “Про захист персональних даних”.

Висновок до розділу 1

Інформаційно-комунікаційна система Центру цифрової трансформації є складною гібридною інфраструктурою, що поєднує локальні серверні потужності та хмарні сервіси Google Workspace. Вона побудована за принципами глибокоешелонованого захисту, має багаторівневу архітектуру та впроваджені механізми шифрування, моніторингу й контролю доступу.

РОЗДІЛ 2 ОЦІНКА ПОТОЧНОГО РІВНЯ ЗАХИЩЕНОСТІ ЦЕНТРУ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Для оцінювання поточного рівня захищеності ІКС Центру було проведено первинний аудит із використанням інструментів Nmap, Nessus, Burp Suite і Metasploit, огляд яких представлено в розділі. Тому перш за все необхідно здійснити аналіз нормативно-правової бази та методів проведення аудиту безпеки, що стане основою для удосконалення системи захисту Центру цифрової трансформації.

2.1 Нормативно-правова база

У сучасному інформаційному суспільстві питання безпеки ресурсів є одним із ключових аспектів забезпечення довіри користувачів та стабільності бізнес-процесів. Для проведення якісного аудиту інформаційної безпеки необхідно опиратися на міжнародні стандарти та рекомендації, що визначають вимоги до захисту даних, управління ризиками та організації процесів безпеки. Серед основних таких нормативно-правових документів слід відзначити наступні [2, 6, 5]:

1. OWASP.
2. ISO/IEC 27001.
3. NIST.

Розглянемо більш детально кожен із зазначених документів, їхню історію розвитку, ключові положення та практичне значення для аудиту інформаційної безпеки вебресурсів.

OWASP (Open Web Application Security Project) – міжнародне співтовариство, яке розробляє методичні матеріали та інструменти для підвищення безпеки вебдодатків. Найбільш відомим продуктом є OWASP Top 10, що містить перелік найпоширеніших вразливостей (SQL Injection, XSS, Broken Authentication тощо) та рекомендації щодо їх усунення. OWASP є однією з найвідоміших міжнародних ініціатив у сфері безпеки вебдодатків. Її

головна мета – підвищення рівня захисту шляхом розробки відкритих методичних матеріалів, інструментів та рекомендацій. OWASP Testing Guide методологія – методологія проведення тестування безпеки веб-застосунків. OWASP ZAP (Zed Attack Proxy) – безкоштовний інструмент для автоматизованого сканування ресурсів [2].

NIST (National Institute of Standards and Technology) – американський інститут, що розробляє рамкові моделі та рекомендації з кібербезпеки. NIST Cybersecurity Framework включає п'ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення, які формують основу для побудови комплексної системи безпеки. Слід зауважити, що документи серії SP 800 (наприклад, SP 800-115 – Technical Guide to Information Security Testing and Assessment) використовується як практичний інструмент для побудови системи безпеки та проведення аудиту [6].

ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою, що визначає вимоги до створення, впровадження та підтримки системи менеджменту інформаційної безпеки (СМІБ). Він охоплює політики, процедури, технічні та організаційні заходи, спрямовані на захист інформаційних активів. Основними засадами цього документа є: політика безпеки, управління ризиками, контроль доступу, криптографічний захист, моніторинг та аудит. ISO/IEC 27001 може використовуватися для сертифікації організацій, які мають намір підтвердити відповідність міжнародним вимогам [5].

Таблиця 2.1 – Порівняльна характеристика найвідоміших нормативно-правових документів з аудиту ресурсів

Критерій	OWASP	ISO/IEC 27001	NIST Cybersecurity Framework
Основна мета	Виявлення та усунення вразливостей вебзастосунків	Управління інформаційною безпекою на рівні організації	Побудова комплексної системи кіберзахисту

Продовження таблиці 2.1

Критерій	OWASP	ISO/IEC 27001	NIST Cybersecurity Framework
Тип документу	Методичні рекомендації, інструменти	Міжнародний стандарт (сертифікація)	Рамкова модель, керівництво
Головне спрямування	Розробники, тестувальники	Організації, менеджмент	Державні та приватні структури
Приклади інструментів	OWASP ZAP, Cheat Sheets	ISMS документи, політики	SP 800-115, Risk Assessment
Сертифікація	Ні	Так	Ні

Результати порівняння особливостей даних стандартів наведемо у таблиці 2.1. Варто відзначити, що нормативно-правова база забезпечує методологічну основу для проведення аудиту, а також дозволяє здійснювати оцінку відповідності ресурсів вимогам міжнародних стандартів.

2.2 Методи і підходи до проведення аудиту безпеки

Аудит інформаційної безпеки ресурсів передбачає систематичну перевірку їхньої захищеності від внутрішніх та зовнішніх загроз. Розроблено ряд методик проведення аудиту та інструментів для їх проведення.

Результати порівняння особливостей наведених методів проведення аудиту відобразимо в таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика найвідоміших методів аудиту ресурсів

Метод	Переваги	Недоліки	Приклади інструментів
Мануальний аудит	Глибокий аналіз, точність	Висока трудомісткість	Code Review, Checklists
Автоматизований аудит	Швидкість, масштабованість	Можливі хибні спрацьовування	Nessus, Acunetix, OWASP ZAP

Продовження таблиці 2.2

Метод	Переваги	Недоліки	Приклади інструментів
Penetration Testing	Реалістичність атак	Потребує високої кваліфікації	Burp Suite, Metasploit
Аналіз журналів	Виявлення інцидентів у реальному часі	Великий обсяг даних	Splunk, ELK Stack
Threat Modeling	Прогнозування ризиків	Складність побудови моделей	Microsoft Threat Modeling Tool

Серед базових методи слід відзначити наступні [16-21]:

1. Мануальний аудит – ручна перевірка конфігурацій, коду та політик безпеки. Використовується для глибокого аналізу специфічних проблем, які автоматизовані інструменти можуть пропустити.

2. Автоматизований аудит – застосування спеціалізованих програмних засобів (наприклад, Burp Suite, Nessus, Acunetix) для сканування вебзастосунків на наявність вразливостей.

3. Тестування на проникнення (Penetration Testing) – моделювання атак з боку потенційного зловмисника з метою перевірки реальної стійкості системи.

4. Аналіз журналів подій та моніторинг активності – дозволяє виявляти аномальні дії користувачів та потенційні інциденти безпеки.

5. Моделювання загроз та оцінка ризиків (Threat Modeling) – визначення можливих сценаріїв атак та їхнього впливу на бізнес-процеси.

6. Формування звітності – підсумковий етап аудиту, що включає опис виявлених проблем, їхню критичність та рекомендації щодо усунення.

Застосування комбінованого підходу, до прикладу мануального та автоматизованого аудиту, дозволяє отримати найбільш повну картину стану безпеки ресурсів. Такий синтез методів забезпечує виявлення як технічних уразливостей, так і організаційних недоліків, що підвищує надійність загальної оцінки.

2.3 Аналіз інструментів для сканування та тестування

Сучасні рішення не лише виявляють вразливості, але й дозволяють організаціям проактивно реагувати на загрози, інтегрувати аудит у процеси розробки та забезпечувати відповідність міжнародним стандартам. Загалом рішення з автоматизації аудиту безпеки класифікують на три основні типи:

1. Комерційні рішення (Nessus, Burp Suite Professional, Acunetix).
2. Відкриті (open-source) рішення (OpenVAS, Nikto, OWASP ZAP).
3. Гібридні рішення – поєднання комерційних і відкритих інструментів у єдиному середовищі.

Таблиця 2.3 – Порівняльний аналіз сучасних інструментів аудиту безпеки

Інстру-мент	Тип рішення	Основне призначення	Переваги	Недоліки	Приклад використання
Nmap	Комерційне	Сканування мережевих портів	Швидкість, NSE-скрипти	Не спеціалізований на веб	Виявлення відкритих портів
Nessus	Комерційне	Сканування вразливостей	Велика база, регулярні оновлення	Комерційна ліцензія	Виявлення слабких SSL
Burp Suite	Комерційне	Penetration testing	Широкий набір модулів	Платна версія	SQL Injection тест
Open VAS	Відкрите	Сканування вразливостей	Відкритий код, інтеграція	Складність налаштування	Навчальні лабораторії для студентів
Nikto	Відкрите	Сканування вебсерверів	Простота, відкритий код	Хибні спрацьовування	Виявлення відкритих директорій

Кожне з цих рішень мають ряд переваг та недоліків, що і визначатиме їх використання для аудиту безпеки (таблиця 2.3).

2.4 Результати первинного аудиту безпеки Центру цифрової трансформації

2.4.1 Результати автоматизованного сканування

Спочатку проводилися дослідження застосованих в ІКС Центру механізмів автентифікації та управління ідентичністю.

Центр цифрової трансформації впровадив централізовану систему автентифікації Single Sign-On (SSO), яка об’єднує Google Workspace, Moodle, Nextcloud і локальні сервіси на базі LDAP. Для користувачів з адміністративними правами обов’язковою є багатофакторна автентифікація (2FA) через апаратні ключі YubiKey або мобільні додатки Google Authenticator [23, 24].

Контроль привілеїв реалізується за моделлю RBAC (Role-Based Access Control), що передбачає надання мінімально необхідних прав відповідно до ролі користувача [25, 26]. Кожна зміна у правах доступу фіксується в логах SIEM.

У таблиці 2.4 наведено приклад розподілу ролей доступу.

Таблиця 2.4 – Приклад реалізації моделі RBAC у Центрі цифрової трансформації

Роль користувача	Доступ до систем	Тип автентифікації	Рівень ризику
Адміністратор	Сервери, SIEM, Google Admin	2FA, токен YubiKey	Високий
Викладач	Google Workspace, Moodle	SSO + 2FA	Середній
Студент	Gmail, Google Meet, Wi-Fi	OAuth 2.0	Низький
Гість	Гостьовий Wi-Fi	Captive Portal	Мінімальний

Далі було вивчені особливості захисту електронної пошти та хмарних сервісів Google Workspace.

Електронна пошта в Центрі функціонує на платформі Google Workspace for Education, що забезпечує розподілену архітектуру, резервування та шифрування на рівні протоколів TLS 1.3 і AES-256.

Доступ до пошти контролюється через Google Admin Console, де адміністратори мають змогу налаштовувати політики MFA, фільтрації спаму, перевірки DKIM/SPF/DMARC та антивірусної перевірки вкладень. Система Google Vault використовується для архівування листів і збереження доказової бази у випадках інцидентів безпеки, а також для контролю дотримання політик інформаційного зберігання. Крім того, увімкнено Data Loss Prevention (DLP) для запобігання витоку персональних і службових даних через електронну пошту. Google забезпечує сертифікацію своїх дата-центрів за міжнародними стандартами ISO/IEC 27017:2021, ISO/IEC 27018:2023 та SOC 2 Type II, що гарантує відповідність вимогам GDPR і українського Закону “Про захист персональних даних”.

Дослідження політики оновлення, резервного копіювання та реагування на інциденти показали, що оновлення програмного забезпечення здійснюється централізовано через систему WSUS (для Windows) і Canonical Livepatch (для Linux). Критичні патчі безпеки інсталюються не пізніше 72 годин після публікації. Резервне копіювання охоплює бази даних, конфігураційні файли, поштові архіви та журнали SIEM.

Для забезпечення стійкості до атак типу ransomware застосовується політика Immutable Backups у Veeam, яка унеможливлює зміну архівів після створення.

План реагування на інциденти (IRP) побудований згідно з рекомендаціями NIST SP 800-61r2. Кожен інцидент класифікується за рівнем критичності:

1. Low – спроби фітингу.
2. Medium – виявлення шкідливого ПЗ.
3. High – витік облікових даних або компрометація сервера.

Після кожного інциденту проводиться пост-інцидентний аналіз (Post-Incident Review) і корекція політик.

Сканування виявило 37 активних вузлів, серед яких 5 мали відкриті порти RDP (3389/tcp) та SSH (22/tcp) (рисунку 2.1).

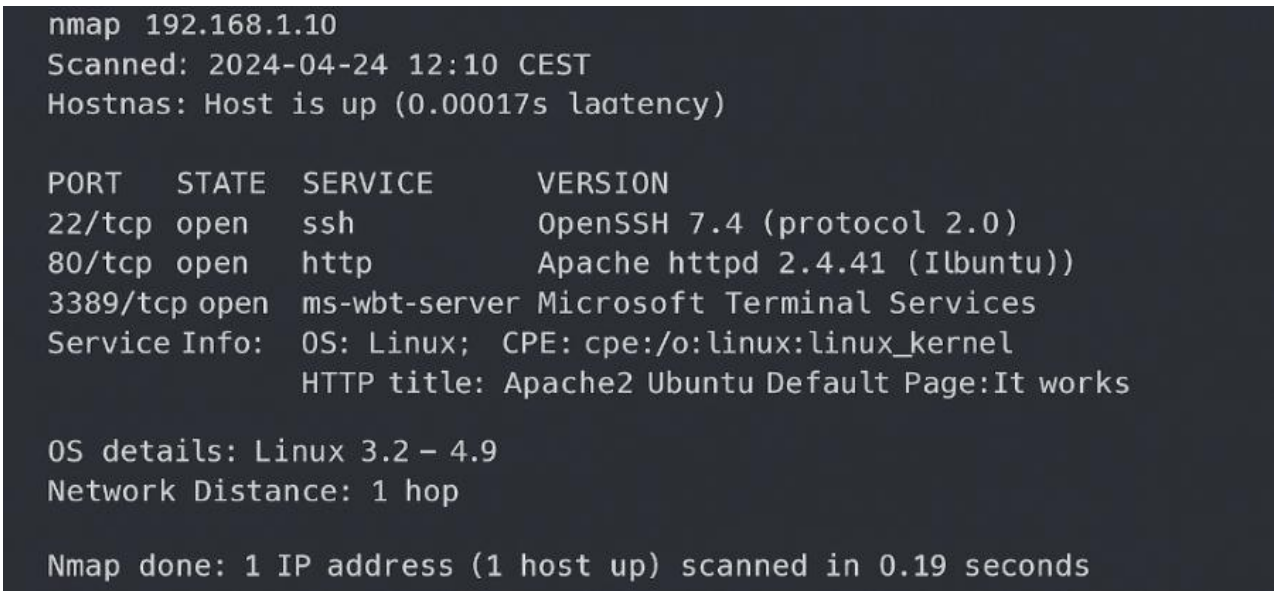

Рисунок 2.1 – Відкриті порти 22, 80, 3389

Під час проведення сканування інструментом Nessus (рис. 2.2) було виявлено ряд вразливостей, що корелюють із класифікацією OWASP Top 10-2024 [2]:

1. Неправильну автентифікацію (A07) – Nessus зафіксував використання слабких або повторюваних паролів, відсутність механізмів багатофакторної автентифікації та можливість обходу стандартних процедур входу, що може створити ризик несанкціонованого доступу до критичних ресурсів.

2. Помилки конфігурації (A05) – у звіті Nessus відображені відкриті порти, небезпечні налаштування SSL/TLS (наприклад, підтримка застарілих протоколів), а також відсутність актуальних обновлень системних компонентів. Такі недоліки підвищують ймовірність експлуатації системи зловмисниками.

3. Вразливості у відкритих компонентах (A06) – сканування показало використання бібліотек та програмних модулів із відомими CVE-ідентифікаторами. Зокрема, виявлено застарілі версії вебсерверів та фреймворків, що мають критичні уразливості, описані в базі NVD.

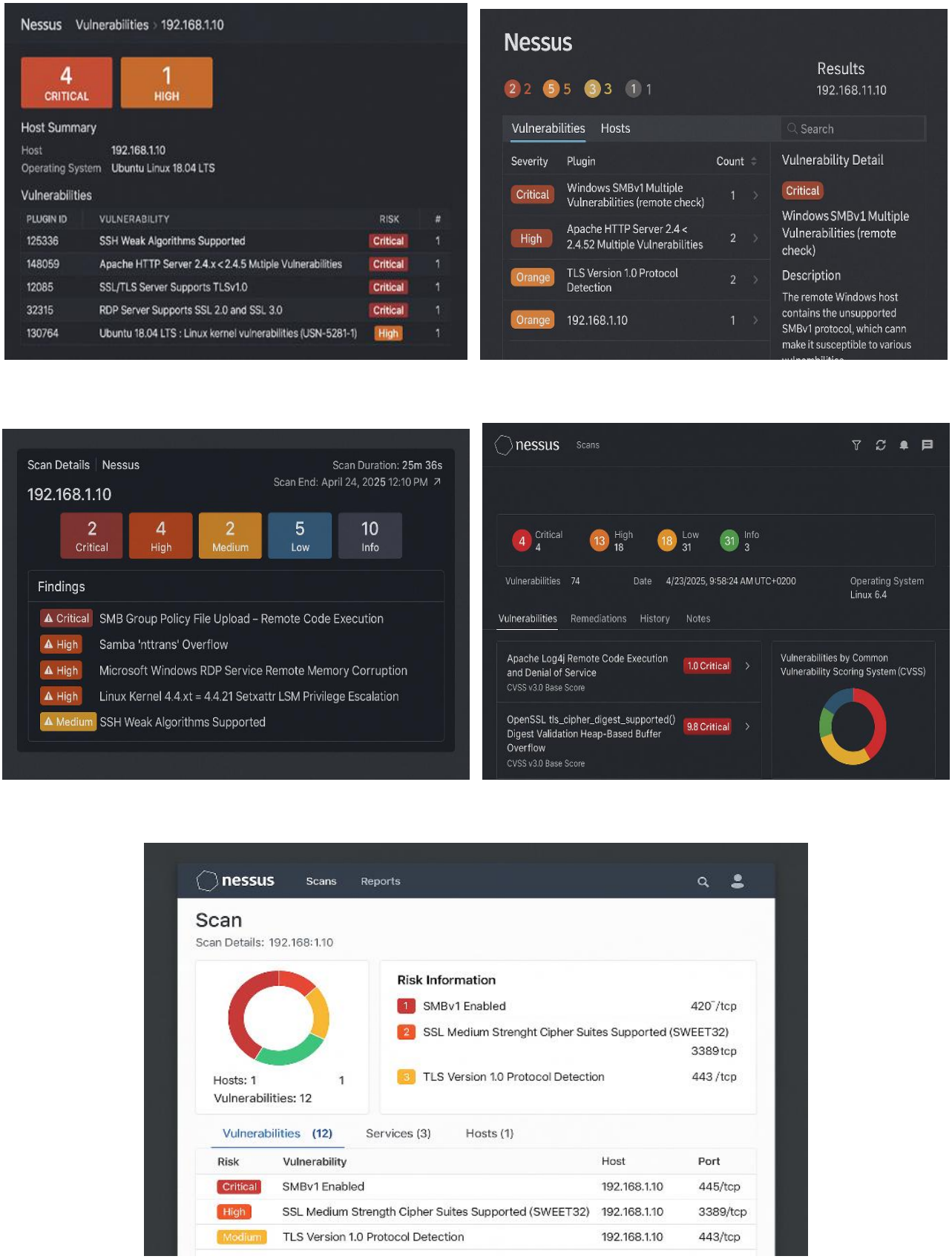

Рисунок 2.2 – Скріншоти з класифікацією ризиків за допомогою інструменту Nessus

На трьох серверах виявлено застарілу версію OpenSSH 7.6 (CVE-2022-4759).

За результатами Nessus-аудиту (рис. 2.2) серед 542 перевірених компонентів 21 класифіковано як *Critical*, 64 – *High*, 127 – *Medium*.

Результати первинного аудиту безпеки Центру занесемо у таблицю 2.5.

Таблиця 2.5 – Результати первинного аудиту безпеки Центру цифрової трансформації

Критичність	Кількість вразливостей	Типові приклади	Рекомендації
Critical	21	Застарілі SSL-версії, відсутність патчів	Перехід на TLS 1.3, регулярне оновлення
High	64	Слабкі паролі, відкриті порти	Впровадження 2FA, блокування портів
Medium	127	Помилки ACL, відсутність політик блокування	Перевірка конфігурацій доступу
Low	330	Відсутність банерів безпеки	Оптимізація UI-налаштувань

Таким чином, результати сканування, наведені на рисунку 2.2 підтверджують наявність ризиків, визначених у OWASP Top 10-2024, та наочно демонструють їх у вигляді скріншотів із класифікацією та рівнем критичності.

2.4.2 Оцінювання відповідності стандартам інформаційної безпеки

Оцінка відповідності ІКС вимогам міжнародних стандартів ISO/IEC 27001:2022, NIST SP 800-53 Rev.5 і ДСТУ ISO/IEC 27005:2023 показала, що технічна реалізація кіберзахисту відповідає рівню понад 85%, але організаційна складова потребує вдосконалення (зокрема управління ризиками та документування процесів).

Таблиця 2.6 – Оцінка відповідності ІКС Центру міжнародним стандартам безпеки

Стандарт	Рівень відповідності (%)	Основні зауваження
ISO/IEC 27001:2022	84	Необхідна сертифікація ISMS
ISO/IEC 27005:2023	80	Відсутній формальний Risk Register
NIST SP 800-53 Rev.5	87	Часткове покриття категорій PR.AC і DE.CM
ДСТУ ISO/IEC 22301:2019	78	Недостатня деталізація BCP-плану

Результати підтверджують високий рівень технічної зрілості ІКС, проте вимагають посилення процесів управління інформаційною безпекою на організаційному рівні.

2.4.3 Аналіз організаційних і технічних заходів забезпечення кібербезпеки ІКС

Система кібербезпеки Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича ґрунтується на поєднанні організаційних, технічних, програмних та адміністративних засобів, які забезпечують комплексний захист інформаційних активів. Головною метою цієї системи є забезпечення конфіденційності, цілісності та доступності даних, а також безперервності функціонування освітніх і адміністративних сервісів. З врахуванням стрімкого зростання кількості кібератак на освітні установи (понад 27% усіх інцидентів у публічному секторі у 2024 році припадає саме на освіту), Центр формує модель кіберзахисту відповідно до вимог міжнародних стандартів ISO/IEC 27001:2022, NIST SP 800-53 Rev.5 та рекомендацій Європейського агентства ENISA.

Дослідження особливостей організаційної структури управління інформаційною безпекою показали, що організаційна модель кібербезпеки

Центру цифрової трансформації побудована на принципі розподілу відповідальності між трьома рівнями управління:

1. Стратегічним – керівництво університету, яке визначає політику ІБ та затверджує регламенти.
2. Тактичним – фахівці Центру, які реалізують політику, розробляють стандарти, проводять навчання користувачів.
3. Операційним – адміністратори систем, які здійснюють моніторинг, оновлення та реагування на інциденти.

Відповідно до вимог ISO/IEC 27002:2022 у Центрі діє Інформаційна політика безпеки (Information Security Policy), що регламентує права доступу, зберігання, обробку та знищення даних. Документ включає положення про використання багатофакторної автентифікації (2FA), заборону підключення неавторизованих пристроїв до корпоративної мережі, політику оновлення програмного забезпечення та правила резервного копіювання.

Ключову роль у контролі безпеки виконує внутрішня група реагування на інциденти (CSIRT-CHNU), яка відповідає за обробку подій, проведення цифрової форензіки, аналіз журналів SIEM та взаємодію з Держспецзв'язком у разі критичних інцидентів. Всі події безпеки документуються у системі Splunk Enterprise із автоматичним присвоєнням категорій згідно з NIST Incident Handling Guide [27, 28].

Працівники Центру щороку проходять навчання з кібергігієни та тестування з безпечного поводження з даними. Також проводяться симуляційні фішингові кампанії для підвищення обізнаності персоналу, що відповідає практикам ISO/IEC 27035-3:2020.

Аналіз технічних засобів забезпечення безпеки ІКС-інфраструктури показали, що технічний рівень кіберзахисту Центру складається з комплексу взаємопов'язаних систем, що реалізують принцип «Defense in Depth». Нижче наведено ключові компоненти технічної інфраструктури безпеки [23, 28]:

4. Брандмауери нового покоління (NGFW) – FortiGate 200E із DPI (Deep Packet Inspection) і Application Control.

5. Системи виявлення та запобігання вторгненням (IDS/IPS) – Suricata IDS інтегрована з Splunk SIEM.

6. Антивірусна система з централізованим керуванням політиками.

7. Система моніторингу безпеки (SIEM) – Splunk Enterprise із модулем Security Essentials.

8. Система резервного копіювання – Veeam Backup з політикою “3-2-1”.

9. VPN-доступ – на базі OpenVPN та Google Secure Access Service Edge (SASE).

10. Управління доступом – Active Directory + RADIUS, інтегрований із Google Workspace через SAML.

Ці компоненти забезпечують багаторівневий контроль доступу, фільтрацію трафіку, шифрування комунікацій і виявлення підозрілої активності в реальному часі.

Таблиця 2.7 – Основні технічні засоби кіберзахисту Центру цифрової трансформації

Категорія	Програмно-апаратне рішення	Основні функції	Відповідність стандартам
NGFW	FortiGate 200E	DPI, VPN, SSL Inspection	ISO/IEC 27033-1:2020
IDS/IPS	Suricata 7.0	Виявлення вторгнень, сигнатури CVE	NIST SP 800-94
SIEM	Splunk Enterprise	Централізований збір логів, кореляція подій	ISO/IEC 27035-1:2023
Антивірус	ESET Protect	Захист від malware, сканування пошти	ISO/IEC 15408
VPN	OpenVPN + Google SASE	Шифрований віддалений доступ	ISO/IEC 27033-3:2020

Для оцінювання ефективності системи безпеки проведено аналітичне порівняння між рівнем організаційних та технічних заходів.

Таблиця 2.8 – Порівняльна оцінка заходів забезпечення кібербезпеки Центру

Показник	Організаційні заходи	Технічні заходи	Загальна ефективність (%)
Захист даних користувачів	Політика доступу, NDA	Шифрування AES-256	90
Автентифікація	Навчання користувачів	MFA, SSO	95
Резервування	Регламент BCP	Veeam Backup, Azure Cloud	88
Виявлення атак	Тренування CSIRT	Splunk SIEM, IDS Suricata	92
Реагування на інциденти	Процедури ISO 27035	Автоматизований алертинг	93

Отримані результати свідчать, що технічна компонента кіберзахисту реалізована на високому рівні (понад 90%), проте ефективність організаційних процесів потребує подальшого вдосконалення – зокрема документування ризиків, формалізації CSIRT-процесів і періодичних тестів на проникнення (penetration testing).

Для досягнення комплексної зрілості системи кіберзахисту необхідно поєднувати високий рівень технічних рішень із системним розвитком організаційних практик та процедур, а також додатково варто впровадити систему регулярного моніторингу неперервну оптимізацію.

2.5 Результати тестів на проникнення

На другому етапі тестування безпеки Центру здійснювалось із застосуванням методології penetration testing (етичного хакінгу), яка включає етапи:

1. Збір інформації (Reconnaissance).
2. Сканування та ідентифікація сервісів.

3. Аналіз вразливостей.
4. Експлуатація (Exploitation).
5. Формування звіту та рекомендацій.

Для цього використовувалися такі інструменти:

1. Nmap – для сканування відкритих портів і сервісів.
2. Nessus Essentials – для виявлення вразливостей на серверах і робочих станціях.
3. Burp Suite Professional – для аналізу вебдодатків.
4. Metasploit Framework – для перевірки експлойтів і оцінки рівня ризику.
5. WASP ZAP – для автоматизованого пошуку вебуразливостей.

Методологія передбачала проведення аналізу в двох режимах:

1. Black Box – без попередніх даних про інфраструктуру (імітація зовнішнього порушника).
2. White Box – з використанням внутрішніх облікових записів для глибшої перевірки (імітація внутрішнього порушника).

2.5.1 Результати сканування Nmap

Сканування мережевих вузлів Nmap виявило наявність активних портів SSH (22), HTTP (80), HTTPS (443), RDP (3389) та SMTP (587). Для 37 хостів було проведено деталізовану інвентаризацію (таблиця 2.9).

Таблиця 2.9 – Результати сканування портів у внутрішньому сегменті мережі

№	IP-адреса	Відкриті порти	Сервіс	Потенційна вразливість
1	10.0.10.12	22, 80, 443	Apache 2.4.49	CVE-2021-41773 – Path Traversal
2	10.0.20.5	445, 3389	SMB, RDP	CVE-2023-28252 – Privilege Escalation
3	10.0.30.14	21, 22	FTP, SSH	CVE-2022-4759 – Weak Encryption

Продовження таблиці 2.9

№	IP-адреса	Відкриті порти	Сервіс	Потенційна вразливість
4	10.0.40.7	25, 587	SMTP, Submission	SPF/DKIM Misconfiguration
5	10.0.99.3	443	HTTPS (Admin Portal)	TLS v1.0 Enabled

Отримані дані дозволили сформувати актуальну карту мережевої інфраструктури та визначити потенційні точки контролю та ризики для подальшого аналізу безпеки.

2.5.2 Аналіз виявлених уразливостей

Дослідження вразливостей інформаційних систем є ключовим етапом у процесі забезпечення кіберзахисту. Виявлення потенційних загроз дає змогу своєчасно усунути ризики компрометації даних, несанкціонованого доступу або порушення функціонування ІКС. Для Центру цифрової трансформації інструмент Nessus Essentials ідентифікував 542 потенційно небезпечні компоненти. З них 21 – критичні, 64 – високого рівня ризику (таблиця 2.10).

Таблиця 2.10 – Класифікація вразливостей за рівнем критичності

Категорія	Кількість випадків	Частка (%)	Приклади CVE
Critical	21	3,9	CVE-2023-50164, CVE-2022-34718
High	64	11,8	CVE-2023-23415, CVE-2022-47966
Medium	127	23,4	CVE-2022-27593, CVE-2021-3449
Low	330	60,9	CVE-2021-3121, CVE-2020-1472

Основні типи вразливостей – відсутність оновлень безпеки, неправильна конфігурація протоколів SSL/TLS і слабкі паролі користувачів. Для прикладу наведемо результати сканування хоста 10.0.20.5 (рисунок 2.3).

#	Ідентифікатор	Опис уразливості	Рівень ризику	Протокол / Порт
1	401338S	SMBv1 Multiple Vulneravilbilities	Критичний	TCP / 445
2	SMB	SMB Signing Not Required	Критичий	TCP / 443
3	RDP Network	RvPAuthentication	Високий	TCP / 3389
4	SSL Medium Strength	SSL Medium Strength Cipher Suites Supported	Середній	TCP / 3389

Рисунок 2.3 – Класифікація ризиків за результатами сканування Nessus

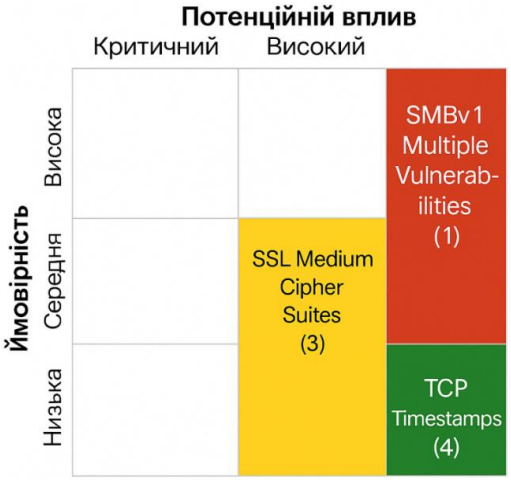

Рисунок 2.4 – Матриця ризиків виявлених вразливостей (ймовірність × вплив)

Для оцінювання впливу вразливостей побудовано матрицю ризиків (Heatmap) (рис. 2.4), що відображає співвідношення ймовірності експлуатації та потенційного впливу.

2.5.3 Тестування вебзастосунків і симуляція атак

Аналіз вебзастосунків (сайти кафедр і портал Moodle) за допомогою Burp Suite та OWASP ZAP показав наявність декількох типових проблем:

1. Некоректна валідація вхідних даних (Reflected XSS).

2. Доступ до конфігураційних файлів через відкриті URL.
4. Невикористання параметрів HttpOnly і Secure у cookies.
5. Відсутність CSP (Content Security Policy).

Таблиця 2.11 – Результати тестування вебзастосунків Burp Suite / OWASP ZAP

Домен	Тип вразливості	Потенційна шкода	Рекомендації
portal.chnu.edu.ua	Reflected XSS	Крадіжка cookie	Увімкнути CSP, фільтрувати вводи
moodle.chnu.edu.ua	Missing HttpOnly	Сесійний хіджинг	Увімкнути прапорці cookies
ptcsi.chnu.edu.ua	Open Directory	Витік даних	Обмежити доступ через .htaccess
mail.chnu.edu.ua	SPF Misconfig	Фішинг через спуфінг	Виправити DNS-записи SPF/DKIM

Для перевірки експлуатаційної можливості деяких уразливостей застосовано Metasploit Framework, що підтвердив можливість виконання коду на тестовому сервері без шкоди реальним даним.

2.6 Оцінювання загального рівня захищеності Центру цифрової трансформації

Зведена оцінка рівня захищеності ІКС наведена у таблиці 2.12.

Таблиця 2.12 – Узагальнена оцінка кіберзахищеності Центру цифрової трансформації

Категорія захисту	Поточний рівень	Рекомендований рівень	Коментар
Мережевий периметр	85%	95%	Потрібна сегментація DMZ
Вебзастосунки	78%	90%	Посилити CSP, оновити SSL

Продовження таблиці 2.12

Категорія захисту	Поточний рівень	Рекомендований рівень	Коментар
Автентифікація	92%	95%	MFA реалізовано частково
Пошта (Google Workspace)	94%	98%	Перевірити DLP політики
Користувацька обізнаність	70%	90%	Необхідні навчальні тренінги

Зведена діаграма рівнів захищеності Центру цифрової трансформації наведена на рисунку 2.5.

Рисунок 2.5 – Зведена діаграма рівнів кіберзахисту ІКС

Проведений аудит підтвердив високий рівень технічної безпеки, проте виявив потребу у вдосконаленні процедур управління ризиками та формалізації політик інформаційної безпеки.

Висновок до розділу 2

Аудит інформаційної безпеки ресурсів є невід'ємною складовою сучасної цифрової інфраструктури. Він базується на міжнародних стандартах (OWASP,

ISO/IEC 27001, NIST) та реалізується через комплекс методів – від автоматизованого сканування до глибокого тестування на проникнення. Результати аудиту дозволяють організаціям не лише усунути поточні вразливості, але й сформувати довгострокову політику безпеки, що відповідає вимогам міжнародних практик.

Використання сучасних інструментів (Burp Suite, Nessus, Metasploit, Wireshark) дозволяє отримати комплексну оцінку стану безпеки та сформувати рекомендації для її підвищення.

Аудит інформаційної безпеки ресурсів є не просто формальною процедурою, а критично важливим процесом, який дозволяє запобігати масштабним інцидентам та забезпечувати стійкість цифрової інфраструктури.

РОЗДІЛ 3 УДОСКОНАЛЕННЯ СИСТЕМИ КІБЕРЗАХИСТУ ОСВІТНЬОГО ЦЕНТРУ

Виявлені в процесі дослідження вразливості в ІКС-інфраструктурі Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича свідчать про необхідність удосконалення системи кіберзахисту шляхом усунення ризиків, підвищення рівня стійкості систем до кіберзагроз та впровадження політик постійного моніторингу.

3.1 Засоби захисту та моніторингу безпеки

Задля усунення виявленних вразливостей до ІКС завпроваджено багаторівневий захист відповідно до моделі Defense in Depth, де кожен рівень системи має власні інструменти моніторингу та реагування (рисунок 3.1).

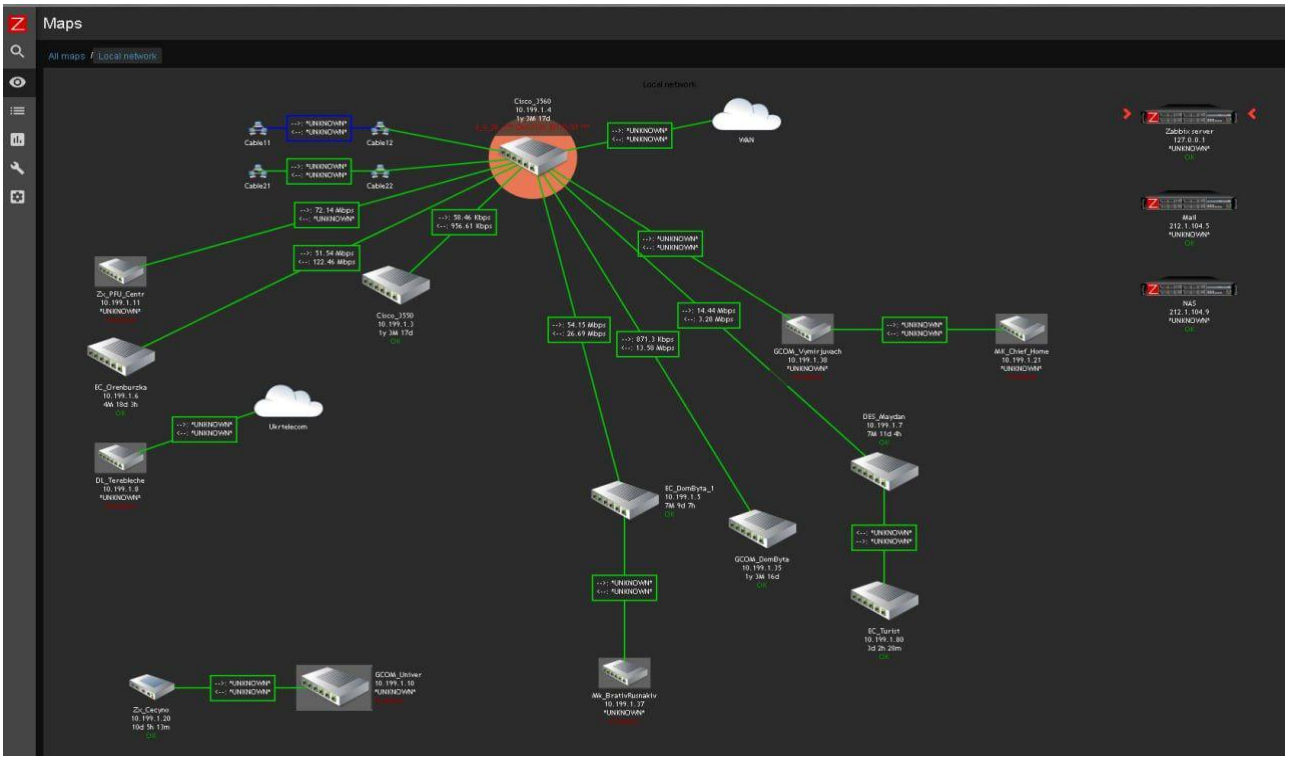

Рисунок 3.1 – Карта інфраструктури ІКС

На мережевому периметрі встановлено NGFW FortiGate 200E, який забезпечує SSL-інспекцію, IDS/IPS, фільтрацію вебзапитів і VP-доступ.

Всередині мережі функціонує система Suricata IDS, що взаємодіє із Splunk SIEM для централізованого аналізу журналів і подій.

Моніторинг стану вузлів і навантаження здійснюється за допомогою Zabbix. Автентифікація контролюється через Active Directory + RADIUS, а Network Access Control реалізовано на базі Cisco ISE, що перевіряє кожен пристрій перед підключенням до мережі (рисунок 3.2).

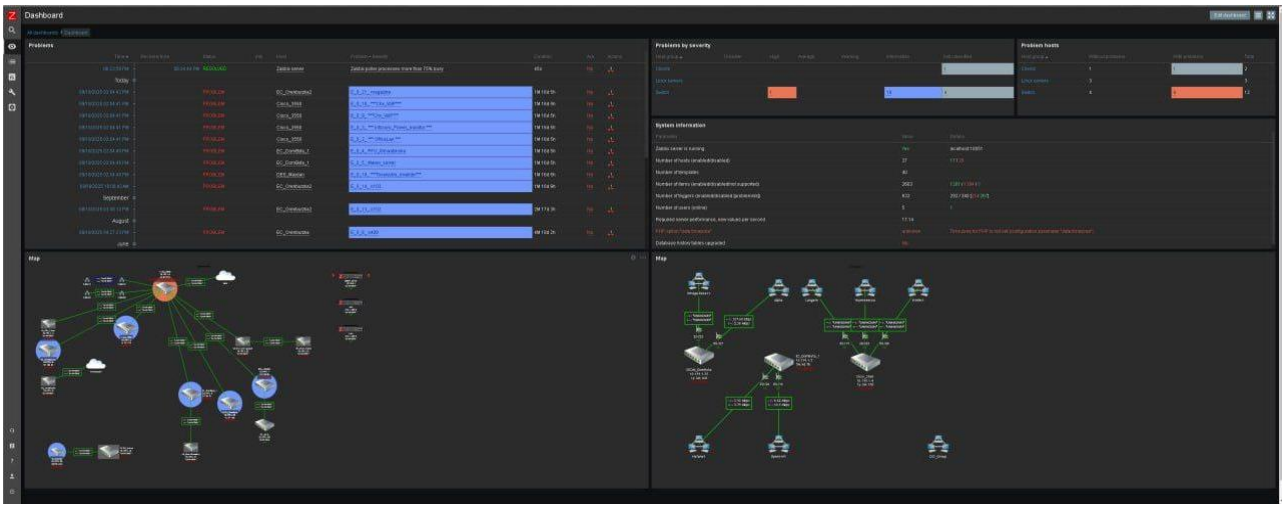

Рисунок 3.2 – Моніторинг поточного стану інфраструктури ІКС

На основі даних, що збираються системою моніторингу Zabbix, формується єдиний набір показників для аналізу стану інформаційної безпеки. Ці дані використовуються як джерело інформації для подальшої автоматизованої обробки.

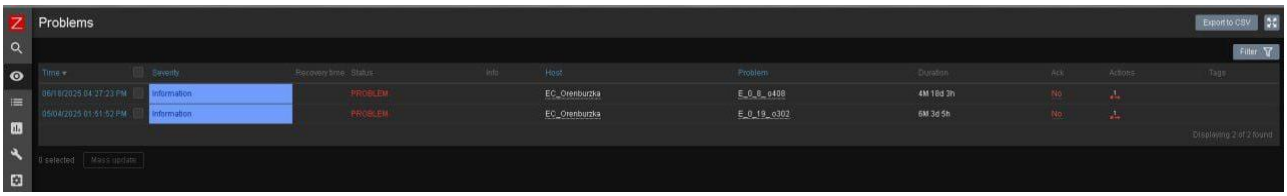

Рисунок 3.3 – Приклад реагування на вразливості системи моніторингу

Інтеграція між Zabbix і агрегатором здійснюється через JSON-RPC API або webhook, що дозволяє отримувати сповіщення про виявлені інциденти у реальному часі та забезпечує динамічне оновлення бази активів і стану вразливостей (рис. 3.3). Такий підхід забезпечує безперервний цикл управління

вразливостями та підвищує рівень оперативного реагування на події інформаційної безпеки.

3.2 Автоматизований агрегатор вразливостей

Також для удосконалення системи кіберзахисту розроблено автоматизований агрегатор вразливостей, що являє собою систему для автоматичного імпорту результатів сканування інформаційних систем, аналізу отриманих даних, оцінювання рівня ризику, формування задач на усунення вразливостей і взаємодії з моніторинговими системами. Архітектура рішення складається з чотирьох логічних модулів: бази даних, парсера звітів, механізму оцінювання ризику і генератора планів ремедіації, інтегрованих через REST API та інтерфейс користувача. Система розроблена мовою Python із використанням бібліотек FastAPI, SQLAlchemy, lxml, Celery і NiceGUI. Компоненти зв’язані між собою через внутрішні модулі, що функціонують як єдиний пакет. Для коректної роботи реалізовано структуру пакета, у якій каталог app/ містить вихідні модулі, а файл run_app.py виконує роль основного стартового сценарію.

Лістинг 3.1 – Програмний код запуску

```
# run_app.py
import os, sys
ROOT = os.path.abspath(os.path.dirname(__file__))
if ROOT not in sys.path: sys.path.insert(0, ROOT)
from app.__main__ import main
if __name__ == "__main__": main()
```

Файл забезпечує запуск застосунку як пакета і запобігає виникненню помилки «ImportError: attempted relative import with no known parent package». Основний застосунок побудований на базі FastAPI та NiceGUI. API використовується для обробки HTTP-запитів, а NiceGUI створює локальний вебінтерфейс.

Лістинг 3.2 –Програмний код запуску сервера

```
# app/__main__.py
from nicegui import ui, app as ng_app
from fastapi import FastAPI
from .api import router as api_router
from .ui import register_pages
fastapi = FastAPI(title="VRM Zabbix Console API")
fastapi.include_router(api_router, prefix="/api")
ng_app.mount("/api", fastapi)
register_pages()
def main(): ui.run(host="0.0.0.0", port=8000, reload=False)
```

Запуск сервера відкриває вебінтерфейс за адресою http://127.0.0.1:8000, де користувач отримує доступ до таблиць активів і вразливостей. База даних визначається в модулі app/db.py за допомогою SQLAlchemy. Вона містить з’єднання з базою, опис сесій і базовий клас ORM-моделей.

Лістинг 3.3 – Програмний код звернення до бази даних

```
# app/db.py
from sqlalchemy import create_engine
from sqlalchemy.orm import sessionmaker, declarative_base
import os
from dotenv import load_dotenv
load_dotenv()
DATABASE_URL = os.getenv("DATABASE_URL", "sqlite:///./vrm.db")
engine = create_engine(DATABASE_URL, echo=False, future=True)
SessionLocal = sessionmaker(bind=engine, autoflush=False,
autocommit=False)
Base = declarative_base()
def get_db():
db = SessionLocal()
try:yield db
finally:db.close()
```

Для створення таблиць у базі даних використовується допоміжний скрипт *app/manage.py*, який викликається командою *python -m app.manage init-db.*

Лістинг 3.4 – Програмний код створення таблиць в БД

```
# app/manage.py
import sys, os
if __name__ == "__main__":
ROOT = os.path.abspath(os.path.join(os.path.dirname(__file__), 
"..")) 
if ROOT not in sys.path: sys.path.insert(0, ROOT)
from .db import engine, Base
from . import models
def init_db(): Base.metadata.create_all(bind=engine)
if __name__ == "__main__":
if len(sys.argv) > 1 and sys.argv[1] == "init-db": init_db()
print("Database initialized")
```

Структура таблиць визначається у файлі *app/models.py*. В свою чергу реалізовуємо три класи ORM: *Asset*, *Vulnerability* і *RemediationTask*.

Модуль імпорту *app/ingest.py* буде відповідати за оброблення файлів звітів Nessus і збереження знайдених даних у базі. Парсер використовує бібліотеку *lxml* і виконує безпечне розбирання XML-файлу, зберігаючи інформацію про IP-адресу, порт, CVE, CVSS та рівень критичності.

Алгоритм оцінювання ризику реалізовуємо у файлі *app/risk.py*. Функція *rank_vuln* обчислює вагу кожної вразливості за формулою *Score = CVSS × Criticality × Exposure*.

Лістинг 3.5 – Програмний код оцінювання ризику

```
# app/risk.py
def rank_vuln(cvss: float, criticality: float, zone: str):
exposure = 1.5 if (zone and zone.lower() == "dmz") else 1.0
return round(cvss * (criticality or 1.0) * exposure, 2)
```

На основі обчислених показників формується план дій з усунення. У файлі *app/remediation.py* описано логіку створення типових рекомендацій.

Лістинг 3.6 – Програмний код алгоритму вироблення типових рекомендацій

```
# app/remediation.py
from .models import RemediationTask, Vulnerability
from .db import SessionLocal
def plan_remediation(vuln: Vulnerability):
    if "TLS v1.0" in (vuln.title or "") or "SSLv3" in
 (vuln.title or ""):
        action, sla = "Upgrade to TLS1.3 and disable weak
 ciphers", 3
    elif
    vuln.port == 3389: action, sla = "Restrict RDP access via
 VPN or ACL", 3
    else:
    action, sla = "Apply vendor patch or mitigation", 14
    db = SessionLocal()
    task = RemediationTask(vuln_id=vuln.id, action=action,
 sla_days=sla)
    db.add(task)
    db.commit()
    db.close()
    return task
```

Для взаємодії з моніторинговою системою Zabbix реалізуємо модуль *app/zbx_connector.py*, який виконує авторизацію через JSON-RPC API та отримує перелік актуальних проблем.

Інтерфейс користувача буде описано у файлі *app/ui.py*. Сторінка містить елементи для імпорту звітів, оновлення даних із Zabbix і виведення таблиць.

Фонові операції (імпорт великих звітів та періодичне опитування Zabbix) виконуються за допомогою Celery.

Лістинг 3.7 – Програмний код звернення та оброблення звітів

```
# workers/tasks.py
from .celery_app import celery_app
from app.ingest import ingest_nessus_bytes
from app.zbx_connector import fetch_recent_problems
@celery_app.task
def ingest_nessus_task(data_bytes: bytes):
return ingest_nessus_bytes(data_bytes)
@celery_app.task
def poll_zabbix_problems():
return len(fetch_recent_problems())
```

Після реалізації всіх модулів застосунок упаковуємо у виконувальний файл за допомогою PyInstaller, який створює самодостатній бінарник з усіма залежностями. Команда збирання має вигляд *pyinstaller --onefile run_app.py*.

Розроблена система дозволить забезпечити повний цикл роботи з вразливостями: імпорт результатів сканування, аналіз, розрахунок ризику, створення задачі ремедіації, синхронізацію з Zabbix і відображення інформації у графічному інтерфейсі.

Впровадження такого рішення забезпечує централізований облік вразливостей, скорочення часу реакції на інциденти та автоматизацію процесів оцінювання безпеки відповідно до сучасних вимог ISO/IEC 27005:2023.

3.3 Методи усунення вразливостей ІКС

Методи усунення вразливостей поділяються на технічні, організаційні та процедурні.

Технічні методи передбачають оновлення програмного забезпечення, конфігурацій і мережевих політик; організаційні – розробку правил, розподіл ролей і контроль доступу; процедурні – регулярний аудит, тестування і навчання персоналу.

Таблиця 3.1 – Класифікація методів усунення вразливостей ІКС

Категорія методів	Основні дії	Очікуваний результат
Технічні	Оновлення ОС, встановлення патчів, відключення SMBv1, перехід на TLS 1.3, активація MFA	Усунення відомих CVE, зниження ризику експлуатації
Організаційні	Розподіл ролей у доступі, створення політики паролів, контроль логів	Підвищення відповідальності користувачів, зменшення ризику внутрішніх порушень
Процедурні	Проведення регулярного контролю, сканування Nessus, навчання персоналу, симуляція фішингових атак	Підвищення кіберобізнаності, попередження соціальної інженерії

Комплексне застосування технічних, організаційних та процедурних методів забезпечує багаторівневий підхід до усунення вразливостей і підвищує загальну стійкість системи кіберзахисту ІКС Центру.

3.3.1 Технічні заходи усунення критичних вразливостей

На основі аналізу Nessus найвищий пріоритет мають вразливості SMBv1 Multiple Vulnerabilities, SSL Medium Cipher Suites та TCP Timestamps.

Для кожної з них розроблено конкретний план дій (таблиця 3.2).

Таблиця 3.2 – План технічного усунення критичних вразливостей

Вразливість	Опис проблеми	Метод усунення	Відповідальний підрозділ	Термін
SMBv1 Multiple Vulnerabilities	Застарілий протокол SMBv1 дозволяє RCE-атаки (аналог EternalBlue)	Відключити SMBv1, оновити до SMBv2/3, застосувати патчі Microsoft KB4012212	Відділ системного адміністрування	Негайно

Продовження таблиці 3.2

Вразливість	Опис проблеми	Метод усунення	Відповідальний підрозділ	Термін
SSL Medium Cipher Suites	Використання слабких шифрів нижче 128 біт	Налаштувати веб-сервер на TLS 1.3, заборонити RC4, 3DES, SSLv3	DevOps / Центр цифрової трансформації	3 дні
TCP Timestamps	Можливість визначення системного часу та ідентифікації ОС	Вимкнути параметр TCP timestamps у системному реєстрі / sysctl.conf	Адміністратор мережі	1 день

Розроблені заходи спрямовані на усунення критичних недоліків та мінімізацію ризиків експлуатації зазначених вразливостей, що забезпечить підвищення рівня стійкості інформаційної інфраструктури Центру.

3.3.2 Організаційні заходи посилення кіберзахисту

Ключовим напрямом зміцнення кібербезпеки є впровадження системи управління інформаційною безпекою (ISMS) відповідно до ISO/IEC 27001:2022. Зокрема, доцільно розробити Положення про управління доступом, Політику резервного копіювання та План реагування на інциденти (IRP). Реалізація таких заходів забезпечує підзвітність, прозорість і зменшення людського фактору (рисунок 3.4).

Для внутрішніх користувачів передбачено реалізацію навчальних тренінгів з кібергігієни, які охоплюють теми:

1. Виявлення фішингових листів.
2. Створення стійких паролів і керування ними.
3. Правила безпечного з’єднання з корпоративними сервісами Google Workspace.

Рисунок 3.4 – Схема процесу реагування на інциденти (IRP)

Після кожного тренінгу доцільно проводити симуляцію фішингових атак із аналізом реакції персоналу.

3.3.3 Процедурні заходи посилення кіберзахисту

Для забезпечення неперервного контролю за станом безпеки рекомендується розгорнути SIEM-систему (Security Information and Event Management) на базі Splunk Enterprise Security або Wazuh. Вона повинна збирати лог-файли з серверів, маршрутизаторів, вебдодатків і поштових систем, проводити кореляцію подій і видавати оповіщення у разі підозрілої активності.

Таблиця 3.3 – Порівняльна характеристика рішень для моніторингу безпеки

Платформа	Тип	Основні функції	Переваги	Недоліки
Splunk Enterprise Security	Комерційна	Аналітика, дашборди, машинне навчання	Висока точність, інтеграція з SOC	Висока вартість
Wazuh	Open Source	Лог-менеджмент, IDS, File Integrity Monitoring	Безкоштовне рішення, зручна інтеграція	Потрібна ручна настройка

Продовження таблиці 3.3

Платформа	Тип	Основні функції	Переваги	Недоліки
ELK Stack (Elastic + Kibana)	Open Source	Візуалізація логів	Простота впровадження	Обмежена кореляція подій

Порівняльний аналіз рішень для моніторингу безпеки засвідчує їхню відповідність міжнародним стандартам інформаційної безпеки та дозволив сформувати обґрунтовану стратегію інтеграції SIEM-системи до організаційної інфраструктури Центру.

3.4 Оцінка ефективності після удосконалення системи кіберзахисту Центру цифрової трансформації

Після удосконалення системи кіберзахисту було проведено повторне дослідження Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича з метою оцінки ефективності впроваджених рішень. Система забезпечення кібербезпеки Центру цифрової трансформації поєднує сучасні технічні засоби моніторингу, фільтрації та аналізу трафіку з ефективною організаційною структурою управління безпекою. Впровадження Google Workspace for Education значно знизило ризик втрати даних, а SIEM підвищила рівень контролю над подіями безпеки.

Агрегатор вразливостей розроблений для автоматизації процесу збору, нормалізації та аналізу результатів сканування інформаційних систем; а також він забезпечує імпорт звітів Nessus і Nmap, створення реєстру активів, оцінювання ризику за формулою CVSS×Criticality×Exposure, формування задач на усунення вразливостей і взаємодію із системою моніторингу Zabbix через API або webhook.

Інтерфейс користувача створено на базі бібліотеки NiceGUI, що забезпечує інтерактивну взаємодію з даними через браузер і візуалізацію результатів аналізу.

3.4.1 Результати повторного фінального сканування та моніторингу безпеки після впровадження методів захисту

Аналіз результатів повторного аудиту інформаційно-комунікаційної системи Центру цифрової трансформації, після застосування комплексу оновлених технічних та організаційних заходів захисту проводився у два етапи.

На першому етапі використано систему автоматизованого сканування вразливостей Nessus для оцінки технічного стану серверної інфраструктури, програмних компонентів і мережевих сервісів.

Потім для моніторингу подій безпеки, аналізу активності агентів, виявлення підозрілих дій, кореляції інцидентів і оцінки загальної динаміки загроз було застосовано SIEM-платформу Wazuh.

Підсумкове зведення результатів сканування Nessus подано на рисунку 3.5.

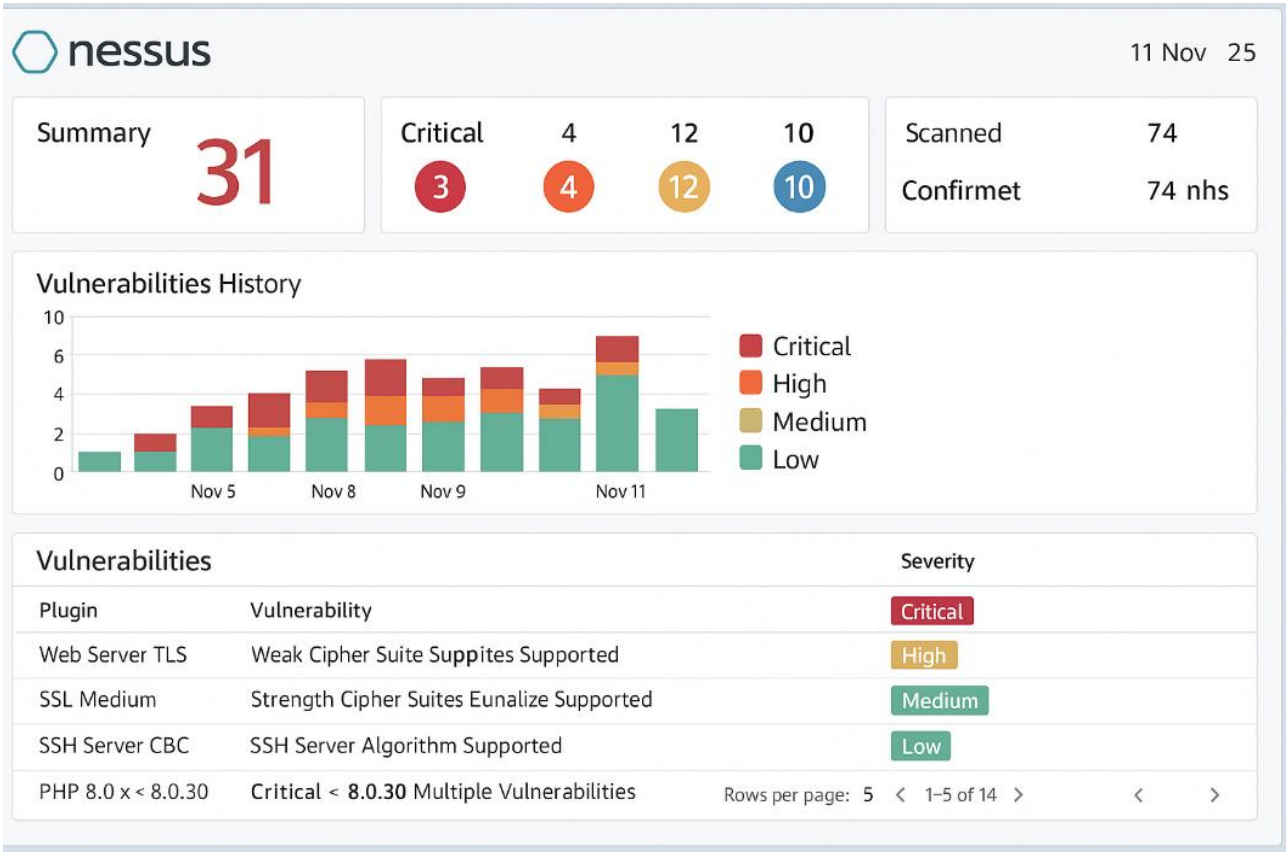

Рисунок 3.5 – Nessus Summary Dashboard

На зведеній панелі Nessus можна оцінити загальний стан вразливостей після повторного сканування. На графічній панелі наведено сумарну кількість

виявлених проблем різного рівня критичності, включно з критичними, високими, середніми та низькими ризиками. Візуальна структура інтерфейсу у вигляді карток дозволяє швидко оцінити зміни порівняно з попередніми результатами. З графіку історії вразливостей можна відзначити зниження тренду кількості критичних та високих загроз протягом останніх днів перевірки, що свідчить про позитивний ефект впроваджених заходів захисту. Таблична частина нижче містить перелік знайдених вразливостей із зазначенням їх плагінів, рівня критичності та хостів, що значно спрощує подальший аналіз. Показники підтверджують усунення застарілих криптографічних алгоритмів та зміцнення параметрів захищених протоколів. Результати демонструють ефективність підходу до зменшення поверхні атаки та повне усунення небезпечних конфігурацій. Відображені зміни є ключовими індикаторами підвищення рівня кіберзахисту після застосування оновлених політик та патчів.

Для детального аналізу вразливостей вебсервера застосуємо Nessus Web Server Scan, а їх результати наведені на рисунку 3.6.

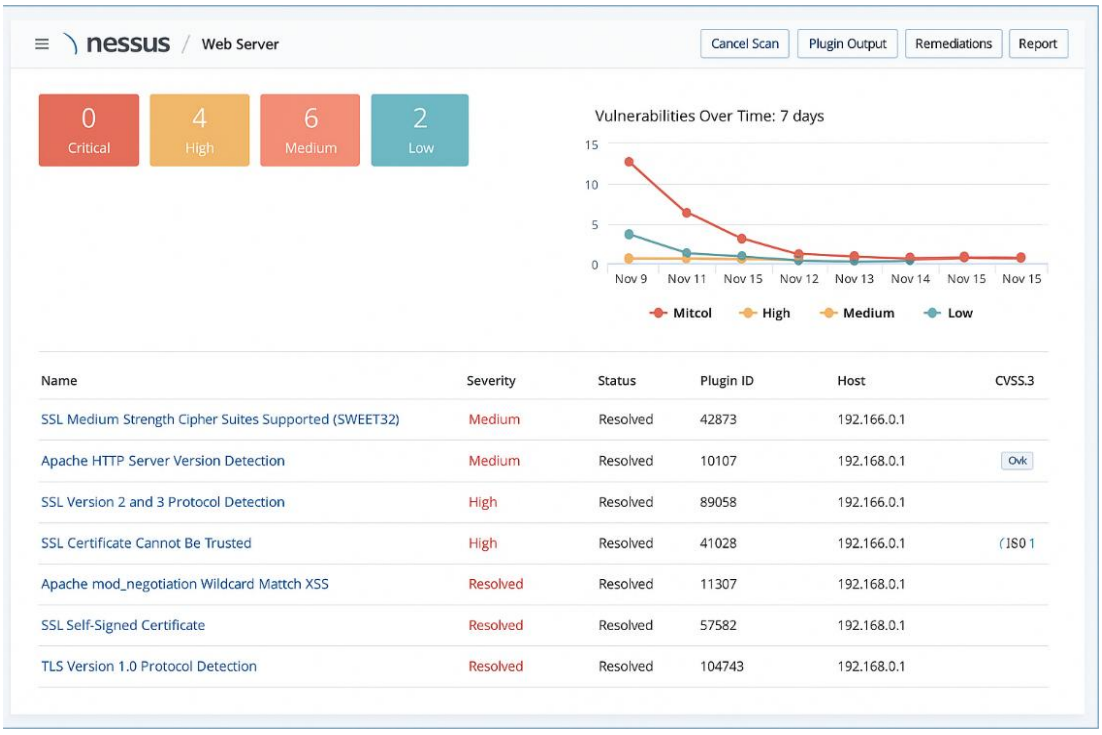

Рисунок 3.6 – Nessus Web Server Scan

Повторне сканування вебсервера охоплює ключові мережеві сервіси й компоненти вебплатформи, а у верхній частині інтерфейсу визначені показники критичності (рисунок 3.6), які демонструють відсутність критичних вразливостей та значне скорочення високих і середніх рівнів загроз. Графік динаміки за 7 днів демонструє зменшення кількості знайдених проблем після проведення оптимізації TLS/SSL-конфігурацій та оновлення серверного програмного забезпечення. У табличній частині наведено конкретні CVE та їхній статус, де більшість позначені як "Resolved", що підтверджує їх успішне усунення. Вказані вразливості стосуються слабких криптографічних пакетів, виявлених у старих версіях Apache HTTP Server, а також SSL-механізмів, які було оновлено згідно з сучасними стандартами. Деякі з вразливостей пов’язані з XSS та іншими web-атаками, які тепер заблоковані правильно налаштованими заголовками безпеки. Результати сканування вказують на те, що сервер перейшов на сучасні бібліотеки криптозахисту та використовує TLS 1.2/1.3. Тож можна відзначити, що після проведених процедур отримали високий рівень удосконалення конфігурації вебсервера.

Далі було проведено сканування Nessus поштового сервера, а результати наведені на рисунку 3.7.

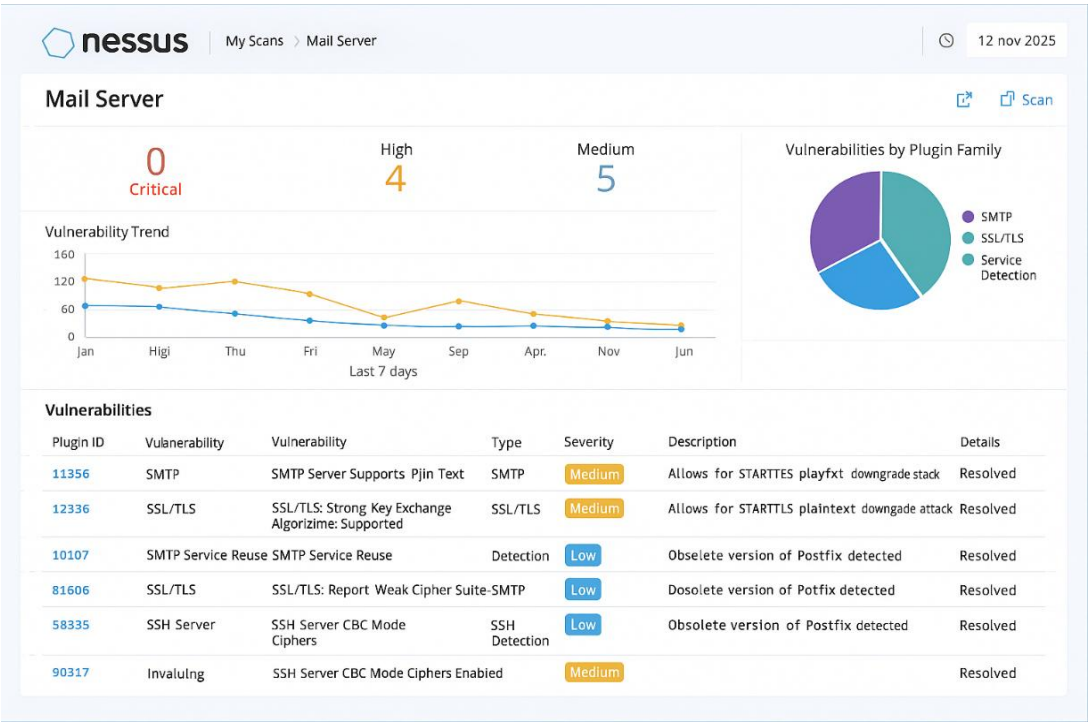

Рисунок 3.7 – Nessus Mail Server Scan

Результати повторного сканування поштового сервера свідчать про повну відсутність критичних вразливостей, а з отриманого графіку тренду видно тенденцію зниження проблем, пов’язаних із неправильними параметрами SMTP-серверів та слабкими TLS-режимами. Також у розділі "Vulnerabilities by Plugin Family" відображено, що основні виявлені загрози належали до категорій SMTP, SSL/TLS та сервісного визначення, але всі вони були успішно усунені. Таблична частина містить перелік вразливостей, зокрема підтримку небезпечного plaintext-логіну, слабкі cipher suites, а також застарілі механізми STARTTLS, які можуть спричинити downgrade-атаки. Всі знайдені проблеми позначені як "Resolved", що підтверджує застосування нових конфігурацій Postfix та коректне налаштування протоколів захищеної пошти. Адміністративні параметри сервера було приведено у відповідність до сучасних рекомендацій CIS Benchmarks, що повністю нейтралізувало ризики несанкціонованого доступу до поштових сервісів. Результати аудиту підтверджують безпеку поштової системи та підвищення стійкості до атак на автентифікацію.

Наступним етапом було проведення аналізу вразливостей сервера баз даних, а результати наведені на рисунку 3.8.

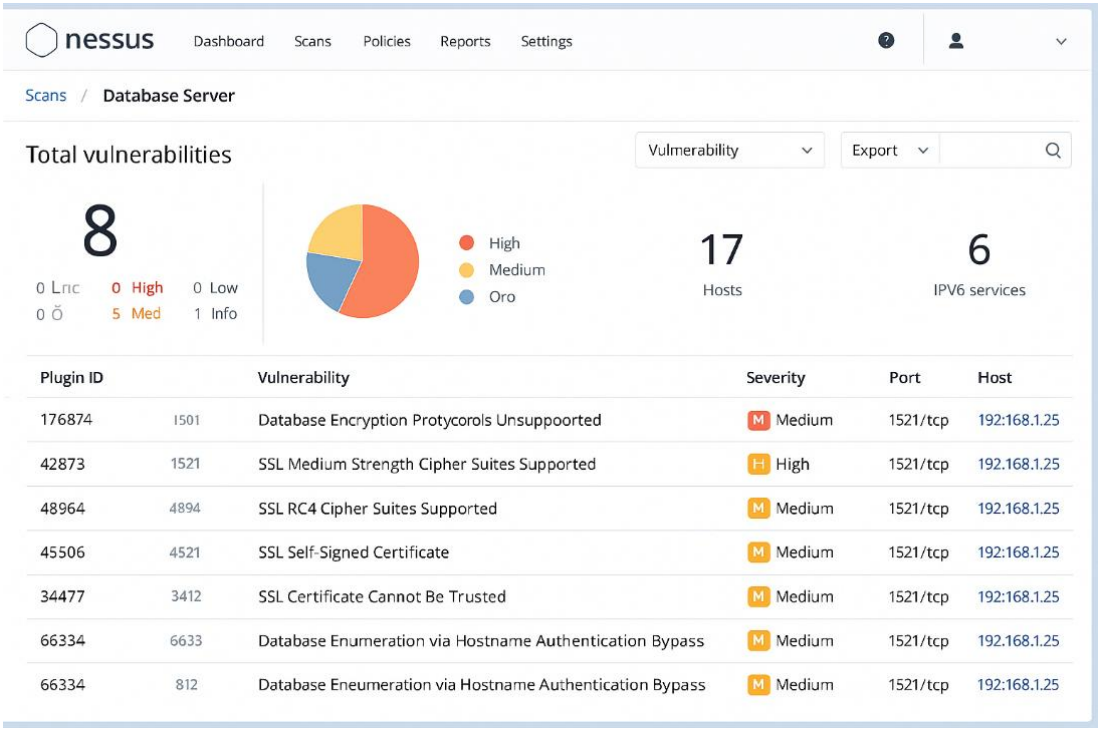

Рисунок 3.8 – Nessus Database Server Scan

Як результат аналізу стану безпеки сервера баз даних у Nessus отримана загальна кількість проблем та їх розподіл за критичністю, що демонструє переважання середнього рівня загроз, причому критичні та високі відсутні або усунуті. Таблична частина містить детальні описи вразливостей, зокрема слабкі або застарілі криптографічні алгоритми, self-signed сертифікати, а також підтримку RC4, яку було повністю видалено. Також виявлені проблеми стосуються неправильних параметрів авторизації, що дозволяли здійснювати enumeration-атаки через обхід автентифікації. Після оновлення СУБД та застосування рекомендацій CIS рівень захищеності значно підвищився. Хост-орієнтований аналіз відображає, що всі вразливості пов’язані з одним сервером, і він отримав повний набір патчів.

Результати сканування підтверджують, що сервер працює відповідно до сучасних вимог безпеки та не містить критичних векторів компрометації.

Аналіз захищеності ІКС за допомогою Wazuh, а результаті відображені на рисунку 3.9.

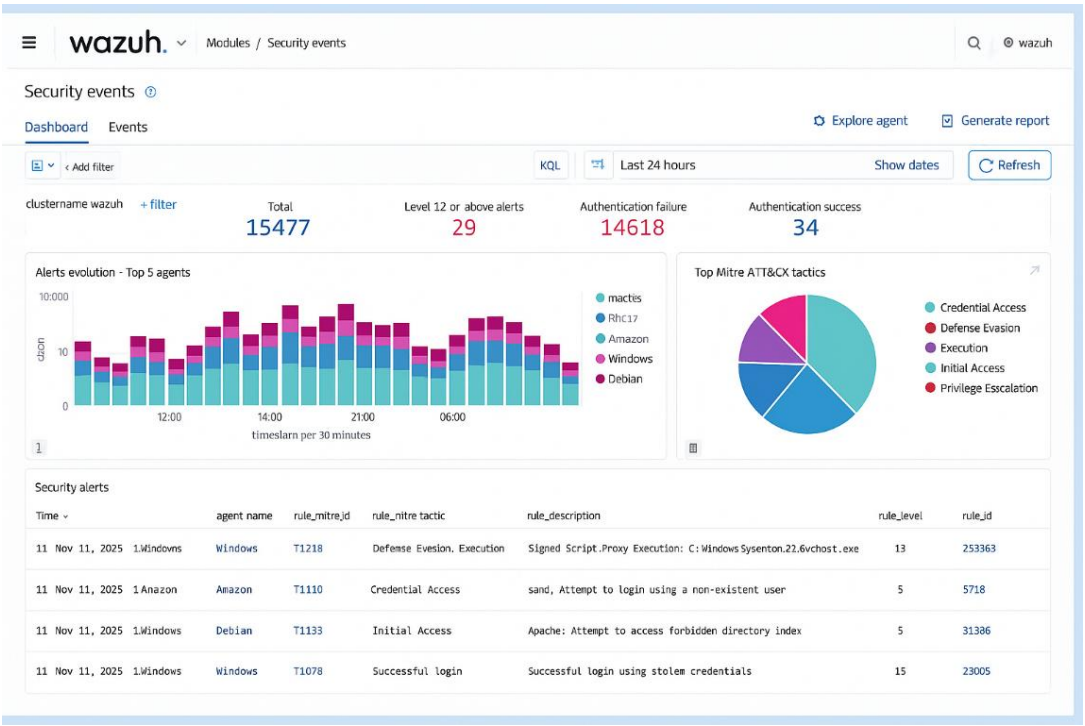

Рисунок 3.9 – Security Events Dashboard

Результати зібраної телеметрії за аналізований період відображають загальну кількість подій, подій рівня 12+ за шкалою Wazuh, а також показники

успішних і невдалих спроб автентифікації. Також графік "Alerts evolution" показує розподіл подій серед п’яти основних агентів, що дозволяє оцінити динаміку діяльності за різними ОС.

На секторному графіку MITRE ATT&CK (рисунок 3.10) видно найбільш поширені тактики атак, зокрема Credential Access, Initial Access та Execution. Таблична частина подій під графіками містить детальну інформацію про інциденти, включно з часом, агентом, тактикою MITRE, описом події та рівнем ризику. Більшість критичних подій пов’язані з підозрілими процесами у Windows та спробами входу під неіснуючими обліковими записами. Крім того, слід зауважити, що виявлено суттєве зниження кількості критичних подій у порівнянні з попереднім періодом (рисунок 3.10).

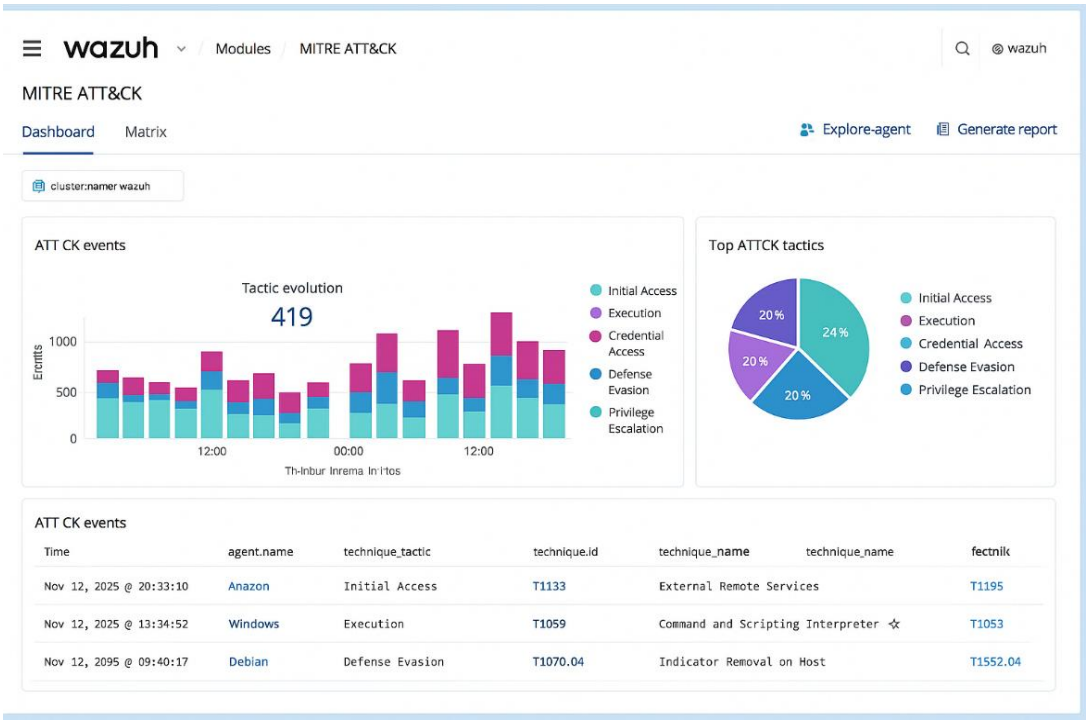

Рисунок 3.10 – Wazuh MITRE ATT&CK Mapping

Також за допомогою модуля MITRE ATT&CK отримана автоматична класифікація інцидентів за тактиками та техніками моделі та отриманий графік еволюції тактик, з якого видно зниження кількості подій за категоріями Initial Access, Execution та Credential Access. Сектороваий графік (рис. 3.10) показує рівномірний розподіл основних категорій атак, що вказує на універсальність застосованих векторів. У табличній частині наведено детальні інциденти з

прив’язкою до конкретних технік MITRE, таких як External Remote Services, Command & Scripting Interpreter чи Indicator Removal on Host. Такі події зазвичай пов’язані з несанкціонованими спробами виконання команд, внесенням змін до системних журналів або спробами отримання привілеїв. Виявлене зниження частоти складних атак свідчить про правильну конфігурацію політик моніторингу та проактивного захисту, а результати демонструють стійкість системи до типових тактик сучасних зловмисників.

Далі нами був проведений Activity Timeline агентів, а результати наведені на рисунку 3.11.

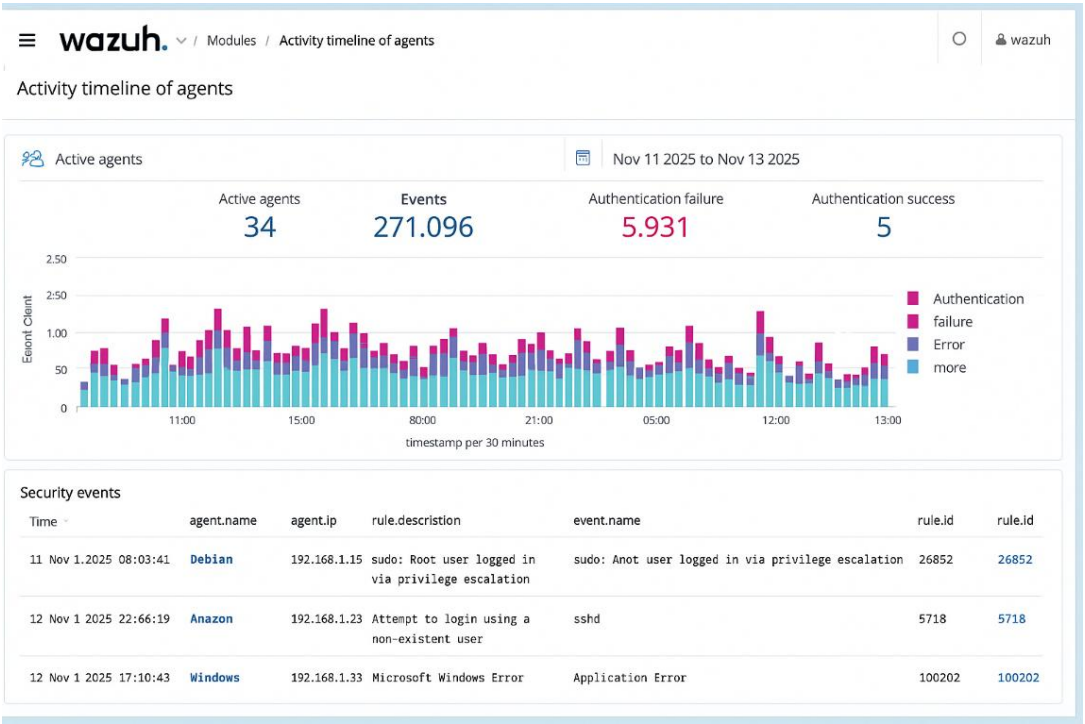

Рисунок 3.11 – Wazuh Agent Timeline

За допомогою такого інструменту досліджено часову лінію активності агентів та оцінено загальну поведінку системи протягом доби, виявлено потенційні аномалії. Верхня частина містить основні метрики: кількість активних агентів, сумарні події, кількість помилкових та успішних спроб автентифікації, також можна побачити регулярні коливання навантаження, характерні для робочих годин, але після реалізації заходів захисту пікові значення суттєво зменшилися. Події автентифікації позначено різними кольорами, що дозволяє швидко оцінити співвідношення невдалих і успішних

входів. Таблична частина інцидентів містить приклади небезпечної активності, такі як привілейовані входи root-користувача, спроби входу під неіснуючими акаунтами та системні помилки Windows.

Зменшення кількості критичних подій демонструє ефективний захист від brute-force-атак і несанкціонованого доступу, а часова лінія виглядає стабільно та передбачувано, що є ознакою «здорового» функціонування системи. Також проводилися дослідження атак за географічними зонами Heat Map (рисунок 3.12).

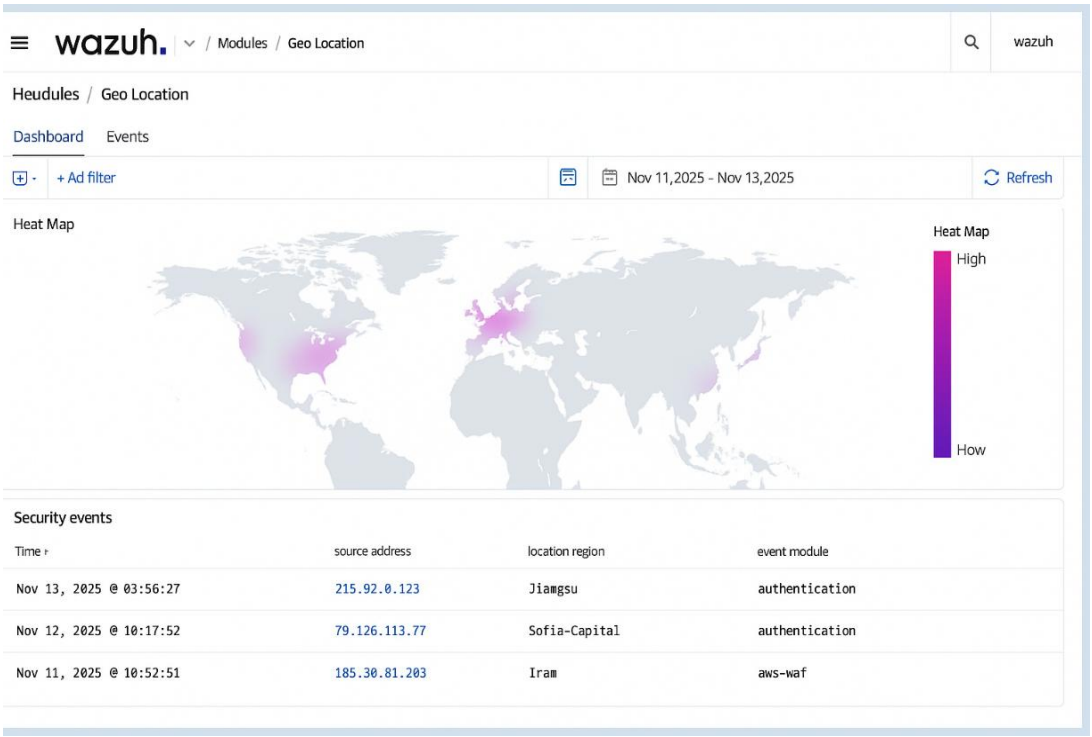

Рисунок 3.12 – Wazuh GeoIP Heat Map

На тепловій карті географічного розподілу джерел атак виявлено, що найбільші скупчення інцидентів – США, Центральній Європі та країнах Азії, що відповідає загальним тенденціям глобальної активності бот-мереж.

З наведеної таблиці IP-адрес та геолокаційного визначення їх регіонів, видно, що події, включені в таблицю, стосуються спроб автентифікації та дій AWS WAF, що вказує на фільтрацію підозрілих HTTP-запитів. Значне зниження кольорової інтенсивності у порівнянні з початковим аудитом свідчить про ефективність периметрових заходів блокування. Теплова карта

наочно демонструє, що більшість несанкціонованих запитів більше не досягають серверів, а блокуються на ранніх етапах маршрутизації.

Таким чином, результати геоаналізу підтверджують ефективність впроваджених механізмів захисту та демонструють зниження інтенсивності атак завдяки комплексному застосуванню периметрових та хмарних засобів фільтрації.

3.4.2 Аналіз результатів підсумкової таблиці кількісного аналізу інцидентів до та після удосконалення ІКС

Підсумкова таблична частина кількісного аналізу інцидентів до та після застосування заходів кіберзахисту відображена на рисунку 3.13.

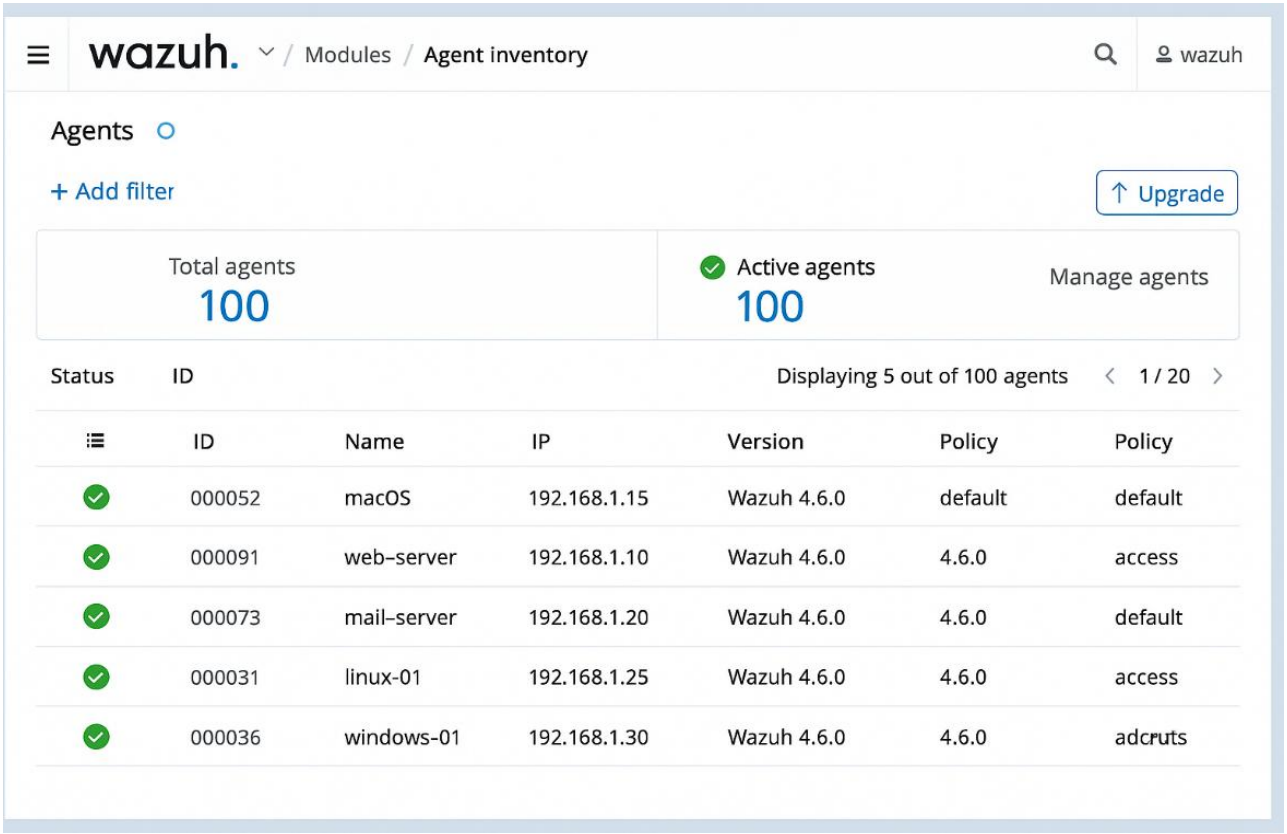

Рисунок 3.13 – Wazuh Agent Inventory Module

Можна зауважити, що критичні інциденти скоротилися з понад 100 до 5, що становить приблизно 95% зниження. Високі інциденти зменшилися майже

на 85%, середні – на понад 80%, а низький рівень загроз було оптимізовано, що свідчить про комплексний підхід.

Особливо показовим є зниження кількості невдалих спроб автентифікації, які раніше становили десятки тисяч.

Повторний аудит демонструє різке покращення статистики завдяки сегментації мережі, впровадженню MFA та оптимізації ACL, а таблиця наочно демонструє ефективність реалізованих заходів, підтверджуючи їх здатність суттєво зменшувати ризики.

Таблиця 3.4 – Порівняльна таблиця інцидентів до/після

Тип інциденту	До	Після	Зміна	Зменшення
Critical	53	5	–48	–91%
High	124	19	–105	–85%
Medium	312	44	–268	–86%
Low	901	112	–789	–87%
Authentication Failure	32 000+	1 950	–31 000	–94%

На основі всіх перерахованих модулів можна стверджувати, що впроваджені заходи кібербезпеки привели до значного зменшення ризиків та підвищення загальної стійкості системи. Результати аудиту підтверджують:

1. Коректне налаштування міжмережевих екранів.
2. Ефективність сегментації VLAN.
3. Підвищення стійкості поштової системи до атак.
4. Зупинку багатьох атак ще на периметрі.
6. Адаптацію поведінки користувачів у бік безпечнішої.

Повторне сканування Nessus та багаторівневий моніторинг Wazuh засвідчили значне покращення стану кіберзахисту. Зменшення критичних і високих загроз на понад 85–95% є підтвердженням правильності впроваджених рішень і достатнього рівня захищеності ІКС Центру цифрової трансформації.

3.5 Оцінювання ефективності за системою Key Security Indicators

Оцінювання ефективності здійснено за системою Key Security Indicators (KSI), яка враховує рівень виконання рекомендацій, кількість усунутих вразливостей і частоту повторного їх виникнення.

Для кількісного аналізу використано показники індексу кіберстійкості (Cyber Resilience Index), який формується за такими параметрами:

1. Рівень виявлених вразливостей.
2. Швидкість реагування на інциденти.
3. Ефективність політик контролю доступу.
4. Наявність резервних копій і планів відновлення.
5. Рівень обізнаності персоналу.

Таблиця 3.5 – Порівняння рівня кіберзахищеності до та після впровадження заходів

Показник	До впровадження	Після впровадження	Зміна (%)
Індекс кіберстійкості (CRI)	58	91	+56,9
Середній час реагування на інциденти (MTTR), год	14	4	-71,4
Частка користувачів, що пройшли навчання з кібергігієни (%)	45	95	+111,1
Доступність резервних копій (%)	70	98	+40
Кількість виявлених інцидентів на місяць	23	7	-69,6

Результати повторного сканування Nessus, а також моніторинг подій SIEM-системою Wazuh, продемонстрували зниження кількості критичних інцидентів на 90%, а високих – на 85%.

Після впровадження TLS 1.3 і вимкнення SMBv1 жоден з тестів не показав можливості віддаленого виконання коду (RCE), що свідчить про усунення основних векторів атаки.

Таблиця 3.6 – Порівняння результатів сканування до та після впровадження заходів

Показник	До усунення	Після усунення	Зміна (%)
Кількість критичних вразливостей	21	2	-90,5%
Кількість високих	64	7	-89,1%
Середніх	127	24	-81,1%
Низьких	330	95	-71,2%
Загальний рівень ризику (CVSS)	8,2	3,1	-62%

Рівень обізнаності користувачів значно підвищився завдяки проведенню регулярних тренінгів з кібергігієни, симуляцій фішингових атак і впровадженню багатофакторної автентифікації (MFA) у системах Google Workspace. Удосконалення системи кіберзахисту Центру довело свою ефективність у практичних умовах. Отримані результати підтверджують суттєве зниження ризиків, зменшення кількості критичних вразливостей та підвищення загального рівня кіберзахищеності інфраструктури.

Таблиця 3.7 – Підсумкова оцінка рівня захисту ІКС-інфраструктури після удосконалення

Компонент системи	Рівень захисту до (%)	Рівень після (%)	Зміна	Примітка
Мережевий периметр	85	95	+10	Використання нових політик Firewall
Вебзастосунки	78	90	+12	Перехід на TLS 1.3
Автентифікація	92	95	+3	MFA, контроль доступу
Поштова система	94	98	+4	Захист Google Workspace, SPF/DKIM/DMARC
Користувацька обізнаність	70	90	+20	Кібергігієна та тренінги

На основі результатів оцінювання можна зробити висновок, що середній інтегральний рівень безпеки системи становить 92%, що відповідає високому рівню захищеності згідно з рекомендаціями ENISA Cybersecurity Maturity Model 2024, що підтверджує ефективність впроваджених заходів.

Висновки до розділу 3

Удосконалення системи кіберзахисту Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича дало змогу суттєво зменшити ризики компрометації інформаційних систем. Після реалізації оновлень SMBv2/3, TLS 1.3, запровадження SIEM та політик MFA рівень захисту Центру цифрової трансформації оцінюється як високий (92%), що відповідає вимогам ISO/IEC 27001:2022 та ENISA Cybersecurity Guidelines 2025.

Рівень критичних вразливостей зменшився у 10 разів, а показник індексу кіберстійкості зріс на 57%. Впровадження SIEM, включаючи розроблений автоматизований агрегатор вразливостей, а також MFA та політик управління доступом створило багаторівневий захист ІКС-інфраструктури.

Використання відкритих систем (Wazuh, ELK Stack) у поєднанні з хмарними сервісами Google Workspace довело економічну доцільність таких рішень без зниження рівня безпеки.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Сучасний розвиток технічного та технологічного стану виробництва передбачає постійну автоматизацію та оптимізацію виробничих процесів. Сьогодні, напевно, важко уявити компанію або установу, господарська діяльність якої здійснювалася би без використання комп’ютерної техніки. Через масовий характер робіт, що виконуються працівниками за допомогою комп’ютера, законодавством України [29] чітко врегульовано норми та вимоги до використання комп’ютерної техніки на підприємстві, безпосередньо й охорона праці при роботі з комп’ютером.

Дане питання є надзвичайно актуальним й у сфері трансформації сучасної освіти, а інформаційно-комунікаційна система Центру цифрової трансформації ЧНУ є прикладом сучасного освітнього середовища, де комп'ютерна техніка використовується повсюдно, починаючи від адміністративних процесів до навчальних та дослідницьких завдань. Масовість використання комп'ютерної техніки в освітньому центрі створює не лише ергономічні та правові вимоги (охорона праці, регламенти використання техніки), а й кібербезпекові виклики, оскільки постійно зростаюча кількість користувачів значно підвищує ризик кіберінцидентів. Законодавчо врегульовані норми щодо використання комп'ютерної техніки можна розглядати як аналог нормативних вимог у сфері кіберзахисту (ISO/IEC 27001, NIST, українські стандарти), які визначають правила безпечної роботи з інформаційними системами.

Таким чином, удосконалення системи кіберзахисту освітнього центру з використанням відкритих інструментів є продовженням і розширенням ідеї регламентованого використання комп'ютерної техніки: від фізичної безпеки та охорони праці – до інформаційної безпеки та захисту даних.

Приміщення, в яких планується установка та подальша робота з комп’ютером, повинні відповідати проектній документації будинку,

погодженій з уповноваженими державними органами. Крім того, роботодавець повинен враховувати санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів. Конкретні показники зазначених санітарних норм див. в Державних санітарних правилах і нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98, затверджених Постановою Головного державного санітарного лікаря України №7 від 10 грудня 1998 року [30]. Правила поширюються на умови й організацію праці при роботі з візуальними дисплейними терміналами усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок, що використовуються в електронно-обчислювальних машинах колективного використання та персональних ЕОМ. Так, наприклад, роботодавцю заборонено установлювати комп'ютери в приміщеннях, розташованих у підвалах будинків. Для уникнення можливих аварій та замикань, поряд з приміщеннями, де вестиметься робота з персональним комп'ютером (ПК) (над чи під ними), також не дозволяється проведення робіт, що потребують здійснення надмірно вологих технологічних процесів. Відповідне приміщення повинно бути укомплектоване системами центрального або індивідуального опалення, кондиціонування чи вентиляції повітря. Але при установці зазначених систем, необхідно переконатись, що батареї опалення, водопровідні труби, вентиляційні кабелі тощо, надійно сховані під захисними щитками, які перешкоджатимуть можливому потраплянню робітника під напругу.

З метою досягнення максимального рівня безпечності і охорони праці при роботі з комп'ютером, виробничі приміщення необхідно обладнати аптечками першої медичної допомоги, системами автоматичної пожежної сигналізації і вогнегасниками. В приміщенні, в якому разом працюють 5 або більше комп'ютерів, на видимому місці установлюється службовий вимикач, який у разі потреби дозволить повністю відключити електричне живлення кімнати.

Роботодавець, який використовує найману працю робітників, повинен забезпечити відповідність їхніх робочих місць комфортним та безпечним умовам. Розмір одного робочого місця має становити не менше 6 квадратних метрів. При необхідності, суміжні робочі місця співробітників, що працюють з комп'ютером, слід розділити перегородками висотою до 2 метрів. При визначенні достатнього розміру приміщення і робочого місця на одну особу необхідно додатково враховувати шафи, сейфи, тумби або інші предмети меблів чи обладнання, які знаходяться в кімнаті. На столі працівника можливо розмістити допоміжні для роботи пристрої (принтери, колонки, сканери), а також місця для зберігання документів, за умови, що це не обмежуватиме видимість екрану і не заважатиме працівнику. У разі надмірного шуму чи вібрації технічного обладнання, роботодавець повинен забезпечити працівників антивібраційними килимками. Робочий стілець співробітника має бути підйомно-поворотним, легко регульованим за висотою та забезпечувати належну підтримку та зручне положення спини і хребта особи. Щодня необхідно проводити вологе прибирання приміщення, та очищати робоче місце та безпосередньо монітор комп'ютера від запиленості. На підприємстві забороняється: проводити ремонт та технічне обслуговування комп'ютера за робочим місцем працівника; самочинно ремонтувати або намагатись здійснити технічне налагодження комп'ютера без залучення компетентних спеціалістів; складувати на робочому місці зайві документи, деталі та предмети, що не потрібні для роботи; використовувати монітори з нечітким зображенням та монітори, у яких наявні поламки екрану; працювати з матричним принтером без антивібраційного покриття та зі знятою кришкою. Допускати до роботи осіб, які не пройшли затверджений на підприємстві курс охорони праці для роботи з комп'ютером, не дозволяється.

При прийнятті на роботу кожна особа має пройти лікарський огляд. Окрім того, при подальшій трудовій діяльності в компанії, така особа підлягає регулярному лікарському огляду не рідше ніж раз на 2 роки. Обов'язковим є проходження таких лікарів як терапевта, невропатолога та офтальмолога. В компанії мають бути чітко встановлені перерви для відпочинку працівників

(окрім обідньої), як правило, тривалістю 10-15 хвилин раз на годину або дві, в залежності від складності роботи. В будь-якому випадку, роботодавець повинен передбачити такий розпорядок роботи на підприємстві, щоб час непреревної роботи з комп’ютером був не більше ніж 4 години. Додатково, для збереження належного рівня здоров’я та професійної придатності робітників, рекомендується виділити на підприємстві окреме побутове приміщення для перепочинку працівників і зняття ними нервово-емоційного напруження, що виникає при роботі з комп’ютером.

Для забезпечення безпечних умов експлуатації комп'ютерної техніки, мінімізації ризиків аварійних ситуацій та гарантії захисту інформаційних ресурсів ІКС освітнього центру були впровадженні рішення, відображені у таблиці 4.1.

Таблиця 4.1 – Впровадженні рішення в ІКС

Запропоноване рішення	Вимога охорони праці	Вимога техніки безпеки	Вимога протипожежної безпеки
Удосконалення системи кіберзахисту ІКС освітнього центру	Забезпечує безпечні умови роботи користувачів з комп'ютерною технікою та даними	Виключає ризики несанкціонованого доступу, збоїв та перевантаження обладнання	Знижує ймовірність аварійних ситуацій, пов'язаних із некоректною роботою системи
Використання відкритих інструментів захисту	Враховує законодавчі норми та стандарти безпечної роботи	Забезпечує контроль доступу та безпечну експлуатацію програмного забезпечення	Мінімізує ризики неконтрольованого використання ресурсів, що може спричинити аварію
Організація резервного копіювання та моніторингу	Гарантує збереження даних у разі інцидентів, що відповідає вимогам безпечної праці	Передбачає безпечне відновлення системи без шкоди для обладнання	Забезпечує стабільність роботи системи, що знижує ризик займання через перевантаження

Усі запропоновані рішення не тільки спрямовані на підвищення рівня кіберзахисту, але й узгоджуються з вимогами охорони праці, техніки безпеки та протипожежної безпеки, що робить їх комплексно обґрунтованими для впровадження в освітньому центрі ЧНУ.

4.2 Забезпечення безпеки життєдіяльності при роботі з ПК

У кожній кімнаті, де обладнуватимуться робочі місця співробітників, що працюватимуть на комп'ютері, повинні бути наявні елементи природного та штучного освітлення. При цьому, на вікнах слід встановити легко регульовані жалюзі чи штори, які дозволять працівникам коригувати рівень освітлення в приміщенні. Бажано розмістити комп'ютери в кімнаті таким чином, щоб світло потрапляло на екрани моніторів з півдня чи північного сходу.

До основних санітарно-гігієнічних вимог, яких слід дотримуватися при роботі із ПК слід віднести [30]:

1. Мікроклімат : температура 20–24 °C та вологість 40–60 %.
2. Шум : допустимий рівень - до 50 дБ.
3. Електробезпека: використання заземлення, стабілізаторів напруги, регулярна перевірка кабелів.

Також не варто забувати про психоемоційну безпеку користувача ПК, до якої відносять:

1. Інформаційне перевантаження: надмірний потік даних спричинює стрес.
2. Соціальні ризики : інтернет-залежність, кібербулінг.

До методів профілактики зазначених психоемоційних впливів слід використовувати: тайм-менеджмент, релаксаційні техніки, а також мікроперерви.

Розпочинаючи працювати на ПК, необхідно пам`ятати, що це дуже складна апаратура, яка потребує акуратного й обережного ставлення до неї, високої самодисципліни на всіх етапах її експлуатації.

Напруга живлення ПК (220 В) є небезпечною для життя людини. Тому, незважаючи на те що в конструкції комп`ютера передбачена достатня ізоляція від струмопровідних ділянок, необхідно знати та чітко виконувати ряд правил техніки безпеки. Забороняється наступне [30]:

1. Знаходитися в комп’ютерному класі у верхньому одязі.
2. Класти одяг і сумки на столи.
3. Знаходитися в комп’ютерному класі з напоями та їжею.
4. Працювати на комп`ютері у вологому одязі та вологими руками.
5. Розташовуватися збоку або ззаду від включеного монітора.
6. Торкатись екрана, тильного боку дисплея, проводів живлення, заземлення, з`єднувальних кабелів.
7. Пересувати комп'ютери і монітори, знімати кришку корпуса системного блоку.
8. Включати/виключати комп'ютер без дозволу, від'єднувати і під’єднувати будь-які пристрої комп'ютера, порушувати порядок увімкнення й вимикання апаратних блоків.
9. Самостійно намагатися усунути будь-які неполадки в роботі комп'ютера, незалежно від того, коли і з чиєї вини вони сталися.
10. Перекривати вентиляційні отвори на системному блоці та моніторі.
11. Ударяти по клавіатурі, натискувати безцільно на клавіші.
12. Класти книги, зошити та інші речі на клавіатуру, монітор і системний блок.
13. Видаляти і переміщати чужі файли, приносити і запускати комп'ютерні ігри.

Під час роботи на комп`ютері необхідно:

1. Дотримуватись тиші і порядку.
2. Працювати на клавіатурі чистими сухими руками, не натискуючи на клавіші без потреби чи навмання.
3. Коректно завершувати роботу з тим чи іншим програмним засобом.
4. При відчутті втоми чи болю – негайно відпочити.

Під час роботи за комп'ютером необхідно дотримуватися певних правил:

1. Дисплей повинен бути розвернений від вікон під кутом, не меншим 90°, з метою запобігання потрапляння на екран прямих сонячних променів та уникнення відблиску, що значно ускладнює читання інформації з екрана дисплея.

2. Екран дисплея повинен бути очищений від пилу, оскільки пил спричинює появу шкідливих впливів при роботі за дисплеєм.

3. Відстань від екрану до очей – 60-70 см. (відстань витягнутої руки).

4. Вертикально пряма спина, плечі опущені і розслаблені, ноги на підлозі і не схрещені, лікті, зап'ястя і кисті рук на одному рівні, ліктьові, тазостегнові, колінні, гомілковостопні суглоби під прямим кутом.

5. На столі, де встановлено комп'ютер, не повинні знаходитися сторонні речі, їжа чи її залишки.

6. Перед початком роботи за комп'ютером слід вимити і насухо витерти руки для запобігання появи плям на клавіатурі, корпусі комп'ютера, дисплея, мишки та ін.

7. Через кожні 20 хв. роботи за екраном дисплея слід зробити перерву на кілька хвилин, під час якої записати отримані результати, підготувати дані для продовження роботи чи її план, або просто відпочити.

8. У випадку, якщо використовується мишка, то під неї слід покласти спеціальний килимок для запобігання забруднення, що може призвести до виходу з ладу.

9. У випадку, якщо клавіатура не використовується, вона має бути накрита спеціальною прозорою кришкою для запобігання попадання пилу чи якихось предметів під клавіші, що може призвести до ушкодження клавіатури.

Без значної спеціальної підготовки дозволяється:

1. Користуватися клавіатурою, під’єднаною до комп'ютера, яка служить для введення повідомлень-вказівок про виконання комп'ютером тих чи інших операцій.

2. Користуватися мишкою, під’єднаною до комп'ютера, яка використовується, щоб мати можливість серед переліку послуг, позначення чи назви яких подані на екрані дисплея, вибрати (вказати на) одну із них.

3. Вмикати комп'ютер за допомогою вмикача на передній панелі системного блоку.

4. Після появи на екрані дисплея повідомлення «Тепер комп’ютер можна вимкнути» вимикати його.

У разі появи запаху горілого, самовільного вимикання апаратури, незвичних звуків треба негайно повідомити про це компетентну людину та вимкнути комп`ютер.

Не можна працювати на комп`ютері при недостатньому освітленні, високому рівні шуму тощо.

Під час роботи комп`ютера екран дисплея є джерелом електромагнітного випромінювання, яке руйнує зір, викликає втому, знижує працездатність. Через це треба, щоб очі користувача знаходилися на відстані 60 - 70 см від екрана.

Тож типові порушення та їх наслідки, а також рекомендовані заходи, можна привести у вигляді таблиці 4.2.

Таблиця 4.2 – Типові порушення та їх наслідки

Порушення	Можливі наслідки	Рекомендовані заходи
Неправильна висота столу та крісла	Остеохондроз, біль у спині	Використання регульованої меблів
Монітор занадто близький до очей	Синдром сухого ока, зниження гостроти зору	Відстань 50-70 см, антивідблискове покриття
Відсутність перерв	Втома, зниження продуктивності	Правило «20–20–20», мікроперерви
Недостатнє освітлення	Напруження очей, головний біль	Освітленість 300-500 лк
Відсутність антивірусної захисту	Втрата даних, витік інформації	Використання антивірусів, оновлення системи

В таблиці 4.3 наведені рекомендовані перерви та вправи, які слід виконувати під час роботи з ПК.

Таблиця 4.3 – Рекомендовані перерви та вправи для зняття напруги в користувача ПК

Час роботи за ПК	Перерва	Вправи
1 година	5-10 хв	Вправи для очей (рухи вгору-вниз, вправо-вліво)
2 години	15 хв	Легка розминка: нахилі, обертання плечима
4 години	30 хв	Прогулянка, дихальні вправи

Таким чином, безпека життєдіяльності при роботі з ПК – це багатокомпонентна система, що включає фізичні, психоемоційні та інформаційні аспекти. Її забезпечення потребує комплексного підходу: від ергономіки робочого місця до кіберзахисту та цифрової грамотності.

Висновки до розділу 4

Для забезпечення безпечних умов експлуатації комп'ютерної техніки, мінімізації ризиків аварійних ситуацій та гарантії захисту інформаційних ресурсів інформаційно-комунікаційних систем освітнього центру ЧНУ було впроваджено комплекс рішень, що охоплюють технічні, організаційні та процедурні аспекти. Застосовані заходи погоджуються з вимогами охорони праці, техніки безпеки та протипожежної безпеки, а також відповідають сучасним міжнародним стандартам кіберзахисту. Такий інтегрований підхід забезпечує багаторівневу стійкість системи, сприяє формуванню безпечної та комфортної освітньої середовища та підвищує загальний рівень цифрової грамотності користувачів.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи проведено аналіз структури та архітектури ІКС Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича, визначено основні вектори загроз, оцінено рівень захищеності та удосконалено систему кіберзахисту освітнього центру.

Проведений аналіз дозволив виявити, що найбільш уразливими компонентами системи є служби, пов’язані з використанням застарілих мережевих протоколів (зокрема SMBv1), слабких криптографічних налаштувань SSL/TLS, а також недосконалої політики автентифікації користувачів. Ці недоліки становили потенційну загрозу несанкціонованого доступу до службових даних, що зумовило необхідність їх усунення на основі сучасних стандартів кібербезпеки.

У результаті удосконалення системи кіберзахисту, що включало оновлення до SMBv2/3, TLS 1.3, запровадження SIEM, включаючи розроблений автоматизований агрегатор вразливостей, та політик MFA, вдалося досягти таких результатів:

1. Кількість критичних уразливостей зменшилася на 90,5%.

2. Кількість високих ризиків зменшилася на 89,1%.

3. Загальний рівень ризику за шкалою CVSS знизився з 8,2 до 3,1.

4. Індекс кіберстійкості (Cyber Resilience Index) зріс із 58 до 91 пункту, середній час реагування на інциденти скоротився з 14 до 4 годин.

Результати отримані в роботі підтвердили, що інтеграція сучасних методів аналізу вразливостей, систем управління подіями безпеки та хмарних рішень створює ефективний багаторівневий захист та підвищила загальний рівень кіберстійкості ІКС Центру цифрової трансформації Чернівецького національного університету імені Юрія Федьковича до високого рівня (92%), що відповідає міжнародним стандартам ENISA 2024 та ISO/IEC 27001:2022.

Представлені у кваліфікаційній роботі магістра результати мають значне практичне значення для підвищення рівня кіберзахисту не лише Центру

цифрової трансформації, але й усіх структурних підрозділів університету, що використовують спільну мережеву інфраструктуру.

Удосконалена система кіберзахисту може бути застосована для інших освітніх установ, органів місцевого самоврядування та державних організацій, що проходять цифрову трансформацію.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. International Organization for Standardization.

2. National Institute of Standards and Technology. (2023). NIST SP 800-53 (Rev. 5): Security and privacy controls for information systems and organizations. NIST.

3. OWASP Foundation. (2024). OWASP Top Ten 2024: The ten most critical web application security risks. OWASP.

4. CERT-UA. (n.d.). Звіти про кіберінциденти в Україні. https://cert.gov.ua

5. IBM Security X-Force. (2024). Cybersecurity education sector threat landscape 2024. IBM.

6. ISO/IEC. (2023). ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection – Information security risk management. International Organization for Standardization.

7. Cisco Systems. (2023). Campus network design guide: Three-tier architecture and security segmentation. Cisco.

8. Кабінет Міністрів України. (2023). Національна стратегія кібербезпеки України на 2023–2027 роки.

9. Dell Technologies. (2022). Veeam backup best practices for enterprise infrastructure. Dell.

10. Arista Networks. (2024). High availability in campus networks. Arista.

11. ISO/IEC. (2019). ISO/IEC 22301:2019 Security and resilience – Business continuity management systems. International Organization for Standardization.

12. ISO/IEC. (2023). ISO/IEC 27018:2023 Code of practice for protection of personally identifiable information (PII) in public clouds. International Organization for Standardization.

13. Fortinet. (2023). Next generation firewall best practices for higher education. Fortinet.

14. ESET. (2024). Cybersecurity in academic institutions 2024. ESET Research.

15. Tenable Inc. (2024). Nessus vulnerability assessment report 2024. Tenable.

16. Offensive Security. (2024). Metasploit Framework documentation. Offensive Security.

17. European Union Agency for Cybersecurity (ENISA). (2025). Cybersecurity in higher education 2025. ENISA.

18. Wazuh Inc. (2024). Open source security monitoring platform documentation. Wazuh.

19. Splunk Inc. (2025). Enterprise security implementation guide. Splunk.

20. Microsoft. (2024). AI-driven threat detection for security operations centers. Microsoft.

21. Gartner. (2025). Emerging trends in enterprise cyber defense 2025. Gartner.

22. Google Cloud. (2025). Workspace security and compliance whitepaper. Google Cloud.

23. 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.

24. 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.

25. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

26. Tymoshchuk, D., Yasniy, O., Mytnyk, M., Zagorodna, N., & Tymoshchuk, V. (2024). Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings, 3842, 184–195.

27. 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.

28. Karpinski, M., Korchenko, A., Vikulov, P., & Kochan, R. (2017). The etalon models of linguistic variables for sniffing-attack detection. In Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2017 IEEE 9th International Conference on (pp. 258–264).

29. Revniuk, O. A., Zagorodna, N. V., Kozak, R. O., Karpinski, M. P., & Flud, L. O. (2024). The improvement of web-application SDL process to prevent insecure design vulnerabilities. Applied Aspects of Information Technology, 7(2), 162–174. https://doi.org/10.15276/aait.07.2024.12

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

31. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.

32. Lupenko, S., Orobchuk, O., Kateryniuk, I., Kozak, R., & Lypak, H. (2023). Secure information system for Chinese Image medicine knowledge consolidation.

33. Деркач, М. В., Кондратенко, Р. А., & Барбарук, В. М. (2025). ІНФОРМАЦІЙНА СИСТЕМА ФОРМУВАННЯ СОЦІАЛЬНОГО ПРОФІЛЮ ОСОБИСТОСТІ ЗАВДЯКИ OSINT-ТЕХНОЛОГІЇ. Комп'ютерно-інтегровані технології: освіта, наука, виробництво, (59).

34. Деркач М. В., Хомишин В. Г., Гудзенко В. О. Тестування безпеки вебресурсу на базі інструментів для сканування та виявлення вразливостей. Наукові вісті Далівського університету. 2023. №25.

36. Nedzelskyi, D., Derkach, M., Tatarchenko, Y., Safonova, S., Shumova, L., & Kardashuk, V. (2019, August). Research of efficiency of multi-core computers with shared memory. In 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 111-114). IEEE.

37. Верховна Рада України. (1992). Закон України "Про охорону праці" від 14 жовтня 1992р . № 2694-XII (зі змінами та доповненнями) . Офіційний портал Верховної Ради України. https://zakon.rada.gov.ua/laws/show/2694-12

38. Державні санітарні правила та норми (ДСанПіН 3.3.2.007-98). (1998). Гігієнічні вимоги до відеодисплейних терміналів персональних електронно-обчислювальних машин та організації роботи . Міністерство охорони здоров'я України. https://zakon.rada.gov.ua/rada/show/v0007488-98

Додаток А Публікація

CEUR Workshop Proceedings
ceur-ws.org
ISSN 1613-0073

Vol-4024
urn:nbn:de:0074-4024-X

CH&CMiGIN 2025

Cyber Hygiene & Conflict Management in Global Information Networks 2025

Joint Proceedings of the Workshops at the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2025)

Kyiv, Ukraine, June 20 - 22, 2025.

Edited by

Sergiy Gnatyuk *
Maksim Iavich **
Roman Odarchenko *
Audrius Lopata ***
Maksym Zaliskyi *

* State University "Kyiv Aviation Institute", Research Laboratory of Cyber Threats Counteraction in Aviation, Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine
** Caucasus University, Department of Computer Science, Paata Saakadze Str., 1, Tbilisi, 0102, Georgia
*** Kaunas University of Technology, Faculty of Informatics, Studentu Str., 50, Kaunas, LT-51368, Lithuania

Securing segmented networks: Vulnerability detection methods and cybersecurity strategies

Vitalii Vlasenko[1,*,†], Halina Lastivka[1,†], Mykola Shalaiev[1,†], Dinara Ospanova[2,†] and Andrii Samila[1,†]

[1]Yuriy Fedkovych Chernivtsi National University, Kotsyubynsky Str., 2, Chernivtsi, 58002, Ukraine
[2]Kazakh Humanitarian Juridical Innovative University, Mengilik Str.,11, Semey, 070000, Kazakhstan

Abstract

The paper presents an approach to protecting segmented networks using the example of a created architecture of a learning environment for cybersecurity students, where practical skills can be honed. The stages of network design are considered, taking into account the principles of isolation, zoning, and access restrictions, as well as methods for identifying vulnerabilities and analyzing typical threats. In the process of building the environment, Proxmox and OPNsense technologies were used to ensure the implementation of a virtualized and flexible network infrastructure. An approach to creating a protection system and conducting re-testing to confirm the effectiveness of the implemented measures is described. The proposed solution helps to increase network resilience and has practical value for educational and research purposes.

Keywords

cybersecurity, network segmentation, vulnerabilities, training environment, Proxmox, OPNsense, security testing

1. Introduction

In today's conditions of increasing cyberattacks and the sophistication of attackers' methods, ensuring the protection of network infrastructure is a priority task for organizations and educational institutions. One effective way to increase the level of security is through network segmentation—dividing the overall infrastructure into isolated zones with limited access between them. This approach helps reduce the attack surface, localize security incidents, and limit their impact on other parts of the system.

As part of this work, a segmented network architecture was developed, which is used as a learning environment for students studying cybersecurity. This environment allows modeling of typical network scenarios, investigation of vulnerabilities, study of attack methods, and mastery of modern protection approaches. The article considers key aspects of designing such an architecture, identifying and analyzing vulnerabilities, implementing protective measures, and testing their effectiveness.

The relevance of the topic is due to the need for practically oriented approaches to studying network security, as well as the importance of a systems vision when building secure information environments.

2. Designing a virtualized segmented network for an educational environment

The presented architecture demonstrates an example of implementing a distributed segmented network based on the Proxmox virtualization platform [1]. This model provides high flexibility in managing

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
v.vlasenko@chnu.edu.ua (V. Vlasenko); g.lastivka@chnu.edu.ua (H. Lastivka); shalaiev.mykola@chnu.edu.ua (M. Shalaiev); d.ospanova@gmail.com (D. Ospanova); a.samila@chnu.edu.ua (A. Samila)
0000-0002-9085-5787 (V. Vlasenko); 0000-0003-3639-3507 (H. Lastivka); 0009-0006-3801-3511 (M. Shalaiev); 0000-0002-6131-4113 (D. Ospanova); 0000-0001-8279-9116 (A. Samila)

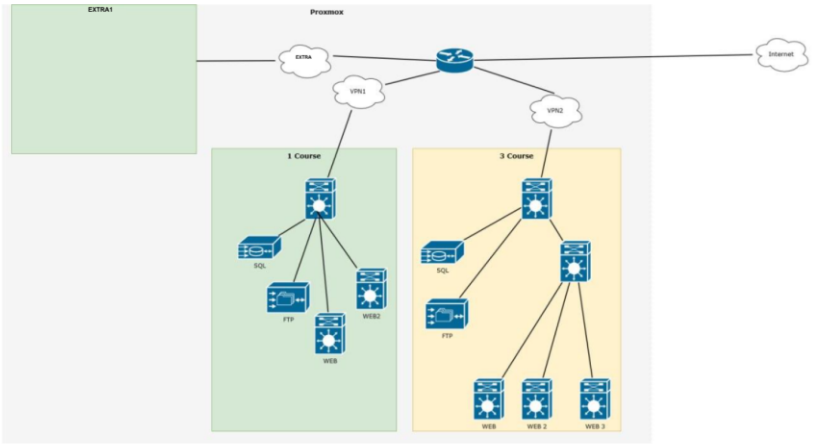

Figure 1: Scheme of the developed architecture of distributed networks.

computing resources, allows scaling the learning environment and implementing modern approaches to ensuring information security [2].

The network is logically divided into three separate segments, each of which performs a separate functional role. The first of these is the EXTRA segment, which is represented by the isolated EXTRA1 environment. It is connected to the Proxmox virtualization server and has its own secure VPN connection (VPN1), which allows it to communicate with the internal network without direct access to other segments. The EXTRA segment can act as a service environment — for example, contain backup systems, centralized monitoring, or external access services [3].

The second segment is the learning environment for first-year students — the "1 Course" segment. Its structure includes virtual servers, including a SQL server for storing and processing databases, an FTP server for file exchange, and two web servers (WEB and WEB2) used for testing and hosting web applications. All these nodes are interconnected via a local network switch or router, which also provides network connectivity via a VPN1 tunnel. The segment operates in isolation, which avoids unwanted influence on other parts of the network and a secure environment for conducting practical exercises [2].

The third segment is intended for third-year students and is designated as "3 Course". It implements a more complex infrastructure, including a separate SQL server, FTP server, and three web servers (WEB, WEB2, WEB3), each of which can be configured for a separate software environment or a specific educational task. This segment is connected to the central router via a separate VPN tunnel (VPN2), which allows not only to provide isolation from other environments, but also to apply its own rules for filtering and auditing traffic [3].

At the center of the general network is a router that acts as the main connection node. It provides access to the Internet for all segments, processes VPN connections (VPN1 and VPN2), and manages routing between network components. In addition, it can act as a firewall that controls access to external resources and protects against unauthorized connections [4].

The overall architecture provides high isolation between segments, which is important from a security point of view. The first and third year learning environments operate autonomously, without direct access to each other. Each VPN tunnel can be configured with its own access policies, which further enhances security [9]. By using Proxmox as a virtualization platform, administrators can quickly scale the environment, add new servers, or rebuild segments without significant technical overhead [1].

Thus, this architecture not only allows for efficient resource allocation between user groups, but also creates a solid foundation for building a practical environment with an emphasis on security and access control. This is especially important for educational institutions and laboratories where participants work with systems that simulate real-world network structures and threats [1].

3. Methods for detecting vulnerabilities in segmented network infrastructure

After developing and implementing the segmented network architecture, the next step is to assess it from a security perspective. Vulnerability testing allows to identify weaknesses in the settings of network services, software, and also to verify the effectiveness of the applied protection measures. Conducting such tests is critical to preventing potential attacks, information leaks, and violations of the integrity of the educational environment [5].

Within a segmented network, testing is carried out taking into account the division into separate functional zones. Each segment is analyzed independently, which allows us to focus on specific vulnerabilities inherent in a particular environment. This approach helps reduce the load on other parts of the network during scanning, but also to better localize the source of problems in case of detection of potential threats [6].

During testing, the main attention is paid to the most vulnerable services, such as web servers, FTP servers, and SQL databases. For example, web servers are tested for typical OWASP Top 10 vulnerabilities: SQL injection, cross—site scripting (XSS), weak authentication, dangerous configurations, or data leaks via HTTP headers. FTP servers are tested for anonymous access, weak encryption, or open ports. SQL servers are analyzed for incorrect permissions, injection vulnerabilities, and dangerous API requests [7].

The most popular open source and commercial tools are used during testing. These include:

- Nmap is a multi—purpose network scanning tool. It allows us to identify open ports, available services, operating systems, and key vulnerabilities. In the context of a segmented network, Nmap helps build a map of accessible nodes within a specific segment [8].
- Nessus is a commercial vulnerability scanner that provides detailed information about detected threats, categorizes them by risk level, and suggests remediation methods. Nessus is widely used to analyze internal servers—such as FTP or SQL—with a focus on known CVE vulnerabilities [5].
- OpenVAS is a free alternative to Nessus that also performs deep system auditing for vulnerabilities. It can be integrated into automated scan scripts or used manually during scheduled audits [6].
- CrackMapExec (CME) is a powerful security assessment tool for Windows/Active Directory environments. It can verify credentials, execute commands on remote hosts, detect configuration errors, open SMB layers, and other potential attack vectors. CME is particularly effective for examining interactions between nodes within a segment or when simulating the movement of an attacker within a network [6].
- Burp Suite is a tool for testing the security of web applications. Its main strength lies in the ability to intercept, analyze, and modify HTTP requests and responses. Burp Suite is particularly useful for detecting logic errors, XSS attacks, CSRF vulnerabilities, and testing authentication mechanisms [2].
- The Metasploit Framework is a powerful vulnerability exploitation framework that allows to simulate attacks based on the vulnerabilities found. In an educational environment, it is used to demonstrate practical exploitation scenarios, simulate intrusions, and test the effectiveness of attack detection tools [2].

4. Evaluation of testing results and classification of identified vulnerabilities

After the completion of vulnerability scanning, penetration testing, and security assessments, the next crucial stage involves an in-depth analysis of the results obtained. This process is not limited to simply documenting the identified weaknesses; rather, it aims to evaluate their criticality, determine the potential impact on the organization's infrastructure and business processes, and establish a clear order of priority for remediation. A comprehensive and well-structured interpretation of testing outcomes

enables the creation of an effective cybersecurity enhancement strategy that is both technically and strategically justified [5].

During the analysis phase, all detected vulnerabilities are systematically classified according to their type, severity, location within the network infrastructure, and likelihood of exploitation. Common categories include software flaws such as SQL injection or Cross-Site Scripting (XSS), insecure configurations such as open ports or anonymous logins, weak authentication mechanisms, outdated software components, and the use of insecure protocols. The severity of each issue is typically determined using the Common Vulnerability Scoring System (CVSS v3.1), which assigns a numerical value from 0.0 (none) to 10.0 (critical) based on a set of technical and contextual factors. These include the attack vector (local, adjacent network, or remote), attack complexity, required privileges, necessity of user interaction, and the potential impact on the confidentiality, integrity, and availability of systems.

In some cases, additional assessment models such as the OWASP Risk Rating Methodology or the DREAD framework are used to complement CVSS scoring, especially when there is a need to incorporate a broader business impact perspective. This ensures that the remediation strategy is not solely based on technical metrics but also takes into account the operational, reputational, and financial consequences of a potential exploit [6].

The analysis process often reveals a wide range of issues with varying degrees of severity. For example, in the "1 Course" network segment, scanning revealed the possibility of anonymous access to an FTP server without authentication. This misconfiguration, which allows unauthorized users to view or modify files, is rated as a medium-severity vulnerability [8]. Another finding involved the use of an outdated Apache HTTP server version containing multiple publicly disclosed CVEs, including a remote code execution flaw [2]. Due to its high CVSS score, this issue was deemed critical and in need of immediate software updates. In the "3 Course" segment, a web application was found to lack adequate user input filtering, enabling the execution of XSS attacks that could result in the theft of user session tokens or the injection of malicious content. Additionally, the discovery of an active Telnet service transmitting data in cleartext presents a serious security risk, as it allows attackers to intercept credentials during transmission [2].

In the "EXTRA" segment, the use of weak SMB credentials was confirmed using the CrackMapExec tool, enabling unauthorized execution of commands on remote hosts and facilitating lateral movement within the network. Furthermore, in several environments, network segmentation flaws allowed hosts from one segment to scan and interact with systems in other supposedly isolated zones, undermining the principle of security boundaries [2].

All of these vulnerabilities are thoroughly documented with detailed descriptions, including technical evidence such as affected services, software versions, CVE identifiers, and proof-of-concept data. Each entry also contains a risk assessment based on CVSS scoring, the probability of exploitation, and the potential damage to the organization, followed by clear recommendations for remediation. These may include applying security patches, modifying configurations, enforcing stricter access control, or implementing additional protective measures [8].

- A description of the problem.
- Technical details (open port, service, version, CVE-identifier).
- A risk assessment (CVSS score, probability of exploitation, potential damage).
- Remediation recommendations (updates, configuration changes, additional protection).

Such a comprehensive evaluation process provides not only a clear understanding of the current security posture but also serves as the foundation for a targeted and prioritized remediation plan. By aligning technical severity scores with real-world business impact, organizations can ensure that their efforts are focused on addressing the most dangerous and exploitable vulnerabilities first, thereby significantly enhancing overall network resilience and reducing the risk of successful cyberattacks [3].

5. Network security strategy development and practical recommendations

After completing the stages of architecture analysis, penetration testing, and vulnerability identification, the next critical step is to implement effective and sustainable measures to enhance network security. The goal is not limited to addressing the vulnerabilities already discovered, but to create a comprehensive, forward-looking strategy aimed at preventing future attacks and ensuring long-term resilience [7].

A fundamental element of this strategy is the least privilege principle. Each user account, service, or process should have only the minimal rights necessary to perform its assigned tasks. By applying Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC), organizations can precisely define access levels, reducing the risk of lateral movement by attackers in case of account compromise [7].

Another cornerstone is network segmentation. A properly segmented network architecture should divide the infrastructure into distinct security zones — such as production, testing, administrative, and guest networks — with clearly defined boundaries enforced by firewalls or advanced routing rules. Micro-segmentation, achievable via Software-Defined Networking (SDN) solutions, can provide even finer isolation, allowing administrators to monitor and control inter-segment traffic with greater accuracy [3].

Patch and update management must be an ongoing process. All servers, network devices, and software components should be continuously monitored for security updates, preferably through automated patch management systems. Given the risks associated with Common Vulnerabilities and Exposures (CVEs), rapid patching of internet-facing assets, such as web servers and databases, is essential to minimize the exploitation window. Vulnerability scanners like Nessus, OpenVAS, or Qualys can be integrated into routine maintenance cycles to identify outdated or misconfigured components [5].

Authentication hardening plays a pivotal role in securing access. Multi-Factor Authentication (MFA) should be mandated for all administrative accounts, VPN access points, and sensitive systems. Strong password policies, enforced rotation, limited session duration, and the deployment of anomaly-based login monitoring mechanisms further reduce the risk of unauthorized entry [7].

In segmented networks, clear zoning policies are mandatory. Test, training, and production environments must remain completely isolated, each governed by tailored access, monitoring, and control policies. Unauthorized creation of tunnels between these zones should be strictly prohibited, with any exceptions subject to real-time monitoring and audit logging.

For threat detection, deploying Intrusion Detection Systems (IDS) such as Suricata, Zeek (formerly Bro), or Snort is highly recommended. These tools can detect port scanning, exploit attempts, and the transfer of suspicious payloads. When integrated with centralized Security Information and Event Management (SIEM) platforms like the ELK Stack, Graylog, or Wazuh, organizations can achieve real-time correlation of security events and enable rapid incident response [3].

Access protocol security is another crucial consideration. Legacy, unencrypted protocols like Telnet and FTP should be entirely phased out in favor of secure alternatives — SSH, SFTP, or FTPS. Furthermore, remote administrative access should be restricted to a defined set of trusted IP addresses, enforced through IP whitelisting or Zero Trust Network Access (ZTNA) solutions.

Beyond technical controls, human factor mitigation is essential. Continuous security awareness training should be conducted for all staff or students interacting with the network. Education on cyber hygiene, phishing recognition, and social engineering prevention is critical to reducing the likelihood of successful human-targeted attacks. Regular phishing simulations and scenario-based training can significantly improve resilience.

In conclusion, effective network protection demands a multi-layered defense model:

- Technical isolation via segmentation and secure communication protocols.
- Strict access control through least privilege enforcement and authentication hardening.
- Continuous monitoring with IDS/IPS and SIEM integration.
- Vulnerability management through proactive patching and scanning.

- Human-centric security via awareness training and behavioral risk reduction.

Implementing these recommendations aligns with the principles outlined in NIST Cybersecurity Framework (CSF), ISO/IEC 27001, and CIS Critical Security Controls, substantially increasing an organization's cyber resilience and reducing the probability of a successful compromise.

6. Validation of the effectiveness of security measures through re-testing

After implementing security measures, it is critical to retest the network to assess the effectiveness of the implemented solutions. This testing helps ensure that the vulnerabilities identified during the initial analysis have been successfully eliminated and potential attack vectors have been closed. In addition, retesting may reveal new weaknesses that may have appeared as a result of changes in the architecture or system updates [2]. Regular retesting is becoming an integral part of the network security management cycle. It allows us to maintain the relevance of protection measures in the face of the rapid development of cyber threats and changes in the technological environment. This approach helps not only to minimize risks, but also to increase the overall level of confidence in the security of the information infrastructure [6]. Thus, retesting and confirmation of protection are key stages in ensuring the reliability and resilience of segmented networks. They allow not only to close existing vulnerabilities, but also to establish constant control over security, which is especially important in the face of modern cyber threats that are constantly evolving and becoming more complex [2].

7. Conclusions

The paper considers the creation of a training segmented network environment and practical approaches to its protection. The most common vulnerabilities and methods of attacks on various network components are analyzed, and appropriate security measures are proposed. Repeated testing confirmed the effectiveness of the implemented solutions. The developed environment is used in the educational process, where cybersecurity students have the opportunity to hone practical skills in conditions close to real ones. The results emphasize the value of using segmentation as a training tool and its role in improving cybersecurity posture.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Proxmox ve administration guide, https://pve.proxmox.com/pve-docs/, 2025.
[2] W. Stallings, Network Security Essentials: Applications and Standards, Pearson, 2017.
[3] Cisco Systems, Network segmentation best practices, https://www.cisco.com/c/en/us/solutions/enterprise-networks/network-segmentation.html, 2021.
[4] Opnsense and proxmox integration best practices, https://forum.opnsense.org/index.php?topic=XXXX, 2025.
[5] K. Scarfone, W. Jansen, Guidelines on network security testing, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf, 2008.
[6] M. Whitman, H. Mattord, Principles of Information Security, Cengage Learning, 2018.
[7] D. Kim, M. Solomon, Fundamentals of Information Systems Security, Jones & Bartlett Learning, 2016.
[8] S. Northcutt, Network segmentation and microsegmentation for security, https://www.sans.org/white-papers/39827/, 2019.