УДК: 004.056:004.75:37.016
JEL Classification: I23; O33; M15
DOI 10.35433/ISSN2410-3748-2025-2(37)-19

Вербовський Ігор
кандидат педагогічних наук, доцент
начальник навчального відділу,
доцент кафедри професійно-педагогічної,
спеціальної освіти, андрагогіки та управління
Житомирський державний університет імені Івана Франка
https://orcid.org/0000-0001-7202-3429

Шелуха Олексій
кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»
https://orcid.org/0000-0002-6088-8262

УПРАВЛІННЯ КІБЕРРИЗИКАМИ В ОСВІТНЬОМУ СЕРЕДОВИЩІ

Стаття присвячена комплексному дослідженню методів і технологій моніторингу й аналізу кіберзагроз в освітньому середовищі, що набуває особливої актуальності в умовах стрімкої цифровізації та зростання залежності закладів освіти від цифрових платформ, електронного документообігу, дистанційного навчання та хмарних сервісів. Розкрито сутність сучасних загроз, характерних для освітньої інфраструктури, зокрема фішингових атак, несанкціонованого доступу, шкідливого програмного забезпечення, витоків даних здобувачів освіти та персоналу, а також маніпулятивних інформаційних впливів.

Для досягнення мети дослідження застосовано порівняльний аналіз технологічних рішень, що використовуються в міжнародній практиці кіберзахисту освітніх установ. У поєднанні з методами синтезу, індукції, узагальнення та логічного моделювання це дало змогу обґрунтувати оптимальні підходи до побудови систем виявлення й запобігання кіберзагрозам. Проаналізовано застосування методів аналізу журналів подій, систем SIEM, технологій IDS/IPS, сигнатурних і поведінкових моделей аналізу шкідливої активності, а також можливості машинного навчання для прогнозування кіберризиків. Критичний огляд сучасних наукових підходів дав змогу визначити основні вимоги до ефективної системи кіберзахисту освітнього середовища та виокремити її функціональні компоненти.

У статті представлено оцінку готовності українських закладів освіти до впровадження сучасних кіберзахисних технологій, описано типові проблеми, пов'язані з недостатністю фінансування, низькою цифровою культурою персоналу та відсутністю стандартизованих протоколів реагування на кіберінциденти. Запропоновано практичні рекомендації щодо підвищення рівня кіберстійкості: посилення інфраструктурної безпеки, упровадження централізованих систем моніторингу, регулярне навчання педагогів і здобувачів освіти, застосування європейських протоколів кібергігієни та адаптація найкращих практик міжнародних організацій, зокрема ENISA та ISO/IEC. Практична значущість роботи полягає в тому, що сформовані рекомендації та висновки можуть бути використані керівниками закладів освіти, фахівцями IT-підрозділів та державними

органами під час розробки політик інформаційної безпеки, підвищення кіберстійкості й створення безпечного цифрового освітнього середовища.

Ключові слова: *кібербезпека в освіті, інформаційна безпека, цифрове освітнє середовище, контроль безпеки, методи виявлення загроз.*

CYBER RISK MANAGEMENT IN THE EDUCATIONAL ENVIRONMENT

This article is devoted to a comprehensive study of methods and technologies for monitoring and analyzing cyber threats in the educational environment, which is particularly relevant in the context of rapid digitalization and the growing dependence of educational institutions on digital platforms, electronic document management, distance learning, and cloud services. The article reveals the nature of modern threats characteristic of educational infrastructure, in particular phishing attacks, unauthorized access, malicious software, data leaks of students and staff, as well as manipulative information influences.

To achieve the research objective, a comparative analysis of technological solutions used in international cyber security practices for educational institutions was applied. Combined with methods of synthesis, induction, generalization, and logical modeling, this made it possible to substantiate optimal approaches to building systems for detecting and preventing cyber threats. The application of event log analysis methods, SIEM systems, IDS/IPS technologies, signature and behavioral models of malicious activity analysis, as well as the possibilities of machine learning for predicting cyber risks were analyzed. A critical review of current scientific approaches made it possible to identify the basic requirements for an effective cyber protection system for the educational environment and to highlight its functional components.

The article presents an assessment of the readiness of Ukrainian educational institutions to implement modern cyber protection technologies, describes typical problems related to insufficient funding, low digital culture of staff, and the lack of standardized protocols for responding to cyber incidents. Practical recommendations are proposed to increase cyber resilience: strengthening infrastructure security, introducing centralized monitoring systems, regular training of teachers and students, applying European cyber hygiene protocols, and adapting the best practices of international organizations, in particular ENISA and ISO/IEC. The practical significance of the work lies in the fact that the conclusions and recommendations can be used by heads of educational institutions, IT specialists, and government agencies when developing information security policies, improving cyber resilience, and creating a secure digital educational environment.

Keywords: *cybersecurity in education, information security, digital educational environment, security control, threat detection methods.*

Постановка проблеми. Сучасний етап цифрового розвитку української освіти характеризується стрімким впровадженням інформаційно-комунікаційних технологій (далі – ІКТ), які є невіддільним елементом освітнього процесу, управлінських рішень та комунікації між учасниками освітнього середовища. Використання електронних журналів, дистанційних платформ, хмарних сервісів і систем управління навчанням формує нові можливості для підвищення якості освіти, водночас створюючи додаткові ризики, пов’язані з кіберзагрозами різного характеру. В умовах воєнного стану

та загальної нестабільності ці ризики значно посилюються, оскільки освітня інфраструктура стає потенційною мішенню для кібератак, спрямованих на порушення роботи систем, викрадення даних або дестабілізацію освітнього процесу.

За таких умов виникає об’єктивна потреба в ґрунтовному дослідженні методів і технологій, здатних оперативно виявляти, аналізувати та мінімізувати кіберризики. Системне вивчення сучасних підходів до моніторингу кіберзагроз, оцінка їхньої ефективності та можливостей застосування в українських закладах освіти зумовлюють актуальність обраної проблеми й визначають необхідність наукового обґрунтування шляхів підвищення кіберстійкості освітнього середовища.

Аналіз останніх досліджень та публікацій. Проблема гарантування кібербезпеки в цифровому освітньому середовищі активно досліджується українськими та закордонними науковцями в контексті зростання залежності закладів освіти від ІКТ. У працях М. Швардак систематизовано основні кіберзагрози освітньому середовищу й проаналізовано їхній вплив на стабільність функціонування цифрових освітніх платформ [1, с. 32]. В. Коваленко й Т. Осипчук акцентують на ролі людського чинника, обґрунтовуючи необхідність системної підготовки педагогів із питань кібербезпеки як основної умови зниження вразливості освітнього середовища [2, с. 37]. Організаційний вимір кібербезпеки закладів вищої освіти розкрито в дослідженнях В. Савченка та О. Маклюк, де кіберзахист розглядається як елемент інформаційної політики освітніх установ [3].

Технологічні аспекти захисту інформації в освітній сфері висвітлено в роботах Г. Бахмат (H. Bakhmat) та співавторів, які підкреслюють значення захищених цифрових інструментів у підготовці педагогічних кадрів [4]. Комплексні системи захисту інформації, зокрема автентифікаційні механізми, криптографічні засоби й системи виявлення вторгнень, проаналізовано в працях Б. Павлюка, Б. Розпутньої та В. Кисліцина [5].

У ширшому безпековому та інституційному контексті M. Pleskach (М. Плескач) та співавтори визначають концептуальні засади формування національної системи кібербезпеки, які можуть бути адаптовані до потреб освітньої сфери [6]. Міжнародно-правові аспекти гарантування кібербезпеки та необхідність гармонізації національного законодавства з європейськими стандартами досліджують О. В. Пчеліна та співавтори (O. V. Pchelina et al.) [7]. Перспективи застосування технологій штучного інтелекту (далі – ШІ) для виявлення складних кібератак і підвищення ефективності моніторингу цифрових систем розглядають В. Ткачов (V. Tkachov) та співавтори [8]. Проблеми захисту критичної інформаційної інфраструктури, зокрема освітніх установ, досліджено в працях Н. Чаудгурі та В. Гкіулоса (N. Chowdhury, V. Gkioulos), Л. Магларас та співавторів (L. Maglaras et al.), які акцентують на взаємозв'язку кіберосвіти з національною безпекою [9; 10]. Окрему увагу в наукових дослідженнях приділено розвитку кіберосвітніх програм і формуванню цифрових компетентностей фахівців. Зокрема, вимоги до змісту освітніх програм у сфері цифрової трансформації та кібербезпеки обґрунтовують К. Аалтола (K. Aaltola), Г. Руослагті (H. Ruoslahti), Е. В. Гетем (E. V. Goethem), М. Істон (M. Easton) [11; 12]. Модель Європейської кібербезпекової мережі (ECSCON), у якій відображено перспективи міждержавної координації у сфері кіберзахисту освітніх систем, запропонували Г. Пенчев (G. Penchev), А. Шаламанова-Філіпова (A. Shalamanova-Filipova) [13]. Питання формування безпечного цифрового освітнього середовища як цілісної кіберосвітньої екосистеми висвітлено в працях В. Юскович-Жуковської та співавторів [14].

Узагальнення результатів аналізу наукових джерел засвідчує, що попри значний обсяг досліджень у сфері кібербезпеки освіти, недостатньо розробленими залишаються питання практичної імплементації комплексних систем моніторингу кіберзагроз, адаптованих до ресурсних можливостей закладів освіти, що й зумовлює актуальність подальших досліджень у цьому напрямі.

Виділення нерозв'язаних раніше частин загальної проблеми. Попри зростання кількості наукових досліджень у сфері кібербезпеки, залишається обмежено вивченою низка аспектів забезпечення захисту освітнього середовища. Зокрема, відсутній комплексний аналіз функціонування систем кіберзахисту освітніх установ за умови підвищеного навантаження, нестабільності та трансформації освітнього процесу, особливо в період воєнного стану. Більшість наявних публікацій зосереджена на загальних питаннях інформаційної безпеки, тоді як специфіка освітньої інфраструктури та цифрової взаємодії учасників освітнього процесу висвітлюється фрагментарно.

Недостатньо дослідженими залишаються можливості практичного застосування сучасних систем моніторингу кіберзагроз, зокрема SIEM, IDS/IPS, технологій поведінкового аналізу й інструментів ШІ, саме в контексті закладів освіти. Окремої уваги потребує проблема адаптації закордонних моделей кіберзахисту до українських реалій, що характеризуються обмеженими ресурсами, неоднорідністю цифрової інфраструктури та різним рівнем цифрової компетентності персоналу.

Наукова цінність дослідження полягає в комплексному аналізі теоретичних і прикладних аспектів забезпечення кіберзахисту освітнього середовища, систематизації актуальних викликів, оцінці ефективності сучасних технологій моніторингу й розробленні практичних рекомендацій, спрямованих на підвищення кіберстійкості українських закладів освіти.

Метою статті є дослідження та систематизація сучасних методів і технологій моніторингу й аналізу кіберзагроз в освітньому середовищі, що дасть змогу розробити рекомендації для підвищення кіберстійкості закладів освіти та забезпечення захисту даних учасників освітнього процесу.

Завдання роботи:

- проаналізувати сучасний стан кіберзахисту в освітній сфері та рівень застосування технологій моніторингу й аналізу кіберзагроз;
- визначити основні виклики та вразливості, зумовлені інтенсивною цифровізацією освітнього середовища й зростанням кількості кіберінцидентів;

- дослідити можливості застосування систем SIEM, IDS/IPS, поведінкового аналізу й інструментів ШІ для проактивного виявлення й запобігання кіберзагрозам;

- розробити рекомендації для впровадження ефективних моделей моніторингу та реагування на кіберінциденти з урахуванням українських реалій, ресурсних обмежень та міжнародних стандартів.

Виклад основного матеріалу. В умовах сучасної цифрової трансформації освіти цифрові технології стали невіддільною частиною організації освітнього процесу. Електронні журнали, системи управління, освітні платформи, інструменти дистанційного навчання й хмарні сервіси створюють новий формат взаємодії між учасниками освітнього середовища, що зумовлює зростання залежності закладів освіти від стійкості та надійності цифрової інфраструктури [15].

Розширення використання цифрових сервісів супроводжується підвищенням ризиків кіберінцидентів, наслідками яких можуть бути порушення освітнього процесу, фінансові втрати й зниження довіри користувачів [1, с. 27]. З огляду на це кібербезпека набуває статусу фундаментальної умови стабільного функціонування освітніх організацій і важливої складової їхньої інформаційної політики.

Для системного розуміння кіберзахисту в освітній сфері доцільно виокремити основні напрями захисту цифрового середовища: від мережевої та хмарної безпеки до захисту даних і формування кібергігієни користувачів. Узагальнену модель сучасних видів кібербезпеки в освіті представлено на рис. 1.

Представлені напрями кібербезпеки засвідчують, що ефективний захист цифрового освітнього середовища можливий лише за умови інтеграції технологічних і організаційних заходів у межах єдиної системи управління безпекою.

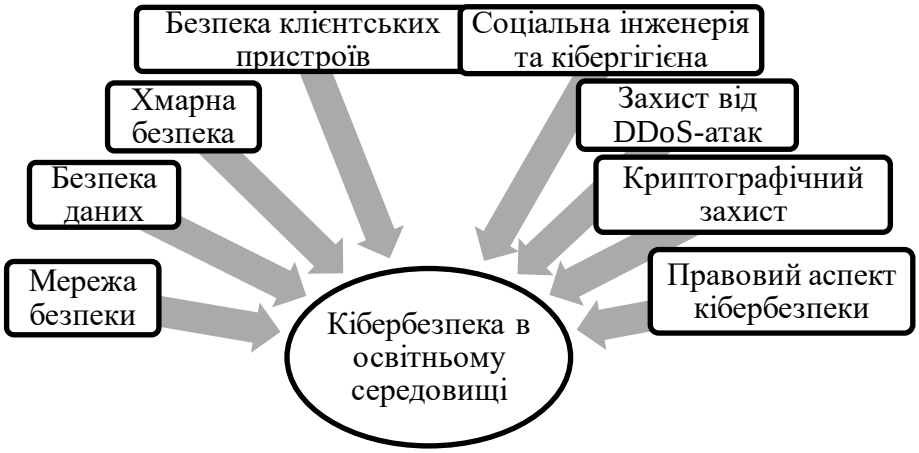

Рис. 1. Сучасні види кібербезпеки в освітній сфері

Джерело: сформовано авторами

За умов зростання соціально орієнтованих загроз, зокрема фішингу та кібербулінгу, важливого значення набуває розвиток цифрової культури користувачів і формування сталої кібергігієни. Навчання здобувачів освіти, викладачів і технічного персоналу принципам безпечної поведінки сприяє значному зниженню ризиків, пов’язаних із застосуванням маніпулятивних технік. Водночас стабільність функціонування освітніх платформ забезпечується поєднанням організаційних заходів із технологічними рішеннями: від криптографічних методів захисту до інструментів протидії DDoS-атакам [11].

Правове регулювання також посідає помітне місце в системі кібербезпеки, оскільки встановлює вимоги до обробки персональних даних, визначає обов’язки установ та забезпечує відповідальність за їхні порушення. Сукупність цих елементів демонструє, що кібербезпека в освіті є багатовимірною системою, що поєднує технічні засоби, політики управління й людський чинник. Саме інтеграція цих складників дає змогу формувати стійке й захищене цифрове середовище, здатне ефективно протидіяти сучасним кіберзагрозам [8].

У процесі цифровізації освітнього середовища ці загрози набули нових форм і масштабів. Розширення доступу до онлайн-платформ, використання

хмарних сервісів, зростання обсягу персональних даних та активне впровадження дистанційних технологій спричинили появу низки вразливих точок, які можуть бути використані зловмисниками. З огляду на це аналіз типових кіберзагроз є необхідною передумовою формування ефективної стратегії безпеки закладу освіти.

У табл. 1 систематизовано основні види кіберзагроз.

Таблиця 1

Основні загрози кібербезпеці в цифровій освіті

Кіберзагроза	Сутність загрози	Можливі наслідки	Заходи щодо запобігання
Несанкціонований доступ до освітніх платформ	Доступ до облікових записів через слабкі паролі, фішинг або вразливості систем	Витік даних; зміна навчальних матеріалів; маніпуляція оцінюванням	Багатофакторна автентифікація; політика складних паролів; аудит доступу
Фішинг і соціальна інженерія	Шахрайські повідомлення з метою отримання конфіденційної інформації	Компрометація акаунтів; поширення шкідливого ПЗ	Фільтрація повідомлень; антивірусний захист; систематичне навчання користувачів
Витік персональних даних	Несанкціонований доступ до баз даних	Шахрайство; цільові кібератаки; репутаційні втрати	Криптографічне шифрування; резервне копіювання; контроль доступу
Кібербулінг (кіберзнущання)	Анонімні образи та погрози через цифрові канали	Психологічна шкода; зниження навчальної мотивації	Чіткі політики етичної поведінки; модерація; ефективні канали повідомлення
Віруси та шкідливе ПЗ	Проникнення malware через файли або посилання	Втрата даних; блокування систем; витік інформації	Регулярне оновлення всього програмного забезпечення; антивірусний захист; контроль файлів
DDoS-атаки на освітні сервіси	Перевантаження серверів з метою порушення доступності	Переривання освітнього процесу; фінансові втрати	Фільтрація трафіку; проактивний захист інфраструктури
Вразливості програмного забезпечення	Використання застарілого або нелегального програмного забезпечення	Несанкціонований доступ; упровадження шкідливого коду	Ліцензійне програмне забезпечення; регулярні оновлення та сканування вразливостей

Джерело: сформовано авторами за джерелами [1, 3, 8]

Аналіз загроз свідчить про необхідність комплексних заходів запобігання, що поєднують технічні рішення й підвищення цифрової грамотності.

Забезпечення сталого кіберзахисту освітнього середовища потребує поєднання організаційних, технічних і програмних заходів у межах цілісної системи інформаційної безпеки. Оскільки цифрові сервіси є базовою інфраструктурою сучасного закладу освіти, саме комплексний підхід визначає ефективність мінімізації ризиків та оперативного реагування на кіберінциденти.

Головним елементом таких систем є механізми ідентифікації й автентифікації користувачів, що забезпечують контроль доступу до інформаційних ресурсів. У практиці освітніх установ застосовуються паролі, біометричні рішення, смарткартки та токени, а багатофакторна автентифікація значно знижує ризик несанкціонованого доступу до навчальних платформ [14].

Перспективним напрямом розвитку інституційної кібербезпеки є впровадження поведінкового аналізу користувачів (UEBA), який дає змогу виявляти аномалії, пов’язані з компрометацією облікових записів або підготовкою атак. Для освітнього сектору з великою кількістю користувачів UEBA забезпечує превентивний контроль, недоступний для традиційних сигнатурних засобів.

Важливу роль у підвищенні ефективності виявлення загроз відіграють алгоритми ШІ та машинного навчання, здатні аналізувати великі масиви даних, розпізнавати атаки нульового дня й адаптувати моделі ризиків до динаміки кіберзагроз.

Основним компонентом комплексного захисту є SIEM-системи, що забезпечують централізований збір і кореляцію подій із різних елементів цифрової інфраструктури. Моніторинг у реальному часі дає змогу оперативно виявляти аномальну активність і мінімізувати вплив людського чинника під час реагування на інциденти [11].

Подальший розвиток систем моніторингу пов’язаний із використанням платформ кіберрозвідки (TIP/CTI), які забезпечують актуалізацію індикаторів компрометації та підвищують точність виявлення фішингових кампаній.

Автоматизація реагування реалізується через платформи SOAR, що дають змогу оперативно блокувати загрози й підтримувати безперервність освітнього процесу за умов обмежених кадрових ресурсів.

Додатковими елементами системи захисту є sandbox-аналіз для дослідження шкідливих файлів, криптографічні засоби захисту даних (AES, RSA, SSL/TLS), а також системи IDS/IPS і антивірусне програмне забезпечення, які формують активний периметр безпеки освітньої інфраструктури (табл. 2).

Таблиця 2

Основні технологічні елементи інтегрованих систем інформаційної безпеки в освітньому середовищі

Технологічний компонент	Опис
Засоби ідентифікації та автентифікації користувачів	Забезпечують перевірку особи користувачів і контроль доступу до цифрових ресурсів закладу освіти шляхом використання паролів, біометричних параметрів, смарткарток чи інших засобів автентифікації
Криптографічні інструменти захисту даних	Забезпечують конфіденційність і цілісність інформації під час її передавання та зберігання шляхом застосування сучасних алгоритмів і протоколів шифрування (AES, RSA, SSL/TLS)
Системи виявлення та запобігання вторгненням (IDS/IPS)	Застосовуються для моніторингу й аналізу мережевих потоків даних для ідентифікації аномальної або потенційно небезпечної активності, а також для автоматичного реагування шляхом обмеження або припинення несанкціонованих спроб доступу та мережевих атак
Антивірусне програмне забезпечення	Забезпечує виявлення, ізоляцію та видалення шкідливого програмного забезпечення, запобігаючи порушенню роботи інформаційних систем закладу освіти
Платформи кіберрозвідки та аналізу загроз (TIP / CTI)	Забезпечують збір, аналіз та актуалізацію інформації про сучасні кіберзагрози, індикатори компрометації та уразливості для підвищення проактивності систем захисту
SOAR-платформи автоматизації реагування	Дають змогу автоматизувати процеси реагування на кіберінциденти шляхом використання сценаріїв дій, що скорочує час реагування та зменшує навантаження на IT-персонал
EDR / XDR-рішення для захисту кінцевих точок	Забезпечують моніторинг та аналіз поведінки кінцевих пристроїв користувачів для виявлення складних і прихованих атак у реальному часі
Інструменти управління вразливостями (Vulnerability Management)	Призначені для систематичного виявлення, оцінювання та пріоритизації уразливостей у програмному забезпеченні й мережевій інфраструктурі освітніх установ

Джерело: *сформовано авторами за джерелами [5, 8, 11–15]*

Представлені в табл. 2 технологічні компоненти демонструють, що ефективний кіберзахист освітніх установ можливий лише за умови комплексного поєднання взаємодоповнювальних інструментів. Перехід від ізольованого застосування окремих засобів захисту до інтегрованого технологічного стеку (TIP/CTI, SOAR, EDR/XDR, Vulnerability Management) свідчить про еволюцію систем кібербезпеки від реактивної до проактивної та ризикоорієнтованої моделі.

Для узагальнення структурних і функціональних компонентів системи моніторингу й аналізу кіберзагроз у закладі освіти доцільно представити її архітектуру як інтегровану модель, що відображає взаємозв'язки між рівнями збору даних, аналітичної обробки й ухвалення управлінських рішень (рис. 2).

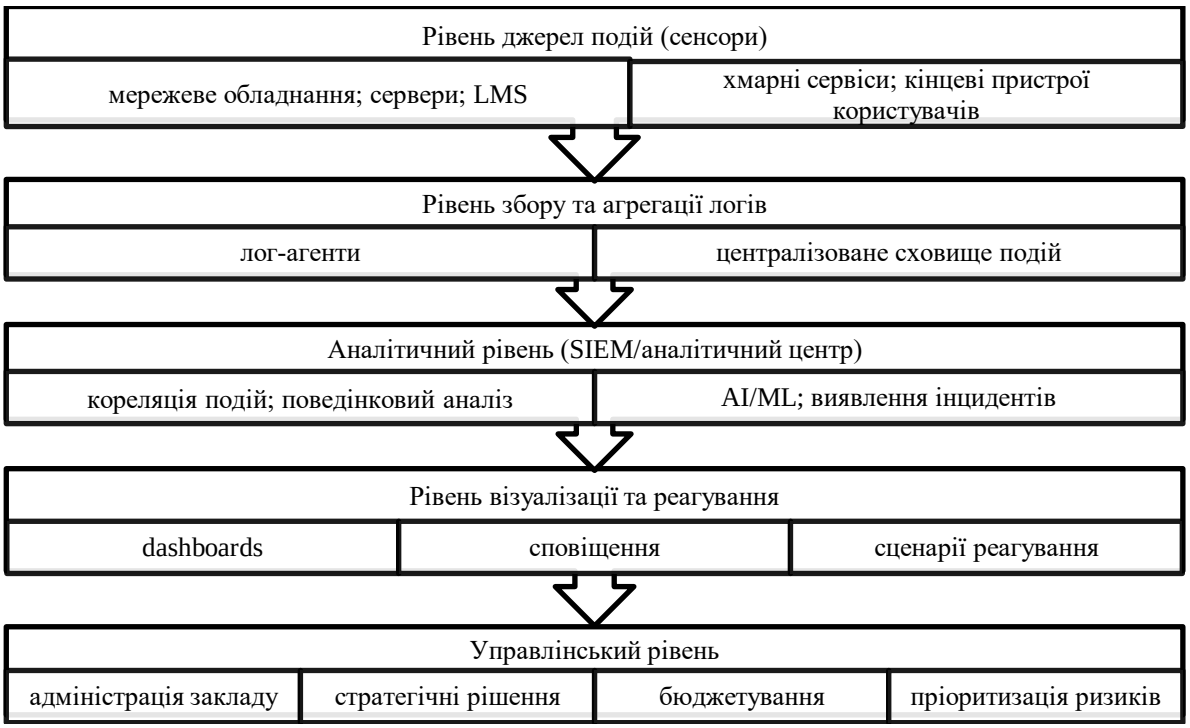

Рис. 2. Архітектура системи моніторингу та аналізу кіберзагроз у закладі освіти

Джерело: сформовано авторами

Представлена на рис. 2 архітектура відображає інтегрований характер системи моніторингу та аналізу кіберзагроз, що поєднує засоби збору подій, аналітичну обробку даних і механізми підтримки управлінських рішень. Ця

структура забезпечує безперервний контроль стану інформаційної безпеки, своєчасне виявлення аномальної активності й адаптацію системи до умов освітнього середовища з урахуванням ресурсних обмежень закладу освіти.

Проєктування системи моніторингу кіберзагроз доцільно здійснювати на основі багаторівневої архітектури, що охоплює всі етапи життєвого циклу подій безпеки: від фіксації сигналів до ухвалення управлінських рішень. Основні рівні такої архітектури та їхнє функціональне призначення узагальнено в табл. 3.

Таблиця 3

Рівні архітектури системи моніторингу кіберзагроз

Рівень системи	Функціональне призначення
Рівень збору даних	Фіксація подій безпеки з мережевого обладнання, серверів, освітніх платформ (LMS), хмарних сервісів і кінцевих пристроїв користувачів
Централізація та нормалізація логів	Агрегація, фільтрація й уніфікація подій для забезпечення кореляційного аналізу та єдиної часової шкали інцидентів
Аналітичний рівень (SIEM / SOC)	Кореляція подій, виявлення аномалій, застосування сигнатурних і поведінкових моделей, прогнозування кіберінцидентів
Рівень реагування	Формування сповіщень, запуск сценаріїв реагування, підтримка автоматизованих або напівавтоматизованих заходів
Рівень візуалізації	Представлення агрегованих показників, індикаторів ризику та динаміки інцидентів для керівництва та фахівців закладу освіти
Інтеграційний рівень	Взаємодія з наявною цифровою інфраструктурою (LMS, електронні журнали, кадрові та фінансові системи)

Джерело: *сформовано авторами*

Вибір технологічного стеку має здійснюватися з урахуванням фінансових і кадрових можливостей закладу освіти. Комерційні рішення забезпечують високий рівень автоматизації, тоді як open-source платформи дають змогу реалізувати функції моніторингу за умови наявності кваліфікованих фахівців. У практиці закладів освіти доцільним є комбінований підхід, що поєднує гнучкість та економічну доцільність. Управління впровадженням системи моніторингу має ґрунтуватися на ризикоорієнтованому підході, що передбачає пріоритизацію захисту важливих цифрових активів. Поетапне впровадження дає змогу знизити фінансове навантаження та забезпечити поступове підвищення рівня кіберстійкості закладу освіти.

Таким чином, система моніторингу та аналізу кіберзагроз у закладі освіти має ґрунтуватися на інтегрованій архітектурі, що поєднує технічні, аналітичні та управлінські компоненти. Запропонований підхід забезпечує адаптацію до змін цифрового середовища, підвищує ефективність виявлення інцидентів і створює основу для обґрунтованих управлінських рішень навіть за умови обмежених ресурсів. Ефективність кіберзахисту освітнього середовища визначається не лише наявністю технологічних рішень, а й обґрунтованим вибором методів моніторингу й аналізу кіберзагроз та організацією процесів їхнього застосування в режимі реального часу. Для закладів освіти з великою кількістю користувачів і динамічними сценаріями взаємодії важливим є поєднання різних методів моніторингу, що забезпечують своєчасне виявлення інцидентів без порушення стабільності освітніх сервісів. У практиці захисту кібербезпеки освітніх установ застосовуються взаємодоповнювальні методи моніторингу, що відрізняються рівнем втручання в роботу систем і глибиною аналізу подій (табл. 4).

Таблиця 4

Основні методи моніторингу кіберзагроз в освітньому середовищі

Метод	Характеристика	Практичне значення для освіти
Пасивний моніторинг	Аналіз логів, мережевого трафіку та системних подій без втручання в роботу цільових систем	Безперервний контроль без негативного впливу на стабільність навчальних платформ
Активний моніторинг	Сканування мережі, перевірка конфігурацій і вразливостей інфраструктури	Виявлення слабких місць за умови обмеженого та контрольованого застосування
Подієвий моніторинг	Аналіз журналів автентифікації, доступу та системних подій за допомогою SIEM-систем	Основа для оперативного виявлення спроб несанкціонованого доступу та інших інцидентів
Мережевий моніторинг	Аналіз мережевих потоків (NetFlow, sFlow, IPFIX) та пакетного трафіку	Виявлення DDoS-атак і аномального навантаження та несанкціонованої передачі даних
Моніторинг доступу	Контроль входів, пристроїв і часових патернів учасників освітнього процесу	Виявлення компрометації облікових записів і внутрішніх зловживань
Поведінковий аналіз (UEBA)	Виявлення відхилень від встановленої нормальної поведінки	Ідентифікація складних і раніше невідомих загроз

Джерело: сформовано авторами

Моніторинг кіберзагроз у режимі реального часу реалізується як послідовний процес, що охоплює фіксацію подій сенсорами, централізований збір і кореляцію даних, виявлення аномалій та оперативне реагування на інциденти. У разі перевищення порогових значень або ідентифікації підозрілої активності система формує сповіщення та ініціює автоматизовані або напівавтоматизовані дії, що дає змогу мінімізувати вплив інцидентів і забезпечити безперервність освітнього процесу.

Для підвищення ефективності аналізу кіберзагроз у системах моніторингу застосовуються сигнатурний, кореляційний і поведінковий аналіз, а також sandbox-дослідження підозрілих об'єктів. Доповнення SIEM-платформ даними з Threat Intelligence Platforms (TIP) забезпечує контекстуалізацію подій і проактивний характер кіберзахисту, що є важливим для закладів освіти.

Упровадження систем моніторингу кіберзагроз в освітніх закладах є управлінським процесом, що охоплює стратегічний, тактичний та операційний рівні й потребує чіткого розподілу відповідальності (табл. 5).

Таблиця 5

Рівні управління та відповідальність у сфері кібермоніторингу

Рівень	Основні функції
Стратегічний	Визначення кібербезпеки як пріоритету, формування та затвердження політик, ресурсне забезпечення
Тактичний	Вибір оптимальних технологій, планування впровадження системи, встановлення KPI ефективності захисту
Операційний	*Щоденний моніторинг, оперативне реагування на інциденти, контроль виконання процедур кіберзахисту*

Джерело: *сформовано авторами*

Цифрова трансформація освіти значно розширює можливості освітнього процесу, однак її ефективність безпосередньо залежить від рівня інформаційної безпеки. Стійке цифрове освітнє середовище формується на основі поєднання технологічних рішень, організаційних механізмів і розвитку цифрової культури учасників освітнього процесу. Кіберзахист у цьому контексті має розглядатися

як системна діяльність, спрямована на управління ризиками, профілактику інцидентів і гарантування безпечної поведінки користувачів.

Основним елементом такої системи є внутрішня політика кібербезпеки, що визначає правила користування цифровими ресурсами, управління обліковими записами, вимоги до захисту даних і алгоритми реагування на інциденти. Нормативна визначеність дає змогу знизити ймовірність помилок і підвищити відповідальність користувачів.

Особливу роль відіграє захист облікових записів і даних, який забезпечується багатофакторною автентифікацією, диференційованим доступом, шифруванням інформації й регулярним оновленням програмного забезпечення. Такі заходи істотно знижують ризик несанкціонованого доступу та експлуатації відомих уразливостей [4].

Не менш важливим чинником є розвиток цифрової грамотності та кібергігієни. Поінформованість щодо фішингу, соціальної інженерії та маніпулятивних практик формує здатність учасників освітнього процесу своєчасно розпізнавати загрози й запобігати їм [2, с. 38].

Системний моніторинг подій безпеки, аналіз мережевого трафіку та наявність узгоджених планів реагування дають змогу оперативно виявляти інциденти й забезпечувати безперервність роботи освітніх платформ. Додатковими елементами кіберстійкості є резервне копіювання даних, захист серверної інфраструктури та протидія шкідливому програмному забезпеченню й DDoS-атакам.

Отже, комплексне застосування організаційних, технічних і освітніх заходів формує цілісну систему кіберзахисту, здатну забезпечити стабільне та безпечне функціонування цифрового освітнього середовища.

Висновки. Дослідження встановило, що зростання рівня цифровізації освіти значно підвищує кіберризики, пов’язані з використанням освітніх платформ, мережевих сервісів і хмарної інфраструктури. За таких умов системний моніторинг та аналіз кіберзагроз є важливим інструментом забезпечення безперервності освітнього процесу.

Обґрунтовано доцільність поетапного впровадження системи моніторингу кіберзагроз у закладі освіти. Перший етап передбачає ідентифікацію критичних цифрових активів та оцінку ризиків. Другий охоплює впровадження основних засобів збору й централізації подій безпеки. Третій етап пов'язаний із застосуванням SIEM-рішень і поведінкового аналізу, а завершальний – з автоматизацією реагування на інциденти за допомогою SOAR-платформ та інструментів кіберрозвідки.

Визначено, що ефективність системи моніторингу залежить від наявності людських, фінансових і технічних ресурсів. Визначальну роль відіграють кваліфіковані фахівці з кібербезпеки, здатні здійснювати аналітичну інтерпретацію подій. Фінансові ресурси визначають вибір технологічних рішень, а технічні – можливості масштабування інфраструктури й резервного копіювання.

Запропоновано оцінювати результативність системи моніторингу за такими критеріями: час виявлення інцидентів, ефективність реагування, зменшення кількості повторних атак, стабільність роботи освітніх сервісів і відповідність внутрішнім політикам інформаційної безпеки.

З управлінського погляду доведено, що кібербезпека має розглядатися як елемент стратегічного управління закладом вищої освіти. Керівникам доцільно інтегрувати моніторинг кіберзагроз у програми цифрового розвитку, визначати відповідальних осіб та забезпечувати регулярний контроль ефективності впроваджених заходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Швардак М. В. Кібербезпека у цифровому освітньому просторі. *Науковий журнал Хортицької національної академії.* 2025. № 1(12). С. 26–33. https://journal.khnnra.edu.ua/index.php/njKhNA/article/view/233

2. Коваленко В., Осипчук Т. Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Фізико-*

математична освіта. 2024. № 39(2). С. 35–41. DOI: https://doi.org/10.31110/fmo2024.v39i2-05

3. Савченко В., Маклюк О. Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство.* 2024. № 60. DOI: https://doi.org/10.32782/2524-0072/2024-60-24

4. Bakhmat N., Popadych O., Derkach L., Shvardak M., Lukashchuk M., Romanenko V. Using Information Technologies to Train Today Teachers in the Educational Environment. *Revista Romaneasca Pentru Educatie Multidimensionala.* 2022. Vol. 14(2). P. 479–499. DOI: https://doi.org/10.18662/rrem/14.2/591

5. Павлюк Б. В., Розпутня Б. М., Кисліцин В. В. Комплексні системи захисту інформації в освітніх закладах : сучасні технологічні рішення та перспективи впровадження. *Педагогічна Академія : наукові записки.* 2024. № 7. DOI: https://doi.org/10.57125/pedacademy.2024.06.29.10

6. Standardization in the Field of Cybersecurity and Cyber Protection in Ukraine / M. Pleskach et al. *Information & Security: An International Journal*. 2020. Vol. 45. P. 57–76. URL: https://doi.org/10.11610/isij.4504 (date of access: 18.12.2025).

7. Pchelina O. V., Skulysh Y. D., Buglak I., Myroniuk R. V. Experiencia internacional en garantizar la ciberseguridad en el país y posibilidad de aplicarla en Ucrania. *DIXI*. 2021. Vol. 23. No. 2. P. 1–16. DOI: https://doi.org/10.16925/2357-5891.2021.02.01

8. Penchev G., Shalamanov V. Governance consulting services and tools: Governance model design for collaborative networked organisations in the cyber domain. *Information & Security: An International Journal*. 2022. Vol. 53. No. 1. P. 147–160. DOI: https://doi.org/10.11610/isij.5310

9. Chowdhury N., Gkioulos V. Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*. 2021. Vol. 40. P. 100361. DOI: https://doi.org/10.1016/j.cosrev.2021.100361

10. Maglaras L., Janicke H., Ferrag M. A. Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*. 2022. Vol. 22, no. 14. P. 5105. DOI: https://doi.org/10.3390/s22145105

11. Aaltola K., Ruoslahti H. Societal Impact Assessment of a Cyber Security Network Project. *Information & Security: An International Journal*. 2020. Vol. 46, no. 1. P. 53–64. URL: https://doi.org/10.11610/isij.4604 (date of access: 18.12.2025).

12. Goethem E. V., Easton M. Public-Private Partnerships for Information Sharing in the Security Sector: What's in It for Me?. *Information & Security: An International Journal*. 2021. Vol. 48. P. 21–35. URL: https://doi.org/10.11610/isij.4809 (date of access: 18.12.2025).

13. Penchev G., Shalamanova-Filipova A. A Governance Model for an EU Cyber Security Collaborative Network – ECSCON. *Information & Security: An International Journal.* 2020. Vol. 46. No. 1. P. 99–113. DOI: https://doi.org/10.11610/isij.4607

14. Юскович-Жуковська В. І., Соловей Л. Я., Лотюк Ю. Г., Близнюк С. В. Формування безпекового цифрового освітнього середовища. *Вісник Міжнародного економіко-гуманітарного університету імені Академіка Степана Дем'янчука.* 2025. № 2. С. 208–213. DOI: https://doi.org/10.32782/3041-2021/2025-2-31

15. 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

REFERENCES

1. Shvardak, M. V. (2025). Cybersecurity in the digital educational space [Kiberbezpeka u tsyfrovomu osvitnomu prostori]. *Scientific Journal of the Khortytsia National Academy*, *1*(12), 26–33. https://doi.org/10.51706/27073076-2025-12-2 [in Ukrainian].

2. Kovalenko, V., & Osypchuk, T. (2024). The problem of developing teachers digital competence in cybersecurity in general secondary education institutions [Problema rozvytku tsyfrovoi kompetentnosti z kiberbezpeky vchyteliv zakladiv zahalnoi serednoi osvity]. *Physical and Mathematical Education*, *39*(2), 35–41. https://doi.org/10.31110/fmo2024.v39i2-05 [in Ukrainian].

3. Savchenko, V., & Makliuk, O. (2024). Cybersecurity as a factor of the effectiveness of higher education institutions [Kiberbezpeka yak faktor efektyvnosti funktsionuvannia zakladiv vyshchoi osvity]. *Economics and Society*, *60*. https://doi.org/10.32782/2524-0072/2024-60-24 [in Ukrainian].

4. Bakhmat, N., Popadych, O., Derkach, L., Shvardak, M., Lukashchuk, M., & Romanenko, V. (2022). Using information technologies to train today teachers in the educational environment. *Revista Romaneasca Pentru Educatie Multidimensionala*, *14*(2), 479–499. https://doi.org/10.18662/rrem/14.2/591

5. Pavliuk, B. V., Rozputnia, B. M., & Kyslytsyn, V. V. (2024). Complex information security systems in educational institutions: Modern technological solutions and prospects [Kompleksni systemy zakhystu informatsii v osvitnikh zakladakh: Suchasni tekhnolohichni rishennia ta perspektyvy vprovadzhennia]. *Pedagogical Academy: Scientific Notes*, *7*, 1–17. https://doi.org/10.57125/pedacademy.2024.06.29.10 [in Ukrainian].

6. Pleskach, M., Pleskach, V., Semenchenko, A., Myalkovsky, D., & Stanislavsky, T. (2020). Standardization in the field of cybersecurity and cyber protection in Ukraine. *Information & Security An International Journal*, *45*, 57–76. https://doi.org/10.11610/isij.4504

7. Pchelina, O. V., Skulysh, Y. D., Buglak, I., & Myroniuk, R. V. (2021). Experiencia internacional en garantizar la ciberseguridad en el país y posibilidad de aplicarla en Ucrania. *DIXI*, 23(2), 1–16. https://doi.org/10.16925/2357-5891.2021.02.01

8. Penchev, G., & Shalamanov, V. (2022). Governance consulting services and tools: Governance model design for collaborative networked organisations in the cyber domain. *Information & Security An International Journal*, *53*, 147–160. https://doi.org/10.11610/isij.5310

9. Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

10. Maglaras, L., Janicke, H., & Ferrag, M. A. (2022). Cybersecurity of Critical Infrastructures: Challenges and Solutions. *Sensors*, *22*(14), 5105. https://doi.org/10.3390/s22145105

11. Aaltola, K., & Ruoslahti, H. (2020). Societal impact assessment of a cyber security network project. *Information & Security An International Journal*, *46*(1), 53–64. https://doi.org/10.11610/isij.4604

12. Van Goethem, E., & Easton, M. (2021). Public-private partnerships for information sharing in the security sector: What's in it for me? *Information & Security An International Journal*, *48*, 21–35. https://doi.org/10.11610/isij.4809

13. Penchev, G., & Shalamanova, A. (2020). A Governance Model for an EU Cyber Security Collaborative Network – ECSCON. *Information & Security: An International Journal*, *46*(1), 99–113. https://doi.org/10.11610/isij.4607

14. Yuskovych-Zhukovska, V. I., Solovei, L. Ya., Lotiuk, Yu. H., & Blyzniuk, S. V. (2025). Formuvannia bezpekovoho tsyfrovoho osvitnoho seredovyshcha [Formation of a secure digital educational environment]. *Visnyk Mizhnarodnoho ekonomiko-humanitarnoho universytetu imeni Akademika Stepana Demianchuka*, *2*, 208–213. https://doi.org/10.32782/3041-2021/2025-2-31 [In Ukrainian].

15. Trofymenko, O. H., Lohinova, N. I., Manakov, S. Yu., & Dubovoi, Ya. V. (2022). Kiberzahrozy v osvitnomu sektori [Cyber threats in the educational sector]. *Kiberbezpeka: osvita, nauka, tekhnika*, *4*(16), 76–84. https://doi.org/10.28925/2663-4023.2022.16.7684 [In Ukrainian].

Стаття надійшла до редакції 03.11.2025