

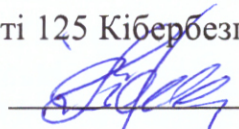
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології моніторингу та аналізу кіберзагроз в освітньому
середовищі»

Виконав: студент 2-го курсу групи ЗКБм-24-1

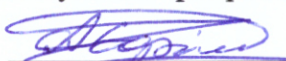
Спеціальності 125 Кібербезпека та захист інформації

 Ігор ВЕРБОВСЬКИЙ

Керівник: доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Житомир – 2025

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека та захист інформації»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

06 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Вербовський Ігор Андрійович

Тема роботи «Методи та технології моніторингу та аналізу кіберзагроз в освітньому середовищі»

затверджена Наказом університету від 06 жовтня 2025 р. № 566/с

Термін здачі студентом закінченої роботи 16 грудня 2025 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. Інформаційна інфраструктура цифрового освітнього середовища, що включає локальні мережі закладів освіти, хмарні та дистанційні сервіси, а також системи управління освітнім процесом.

2. Методи і технології ідентифікації, моніторингу та аналізу кіберзагроз, а також засоби автоматизованого реагування і управління інцидентами кібербезпеки в освітніх установах.

Обладнання та програмне забезпечення:

1. Програмне забезпечення для моделювання та емулювання мережевої інфраструктури: GNS3.

2. Віртуалізаційне середовище: VMware Workstation / VirtualBox.

3. Віртуальні серверні та клієнтські операційні системи: Windows Server 2019, Ubuntu Server 20.04/22.04 LTS, Ubuntu Desktop.

4. Системи моніторингу та управління подіями інформаційної безпеки (SIEM): Wazuh (Manager, Indexer, Dashboard, Agent).

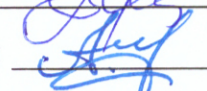
5. Системи виявлення та аналізу мережевих подій: Suricata, Zeek.

6. Інструменти аналізу мережевого трафіку та подій безпеки: Wireshark, Elastic Stack (Elasticsearch, Logstash, Kibana).

7. Засоби централізованого збору та аналізу журналів подій: Syslog, Filebeat.

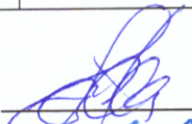
8. Інструменти тестування та аналізу безпеки: Nmap, Metasploit Framework.

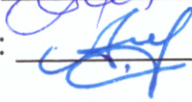
Студент:  Ігор ВЕРБОВСЬКИЙ

Керівник:  Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Терміни виконання етапів роботи	Примітка
1.	Затвердження теми	06.10.2025	
2.	Постановка завдання та визначення мети й завдань дослідження	06.10.2025–08.10.2025	
3.	Аналіз літературних джерел	09.10.2025–15.10.2025	
4.	Аналіз інформаційної інфраструктури та кіберзагроз освітнього середовища	16.10.2025–20.10.2025	
5.	Аналіз методів і технологій моніторингу та аналізу кіберзагроз	21.10.2025 – 26.10.2025	
6.	Обґрунтування вибору програмних рішень для моніторингу кіберзагроз	27.10.2025 – 31.10.2025	
7.	Моделювання системи моніторингу та аналізу кіберзагроз в освітньому середовищі	01.11.2025 – 07.11.2025	
8.	Розробка багаторівневої моделі захисту цифрового освітнього середовища	08.11.2025 – 13.11.2025	
9.	Аналіз результатів моделювання та оцінка ефективності запропонованих рішень	14.11.2025 – 18.11.2025	
10.	Формування висновків та пропозицій щодо підвищення кібербезпеки	19.11.2025 – 22.11.2025	
11.	Оформлення розділів пояснювальної записки	23.11.2025 – 05.12.2025	
12.	Оформлення списку використаних джерел та додатків	06.12.2025 – 10.12.2025	
13.	Остаточне оформлення пояснювальної записки	11.12.2025 – 16.12.2025	
14.	Подання завершеної кваліфікаційної роботи на кафедру	16.12.2025	
15.	Підготовка презентації та доповіді до захисту	17.12.2025 – 22.12.2025	
16.	Захист випускної кваліфікаційної роботи	23.12.2025	

Студент:  Ігор ВЕРБОВСЬКИЙ

Керівник:  Олексій ШЕЛУХА

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему «Методи та технології моніторингу та аналізу кіберзагроз в освітньому середовищі» складається зі вступу, трьох розділів, висновків, списку використаної літератури, додатків і має 99 сторінок основного тексту, 6 рисунків, 4 таблиці, 4 сторінки додатків. Список використаних джерел містить 83 найменування і займає 11 сторінок. Загальний обсяг роботи – 104 сторінки.

Метою роботи є обґрунтування, проектування та моделювання системи моніторингу та аналізу кіберзагроз у цифровому освітньому середовищі університету на основі сучасних методів, технологій та галузевих стандартів кібербезпеки.

У роботі визначено основні завдання забезпечення кібербезпеки освітнього середовища, проаналізовано інформаційну інфраструктуру університету та характерні для неї кіберзагрози, узагальнено базові методи й технології моніторингу кіберінцидентів, а також вимоги нормативних документів і стандартів (зокрема, NIST CSF, ISO/IEC 27035) до організації процесів виявлення та реагування на інциденти інформаційної безпеки. Розглянуто особливості цифрового освітнього середовища Житомирського державного університету імені Івана Франка, обґрунтовано вибір програмно-апаратних рішень для моніторингу подій безпеки й мережевого трафіку, побудовано проєктну модель багаторівневої системи моніторингу та аналізу кіберзагроз із виокремленням рівнів ідентифікації та автентифікації, моніторингу, аналітики та реагування. Показано розробку архітектури системи на основі SIEM/SOAR-платформи з інтеграцією з інфраструктурою університету, наведено результати моделювання процесів виявлення та оброблення інцидентів, сформовано рекомендації щодо впровадження ризик-орієнтованого підходу, використання показників MTTD/MTTR та удосконалення політик кібербезпеки в закладах вищої освіти.

Ключові слова: АНАЛІЗ ІНЦИДЕНТІВ, КІБЕРБЕЗПЕКА, МОНІТОРИНГ КІБЕРЗАГРОЗ, ОСВІТНЄ СЕРЕДОВИЩЕ, СИСТЕМА SIEM, СИСТЕМА SOAR, УПРАВЛІННЯ КІБЕРРИЗИКАМИ, ЦИФРОВИЙ УНІВЕРСИТЕТ.

ANNOTATION

The final qualification work on the topic “Methods and technologies for monitoring and analyzing cyber threats in the educational environment” consists of an introduction, three chapters, conclusions, a list of references, appendices, and has 99 pages of main text, 6 figures, 4 tables, and 4 pages of appendices. The list of references contains 83 items and occupies 11 pages. The total volume of the work is 104 pages.

The aim of the work is to justify, design, and model a system for monitoring and analyzing cyber threats in the university's digital educational environment based on modern methods, technologies, and industry cybersecurity standards.

The paper identifies the main tasks of ensuring cybersecurity in the educational environment, analyzes the university's information infrastructure and the cyber threats characteristic of it, summarizes the basic methods and technologies for monitoring cyber incidents, as well as the requirements of regulatory documents and standards (in particular, NIST CSF, ISO/IEC 27035) for organizing processes for detecting and responding to information security incidents. The features of the digital educational environment of Ivan Franko State University of Zhytomyr are considered, justifies the choice of software and hardware solutions for monitoring security events and network traffic, and builds a project model of a multi-level system for monitoring and analyzing cyber threats, distinguishing between the levels of identification and authentication, monitoring, analytics, and response. The development of a system architecture based on the SIEM/SOAR platform with integration into the university infrastructure is shown, the results of modeling the processes of incident detection and processing are presented, and recommendations are made for the implementation of a risk-oriented approach, the use of MTTD/MTTR indicators, and the improvement of cybersecurity policies in higher education institutions.

Keywords: INCIDENT ANALYSIS, CYBERSECURITY, CYBERTHREAT MONITORING, EDUCATIONAL ENVIRONMENT, SIEM SYSTEM, SOAR SYSTEM, CYBER RISK MANAGEMENT, DIGITAL UNIVERSITY.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОСВІТНЬОГО СЕРЕДОВИЩА.....	10
1.1. Аналіз інформаційної інфраструктури та кіберзагроз освітнього середовища	10
1.2. Аналіз методів та технологій моніторингу кіберзагроз	15
1.3. Постановка завдання дослідження	37
Висновки до розділу 1	42
РОЗДІЛ 2. ДОСЛІДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ КІБЕРЗАГРОЗ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ	44
2.1. Аналіз цифрового освітнього середовища Житомирського державного університету імені Івана Франка	44
2.2. Вимоги до забезпечення кібербезпеки в освітніх установах	53
2.3. Обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі	57
Висновки до розділу 2.....	69
РОЗДІЛ 3. МОДЕЛЮВАННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ КІБЕРЗАГРОЗ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ	71
3.1. Особливості інтеграції систем моніторингу в цифрове освітнє середовище	71
3.2. Моделювання багаторівневої системи захисту цифрового освітнього середовища	76
3.3. Аналіз отриманих результатів та пропозиції для подальших досліджень	82
Висновки до розділу 3	86
ВИСНОВКИ	88
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	90
ДОДАТКИ	100

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AI – Artificial Intelligence – штучний інтелект.

BYOD – Bring Your Own Device – власний пристрій користувача.

CTI – Cyber Threat Intelligence – кіберрозвідка щодо загроз.

DLP – Data Loss Prevention – система запобігання витоку даних.

IDS – Intrusion Detection System – система виявлення вторгнень.

IoC – Indicator of Compromise – індикатор компрометації.

IoT – Internet of Things – Інтернет речей.

IPS – Intrusion Prevention System – система запобігання вторгнень.

LMS – Learning Management System – система управління навчанням.

MFA – Multi-Factor Authentication – багатофакторна автентифікація.

ML – Machine Learning – машинне навчання.

SIEM – Security Information and Event Management – система управління інформаційною безпекою та подіями.

SOAR – Security Orchestration, Automation and Response – оркестрація, автоматизація та реагування на інциденти безпеки.

UEBA – User and Entity Behavior Analytics – аналітика поведінки користувачів та об'єктів.

VPN – Virtual Private Network – віртуальна приватна мережа.

ZTA – Zero Trust Architecture – архітектура нульової довіри.

ВСТУП

Актуальність. Постійне зростання кількості кібератак на заклади вищої освіти та розширення цифрового навчального середовища обумовлюють необхідність розробки ефективних механізмів захисту, що базуються на системному аналізі існуючих загроз та впровадженні інноваційних моніторингових рішень. Вплив кіберзлочинності може проявлятися через компрометацію даних студентів і викладачів, дестабілізацію роботи освітніх платформ і порушення освітнього процесу, тому питання захищеності інформаційної інфраструктури набуває пріоритетного значення для освітньої сфери.

Мета роботи полягає у визначенні оптимальних підходів до впровадження систем моніторингу та аналізу кіберзагроз, які сприятимуть підвищенню рівня кіберстійкості закладів освіти і захисту їх інформаційних ресурсів. Реалізація означеної мети передбачає обґрунтування вибору сучасних технологій моніторингу, системного аналізу факторів ризику та розробку моделі багаторівневої системи захисту, що відповідає актуальним нормативним вимогам, державним стандартам та національній стратегії кібербезпеки України.

Для досягнення поставленої мети передбачимо розв'язання наступних завдань:

- аналіз існуючих методів забезпечення кібербезпеки освітнього середовища;
- оцінка сучасних технологій моніторингу кіберзагроз та моделювання інцидентів;
- формулювання вимог до безпечної інфраструктури ЗВО та обґрунтування критеріїв ефективності захисту;
- розробка теоретичних основ і практичних рекомендацій щодо проєктування та інтеграції систем моніторингу й аналізу кіберзагроз у цифрове освітнє середовище.

Об’єктом дослідження є інформаційна інфраструктура цифрового освітнього середовища, що включає локальні мережі закладів освіти, хмарні та дистанційні сервіси, а також системи управління освітнім процесом.

Предметом дослідження виступають методи і технології ідентифікації, моніторингу та аналізу кіберзагроз, а також засоби автоматизованого реагування і управління інцидентами кібербезпеки в освітніх установах.

Апробація результатів дослідження: Результати кваліфікаційної роботи були представлені на міжнародних та всеукраїнських наукових конференціях, що підтверджується публікаціями тез доповідей:

1. Вербовський І. А. Кібербезпека фінансових операцій закладів вищої освіти в умовах тотальної цифровізації. Організаційно-правові аспекти публічного управління : матеріали XII Міжнар. наук.-практ. Інтернет-конф., 24 квіт. 2025 р. Полтава : Нац. ун-т ім. Юрія Кондратюка, 2025. С. 180-183. URL: <https://eprints.zu.edu.ua/45562/>

2. Вербовський І., Шелуха О. Моделювання поведінки користувачів в освітніх LMS-системах. Науковий пошук молодих дослідників : зб. наук. пр. студентів, магістрантів та викл. Житомир : Вид-во ЖДУ ім. І. Франка, 2025. Вип. 18. С. 33-37. URL: <https://eprints.zu.edu.ua/44884/>

3. Вербовський І.. Кібербезпека в цифровому освітньому середовищі: виклики, загрози та шляхи їх подолання : зб. матеріалів конф., 22-23 трав. 2025 р. Житомир : Вид-во ЖДУ, 2025. С. 17-22. URL: <https://eprints.zu.edu.ua/id/eprint/45524>

4. Вербовський І. Кібербезпека у цифрових фінансових системах закладів вищої освіти: ризики та засоби захисту. Science and Information Technologies in the Modern World : 2 Міжнар. наук.-практ. конф., 21-23 трав. 2025 р. Афіни, 2025. С. 199–202. URL: <https://eprints.zu.edu.ua/43825/>

5. Verbovskyi I. Classification and main types of cyber threats to the educational environment. Global Trends in Science: Research, Innovation and Development : 1st International Scientific and Practical Conference. Varna, 2025. P. 118–121.. URL: <https://eprints.zu.edu.ua/44270/>

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОСВІТНЬОГО СЕРЕДОВИЩА

1.1. Аналіз інформаційної інфраструктури та кіберзагроз освітнього середовища

У сучасних умовах українське освітнє середовище зазнало потужного впливу як геополітичних, так і технологічних факторів, що спричинило необхідність інтеграції інноваційних систем безпеки на всіх рівнях управління та функціонування закладів освіти.

Інформаційна інфраструктура освітнього середовища охоплює не лише матеріально-технічні ресурси, а й цифрові платформи, системи управління навчанням (Learning Management System, LMS), корпоративні інформаційні мережі, сервери, сховища даних, лабораторні комплекси, бібліотечні ресурси, IoT-пристрої та віддалений доступ до навчального контенту. В умовах війни та масового переходу до змішаного і дистанційного навчання суттєво зросло навантаження на цифрову інфраструктуру, що призвело до масштабного впровадження хмарних сервісів, підвищених вимог до кіберстійкості та багаторівневого резервного копіювання даних [7, 26].

Серед ключових компонентів цифрової інфраструктури освітніх закладів виділяють внутрішні мережі з доступом до Інтернету, електронні журнали та щоденники, системи електронного документообігу та управління персональними даними, платформи для онлайн-освіти, а також портали для наукових досліджень і професійної комунікації. До інфраструктури часто залучаються незалежні веборієнтовані сервіси сторонніх постачальників, що розширює діапазон потенційних кіберзагроз через послаблення зон відповідальності та виникнення взаємозалежних уразливостей.

Проблематика забезпечення цілісності і безпеки інформаційної інфраструктури є однією з найактуальніших для сучасної освіти. За результатами останніх досліджень, саме цифрова залежність освітнього процесу, підвищена відкритість освітніх мереж, дефіцит спеціалізованих кадрів, недостатність

фінансування, недосконалість нормативних політик і низька культура кібергігієни створюють сприятливий ґрунт для виникнення нових кіберризиків. До них належать цілеспрямовані атаки на електронні системи управління, фішингові кампанії, злам акаунтів викладачів та студентів, розповсюдження шкідливого програмного забезпечення через навчальні платформи, атаки типу DDoS, захоплення ресурсів для прихованого майнінгу, а також маніпуляції з освітніми даними[4].

Вплив зовнішніх і внутрішніх факторів на захищеність освітньої інфраструктури суттєво зріс у 2023–2025 рр. Особливу увагу привертає збільшення кількості кібератак, спрямованих на зупинку або дезорганізацію освітнього процесу, що супроводжується крадіжками персональних даних, інтелектуальної власності, академічного програмного забезпечення. Також спостерігається зростання інцидентів, пов'язаних із соціальною інженерією, використанням компрометованих облікових даних та цільовими атаками на ІТ-інфраструктуру закладів освіти, в тому числі на критичні сервіси дистанційного навчання та віртуальні лабораторії [13, 22].

Одним із вагомих бар'єрів впровадження надійної кібербезпеки у секторі освіти є інституціональна неготовність, недостатня інтеграція процедур реагування на інциденти, а також хронічна нестача фінансування на модернізацію технічних рішень. За результатами аналітики, лише третина закладів освіти систематично оновлює програмне забезпечення, тоді як більшість використовує застарілі системи без централізованого моніторингу подій безпеки [4]. Особливої уваги потребує питання організації якісного навчання та підвищення цифрової компетентності керівного і технічного персоналу, що підтверджується найновішими дослідженнями у сфері кіберосвіти.

Стратегічні підходи до трансформації інформаційної інфраструктури передбачають впровадження SIEM-рішень (систем управління інформаційною безпекою та подіями), багаторівневих засобів аутентифікації, ізоляції навчальних сегментів мереж, регулярного проведення кібернавчань, а також

розвитку партнерства між закладами освіти, державною владою, бізнесом і міжнародними організаціями для протидії кібератакам. Крім специфічних технологічних інструментів, дослідники відзначають критичне значення формування культури кібергігієни та систематичного аудиту інформаційних активів. Практичний досвід свідчить про ефективність впровадження політик «Zero Trust», сегментованих локальних мереж, використання захищених шлюзів для обробки критичних освітніх даних та розбудови Disaster Recovery Plan як ключового елементу забезпечення безперервності освітнього процесу при кіберінцидентах [4, 10].

В освітньому середовищі України однією з найважливіших підсистем є електронні освітні платформи, зокрема Єдина державна електронна база з питань освіти (ЄДЕБО), що виконує функцію інтеграційної ланки між різними рівнями освітніх установ і державними службами. Порушення цілісності чи недоступність таких систем може паралізувати ключові освітні процеси, призвести до зривів у системі вступу, забезпечення інформування та акредитації спеціальностей. Тому удосконалення процедур моніторингу і швидкого реагування на інциденти інформаційної безпеки є безумовним пріоритетом нормативного розвитку.

У контексті поточних трансформацій освітня інформаційна інфраструктура включає і системи відеоспостереження, бездротові сенсорні мережі, ресурси для інтерактивного навчання та віддаленої співпраці, які потребують належного захисту як на фізичному, так і на програмному рівні. Комплексна побудова безпечної інфраструктури передбачає впровадження стандартів ENISA, рекомендацій Національної служби кібербезпеки й вимог Закону України «Про основні засади забезпечення кібербезпеки України» та нормативних актів МОН, що скеровують політику кіберзахисту в освітньому секторі [19].

Особливе значення має здійснення комп'ютерного аудиту й аналізу активів кібервтручання – це дозволяє визначати тренди, зону критичних уразливостей та підґрунтя для формування цілісної стратегії розвитку безпечного освітнього

середовища. Науковці підкреслюють необхідність впровадження гібридних моделей захисту із залученням як централізованих, так і децентралізованих рішень, розширення спектра аналітики інцидентів, автоматизації виявлення аномалій і прихованих погроз.

Щоб глибше усвідомити спектр сучасних викликів та визначальних загроз, що супроводжують функціонування інформаційної інфраструктури закладів освіти, доцільно звернутися до аналітичних та емпіричних даних, що дозволяють об'єктивно оцінити стан безпеки освітнього середовища в умовах цифровізації та загострення зовнішніх і внутрішніх ризиків. На тлі зростання інтенсивності кібератак, поширення різних типів шкідливого програмного забезпечення та соціотехнічних впливів, а також дедалі складнішої архітектури цифрових навчальних екосистем, постає нагальна потреба в структурованому аналізі чинників уразливості й стратегій протидії. У цьому контексті систематизація характеристик, ризиків і механізмів протидії загрозам надає змогу не лише продемонструвати масштаб проблеми, а й окреслити пріоритети для подальшого розвитку політик безпеки та впровадження технічних і організаційних заходів щодо їхньої мінімізації (Таблиця 1.1).

Таблиця 1.1

Огляд ключових ризиків та рішень щодо захисту інформаційної інфраструктури закладів освіти

Основні компоненти інфраструктури	Типові кіберзагрози	Фактори вразливості	Поточні рішення
LMS та хмарні сервіси	Фішинг, DDoS, malware	Відсутність резервування, слабкі паролі	Аутентифікація MFA, SIEM, навчання персоналу
Сервери/БД	Несанкціонований доступ, шифрування даних	Відсутність сегментації, незахищені протоколи	Сегментування мереж, регулярний аудит
Мережеве обладнання	DOS, пристрої ботнет	Слабкі/застарілі прошивки, відкрите адміністрування	Оновлення ПЗ, використання VPN, моніторингові системи
Мобільні пристрої студентів	Вірусні програми, втрати даних	Відсутність політик, BYOD без контролю	MDM-рішення, політики безпеки пристроїв

У сучасному цифровому освітньому середовищі найбільш уразливими елементами інформаційної інфраструктури залишаються платформи управління навчанням (LMS), хмарні сервіси, сервери, мережеве обладнання й різноманітні кінцеві пристрої користувачів. Характерним є домінування ризиків, пов'язаних із цільовими атаками соціальної інженерії, персоніфікованим фішингом, проведенням DDoS, розповсюдженням шкідливого програмного забезпечення через відкриті мережеві сегменти, а також використанням слабкостей у політиках автентифікації та біометричних даних.

Найчастіше спостерігаються випадки експлуатації застарілого або вразливого програмного забезпечення, недостатнього резервування, недосконалої сегментації мереж, відсутності ефективного адміністрування та централізованих засобів моніторингу. Негативно впливає також недостатня цифрова компетентність персоналу та низький рівень культури кібергігієни серед студентів і працівників, що підсилює ризик компрометації облікових записів і поширення атаки всередині освітньої екосистеми.

У відповідь на виявлені виклики, впроваджуються багаторівневі стратегії захисту – від модернізації політик автентифікації (MFA/2FA), переходу до систем управління подіями інформаційної безпеки (SIEM), організації сегментованих локальних мереж і централізованого аудиту до впровадження засобів MDM (Mobile Device Management) для контролю мобільних пристроїв і регулярних навчань з кібергігієни. Розроблення й реалізація комплексних стратегій безпеки стає фундаментальною передумовою підвищення стійкості та безперервності функціонування освіти на всіх рівнях – від локального сегменту до інтегрованих національних освітніх платформ. Спираючись на структурований розподіл критичних активів за ступенем ризику, сучасна освітня політика орієнтується на пріоритетне зміцнення найбільш уразливих ланок інфраструктури, формування культури відповідального користування цифровими ресурсами й розбудову гнучких міжсекторальних партнерств для сталого розвитку безпечного освітнього простору.

Таким чином, сучасна інформаційна інфраструктура освітнього середовища є складною динамічною системою, яка потребує впровадження інтегрованого підходу до кіберзахисту, розвитку професійної культури безпеки, систематичного підвищення кіберкомпетентності й застосування інноваційних технологій моніторингу та реагування. Це дозволить не лише мінімізувати ризики, а й створити фундамент для сталого функціонування й розвитку освіти в умовах багатовекторних викликів і глобальних цифрових трансформацій.

1.2. Аналіз методів та технологій моніторингу кіберзагроз

В умовах цифровізації освіти, впровадження дистанційного навчання і зростання обсягів обробки особистих даних учасників освітнього процесу, питання ефективного моніторингу кіберзагроз стає ключовим для збереження цілісності та конфіденційності інформаційних ресурсів. Сучасні дослідження виділяють такі основні цілі моніторингу: завчасне виявлення вторгнень, виявлення атипових подій у мережевій інфраструктурі, аналіз слабких місць системи, а також забезпечення швидкого реагування на інциденти [63, 76].

Актуальність питання обумовлена не лише технічними, а й соціальними аспектами – зростанням кількості кіберінцидентів в освітніх установах, різноманітністю атак, а також обмеженими ресурсами для впровадження комплексного захисту. До найпоширеніших кіберзагроз у закладах освіти належать фішинг, шкідливо програмне забезпечення (malware), атаки типу DDoS, витоки та підміна персональних даних, атаки на IoT-пристрої та системи управління навчальними матеріалами (LMS). Наприклад, за даними Arctic Wolf (2024), кібератаки з використанням соціальної інженерії та експлуатації вразливостей Інтернет-ресурсів шкіл та університетів стрімко зростають, акцентуючи значення систематичного моніторингу та навчання учасників освітнього процесу основам кібергігієни [76].

Методи моніторингу кіберзагроз умовно поділяють на пасивні та активні. Пасивний моніторинг передбачає збір та аналіз логів, трафіку, повідомлень про помилки та інформації з встановлених агентів без втручання у роботу

інфраструктури. Активний – полягає у моделюванні атак, використанні honeypot-систем, тестуванні на проникнення (penetration testing) для виявлення реально існуючих уразливостей. Обидва підходи ефективно комбінуються у сучасних системах моніторингу. Додатково, активно розвивається використання засобів машинного навчання та штучного інтелекту для аналізу аномалій, прогнозування виникнення атак, автоматизованого реагування, що значно підвищує оперативність і точність захисних заходів [41, 56].

Технологічна база моніторингу кіберзагроз в освіті включає:

- системи виявлення та запобігання вторгнень (IDS/IPS), серед яких Snort, Suricata, Zeek;
- SIEM-платформи (Security Information and Event Management; наприклад, IBM QRadar, Splunk, ArcSight), що агрегують та аналізують події з різних джерел для виявлення складних атак;
- DLP-системи (Data Loss Prevention), спрямовані на запобігання витоку конфіденційних даних;
- моніторинг мережевих аномалій за допомогою штучного інтелекту: використання поведінкових моделей учасників освітнього процесу для виявлення атипових дій;
- використання санітарних зон та sandbox-платформ для безпечного аналізу підозрілих файлів;
- реалізація Zero Trust Architecture у хмарних рішеннях, що передбачає багаторівневу автентифікацію, контроль доступу й постійний аудит [56].

Значною перевагою сучасних SIEM-платформ є їх здатність інтегруватися із зовнішніми сервісами threat intelligence та надавати можливість корелювати дані не лише з внутрішніх, а й глобальних джерел, що є особливо важливим для виявлення масових або цілеспрямованих атак, таких як атаки на ланцюг постачання освітнього ПЗ. Сучасні дослідження показують, що впровадження адаптивних компонентів SIEM дозволяє автоматично генерувати сценарії реагування, знижуючи людський фактор у вирішенні інцидентів [41, 56].

В освітньому середовищі поширеним є підхід до реалізації моніторингу у вигляді багаторівневої архітектури (Рис. 1.1):

Базовий рівень – організаційно-процедурний, де впроваджуються політики безпеки, навчання учасників, реєстрація та аудит дій.

Технічний рівень – забезпечується засобами IDS/IPS, фаєрволами, захищеними шлюзами, DLP та шифруванням даних.

Аналітичний рівень – орієнтований на постійний аналіз журналів, інцидентів та оцінку ефективності впроваджених заходів.

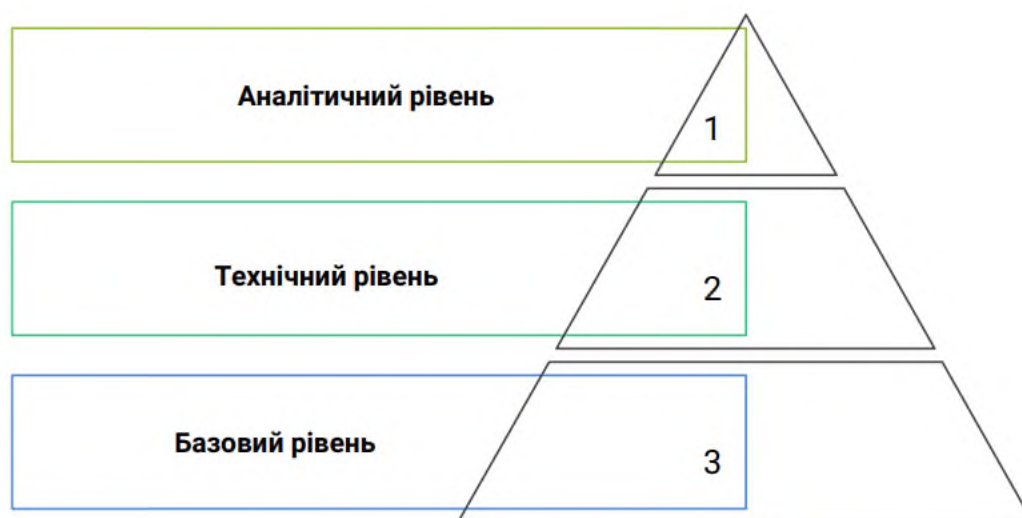


Рисунок 1.1 – Багаторівнева архітектура моніторингу в освітньому середовищі

Варто зазначити, що особливу увагу вітчизняні дослідники приділяють питанню комплаєнсу з актуальними нормативними актами, зокрема законам України «Про захист персональних даних» й «Про захист інформації в інформаційно-телекомунікаційних системах». Це обумовлює необхідність впровадження технічних і організаційних засобів, що відповідають національним і європейським стандартам, особливо щодо зберігання, передачі й обробки персональних даних студентів і працівників [17, 18].

Інноваційним напрямом моніторингу кіберзагроз для закладів освіти є розширене використання колективних систем обміну інформацією про інциденти (Cyber Threat Intelligence Sharing Platforms), що дозволяє отримувати оперативні попередження щодо нових типів атак і підвищує ефективність

реагування на загрози. Сонячним прикладом є міжнародні ініціативи (наприклад, ENISA, REN-ISAC), які пропонують методичну підтримку і шаблони для оцінки ризиків в університетських мережах [32].

Для забезпечення цілісного уявлення про сучасні підходи до моніторингу кіберзагроз доцільно не лише описувати окремі методи, а й логічно зіставляти їх у структурованому форматі. Саме тому детальний порівняльний аналіз основних технологій та інструментів моніторингу уможливорює більш глибоке розуміння їхніх ключових функцій, а також дозволяє визначити їхню ефективність у типових освітніх сценаріях. В таблиці 2 представлено узагальнений огляд найбільш використовуваних методів і рішень у сфері кібербезпеки освітнього середовища.

Таблиця 1.2

Основні методи і технології моніторингу кіберзагроз у освітньому середовищі

Метод/технологія	Основна ідея/функція	Приклад впровадження
IDS/IPS	Виявлення/запобігання вторгнень	Snort, Suricata, Zeek
SIEM	Централізований збір і аналіз подій	IBM QRadar, Splunk, ArcSight
DLP	Захист від витоків даних	Symantec DLP, McAfee DLP
ML/AI-аналіз аномалій	Виявлення відхилень у поведінці	Системи поведінкового моніторингу
Honeypot і sandboxing	Обман атакуючих, безпечний аналіз	Cuckoo Sandbox
Threat Intelligence Sharing	Спільний обмін знаннями й попередженнями	REN-ISAC, ENISA
Zero Trust Architecture	Мінімізація довіри, постійний аудит	Хмарні сервіси з багатофакторною автентифікацією

IDS (Intrusion Detection Systems) та IPS (Intrusion Prevention Systems) є фундаментальними компонентами забезпечення кібербезпеки сучасного освітнього середовища. В умовах глибокої цифровізації закладів освіти ці системи набувають особливого значення, оскільки дозволяють своєчасно виявляти, класифікувати та блокувати широкий спектр кіберзагроз, спрямованих на інформаційну інфраструктуру закладів освіти. Останніми роками обсяги трафіку і різноманітність атак у мережах ЗВО значно зросли, що зумовлює

потребу постійного вдосконалення механізмів моніторингу та реагування на інциденти безпеки [71].

IDS – це комплекс технічних і програмних рішень, які призначені для аналізу потоків даних, моніторингу подій у мережі та інформаційних системах із метою виявлення ознак несанкціонованого доступу, атак або порушень політик кібербезпеки. IDS здатні виявляти як відомі (signature-based), так і невідомі (anomaly-based) загрози за допомогою методів аналізу сигнатур чи аномалій відповідно. Застосування сигнатурного аналізу дозволяє оперативно фіксувати добре відомі шаблони атак, водночас методи аномалій розширюють можливості системи у виявленні нових чи змінених загроз, що ще не мають уніфікованих ознак у базах даних [42, 71].

У сучасних реалізаціях IDS належить місце штучному інтелекту та машинному навчанню, що дозволяє системам розпізнавати складні поведінкові патерни, суттєво зменшуючи показник хибних спрацювань (false positives) та даючи змогу динамічно адаптуватися до нових форм атак. Дослідження показують, що інтегровані моделі – Random Forest, XGBoost, Gradient Boosting та інші сучасні алгоритми – здатні забезпечити точність і надійність понад 93% під час роботи із реальними потоком мережевого трафіку навчальних закладів.

Важливою характеристикою IDS є пасивність дій: система лише сигналізує про виявлену загрозу, фіксує інцидент у журналах подій та інформує адміністратора про необхідність подальших дій. Проте значна кількість атак із високою швидкістю розповсюдження (наприклад, мережеві черв'яки, автоматизовані сканери, новітні криптолокери тощо) вимагає розширення можливостей реагування, що веде до впровадження рішень класу IPS.

IPS – остання генерація систем моніторингу, які поєднують можливості виявлення й активного попередження загроз. Ці системи розташовуються безпосередньо на шляху основних потоків даних (in-line) та здатні автоматично блокувати підозрілі з'єднання, фільтрувати трафік або змінювати маршрутизацію, щоб мінімізувати вплив загрози ще на етапі її зародження. IPS використовують принципи моделей IDS для ідентифікації загроз, проте

доповнюють їх інструментами активного втручання: завершення сеансу, автоматичне застосування правил доступу, обмеження чи цілковите відключення окремих вузлів мережі [44].

У контексті освітніх закладів, особливе значення має правильне впровадження IDS/IPS із урахуванням відкритості та академічної гнучкості цифрового середовища. Мережа ЗВО зазвичай характеризується гетерогенністю пристроїв, розмаїттям операційних систем і сервісів, а також підвищеною увагою до захисту приватності й академічної свободи користувачів. Тому, обираючи систему IDS/IPS, необхідно враховувати вимоги до масштабованості, продуктивності, можливості інтеграції з існуючими платформами та зручності адміністрування [11].

Зокрема, під час оцінки ефективності IDS/IPS у цифровому освітньому середовищі рекомендується застосовувати такі критерії, як:

- здатність ідентифікувати як загальновідомі, так і нові типи атак;
- адаптивність до швидких змін топології мережі та зростання навантаження;
- мінімізація затримок і впливу на якість освітнього процесу;
- підтримка комплексної політики моніторингу, що враховує академічну етику та конфіденційність [11, 53].

Значна увага сучасних досліджень приділяється питанням побудови якісних датасетів для навчання та тестування IDS, зокрема для виявлення атак у специфічному середовищі ЗВО. Досвід світових університетів засвідчує, що використання реальних мережевих даних у навчальних моделях підвищує обґрунтованість і результативність впроваджуваних систем захисту. Водночас вважається важливим налаштування процедури постійного аудиту, перевірки й оновлення висновків IDS/IPS, що дозволяє уникати деградації якості захисту у відповідь на зміну ландшафту кіберзагроз [71].

Синергія методів моніторингу IDS та активної протидії IPS дозволяє досягти високого рівня кіберстійкості освітньої інфраструктури. Постійний діалог між адміністраторами, розробниками рішень та експертним середовищем

відіграє ключову роль у постійному вдосконаленні процесів моніторингу, виявлення та нейтралізації кіберзагроз. Сучасні дослідження наполягають на доцільності впровадження гібридних архітектур, що поєднують класичні IDS/IPS із новітніми інтелектуальними модулями, honeypots, SIEM-платформами та іншими інструментами для глибокого аналізу атак і побудови адаптивної стратегії захисту [31, 52].

Таким чином, IDS/IPS виступають базовим елементом екосистеми кіберзахисту освітнього середовища, забезпечуючи раннє виявлення загроз, миттєве реагування й адаптацію до актуальних викликів. Вибір, конфігурація й постійне вдосконалення цих систем має спиратися на результати наукових досліджень, аналізу кращих практик та дотримання міжнародних стандартів у сфері кібербезпеки закладів освіти.

SIEM (Security Information and Event Management) є центральним елементом систем управління безпекою закладу освіти, забезпечуючи збір, кореляцію та аналіз подій безпеки із різних джерел у реальному часі. Система SIEM виконує декілька ключових функцій – централізований моніторинг журналів подій, виявлення загроз, автоматичне сповіщення про інциденти та підтримку розслідувань кіберінцидентів. Для освітніх закладів цей інструмент дозволяє отримати цілісне уявлення про стан кібербезпеки і оперативно реагувати на аномальні дії в інфраструктурі, що особливо цінно у багатокомпонентному середовищі зі змішаним доступом (зокрема, хмарні платформи, LMS, особисті пристрої тощо) [37, 39, 46].

Системи SIEM збирають та агрегують дані з різних джерел, таких як IDS/IPS, файрволи, хостові системи, мережеве обладнання, хмарні сервіси, та створюють єдиний репозиторій журналів, який піддається автоматизованому й аналітичному аналізу. В основі функціонала лежать механізми кореляції подій: наявність очевидних чи прихованих взаємозв'язків між подіями дозволяє виявляти складні атаки, що складаються з декількох стадій (наприклад, фішинг + проникнення + ексфільтрація даних), а не лише реагувати на окремі аномалії.

Особливістю SIEM є підтримка реального часу («real-time monitoring»): система миттєво реагує на підозрілу активність, сповіщаючи адміністраторів та аналітиків безпеки про інциденти, які мають високий пріоритет чи невідкладний характер. Сучасні SIEM-платформи поєднують класичні правила кореляції, використання інтегрованих чи зовнішніх потоків threat intelligence (перелік відомих індикаторів компрометації – IOC), а також машинне навчання для виявлення нових («невідомих») загроз. Зокрема, машинне навчання дозволяє виявляти відхилення від «білого профілю» поведінки, наприклад, атипові часи підключення, нетипову геолокацію користувача чи незвичну інтенсивність передачі даних.

SIEM у закладах освіти відіграє особливу роль через складність інформаційної інфраструктури та велику кількість різномірних користувачів – студентів, викладачів, адміністраторів, наукових співробітників. Для таких середовищ характерна висока динаміка змін складу користувачів, застосування BYOD-політик (Bring Your Own Device) і постійний доступ до хмарних та локальних ресурсів. Саме тому SIEM дозволяє:

- виявляти спроби неавторизованого доступу до дослідницької чи персональної інформації;
- відстежувати підозрілу активність у різних підрозділах закладу (від кампусу до віддалених сервісів);
- збирати повні дані для реагування на інциденти та проведення пост-інцидентного аналізу;
- автоматизувати процес реагування та містити шаблони швидкого реагування для зменшення часу вирішення інциденту [34, 43].

Ще одна важлива особливість – легальність та відповідність стандартам: впровадження SIEM допомагає закладам освіти дотримуватись міжнародних і локальних вимог з кібербезпеки (зокрема, GDPR, ISO/IEC 27001, NIST 800-53), оскільки забезпечується централізований журнал подій, доказова база для розслідувань, регулярна звітність. SIEM може генерувати спеціалізовані звіти

для аудиторів та органів контролю, що підтверджують відповідність політикам захисту даних.

Розглядаючи специфіку інтеграції в освітнє середовище, варто підкреслити наступні аспекти:

- інтеграція з різноманітними джерелами подій: SIEM легко масштабується для збору даних з внутрішніх та зовнішніх систем, включаючи хмарні сервіси, фреймворки керування ідентифікацією користувачів (IdM), VPN-платформи, електронні щоденники тощо;

- автоматизація реагування: впровадження інтегрованих механізмів SOAR (Security Orchestration, Automation and Response) дозволяє автоматично блокувати підозрілу активність, блокувати облікові записи чи сегментувати мережу під час атаки;

- підтримка обміну даними: сучасні SIEM забезпечують взаємодію із threat intelligence-платформами, дозволяючи співставляти внутрішні події зі світовими трендами загроз та отримувати рекомендації для вдосконалення захисту.

В освітніх установах серед найпоширеніших рішень – IBM QRadar, Splunk, ArcSight, що мають функціонал як для локального розгортання, так і для хмарної інфраструктури, підтримку адаптивних політик, інтерфейси інтеграції з навчальними платформами та розвинуті засоби аналітики для забезпечення гнучкої налаштовуваності під специфічні бізнес-процеси закладу.

Типові виклики для SIEM в освіті полягають у високому рівні «шуму» (наявність великої кількості подій і не всі з них – індикатори реальної атаки), потребі адаптації під різнотипні сервіси, а також обмежених людських і фінансових ресурсах для комплексного моніторингу. Вирішити зазначені проблеми дає змогу застосування автоматизованих засобів фільтрації, використання threat intelligence, а також запровадження штучного інтелекту для пріоритезації інцидентів.

Таким чином, SIEM виступає не лише технічним інструментом централізованого моніторингу, але і стратегічним елементом управління

ризиками та безпекою освітньої екосистеми, підвищуючи стійкість до новітніх кіберзагроз, забезпечуючи відповідність законодавству і зберігаючи довіру до цифрових сервісів університету.

У сучасному цифровому освітньому середовищі питання забезпечення цілісності, конфіденційності та доступності інформації набуває особливого значення, зважаючи на активне використання хмарних сервісів, дистанційних платформ і великої кількості відкритих каналів передачі даних. Однією з найбільш ефективних технологій превентивного типу, яка використовується для контролю, моніторингу та захисту чутливих і службових даних, є система попередження витоку даних – Data Loss Prevention (DLP).

DLP – це комплексна методика й набір технологічних рішень для запобігання випадковим і навмисним витокам конфіденційної інформації за межі організації, що реалізуються через спеціалізоване програмне забезпечення. Основна функція таких систем – ідентифікувати, аналізувати та контролювати статус даних (у використанні, русі та стані спокою) у внутрішніх і зовнішніх інформаційних потоках університету, інтегруючись у корпоративне середовище задля мінімізації ризиків витоку критичних даних [12, 15].

Принцип дії DLP базується на декількох механізмах:

- глибокий аналіз вмісту інформації, що передається через мережу, із застосуванням стохастичних та сигнатурних алгоритмів, розпізнавання типових структур даних, текстових шаблонів, хеш-функцій, цифрових водяних знаків, а також контекстного аналізу метаданих (ініціатор транзакції, тип даних, носій, адресат, часові характеристики тощо) [12];

- розмежування доступу та контроль спроб пересилання або модифікації файлів із використанням корпоративної електронної пошти, хмарних сервісів, зовнішніх носіїв, мобільних пристроїв [51];

- блокування несанкціонованих операцій: у разі виявлення передачі критичної інформації за межі корпоративного периметру програма перевіряє операцію та фіксує або блокує її, повідомляючи відповідального фахівця із кібербезпеки. Прикладом може слугувати автоматичне блокування спроби

надіслати таблицю з особистими даними студентів із корпоративної пошти на приватну адресу [12, 15];

- автоматизований моніторинг усіх інформаційних потоків та журналювання дій користувачів у режимі реального часу: це дозволяє своєчасно реагувати на інциденти, а також формує якісний аудиторський трафік для подальшого аналізу кіберзагроз [59].

DLP-технології у закладах освіти мають ряд специфічних задач, серед яких:

- захист персональних даних студентів і співробітників відповідно до вимог GDPR та чинного українського законодавства у сфері кібербезпеки й освіти, включаючи нормативи НАЗК й МОН [2, 51];

- управління контролем доступу до наукових досліджень, дисертацій, електронних баз даних студентів і викладачів, сертифікатів, звітів про наукову діяльність, медичних та фінансових даних освітніх установ [2, 12];

- моніторинг активності користувачів із метою виявлення підозрілих дій, нетипових моделей поведінки, спроб несанкціонованого копіювання або завантаження великих обсягів даних [62];

- інтеграція із системами SIEM (Security Information and Event Management) для побудови єдиної аналітичної моделі реагування на кіберзагрози – це забезпечує ефективне управління ризиками та відповідність політиці кібербезпеки університету.

Дослідження ефективності DLP-систем у сфері освіти засвідчує, що їх використання дозволяє суттєво знижувати рівень ризику витоку корпоративної й особистої інформації, блокувати як зовнішні атаки, так і внутрішні загрози (навмисне чи випадкове переміщення даних). Зокрема, сучасні рішення (Symantec DLP, McAfee DLP, Safetica, Digital Guardian) підтримують багаторівневий захист для локальних серверів, хмарних платформ та мобільних пристроїв освітніх закладів. Впровадження DLP-технологій також сприяє формуванню культури інформаційної безпеки серед користувачів – проведення

тренінгів та інформаційних кампаній серед викладачів і студентів дозволяє мінімізувати випадки витоку даних через людський фактор [15, 62].

Окремою складовою сучасної DLP є застосування методів машинного навчання, раннього виявлення загроз, розпізнавання нетипових поведінкових патернів для автоматизації моніторингу інформаційних потоків. Сучасні DLP-системи підтримують інтеграцію з SIEM, IAM, IDS/IPS та іншими захисними механізмами, що дозволяє будувати централізовану захищену екосистему університету відповідно до принципів «Zero Trust» [62].

Крім основних технічних та організаційних чинників, слід враховувати й виклики, пов'язані із впровадженням DLP: належна ідентифікація критичної інформації, мінімізація впливу на продуктивність роботи користувачів, відповідність міжнародним стандартам кібербезпеки й уникнення надмірної бюрократизації процесу користування технологіями захисту. Проте, у разі системної інтеграції DLP із традиційними системами управління інформаційною безпекою, університети здатні забезпечити високий рівень захисту освітнього контенту, інтелектуальної власності й відповідати сучасним викликам цифрової трансформації.

Таким чином, DLP є незамінною складовою управління кіберризиками в закладах вищої освіти, оскільки забезпечує багатофакторний захист критичних інформаційних активів, гарантує відповідність чинним нормативним вимогам, підвищує довіру до освітніх цифрових сервісів, стимулює розвиток культури інформаційної безпеки та дозволяє ефективно протистояти складним й новітнім кіберзагрозам освітнього середовища.

ML/AI-аналіз аномалій також є надзвичайно актуальним і ефективним методом моніторингу кіберзагроз у цифровому освітньому середовищі, що в останні роки стрімко розвивається та демонструє високу результативність у порівнянні з традиційними інструментами. Цей підхід заснований на використанні методів машинного навчання (ML) і штучного інтелекту (AI), головною метою яких є виявлення відхилень (аномалій) у поведінці користувачів, мережевого трафіку, доступі до освітніх ресурсів і внутрішніх

інформаційних систем. Основна перевага методології полягає у її здатності аналізувати великі обсяги різнотипових даних у реальному часі, автоматично будувати профілі “нормальної” активності та своєчасно сигналізувати про потенційні вторгнення, зловмисні дії чи нові небезпеки, що ще не мають чітких сигнатур [57, 61].

Серед ключових технології ML/AI-аналізу аномалій виділяють супервізоване, несупервізоване та змішане (гібридне) машинне навчання. Супервізовані методи (наприклад, Random Forest, Support Vector Machines – SVM, Neural Networks) потребують розмічених даних для побудови детекторів аномалій, тоді як несупервізовані (наприклад, K-середніх, Isolation Forest, автоенкодери) дозволяють виявляти нові, раніше невідомі типи вторгнень шляхом аналізу внутрішньої структури трафіку або поведінкових патернів. Гібридні підходи комбінують переваги вказаних моделей, забезпечуючи якісніше виявлення складних атак, типових для сучасних цифрових освітніх середовищ.

В освітніх установах методів аномалій широко застосовують для захисту від внутрішніх і зовнішніх загроз, таких як несанкціонований доступ, підозріла активність користувачів, атаки типу DoS/DDoS, розповсюдження шкідливого ПЗ чи спроби викрадення персональних даних студентів і працівників. Наприклад, у дослідженні, проведеному у вищому навчальному закладі Карнегі-Меллон (CMU), було розроблено мультиалгоритмічну систему аналізу аномалій для мережевого трафіку освітніх платформ. Вона включала різні ML-моделі (Random Forest, SVM, Neural Networks), що давало змогу досягати точності виявлення до 92% із суттєвим зниженням кількості хибнопозитивних спрацювань із 15% до 4% порівняно з традиційними системами [68].

Ключовими етапами впровадження ML/AI-аналізу аномалій є:

- збір і попередня обробка даних із різних джерел (мережеві журнали, логи LMS, система аутентифікації, firewall, SIEM-платформи);
- побудова навчальних вибірок і позначення даних (у разі супервізованих моделей);

- відбір релевантних ознак та їхнього нормування;
- навчання моделей (Random Forest, SVM, Neural Networks, автоенкодера й інші) та перевірка на достовірності й узагальнюваності (методи крос-валідації);
- побудова системи оперативного моніторингу та реагування на інциденти.

Для виявлення аномалій у мережевому трафіку навчальних закладів часто використовуються тестові датасети типу CICIDS2017, UNSW-NB15, що містять як «нормальні», так і аномальні записи різних інцидентів. Сучасні моделі ML забезпечують детекцію різних видів атак (DoS, brute force, ботнети, фішинг, внутрішні порушення тощо) із точністю понад 90%, причому завдяки автоенкодерам і ізоляційним лісам істотно підвищується чутливість до нових («zero-day») загроз [57, 68].

Особливості інтеграції ML/AI-аналізу аномалій у цифрове середовище вищої школи включають:

- гнучкість масштабування (аналіз у реальному часі для середовищ із тисячами унікальних користувачів);
- здатність автоматичного оновлення моделей з урахуванням змін у поведінці користувачів та появи нових загроз (online learning, transfer learning);
- автоматизовану генерацію інцидентів для інтеграції з SIEM, DLP або системами миттєвого реагування.

Серед сучасних комерційних і відкритих рішень для ML/AI-аналізу аномалій в освітньому секторі використовують Splunk AI, IBM QRadar, Arctic Wolf, а також open-source-фреймворки на основі Python-екосистеми (scikit-learn, TensorFlow, PyTorch). Іншими словами, ML/AI-аналіз аномалій стає невід'ємною складовою цифрової інфраструктури освітніх закладів, дозволяючи оптимізувати процеси моніторингу, підвищити стійкість до сучасних атак і зміцнити довіру до електронних освітніх ресурсів користувачів [30, 68].

Водночас варто враховувати і сучасні виклики впровадження ML/AI у сфері моніторингу кіберзагроз: дисбаланс даних, проблема хибнопозитивних

спрацьовувань, необхідність пояснюваності моделі при аудиті, а також технічні бар'єри й кадрові обмеження для невеликих та малобюджетних освітніх закладів.

Оперативне впровадження сучасних методів ML/AI-аналітики в освітньому середовищі закладає підґрунтя для істотного підвищення рівня кібербезпеки, забезпечує адаптацію захисних заходів до швидко змінних запитів академічного простору та дає можливість ефективно реагувати на нові загрози й атакуючі вектори. Наукові дослідження підтверджують високий потенціал застосування таких підходів для вузькоспрямованого виявлення нетипових кіберінцидентів, а також для автоматизованого масштабування захисних процесів – від аналізу мережевої активності до розбудови політик безпеки та захисту персональних даних в освітніх установах, відповідно до діючих норм та стандартів академічної доброчесності. Значною мірою підвищити результативність оперативного виявлення, класифікації й аналізу кіберзагроз у цифровому освітньому середовищі дозволяє застосування спеціалізованих технологій, серед яких особливу увагу заслуговують honeypot (технологія пасток для атакуючих) і sandboxing (технологія ізольованого виконання потенційно шкідливого коду).

Honeypot – це спеціалізований інструмент кіберзахисту, що функціонує як інтерактивний псевдосервер, пристрій, аплікація чи частина інформаційної інфраструктури, навмисно ослаблена або з імітованими вразливостями для залучення, ідентифікації й детального аналізу дій потенційних атакуючих. Основна ідея полягає у створенні ізольованого середовища, яке зовні виглядає як приваблива мішень для зловмисників, але фактично не містить критичних ресурсів освітнього закладу. Таким чином, організується детекція – всі маніпуляції, експлоїти, фейкові установлення шкідливого програмного забезпечення, мережеві сканування, атаки на автентифікацію та спроби підбору паролів піддаються глибокому аналізу через інтеграцію системи honeypot із реальними засобами логування та моніторингу [65].

Інноваційні моделі honeypot, описані у наукових публікаціях, передбачають використання гнучких фреймворків для автоматичного

налаштування та централізованого управління пастками (наприклад, SMASH, Modern Honeynet, Cowrie, Wordpot), що забезпечують реалістичне моделювання освітнього контексту й дозволяють збирати взаємодії атакуючих у віртуалізованому середовищі (VMware, Docker, GNS3). Ключовими принципами є:

- динамічність: автоматичне розгортання пасток різних типів відповідно до змін інфраструктури;
- ізоляція: строгий поділ сегментів honeypot від реальних серверів освітньої установи;
- глибина спостереження: логування команд, мережевого трафіку, експлойтів (APT, ransomware, phishing);
- інтеграція: взаємодія з SIEM/IDS/IPS та аналітичними підсистемами.

Практична цінність honeypot у ЗВО полягає у можливості раннього виявлення нових векторів атак, формуванні кіберінтелекту (threat intelligence) щодо сучасних засобів і тактик кіберзлочинців, а також у забезпеченні навколишньої безпеки навіть в умовах недостатнього ресурсного оснащення традиційної інфраструктури. Окрім цього, honeypot може виконувати роль навчального інструмента для студентів кафедри кібербезпеки, дозволяючи вивчати реальні атаки в контрольованих, ізольованих умовах [28].

Sandboxing – це технологія створення ізольованого «пісочниці», у межах якої запускається потенційно шкідливий процес, файли або додатки, що дозволяє дослідити їхню поведінку, не наражаючи на ризик основну IT-інфраструктуру освітнього закладу. Сучасні sandboxes базуються на принципах гібридного аналізу – поєднання статичного та динамічного аналізу, симуляції діяльності користувача й емулявання системних взаємодій, а також інтеграції механізмів штучного інтелекту (ML/AI). Застосування sandbox-інструментів забезпечує [64]:

- аналіз шкідливих об'єктів (PE, EXE, PDF, DOC, скрипти, аплети):
- детекція аномальної активності на основі поведінкових маркерів;

- виявлення zero-day: відстеження нових загроз, які ще не присутні у сигнатурних базах антивірусів;

- ефективність протидії обходу: запуск шкідливого ПЗ у середовищах, що максимально імітують дії реального користувача, опір сучасним технікам «evasion»;

- глибока інтеграція із SIEM/EDR/SOAR: автоматична реакція та прийняття рішень щодо ізоляції, блокування, реверсивного аналізу тощо.

У сукупності, технології honeypot та sandboxing стають незамінними компонентами сучасної системи моніторингу кіберзагроз в освітньому середовищі: вони дозволяють реагувати на атаки на ранніх стадіях, накопичувати актуальний кіберінтелект, забезпечити відповідність нормативним вимогам доброчесності та безпеки, а також сприяти формуванню інноваційних освітніх практик, спрямованих на підготовку фахівців нового покоління у сфері кібербезпеки. Такі підходи логічно узагальнюються у наведеній нижче таблиці, яка характеризує основні методи й технології моніторингу кіберзагроз у ЗВО, їхні переваги й обмеження.

Після детального розгляду ролі honeypot та sandboxing у системах моніторингу кіберзагроз доцільно звернутися до комплексного порівняння основних підходів, що мають ключове значення для забезпечення кіберстійкості освітнього середовища. Наступний детальний аналіз стосується розгляду одного з найбільш перспективних і затребуваних інструментів у цій сфері – «Threat Intelligence Sharing», який все ширше впроваджується у структурах захисту освітніх установ завдяки своїй здатності підвищувати рівень реакції на новітні кіберзагрози.

«Threat Intelligence Sharing» (обмін кіберрозвідувальною інформацією про загрози) – це мультидисциплінарна стратегія, що базується на участі освітніх організацій у спеціалізованих платформах і мережах співпраці, спрямованих на централізований збір, структурування та автоматизований обмін інформацією про поточні атаки, уразливості, тактики та індикатори компрометації (IoC) між учасниками сектору. Центральним елементом підходу є сумісне використання

структурованих даних (наприклад, за допомогою стандарту STIX/TAXII), що спрощує інтероперабельність різних систем моніторингу у закладах освіти. Такі рішення дозволяють освітнім установам отримувати актуальні попередження про загрози, зменшувати час реагування на атаки та швидко залучати ресурси для нейтралізації складних кібератак завдяки швидкому доступу до узагальнених знань різних організацій та міжнародних партнерів [45, 50].

Практична реалізація подібних стратегій передбачає обов'язкову участь у платформах на кшталт REN-ISAC (Research and Education Networks Information Sharing and Analysis Center), що спеціалізується на кібербезпеці вищої освіти, та співпрацю з ініціативами Європейської агенції з кібербезпеки ENISA. REN-ISAC надає можливість членам інформаційної спільноти освітнього сектору оперативно надсилати та отримувати повідомлення про інциденти, аналізувати нові вектори атак, отримувати індикатори компрометації для налаштування внутрішніх систем, а також формувати колективну стратегію раннього виявлення загроз. На рівні ЄС ENISA забезпечує методологічний, консультаційний та технологічний супровід з питань організації процесів STI-шерингу, стандартизації форматів та процедур обміну даними.

Впровадження «Threat Intelligence Sharing» особливо критичне для освітнього середовища через динамічність навчальних процесів, присутність великої кількості взаємодіючих цифрових інфраструктур, доступність різноманітних навчальних платформ, а також підвищений рівень відкритості мережі університету до зовнішніх підключень. Це зумовлює додаткову потребу у своєчасному оновленні переліків IoC та обміні інформацією про нові кампанії атак – таких, як phishing, ransomware, експлуатація вразливостей у LMS чи втручання у систему відеоконференцій. Починаючи вже з 2020-х років, найбільш прогресивні університети активно приділяють увагу формуванню власних internal threat intelligence competence centers – і одночасно підключаються до зовнішніх інформаційних хабів та відкритих платформ обміну, наприклад, Open Threat Exchange (OTX) або MISP.

Серед ключових переваг Threat Intelligence Sharing виділяють такі [73]:

- підвищення обізнаності про поточні та майбутні загрози на секторному та міжгалузевому рівні, що дозволяє швидко реагувати на нові типи атак, у т.ч. zero-day атаки та масові кампанії;

- значне скорочення часу між появою нової загрози та впровадженням захисних заходів завдяки обміну структурованими ІоС та тактиками нападників серед партнерів;

- можливість ідентифікувати тенденції атак та атакуючих угруповань завдяки крос-платформному аналізу, що особливо цінно для обмежених ІТ-служб ЗВО.

Водночас існують і обмеження:

- проблеми стандартизації форматів даних і протоколів обміну між різними платформами, що ускладнює інтеграцію із внутрішніми SIEM-системами в університетах;

- ризики розкриття чутливої інформації щодо інфраструктури ЗВО чи персональних даних під час відкритого обміну, що потребує правової регламентації, контролю доступу та захисту даних відповідно до GDPR;

- необхідність забезпечення високого рівня довіри між учасниками платформ, створення чітких політик анонімізації та відповідальності за достовірність наданої інформації.

З огляду на актуальні дослідження й аналітичні звіти (наприклад, ENISA CTI Overview 2024), найбільш успішною моделлю Threat Intelligence Sharing для освітнього середовища визнається використання гібридних схем із комбінацією локальних competence centers та участю у міжнародних галузевих спільнотах. Це дозволяє забезпечити максимальну інформованість, балансувати оперативність реагування та дотримання норм регуляторної політики, та інтегрувати отримані знання у системи SIEM, DLP та інші рішення, що вже функціонують у цифровому освітньому середовищі [45].

Threat Intelligence Sharing є одним з фундаментальних компонентів сучасного підходу до забезпечення кібербезпеки у закладах вищої освіти, а його стратегічне впровадження забезпечує розвиток навичок колективної протидії

кіберзагрозам, відповідність сучасним вимогам нормативних актів та розвиток інноваційної культури кіберзахисту в освіті. Однак ефективне реагування на динамічні кіберзагрози передбачає не лише обмін актуальною інформацією, а й застосування концептуально нових підходів до управління доступом і захисту цифрової інфраструктури. Одним із найперспективніших методів у цьому контексті є Zero Trust Architecture – архітектурне рішення, орієнтоване на принцип «ніколи не довіряй, завжди перевіряй», що набуває все більшої популярності у науковій літературі та світовій практиці захисту освітніх екосистем.

Поняття Zero Trust Architecture (ZTA) виникло у відповідь на обмеження традиційних периметральних моделей безпеки, котрі характеризуються значною уразливістю до сучасних складних атак та несанкціонованого доступу до ресурсів освіти. ZTA базується на тому, що жоден користувач, пристрій чи система не повинні розглядатися як такі, що заслуговують на довіру лише через своє перебування у внутрішній мережі; навпаки, усі суб'єкти та об'єкти вважаються потенційно небезпечними доти, доки не проведено їх ідентифікацію, автентифікацію та оцінку ризику [29, 67].

Згідно з дослідженнями National Institute of Standards and Technology, Zero Trust Architecture складається з низки технологічних і процесуальних компонентів, серед яких ключовими є: системи управління ідентифікацією та доступом (IAM), політики мікросегментації мережі, постійний моніторинг поведінки та оцінка стану пристроїв, а також динамічний аналіз контексту запитів на доступ до ресурсів [67].

Основні етапи реалізації ZTA в освітньому середовищі охоплюють [29, 82]:

- впровадження мікросегментації мережі шляхом поділу інфраструктури на логічні ізольовані сегменти з чітко фіксованими правилами взаємодії між ними;

- використання адаптивних механізмів автентифікації та авторизації – багатофакторна автентифікація (MFA), контекстна перевірка, аналіз поведінкових патернів користувачів;
- підключення централізованих систем моніторингу (SIEM, UEBA, SOAR) для безперервного аналізу подій, виявлення аномалій та орієнтованої реакції на інциденти;
- формування політик доступу на основі принципу найменших привілеїв та оцінки ризиків кожної транзакції у режимі реального часу;
- регулярне оновлення правил доступу, ізоляція критичних ресурсів та динамічне реагування на зміну контексту, зокрема зміни статусу пристроїв чи користувачів.

Сучасні дослідження вказують, що саме інтеграція Zero Trust Architecture дозволяє значно підвищити стійкість освітніх платформ до сучасних кіберзагроз, адже реалізується система багаторівневого контролю доступу та адаптивного управління ризиками. Наприклад, результати емпіричних оцінок демонструють, що впровадження ZTA веде до істотного зниження збитків від атак – зменшення середнього ризикового впливу на \$684 тисячі за 4 роки. Водночас, методика Zero Trust сприяє перевірці кожної дії в освітній інфраструктурі та забезпечує захист від внутрішніх та зовнішніх атак, включаючи підвищену ефективність захисту при роботі з віддаленими користувачами, гібридними хмарами та мобільними пристроями [29].

Механізми Zero Trust Architecture для моніторингу кіберзагроз передбачають використання декількох технологічних шарів:

система управління ідентифікацією та доступом (IAM): дозволяє однозначно ідентифікувати користувачів й пристрої, як правило включає багатофакторну автентифікацію та перевірку пов'язаних параметрів кожного запиту [38, 67];

мікросегментація мережі: дає змогу створювати ізольовані зони у цифровому освітньому середовищі та мінімізувати площу атаки – навіть у разі компрометації одного сегменту решта залишається захищеною [67, 81];

контекстний контроль доступу: рішення базуються на аналізі ризику для кожного транзакційного доступу, враховуючи серед іншого місцезнаходження, тип пристрою, історію поведінки та активність у системі [48];

інтеграція SIEM/UEBA/SOAR: застосування платформ безперервного моніторингу, аналізу взаємодій та автоматизованої реакції на інциденти дозволяє не лише оперативно виявляти загрози, а й автоматизувати дії для локалізації ризиків [38, 77];

оцінка та управління станом пристроїв: перевірка захищеності, відповідність політикам та регламенту, ізоляція поточно уражених пристроїв від ключових ресурсів [29, 67].

На практиці повноцінне використання методів Zero Trust Architecture у закладах освіти передбачає інтеграцію алгоритмів машинного навчання для поведінкового аналізу – це дозволяє автоматизовано виділяти аномалії у активності користувачів, підвищити точність реагування на складні багатовекторні атаки та знизити кількість помилкових спрацювань за рахунок моделі контекстного ухвалення рішень [82, 79].

Інституційний менеджмент ризиків, згідно з сучасними дослідженнями, має охоплювати не лише технічну імплементацію ZTA, а й розробку внутрішніх політик для персоналу та студентів, регулярне навчання та підвищення кіберкультури, аудит результатів впровадження і багаторівневу модифікацію політик в залежності від змін у цифровому середовищі [82, 38, 48].

Втім, слід зазначити, що впровадження Zero Trust Architecture в освітньому середовищі супроводжується низкою викликів. У наукових працях зазначаються такі аспекти:

- високі фінансові та організаційні витрати на модернізацію інфраструктури та розгортання нового програмного забезпечення;
- необхідність інтеграції різноманітних Legacy-систем без втрати критичних функцій;
- ускладнення управління системою при великій кількості користувачів та ресурсів, притаманній ЗВО;

- потреба у постійному оновленні політик, тренінгів для персоналу та моніторингу актуальних кіберзагроз;
- ймовірність помилкових спрацювань та перенавантаження операторів системи моніторингу через часті сигнали про аномалії.

Водночас, успішна імплементація Zero Trust Architecture у цифровому освітньому середовищі дозволяє суттєво підвищити рівень кіберзахисту, знизити ризики витоків персональних даних, впровадити гнучкі моделі доступу для дистанційного та змішаного навчання, а також забезпечити відповідність сучасним стандартам міжнародних нормативних актів, зокрема GDPR, FERPA, ISO/IEC 27001 тощо.

Отже, використання принципів Zero Trust Architecture має стати базовою складовою стратегічних програм кіберзахисту сучасних освітніх установ. Це дає змогу не лише реагувати на новітні загрози, а й формувати захищене, гнучке та технологічно розвинене цифрове освітнє середовище, у якому безпека особистих даних, інтелектуальної власності та академічних процесів забезпечується на принципово новому рівні.

Таким чином, сучасні тенденції розвитку моніторингу кіберзагроз у сфері освіти підтверджують необхідність комплексного, багаторівневого та інтегративного підходу до захисту, орієнтованого на новітні технології та співпрацю із зовнішніми експертними ресурсами. Цей підхід забезпечує не лише безперервність освітнього процесу, а й формування надійного фундаменту для безпечної цифрової трансформації освіти.

1.3. Постановка завдання дослідження

Постановка завдання дослідження у даній роботі ґрунтується на необхідності забезпечення проактивного моніторингу та аналітики кіберзагроз у цифровому освітньому середовищі закладу вищої освіти з урахуванням сучасних вимог до захисту інформації, безперервності надання освітніх послуг та дотримання міжнародних стандартів управління інформаційною безпекою. Центральним елементом пропонованого підходу є створення інтегрованої

системи моніторингу та аналізу подій інформаційної безпеки, що забезпечує централізований збір, кореляцію та візуалізацію подій з різномірних джерел з метою своєчасного виявлення кіберінцидентів, підтримки процесів реагування та управління ризиками в університетському середовищі. У попередніх дослідженнях доведено зростання кількості атак на освітні інформаційні системи, зокрема на платформи дистанційного навчання, облікові системи студентів і викладачів та хмарні сервіси ЗВО, що обумовлює підвищені вимоги до побудови комплексних систем моніторингу на основі концепцій SIEM/SOAR, Zero Trust та ризик-орієнтованого управління кібербезпекою. Відповідно, актуальність дослідження зумовлена потребою адаптації сучасних методів збору, аналізу й кореляції подій безпеки до специфіки цифрової інфраструктури університету, яка включає LMS, сервіси електронного кампусу, VPN-доступ, хмарні ресурси, мобільні пристрої, IoT-компоненти та інші критичні освітні сервіси.

Метою функціонування розроблюваної системи моніторингу та аналізу кіберзагроз є забезпечення централізованого збору, обробки, кореляції та представлення подій інформаційної безпеки з інформаційних систем університету для своєчасного виявлення загроз, інцидентів і порушень політик безпеки, а також для підтримки процесів реагування, документування та управління кіберризиками в освітньому середовищі. У контексті цієї мети система повинна забезпечувати інтеграцію з ключовими сервісами цифрового університету, підтримувати різні формати обміну даними, механізми аналітики на основі правил та поведінкових моделей, а також формувати індикатори ефективності (наприклад, MTTD, MTTR) для оцінювання поточного стану захищеності освітньої інфраструктури. Додатково мета роботи передбачає узгодження архітектури системи моніторингу з вимогами міжнародних стандартів ISO/IEC 27001:2022 та ISO/IEC 27002:2022, рекомендаціями NIST Cybersecurity Framework та практиками організації центрів моніторингу безпеки (SOC) у сфері вищої освіти.

Вищезазначене обґрунтування актуальності та мети зумовлює постановку наукового завдання, яке полягає в теоретичному та прикладному опрацюванні методів і технологій побудови системи моніторингу та аналізу кіберзагроз у цифровому освітньому середовищі університету, здатної забезпечити безперервний контроль подій, автоматизоване виявлення інцидентів і підтримку процесів реагування відповідно до вимог нормативно-правового та стандартного забезпечення у сфері кібербезпеки. Для досягнення поставленої мети необхідно, по-перше, узагальнити сучасні підходи до моніторингу подій інформаційної безпеки в освітній сфері, визначити їх переваги та обмеження щодо застосування у середовищі ЗВО, зокрема з урахуванням розподіленої архітектури сервісів та активного використання хмарних і мобільних технологій. По-друге, слід формалізувати вимоги до моделі системи моніторингу та аналізу кіберзагроз з урахуванням особливостей інформаційної інфраструктури Житомирського державного університету імені Івана Франка та результатів аналізу кіберзагроз, характерних для освітнього середовища (несанкціонований доступ, компрометація облікових даних, атакування LMS, DDoS-атаки на веб-ресурси, шкідливе ПЗ у хмарних і локальних сервісах тощо).

Підґрунтям для розроблення системи виступає, з одного боку, необхідність підвищення рівня кібербезпеки цифрового освітнього середовища та забезпечення безперервності освітнього процесу, а з іншого – потреба у дотриманні вимог міжнародних стандартів ISO/IEC 27001:2022, ISO/IEC 27002:2022, регламентів щодо захисту персональних даних (зокрема, з орієнтацією на положення GDPR для обробки персональних даних здобувачів освіти та працівників) і національних нормативно-правових актів щодо кіберзахисту інформаційних ресурсів ЗВО. Відповідно до цих вимог у межах дослідження ставиться завдання визначити перелік функціональних та нефункціональних вимог до системи моніторингу, які б одночасно забезпечували відповідність стандартам, масштабованість та інтегровність з існуючими цифровими сервісами університету. Окрему увагу необхідно приділити дотриманню принципів «privacy by design» та «data protection by

default» під час проєктування модулів збору, зберігання та обробки подій безпеки, що містять персональні та службові дані користувачів освітнього середовища.

У рамках першої групи завдань дослідження необхідно сформулювати та формалізувати функціональні вимоги до системи, що передбачають автоматизований збір журналів подій із систем дистанційного навчання, сервісів автентифікації, серверної інфраструктури, мережевого обладнання, баз даних, хмарних платформ і кінцевих пристроїв; підтримку різних форматів журналів (наприклад, Syslog, JSON, XML); фільтрацію, нормалізацію та агрегацію подій з метою подальшого аналізу та кореляції. Наступним підзавданням є формування вимог до підсистеми аналізу та кореляції подій, яка має підтримувати сигнатурні та правил-орієнтовані методи виявлення, поведінковий аналіз з використанням ML/AI-алгоритмів, механізми виявлення аномалій і підозрілої активності користувачів та інформаційних систем, а також класифікацію інцидентів за рівнями критичності з урахуванням контексту освітнього процесу. Додатково необхідно уточнити вимоги до підсистеми реагування, яка повинна забезпечувати автоматичне сповіщення відповідальних осіб про виявлені інциденти, підтримувати сценарії автоматизованого та напівавтоматизованого реагування (playbook-и SOC) і вести реєстр інцидентів та дій реагування для аудиту, навчання персоналу та подальшого вдосконалення політик безпеки.

Окремий блок завдань пов'язаний із розробленням вимог до візуалізації та звітності, що передбачає створення інтерактивних панелей моніторингу для оперативного контролю стану кібербезпеки, формування аналітичних звітів щодо інцидентів, тенденцій атак та рівня ризиків, підтримку експорту звітів у стандартних форматах для подання керівництву університету та зовнішнім контролюючим органам. У контексті нефункціональних вимог необхідно обґрунтувати показники продуктивності (забезпечення обробки подій у режимі 24/7, масштабованість системи відповідно до зростання кількості користувачів і джерел подій, мінімальна затримка між надходженням події та її аналізом), а також сформулювати вимоги до надійності й доступності, включно з резервуванням

даних і компонентів, відмовостійкістю окремих модулів та підтримкою концепцій високої доступності для критичних сервісів. Додатково мають бути сформульовані вимоги до безпеки самої системи моніторингу (автентифікація та авторизація користувачів, розмежування прав доступу, захист каналів передавання даних, журналювання дій користувачів), до сумісності та інтеграції (інтеграція з існуючими цифровими системами ЗВО, підтримка відкритих стандартів і API, можливість підключення зовнішніх джерел кіберрозвідки – threat intelligence), а також до зручності використання (інтуїтивно зрозумілий інтерфейс, підтримка різних ролей користувачів, гнучке налаштування панелей та звітів).

Завершальним елементом постановки завдання є формування вимог до архітектури системи моніторингу та аналізу кіберзагроз, яка має базуватися на модульній багаторівневій структурі та включати рівень збору даних (агенти, конектори, сенсори подій), рівень обробки даних (нормалізація, агрегація, зберігання), аналітичний рівень (модулі кореляції, правила виявлення, нейронні мережі й алгоритми поведінкового аналізу), рівень реагування (SOAR-механізми, оповіщення, автоматизація процедур реагування) та рівень представлення результатів (панелі моніторингу, звіти, користувацькі інтерфейси). Події з різних джерел мають надходити до рівня збору, проходити попередню обробку, передаватися до аналітичного ядра, де результати аналізу використовуються для запуску сценаріїв реагування й актуалізації стану безпеки у візуальних інтерфейсах, що забезпечує замкнений цикл «виявлення – аналіз – реагування – удосконалення» у процесах управління кіберризиками університету. У роботі передбачається дослідити варіанти розгортання системи в локальній інфраструктурі ЗВО, у гібридному середовищі з використанням хмарних сервісів та в умовах підвищених вимог до захисту персональних даних, що дозволить сформулювати рекомендації щодо вибору оптимальної архітектурної конфігурації для вітчизняних університетів з різним рівнем зрілості цифрової інфраструктури.

Висновки до розділу 1

Узагальнення результатів аналізу, проведеного у першому розділі, дозволяє констатувати, що сучасне цифрове освітнє середовище функціонує в умовах високої динаміки кіберзагроз, зумовленої одночасним зростанням цифрової залежності освітніх процесів, інтенсивною інтеграцією хмарних сервісів, LMS-платформ, мобільних і IoT-пристроїв та ускладненням мережевої архітектури закладів освіти. На цьому тлі ключовими чинниками уразливості виступають відкритість освітніх мереж, використання застарілого програмного забезпечення, недостатня сегментація інфраструктури, дефіцит кваліфікованих кадрів і низький рівень культури кібергігієни серед учасників освітнього процесу, що визначає підвищений ризик цілеспрямованих атак, витоків даних та порушення безперервності функціонування критичних освітніх сервісів.

Проведений огляд актуальних методів і технологій моніторингу кіберзагроз засвідчив, що ефективне забезпечення кібербезпеки в освіті можливе лише за умови застосування багаторівневого, інтегрованого підходу, у якому поєднуються IDS/IPS-системи, SIEM-платформи, DLP-рішення, ML/AI-модулі аналізу аномалій, honeypot-та sandbox-технології, механізми колективного обміну кіберрозвідувальною інформацією та концепція Zero Trust Architecture. Таке поєднання дає змогу не лише здійснювати безперервний збір і кореляцію подій безпеки з різномірних джерел, але й значно підвищувати точність виявлення складних багатовекторних атак, скорочувати час реагування на інциденти та формувати адаптивні стратегії захисту, орієнтовані на реальні ризики цифрового освітнього середовища.

Аналіз нормативно-правових засад, а також міжнародних рекомендацій і галузевих ініціатив показав, що вимоги до кібербезпеки закладів освіти дедалі більше орієнтуються на стандарти ISO/IEC 27001, національне законодавство у сфері захисту персональних даних та інформації в інформаційно-телекомунікаційних системах, а також на європейські підходи до організації процесів моніторингу, інцидент-менеджменту й обміну інформацією

про загрози. Відповідність цим вимогам передбачає не тільки впровадження технічних засобів контролю доступу, журналювання та шифрування, а й розбудову інституційної системи управління ризиками, яка включає формування внутрішніх політик безпеки, процедур реагування на інциденти, механізмів звітності, аудиту та підвищення кіберкомпетентності персоналу.

Сформульовані функціональні й нефункціональні вимоги до системи моніторингу та аналізу кіберзагроз відображають виявлені уразливості й тенденції розвитку цифрової інфраструктури закладів вищої освіти та конкретизують ціль дослідження як розроблення модульної багаторівневої системи, здатної здійснювати централізований збір, кореляцію, візуалізацію та підтримку реагування на інциденти в режимі, наближеному до реального часу. Задання на систему інтегрує вимоги щодо масштабованості, відмовостійкості, забезпечення конфіденційності й цілісності освітніх даних, сумісності з існуючими цифровими сервісами університету та можливості підключення зовнішніх джерел threat intelligence, що створює концептуальне підґрунтя для подальшого проектування архітектури багаторівневої системи кіберзахисту цифрового освітнього середовища, реалізація якої буде розглянута у другому розділі.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ КІБЕРЗАГРОЗ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

2.1. Аналіз цифрового освітнього середовища Житомирського державного університету імені Івана Франка

Цифрове освітнє середовище сучасного закладу вищої освіти формується на перетині процесів цифрової трансформації, розвитку електронного навчання та ускладнення кіберзагроз, що вимагає цілісного підходу до його проектування, експлуатації та захисту. З позицій кібербезпеки цифрове освітнє середовище доцільно розглядати як інтегровану сукупність інформаційно-комунікаційної інфраструктури, програмних сервісів підтримки освітнього процесу, електронних ресурсів та цифрових слідів учасників навчання, які функціонують у єдиному керованому просторі з визначеними політиками доступу, моніторингу та реагування на інциденти безпеки (Рис. 2.1).



Рисунок. 2.1. – Компоненти цифрового освітнього середовища

У такій інтерпретації головним є не лише забезпечення функціональності дистанційного та змішаного навчання, а й підтримання цілісності, конфіденційності та доступності освітніх даних, а також стійкості до кіберінцидентів, що узгоджується із сучасним баченням кібербезпеки в цифровому освітньому середовищі за результатами досліджень у сфері вищої освіти.

Цифровізація освітнього середовища Житомирського державного університету імені Івана Франка ґрунтується на системному впровадженні сучасних цифрових платформ, що охоплюють усі основні функціональні компоненти діяльності університету: освітній процес, адміністрування, наукову діяльність, забезпечення якості освіти, електронний документообіг, бібліотечні сервіси та професійний розвиток персоналу. Відповідно до стратегічних документів університету, цифрове середовище визначається як «сукупність цифрових платформ та сервісів, інструментів адміністрування, захищених інформаційних ресурсів і сервісів для збору, збереження, обробки і передавання освітньої, наукової, управлінської та організаційної інформації, що використовує сучасні стандарти інформаційної безпеки на всіх етапах життєвого циклу даних» [6].

Основними складовими цифрового освітнього середовища Житомирського державного університету імені Івана Франка (Рис.2.2) є:

- програмно-апаратний комплекс забезпечення (сервери, робочі станції, мережеві пристрої, захисне мережеве обладнання);
- система управління навчальним процесом та адміністративною діяльністю (електронні курси, журнали, портали академічної мобільності, платформи дистанційного навчання);
- електронна бібліотека, система наукових публікацій, платформи для забезпечення академічної доброчесності;
- інструменти електронного документообігу, цифрові платформи для контролю якості вищої освіти;

– платформи моніторингу діяльності науково-педагогічних працівників та здобувачів;

– програмне забезпечення для підтримки роботи приймальної комісії, формування освітніх програм, підвищення кваліфікації, звітності та електронного портфоліо та ін.

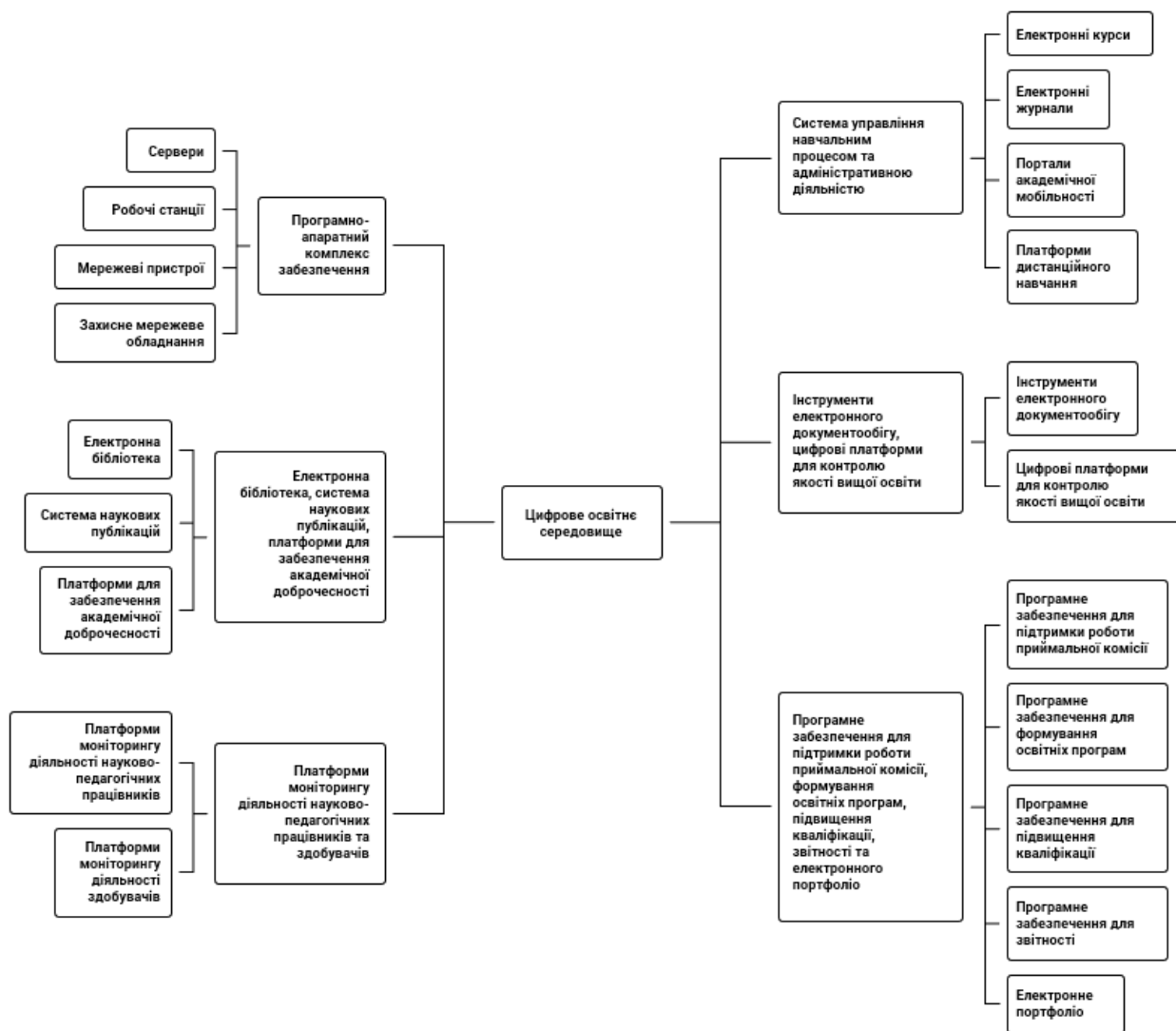


Рисунок 2.2. – Основні складові цифрового освітнього середовища
Житомирського державного університету імені Івана Франка

Впровадження та розвиток цифрового освітнього середовища в університеті уможливило реалізацію таких принципів, як відкритість, прозорість, оперативність взаємодії, персоналізований підхід до освітньої траєкторії кожного здобувача освіти, підвищення академічної доброчесності та кібергігієни всіх учасників університетського середовища.

З метою реалізації принципів відкритості, інноваційності й високого рівня захищеності інформаційного простору в Житомирському державному університеті імені Івана Франка сформовано комплексну цифрову екосистему (Рис. 2.3.), яка охоплює різноманітні напрями освітньої, адміністративної та наукової діяльності. Ключовими структурними елементами цього середовища є сервіси для моніторингу професійної активності та формування цифрових портфоліо (E-portfolio), управління освітніми програмами (Educational Program), автоматизації процесів підвищення кваліфікації (Experience, eTraining), підтримки вступної кампанії (Enter), а також електронна бібліотека, цифрова платформа ZDU Project, системи обліку проживання у гуртожитках (E-hostel) і додаткові ресурси, що суттєво підвищують ефективність усіх процесів університету. Важливе місце у цифровій інфраструктурі займають рішення компанії «Політек-СОФТ», які забезпечують централізоване адміністрування навчального процесу, електронне планування, автоматизацію розкладу, облік контингенту та ведення електронних журналів успішності здобувачів. Програмні продукти інтегруються з іншими платформами екосистеми, сприяють прозорості, ефективній координації діяльності й підвищують рівень захисту даних завдяки сучасним інструментам авторизації та резервного копіювання.



Рисунок 2.3. – Цифрова екосистема Житомирського державного університету імені Івана Франка

До складу цифрового освітнього середовища Житомирського державного університету імені Івана Франка входить низка функціональних платформ, що охоплюють основні освітні й управлінські процеси. Зокрема, мережа програмних продуктів ТОВ «Політек-СОФТ» забезпечує централізоване адміністрування навчального процесу та інформаційного супроводу освітньої діяльності. Програмні модулі «ПС-Навчальний план», «ПС-Навчальний процес», «ПС-Розклад», «ПС-Студент» дозволяють здійснювати електронне планування, формувати індивідуальні навчальні траєкторії, автоматизувати складання розкладів та облік контингенту здобувачів освіти. Ця інтегрована система сприяє не лише прозорості академічної політики, а й підвищенню ефективності освітнього менеджменту, мінімізує ризики несанкціонованого втручання або втрати даних через впроваджені засоби авторизації, контролю доступу й резервного копіювання. Електронні журнали успішності для викладачів і здобувачів освіти створені спеціально для моніторингу прогресу студентів, оперативного зворотного зв'язку, обліку відвідуваності, виконання завдань тощо. За рахунок багаторівневої системи права доступу й захисту персональних даних, зокрема багатофакторної автентифікації, забезпечується інформаційна конфіденційність освітнього процесу, що є одним із ключових принципів кібербезпеки у ЗВО.

Особливе місце посідає платформа E-portfolio (<https://eportfolio.zu.edu.ua/>), яка забезпечує документообіг щодо фіксації та оцінювання наукової, методичної, виховної, профорієнтаційної активності науково-педагогічних працівників. Кожен працівник має особистий електронний кабінет (<https://eportfolio.zu.edu.ua/user/414/>), у якому відслідковуються всі етапи професійної діяльності, а система автоматично формує аналітичні звіти щодо виконання обов'язків і досягнення визначених цілей. Завдяки цьому підвищується рівень прозорості, об'єктивності та стимулювання сумлінної праці персоналу.

Ще одним важливим елементом є Experience (<https://exp.zu.edu.ua/profile/>), вебплатформа для контролю за проходженням стажувань, підвищення

кваліфікації, автоматизованого збору звітності й сертифікації працівників. Інформаційна архітектура цієї системи дозволяє швидко обробляти великі обсяги даних, генерувати статистичні звіти, своєчасно ідентифікувати потреби у професійному розвитку та підвищенні якості людського капіталу університету.

Платформа Enter (<https://enter.zu.edu.ua/>) призначена для автоматизації процедур прийому в університет, включаючи електронну реєстрацію заяв, верифікацію документів та формування єдиної бази даних приймальної кампанії. До ключових переваг платформи варто віднести інтеграцію з національними базами даних та впровадження протоколів двофакторної ідентифікації, що підвищує кіберстійкість усіх етапів прийому абітурієнтів.

Цифровий сервіс EducationProgram (<https://ep.zu.edu.ua/>) є центральною ланкою в управлінні освітніми програмами університету, забезпечуючи їх електронне проєктування, візуалізацію структури, погодження змін і публічну презентацію для здобувачів, стейкхолдерів та органів внутрішнього забезпечення якості освіти. Платформа дає змогу уніфікувати структуру освітніх програм, формалізувати результати навчання, описи компонентів, узгодити обсяг кредитів, форми контролю та зв'язати ці елементи з нормативними документами, що підвищує прозорість та відтворюваність навчального процесу на всіх рівнях. З позицій кібербезпеки важливо, що доступ до адміністративної частини сервісу обмежений автентифікацією працівників, а публічна частина функціонує як відкритий репозиторій структурованої інформації без можливості несанкціонованого редагування, що мінімізує ризики спотворення офіційних даних про освітні програми.

Платформа eTraining (<https://etraining.zu.edu.ua/>) орієнтована на організацію курсів підвищення кваліфікації педагогічних та науково-педагогічних працівників, зокрема розробку, реєстрацію, проведення й оцінювання програм неформальної освіти. Вона підтримує повний цикл управління освітніми програмами підвищення кваліфікації: від онлайн-реєстрації слухачів, доступу до навчальних матеріалів, інтеграції із засобами відеоконференцій (наприклад, Zoom), до генерації електронних сертифікатів та

формування статистичних звітів для внутрішнього моніторингу і зовнішньої звітності. Розробка цієї платформи враховує вимоги захисту персональних даних та безпечної автентифікації користувачів, що є критичним для збереження конфіденційної інформації про освітні траєкторії й результати навчання дорослих.

Система ZDUproject (<https://project.zu.edu.ua/>) виступає спеціалізованим освітнім порталом для організації дистанційного навчання та онлайн-курсів, де розміщуються навчально-методичні матеріали, електронні курси, інтерактивні завдання і тестові модулі. Портал підтримує різні формати контенту (тексти, презентації, відео, тести), надаючи викладачам можливість формувати цілісні електронні курси, а студентам – проходити навчання як у синхронному, так і асинхронному режимах, що узгоджується з сучасними підходами до змішаного та відкритого навчання. З точки зору кібербезпеки важливими є функції персоніфікованого доступу (через облікові записи студентів і викладачів), логування активності, захисту авторських прав на розміщені матеріали й контролю цілісності навчального контенту.

Електронна бібліотека університету (<https://eprints.zu.edu.ua/>) забезпечує відкритий доступ до наукових публікацій, кваліфікаційних праць, навчально-методичних матеріалів, методичних рекомендацій та інших інформаційних ресурсів університету. Вона реалізована на базі репозитарної платформи, що дозволяє формувати метадані публікацій, організовувати пошук за авторами, ключовими словами, роком публікації, типом документа, а також зберігати повні тексти у форматі електронних файлів. Репозитарій виступає одночасно й інструментом популяризації результатів наукової діяльності, і компонентом системи запобігання плагіату, оскільки публічний доступ до матеріалів дозволяє здійснювати перехресну перевірку оригінальності текстів різними інструментами академічної доброчесності.

E-Hostel (<https://ehostel.zu.edu.ua/new-resident-form/>) – це електронна система обліку та організації поселення здобувачів та інших осіб у гуртожитках Житомирського державного університету імені Івана Франка. Форма нового

мешканця на платформі E-Hostel дозволяє здійснити попередню реєстрацію та сформувати пакет необхідних документів для поселення, таких як заява та договір про проживання, які генеруються автоматично на основі введених даних. Система інтегрується з внутрішніми процесами університету, забезпечує захищений електронний документообіг, автоматизований облік мешканців та контроль статусу проживання в усіх гуртожитках закладу. Це значно підвищує прозорість поселення, скорочує час на адміністративні операції та зменшує ризики втрати особистих або організаційних даних у процесі роботи із студентською житловою інфраструктурою.

Додатковими складовими цифрового середовища Житомирського державного університету імені Івана Франка є сервіси електронного документообігу, які дозволяють значно автоматизувати внутрішні управлінські й адміністративні процеси. Застосування таких інструментів дає змогу забезпечити прозорість та контроль на всіх етапах погодження, створення, розгляду й підписання управлінських документів, виключає ризики втрати оригіналів та прискорює ухвалення рішень у масштабах університету. Електронний документообіг інтегрується з іншими платформами університету, формуючи єдиний інформаційний простір для моніторингу виконання, делегування повноважень та збереження архіву документів. Системи документообігу, які застосовує Житомирський державний університет імені Івана Франка, зберігають історію змін та контролюють права доступу до кожного окремого документа, що є важливим чинником кіберстійкості й відповідальності персоналу щодо збереження конфіденційної інформації.

Критичною особливістю цифрового освітнього середовища Житомирського державного університету імені Івана Франка є високий ступінь інтеграції та взаємодії платформ. Використання уніфікованих облікових записів, корпоративних доменів та засобів багатофакторної автентифікації значно підвищує захист даних та зменшує ймовірність несанкціонованого доступу. Вся архітектура екосистеми побудована з врахуванням потреб персонального захисту інформації, персоніфікованого логування діяльності користувачів,

реалізації мінімальних прав доступу для кожної ролі і регулярного ризик-орієнтованого аудиту інфраструктури.

Моніторинг і керування цифровими платформами здійснюється комплексом адміністративних, технічних і організаційних заходів, що включають централізовані панелі керування, використання SIEM-систем, модулів журналювання подій та аналітики. Ці системи дають змогу оперативно відслідковувати спроби злому, порушення політик безпеки чи аномальну активність, що дозволяє вчасно реагувати на кіберзагрози й забезпечувати безперервність освітньої діяльності. Завдяки впровадженню цифрового моніторингу та обробки інцидентів, університет забезпечує виконання стандартів і вимог сучасної кібербезпеки та оптимізує постійну взаємодію різних компонентів цифрового середовища.

Сучасна архітектура цифрового освітнього середовища Житомирського державного університету імені Івана Франка враховує не лише потреби якісної освіти, а й світові і національні вимоги до кібербезпеки. Систематична інтеграція нових сервісів (наприклад, електронних платформ для публікації наукових і навчально-методичних доробків, сервісів перевірки текстів на плагіат, платформ академічної доброчесності) забезпечує університету перевагу у впровадженні інноваційних підходів до цифрового менеджменту й обробки інформації. Застосування сучасних методів захисту даних – шифрування при зберіганні й передаванні, антивірусні комплекси, багаторівнева ідентифікація користувачів, а також регулярне навчання персоналу цифрової гігієни – суттєво мінімізує потенційні загрози та підвищує загальний рівень кіберстійкості освітнього середовища [5, 6].

Важливою особливістю цифрового середовища Житомирського державного університету імені Івана Франка є його відкритість до цифрової трансформації й гнучкість у впровадженні нових сервісів за потреби. Реалізовано ефективну інтеграцію з національними освітніми платформами, стандартами відкритої науки й електронного врядування. Стратегія розвитку університету до 2028 року передбачає подальшу диджиталізацію адміністративних і навчальних

процесів, інвестування у побудову власного дата-центру, а також посилення співпраці з партнерами задля впровадження сучасних аналітичних і захисних рішень. Особлива увага приділяється мотивації персоналу до постійного підвищення цифрових компетентностей та впровадженню процесів багаторівневого моніторингу безпеки [6].

Одним із рушіїв сталого розвитку цифрового середовища Житомирського державного університету імені Івана Франка є високий рівень цифрової культури серед студентів і співробітників, організація системного навчання основам безпечної поведінки в мережі, інструктажі з реагування на кіберінциденти та практична орієнтація навчальних курсів на реальні потреби цифрової економіки. Університет демонструє вміння оперативно реагувати на зміни зовнішнього середовища, впроваджує політику відкритих даних у межах факультетів, бере участь у міжнародних проєктах цифрової освіти, які посилюють цілісність і надійність всіх цифрових компонентів.

Формування комплексного цифрового освітнього середовища Житомирського державного університету імені Івана Франка імені Івана Франка стало системною відповіддю сучасним викликам, що стоять перед університетською спільнотою. Інтеграція інноваційних цифрових платформ і сервісів, підтримка високих стандартів кібербезпеки, організаційна гнучкість, злагоджена взаємодія всіх компонентів та персоніфікований підхід до адміністрування демонструють, що університет сьогодні є одним із лідерів цифрової трансформації в секторах освітньої, наукової та адміністративної діяльності серед закладів вищої освіти України. Це, у свою чергу, зумовлює не лише зростання конкурентоспроможності університету, а й підвищення якості й стійкості усіх освітніх та управлінських процесів в умовах глобальних інформаційних загроз і цифрових трансформацій.

2.2. Вимоги до забезпечення кібербезпеки в освітніх установах

В сучасних умовах цифрової трансформації освітнього середовища питання забезпечення кібербезпеки набуло особливої актуальності. Освітні

установи володіють значним обсягом конфіденційної інформації про студентів, викладачів, адміністративний персонал, а також мають критичну інформаційну інфраструктуру, що використовується для навчального процесу, дослідницької діяльності, управління закладом тощо. Враховуючи специфіку освітніх установ, формування вимог до забезпечення кібербезпеки повинно ґрунтуватися на системному підході, який охоплює організаційні, нормативно-правові, технологічні та освітні аспекти.

На міжнародному рівні одним із ключових орієнтирів для розроблення вимог слугують стандарти ISO/IEC 27001:2022 та ISO/IEC 27002:2022, які визначають рамки інформаційної безпеки і політики захисту даних. В українській практиці реалізація цих стандартів дозволяє сформулювати політику управління ризиками й захисту інформації в контексті закладів освіти. Додатково важливу роль відіграють рекомендації Європейського союзу щодо кібербезпеки в освітньому секторі, що відображають вимоги до захисту персональних даних відповідно до GDPR і Директиви NIS2 [9, 25].

Нормативно-правове забезпечення кібербезпеки для освітніх установ України складається із комплексу актів, серед яких особливо виділяються Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про захист персональних даних», постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» та відповідні галузеві накази Міністерства освіти і науки [19, 18, 16]. Крім того, враховуються вимоги Стратегії кібербезпеки України, що задають орієнтири для будівництва сучасної, стійкої та адаптованої системи захисту інформації в освітніх закладах [20].

Суттєвим елементом організації захисту інформації та IT-інфраструктури є визначення підходів до ідентифікації, оцінки і управління ризиками. В освітніх закладах повинні бути реалізовані процедури ідентифікації типових кіберзагроз, таких як DDoS-атаки на сервери освітніх платформ, несанкціонований доступ до електронних баз даних, фішингові атаки на користувачів, шкідливе програмне забезпечення тощо. Проведення регулярних аудитів інформаційної безпеки,

моніторингу подій, а також впровадження сучасних засобів аналізу журналів доступу – основа превентивного захисту [8, 40].

Кадровий аспект відіграє ключову роль у забезпеченні кібербезпеки освітніх установ. До основних вимог належить підготовка та підвищення кваліфікації персоналу у сфері кібербезпеки, організація регулярного навчання користувачів основам безпечної роботи в цифровому середовищі, формування культури кібергігієни. У 2022 році в Україні були затверджені перші шість професійних стандартів для фахівців із кібербезпеки, у тому числі для посад, пов'язаних з плануванням політики і стратегії кібербезпеки. Це сприяє підвищенню якості кадрового забезпечення кіберзахисту [21].

Важливою складовою реалізації вимог є впровадження багаторівневої системи моніторингу та захисту освітнього цифрового середовища. Для цього освітні установи повинні інтегрувати сучасні програмно-апаратні рішення, які дають змогу автоматично виявляти, локалізувати і блокувати кіберзагрози, аналізувати їхню динаміку та швидко реагувати на інциденти. Особливу цінність мають SIEM-системи, засоби детектування DDoS-атак, антивірусне ПЗ, засоби аналізу вхідних і вихідних мережевих потоків, шлюзи веб-контролю, а також рішення для захисту електронних освітніх платформ і LMS.

Об'єктивізована система вимог також передбачає впровадження заходів для захисту персональних даних, що відповідають чинним вимогам GDPR та українському законодавству. Основні принципи – це мінімізація обсягу оброблюваних даних, формування політики конфіденційності для всіх інформаційних систем, позбавлення зайвого доступу, регулярне шифрування даних на рівні збереження та передачі, а також резервування даних [19].

Наступною вимогою є підготовка і затвердження внутрішніх нормативних документів закладу освіти, що регламентують політику кіберзахисту: положення щодо поводження з інформацією, алгоритми реагування на кіберінциденти, системи управління доступом до даних і ресурсів, а також інструкції для співробітників та учасників освітнього процесу стосовно кібергігієни. З точки зору юридичного забезпечення така діяльність відповідає вимогам не лише

законодавства, але і сучасних рекомендацій Національного координаційного центру кібербезпеки, профільних аналітичних досліджень IPPI.

У практичній площині ефективне забезпечення кібербезпеки передбачає багаторівневий моніторинг подій, автоматизоване реагування на інциденти, проведення систематичних інструктажів з кіберзахисту для персоналу та студентів, впровадження процедур кібергігієни (зміна паролів, багатофакторна автентифікація, інформаційна грамотність), а також регулярний аналіз та оновлення системи кіберзахисту відповідно до новітніх світових тенденцій.

Для комплексного висвітлення провідних аспектів та забезпечення логічної структури аналізу доцільно представити узагальнену таблицю основних вимог до кібербезпеки для освітніх установ, що дозволяє суттєво підвищити доступність і ефективність засвоєння матеріалу, а також окреслити основні напрями практичної реалізації захисту інформації у сучасному цифровому освітньому середовищі (Таблиця 2.1).

Таблиця 2.1.

Основні вимоги до забезпечення кібербезпеки в освітніх установах

№	Вимога	Коротка характеристика
1.	Нормативне забезпечення	Дотримання законодавства у сфері кібербезпеки, внутрішні положення
2.	Управління ризиками	Ідентифікація загроз, регулярний аудит безпеки, моніторинг
3.	Кадрове забезпечення	Підготовка фахівців, удосконалення компетенцій, навчання користувачів
4.	Технічний захист	Інтеграція SIEM, антивірусних систем, систем багаторівневого аналізу
5.	Захист персональних даних	Зберігання, обробка і передача даних відповідно до вимог GDPR, шифрування
6.	Організаційні процедури	Документовані політики кібербезпеки, інструкції, алгоритми реагування
7.	Безперервний моніторинг	Оперативне реагування на кіберінциденти, постійний аудит й оновлення системи

Усі зазначені вище вимоги повинні бути пристосовані до специфіки конкретного закладу, з урахуванням розміру, структури ІТ-інфраструктури, типу освітніх платформ, рівня цифровізації та залучення до міжнародних освітніх мереж. Ефективна імплементація вимог забезпечує не лише захист освітньої

інформації та приватності, а й сприяє сталому розвитку освітніх процесів у цифровому середовищі.

Таким чином, формування системи вимог до забезпечення кібербезпеки в освітніх установах в Україні – це багатофакторний, комплексний процес, що має об'єднувати правові, організаційні та технічні заходи, а також впровадження культури кібергігієни серед усіх учасників освітнього процесу. Дотримання галузевих та міжнародних стандартів, постійна актуалізація політики безпеки, інтеграція сучасних рішень моніторингу і захисту даних – запорука стійкості освітнього закладу перед викликами сучасного цифрового світу.

2.3. Обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі

Обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі неможливе без чіткої логіки відбору, яка враховує як специфіку цифрової інфраструктури університету, так і нормативно-правові вимоги до захисту персональних даних та безперервності освітнього процесу. У контексті Житомирського державного університету імені Івана Франка, де цифрове освітнє середовище вже характеризується значною кількістю веб-сервісів, розподіленими обліковими записами та активним використанням хмарних платформ, системи моніторингу мають підтримувати збір подій з різномірних джерел, кореляцію інцидентів та побудову аналітичних візуалізацій без створення надмірного навантаження на локальні ресурси. Сучасні дослідження з кібербезпеки в закладах вищої освіти підкреслюють, що ключову роль відіграють рішення, здатні інтегруватися в наявні мережеві сегменти університету та підтримувати механізми раннього виявлення інцидентів, зокрема в середовищі LMS, електронних журналів, систем електронного документообігу та студентських порталів. Саме тому підсистема моніторингу в проєктованій системі має будуватися як поєднання відкритих і комерційних інструментів, які доповнюють один одного з точки зору масштабованості, функціональної повноти та відповідності вимогам регуляторів [83].

Логіка відбору програмних рішень для моніторингу та аналізу кіберзагроз базується на багатокритеріальному підході, який враховує технічні, організаційні та правові параметри, релевантні для університетського середовища. З технічної точки зору до ключових критеріїв належать: масштабованість (здатність обробляти зростаючі обсяги логів і телеметрії без деградації продуктивності), інтегрованість у внутрішні мережі ЗВО (підтримка стандартних протоколів журналювання, агентів для кінцевих пристроїв та інтеграції з мережевим обладнанням), підтримка інтерфейсів для SIEM/SOAR-платформ (API, веб-хуки, конектори до платформ керування подіями безпеки). Організаційний вимір включає доступність компетенцій для розгортання та супроводу системи, наявність спільноти підтримки, можливість поетапного впровадження та навчання персоналу служби інформаційної безпеки університету. Правові критерії включають відповідність принципам GDPR, вимогам NIS2 щодо операторів критичних та важливих послуг, а також гармонізацію з українським законодавством у сфері захисту персональних даних та кібербезпеки, що особливо підкреслюється у сучасних роботах із аналізу інформаційної безпеки в Україні.

Окремий блок критеріїв стосується забезпечення конфіденційності та мінімізації обробки персональних даних, оскільки в освітньому середовищі значна частина подій містить конфіденційну інформацію про студентів, викладачів та працівників. Перевага надається тим рішенням, які дозволяють реалізувати принципи «privacy by design» і «data minimization», зокрема передбачають механізми псевдонімізації, маскування або хешування ідентифікаторів користувачів ще на етапі збору та нормалізації логів. Для університетів, що орієнтуються на європейський освітній простір, важливо, щоб платформи моніторингу підтримували контрольований експорт даних, гнучке керування політиками зберігання та аудит доступу до журналів безпеки, що прямо впливає з вимог GDPR і сучасної практики забезпечення кібербезпеки у ЗВО. У дослідженнях, присвячених оцінюванню кіберзагроз в українській вищій освіті, наголошується, що системи моніторингу мають не тільки виявляти інциденти, а й

забезпечувати прозорість процесів обробки даних для суб'єктів персональних даних і регуляторів [1, 83].

У межах проектування системи моніторингу для цифрового освітнього середовища доцільно співставити можливості відкритих і комерційних рішень, враховуючи, що на попередніх етапах дослідження вже було показано доцільність використання SIEM-орієнтованого підходу, інтегрованого з IDS/IPS, DLP та засобами Threat Intelligence. Відкриті інструменти, такі як ELK Stack (Elastic Stack), Wazuh, Zeek, MISP, OpenCTI та дистрибутив Security Onion, забезпечують гнучкість, відсутність ліцензійних обмежень та можливість глибокої кастомізації під специфіку університетських сервісів. Комерційні рішення, зокрема Splunk та інші промислові SIEM-платформи, надають розширені засоби кореляції подій, підтримку машинного навчання «з коробки» та сервісну підтримку, що може бути критично важливим для ЗВО з обмеженими ресурсами власних SOC-команд. Наукові праці, присвячені побудові SIEM-рішень на базі Elastic Stack в університетському контексті, демонструють, що навіть для середніх за розміром закладів вищої освіти відкриті інструменти можуть забезпечити прийнятну ефективність виявлення загроз за умови правильного налаштування та інтеграції додаткових компонентів аналітики [36, 60].

У сучасних дослідженнях з безпеки освітніх мереж показано, що комбіновані архітектури, у яких відкриті рішення забезпечують базовий збір і зберігання журналів, а комерційні компоненти використовуються для поглибленої аналітики або інтеграції з хмарними сервісами, дозволяють досягти кращого балансу між вартістю, масштабованістю та функціональністю. Для Житомирського державного університету імені Івана Франка, який має розгалужену мережеву інфраструктуру, але обмежені фінансові ресурси порівняно з великими дослідницькими університетами, доцільно розглядати саме таку гібридну модель, у якій ядром системи моніторингу виступають відкриті платформи (ELK Stack, Wazuh, Zeek, MISP/OpenCTI), а комерційні рішення використовуються точково для окремих сегментів або проєктів, що потребують підвищеного рівня сервісної підтримки. Такий підхід узгоджується з

рекомендаціями досліджень щодо кібербезпеки у вищій освіті, де наголошується на необхідності поєднання технічної стійкості, економічної доцільності та нормативної відповідності, зокрема з урахуванням вимог GDPR, NIS2 та українського законодавства у сфері захисту інформації [1, 60, 83].

У сучасних дослідженнях із мережевого моніторингу для освітніх установ відкриті рішення позиціонуються як базовий шар інфраструктури, що забезпечує збір і попередню обробку подій, тоді як комерційні платформи частіше застосовуються для поглибленої аналітики, автоматизації реагування та інтеграції з корпоративними сервісами. ELK Stack (Elastic Stack) доцільно розглядати як універсальний інструмент для централізованого збору, зберігання, пошуку та візуалізації логів, який, за наявності відповідних модулів, може виконувати роль SIEM-компонента в університетській мережі, забезпечуючи масштабованість та гнучкість конфігурації. Дослідження, присвячені безпековій аналітиці на основі Elastic, демонструють можливість побудови адаптивних дашбордів для моніторингу подій у навчальних сервісах, мережевій інфраструктурі та хмарних платформах, що є критично важливим для університетів із розподіленою цифровою екосистемою [66, 74].

Security Onion є інтегрованим дистрибутивом, що поєднує IDS/IPS, засоби мережевого моніторингу та SIEM-функції на базі Elastic, Suricata, Zeek та Wazuh, утворюючи повнофункціональне SOC-подібне середовище, орієнтоване на використання в організаціях з обмеженими ресурсами. Кейс-дослідження впровадження Security Onion в університетському секторі показують, що ця платформа забезпечує достатню масштабованість для обробки мережевого трафіку корпусу і підтримує кореляцію подій з різних сенсорів без суттєвого збільшення витрат на ліцензування. У контексті цифрового освітнього середовища університету такий підхід дозволяє розгорнути централізовану систему спостереження за трафіком між сегментами (LMS, електронний кампус, адміністративні системи), інтегруючи її з існуючими серверами журналювання та мережевим обладнанням [47].

Компоненти Wazuh і Zeek доповнюють один одного у завданнях моніторингу та аналізу кіберзагроз в освітньому середовищі, створюючи єдиний контур спостереження за кінцевими точками й мережевим трафіком. Wazuh, як відкрите SIEM/XDR-рішення, забезпечує збір логів з робочих станцій, серверів і хмарних сервісів, виявлення аномалій та відповідність політикам безпеки, у тому числі тим, що випливають з регуляторних актів щодо захисту персональних даних. Zeek, у свою чергу, виконує роль мережевого монітора з глибоким аналізом трафіку, формуючи деталізовані журнали з'єднань, DNS-запитів, SSL-сесій та інших протоколів, що особливо важливо для виявлення прихованих атак, пов'язаних із використанням освітніх сервісів і віддаленого доступу. Інтеграція Zeek із Wazuh дозволяє збагачувати події мережевого рівня контекстом із кінцевих пристроїв та будувати кореляційні правила, орієнтовані на специфічні сценарії загроз у ЗВО (масові невдалі автентифікації в LMS, підозрілі завантаження навчальних матеріалів, зловмисне використання VPN тощо) [24].

Університетська специфіка вимагає використання не лише класичних SIEM-компонентів, а й платформ кіберрозвідувальної аналітики (Cyber Threat Intelligence, CTI), які дозволяють враховувати актуальні загрози для освітнього сектору. MISP та OpenCTI, що активно аналізуються в сучасних роботах з CTI, забезпечують можливість накопичення, кореляції та спільного використання індикаторів компрометації, тактик і технік атак, включаючи кампанії, спрямовані на університети та науково-освітні мережі. Дослідження користувацького досвіду CTI-платформ показують, що MISP та OpenCTI мають високу гнучкість щодо підтримуваних форматів, можливість інтеграції з SIEM/SOAR-системами через стандартизовані інтерфейси (STIX/TAXII, REST API) і добре підходять для побудови галузевих співтовариств обміну інформацією про загрози. Для університету це означає потенціал підключення до національних або міжнародних освітніх CTI-спільнот, отримання своєчасних індикаторів атак на освітні платформи та їх автоматизоване застосування в правилах кореляції SIEM-системи [32, 70].

Порівняння з комерційними рішеннями, такими як Splunk, демонструє, що останні пропонують розширені можливості інтеграції з широким спектром освітніх сервісів (реєстраційні системи, LMS, веб-портали, хмарні платформи), а також вбудовані сценарії для забезпечення відповідності регуляторним вимогам (FERPA, HIPAA, GDPR та ін.). Аналітичні матеріали, присвячені використанню Splunk у закладах вищої освіти, підкреслюють, що платформа здатна обробляти машинні дані практично з будь-яких джерел та підтримує побудову комплексних дашбордів для безпеки, операційної ефективності та якості освітніх послуг, що може бути корисним для університетів із розвиненою цифровою трансформацією. Разом з тим висока вартість ліцензування, а також залежність від комерційної екосистеми зменшують привабливість таких рішень для університетів із обмеженими бюджетами, особливо якщо вже існує інфраструктура на базі відкритих компонентів (ELK, Wazuh, Zeek, MISP/OpenCTI). З урахуванням попереднього аналізу інфраструктури Житомирського державного університету та наявних ресурсів, найбільш раціональним є сценарій, у якому комерційні платформи розглядаються не як ядро системи, а як опціональні модулі для окремих задач, що потребують підвищеного рівня сервісної підтримки або специфічної функціональності.

Подальше обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі вимагає деталізації критеріїв масштабованості, інтегрованості та підтримки інтерфейсів для SIEM/SOAR у контексті типових навантажень університетської мережі. Дослідження з мережевого моніторингу в галузі вищої освіти підкреслюють, що обсяг подій безпеки, генерованих інфраструктурою ЗВО (LMS, веб-портали, VPN-шлюзи, поштові системи, сховища наукових даних), зростає нелінійно внаслідок цифровізації освітнього процесу, збільшення кількості онлайн-курсів і гібридних форм навчання. У цьому контексті ELK Stack, Wazuh, Zeek, Security Onion та подібні рішення демонструють здатність масштабуватися горизонтально шляхом додавання нових нод, що дає змогу університетам нарощувати потужності відповідно до зростання кількості користувачів та сервісів без радикальної зміни

архітектури. Наявність розвинених інтерфейсів інтеграції (REST API, підтримка STIX/TAXII, модулі для обміну з CTI-платформами, конектори до SIEM/SOAR) дозволяє цим системам органічно вплітатися у загальний контур кіберзахисту університету, який включає IDS/IPS, DLP, системи управління ідентичностями та багатофакторну автентифікацію.

Особливої ваги набувають питання відповідності принципам GDPR та українському законодавству щодо захисту персональних даних під час збору і кореляції подій у системах моніторингу. Сучасні дослідження, присвячені GDPR-сумісній обробці даних у SIEM-системах, наголошують на необхідності впровадження механізмів псевдонімізації та анонімізації в ланцюг обробки логів, що дозволяє зберегти інформативність подій для виявлення інцидентів, одночасно мінімізуючи ризики ідентифікації суб'єктів даних. Рекомендації щодо налаштування SIEM-систем для відповідності GDPR роблять акцент на розмежуванні доступу до первинних логів і псевдонімізованих індексів, впровадженні ролей із принципом «мінімально необхідних повноважень» та чітких політик де-псевдонімізації лише в межах розслідування доведених інцидентів. Для українських університетів це узгоджується з положеннями Закону України «Про захист персональних даних» та сучасними науковими підходами до гармонізації національного законодавства із європейським регулюванням у сфері приватності й кібербезпеки [75].

Вибір конкретних інструментів моніторингу має спиратися на їх здатність технічно підтримувати такі механізми захисту приватності без втрати аналітичної цінності даних. Дослідження архітектур сучасних SIEM-рішень показують, що Elastic Stack, Wazuh і деякі комерційні платформи підтримують впровадження псевдонімізації ще на етапі збору логів за рахунок використання фільтрів, попередньої нормалізації та можливості винесення ключів відповідності у окремі сховища з обмеженим доступом. Низка практичних керівництв із GDPR-сумісного лог-менеджменту демонструє, що організація розділених індексів (псевдонімізований для оперативної аналітики та повний для інцидент-респонсу) дозволяє поєднати вимоги до оперативного моніторингу з

вимогами до захисту персональних даних. З точки зору університету це означає можливість налаштування збору подій у такий спосіб, щоб операційні дашборди SOC-рівня працювали з знеособленими ідентифікаторами, тоді як доступ до персоніфікованих даних був би суворо регламентований та протоколювався для аудиту [35, 55].

Аналіз сучасних емпіричних досліджень кіберзагроз в освітньому секторі підтверджує, що університети залишаються однією з найуразливіших категорій організацій через поєднання відкритості академічного середовища, високої цінності дослідницьких даних та обмежених бюджетів на кібербезпеку. Дослідження, у яких проаналізовано мережеві атаки на окремі університетські підрозділи, демонструють стійку тенденцію до зростання складності атак, включно з багатостадійними кампаніями, спрямованими на викрадення облікових записів, компрометацію поштових сервісів та використання інфраструктури ЗВО як проміжної ланки для атак на інші організації. У таких умовах системи моніторингу мають забезпечувати не лише пасивний збір логів, а й активну кореляцію подій, виявлення аномалій поведінки користувачів і автоматизовану передачу контекстної інформації до СТИ-платформ для уточнення індикаторів загроз. Це підсилює аргументацію на користь вибору рішень, які мають вбудовані або легко інтегровані механізми поведінкової аналітики, підтримку MITRE ATT&CK-орієнтованих дашбордів і можливість оперативного оновлення правил кореляції на основі зовнішніх та внутрішніх джерел кіберрозвідки [33].

Важливо, що наукові публікації, присвячені викликам кібербезпеки у вищій освіті України, наголошують на необхідності побудови систем моніторингу, які поєднують технічні рішення із організаційними заходами – розробкою політик, навчанням персоналу та студентів, формуванням культури кібергігієни. Рекомендації щодо правового забезпечення кібербезпеки в освітній сфері акцентують увагу на створенні в університетах спеціалізованих структур або відповідальних осіб за захист персональних даних і кібербезпеку, які мають контролювати використання систем моніторингу та дотримання вимог до обробки інформації. Таким чином, вибір програмних рішень для моніторингу та аналізу

кіберзагроз в освітньому середовищі має орієнтуватися не лише на технічні характеристики, а й на здатність цих інструментів стати основою для комплексної системи управління кіберризиками, що включає правові, організаційні та освітні компоненти [33, 35].

Узагальнення критеріїв відбору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі доцільно оформити у вигляді структурованої моделі, що поєднує технічні, правові та організаційні виміри. Сучасні наукові та аналітичні праці з впровадження SIEM/SOAR-рішень наголошують, що критичними залишаються: масштабованість (здатність системи обробляти зростаючі обсяги подій у гібридній інфраструктурі), інтегрованість (наявність конекторів до широкого спектра джерел даних та інших засобів захисту), підтримка автоматизації реагування (SOAR-функціонал, інтеграція з СТІ-платформами) та відповідність вимогам регуляторів. У випадку університету це означає, що обрані рішення мають забезпечувати прийнятну продуктивність при пікових навантаженнях (наприклад, під час сесії або масових онлайн-заліків), підтримувати підключення нових сервісів без суттєвих змін архітектури та надавати можливість розширення без пропорційного зростання вартості володіння. Наукові огляди SIEM-інструментів підкреслюють, що відкриті платформи (ELK, Wazuh, Zeek, Security Onion) зазвичай краще відповідають вимогам гнучкої масштабованості, тоді як комерційні системи частіше пропонують розвинені механізми автоматизації та готові інтеграційні модулі [72].

Інтегрованість у внутрішню мережу університету передбачає здатність системи моніторингу працювати з гетерогенними джерелами подій – від серверів автентифікації та LMS до систем контролю доступу до приміщень і відеоспостереження, які дедалі частіше поєднуються з кіберкомпонентом у єдину екосистему безпеки кампусу. Дослідження інтегрованих SIEM/SOAR-підходів показують, що сучасні рішення здатні корелювати дані як з кіберсистем, так і з фізичної безпеки (журнали доступу, події з відеоаналітики), що дозволяє краще виявляти комплексні інциденти – наприклад, компрометацію облікового запису, яка супроводжується аномальною активністю фізичного доступу. Для

Житомирського державного університету це створює підґрунтя для побудови єдиного центру моніторингу, у якому дані з існуючих освітніх платформ, мережевого обладнання, серверів і, потенційно, систем контролю доступу могли б оброблятися у спільному аналітичному контурі. Відкриті інструменти (ELK, Wazuh, Zeek, MISP/OpenCTI) забезпечують необхідну гнучкість інтеграції через API та стандартні формати, тоді як комерційні SIEM/SOAR-платформи пропонують попередньо налаштовані конектори, що скорочує час впровадження за умови наявності відповідного бюджету.

З позицій стратегічного розвитку цифрового освітнього середовища обґрунтований вибір програмних рішень для моніторингу та аналізу кіберзагроз має враховувати не лише поточні потреби, а й перспективу переходу до більш зрілої моделі управління кіберризиками. Аналітичні матеріали з кібербезпеки у вищій освіті вказують, що університети, які впроваджують інтегровані SIEM/SOAR- та CTI-рішення з орієнтацією на поведінкову аналітику й автоматизацію реагування, демонструють вищу стійкість до сучасних атак, включно з цільовими фішинговими кампаніями, компрометацією облікових записів і використанням інфраструктури ЗВО в ланцюгах атак [46, 36]. Для Житомирського державного університету це означає, що обрані відкриті інструменти (ELK Stack, Wazuh, Zeek, Security Onion, MISP, OpenCTI) мають розглядатися як основа масштабованої, інтегрованої та нормативно сумісної системи моніторингу, доповненої, за потреби, цільовими комерційними рішеннями для SOAR-функціоналу або спеціалізованої аналітики. Така модель дає можливість поетапно підвищувати рівень кіберзахисту відповідно до розвитку цифрового освітнього середовища, зберігаючи баланс між вартістю, функціональністю, гнучкістю інтеграції та дотриманням вимог українського й європейського законодавства у сфері захисту інформації та персональних даних.

З огляду на результати аналізу цифрового освітнього середовища університету та сучасних досліджень у галузі кібербезпеки в освіті, логіка відбору програмних рішень для моніторингу та аналізу кіберзагроз базується на необхідності забезпечення повного циклу роботи з подіями: від збору та

нормалізації логів до кореляції, аналітики, візуалізації та автоматизованого реагування.

Порівняльний аналіз відкритих і комерційних рішень, проведений на основі рекомендацій із вибору SIEM-інструментів та кейс-досліджень у вищій освіті, дає змогу сформулювати узагальнені висновки щодо їх придатності для застосування в цифровому освітньому середовищі. Відкриті платформи забезпечують: високу гнучкість налаштування, можливість поетапного впровадження, відсутність ліцензійних витрат, сильну спільноту підтримки, а також технічні механізми реалізації вимог GDPR та українського законодавства через псевдонімізацію, маскування, гнучкі політики логування та розмежування доступу. Комерційні рішення, такі як Splunk та інші промислові SIEM/SOAR-платформи, надають розвинені засоби автоматизованого реагування, попередньо налаштовані інтеграційні модулі та підтримку галузевих шаблонів для освіти, однак вимагають суттєвих фінансових ресурсів і часто прив'язують університет до закритої екосистеми постачальника. Для університету з обмеженим бюджетом та розвинутою внутрішньою експертизою у сфері кібербезпеки це робить відкриті рішення більш привабливими як базовий вибір, із можливістю точкового додавання комерційних компонентів у міру зростання зрілості системи моніторингу.

Аргументація на користь рішень, що забезпечують збір, кореляцію, аналітику та візуалізацію подій без порушення конфіденційності, спирається на сучасні праці, присвячені GDPR-сумісній обробці журналів і правовим аспектам кібербезпеки в освіті. Дослідження демонструють, що впровадження псевдонімізації, анонімізації, селективного логування та чіткого розмежування доступу до різних рівнів деталізації логів дає змогу суттєво знизити ризики порушення приватності без втрати можливостей для виявлення та розслідування інцидентів. Відкриті SIEM-орієнтовані інструменти (Elastic Stack, Wazuh) технічно підтримують такі практики за рахунок гнучких модулів обробки даних і розширюваних схем зберігання, що дає університетам можливість будувати власні моделі захисту приватності, адаптовані до локальних політик і академічних

процесів. У поєднанні з CTI-платформами (MISP, OpenCTI), які працюють переважно з технічними індикаторами загроз, це створює стійку конфігурацію, в якій глибина видимості загроз не вимагає надмірної експозиції персональних даних.

Важливою складовою логіки відбору є також підтримка інтеграції з іншими елементами архітектури кібербезпеки університету – IDS/IPS, DLP, системами керування ідентичностями, засобами багатофакторної автентифікації та Zero Trust-моделями доступу, які були окреслені на попередніх етапах дослідження. У цьому аспекті пріоритет отримують рішення, здатні працювати як «шлюз аналітики» для всієї інфраструктури, приймаючи події з мережевого рівня, кінцевих точок, хмарних сервісів і CTI-джерел, а також передавати тригери на SOAR-платформи чи інші системи реагування.

Таким чином, обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз в освітньому середовищі Житомирського державного університету імені Івана Франка спирається на поєднання багатокритеріального технічного аналізу, вимог українського та європейського законодавства у сфері захисту персональних даних і результатів сучасних досліджень кіберзагроз у вищій освіті. Найбільш доцільним є формування гібридної архітектури, у якій відкриті інструменти (ELK Stack, Wazuh, Zeek, Security Onion, MISP, OpenCTI) виконують роль масштабованого й гнучкого ядра системи моніторингу, що забезпечує збір, кореляцію, аналітику та візуалізацію подій із дотриманням принципів конфіденційності, а комерційні рішення використовуються точково для розширення функціональності (SOAR, спеціалізована аналітика, галузеві модулі). Такий підхід дозволяє університету поступово підвищувати зрілість системи кіберзахисту, адаптуючи її до розвитку цифрового освітнього середовища, зберігаючи при цьому баланс між вартістю володіння, технологічною стійкістю, можливостями інтеграції та відповідністю вимогам GDPR, NIS2 та національного законодавства України.

Висновки до розділу 2

Результати дослідження продемонстрували, що цифрове освітнє середовище Житомирського державного університету імені Івана Франка формується як складна інтегрована екосистема, у якій поєднано навчальні, наукові, адміністративні та сервісні платформи, критичні з огляду на вимоги кіберзахисту. Встановлено, що висока ступінь взаємодії цих платформ, використання єдиних облікових записів, інтеграція з національними освітніми та управлінськими ресурсами суттєво підвищують як ефективність освітнього менеджменту, так і рівень кіберризиків, що актуалізує необхідність впровадження багаторівневої системи моніторингу подій безпеки, управління доступом та безперервного аудиту інфраструктури. Узагальнення характеристик цифрової екосистеми університету засвідчило, що наявні сервіси (E-portfolio, Experience, Enter, EducationProgram, eTraining, ZDUproject, електронний репозитарій, системи електронного документообігу тощо) вже створюють ґрунт для розгортання цілісного контуру кібермоніторингу, орієнтованого на підтримку якості освітнього процесу та захисту даних усіх учасників.

Уточнення та систематизація вимог до забезпечення кібербезпеки в освітніх установах дозволили сформулювати концептуальну рамку, яка об'єднує нормативно-правові засади, організаційні процедури, технічні механізми захисту й освітні заходи з розвитку культури кібергігієни. Було показано, що ефективна модель кіберзахисту університету має спиратися на управління ризиками, дотримання національного законодавства у сфері кібербезпеки та захисту персональних даних, гармонізацію з європейськими підходами (зокрема вимогами GDPR і NIS2), впровадження безперервного моніторингу та багаторівневої автентифікації, а також регламентацію дій персоналу й здобувачів освіти в цифровому середовищі. Аналіз засвідчив, що саме поєднання правових вимог, формалізованих внутрішніх політик і сучасних технічних засобів моніторингу створює передумови для стійкої реалізації принципів конфіденційності, цілісності та доступності освітніх даних.

Обґрунтування вибору програмних рішень для моніторингу та аналізу кіберзагроз у цифровому освітньому середовищі дало змогу визначити доцільність використання гібридної архітектури, у якій ядром виступають відкриті SIEM/XDR-орієнтовані платформи (Elastic Stack, Wazuh, Zeek, Security Onion) з інтеграцією інструментів мережевого моніторингу та кіберрозвідки (MISP, OpenCTI), а комерційні рішення розглядаються як точкове доповнення для спеціалізованих задач. Установлено, що така конфігурація дає змогу забезпечити централізований збір і кореляцію подій із критичних сервісів університету, підтримати механізми псевдонімізації й мінімізації обробки персональних даних відповідно до вимог GDPR, а також підвищити ефективність виявлення загроз через підключення до галузевих спільнот обміну індикаторами компрометації. У підсумку другий розділ підтвердив, що запропонована концепція багаторівневої системи моніторингу та аналізу кіберзагроз, адаптована до специфіки цифрової екосистеми Житомирського державного університету імені Івана Франка, є обґрунтованою, відповідає сучасним науковим і нормативним підходам та створює методологічне підґрунтя для подальшого проектування інтегрованої багаторівневої системи захисту цифрового освітнього середовища.

РОЗДІЛ 3. МОДЕЛЮВАННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ КІБЕРЗАГРОЗ В ЦИФРОВОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

3.1. Особливості інтеграції систем моніторингу в цифрове освітнє середовище

Інтеграція систем моніторингу та аналізу кіберзагроз у цифрове освітнє середовище має розглядатися як поетапний процес, що поєднує технічні, організаційні та нормативні аспекти функціонування закладу вищої освіти, а не як разова інсталяція окремого програмного продукту. У випадку університетів це означає вбудовування засобів спостереження, кореляції подій і реагування у вже наявну сервісноорієнтовану й високодинамічну інфраструктуру, яка охоплює навчальні платформи, адміністративні інформаційні системи, хмарні сервіси та широкий спектр кінцевих пристроїв. Особливістю такого середовища є поєднання академічної свободи і відкритості з жорсткими вимогами до захисту персональних даних здобувачів освіти і працівників, що зумовлює необхідність досягнення балансу між прозорістю моніторингу й дотриманням принципів приватності та мінімізації даних. Інтеграція систем моніторингу в університетську ІКТ-екосистему також повинна забезпечувати сумісність різнорідних джерел подій – журналів мережевого обладнання, систем керування навчальним контентом, систем автентифікації, електронних ресурсів бібліотеки та спеціалізованих наукових сервісів – із єдиним аналітичним контуром, здатним виконувати кореляцію та пріоритизацію інцидентів у реальному часі. У цьому контексті концепція безперервного моніторингу та життєвого циклу кібербезпеки закладу вищої освіти передбачає не лише технічне підключення джерел даних, а й формування процедур, що регламентують взаємодію підрозділів, розподіл ролей, а також оновлення політик безпеки залежно від результатів аналізу подій (Таблиця 3.1).

Ключові виміри інтеграції систем моніторингу в цифрове освітнє середовище
закладу вищої освіти

Вимір інтеграції	Основний зміст	Приклади реалізації в ЗВО
Технічна консолідація джерел подій	Уніфікований збір, нормалізація та кореляція журналів із мережевого обладнання, LMS, систем автентифікації, хмарних сервісів і наукових ресурсів для побудови єдиного аналітичного контуру моніторингу.	Використання центральної платформи SIEM/AI-SIEM із агентами/колекторами на рівні дата-центру, факультетських серверів, Wi-Fi-інфраструктури й хмарних освітніх платформ.
Архітектурна інтеграція в ІКТ-екосистему	Вбудовування засобів спостереження й реагування в багаторівневу інфраструктуру ЗВО, що поєднує локальні ресурси, хмарні сервіси, IoT-компоненти й BYOD-пристрої.	Розгортання розподілених сенсорів у кампусній мережі, лабораторіях, хмарних середовищах та інтеграція журналів провайдерів SaaS/IaaS у єдину систему моніторингу.
Інтелектуальний аналітичний контур	Використання методів машинного навчання та поведінкового аналізу для виявлення аномалій, складних багатокрокових атак і нетипових патернів взаємодії студентів та персоналу з цифровими ресурсами.	AI-орієнтовані SIEM-рішення з UEBA-модулями, які адаптивно налаштовують пороги спрацювань, зменшують кількість хибних тривог і скорочують час виявлення інцидентів у навчальних платформах.
Нормативно-правова відповідність і приватність	Упровадження принципів «privacy by design» і «data protection by default» під час проєктування моніторингу, дотримання вимог GDPR щодо обробки персональних даних здобувачів освіти та працівників.	Псевдонімізація та мінімізація даних у журналах подій, розмежування доступу до аналітичних панелей, ведення журналів доступу та проведення оцінок впливу на захист даних (DPIA) для нових сценаріїв моніторингу.
Організаційно-процесний вимір	Формування постійно діючих функцій моніторингу та реагування (SOC або спеціалізованої команди), регламентація ролей, процедур ескалації інцидентів, взаємодії з академічними та адміністративними підрозділами.	Використання гібридних моделей SOC-as-a-Service, створення студентських або змішаних SOC, розроблення та тестування планів реагування й відновлення для типових інцидентів.
Освітньо-управлінська інтеграція	Вбудовування результатів моніторингу у процеси управління ЗВО, планування освітнього процесу та розвитку культури безпеки серед учасників освітнього середовища.	Використання аналітичних звітів моніторингу для коригування політик доступу до освітніх ресурсів, оновлення регламентів використання цифрових сервісів і включення кейсів реальних інцидентів у навчальні програми.

Важливою особливістю інтеграції є необхідність урахування багаторівневої архітектури цифрового освітнього середовища, де співіснують локальні ресурси університету, хмарні сервіси постачальників освітніх платформ, віддалені дослідницькі ресурси та власні розробки закладу. Для забезпечення цілісного моніторингу в такій архітектурі доцільно використовувати підхід, який поєднує центральну платформу типу SIEM/AI-SIEM з розподіленими сенсорами на рівні мережевої інфраструктури, серверів додатків і кінцевих пристроїв, що дає змогу формувати єдине «поле спостереження» за подіями безпеки. При цьому інтеграція повинна враховувати специфіку навчальних процесів: пікові навантаження під час сесії і масового доступу до LMS, використання BYOD-пристроїв, підключення IoT-компонентів у лабораторіях і кампусній інфраструктурі, а також наявність «тіньових» IT-сервісів, які можуть бути джерелом додаткових ризиків. З огляду на це, сучасні підходи до розбудови систем моніторингу в закладах вищої освіти ґрунтуються на принципах нульової довіри, розширеній аутентифікації користувачів та пристроїв, а також на інтеграції засобів поведінкового аналізу, здатних виявляти аномалії у взаємодії студентів і персоналу з цифровими ресурсами. Успішність інтеграції визначається не лише кількістю підключених джерел подій, а насамперед якістю отриманих аналітичних висновків і здатністю університету оперативно адаптувати освітні та адміністративні процеси відповідно до виявлених кіберзагроз [69].

Успішна інтеграція систем моніторингу у цифрове освітнє середовище безпосередньо залежить від здатності забезпечити стандартизований збір, нормалізацію та кореляцію подій безпеки з різнорідних джерел, притаманних інфраструктурі закладу вищої освіти. Університетські мережі, як правило, поєднують центральні дата-центри, факультетські сервери, лабораторні сегменти, бездротову інфраструктуру кампусу, хмарні платформи та спеціалізовані освітні й наукові сервіси, що зумовлює високу неоднорідність форматів журналів та протоколів взаємодії. Для усунення розрізненості джерел подій застосовуються механізми єдиного логування та використання агентів або

колекторів, які трансформують події до уніфікованої моделі (наприклад, за допомогою формалізованих схем полів подій), що дозволяє системі моніторингу виконувати ефективну кореляцію та виявляти складні багатокрокові атаки. При цьому особливе значення має інтеграція з системами керування ідентифікацією та доступом, сервісами федеративної автентифікації та навчальними платформами, оскільки саме ці компоненти містять контекст поведінки користувачів, ролей, навчальних курсів і ресурсів, необхідний для коректної інтерпретації інцидентів. Сучасні дослідження підкреслюють, що системи класу AI-SIEM для закладів вищої освіти є найбільш результативними саме за умов глибокої інтеграції в освітні сервіси та врахування освітньої специфіки трафіку, патернів відвідування курсів і взаємодії студентів з цифровими ресурсами [78].

Окремий блок завдань інтеграції пов'язаний із забезпеченням відповідності вимогам захисту персональних даних та регуляторним нормам, насамперед європейському законодавству у сфері приватності, яке поширюється на університетські інформаційні системи. Особливість моніторингу у цифровому освітньому середовищі полягає в тому, що значна частина контрольованих подій містить персональні ідентифікатори здобувачів освіти, дані про успішність, траєкторії навчання, комунікації в освітніх платформах та інші чутливі атрибути, що вимагає впровадження підходів «privacy by design» і «data protection by default» уже на етапі проєктування систем моніторингу. У практиці університетів це означає реалізацію механізмів псевдонімізації та мінімізації даних, жорсткого розмежування доступу до аналітичних панелей, ведення журналів доступу до даних моніторингу, а також проведення регулярних оцінок впливу на захист даних для нових сценаріїв використання систем спостереження. Дослідження у сфері автоматизованого забезпечення відповідності стандартним контролям безпеки показують, що поєднання засобів моніторингу з моделями відповідності дозволяє університетам автоматизувати перевірку дотримання вимог нормативних актів і формувати доказову базу для внутрішнього та зовнішнього аудиту [54]. Таким чином, інтеграція систем моніторингу в освітнє середовище неможлива без одночасної побудови цілісної моделі управління даними та

приватністю, що враховує як технічні, так і організаційні обмеження закладу вищої освіти.

Подальший розвиток систем моніторингу в цифровому освітньому середовищі зумовлює інтеграцію традиційних засобів збору журналів і кореляції подій із інтелектуальними компонентами, що використовують методи машинного навчання та штучного інтелекту для виявлення аномалій і складних кіберзагроз. Такі рішення дають змогу адаптувати порогові значення, моделі поведінки користувачів та сценарії реагування до реальної динаміки навчальних процесів, зменшуючи кількість хибних спрацювань і підвищуючи чутливість до нетипових дій у навчальних платформах, хмарних ресурсах і дослідницькій інфраструктурі університету. Особливого значення набуває можливість поєднання розширеного моніторингу мережевого трафіку, журналів аутентифікації та діяльності в LMS із контекстуальною інформацією про навчальні курси, графік освітнього процесу і цифрові сліди академічної активності, що дозволяє відрізнити легітимні пікові навантаження (наприклад, у період сесії) від потенційних DDoS-атак або спроб масового підбору облікових даних. Дослідження у сфері застосування AI-орієнтованих платформ у закладах вищої освіти показують, що інтегровані моделі, які одночасно аналізують події безпеки, поведінкові патерни та контент взаємодії користувачів, дають змогу істотно скоротити середній час виявлення і реагування на інциденти, а також підвищують стійкість цифрового освітнього середовища до нових, раніше невідомих типів атак [78]. У цьому контексті важливо закладати у проєкт інтеграції можливість подальшого розширення інтелектуальних модулів, використання відкритих форматів обміну даними та узгодження алгоритмів із етичними вимогами до застосування штучного інтелекту в освіті, зокрема щодо прозорості рішень та недискримінаційності моделей.

Не менш важливим виміром інтеграції є організаційно-процесний аспект, пов'язаний з розгортанням у закладі вищої освіти функцій центру операцій безпеки або принаймні спеціалізованої команди, що відповідає за моніторинг, аналіз і реагування на інциденти. Для університетів характерні обмежені ресурси

та необхідність поєднання навчальної, наукової й адміністративної діяльності, тому на практиці часто застосовуються гібридні моделі, у яких власна команда моніторингу взаємодіє з галузевими центрами обміну інформацією про кіберзагрози та використовує зовнішні сервіси підтримки SOC для складних розслідувань. Досвід провідних університетів демонструє ефективність студентських або змішаних (student-run) SOC, де під керівництвом фахівців здобувачі освіти залучаються до процесів моніторингу, кореляції подій і моделювання інцидентів, що одночасно підвищує захищеність інфраструктури й формує практичні компетентності майбутніх фахівців з кібербезпеки. Для інтегрованих систем моніторингу важливо формалізувати процедури ескалації інцидентів, розробити плани реагування і відновлення для типових сценаріїв, забезпечити регулярне тестування процесів і навчання персоналу, а також налагодити взаємодію з адміністративними, навчальними й ІТ-підрозділами університету на основі узгоджених політик і регламентів.

Отже, інтеграція систем моніторингу в цифрове освітнє середовище має розглядатися як багатокomпонентний процес, що поєднує технологічну консолідацію джерел подій, побудову інтелектуального аналітичного контуру, дотримання вимог захисту персональних даних і регуляторних норм, а також створення сталих організаційних механізмів управління кібербезпекою університету. Її результативність визначається не лише впровадженими програмно-апаратними засобами, а насамперед здатністю закладу вищої освіти інтегрувати моніторинг у власні освітні та управлінські процеси, забезпечити підтримку з боку керівництва, розвивати культуру безпеки серед учасників освітнього процесу й системно використовувати отримані аналітичні дані для підвищення стійкості цифрового середовища до кіберзагроз.

3.2. Моделювання багаторівневої системи захисту цифрового освітнього середовища

Моделювання багаторівневої системи захисту цифрового освітнього середовища Житомирського державного університету імені Івана Франка

доцільно здійснювати на основі концепції «багаторівневого захисту» (defense-in-depth), яка передбачає послідовне нашарування організаційних, технічних та освітніх заходів, інтегрованих у єдину архітектуру моніторингу та реагування на інциденти кібербезпеки (Рис. 3.1). Такий підхід узгоджується з принципами NIST Cybersecurity Framework, де функції ідентифікації, захисту, виявлення, реагування та відновлення розглядаються як взаємопов'язані елементи життєвого циклу управління кіберризиками, що особливо актуально для університетів із розгалуженою цифровою інфраструктурою та значним обсягом персональних даних здобувачів освіти та працівників. В умовах Житомирського державного університету, де цифрове освітнє середовище поєднує навчальні платформи, корпоративні сервіси, наукові ресурси, сервіси електронного документообігу та спеціалізовані інформаційні системи, багаторівнева система захисту має бути спроектована як інтегрована модель, що поєднує рівень ідентифікації та автентифікації користувачів, рівень моніторингу, рівень аналітики й реагування та рівень формування культури цифрової безпеки.

Перший рівень проєктної моделі – рівень ідентифікації та автентифікації користувачів – забезпечує базову ланку контролю доступу до ресурсів цифрового освітнього середовища та слугує точкою входу до всієї системи defense-in-depth. У контексті університету доцільно будувати цей рівень на принципах єдиного простору ідентичності (Identity and Access Management, IAM), де всі ролі (студенти, науково-педагогічні працівники, адміністрація, технічний персонал, зовнішні користувачі) формалізуються через політики доступу, прив'язуються до реєстру користувачів і синхронізуються з каталогами автентифікації (наприклад, на основі протоколів SAML або OAuth 2.0/OpenID Connect). Використання багатофакторної автентифікації, контекстних атрибутів доступу (місце, час, тип пристрою) та принципу мінімально необхідних привілеїв корелює з підходами NIST до управління ідентичністю та доступом, а також з рекомендаціями щодо побудови Zero Trust-архітектур, у яких довіра не ґрунтується виключно на розташуванні користувача у внутрішній мережі [58].

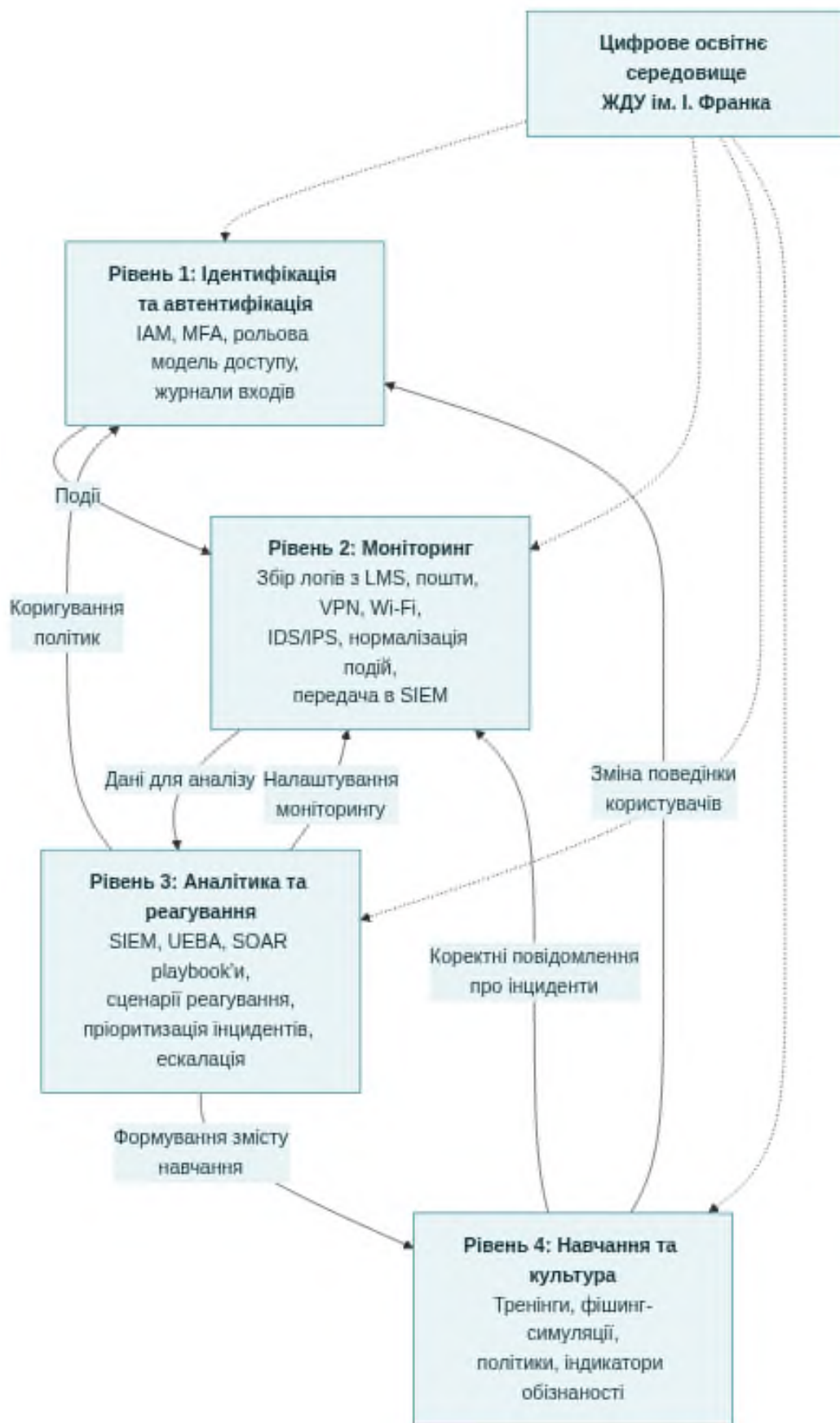


Рисунок 3.1 – Багаторівнева система захисту цифрового освітнього середовища університету

Саме на цьому рівні формується якісна подієва база: всі події автентифікації, спроби входу, зміни ролей та прав доступу мають журналюватися та передаватися на рівень моніторингу й аналітики, що створює основу для подальшого виявлення аномальної активності.

Другий рівень – рівень моніторингу – відповідає за централізований збір, агрегування та кореляцію журналів безпеки, мережевого трафіку та подій доступу з основних компонентів цифрового освітнього середовища університету. У світлі стандарту ISO/IEC 27035, який визначає життєвий цикл управління інцидентами (підготовка, виявлення і звітування, оцінка й реагування, аналіз після інциденту й покращення), моніторинг виступає ключовим механізмом реалізації фаз виявлення і первинної реєстрації інцидентів [49]. Для університетського середовища доцільно побудувати архітектуру моніторингу на основі SIEM-платформи та мережевих сенсорів, які збирають журнали з навчальних платформ, систем електронної пошти, VPN-шлюзів, міжмережевих екранів, систем віртуалізації, Wi-Fi-інфраструктури, а також з хмарних сервісів, що використовуються в освітньому процесі. Приклади впровадження подібних рішень в університетах ЄС свідчать, що комплексний моніторинг трафіку й логів дозволяє суттєво підвищити швидкість виявлення загроз, таких як несанкціонований доступ до облікових записів, спроби масового зламування паролів або нетипове використання привілейованих акаунтів. Критично важливим є проектування схеми нормалізації логів та їх маркування відповідно до таксономій NIST чи MITRE ATT&CK, що спрощує подальшу побудову кореляційних правил і сценаріїв реагування [58].

Третій рівень проєктної моделі – рівень аналітики та реагування – покликаний перетворити масиви подієвих даних, що надходять із рівня моніторингу, на структуровані інциденти, які обробляються в межах єдиного процесу управління інцидентами відповідно до ISO/IEC 27035. У межах цифрового освітнього середовища університету доцільно формувати центр моніторингу й реагування (умовний SOC рівня закладу вищої освіти), де

SIEM-платформа акумулює журнали безпеки, а SOAR-компоненти реалізують оркестрацію та часткову автоматизацію реагування: блокування підозрілої сесії, примусову зміну пароля, тимчасове відключення компрометованого облікового запису, ізоляцію робочої станції з підозрою на зараження. Такий підхід узгоджується з NIST Cybersecurity Framework, який розглядає виявлення, реагування та відновлення як безперервний цикл, а також передбачає документування сценаріїв реагування, які можна стандартизувати у вигляді «playbook» для типових інцидентів, характерних для університетів (компрометація облікового запису LMS, витік даних студентського е-портфолію, шифрування серверів резервних копій). Для Житомирського державного університету важливо, щоб на цьому рівні було забезпечено формалізований процес пріоритизації інцидентів, з урахуванням впливу на безперервність навчального процесу, конфіденційність персональних даних та відповідність вимогам GDPR і національного законодавства у сфері захисту інформації, що відповідає підходам, описаним у сучасних дослідженнях із застосуванням NIST CSF у секторі освіти.

У межах рівня аналітики особливого значення набуває використання ризик-орієнтованих метрик та індикаторів ефективності (KPI/KRI), які дозволяють оцінювати результативність заходів моніторингу й реагування не лише за фактом інцидентів, а й з погляду динаміки зменшення часу виявлення (MTTD) та часу реагування (MTTR). Практика університетів Європейського Союзу свідчить, що інтеграція SIEM/SOAR-рішень із системами керування вразливостями, каталогами користувачів, сервіс-деском та репозитаріями знань дає змогу створити замкнений цикл «виявлення – аналіз – реагування – навчання», у якому результати розбору інцидентів використовуються для коригування політик доступу, оновлення сигнатур, моделей аномалій та сценаріїв навчання персоналу. Для Житомирського державного університету це означає доцільність побудови такої архітектури, у якій SIEM-платформа, використана на рівні моніторингу, доповнюється модулями поведінкової аналітики користувачів (UEBA) та автоматизованими процедурами ескалації

інцидентів до відповідальних структурних підрозділів, що відповідає рекомендаціям NIST щодо адаптивного управління кіберризиками в децентралізованому академічному середовищі.

Четвертий рівень – рівень навчання персоналу та формування культури цифрової безпеки – є критичним для стійкості всієї багаторівневої системи, оскільки більшість інцидентів у сфері освіти пов'язані з людським фактором: фішинговими атаками, помилковими налаштуваннями, неналежним поводженням із носіями інформації. Європейські дослідження та рекомендації ENISA наголошують, що побудова сталої культури кібербезпеки в освітніх закладах має ґрунтуватися на системних програмах підвищення обізнаності, інтеграції елементів цифрової безпеки в навчальні плани, регулярних тренінгах, симуляціях фішингових атак та інформаційних кампаніях, синхронізованих із Європейським місяцем кібербезпеки. Для Житомирського державного університету це передбачає розроблення багаторівневої програми навчання, диференційованої за цільовими групами: базові курси цифрової гігієни для студентів, спеціалізовані тренінги з безпечної роботи з персональними даними та хмарними сервісами для науково-педагогічних працівників, розширені програми для ІТ-персоналу та адміністраторів освітніх платформ, а також проведення регулярних міжкафедральних семінарів і навчань з моделювання інцидентів за сценаріями, що відповідають ISO/IEC 27035. Результати таких програм мають оцінюватися за допомогою кількісних і якісних показників (рівень участі, результати тестування, частота кліків на фішингові посилання, кількість самостійно ініційованих повідомлень про підозрілу активність), що дозволяє інтегрувати їх у систему управління ризиками кібербезпеки університету.

Взаємозв'язок між описаними рівнями багаторівневої системи захисту цифрового освітнього середовища університету проявляється в тому, що кожен наступний рівень не лише спирається на попередній, а й генерує дані та знання для його вдосконалення, формуючи замкнений контур безперервного покращення, характерний для сучасних кібербезпекових фреймворків. Рівень

ідентифікації та автентифікації створює структуровану подієву базу щодо поведінки користувачів, яка через рівень моніторингу потрапляє до SIEM-системи, де на рівні аналітики та реагування формується розширений контекст інцидентів, а результати розбору інцидентів і тренди атак використовуються для коригування політик доступу та налаштувань моніторингу. Водночас рівень навчання персоналу та культури цифрової безпеки, спираючись на дані про інциденти й уразливі поведінкові патерни, забезпечує цілеспрямоване підвищення обізнаності та компетентності користувачів, що зменшує ймовірність успішних атак та підвищує якість початкового повідомлення про інциденти, що прямо відповідає рекомендаціям ISO/IEC 27035 щодо інтеграції навчання й обізнаності в процес управління інцидентами. Для Житомирського державного університету впровадження такої цілісної багаторівневої системи на основі принципів defense-in-depth, NIST Cybersecurity Framework та стандарту ISO/IEC 27035 створює передумови для суттєвого підвищення рівня захищеності цифрового освітнього середовища, скорочення часу виявлення й реагування на інциденти, а також формування сталої культури кібербезпеки серед усіх учасників освітнього процесу, що є критично важливим в умовах зростання інтенсивності та складності кіберзагроз.

3.3. Аналіз отриманих результатів та пропозиції для подальших досліджень

Відповідно до проєктної моделі, представленої у п.3.2 (рис. 3.1.) на першому рівні потрібно передбачити рівень ідентифікації та автентифікації користувачів.

Усі навчальні, організацій та наукові сервіси університету мають авторизований вхід відповідно до встановлених ролей. Водночас цей рівень не вибудовано на принципах єдиного простору ідентичності (Identity and Access Management, IAM). Доступ до внутрішнього порталу університету можливий тільки в внутрішньої мережі університету. Також в більшості з них не передбачено використання багатофакторної автентифікації. Водночас усі

співробітники та здобувачі університету, які мають корпоративні пошти мають змогу налаштувати багатофакторну автентифікацію, що дасть можливість знизити ризик несанкціонованого доступу до облікового запису.

Сервіс eportfolio передбачає ведення журналу обліку змін, дані з якого передаються на рівень моніторингу й аналітики, що створює основу для подальшого виявлення аномальної активності.

В Житомирському державному університеті імені Івана Франка призначено відповідальних за створення та адміністрування облікових записів користувачів. Відповідальним за корпоративні пошти є системний адміністратор, відповідальними за облікові записи здобувачів у системі Деканат є заступники деканів факультетів/інститутів та секретарі деканатів (відповідальні за роботу з персональними даними), начальник навчального відділу (відповідальний з реагування на інциденти).

Мережева інфраструктура університету побудована з урахуванням принципу сегментації. Окремі логічні сегменти мережі виділено для: адміністративних систем; освітніх платформ (портал ZDUproject, електронні журнали); серверної інфраструктури та баз даних; студентського доступу; гостьових і публічних мереж (або сервісів із різними типами доступу). Наприклад сервіс eportfolio.zu.edu.ua має гостьовий доступ (без авторизації), який передбачає видимість тільки загальної інформації про науково-педагогічних працівників, їхню освіту, професійних розвиток, наявність пунктів профактивності, публікаційна активність тощо (Додаток А). Водночас особиста інформація про дату народження, номер телефону тощо, залишається видимою тільки для адміністративного персоналу (відділ кадрів, декан тощо).

Аналогічна ситуація з вкладкою «Освітні програми». Публічна сторінка дає доступ лише до сканованих pdf документів (Додаток А), а авторизований доступ для користувачів дає можливість підвантажувати необхідні складові НМК, а гаранту освітньої програми, завідувачу кафедри – перевіряти наявність завантажених складових ОК (Додаток Б).

Для авторизованих користувачів вхід у сервіси experience, eTraning, ZDUProject, Enter, Educational Program тощо (рис. 3.2.).

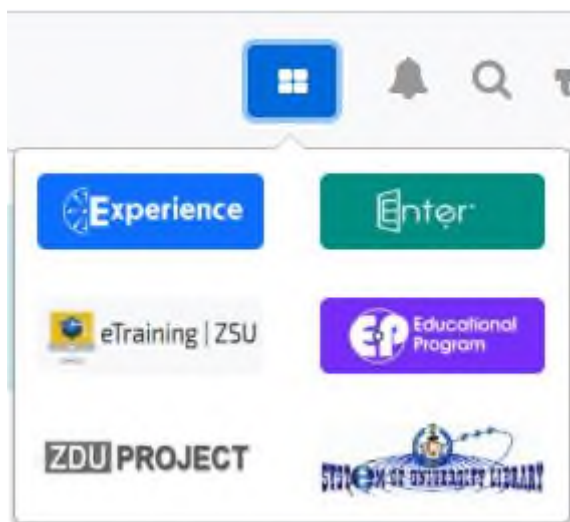


Рисунок 3.2. – Інтеграція сервісів університету у eportfolio

Відповідно у вказаних сервісах теж кожний користувач має доступ лише до ресурсів, які визначено його роллю. У додатку В наведено приклад доступу до сервісу Educational Program неавторизованим користувачам. Для гаранта його функціонал передбачає конструювання проекту та освітньої програми, для науково-педагогічного працівника – робота виключно з освітніми компонентами, що визначено відповідними ролями (Додаток Г). Гаранти освітніх програм мають декілька функціоналів: і як гарант, і як науково-педагогічні працівники.

Між сегментами встановлено міжмережеві екрани (firewalls) з обмежувальними правилами доступу. Для виявлення потенційних атак і аномальної активності застосовуються системи IDS/IPS, які дозволяють оперативно реагувати на інциденти безпеки.

Віддалений доступ до внутрішніх ресурсів реалізується виключно через захищені канали (VPN) з контролем автентифікації та журналюванням дій користувачів.

Реалізовано систему регулярного (1 раз на тиждень) резервного копіювання, що забезпечує збереження даних у разі технічних збоїв, кібератак

або людських помилок. Резервні копії зберігаються у захищених сховищах із контрольованим доступом, а процедури відновлення періодично тестуються.

Для здобувачів освіти та працівників університету реалізуються регулярні заходи з підвищення обізнаності у сфері інформаційної безпеки. Вони включають: інструктажі з безпечної роботи в цифровому освітньому середовищі; ознайомлення з правилами створення та зберігання паролів; роз'яснення ризиків фішингу, соціальної інженерії та витоку даних; рекомендації щодо безпечного використання особистих пристроїв (BYOD).

Навчальні матеріали інтегруються в освітній процес і доводяться до відома користувачів через внутрішні портали та офіційні канали комунікації.

З метою забезпечення реалізації другого та третього рівнів системи захисту цифрового освітнього середовища університету є потреба у створенні єдиної оболонки, яка реалізовує санкціонований авторизований доступ до усіх інформаційних сервісів університету та їх інтеграцію у єдиний цифровий простір.

З метою покращення рівня системи моніторингу та аналізу кіберзагроз в цифровому освітньому середовищі сформулюємо рекомендації:

1. Впровадити єдину систему управління ідентифікацією та доступом (IAM) з рольовою моделлю (RBAC). Слід забезпечити автоматизований перегляд прав доступу, блокування неактивних облікових записів і своєчасне відкликання доступів у разі зміни ролі або звільнення працівників.

2. Забезпечити обов'язкове використання багатофакторної автентифікації (MFA) для облікових записів викладачів, адміністративного та технічного персоналу, а також для доступу до елементів цифрового середовища.

3. Впровадити централізоване журналювання подій і моніторинг безпеки (SIEM або його аналоги). Рекомендується розробити та затвердити процедури реагування на інциденти з чітким визначенням ролей, каналів оповіщення та алгоритмів дій у кризових ситуаціях.

4. Систематично проводити внутрішні аудити інформаційної безпеки, періодичні penetration-тести та перевірки відповідності політик і технічних

засобів актуальним загрозам. Це дозволяє своєчасно виявляти вразливості та коригувати заходи захисту.

5. Впроваджувати нейронні мережі у систему кібермоніторингу. Вони можуть застосовуватися для аномального аналізу поведінки користувачів і систем. Навчена модель формує уявлення про «нормальну» поведінку (типові входи в систему, часові шаблони доступу, обсяг трафіку) і виявляє відхилення, що можуть свідчити про кібератаки або компрометацію облікових записів. Для цього доцільно використовувати: автоенкодера; рекурентні нейронні мережі (RNN); моделі на основі LSTM/GRU. Нейронні мережі ефективні для класифікації мережевого трафіку та виявлення шкідливої активності. Моделі здатні аналізувати пакети даних, потоки та статистичні характеристики трафіку для визначення: DDoS-атак; сканування мережі; несанкціонованих підключень; прихованих каналів передачі даних. Для цих завдань можуть застосовуватися згорткові нейронні мережі (CNN) та гібридні моделі. Інтеграція нейронних мереж із системами реагування (SOAR) дозволяє: автоматично визначати рівень критичності інциденту; пропонувати оптимальні сценарії реагування; зменшувати час між виявленням і нейтралізацією загрози. У перспективі можливе частково автономне реагування на типові інциденти з низьким рівнем ризику.

Узагальнюючи вище зазначені рекомендації, варто зазначити, що впровадження нейронних мереж у систему моніторингу та аналізу кіберзагроз є перспективним напрямом розвитку кібербезпеки цифрового освітнього середовища. Поєднання класичних методів SIEM із нейромережевими підходами дозволяє створити адаптивну, інтелектуальну систему захисту, здатну ефективно протидіяти сучасним і майбутнім кіберзагрозам.

Висновки до розділу 3

Результати дослідження засвідчили, що запропонована модель інтеграції системи моніторингу та аналізу кіберзагроз у цифрове освітнє середовище університету є логічним продовженням концепції багаторівневого захисту,

сформованої з урахуванням NIST Cybersecurity Framework та стандартів управління інцидентами ISO/IEC 27035. Сформовано цілісну архітектуру, у якій рівні ідентифікації та автентифікації, моніторингу, аналітики й реагування, а також формування культури цифрової безпеки функціонують як взаємопов'язані підсистеми єдиного контуру управління кіберризиками, адаптованого до специфіки університетського середовища. У межах цієї архітектури доведено, що саме інтеграція централізованого журналювання, SIEM/AI-SIEM-рішень, SOAR-компонентів та поведінкової аналітики користувачів створює підґрунтя для оперативного виявлення аномалій, скорочення часу виявлення та реагування на інциденти, а також для підтримки вимог щодо захисту персональних даних відповідно до європейських регуляторних підходів.

Здійснене моделювання багаторівневої системи захисту для Житомирського державного університету імені Івана Франка продемонструвало, що поєднання технічних засобів моніторингу з організаційними механізмами (визначення ролей, процедур ескалації, регламентів взаємодії підрозділів) та освітніми заходами з формування культури кібербезпеки дає змогу перетворити цифрове освітнє середовище із пасивного об'єкта захисту на керовану, ризик-орієнтовану систему. Виявлено, що практична реалізація запропонованої моделі в університеті потребує подальшого посилення компонентів управління ідентичністю (IAM), розширення застосування багатофакторної автентифікації, розгортання повнофункціональної платформи централізованого моніторингу подій безпеки та впровадження механізмів автоматизованого реагування, зокрема на основі нейромережових методів аналізу аномалій. Отримані результати створюють методологічне підґрунтя для подальших досліджень, спрямованих на розроблення формальних моделей оцінювання ефективності багаторівневих систем захисту в закладах вищої освіти, інтеграцію показників стійкості цифрового освітнього середовища до кіберзагроз у системи внутрішнього забезпечення якості освіти та поглиблене вивчення впливу програм підвищення обізнаності на зниження кіберризиків у академічному секторі.

ВИСНОВКИ

Узагальнення результатів проведеного дослідження дає підстави стверджувати, що поставлена мета – обґрунтування, проєктування та моделювання системи моніторингу й аналізу кіберзагроз у цифровому освітньому середовищі закладу вищої освіти – досягнута, а всі сформульовані завдання отримали логічне теоретичне та прикладне вирішення. Сформовано цілісне науково-методичне підґрунтя для впровадження багаторівневої системи кіберзахисту університету, орієнтованої на сучасні стандарти, нормативні вимоги та практичні потреби цифрового університету.

Аналіз існуючих методів забезпечення кібербезпеки освітнього середовища показав, що інформаційна інфраструктура закладів вищої освіти є складною, розподіленою та високозалежною від мережевих, хмарних і платформних сервісів, що зумовлює широкий спектр потенційних кіберзагроз. Виявлено, що поширені підходи до захисту (класичні мережеві фаєрволи, антивірусні рішення, епізодичний аудит безпеки) є недостатніми в умовах зростання кількості та складності атак, активного використання соціальної інженерії, IoT-пристроїв та віддаленого доступу, а також залишають низку критичних уразливостей через фрагментарність контролю, відсутність централізованого моніторингу й несистемний характер оновлення політик безпеки.

Оцінка сучасних технологій моніторингу кіберзагроз та моделювання інцидентів засвідчила, що найбільш перспективними є інтегровані рішення, які поєднують можливості IDS/IPS, SIEM/SOAR-платформ, DLP-систем, ML/AI-аналізу аномалій, honeypot- і sandbox-технологій та платформ обміну інформацією про загрози. Доведено, що комплексне застосування цих технологій у межах освітнього середовища забезпечує підвищення точності виявлення атак, скорочення часу реагування, прозорість подій безпеки в різних сегментах інфраструктури та підтримку циклу інцидент-менеджменту відповідно до вимог стандартів ISO/IEC 27001, ISO/IEC 27035 та NIST CSF.

Формулювання вимог до безпечної інфраструктури закладу вищої освіти та обґрунтування критеріїв ефективності захисту дозволило виокремити ключові

функціональні та нефункціональні характеристики системи моніторингу й аналізу кіберзагроз. Визначено, що система має забезпечувати повноту та безперервність збору подій, підтримку багатоджерельного аналізу, можливість автоматизованого реагування, масштабованість, відмовостійкість, сумісність із чинною інфраструктурою, а також відповідність вимогам законодавства щодо захисту персональних даних та інформації з обмеженим доступом. Запропоновано критерії ефективності, що охоплюють показники скорочення часу виявлення та реагування на інциденти, зменшення кількості успішних атак, рівень покриття критичних активів моніторингом та ступінь інтеграції технічних і організаційних заходів безпеки.

Розробка теоретичних основ і практичних рекомендацій щодо проектування та інтеграції систем моніторингу й аналізу кіберзагроз у цифрове освітнє середовище завершилася побудовою багаторівневої моделі захисту, орієнтованої на специфіку університетської інфраструктури. У межах моделі структуровано рівні ідентифікації та автентифікації, технічного моніторингу, аналітики й оркестрації реагування, а також рівень організаційно-процедурних заходів і формування культури кібербезпеки, що забезпечує замкнений цикл «виявлення – аналіз – реагування – удосконалення». Сформульовано практичні рекомендації щодо поетапного впровадження системи, вибору програмно-апаратних рішень, інтеграції з існуючими сервісами університету, побудови регламентів роботи підрозділів та організації навчання користувачів основам цифрової безпеки.

Узагальнюючи результати дослідження, можна стверджувати, що запропонований підхід до моніторингу та аналізу кіберзагроз у цифровому освітньому середовищі формує надійну методичну й технологічну основу для підвищення кіберстійкості закладів вищої освіти та забезпечення безперервності освітніх процесів в умовах зростання кіберзагроз. Розроблена модель та практичні рекомендації можуть бути використані для модернізації систем управління інформаційною безпекою університетів, адаптації внутрішніх політик до сучасних стандартів та розробки подальших наукових і прикладних проєктів у сфері кібербезпеки освітнього сектору.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Асірян С. Р., Алексанян К. А. GDPR як стандарт захисту персональних даних в Європейському Союзі. *Право і суспільство*. 2021. № 6. С. 298-302. DOI: <https://doi.org/10.32842/2078-3736/2021.6.43>
2. Воронкова В. Г., Метеленко Н. Г., Ажажа М. А., Арабаджієв Д. Ю., Нікітенко В. О., Дашков А. О., Венгер О. М., Фурсін О. О., Шарапова Т. А., Цикін Д. С. Інтеграція цифрових технологій у систему безпеки: адаптація до нових викликів і можливостей. *Цифрова трансформація промислового менеджменту у контексті викликів, можливостей та змін* : монографія / за ред. Воронкової В. Г.О., Метеленко Н. Г. Львів – Торунь : Liha-Pres, 2024. С. 432-562. DOI: <https://doi.org/10.36059/978-966-397-413-2-9>
3. Гайович Є. Ф., Тополянський С. І. Кібербезпека в системі сучасної вищої освіти: реалії та перспективи подальшого розвитку. *Науковий вісник Ужгородського університету. Серія : Педагогіка. Соціальна робота*. 2025. Вип. 1 (56). С. 45-50. DOI: <https://doi.org/10.24144/2524-0609.2025.56.45-50>
4. Дей Г. А. Кібербезпека в українських закладах освіти: основні проблеми та шляхи розв'язання. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2025. № 2. С. 35-43. DOI: <https://doi.org/10.32782/tnv-pub.2025.2.5>
5. Електронна бібліотека Житомирського державного університету імені Івана Франка. URL: <https://eprints.zu.edu.ua/>
6. Житомирський державний університет імені Івана Франка. Стратегія цифрової трансформації Житомирського державного університету імені Івана Франка. Житомир, 2023. URL: <https://zu.edu.ua/offic/dig-strategies-2028.pdf>.
7. Інформаційно-аналітичний огляд ЗМІ з питань цифровізації та цифрової трансформації сфери освіти. Частина 2, 2025 [Електронний ресурс] / уклад. Т. Годецька ; ДНПБ України ім. В. О. Сухомлинського. Київ, 2025. 7 с. URL: https://dnpb.gov.ua/wp-content/uploads/2025/10/Monitoring_ZMI_2025_vol_02.pdf

8. Каулька О., Пономарьова Л. Забезпечення кібербезпеки в освітніх установах: обізнаність, правила, стратегія. *Фахова передвища освіта*. 2025. URL: <https://osvitafp.com.ua/2025/02/07/zabezpechennia-kiberbezpeky-v-osvitnikh-ustanovakh-obiznanist-pravyla-stratehiia/>
9. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. № 10 320 с.
10. Колеснік Н.В., Мандрикевич Б. М., Нікульченко В. В. Організація безпечного освітнього середовища в умовах воєнного стану. *Інноваційна педагогіка*. 2025. Випуск 80, Том 1. С. 125-129. DOI: <https://doi.org/10.32782/2663-6085/2025/80.1.25>
11. Корзаченко О. В., Поліщук Є. А. Методологічні засади щодо вибору ідс/іпс для організації. *Моделювання та інформаційні системи в економіці*. 2019. № 98. С. 135-146. DOI: <http://doi.org/10.33111/mise.98.14>
12. Мужанова Т.М., Легомінова С. В., Якименко Ю. М., Мордас І. В. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. *Кібербезпека: освіта, наука, техніка*. 2021. Том 1, № 13. С. 50–62. DOI: <https://doi.org/10.28925/2663-4023.2021.13.5062>
13. Назаркевич М., Висоцька В., Юринець Р., Наконечний Н. Методи реалізації виявлення дезінформації у соціальних мережах на основі штучного інтелекту. *Кібербезпека: освіта, наука, техніка*. 2025. № 2 (30). С. 209–223. DOI: <https://doi.org/10.28925/2663-4023.2025.30.965>
14. Оболонська Я. О., Віщук І. В. Сучасні технології моніторингу та реагування на кіберзагрози. // Матеріали LIV Всеукраїнської науково-технічної конференції підрозділів ВНТУ, Вінниця, 24-27 березня 2025 р. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/49601/23369.pdf?sequence=3&isAllowed=y>

15. Полотай О. І., Пузир А. О. Аналіз засобів запобігання витоку конфіденційної інформації на підприємствах, на прикладі системи DLP. *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. Том 30. С. 134-144. DOI: <https://doi.org/https://doi.org/10.32447/20784643.30.2024.13>
16. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.09.2019 р. № 518. URL: <https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text>
17. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
18. Про захист персональних даних: Закон України від 01.07.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
20. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#n12>
21. Реформування системи підготовки професійних кадрів у сфері кібербезпеки в Україні: затверджені перші шість професійних стандартів. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://cip.gov.ua/ua/news/reformuvannya-sistemi-pidgotovki-profesiinikh-kadriv-u-sferi-kiberbezpeki-v-ukrayini-zatverdzheni-pershi-shist-profesiinikh-standartiv>
22. Річний аналітичний огляд: жовтень 2023 – вересень 2024 [Електронний ресурс] / Національний координаційний центр кібербезпеки при РНБО України. Київ, 2025. 64 с. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf

23. Савчук С. О. Державна політика протидії кіберзлочинності : дис.... канд. наук з дерд. управ. : 25.00.05 / Державний університет «Житомирська політехніка». Житомир, 2024. 177 с.
24. Смірнова Т., Константинова Л., Коноплицька-Слободенюк О., Козлов Я., Кравчук О., Козірова Н., Смірнов О. Дослідження сучасного стану SIEM-систем. *Кібербезпека: освіта, наука, техніка*. 2024. № 1 (25). С. 6-18. DOI: <https://doi.org/10.28925/2663-4023.2024.25.618>
25. Соколов В., Складанний П. Порівняльний аналіз стратегій побудови другого та третього рівня освітніх програм зі спеціальності 125 «Кібербезпека». *Кібербезпека: освіта, наука, техніка*. 2023. Том 4, № 20. С. 183–204. DOI: <https://doi.org/10.28925/2663-4023.2023.20.183204>
26. Стратегія освітнього кластера в Україні 2023–2025 [Електронний ресурс] / ЮНІСЕФ, Save the Children, Міністерство освіти і науки України, Український освітній кластер. Київ, 2023. 72 с. URL: https://whocares-pss.info/wp-content/uploads/2025/01/Education-Cluster-and-UNICEF-2023-Ukraine-Education-Cluster-Strategy-2023-2025_in-ukr.pdf
27. Трофименко О. Г. Логінова Н. І., Манаков С. Ю., Дубовой Я. В. Кіберзагрози в освітньому секторі. *Кібербезпека: освіта, наука, техніка*. 2022. № 4 (16). С. 76–84. DOI: <https://doi.org/10.28925/2663-4023.2022.16.7684>
28. Eliot N., Kendall D., Brockway M. A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills. *IEEE Access*. 2018. Volume 6. P. 34884–34895. 2018. URL: <https://ieeexplore.ieee.org/document/8396216>
29. Adahman Z., Malik A. W., Anwar Z. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security*. 2022. Volume 122. DOI: <https://doi.org/10.1016/j.cose.2022.102911>
30. Adevait. Boosting Cybersecurity With AI Anomaly Detection and Prevention. URL: <https://adevait.com/artificial-intelligence/ai-anomaly-detection-and-prevention>

31. Adu-Kyere, A., Nigussie E., Isoaho J. Analyzing the effectiveness of IDS/IPS in real-time with a custom in-vehicle design. *Procedia Computer Science*. 2024. Volume 238. P. 175–183. DOI: <https://doi.org/10.1016/j.procs.2024.06.013>
32. Alaeifar P., Pal S., Jadidi Z., Hussain M., Foo E. Current approaches and future directions for cyber threat intelligence sharing: A survey. *Journal of Information Security and Applications*. 2024. Volume 83. DOI: <https://doi.org/10.1016/j.jisa.2024.103786>
33. Angelova E. Cybersecurity in Higher Education: Challenges and Measures for Information Storage. *Bulgarian Journal of International Economics and Politics*. 2024. № 2. P. 110-126. DOI: <https://doi.org/10.37075/BJIEP.2024.2.07>
34. BitLyft Cybersecurity. Higher Ed Institutions Need SIEM Software. URL: <https://www.bitlyft.com/resources/siem-software-higher-education-institutions>
35. Blikhar M. Legal regulation of personal data protection. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*. 2024. Vol. 11, № 1 (41). P. 26-33. DOI: <https://doi.org/10.23939/law2024.41.026>
36. Bunting D. Can You Use the ELK Stack as a SIEM? A Fresh Take. ChaosSearch. 2023. URL: <https://www.chaossearch.io/blog/elk-stack-siem>
37. Chinthala S. Using SIEM Tools for Cyber Security: Enhancing Threat Detection and Response : A Qualitative Study. Research Paper. 2024. DOI: <https://doi.org/10.13140/RG.2.2.26578.57286>
38. Cisco. Modernizing Cybersecurity for Universities: Solution Brief. URL: <https://www.cisco.com/c/en/us/solutions/collateral/security/modernizing-cybersecurity/modernizing-cybersecurity-universities-sb.html>
39. CodeSecure Solutions. Education SIEM Implementation: Protecting Chennai Academic Institutions. URL: <https://codesecure.in/blogs/education-siem-implementation-protecting-chennai-academic-institutions/>
40. Cyber Digest. Огляд подій в сфері кібербезпеки, березень 2023 р. / Рада національної безпеки і оборони України. Київ, 2023. 49 с. URL: https://www.rnbo.gov.ua/files/2023/NKCK/%D0%BA%D0%B2%D1%96%D1%82%D0%B5%D0%BD%D1%8C/Cyber%20digest_March_2023_UA.pdf

41. Daim T., Yalcin, H., Mermoud A. Monitoring cybersecurity technology through the years: a technology mining approach through bibliometrics and patent analysis. *Journal of Cyber Security Technology*. 2024. P. 1–37. DOI: <https://doi.org/10.1080/23742917.2024.2400729>
42. DataGuard. How intrusion detection systems help identify cyber threats. URL: <https://www.dataguard.com/blog/how-intrusion-detection-systems-help-identify-cyber-threats/>
43. Dirsec. The Hidden Threat: Why 83% of Universities Without SIEM and Identity Tools Are Vulnerable. URL: <https://www.dirsec.com/insights/the-hidden-threat-why-83-of-universities-without-siem-and-identity-tools-are-vulnerable/>
44. EduTech Global. Cybersecurity in Higher Education: Strategies to Safeguard Data and Systems. URL: <https://edutech.global/cybersecurity-in-higher-education-2/>
45. European Union Agency for Cybersecurity (ENISA). Cyber Threat Intelligence Overview. 2020. 23 p. URL: <https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20CTI%20Overview%20A4.pdf>
46. Exabeam. What Is SIEM? 7 Pillars and 13 Core Features [2025 Guide]. URL: <https://www.exabeam.com/explainers/siem/what-is-siem/>
47. Fuentes-García M., Camacho J., Maciá-Fernández G. Present and Future of Network Security Monitoring. *IEEE Access*. 2021. Volume 9. P. 112744-112760. DOI: <https://doi.org/10.1109/ACCESS.2021.3067106>
48. He Yu., Huang D., Chen Lei, Ni Yi, Ma X. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*. 2022. Volume 2022, Issue 1. DOI: <https://doi.org/10.1155/2022/6476274>
49. International Organization for Standardization; International Electrotechnical Commission. ISO/IEC 27035-1:2023 Information technology – Information security incident management – Part 1: Principles and process. International Standard 78973. URL: <https://www.iso.org/standard/78973.html>

50. Jin B., Kim E., Lee H., Bertino E., Kim D., Kim H. Sharing cyber threat intelligence: Does it really help? *Network and Distributed System Security*. 2024. P. 1-20. DOI: <https://dx.doi.org/10.14722/ndss.2024.24228>
51. Kingston Technology. Що таке запобігання втраті даних (Data Loss Prevention або DLP)? URL: <https://www.kingston.com/ua/blog/data-security/data-loss-prevention-dlp>
52. Kumar A., Abhishek K., Ghalib M. R., Shankar A., Cheng X. Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks*. 2022. Volume 8, Issue 4. P. 540-551. DOI: <https://doi.org/10.1016/j.dcan.2022.05.027>
53. Lahoud H. A., Tang X. Information security labs in IDS/IPS for distance education. *Proceedings of the 7th Conference on Information Technology Education*. 2006. P. 47–52. DOI: <https://doi.org/10.1145/1168812.1168826>
54. MoldStud. Managing compliance with General Data Protection Regulation (GDPR) in university systems. URL: <https://moldstud.com/articles/p-managing-compliance-with-general-data-protection-regulation-gdpr-in-university-systems>
55. Muhammad A. R., Sukarno P., Wardana A. A. Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning. *Procedia Computer Science*. 2023. Volume 217. P. 1406-1415. DOI: <https://doi.org/10.1016/j.procs.2022.12.339>
56. Mushtaq S., Mohsin M., Mushtaq MM. A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors*. 2025. Volume 25, Issue 19. DOI: <https://doi.org/10.3390/s25196118>
57. Nab N., Rahman M. M., Ghosh S. K., Alam S., Barua R., Asaduzzaman M., Shatu N. R. Machine Learning-Based Anomaly Detection for Cyber Threat Prevention. *Journal of Primeasia*. 2025. 6(1). P. 1-8. DOI: <https://doi.org/10.25163/primeasia.6110172>
58. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). 2024. Gaithersburg, MD: NIST. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

59. Netwave. Що таке DLP-системи: види, можливості, порівняння рішень.
URL: <https://netwave.ua/blog/shho-take-dlp-systemy-vydy-mozhlyvosti-porivnyannya-rishen/>
60. Network security monitoring with Wazuh and Zeek. Wazuh Blog, 2025.
URL: <https://wazuh.com/blog/network-security-monitoring-with-wazuh-and-zeek/>
61. Onyinye Obioha-Val. The Role of Artificial Intelligence (AI) in Enhancing Cybersecurity for Educational Technologies in US Public Schools. *Asian Journal of Research in Computer Science*. 2024. Volume 17, Issue 11. P. 114–133.
DOI: <https://doi.org/10.9734/ajrcos/2024/v17i11523>.
62. Ozman F. M. Implementing Data Loss Prevention (DLP). *World Journal of Advanced Engineering Technology and Sciences*. 2025. № 15 (02). P. 2427-2436.
DOI: <https://doi.org/10.30574/wjaets.2025.15.2.0792>
63. Parfonova I., Zinchenko O. Countering Cyber Threats In The Context Of Digital Educational Technologies In The Higher Education System Of Ukraine. *Scientific Journal of Polonia University*. 2025. № 67 (6). P. 230-238.
DOI: <https://doi.org/10.23856/6729>
64. Pokhrel R. P. Behavioral analysis of malware using sandboxing techniques. *International Journal of Science and Research Archive*, 2025. № 15 (03). P. 582-586.
DOI: <https://doi.org/10.30574/ijrsra.2025.15.3.1781>
65. Qurbonaliyeva D., Abduraxmanova G. Analysis of Methods of Attracting Attackers in the Honeypot. *ICFNDS '24: Proceedings of the 8th International Conference on Future Networks & Distributed Systems*. 2025. P. 897-904. DOI: <https://doi.org/10.1145/3726122.3726253>
66. Regi S., Kaur G. Improving Threat Detection with Elastic Stack based Security Information and Event Management. *International Journal for Research in Applied Science & Engineering Technology*. 2024. Volume 12, Issue IV. P. 2428-2431.
DOI: <https://doi.org/10.22214/ijraset.2024.60266>
67. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: National Institute of Standards and Technology. 2020. 53 p.
DOI: <https://doi.org/10.6028/NIST.SP.800-207>

68. Roshanaei M. Jachura M. Integrating AI in Cybersecurity Higher Education: A Path to Workforce Readiness. *Journal of Intelligent Learning Systems and Applications*. 2025. Vol 17, № 2. P. 45-67. DOI: <https://doi.org/10.4236/jilsa.2025.172005>
69. Sadiqzade Z., Alisoy H. Cybersecurity and Online Education – Risks and Solutions. *Luminis Applied Science and Engineering*. 2025. Vol. 2, № 1. P.4-12. DOI: <https://doi.org/10.69760/lumin.20250001001>
70. Saeed S., Suayyid S. A., Al-Ghamdi M. S., Al-Muhaisen H., Almuhaideb A.M. A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience. *Sensors*. 2023. Volume 23, Issue 16. DOI: <https://doi.org/10.3390/s23167273>
71. Sindika D., Nicholaus M., Hamadi N. Improving Network Security: An Intrusion Detection System (IDS) Dataset from Higher Learning Institutions, Mbeya University of Science and Technology (MUST), Tanzania. *East African Journal of Information Technology*. 2024. Vol 7, № 1. P. 23-38. DOI: <https://doi.org/10.37284/EAJIT.7.1.1679>
72. Sridharan A., Kanchana V. SIEM integration with SOAR. *International Conference on Futuristic Technologies*. 2022. DOI: <https://doi.org/10.1109/INCOFT55651.2022.10094537>
73. Staiger T. Cyber Threat Intelligence Sharing Platforms: A Comprehensive Analysis of Software Vendors and Research Perspectives. Master's thesis, University of Innsbruck. 2021. 84 p. URL: <https://ulb-dok.uibk.ac.at/ulbtirolhs/download/pdf/6676638>
74. Tudela K. N. B., Patilla H. J. Security Onion as a Network Auditing Tool at the San Cristóbal de Huamanga National University. *International Journal of Advanced Computer Science and Applications*. 2025. Volume 14, № 3. P. 138-149. DOI: <https://dx.doi.org/10.14569/IJACSA.2025.0160314>
75. Varanda A., Santos L., Costa R. L. de C., Oliveira A., Rabadão C. Log pseudonymization: Privacy maintenance in practice. *Journal of Information Security and Applications*. 2021. Volume 63. DOI: <https://doi.org/10.1016/j.jisa.2021.103021>
76. Verbovskyi I. Classification and main types of cyber threats to the educational environment. *Global Trends in Science: Research, Innovation and*

Development : 1st International Scientific and Practical Conference. Varna, 2025. P. 118–121. URL: <https://eprints.zu.edu.ua/44270/>

77. Veriato. Cybersecurity in Higher Education: Understanding the Threats & Adopting A Zero Trust Approach. URL: <https://veriato.com/blog/cybersecurity-in-higher-education-understanding-the-threats-adopting-a-zero-trust-approach/>

78. Wada I. U., Izibili G. O., Babayemi T., Abdulkareem A., Macaulay O. M., Emadoye A. AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews*. 2025. № 25 (03). P. 2233-2245. DOI: <https://doi.org/10.30574/wjarr.2025.25.3.0989>

79. Wang X., Bhuse V., Cheng Yu. A Zero Trust Module for Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education*. 2025. Volume 12, № 1. P. 1-10. URL: <https://www.ycheng.org/papers/cisse2025.pdf>

80. Wannere K. Exploring the Implementation and Challenges of Zero Trust Security Models in Modern Network Environments. *International Journal of Engineering Research & Technology*. 2025. Volume 14, Issue 05. URL: <https://www.ijert.org/exploring-the-implementation-and-challenges-of-zero-trust-security-models-in-modern-network-environments>

81. Yesin V., Vilihura V., Uzlov D. Zero trust architecture: challenges and recommendations for successful implementation. *Radiotekhnika*. 2024. 3(218). P. 7–34. DOI: <https://doi.org/10.30837/rt.2024.3.218.01>

82. Zanasi C., Russo S., Colajanni M. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*. 2024. Volume 156. DOI: <https://doi.org/10.1016/j.adhoc.2024.103414>

83. Zybin S., Bondarchuk O., Piroh O., Suprun O., Kyshakevych S. Cybersecurity on Ukrainian Higher Education: Threats and protection measures. *Eduweb*. 2025. № 19 (2). P. 38-52. DOI: <https://doi.org/10.46502/issn.1856-7576/2025.19.02.3>

ДОДАТКИ

Інформація з ресурсу eportfolio, яка доступна неавторизованим користувачам

Е-портфоліо Користувачі Освітні програми Заходи Публічна інформація



Вербовський Ігор Андрійович

Факультет / Інститут: Начально-науковий інститут педагогіки
Кафедра: Професійно-педагогічної, спеціальної освіти, андрагогіки та управління
Електронна пошта: Verbovskiy-I@zu.edu.ua
Посада: Доцент

Освіта, вчене звання / науковий ступінь

Актуальні пункти професійної активності

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Професійний розвиток

Викладацька діяльність

Виховна робота

Адміністративна діяльність

Планування індивідуальної роботи

- + 1.1 Наявність публікацій у наукових виданнях, що включені до наукометричних баз, зокрема Scopus, Web of Science Core Collection (8)
- + 1.2 Наявність публікацій у періодичних наукових виданнях, що включені до переліку фахових видань України (36)
- + 2 Патенти та авторські свідоцтва (0)
- + 3 Наявність виданого підручника чи навчального посібника або монографії (0)
- + 4 Наявність виданих навчально-методичних посібників/посібників для самостійної роботи здобувачів вищої освіти та дистанційного навчання, електронних курсів на освітніх платформах ліцензіації, конспектів лекцій/практикумів/методичних вказівок/рекомендацій/робочих програм, інших друкованих навчально-методичних праць (3)

Е-портфоліо Користувачі Освітні програми Заходи Публічна інформація

Головна / F3 Комп'ютерні науки / Комп'ютерні науки / Магістр / 2025

Освітня програма F3 Комп'ютерні науки / Комп'ютерні науки Магістр 2025 рік [pdf](#)

Модернізація ОП:
- 2025 [pdf](#)

Навчальний план:
Денна форма навчання [pdf](#)
Робочий план 2025/2026 [pdf](#)

Обов'язкові освітні компоненти:

Професійна комунікація іноземною мовою, номер 1.1.1
Навчальна програма [pdf](#)
Робоча програма 2025/2026 [pdf](#)
Силабус [pdf](#)

Методика наукових досліджень, номер 1.1.2
Навчальна програма [pdf](#)
Робоча програма 2025/2026 [pdf](#)
Силабус [pdf](#)

Інтелектуальна власність, номер 1.1.3
Навчальна програма [pdf](#)
Робоча програма 2025/2026 [pdf](#)
Силабус [pdf](#)

Менеджмент IT-проектів, номер 1.1.4
Навчальна програма [pdf](#)
Робоча програма 2025/2026 [pdf](#)
Силабус [pdf](#)

Функціонал ресурсу eportfolio, доступний гаранту освітніх програм у режимі перевірки/редагування (для науково-педагогічних працівників)

Перевірка ОП

Ця сторінка може допомогти перевірити номери навчальних програм і наявність завантажених робочих програм та силабусів.

Зверніть увагу. Тут не показано дані які точно мають бути завантажені, а просто перевірка послідовності номерів НП та прикріплених до них робочих програм і силабусів.

Сторінка із ОП

Налаштування:

Записи на перевірці: ☒

Відхилені записи: ☒

Користувач який завантажив запис: ☐

Користувач який перевіряв запис: ☐

Перевіряти нумерацію Навчальної програми: ☒

Перевіряти наявність Робочої програми: ☒

Перевіряти наявність Силабуса: ☒

Кількість кредитів ECTS: ☐

Форма звітності для Робочих Програм: ☐

Показати

Сторінка для завантаження даних для ОП F3 Комп'ютерні науки / Комп'ютерні науки Магістр 2025 рік

📌 Освітня програма F3 Комп'ютерні науки / Комп'ютерні науки Магістр 2025 рік

pdf

docx

Рецензія: ☐ Не показувати рецензію ☐ Не показувати рецензію неавторизованим

Рецензія 1 pdf

Модернізація ОП: Очікує перевірки

📌 2024 - 2025

pdf

docx

Акредитація:

Акредитацію не завантажено

Завантажити

Навчальний план:

Завантажити Навчальний план

📌 Денна форма навчання

PDF

xls

Підтверджено

Завантажити Робочий план

📌 Робочий план 2025/2026

PDF

xls

Підтверджено

Обов'язкові освітні компоненти:

Професійна комунікація іноземною мовою, номер 1.1.1

📌 Навчальна програма

PDF

docx

Підтверджено

📌 Робоча програма 2025/2026

PDF

docx

Підтверджено

📌 Силабус

PDF

docx

Підтверджено

Методика наукових досліджень, номер 1.1.2

📌 Навчальна програма

PDF

docx

Підтверджено

📌 Робоча програма 2025/2026

PDF

docx

Підтверджено

📌 Силабус

PDF

docx

Підтверджено

Функціонал сервісу Educational Program, доступний не авторизованим користувачам

 Educational Program

[Головна](#) [Освітні програми](#) [Проекти](#)

[Вхід](#)

Пошук

Пошук

Фільтри

Рік:
2025

Рівень:
Другий (Магістерський)

Завершено редагування:
Усі

Фільтрувати

Історія та археологія

Назва англійською History and Archeology	Рік 2025	Рівень Перший (Бакалаврський)
Тип Освітньо-професійна	Статус Проект	Форма здобуття освіти очна (денна)
Спеціальність 03 Гуманітарні науки / 032 Історія та археологія	Кафедра Історії України	ID в EDBO 5504

Маркетинг

Назва англійською Marketing	Рік 2025	Рівень Перший (Бакалаврський)
Тип Освітньо-професійна	Статус Проект	Форма здобуття освіти очна (денна)
Спеціальність 07 Управління та адміністрування / 075 Маркетинг	Кафедра Економіки, менеджменту, маркетингу та готельно-ресторанної справи	ID в EDBO 5256

Функціонал service Educational Program, доступний гарантам освітніх програм

Головна / Освітні програми / Комп'ютерні науки

[⌂ Повернутись](#)
[📄 Навчальний план](#)
[📄 Експорт інформації у WORD](#)

[⬇ Згенерувати ОП](#)

Освітня програма: **Комп'ютерні науки**

Назва англійською Computer Sciences	Рік 2025	Рівень Другий (Магістерський)
Тип Освітньо-професійна	Статус Діюча	Форма здобуття освіти очна (денна)
Спеціальність F Інформаційні технології / F3 Комп'ютерні науки	Кафедра Комп'ютерних наук та інформаційних технологій	ID в EDBO 78896

[↗ Переглянути на E-портфоліо](#)

Номер сертифікату 15198	Номер рішення 21	📄 Сертифікат
Сертифікат виданий Національне агентство із забезпечення якості вищої освіти	Дата рішення 21.06.2025 Дійсний до 01.07.2030	

Гарант
Постова Світлана Анатоліївна

Дані про освітню програму

Розробники

Загальна інформація

Мета та цілі

Характеристика

Придатність випускників до працевлаштування та подальшого навчання

Викладання та оцінювання

Компетентності

Програмні результати навчання

Перелік освітніх компонент

Структурно логічна схема

Ресурсне забезпечення