DOI: https://doi.org/10.32782/2308-1988/2025-53-83
УДК 004.65.056:330.3

Синицький Ростислав Костянтинович
аспірант,
асиситент кафедри інформаційних систем в економіці,
Київський національний економічний університет імені Вадима Гетьмана
ORCID: https://orcid.org/0009-0002-6271-3041

Synytskyi Rostyslav
Kyiv National Economic University named after Vadym Hetman

ЦИФРОВА ГІГІЄНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА В ЦИФРОВІЙ ОСВІТНІЙ ДІЯЛЬНОСТІ

DIGITAL HYGIENE AND INFORMATION SECURITY IN SCOPE OF DIGITAL EDUCATIONAL ACTIVITIES

Анотація. Публікацію присвячено основним теоретичним та методологічним основам цифрової гігієни та інформаційної безпеки у сфері цифрової освітньої діяльності. Підкреслено тенденцію до збільшення кібератак на освітній сектор. Виявлено, що через значно більшу чисельність студентів порівняно з викладачами, саме вони є найбільш вразливими до атак і часто стають інструментами для розповсюдження шкідливого програмного забезпечення. Особливу увагу приділено проблематиці наявності ефективних методів та засобів забезпечення цифрової гігієни та інформаційної безпеки як для платформ дистанційного навчання, так і для викладацько-наукової діяльності. Окреслено необхідні кроки для подальшого поглибленого вивчення цієї теми, включаючи розробку нових методів захисту, проведення систематичного навчання студентів і викладачів щодо безпечної поведінки в цифровому середовищі та розширення нормативно-правової бази для ефективного управління інформаційною безпекою в освітньому секторі.
Ключові слова: цифрова гігієна, інформаційна безпека, дистанційне навчання, кіберзагрози, шкідливе програмне забезпечення, штучний інтелект, освітні платформи.

Summary. This publication outlines the main theoretical and methodological foundations of digital hygiene and information security for both teachers and students in the field of digital educational activities. In today's digital transformation of education, every participant in the educational process must be confident in the security of the platforms and methods of distance learning used by higher education institutions. Given the trend towards an increase in cyberattacks on the education sector, information protection is a critically important aspect of university activities. Students are the basis of the existence of teaching activities in higher education institutions, because without them the educational process is impossible, however, due to the significantly larger number of students compared to teachers, they are the most vulnerable to attacks and often become tools for the distribution of malicious software. The main targets of attackers remain teachers and administrative staff of higher education institutions, since it is they who have access to important data, educational process management systems, financial resources and scientific developments. Particular attention is paid to the issue of the availability of effective methods and means of ensuring digital hygiene and information security for both distance learning platforms and teaching and research activities. Failures or suspension of activities in this area can cause both significant financial and reputational losses for a higher education institution. Loss or compromise of scientific data can significantly affect the competitiveness of a university both at the national and international levels. In the context of modern digital threats, the implementation of advanced technologies, including artificial intelligence, to ensure security and automate threat monitoring is important. The use of machine learning algorithms allows you to detect anomalous activity in educational systems, prevent potential attacks and respond promptly to incidents. The necessary steps are outlined for further in-depth study of this topic, including the development of new protection methods, systematic training of students and teachers on safe behavior in the digital environment, and expansion of the regulatory framework for effective information security management in the education sector.
Keywords: digital hygiene, information security, distance learning, cyber threats, malware, artificial intelligence, educational platforms.

Постановка проблеми. Тема інформаційної безпеки та цифрової гігієни є надзвичайно актуальною сьогодні, адже соціальна інженерія є майже основним методом отримання незаконного доступу до ресурсів, адже це набагато простіше і з точки фінансових і часових затрат на підготовку, організацію та проведення атаки. Наявні методи вимагають фундаментальних змін у розробці

мережевої безпеки, що вимагає серйозних оновлень інфраструктури, та є дорогим і трудомістким процесом. Крім того, суворий контроль доступу іноді може перешкоджати продуктивності та співпраці користувачів, особливо в академічному середовищі, яке покладається на відкритий доступ до ресурсів. В освітньому середовищі, легкість доступу має серйозний вплив, адже сувора політика архітектури нульової довіри може перешкоджати безперебійній співпраці між студентами, викладачами та дослідниками. Постійні зусилля щодо вирішення нових викликів і узгодження з глобальними стандартами підкреслюють необхідність захисту інформації в епоху цифрових технологій, проте незважаючи на потужну законодавчу та інституційну базу, Україна стикається з проблемами практичної реалізації заходів інформаційної безпеки, адже швидкий технологічний прогрес, кіберзагрози, що розвиваються, і необхідність постійного нарощування потенціалу вимагають постійних реформ.

Аналіз останніх досліджень та публікацій. Питання цифрової гігієни та інформаційної безпеки в цифровій освітній діяльності було висвітлено у роботі Бурова О., Бутнік-Сіверського О., Орлюк О., та Горської К. [1], де яскраво висвітлені питання кібербезпеки та цифрової гігієни в освітньому процесі, підкреслюючи, що традиційні підходи інколи не здатні виявляти та протидіяти новим складним атакам. Проте Бікулов Т.Д. [2], підкреслює що, незважаючи на переваги електронного навчання, освітній сектор стикається з численними кіберзагрозами, такими як атаки відмови в обслуговуванні, програми-вимагачі та фішингові атаки. У статті аналізуються такі ризики та пропонуються методи захисту для освітніх установ.

Також у звіті Check Point Software Technologies [3] чітко окреслено, що саме університети та заклади вищої освіти стають основними цілями для зростаючого хактивізму в світі за останні кілька років. Проте в звіті ENISA [4] чітко визначено недостатнє врахування людського фактору, адже більшість наявних методів протидій загрозам зосереджені на технічних аспектах атак, однак соціальна інженерія залишається одним із найефективніших методів.

Згідно з дослідженням Palo Alto Networks, 2023 [5], 80% атак на хмарні середовища відбувається через неправильно налаштовані системи безпеки або неналаштовані доступи до хмари самим користувачем, а отже крадіжка облікових даних адміністратора системи Moodle та маніпуляції з API для отримання доступу до даних інших користувачів сайту університету будуть менш ймовірними і їх вагові коефіцієнти будуть меншими ніж у експлуатації вразливостей контейнеризації.

Метою статті є дослідження і аналіз ефективності різних існуючих імплементованих підходів до захисту систем дистанційного навчання через оцінку сучасних загроз для цифрової освітньої діяльності в Україні.

Виклад основного матеріалу дослідження. Загальноприйняте поняття «інформаційна безпека» охоплює майже все що стосується захисту інформаційних систем і даних від несанкціонованого доступу, розголошення, зміни та знищення. В Україні рамки, як поняття, так і поле дії інформаційної безпеки визначаються поєднанням національного законодавства, міжнародних угод, нормативних актів, тощо. Вітчизняний підхід до інформаційної безпеки характеризується комплексною законодавчою базою, чітким визначенням ключових понять, спеціальним інституційним наглядом та активною залученістю до міжнародного співробітництва.

Ратифікація CETS 108 свідчить про прагнення вітчизняних експертів привести систему захисту даних у відповідність до європейських стандартів, що сильно сповільнює темпи розвитку атак. Крім того, тривають зусилля щодо гармонізації законодавства з Загальним регламентом захисту даних Європейського Союзу з метою покращення механізмів захисту персональних даних користувачів різних систем державного рівня, таких як Дія та сприяння міжнародній співпраці. Окрім законодавчої фрагментації, держава стикається зі значними перешкодами в практичній реалізації та забезпеченні своєї політики інформаційної безпеки, адже, наприклад, органи, відповідальні за нагляд за інформаційною безпекою, такі як Державна служба спеціального зв'язку та захисту інформації та Група реагування на комп'ютерні надзвичайні ситуації України (CERT-UA) [6], часто працюють з обмеженими ресурсами та повноваженнями, і це сильно впливає на їх здатність ефективно реагувати на інциденти інформаційної безпеки.

Ефективна інформаційна безпека часто вимагає тісної співпраці між державними установами та організаціями приватного сектору. Наразі такій співпраці заважає відсутність чітких рамок і довіри між цими секторами, що призводить до фрагментарних зусиль у вирішенні питань пов'язаних з інформаційною безпекою. Як в державному так і в приватному секторах бракує кваліфікованих фахівців з кібербезпеки, що дуже яскраво видно через вплив такого фактору на здатність ефективно впроваджувати та контролювати заходи безпеки, роблячи системи, що і так в де-яких випадках, не мали потрібного рівню захисту, ще більш вразливими до атак. Станом на сьогодні, ні законодавство, ні політики безпеки, ні технічні навички спеціалістів державних установ часто не встигають за витонченістю та частотою кібератак.

Реалізація регулярних навчальних програм семінарів та інформаційних кампаній у державному секторі, зокрема і в закладах вищої освіти,

забезпечить озброєння персоналу найновішими знаннями та навичками для боротьби з новими загрозами. Крім того, створення механізмів для періодичного перегляду та оновлення політик і процедур безпеки дозволить організаціям активно адаптуватися до мінливого середовища загроз, а також, можна включити проведення регулярних перевірок з цифрової гігієни та інформаційної безпеки, моделювання кіберінцидентів, тобто проведення пентесту і сприяння створенню середовища, у якому відгуки та отримані уроки систематично інтегруються в практику. Для державного сектору, зокрема для середовищ навчання, як наприклад у закладах вищої освіти це була б одна із найкращих практик попередження втручанню у роботу внутрішніх систем.

Кібератаки на сектор освіти різко зросли в останні роки, що підкреслює критичну важливість надійних заходів захисту інформації в університетах. Студенти, як найбільша група осіб, що є основою у вищих навчальних закладах, особливо сприйнятливі до кіберзагроз і можуть ненавмисно стати каналом розповсюдження зловмисного програмного забезпечення. Проте, викладачі та адміністративний персонал, які мають доступ до конфіденційних даних та інституційних ресурсів, залишаються основними цілями для атак. У 2023 році сектори освіти та досліджень зазнавали в середньому близько 1800 кібератак на тиждень, що на 258% більше, ніж у попередньому році. Варто відзначити, що 1537 із цих інцидентів призвели до витоку конфіденційних даних, що відображає приголомшливе зростання випадків витоку даних на 546% [7]. Цей сплеск витоку даних дуже яскраво підкреслює вразливість освітнього сектору до діяльності кіберзлочинців, та зростаючу некомпетентність персоналу закладів освіти до навичок цифрової гігієни.

Атаки програм-вимагачів набули особливого поширення [7–11]. У 2023 році кількість відомих атак програм-вимагачів націлених на вищі навчальні заклади по всьому світі зросла більш ніж удвічі, збільшившись зі середнього показника у 129 інцидентів у 2022 році до 265. Зокрема, вищі навчальні заклади спостерігали зростання кількості атак на 70% з ескалацією з середнього показника у 68 у 2022 році до 116 у 2023 році. Ці цифри, ймовірно, недооцінюють справжні масштаби, оскільки вони враховують лише випадки, коли викупи не були сплачені, адже більшість атакованих воліють не розголошувати подібні інциденти для попередження репутаційних втрат [12]. Студенти представляють значну вразливість у системі кібербезпеки університету. Широке використання ними персональних пристроїв і взаємодія з різними онлайн-платформами підвищує ризик ненавмисного використання шкідливого програмного забезпечення всередині захищеної мережі закладу освіти. Децентралізований характер діяльності студентів ускладнює застосування єдиних статичних протоколів безпеки, що ускладнює ефективне зниження цих ризиків. Викладацький та адміністративний персонал також є головною мішенню через їхній доступ до критично важливих даних внутрішніх систем, включаючи результати досліджень, фінансові записи та особисту інформацію студентів і співробітників. Кіберзлочинці часто використовують фішингові атаки, що є частиною атак соціальної інженерії, щоб отримати можливість використати доступ рівня викладача.

Фінансові наслідки цих кібератак значні [13]. Порушення процесу роботи в освітніх установах коштували країнам Європи та США у середньому майже 4 мільйони доларів у 2023 році, охоплюючи витрати, пов’язані з відновленням системи, судові збори, регуляторні штрафи та шкоду репутації. Крім того, саме через програми-вимагачі, що могли бути завантажені випадково або примусово під дією шантажу, призвели до значних збоїв у роботі, адже середній час простою закладів становив 12,6 навчальних днів у 2023 році проти 8,7 днів у 2021 році [14]. Мотиви атакуючих нестатичні, адже навчальні заклади зберігають величезну кількість конфіденційних даних, зокрема персональну інформацію та цінну інтелектуальну власність, що робить їх привабливими цілями. Відкритий і спільний характер академічних середовищ, що характеризується широким доступом до безпровідних мереж і різноманітною базою користувачів, ще більше посилює їхню вразливість.

Зміна поточних та розробка із подальшим впровадженням надійних механізмів реагування на інциденти має можливість мінімізувати вплив кібератак на системи віддаленого навчання. Встановлення чітких протоколів для виявлення інцидентів безпеки, звітування та реагування на них, а також створення спеціальних груп реагування на інциденти з визначеними ролями та відповідальністю забезпечить скоординований та ефективний підхід до управління подіями кібербезпеки. Також гарним рішенням буде проведення регулярних тренувань та моделювання атак, щоб перевірити ефективність цих протоколів і визначити області для вдосконалення. Саме в таких випадках співпраця з міжнародними організаціями з кібербезпеки може надати доступ до додаткових ресурсів і досвіду під час тестів або реальних інцидентів. Впровадження підходів, орієнтованих на оцінку ризику, є важливим кроком у забезпеченні ефективної інформаційної безпеки, оскільки дозволяє визначати пріоритетність ресурсів та зусиль на основі потенційних загроз і вразливостей. Комплексна оцінка ризиків дає змогу організаціям ідентифікувати критично важливі активи, аналізувати ймовірність загроз і оцінювати їх потенційний вплив. Це дозволяє впроваджувати ефективні

механізми контролю, адаптовані до конкретних потреб і контексту організації або закладу освіти.

Одним із ключових аспектів забезпечення безпеки є посилення контролю за ланцюгами поставок, оскільки сучасні організації дедалі частіше залежать від сторонніх постачальників і партнерів та їх програмного забезпечення. Впровадження суворих вимог безпеки для всіх учасників ланцюга постачання, проведення регулярних перевірок та укладання контрактів із чітко визначеними заходами безпеки допоможуть мінімізувати потенційні загрози. Гарантія того, що всі залучені сторони відповідають національним та міжнародним стандартам інформаційної безпеки, знижує ризик компрометації інформаційних активів через зовнішніх партнерів. Використання передових технологій шифрування, ефективних механізмів контролю доступу та стратегій запобігання втраті даних сприятиме забезпеченню конфіденційності, цілісності та доступності інформації. Регулярний моніторинг і проведення аудитів обробки даних дозволять вчасно виявляти потенційні загрози та забезпечувати дотримання високих стандартів безпеки.

Не менш важливим напрямом розвитку є інвестиції в освіту з кібербезпеки та підготовку кваліфікованих спеціалістів, оскільки нестача фахівців у цій сфері є серйозною перешкодою для ефективного захисту інформаційних систем. Запровадження спеціалізованих навчальних програм у вищих навчальних закладах і технічних інститутах сприятиме формуванню нового покоління експертів, здатних ефективно реагувати на сучасні кіберзагрози. Інтеграція основ кібербезпеки в загальноосвітні програми допоможе підвищити цифрову грамотність громадян та сприятиме формуванню культури безпечної поведінки в кіберпросторі.

На еволюцію та адаптацію моделей безпеки в цифровій освітній діяльності суттєво вплинули технологічний прогрес, нові кіберзагрози та зміна нормативного середовища. З часом традиційні моделі безпеки змінились, щоб адаптуватись до зростаючої складності цифрових освітніх екосистем, включаючи хмарні навчальні платформи, інфраструктури віддаленого доступу та навіть найновіші освітні інструменти на основі штучного інтелекту. Короткострокова еволюція цих моделей особливо очевидна у відповідь на серйозні інциденти кібербезпеки, глобальні кризи та швидкий перехід до онлайн-освіти враховуючи глобальні події на кшталт пандемії.

Розробка комплексної Національної стратегії кібербезпеки з чіткими цілями та показниками ефективності є важливою умовою для системного підходу до кіберзахисту. Ця стратегія повинна включати механізми оцінки ризиків, визначати відповідальні органи, встановлювати конкретні ініціативи та показники ефективності для різних секторів економіки та державного управління. Важливою складовою стратегії має бути механізм постійного оновлення та адаптації до нових загроз, що забезпечить її актуальність у динамічному середовищі кіберзагроз. Регулярні оцінки ефективності заходів та навчання персоналу мають стати обов'язковими для всіх державних установ і критичних інфраструктур.

Зростання ролі навчання з питань кібербезпеки в моделях стратегії безпеки свідчить про ще один важливий еволюційний розвиток. У той час як попередні моделі безпеки зосереджувались насамперед на технічному контролі, зараз установи визнають критичну роль людського фактору в кібербезпеці. Програми підвищення обізнаності в кіберпросторі та кібергігієни були інтегровані в стратегії безпеки, щоб навчити студентів, викладачів і адміністративний персонал найкращим практикам виявлення та зменшення впливу кіберзагроз. Навчальні програми наголошують на необхідності розвивати навички безпечного вебперегляду, безпечного користування електронною поштою, обізнаності про фішинг і безпечному керуванні паролями. Зміцнюючи культуру кібербезпеки в навчальних закладах, підвищення обізнаності зменшує ймовірність людських помилок та шансів на успіх атак соціальної інженерії, що сприяють порушенням безпеки.

Прийняття моделей безпеки на основі блокчейну після росту та розповсюдження криптовалюти стало багатообіцяючим нововведенням у захисті цифрових освітніх записів і облікових даних. До прикладу, традиційні системи баз даних вразливі до підробки даних і несанкціонованих змін, коли технологія Blockchain забезпечує децентралізований і захищений від несанкціонованого втручання механізм для зберігання академічних облікових даних, сертифікатів і цифрових ідентифікаторів. Навчальні заклади потроху починають досліджувати блокчейн-рішення для безпечної перевірки даних, гарантуючи автентичність і цілісність академічних записів. Education Blockchain Initiative активно досліджує застосування технології розподіленого реєстру для підвищення інформаційної безпеки в освітніх системах [15].

На короткострокову еволюцію моделей безпеки також вплинуло зростання проблем кіберфізичної безпеки в навчальних закладах. Із поширенням пристроїв Інтернету речей у розумних класах стратегії безпеки тепер включають також необхідність забезпечення безпеки для Інтернету речей для запобігання несанкціонованому доступу до підключених пристроїв. Розумні дошки, інтерактивні засоби навчання та системи спостереження вимагають надійних механізмів безпеки для запобігання потенційним вторгненням. IoT Security Foundation (IoTSF) [16] розробили інструкції щодо захисту підключених освітніх пристроїв,

наголошуючи на сегментації мережі, оновлення мікропрограми та автентифікації пристроїв.

Іншим новим адаптивним механізмом у моделях безпеки є застосування методів гейміфікації для покращення навчання та підвищення обізнаності з кібербезпеки [17–18]. Навчання з кібербезпеки, як наприклад змагання із захоплення прапора і навчальні програми на основі моделювання мають бути інтегровані в стратегії безпеки, щоб залучити користувачів до активного навчання.

Новий час диктує нові умови, тому новим підходом стали моделі безпеки на основі штучного інтелекту, які використовують машинне навчання та аналіз даних для прогнозування та запобігання кіберзагрозам. Подібні моделі аналізують величезні обсяги даних безпеки, виявляють аномальну поведінку та автоматизують реагування для зменшення ризиків [19]. Такі моделі, керовані штучним інтелектом, особливо корисні у великих або надвеликих навчальних закладах, де є пряма нестача персоналу, а відповідно й ручного моніторингу безпеки теж недостатньо для боротьби зі зростаючим обсягом кіберзагроз. Системи безпеки, під управлінням штучного інтелекту, такі як аналітика поведінки користувачів і автоматизовані платформи реагування на інциденти, пропонують проактивний захист, виявляючи загрози та реагуючи на них у реальному часі [20].

Хоча ці моделі є багатообіцяючими, вони не позбавлені проблем. Системи штучного інтелекту потребують величезних обсягів навчальних даних для ефективного функціонування, а помилки в навчальних наборах даних можуть призвести до помилкових позитивних або негативних результатів, що знижує загальну надійність. Інше серйозне занепокоєння викликає маніпулювання навчанням штучного інтелекту, коли зловмисники маніпулюють моделями штучного інтелекту, вводячи оманливі або шкідливі дані. Кіберзлочинці можуть використовувати слабкі місця в алгоритмах штучного інтелекту, або логічні парадокси, щоб уникнути виявлення, роблячи автоматизований захист неефективним. Крім того, рішення безпеки на основі штучного інтелекту потребують значних інвестицій у обчислювальну потужність та інфраструктуру, що може бути неможливим для багатьох навчальних закладів.

Нажаль ефективність цих моделей обмежена складністю взаємодій у реальному світі, адже зрозуміло, що зловмисники не завжди поводяться раціонально, і непередбачувані загрози можуть використовувати невідомі вразливості у спосіб, який не вдається передбачити математичними моделями. До прикладу, теорія ігор також вимагає великих даних і досвіду моделювання, що ускладнює її ефективне впровадження для неспеціалізованих установ. Крім того, довіра до ймовірнісних результатів може призвести до неправильних рішень щодо безпеки, якщо базові припущення є помилковими або якщо ландшафти загроз неочікувано змінюються.

Моделювання сценаріїв атак є невід'ємною складовою сучасної стратегії кібербезпеки, що дозволяє організаціям передбачати, оцінювати та нейтралізувати потенційні загрози. Цей процес включає створення детальних моделей можливих атак, що допомагає виявити вразливості та розробити ефективні заходи захисту. Варто детальніше розглянути ключові аспекти моделювання сценаріїв атак, методології, що використовуються, та їх значення для забезпечення інформаційної безпеки організацій.

За допомогою моделювання різних випадків, для системи підтримки прийняття рішень можна створити різні результати. Наприклад, надавши випадково або спеціально неправильні дані, можна ідентифікувати в системі неточність та виключити її з загального аналізу. Проте, інколи вагові коефіцієнти можуть змінюватись, як наприклад при процесі моделюванні сценаріїв атак. Нова, або раніше не відома вразливість може сильно змінити показники. Процес моделювання сценаріїв атак в більшості випадків включає в себе наступні етапи:

1. Ідентифікація критичних ресурсів та систем;
2. Виявлення потенційних загроз;
3. Виявлення джерел загроз;
4. Розробка сценаріїв атак;
5. Очікувані наслідки;
6. Оцінка ймовірності реалізації кожного сценарію;
7. Потенційні втрати або вплив;
8. Визначення методів захисту для запобігання або мінімізації впливу.

Фактично, пункти від першого до сьомого є суто теоретичним для системи підтримки прийняття рішення, адже вони не є результатом її роботи, а тільки вхідними даними. Нажаль, навіть при зборі та обробці такої інформації може виникати помилка за людським фактором, адже саме проблемою при прийнятті певних рішень такими системами головним чинником неточностей є потенціал людського опору автоматичному прийняттю рішень [21]. Запровадження системи підтримки прийняття рішень може викликати скептицизм серед IT-адміністраторів і викладачів, які побоюються, що автоматизовані системи переважать їх судження або логіку. Опір запровадженню системи підтримки прийняття рішень може сильно нашкодити ефективності, оскільки групи безпеки можуть ігнорувати згенеровані системою рекомендації на користь, наприклад застарілих традиційних методів прийняття рішень. Щоб вирішити цю проблему, установи повинні зосередитися на стратегіях управління змінами, наголошуючи на тому, що системи підтримки прийняття рішень служать інструментами підтримки, а не заміною людського досвіду. Найкраще, працюватимуть

гібридні підходи, які поєднують аналітику системи підтримки прийняття рішень із людським наглядом.

Існує широкий спектр інструментів та технологій, які підтримують процес моделювання сценаріїв атак, що можуть бути використані закладами вищої освіти для симуляції кібератак, та отримання командами швидкого реагування навичок захисту та реагування на інциденти, а також. Проте, окрім навичок можливо отримати комбіновані дані стосовно кібератак, що будуть наближені до реальних умов. Окрім того, дані для системи підтримки прийняття рішень та ручного розрахунку можна отримати і з систем виявлення та запобігання вторгнень, що зазвичай використовуються для моніторингу мережевого трафіку та виявлення підозрілої активності. Інструменти аналізу вразливостей, такі як сканери вразливостей, які допомагають виявляти слабкі місця в системах та додатках можуть надати, наприклад бал по шкалі CVSS, для оцінки критичності якогось вразливого модулю або частини додатку [22].

Висновки. З огляду на раніше виявлені теоретичні та правові недоліки в системі інформаційної безпеки України, було б добре реалізувати низку стратегічних рішень, спрямованих на підвищення рівня кібербезпеки країни. Такі рішення мають бути зосереджені на законодавчій консолідації, прийнятті найновіших міжнародних стандартів, зміцненні інституційної спроможності, сприянні державно-приватному партнерству та просуванні культури постійного вдосконалення серед населення.

Посилення інтеграції цифрових технологій в освітню діяльність зумовлює необхідність розробки надійних стратегій безпеки для захисту конфіденційної інформації, забезпечення цілісності системи та збереження конфіденційності користувачів. З часом можуть бути розроблені та вдосконалені різні моделі для вибору стратегій безпеки, щоб урахувати динамічний та змінний характер загроз кібербезпеці в цифровій освіті. Ці моделі повинні враховувати структуровані підходи для виявлення ризиків, впровадження заходів безпеки та оптимізації розподілу ресурсів у навчальних закладах. Вибір відповідної стратегії безпеки має вирішальне значення для балансу між безпекою, зручністю використання та ефективністю, одночасно забезпечуючи дотримання відповідних правових і нормативних вимог.

Коротке порівняння існуючих моделей безпеки в цифровій освітній діяльності демонструє необхідність багатогранного і комплексного підходу, який інтегрує управління ризиками, відповідність вимогам, технологічні інновації та рамки співпраці. У той час як традиційні моделі, такі як ISO/IEC 27001 і Defense-in-Depth, забезпечують фундаментальні принципи безпеки, нові моделі, такі як безпека на основі застосування штучного інтелекту може запропонувати інноваційне рішення для протидії сучасним кіберзагрозам. Вибір і впровадження відповідної моделі безпеки має ґрунтуватися на комплексній оцінці ризиків, потребах і вимогах відповідності, забезпечуючи безпечне та стійке цифрове освітнє середовище, проте кіберзагрози продовжують розвиватися, тож ефективність будь-яких моделей безпеки необхідно постійно оцінювати та оновлювати з певною періодичністю.

Ефективність моделей стратегії безпеки в цифровій освітній діяльності залежить від багатьох факторів, у тому числі від природи кіберзагроз, та їх напрямку, доступності інституційних ресурсів і дотримання протоколів безпеки користувачами. Хоча різні моделі пропонують структуровані підходи до зменшення ризиків, кожна з них має сильні та слабкі сторони, які впливають на їх застосування в різних освітніх середовищах, тож оцінка ефективності цих моделей вимагає всебічного аналізу результатів їх впровадження, охоплення безпеки, адаптивності та потенційних обмежень.

Список використаних джерел:

1. Burov O., Butnik-Siverskyi O., Orliuk O., Horska K. Cybersecurity and innovative digital educational environment. *Information Technologies and Learning Tools.* 2020. № 80. С. 414–430. DOI: https://doi.org/10.33407/itlt.v80i6.4159.

2. Yousif Yaseen, K. A. Digital Education: The Cybersecurity Challenges in the Online Classroom (2019–2020). *Asian Journal of Computer Science and Technology,* 2022, Vol. 11(2), Pp. 33–38. DOI: https://doi.org/10.51983/ajcst-2022.11.2.3450

3. Check Point Software Technologies. Cyber Security Report 2024. 2024, Vol1, p.50. URL: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024 (дата звернення: 25.03.2025).

4. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. 2023, pp 70–83. DOI: https://doi.org/10.2824/782573

5. Palo Alto Networks. Prisma Unit 42 Cloud Threat Research. 2023, Vol 7, pp. 4–5. URL: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research (дата звернення: 20.03.2025).

6. CERT-UA. Government Computer Emergency Response Team of Ukraine. (n.d.). URL: https://cert.gov.ua/about-us (дата звернення: 20.03.2025).

7. WatchGuard. Cyberattacks on the education sector increased by 258% last academic year. 2024. URL: https://www.watchguard.com/wgrd-news/blog/cyberattacks-education-sector-258-last-academic-year (дата звернення: 16.03.2025).

8. StateScoop. Ransomware attacks on the education sector declined in early 2024. 2024. URL: https://statescoop.com/ransomware-education-sector-decline-2024/ (дата звернення: 15.03.2025).

9. Bank of America. Cyber Attack Protection for Universities. 2024. URL: https://business.bofa.com/en-us/content/cyber-attack-protection-for-universities.html (дата звернення: 13.03.2025).

10. UpGuard. Top Cybersecurity Problems for Universities and Colleges. 2025. URL: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges (дата звернення: 16.03.2025).

11. Wired. Meet the hired guns who make sure school cyberattacks stay hidden. 2025. URL: https://www.wired.com/story/meet-the-hired-guns-who-make-sure-school-cyberattacks-stay-hidden/ (дата звернення: 16.03.2025).

12. ThreatDown. 2024 State of Ransomware in Education: 92% Spike in K-12 Attacks. 2024. URL: https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/ (дата звернення: 18.03.2025).

13. BitLyft. The Impact of Cyber Attacks on Higher Education & How to Stay Protected. 2024. URL: https://www.bitlyft.com/resources/the-impact-of-cyber-attacks-on-higher-education-how-to-stay-protected (дата звернення: 22.03.2025).

14. Cybersecurity Dive. Ransomware attacks on schools surged in 2023. 2024. URL: https://www.cybersecuritydive.com/news/ransomware-schools-2023/725808/ (дата звернення: 21.03.2025).

15. Lemoie K., & Soares L. Connected impact: Unlocking education and workforce opportunity through blockchain. American Council on Education. 2020. URL: https://ipfs.io/ipfs/QmdEnhQcWHTY4ndotRs1YRpeTdjZGAyisHz8buqfYidkP2 (дата звернення: 03.04.2025).

16. IoT Security Foundation. Securing the Internet of Things. 2023. URL: https://iotsecurityfoundation.org/best-practice-guidelines/ (дата звернення: 01.03.2025).

17. Balakrishna C. and Charlton P. Using Game-based Learning Methods to Demystify Cyber Security Concepts for Adult Learners. Proceedings of the 16th European Conference on Games Based Learning. 2022. № 16. Pp. 73–80. DOI: https://doi.org/10.34190/ecgbl.16.1.804

18. Gjertsen E. G. B., Gjære E. A., Bartnes M. and Flores W. R. Gamification of information security awareness and training. ICISSP 2017 – Proceedings of the 3rd International Conference on Information Systems Security and Privacy. SciTePress. 2017. Pp. 59–70. DOI: https://doi.org/10.5220/0006128500590070

19. Muhammadu Sathik Raja Sathik Raja M. S. The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions. *International Journal of AI, BigData, Computational and Management Studies*. 2025. No. 6(1). Pp.1–9. DOI: https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P101

20. Hussain M. J. A. Survey Based on Behavior Analysis of Artificial Intelligence Using Machine Learning Process. 2024 4th International Conference on Sustainable Expert Systems (ICSES), Kaski, Nepal. 2024. Pp. 1694–1701. DOI: https://doi.org/10.1109/ICSES63445.2024.10763264

21. Шалений В., Зеленяк В., Фадеєв О. Впровадження стратегії розвитку персоналу в умовах діджиталізації. *Modeling the Development of the Economic Systems*. 2024. № 3. С. 137–144. DOI: https://doi.org/10.31891/mdes/2024-13-18

22. Duraz R., Espes D., Francq J., Vaton S. Using CVSS scores can make more informed and more adapted Intrusion Detection Systems. *Journal of Universal Computer Science.* 2024. No. 30(9). pp. 1244–1264. DOI: https://doi.org/10.3897/jucs.131659

References:

1. Burov O., Butnik-Siverskyi O., Orliuk O., Horska K. (2020) Cybersecurity and innovative digital educational environment. *Information Technologies and Learning Tools.* No. 80. pp. 414–430. DOI: https://doi.org/10.33407/itlt.v80i6.4159

2. Yousif Yaseen, K. A. (2022) Digital Education: The Cybersecurity Challenges in the Online Classroom (2019–2020). *Asian Journal of Computer Science and Technology*, Vol.11(2), pp. 33–38. DOI: https://doi.org/10.51983/ajcst-2022.11.2.3450

3. Check Point Software Technologies. Cyber Security Report 2024. (2024). Vol1, p. 50. Available at: https://www.checkpoint.com/resources/report-3854/report--cyber-security-report-2024

4. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. (2023). Pp 70–83. DOI: https://doi.org/10.2824/782573

5. Palo Alto Networks. Prisma Unit 42 Cloud Threat Research. (2023). Vol 7, pp. 4–5. Available at: https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research

6. CERT-UA. Government Computer Emergency Response Team of Ukraine. (n.d.). Available at: https://cert.gov.ua/about-us

7. WatchGuard. Cyberattacks on the education sector increased by 258% last academic year. 2024. Available at: https://www.watchguard.com/wgrd-news/blog/cyberattacks-education-sector-258-last-academic-year

8. StateScoop. Ransomware attacks on the education sector declined in early 2024. (2024). Available at: https://statescoop.com/ransomware-education-sector-decline-2024/

9. Bank of America. Cyber Attack Protection for Universities. (2024). Available at: https://business.bofa.com/en-us/content/cyber-attack-protection-for-universities.html

10. UpGuard. Top Cybersecurity Problems for Universities and Colleges. (2025). Available at: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges

11. Wired. Meet the hired guns who make sure school cyberattacks stay hidden. (2025). Available at: https://www.wired.com/story/meet-the-hired-guns-who-make-sure-school-cyberattacks-stay-hidden/

12. ThreatDown. 2024 State of Ransomware in Education: 92% Spike in K-12 Attacks. (2024). Available at: https://www.threatdown.com/blog/2024-state-of-ransomware-in-education-92-spike-in-k-12-attacks/

13. BitLyft. The Impact of Cyber Attacks on Higher Education & How to Stay Protected. (2024). Available at: https://www.bitlyft.com/resources/the-impact-of-cyber-attacks-on-higher-education-how-to-stay-protected

14. Cybersecurity Dive. Ransomware attacks on schools surged in 2023. (2024). Available at: https://www.cybersecuritydive.com/news/ransomware-schools-2023/725808/

15. Lemoie K., & Soares L. (2020) Connected impact: Unlocking education and workforce opportunity through blockchain. American Council on Education. Available at: https://ipfs.io/ipfs/QmdEnhQcWHTY4ndotRs1YRpeTdjZGAyisHz8buqfYidkP2

16. IoT Security Foundation. Securing the Internet of Things. (2023). Available at: https://iotsecurityfoundation.org/best-practice-guidelines/

17. Balakrishna C. and Charlton P. (2022) Using Game-based Learning Methods to Demystify Cyber Security Concepts for Adult Learners. Proceedings of the 16th European Conference on Games Based Learning. No. 16. pp.73–80. DOI: https://doi.org/10.34190/ecgbl.16.1.804

18. Gjertsen E. G. B., Gjære E. A., Bartnes M. and Flores W. R. (2017) Gamification of information security awareness and training. ICISSP 2017 – Proceedings of the 3rd International Conference on Information Systems Security and Privacy. SciTePress. pp. 59–70. DOI: https://doi.org/10.5220/0006128500590070

19. Muhammadu Sathik Raja Sathik Raja M. S. (2025) The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions. *International Journal of AI, BigData, Computational and Management Studies.* No. 6(1). pp. 1–9. DOI: https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P101

20. Hussain M. J. A. (2024) Survey Based on Behavior Analysis of Artificial Intelligence Using Machine Learning Process. 2024 4th International Conference on Sustainable Expert Systems (ICSES), Kaski, Nepal. pp.1694–1701. DOI: https://doi.org/10.1109/ICSES63445.2024.10763264

21. Shalenyi V., Zeleniak V., & Fadeev O. (2024) Vprovadzhennia stratehii rozvytku personalu v umovakh didzhytalizatsii [Implementation of a staff development strategy in the context of digitalisation]. *Modeling the Development of the Economic Systems*. No. 3. pp. 137–144. DOI: https://doi.org/10.31891/mdes/2024-13-18 (in Ukrainian)

22. Duraz R., Espes D., Francq J., Vaton S. (2024) Using CVSS scores can make more informed and more adapted Intrusion Detection Systems. *Journal of Universal Computer Science.* no. 30(9). pp. 1244–1264. DOI: https://doi.org/10.3897/jucs.131659

Стаття надійшла до редакції 11.04.2025