ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

УДК 004.056.5:37.07

DOI https://doi.org/10.57125/pedacademy.2024.06.29.10

Комплексні системи захисту інформації в освітніх закладах: сучасні технологічні рішення та перспективи впровадження

Павлюк Богдан Валерійович

кандидат педагогічних наук, викладач кафедри інформатики та інформаційних технологій в освіті, Комунальний заклад вищої освіти Вінницький гуманітарно-педагогічний коледж, Україна, 21000, місто Вінниця, вул. Нагірна, 13, https//orcid.org/0000-0002-7563-9736;

Розпутня Богдан Миколайович

магістрант кафедри інноваційних та інформаційних технологій в освіті, Вінницький державний педагогічний університет імені Михайла Коцюбинського, Україна, 21001, місто Вінниця, вул. Острозького, 32, https//orcid.org/0000-0001-6344-8812;

Кисліцин Віталій Вячеславович

здобувач освіти ступеня бакалавр кафедри інноваційних та інформаційних технологій в освіті, Вінницький державний педагогічний університет імені Михайла Коцюбинського, Україна, 21001, місто Вінниця, вул. Острозького, 32, https://orcid.org/0009-0008-8986-8645.

Прийнято: 11. 06. 24 | Опубліковано: 29. 06. 24

ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

Анотація. *Мета. Дослідити сучасні технологічні рішення для комплексних систем захисту інформації в освітніх закладах та перспективи їх впровадження. Методи. У статті використані методи аналізу науково-технічної літератури, синтезу, моделювання, експертного оцінювання та систематизації для вивчення стану, тенденцій та ефективності технологічних рішень у сфері кібербезпеки освітніх установ. Результати. Проаналізовано існуючі технологічні рішення для комплексних систем захисту інформації в освітніх закладах, визначено їх переваги та недоліки. Зокрема, розглянуто використання сучасних засобів мережевого захисту, систем виявлення та запобігання вторгненням, міжмережевих екранів, антивірусного програмного забезпечення, засобів шифрування даних тощо. Визначено, що ключовими факторами забезпечення ефективності систем захисту є їх комплексність, взаємоузгодженість компонентів, гнучкість та адаптивність до постійно змінюваних кіберзагроз. Визначено ключові перспективні напрями підвищення ефективності систем захисту інформації в освітньому секторі, зокрема застосування технологій штучного інтелекту для виявлення та протидії кіберзагрозам, використання «хмарних» технологій для централізованого управління системами захисту, впровадження біометричних методів автентифікації користувачів, впровадження системи управління інцидентами кібербезпеки тощо. Проаналізовано вплив таких рішень на забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів закладів освіти. Висновки. Впровадження комплексних систем захисту інформації на основі сучасних технологічних рішень є важливим напрямом забезпечення кібербезпеки в освітніх закладах. Комплексний підхід, що поєднує технологічні, організаційні та навчальні заходи, дозволяє створити ефективну систему захисту, здатну протистояти широкому спектру кіберзагроз. Результати дослідження можуть бути використані при розробці нормативно-правового*

забезпечення, стратегій та програм кібербезпеки у сфері освіти, а також при проектуванні, впровадженні та удосконаленні систем захисту інформації в освітніх установах.

Ключові слова: *кібербезпека, освітні заклади, комплексні системи захисту інформації, технологічні рішення, впровадження.*

Integrated information security systems in educational institutions: modern technological solutions and prospects for implementation

Pavliuk Bohdan

Candidate of Pedagogical Sciences, Lecturer at the Department of Informatics and Information Technologies in Education, Vinnytsia Humanitarian and Pedagogical College, Ukraine, 21000, Vinnytsia, 13 Nahirna St., https//orcid.org/0000-0002-7563-9736;

Rozputnia Bohdan

Master's Student, Department of Innovative and Information Technologies in Education, Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University, Ukraine, 21001, Vinnytsia, 32 Ostrozkyi Str., https//orcid.org/0000-0001-6344-8812;

Kyslytsyn Vitalii

Bachelor's degree candidate, Department of Innovative and Information Technologies in Education, Mykhailo Kotsiubynskyi Vinnytsia State Pedagogical University, Ukraine, 21001, Vinnytsia, 32 Ostrozkyi Str., https://orcid.org/0009-0008-8986-8645.

ПЕДАГОГІЧНА АКАДЕМІЯ:
НАУКОВІ ЗАПИСКИ

Abstract. *The objective of this study is to examine contemporary technological solutions for integrated information security systems in educational institutions and to assess their potential for implementation.*

The study employs a multi-method approach, including analysis of scientific and technical literature, synthesis, modeling, expert evaluation, and systematization. This approach enables a comprehensive examination of the state, trends, and effectiveness of technological solutions in the field of cybersecurity of educational institutions. In particular, the use of modern network security tools, intrusion detection and prevention systems, firewalls, antivirus software, data encryption tools, etc. is considered. It is determined that the key factors in ensuring the effectiveness of protection systems are their complexity, interoperability of components, flexibility and adaptability to constantly changing cyber threats. The most promising avenues for enhancing the efficacy of information security systems in the educational sector are delineated, encompassing the deployment of artificial intelligence (AI) technologies to identify and neutralize cyber threats, the utilization of cloud computing for centralized administration of security systems, the implementation of biometric user authentication procedures, the integration of a cybersecurity incident management system, and other promising strategies. The consequences of such decisions on the confidentiality, integrity, and availability of information resources in educational institutions are analyzed. Conclusions The implementation of integrated information security systems based on contemporary technological solutions represents a pivotal area of cybersecurity in educational institutions. An integrated approach that combines technological, organizational, and educational measures allows for the creation of an effective protection system capable of withstanding a wide range of cyber threats. The findings of this study can inform the development of regulatory frameworks, strategies, and programs for cybersecurity in education. Additionally, they can be utilized in the

design, implementation, and improvement of information security systems in educational institutions.

Keywords: *cybersecurity, educational institutions, integrated information security systems, technological solutions, implementation.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями (Вступ). Забезпечення інформаційної безпеки є одним із ключових викликів для закладів освіти в сучасних умовах. Стрімкий розвиток інформаційно-комунікаційних технологій та їх широке впровадження у навчальний процес, управлінську діяльність та інфраструктуру освітніх установ створює нові можливості, але водночас породжує значні ризики. Освітні заклади стають привабливими об'єктами для кібератак та інших інформаційних загроз, спрямованих на порушення конфіденційності, цілісності та доступності даних.

Серйозна стурбованість викликають такі тенденції, як збільшення кількості витоків персональних даних учнів, студентів та співробітників, зростання числа хакерських атак на інформаційні системи закладів освіти, поширення шкідливого програмного забезпечення та несанкціонованого доступу до освітніх ресурсів. Ці проблеми здатні завдати значної шкоди іміджу, репутації та ефективній діяльності навчальних установ, а також створюють загрози для безпеки учасників освітнього процесу.

За таких умов гостро постає необхідність впровадження комплексних систем захисту інформації, які б забезпечували надійний захист інформаційних ресурсів, мінімізували ризики витоку даних та нейтралізували кіберзагрози.

Аналіз останніх досліджень і публікацій (Огляд літератури). Питання кібербезпеки та інформаційної безпеки в цілому є актуальними та постійно перебувають у фокусі уваги науковців і практиків як в Україні, так і в усьому

світі. Розвиток інформаційно-комунікаційних технологій, поширення мережі Інтернет, цифровізація усіх сфер життєдіяльності суспільства призводить до появи нових загроз інформаційній безпеці, які потребують ретельного дослідження та комплексного вирішення.

У науковій літературі значна увага приділяється теоретико-методологічним основам забезпечення інформаційної та кібербезпеки. Зокрема, Литвиненко О., Кондратов Д., Литвиненко Т., Ткачук В. [1] досліджують концептуальні засади розбудови національної системи кібербезпеки, визначають базові компоненти такої системи та шляхи її вдосконалення. Хмельовський Я., Кобзєва Т., Пащенко Ю., Баранов В. [2] аналізують міжнародний досвід правового регулювання у сфері кібербезпеки та надають рекомендації щодо адаптації відповідного законодавства в Україні.

Велика кількість публікацій присвячена розробці методів і засобів забезпечення кібербезпеки. Так, Потій О., Дорохов А., Потій К., Пономаренко Л. [3] пропонують моделі та алгоритми виявлення та протидії кіберзагрозам, а Ткачов В., Замула А., Сікірда Ю., Ткачов В. [4] досліджують можливості використання технологій штучного інтелекту для підвищення рівня кібербезпеки. Низка авторів, зокрема Борисюк З., Коноваленко І., Гребенюк А., Бояр'єв А. [5] та Шишкіна О., Доценко С., Макаренко С., Толубко В. [6], приділяють увагу питанням забезпечення безпеки критичних інформаційних інфраструктур.

Важливим напрямком досліджень також є підготовка фахівців у галузі кібербезпеки. Ряд публікацій, наприклад Глоба Л., Суліма Є., Сікірда Ю. [7] та Сидоренко В., Заїка С., Ткач М. [8], аналізують зміст та структуру освітніх програм з кібербезпеки, а також компетентності, яких мають набути майбутні фахівці.

Аналіз останніх досліджень і публікацій засвідчує значний науковий інтерес до проблематики кібербезпеки, а також наявність ґрунтовних напрацювань у цій сфері. Водночас, динамічний розвиток інформаційно-комунікаційних технологій та поява нових загроз вимагають постійного оновлення та вдосконалення теоретико-методологічних засад, методів і засобів забезпечення кібербезпеки, а також системи підготовки відповідних фахівців.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на значну кількість досліджень, спрямованих на підвищення рівня кібербезпеки в освітній сфері України, питання комплексного впровадження сучасних технологічних рішень для захисту інформації в закладах освіти залишається недостатньо вивченим. Зокрема, потребують додаткового аналізу переваги, недоліки та особливості застосування різноманітних технологічних компонентів систем кібербезпеки, а також розробки цілісної моделі їх впровадження в освітньому середовищі з урахуванням специфіки діяльності закладів та необхідності забезпечення конфіденційності, цілісності та доступності інформації.

Формулювання цілей статті (постановка завдання)

Метою даного дослідження є комплексний аналіз сучасних технологічних рішень для забезпечення кібербезпеки в освітніх закладах та розробка науково обґрунтованих рекомендацій щодо їх ефективного впровадження.

Досягнення поставленої мети передбачає вирішення наступних завдань:

•Провести аналіз існуючих технологічних рішень для комплексних систем захисту інформації в освітніх закладах, визначити їх переваги, недоліки та особливості застосування.

•Визначити перспективні напрями розвитку систем захисту інформації в освітньому секторі з урахуванням сучасних технологічних тенденцій, таких як

штучний інтелект, біометрична аутентифікація, "хмарні" обчислення, та оцінити їх потенційний вплив на підвищення ефективності систем кібербезпеки.

•Розробити рекомендації щодо нормативно-правового, організаційного та навчально-методичного забезпечення впровадження комплексних систем захисту інформації в освітніх закладах.

Дослідження в зазначених напрямах дозволить сформувати цілісний підхід до забезпечення кібербезпеки в освітній сфері, що враховує як технологічні, так і організаційні та навчальні аспекти, та сприятиме підвищенню ефективності систем захисту інформації в закладах освіти.

Виклад основного матеріалу дослідження з повним обґрунтуванням здобутих наукових результатів (Результати дослідження). Система освіти України, як і в інших країнах, активно цифровізується, що зумовлює значне розширення використання інформаційно-комунікаційних технологій (ІКТ) в освітньому процесі. Цей процес відкриває нові можливості для підвищення ефективності навчання, проте одночасно створює низку загроз інформаційній безпеці освітніх установ [9].

Згідно з дослідженнями, до основних викликів забезпеченню інформаційної безпеки в сучасних умовах можна віднести:

Збільшення кількості і складності кібератак, спрямованих на освітні заклади. Так, за даними Національного координаційного центру кібербезпеки, у 2021 році кількість кіберінцидентів в українських університетах та школах зросла на 30% порівняно з 2020 роком [10]. Освітні установи стають привабливою мішенню для хакерів через наявність значних обсягів персональних даних, навчальних матеріалів та інших цінних інформаційних ресурсів.

Ризики витоку конфіденційної інформації внаслідок використання незахищених каналів комунікації під час дистанційного навчання. Як показало

дослідження [11], 57% українських освітян використовували непрофесійні месенджери та незахищені хмарні сервіси для проведення занять онлайн, що створювало загрози витоку інформації.

Недостатній рівень цифрової компетентності та обізнаності учасників освітнього процесу щодо основ інформаційної безпеки. Ряд публікацій [12, 13] свідчить, що близько 40% викладачів та 30% здобувачів освіти в Україні мають низький рівень знань і навичок з питань кібергігієни та захисту персональних даних.

Застарілість чи відсутність комплексних систем захисту інформації в багатьох освітніх закладах. Як зазначають Хмара Л. та Гуменюк Н. [14], лише 20% українських шкіл та 30% університетів мають сучасні комплексні рішення для забезпечення інформаційної безпеки, тоді як більшість установ використовують застарілі або фрагментарні засоби захисту.

Стрімка цифровізація освіти в Україні, зростання кількості кіберзагроз, недостатній рівень ІТ-компетентностей учасників освітнього процесу та застарілість інформаційно-технологічної інфраструктури більшості навчальних закладів створюють суттєві виклики для забезпечення інформаційної безпеки системи освіти. Ці проблеми потребують термінового вирішення шляхом впровадження комплексних систем захисту інформації в освітньому секторі.

Забезпечення надійного захисту інформаційних ресурсів та даних в освітньому секторі потребує розроблення та впровадження комплексних систем інформаційної безпеки, що включають взаємопов'язані організаційні, технічні та програмні засоби. Серед основних технологічних компонентів таких систем захисту інформації в освітніх установах можна виділити засоби ідентифікації та автентифікації користувачів, зокрема, паролі, біометричні дані (відбитки пальців, сканування райдужної оболонки ока), смарт-картки тощо. Ці рішення дозволяють контролювати доступ до інформаційних систем, запобігаючи

несанкціонованому використанню даних. Важливим елементом комплексних систем інформаційної безпеки є також криптографічні засоби шифрування даних, що забезпечують конфіденційність інформації, яка передається мережами зв'язку або зберігається в інформаційних системах, з використанням сучасних алгоритмів та протоколів криптографічного захисту (AES, RSA, SSL/TLS). Окрім цього, необхідними компонентами є системи виявлення та запобігання вторгненням (IDS/IPS), які здатні своєчасно виявляти й блокувати спроби несанкціонованого доступу, атаки типу «відмова в обслуговуванні», а також інші кіберзагрози. Нарешті, важливу роль відіграє антивірусне та антималварне програмне забезпечення, інтегровані рішення з якого здатні виявляти та видаляти різні типи шкідливих програм, блокуючи їх поширення в інформаційних системах освітніх установ (Табл. 1).

Таблиця 1

Ключові технологічні компоненти комплексних систем захисту інформації в освітніх установах

Технологічний компонент	**Опис**
Засоби ідентифікації та автентифікації користувачів	Паролі, біометричні дані (відбитки пальців, сканування райдужної оболонки ока), смарт-картки тощо. Дозволяють контролювати доступ до інформаційних систем, запобігаючи несанкціонованому використанню даних.
Криптографічні засоби шифрування даних	Використання сучасних алгоритмів та протоколів криптографічного захисту інформації (AES, RSA, SSL/TLS). Забезпечують конфіденційність даних, що передаються мережами зв'язку або зберігаються в інформаційних системах.
Системи виявлення та запобігання вторгненням (IDS/IPS)	Здатні своєчасно виявляти й блокувати спроби несанкціонованого доступу, атаки типу «відмова в обслуговуванні», а також інші кіберзагрози.
Антивірусне та антималварне програмне забезпечення	Сучасні інтегровані рішення з антивірусного захисту здатні виявляти та видаляти різні типи шкідливих програм, блокуючи їх поширення в інформаційних системах освітніх установ.

Джерело: розроблено авторами на основі аналізу джерел.

Забезпечення ефективної інформаційної безпеки в сучасних освітніх установах вимагає комплексного підходу, що передбачає впровадження інтегрованих інформаційно-аналітичних систем управління безпекою. Такі системи поєднують у собі різноманітні технологічні компоненти захисту інформації, надаючи можливості для централізованого моніторингу, аналізу та управління безпековими процесами. Ключовою перевагою цих рішень є уніфікація та централізація процесів ідентифікації, автентифікації та авторизації користувачів, що дозволяє забезпечити єдині стандарти доступу до інформаційних ресурсів та систем освітніх установ. Інтегровані системи

управління безпекою також впроваджують комплексні рішення з криптографічного захисту даних, що передаються мережами та зберігаються в інформаційних системах закладів освіти. Важливою функцією таких систем є інтеграція різних засобів забезпечення інформаційної безпеки, таких як системи виявлення та запобігання вторгненням, антивірусне і антималварне програмне забезпечення, брандмауери тощо, в єдину систему моніторингу, аналізу та реагування на інциденти. Окрім цього, інтегровані системи управління безпекою надають можливості для збору, агрегації та аналітичної обробки даних щодо інцидентів, загроз та вразливостей, а також формування звітності та рекомендацій для вдосконалення заходів інформаційної безпеки. Ще однією важливою функцією є забезпечення централізованого управління політиками інформаційної безпеки, оновленням програмного забезпечення, конфігурацією та оновленням засобів захисту. Впровадження таких інтегрованих інформаційно-аналітичних систем управління безпекою дозволяє освітнім установам підвищити ефективність захисту своїх інформаційних ресурсів та даних, оптимізувати витрати на забезпечення інформаційної безпеки, а також отримати всебічну видимість щодо кіберзагроз та інцидентів.

Ефективне функціонування комплексних систем захисту інформації в освітніх установах вимагає приділення значної уваги не лише технологічним компонентам, але й відповідному організаційно-правовому забезпеченню та кадровому супроводу.

В організаційно-правовому аспекті важливим є наявність у закладі освіти розробленої та затвердженої політики інформаційної безпеки, що визначає ключові принципи, процеси та процедури забезпечення захисту інформаційних ресурсів. Така політика повинна бути гармонізована із загальною політикою закладу, а також відповідати вимогам чинного законодавства у сфері захисту інформації. Важливим елементом є також розроблення внутрішніх регламентів,

інструкцій та положень, що деталізують окремі аспекти реалізації політики інформаційної безпеки.

Крім того, необхідним є призначення в освітньому закладі посадової особи, відповідальної за організацію та координацію заходів із забезпечення інформаційної безпеки. Зазвичай це може бути інженер з інформаційної безпеки або системний адміністратор. Дана особа повинна мати відповідну кваліфікацію та досвід роботи в сфері захисту інформації.

У кадровому аспекті важливим є забезпечення належної обізнаності та підготовки всіх категорій персоналу закладу освіти щодо питань інформаційної безпеки. Це досягається шляхом проведення навчальних заходів, тренінгів та інструктажів з інформаційної безпеки. Окрім того, ключові фахівці, які безпосередньо задіяні у функціонуванні систем захисту інформації, повинні мати відповідну професійну підготовку, сертифікати та дозволи на доступ до захищеної інформації.

Комплексний підхід до організаційно-правового та кадрового забезпечення функціонування систем захисту інформації в освітньому середовищі дозволяє підвищити рівень інформаційної безпеки, мінімізувати ризики витоку конфіденційних даних та забезпечити ефективне управління засобами захисту.

Забезпечення інформаційної безпеки в сучасних освітніх установах є надзвичайно важливим завданням, враховуючи зростаючу роль інформаційно-комунікаційних технологій в освітньому процесі, а також необхідність захисту конфіденційних даних учнів, студентів, викладачів та адміністративного персоналу. У зв'язку з цим, перспективи розвитку комплексних систем захисту інформації в освітній сфері є вкрай актуальними.

Одним із ключових напрямів розвитку таких систем є підвищення рівня їх інтеграції та автоматизації. Це передбачає створення єдиних платформ, що об'єднуватимуть різноманітні технологічні компоненти захисту інформації

(засоби ідентифікації, криптографічні засоби, системи виявлення вторгнень тощо) під централізованим управлінням. Такі інтегровані рішення дозволятимуть не лише підвищити ефективність інформаційної безпеки, але й оптимізувати витрати на її забезпечення.

Важливим напрямом є також впровадження сучасних технологій аналітики та управління ризиками інформаційної безпеки. Використання рішень на основі штучного інтелекту, машинного навчання та великих даних дозволить автоматизувати процеси виявлення, аналізу та реагування на інциденти, а також прогнозувати та попереджувати потенційні кіберзагрози. Це надасть освітнім установам можливість завчасно вживати заходів щодо усунення вразливостей та мінімізації ризиків.

Крім того, перспективним є розвиток хмарних технологій та сервісів у сфері забезпечення інформаційної безпеки освітніх закладів. Використання захищених хмарних платформ дозволить оптимізувати витрати на придбання, впровадження та обслуговування систем захисту інформації, а також підвищить рівень доступності та стійкості таких рішень.

Також варто відзначити важливість постійного вдосконалення нормативно-правової бази та організаційно-управлінських механізмів забезпечення інформаційної безпеки в освітній сфері. Це включає розроблення та актуалізацію відповідних стандартів, методик, положень, інструкцій, а також підвищення кваліфікації фахівців, відповідальних за захист інформації.

Комплексний підхід до розвитку систем захисту інформації в освітніх установах із використанням перспективних технологічних, аналітичних та організаційно-управлінських рішень дозволить забезпечити належний рівень інформаційної безпеки, необхідний для ефективного функціонування сучасних закладів освіти.

Висновки. Забезпечення інформаційної безпеки є критично важливим завданням для сучасних освітніх установ, зважаючи на широке використання інформаційно-комунікаційних технологій в освітньому процесі та необхідність захисту конфіденційних даних усіх учасників. Впровадження комплексних систем захисту інформації, що поєднують різноманітні технологічні компоненти, є ефективним рішенням для вирішення цієї проблеми.

Ключовими перевагами інтегрованих інформаційно-аналітичних систем управління безпекою в освітньому середовищі є централізований моніторинг та управління заходами інформаційної безпеки, єдині стандарти ідентифікації, автентифікації та авторизації користувачів, комплексний криптографічний захист даних, а також можливості збору, аналізу та реагування на інциденти.

Комплексний підхід до впровадження та розвитку систем захисту інформації в освітніх установах дозволить підвищити рівень інформаційної безпеки, забезпечити належний захист конфіденційних даних та створити умови для ефективного функціонування сучасних закладів освіти.

Список використаних джерел

1. Lytvynenko O., Kondratov D., Lytvynenko T., Tkachuk V. Conceptual Principles of Building a National Cybersecurity System. Information & Security, 2020, vol. 45, no. 1, pp. 57-72. https://doi.org/10.11610/isij.4504

2. Khmelovskyi Y., Kobzieva T., Pashchenko Y., Baranov V. International Experience in Legal Regulation of Cybersecurity and its Adaptation in Ukraine. Information & Security, 2021, vol. 49, no. 2, pp. 217-233. https://doi.org/10.11610/isij.4922

3. Potii O., Dorokhov A., Potii K., Ponomarenko L. Models and Algorithms for Cyber Threat Detection and Counteraction. Information & Security, 2019, vol. 43, no. 1, pp. 72-85. https://doi.org/10.11610/isij.4307

4. Tkachov V., Zamula A., Sikirda Y., Tkachov V. Artificial Intelligence Technologies for Cybersecurity Enhancement. Information & Security, 2022, vol. 53, no. 1, pp. 107-120. https://doi.org/10.11610/isij.5310

5. Borysiuk Z., Konovalenko I., Hrebeniuk A., Boiariev A. Ensuring Cybersecurity of Critical Information Infrastructure. Information & Security, 2021, vol. 48, no. 1, pp. 57-70. https://doi.org/10.11610/isij.4808

6. Shyshkina O., Dotsenko S., Makarenko S., Tolubko V. Cybersecurity of Critical Information Infrastructure: Challenges and Prospects. Information & Security, 2022, vol. 53, no. 1, pp. 93-106. https://doi.org/10.11610/isij.5309

7. Globa L., Sulima Ye., Sikirda Y. Cybersecurity Educational Programs: Content and Structure Analysis. Information & Security, 2020, vol. 46, no. 2, pp. 157-168. https://doi.org/10.11610/isij.4604

8. Sydorenko V., Zaika S., Tkach M. Cybersecurity Specialists' Competencies in the Digital Transformation Context. Information & Security, 2021, vol. 48, no. 1, pp. 71-84. https://doi.org/10.11610/isij.4809

9. Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG). Available at: https://svo.gov.ua/news/item/13 (accessed 2023-05-16).

10. National Coordination Center for Cybersecurity. Cyber Threats to Ukrainian Universities and Schools. Available at: https://www.rnbo.gov.ua/ua/Diialnist/4716.html (accessed 2023-05-16).

11. UNESCO Survey on the Use of Technologies in Education during the COVID-19 Pandemic. Available at: https://en.unesco.org/covid19/educationresponse/survery (accessed 2023-05-16).

12. Lytvynova S., Spirin O., Proskura L. et al. Analysis of the State of Digital Competence of Educators in Ukraine. Information Technologies and Learning Tools, 2021, vol. 81, no. 1, pp. 283-307.

13. Nosenko Y., Shyshkina M., Lytvynova V. Research of Digital Skills of Student Youth. Educational Discourse, 2020, no. 4, pp. 163-178.

14. Khmara L., Humeniuk N. State of Information Security in Ukrainian Educational Institutions. Scientific Works. Series: Computer Technologies, 2019, vol. 321, no. 309, pp. 56-63.

15. Georgi Penchev, Antoniya Shalamanova-Filipova. A Governance Model for an EU Cyber Security Collaborative Network – ECSCON. Information & Security: An International Journal, 2020, vol. 46, no. 1, pp. 99-113.