

<https://doi.org/10.31891/2307-5740-2025-338-37>

УДК 004.73056.5(045)

ЯРЕМКО Світлана

Вінницький торговельно-економічний інститут Державного торговельно-економічного університету

<https://orcid.org/0000-0002-0605-9324>e-mail: s.yaremko@vtei.edu.ua

НОВИЦЬКИЙ Руслан

Вінницький торговельно-економічний інститут Державного торговельно-економічного університету

<https://orcid.org/0000-0002-6895-5175>e-mail: s.yaremko@vtei.edu.ua

РОЗРОБКА КРИТЕРІЇВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ В СИСТЕМАХ УПРАВЛІННЯ НАВЧАННЯМ

У статті розглянуто основні поняття інформаційної безпеки в системах управління навчанням (Learning Management Systems, LMS); досліджено джерела загроз інформаційним ресурсам таких систем, зокрема антропогенних, техногенних та стихійних; висвітлено особливості розробки критеріїв захищеності для забезпечення надійного функціонування LMS. Здійснено аналітичний огляд найбільш поширених у світі стандартів та методологій, що застосовуються для захисту інформації в навчальних середовищах.

Це дозволило виявити переваги і недоліки сучасних підходів до розробки критеріїв захищеності інформаційних ресурсів у системах управління навчанням та запропонувати ряд рекомендацій щодо вдосконалення організації їхньої інформаційної безпеки. Особлива увага була відведена питанням конфіденційності навчальних даних, забезпеченню цілісності освітніх матеріалів і безперервного доступу до платформ.

В цілому, можна відзначити, що створення ефективних критеріїв захищеності інформаційних ресурсів у LMS є ключовим елементом сучасного забезпечення інформаційної безпеки в освітніх структурах. Це сприяє підвищенню довіри до навчальних систем, захисту конфіденційних даних і забезпеченню сталого розвитку цифрового навчального середовища.

Ключові слова: інформаційна безпека, системи управління навчанням, критерії захищеності, джерело загрози, освітнє середовище, стандарти безпеки, методи захисту інформації.

YAREMKO Svitlana, NOVYTSKYI Ruslan

Vinnytsia Trade and Economic Institute of Kyiv National University of Trade and Economics

DEVELOPMENT OF CRITERIA FOR THE SECURITY OF INFORMATION RESOURCES IN LEARNING MANAGEMENT SYSTEMS

The article examines the basic concepts of information security in the context of Learning Management Systems (LMS); the sources of threats to information resources of such systems, including anthropogenic, man-made and natural ones, are investigated; the peculiarities of developing security criteria to ensure reliable functioning of LMS are highlighted. An analytical review of the most common standards and methodologies used in the world to protect information in learning environments is carried out.

This made it possible to identify the advantages and disadvantages of modern approaches to the development of criteria for the security of information resources in learning management systems and to offer a number of recommendations for improving the organization of their information security. Particular attention is paid to the issues of confidentiality of educational data, ensuring the integrity of educational materials and uninterrupted access to platforms.

Based on the analysis of modern learning management systems, the authors proposed the following criteria for assessing their security: the presence of data encryption; user authentication in the system; security monitoring; frequency of parameter updates; reliability of data protection; complexity of implementing security measures, etc. This made it possible to assess the security of the most common LMSs today and provide recommendations on the use of security measures. According to the authors, the prospects for further development of this area may be associated with the implementation of innovative security systems based on both information technologies and intelligent systems, which in general will allow for constant monitoring, prediction and effective elimination of all possible threats to the security of information resources of learning management systems.

Keywords: information security, learning management systems, security criteria, source of threat, educational environment, security standards, methods of information protection.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному світі інформація стає найдорожчим активом у житті людини та суспільства загалом. В епоху інформаційних технологій є можливість майже миттєво отримувати інформацію, яка з'являється кожну секунду в різних куточках світу, зокрема щодо нових освітніх тенденцій, інновацій у навчальному процесі, запуску онлайн-курсів і платформ для дистанційного навчання та багато іншого. У зв'язку з цим усе більшої актуальності набуває питання захисту інформаційних ресурсів систем управління навчанням (Learning Management Systems, LMS) засобами сучасних інформаційних технологій і систем. При цьому основною метою створення критеріїв захищеності інформаційних ресурсів у LMS стає забезпечення надійного зберігання освітніх матеріалів, конфіденційності даних користувачів і стабільності функціонування системи в умовах потенційних загроз.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблемам розробки та впровадження систем захисту інформаційних ресурсів у системах управління навчанням присвячені праці таких вчених, як Б. М. Березюк, Ю. А. Бобало, О.В. Галицький, І. В. Горбатий, І. М. Журавель, М. Д. Кіселичник, О. А. Немкова, В. І. Отенко, І. Я. Тишик Є. І. Яковенко, а також дослідників з КПІ ім. Ігоря Сікорського. Проведені дослідження стали підґрунтям для розробки та впровадження інструментів захисту даних в інформаційних системах.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Разом з тим, незважаючи на значну кількість досліджень у даному напрямку, питання безпеки інформаційних ресурсів, технологій, методів і засобів, що застосовуються для захисту інформаційних ресурсів систем управління навчанням, залишаються актуальними і потребують подальшого розвитку.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є проведення аналітичного огляду сучасних аспектів захисту інформаційних ресурсів в системах управління навчанням та розробка критеріїв оцінювання рівня їх захищеності з метою покращення забезпечення цілісності, доступності та конфіденційності навчальної інформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Для того щоб розробити критерії захищеності інформаційних ресурсів у системах управління навчанням, необхідно здійснити аналітичний огляд основних характеристик найбільш поширених систем та засобів безпеки, які в них застосовуються.

Із джерел [1, 2] відомо, що найбільш затребуваними на сучасному ринку освітніх технологій є програмні продукти провідних розробників: Moodle (Modular Object-Oriented Dynamic Learning Environment), Google Classroom, Blackboard, Canvas, Microsoft Teams for Education, Open edX, а також власні рішення навчальних закладів для управління навчальними процесами. Розглянемо детальніше характеристики найбільш популярних систем.

Система Moodle (Modular Object-Oriented Dynamic Learning Environment) була створена Мартіном Дуг'ямасом у 2002 році з метою організації навчального процесу через інтернет. Завдяки постійним оновленням і активній підтримці спільноти розробників, Moodle стала однією з найпопулярніших платформ для управління навчанням у світі [2].

Платформа Moodle складається з великої кількості модулів, які забезпечують управління курсами, проведення тестувань, моніторинг прогресу студентів, взаємодію через форуми та чати, а також адміністрування навчальних матеріалів. Система реалізована на основі архітектури клієнт-сервер і функціонує у хмарному середовищі або на локальних серверах навчальних закладів.

Зважаючи на широкий спектр задач, які дозволяє вирішувати система Moodle, а також використання передових технологій для забезпечення захищеності та доступності даних, вартість впровадження подібних рішень може бути суттєвою. Moodle підтримує низку механізмів захисту даних, зокрема [3, 4]:

- Шифрування даних при передачі через SSL, що забезпечує захист інформації під час її обміну між сервером і користувачем.
- Механізми автентифікації користувачів, включно з підтримкою одноразових паролів (OTP), OAuth 2.0, LDAP та інших методів.
- Резервне копіювання даних із функцією автоматизації для збереження критичних навчальних матеріалів і записів.
- Розмежування прав доступу завдяки ролям та дозволам, що дозволяє обмежувати доступ до певних ресурсів залежно від статусу користувача (студент, викладач, адміністратор тощо).
- Систему моніторингу активностей, що дозволяє відстежувати дії користувачів для виявлення потенційних загроз чи порушень.

Впровадження Moodle, як і будь-якої системи управління навчанням, потребує залучення кваліфікованих фахівців для її адаптації до потреб навчального закладу. Це може включати налаштування серверного середовища, інтеграцію зі сторонніми сервісами, налаштування безпеки та навчання персоналу, що може зайняти від кількох тижнів до кількох місяців залежно від складності проекту.

Впровадження таких систем забезпечує значні переваги: підвищення ефективності моніторингу навчального процесу на 25–35%; зниження витрат на паперову документацію й адміністрування у середньому на 10%; покращення якості взаємодії між викладачами та студентами – на 30–40%; підвищення швидкості доступу до навчальних ресурсів – у середньому на 20% [2].

Поряд із цим, суттєвим негативним фактором, який може впливати на прийняття рішення про впровадження даної системи управління навчанням, є недостатньо розвинена регіональна мережа консультування, навчання персоналу та сервісного обслуговування системи. Це може ускладнити процес адаптації платформи до специфічних потреб навчального закладу та забезпечення своєчасної технічної підтримки.

Продовжуючи огляд програмних рішень, які є найбільш поширеними для управління навчанням, слід розглянути систему Open edX – одну з провідних платформ для створення та управління масовими відкритими онлайн-курсами (MOOC), а також для підтримки навчального процесу в освітніх установах. Платформа була заснована у 2012 році Масачусетським технологічним інститутом (MIT) і Гарвардським університетом та швидко здобула популярність серед закладів освіти по всьому світу [1].

Серед рішень на основі Open edX є платформи, орієнтовані як на невеликі навчальні заклади, так і на корпоративний сектор та великі освітні організації. Open edX підтримує хмарну інфраструктуру, модульну архітектуру та стандарти обміну даними, такі як SCORM і xAPI. Розширення функціоналу платформи може бути реалізовано за допомогою інтеграції з інструментами Google Workspace, Microsoft Office 365, або іншими популярними сервісами.

Open edX використовує передові технології для забезпечення захищеності та доступності даних, зокрема [3, 5, 6]:

- Безпечну автентифікацію за допомогою інтеграції з системами SAML, OAuth 2.0, а також двохетапну автентифікацію (2FA) для забезпечення додаткового рівня безпеки.

- Шифрування даних за допомогою SSL/TLS-протоколів для запобігання перехопленню конфіденційної інформації.

- Гранулярне управління доступом, що дозволяє налаштовувати ролі та дозволи і обмежити доступ до певних ресурсів залежно від статусу користувача (студент, викладач, адміністратор).

- Моніторинг подій і дій користувачів, що дозволяє вчасно виявляти та реагувати на потенційні загрози.

- Регулярне резервне копіювання через підтримку автоматичного створення резервних копій даних, забезпечуючи їх відновлення у разі втрати.

Серед переваг Open edX можна відзначити відкритий код, що дозволяє користувачам модифікувати платформу відповідно до власних потреб, а також активну міжнародну спільноту, яка постійно вдосконалює систему. Разом із цим, обмеженнями для впровадження є висока складність налаштування платформи, потреба у кваліфікованих спеціалістах для підтримки роботи, а також значні витрати на впровадження для великих масштабів навчання.

Ще одним важливим гравцем на ринку систем управління навчанням є система Blackboard Learn, яка призначена для підтримки комплексного управління освітнім процесом. Blackboard була заснована у 1997 році в США і швидко стала однією з провідних платформ для організації дистанційного навчання та інтеграції цифрових інструментів в освітню діяльність [1].

Blackboard Learn підтримує широкий спектр функціональних можливостей, що дозволяють автоматизувати управління навчальними ресурсами, оцінюванням, комунікацією між учасниками навчального процесу та аналізом навчальної успішності. Платформа орієнтована як на навчальні заклади (школи, університети, коледжі), так і на корпоративне навчання, що робить її універсальним рішенням для підтримки розвитку знань та компетенцій.

Особливістю Blackboard є її модульна структура, яка дозволяє створювати унікальні освітні середовища відповідно до потреб конкретної організації. Система підтримує інтеграцію з іншими програмами за допомогою API, стандартів LTI та SCORM, що дає можливість використовувати її як частину більшого комплексу інформаційних систем. Blackboard також підтримує функції збереження даних у різних форматах (Excel, PDF), створення інтерактивних завдань, автоматизованого тестування та побудови звітів.

У Blackboard використовуються передові технології для захищеності та доступності даних, серед яких [3-6]:

- Шифрування даних за допомогою SSL/TLS-протоколів, що передаються між клієнтом і сервером, запобігаючи несанкціонованому доступу до інформації.

- Розширена автентифікація за допомогою SAML, LDAP, OAuth 2.0, а також двофакторної автентифікації (2FA) для підвищення рівня захищеності облікових записів користувачів.

- Ролі та дозволи, що дозволяє чітко визначати рівень доступу для викладачів, студентів та адміністраторів.

- Аналітика безпеки через використання інструментів моніторингу та аналізу загроз і аномальних дій, забезпечуючи можливість оперативного реагування.

- Захист від DDoS-атак, оскільки Blackboard активно інтегрує засоби для протидії розподіленим атакам та запобігає порушенню доступності сервісу.

- Антивірусний захист завдяки перевірці завантажуваних файлів на наявність шкідливого програмного забезпечення.

- Часті оновлення безпеки завдяки тому, що Blackboard регулярно випускає оновлення системи, які усувають знайдені вразливості та підвищують загальний рівень безпеки.

Серед ключових переваг Blackboard можна відзначити її надійність, можливість масштабування для великих організацій, високий рівень безпеки даних та багатофункціональність. Крім того, платформа має розвинену службу підтримки, яка забезпечує навчання персоналу та консультації з налаштування системи.

Однак, серед недоліків можна виділити відносно високу вартість впровадження і використання платформи, що може стати бар'єром для невеликих освітніх установ. Також для роботи з Blackboard необхідне залучення спеціалістів з IT, які мають досвід роботи з системами управління навчанням, що ускладнює її використання у малих організаціях.

Одним із провідних світових рішень у сфері програмного забезпечення для управління навчальними процесами є система Canvas, розроблена компанією Instructure в 2011 році. Система Canvas є однією з найбільш популярних платформ для онлайн-навчання, яка активно використовується в університетах, школах і корпоративних навчальних програмах по всьому світу. Canvas використовують такі відомі навчальні заклади, як Університет Каліфорнії, Гарвард, Стенфорд, а також корпоративні навчальні програми таких компаній, як LinkedIn, Adobe, Cisco та інші [1, 5].

Система Canvas реалізована на базі сучасних технологій, що дозволяє забезпечити ефективну роботу з великими обсягами даних та гарантувати високий рівень безпеки інформації. Вона працює в хмарному середовищі і підтримує інтеграцію з іншими освітніми та корпоративними платформами, такими як Google Drive, Microsoft Office 365, Zoom та інші. Система підтримує різноманітні операційні системи, зокрема Windows, macOS, iOS і Android [1].

Серед основних переваг Canvas можна відзначити високу масштабованість, простоту використання, інтеграцію з іншими освітніми ресурсами та можливість адаптації під конкретні потреби навчальних закладів. Крім того, Canvas забезпечує високий рівень захищеності інформаційних ресурсів, зокрема через шифрування даних, багатоетапну аутентифікацію, моніторинг безпеки та регулярні оновлення для захисту від нових загроз. З недоліків можна зазначити потребу в постійному доступі до інтернету для повноцінної роботи системи та певні вимоги до конфігурації серверного обладнання.

Ще одним лідером на ринку програмного забезпечення для автоматизації управління навчальним процесом є система Google Classroom, яка була запущена компанією Google у 2014 році. Завдяки простоті використання, інтеграції з іншими продуктами Google та доступності для навчальних закладів усіх рівнів, Google Classroom швидко здобула популярність серед учителів та студентів по всьому світу. Система активно використовується в школах, університетах і для корпоративного навчання, надаючи інтуїтивно зрозумілі інструменти для організації навчального процесу [1, 4].

Google Classroom дозволяє викладачам створювати курси, розподіляти завдання, надавати студентам доступ до матеріалів і оцінювати їхню роботу. Це допомагає забезпечити ефективне управління навчанням без необхідності в складних програмних рішеннях. Система підтримує інтеграцію з іншими інструментами Google, такими як Google Drive, Google Docs, Google Meet та іншими, що дозволяє легко взаємодіяти з навчальними матеріалами, проводити відеоконференції та спільно працювати над документами.

Однією із головних переваг Google Classroom є безкоштовність для освітніх установ, а також можливість масштабування для будь-якої кількості користувачів. Завдяки хмарним технологіям дані зберігаються на серверах Google, що забезпечує високу доступність і надійність зберігання інформації. Крім того, система підтримує багатоетапну аутентифікацію, шифрування даних і має механізми для моніторингу безпеки, що гарантує захищеність інформаційних ресурсів.

З недоліків Google Classroom можна відзначити обмежену кількість функцій порівняно з іншими більш складними платформами, такими як Moodle чи Blackboard, а також залежність від інтернет-з'єднання для роботи. Однак простота використання, доступність та інтеграція з іншими сервісами Google робить її чудовим вибором для шкіл і малих навчальних організацій, а також для корпоративного навчання.

Google Classroom забезпечує високий рівень безпеки завдяки наступним методам захисту [1, 4, 5]:

- Шифрування даних, як під час їх передачі (SSL/TLS протоколи), так і під час зберігання на серверах, що запобігає доступу сторонніх осіб до інформації.

- Контроль доступу завдяки інтеграції з Google Workspace for Education, що дозволяє гнучко керувати доступом до облікових записів, документів та завдань залежно від ролей користувачів (учитель, учень, адміністратор).

- Двоетапна автентифікація (2FA) для захисту облікових записів користувачів, зменшуючи ризик компрометації паролів.

- Антивірусний сканер, що здійснює перевірку на наявність шкідливого програмного забезпечення.

- Створення обмежених освітніх доменів, у межах яких взаємодія учасників навчального процесу є контрольованою та безпечною.

- Резервне копіювання та відновлення через автоматизоване створення резервних копій даних у хмарній інфраструктурі Google, що забезпечує можливість відновлення інформації у разі непередбачених ситуацій.

Ще одним популярним рішенням на ринку програмного забезпечення для управління навчанням є система TalentLMS, яка стала одним із лідерів у світі серед хмарних рішень для навчання та розвитку персоналу. TalentLMS активно використовується в різних країнах Європи, Північної Америки та СНД, а також отримала популярність серед середніх і великих компаній. На сьогодні TalentLMS використовують понад 70000 організацій по всьому світу, серед яких можна знайти такі відомі бренди, як Coca-Cola, KPMG, Accenture, Siemens, Samsung, а також численні навчальні установи [3].

TalentLMS підтримує широкий спектр функцій для організації навчальних курсів, оцінювання результатів, моніторингу прогресу користувачів, а також інтеграції з іншими корпоративними системами. Система є дуже гнучкою та має можливість адаптації під специфічні вимоги будь-якої організації — від великих корпорацій до малих компаній та навчальних центрів. TalentLMS дозволяє створювати курси з інтерактивними матеріалами, тестами, сертифікатами, а також використовувати мультимедійні ресурси для підтримки навчального процесу.

TalentLMS забезпечує високий рівень безпеки завдяки наступним методам захисту [3 - 6]:

- Шифрування даних за допомогою SSL/TLS-протоколів, що захищає інформацію від перехоплення та несанкціонованого доступу.
- Розмежування прав доступу (адміністратор, викладач, учень), забезпечуючи суворий контроль над тим, хто має доступ до конфіденційної інформації.
- Двохетапна автентифікація (2FA), яка додає додатковий рівень захисту для облікових записів користувачів.
- Регулярне резервне копіювання в хмарній інфраструктурі, що дозволяє відновити дані у випадку виникнення надзвичайних ситуацій.
- Захист від атак завдяки тому, що TalentLMS забезпечує моніторинг і захист від DDoS-атак, а також використовує механізми автоматичного виявлення й блокування підозрілих активностей.
- Географічно розподілені сервери, оскільки дані зберігаються на серверах у різних локаціях, що підвищує їх доступність і захищеність.

Одна з ключових переваг TalentLMS полягає в її хмарній архітектурі, що дає можливість доступу до системи з будь-якого місця та на будь-якому пристрої. Це також забезпечує високу масштабованість і гнучкість в управлінні контентом, зберіганні даних та їх обробці. TalentLMS підтримує інтеграцію з різними програмними та апаратними засобами, що дозволяє легко інтегрувати її в існуючі корпоративні структури. Крім того, система забезпечує надійне зберігання даних, надаючи високий рівень безпеки, включаючи шифрування даних, багаторівневу автентифікацію та механізми моніторингу.

З недоліків варто зазначити, що деякі функції, зокрема для великих організацій, можуть вимагати додаткових налаштувань або інтеграцій, що може передбачати певні витрати на впровадження. Однак простота використання, ефективність у підтримці різноманітних форм навчання та можливість масштабування робить TalentLMS привабливою для компаній, що прагнуть покращити управління навчанням своїх співробітників.

На основі проведеного аналітичного огляду найбільш поширених систем управління навчанням та методів і засобів захисту їх інформаційних ресурсів, можна запропонувати ряд критеріїв для покращення їх аналізу з точки зору інформаційної безпеки, використовуючи при цьому наступні умовні позначення для різних ступенів прояву критерію: «-» – критерій відсутній; «-+» – середній ступінь прояву критерію; «++» – критерій відображений на достатньому рівні. Перелік критеріїв, їх характеристика та ступені прояву представлені в табл.1.

Таблиця 1

Критерії оцінювання захищеності інформаційних систем управління навчанням

Критерій	Характеристика критерію	Ступінь прояву критерію
Шифрування даних	Відсутнє шифрування даних	-
	Наявне шифрування даних	++
Автентифікація	Відсутня автентифікація користувачів системи	-
	Стандартний набір функцій для одноетапної автентифікації	-+
	Розширений набір функцій для багатаетапної автентифікації	++
Моніторинг безпеки	Відсутній моніторинг безпеки та централізоване управління доступом	-
	Здійснюється моніторинг безпеки та централізоване управління доступом	++
Частота оновлень	Дані знаходяться на локальному ПК і централізовано не оновлюються	-
	Дані знаходяться на сервері і періодично оновлюються	-+
	Дані знаходяться на сервері і оновлюються в режимі реального часу	++
Надійність захисту даних	Низька або середня надійність захисту даних	-+
	Висока надійність захисту даних	++
Вимоги до ресурсів системи	Не потребує значних ресурсів системи для впровадження засобів захисту інформації	++
	Підвищені вимоги до ресурсів системи для забезпечення захищеності	-+
Складність впровадження засобів захисту	Простота налаштування засобів захисту	++
	Потребує залучення спеціалістів для налаштування безпеки	-+
Сервісна підтримка	Тільки дистанційне консультування з питань безпеки	-+
	Наявність розвинутої системи навчання та підтримки	++

Використовуючи наведені вище критерії, була проведена оцінка найбільш поширених систем управління навчанням (LMS) з точки зору їх захищеності. Результати оцінювання представлені в табл. 2.

Таблиця 2

Оцінка найбільш поширених систем управління навчанням (LMS) з точки зору їх захищеності

Назва системи / Назва критерію	Moodle	Blackboard	Google Classroom	TalentLMS
Шифрування даних	+++	+++	+++	++
Аутентифікація	+++	+++	++	++
Моніторинг безпеки	+++	+++	++	++
Частота оновлень	+++	++	+++	++
Надійність захисту даних	+++	++	+++	++
Вимоги до ресурсів системи	++	++	++	-+
Складність впровадження засобів захисту	++	++	++	++
Сервісна підтримка	++	+++	++	++

На основі проведеного аналізу можна зробити висновки, що серед найбільш популярних систем управління навчанням (LMS), таких як Moodle, Blackboard, Google Classroom, TalentLMS, Canvas та Schoology, є суттєві відмінності в аспектах безпеки. У системі Moodle більше уваги приділено шифруванню даних, що свідчить про високий рівень безпеки та захисту користувацької інформації, що є важливим для забезпечення конфіденційності. У той же час, в TalentLMS цей показник трохи нижчий, що може вказувати на менше універсальне або менш надійне шифрування, що, в свою чергу, може знижувати рівень довіри до захищеності даних користувачів. Крім того, Blackboard та Canvas демонструють високий рівень підтримки та частоту оновлень, що є суттєвими для ефективної роботи системи. У той час як Google Classroom та Schoology мають дещо обмежену сервісну підтримку, що може стати проблемою для навчальних закладів, які потребують оперативної допомоги в разі виникнення складних ситуацій.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ**І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ**

Таким чином, на основі аналітичного огляду та порівняльного аналізу сучасних систем управління навчанням авторами були запропоновані такі критерії оцінювання їх захищеності, як наявність шифрування даних; аутентифікації користувачів в системі; здійснення моніторингу безпеки; частоти оновлень параметрів; надійності захисту даних; складності впровадження засобів захисту тощо. Це дало змогу провести оцінювання захищеності найбільш поширених на сьогодні LMS та надати рекомендації щодо використання засобів захисту в залежності від потреб та умов навчального процесу.

Перспективи подальшого розвитку даного напрямку на думку авторів можуть бути пов'язані зі впровадженням інноваційних систем безпеки, що базуватимуться, як на інформаційних технологіях, так і на інтелектуальних системах, що в цілому дозволить здійснювати постійний моніторинг, передбачення та ефективну ліквідацію усіх можливих загроз безпеці інформаційних ресурсів систем управління навчанням.

Література

1. Кононець Н. В. Система управління навчанням Google Classroom у професійній підготовці фахівців // Методика викладання природничих дисциплін у середній та вищій школі (XXVI Каришинські читання): матеріали міжнар. наук.-практ. конф. (Полтава, 30-31 травня 2019 р.) / Н. В. Кононець. – Полтава: ТОВ «Сімон», 2019. – С. 171-173.
2. Прокопенко А. І., Доценко С. О., Москаленк В. В. та ін. Технології дистанційного навчання: діяльності та ресурси MOODLE: навч. посіб. / А. І. Прокопенко, С. О. Доценко, В. В. Москаленк та ін. – Харків: Харківський нац. пед. ун-т ім. Г. С. Сковороди, 2021. – 49 с.
3. Поворознюк А. І., Поворознюк О. А. Управління інформаційною безпекою: навчально-методичний посібник / А. І. Поворознюк, О. А. Поворознюк. – Харків: НТУ «ХПІ», 2021. – 135 с.
4. Луценко В. М., Прогонов Д. О. Методи та засоби технічного захисту інформації: навч. посіб. / В. М. Луценко, Д. О. Прогонов. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 289 с.
5. Бобало Ю. А., Горбатий І. В., Кіселичник М. Д. Інформаційна безпека: навч. посібник / Ю. А. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарев, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.
6. Галицький О. В. Управління електронними освітніми ресурсами з використанням веб-орієнтованих комп'ютерних систем // Освітній дискурс: збірник наукових праць / Голов. ред. О. П. Кивлюк. – Київ: «Видавництво «Гілея», 2019. – Вип. 13 (5): педагогічні науки. – С. 20-31.

References

1. Kononets N. V. Google Classroom Learning Management System in Professional Training of Specialists // Methods of Teaching Natural Sciences in Secondary and Higher Education (XXVI Karyshyn Readings): Materials of the International Scientific and Practical Conference (Poltava, May 30-31, 2019) / N. V. Kononets. – Poltava: "Simon" LLC, 2019. – Pp. 171-173.

2. Prokopenko A. I., Dotsenko S. O., Moskalenk V. V. et al. Distance Learning Technologies: Activities and Resources of MOODLE: Educational Guide / A. I. Prokopenko, S. O. Dotsenko, V. V. Moskalenk et al. – Kharkiv: Kharkiv National Pedagogical University named after H. S. Skovoroda, 2021. – 49 pages.
3. Povoroznyuk A. I., Povoroznyuk O. A. Information Security Management: Educational and Methodical Guide / A. I. Povoroznyuk, O. A. Povoroznyuk. – Kharkiv: NTU "KPI", 2021. – 135 pages.
4. Lutsenko V. M., Progonov D. O. Methods and Means of Technical Information Protection: Educational Guide / V. M. Lutsenko, D. O. Progonov. – Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2021. – 289 pages.
5. Bobalo Y. A., Horbaty I. V., Kiselychynk M. D., Bondariyev A. P., Voytusik S. S., Horpeniuk A. Ya., Nemiova O. A., Zhuravel I. M., Berezyuk B. M., Yakovenko Y. I., Otenko V. I., Tyshyk I. Ya. Information Security: Educational Guide / Y. A. Bobalo, I. V. Horbaty, M. D. Kiselychynk, A. P. Bondariyev, S. S. Voytusik, A. Ya. Horpeniuk, O. A. Nemiova, I. M. Zhuravel, B. M. Berezyuk, Y. I. Yakovenko, V. I. Otenko, I. Ya. Tyshyk. – Lviv: Lviv Polytechnic Publishing House, 2019. – 580 pages.
6. Halytskyi O. V. Management of Electronic Educational Resources Using Web-Oriented Computer Systems // Educational Discourse: Collection of Scientific Papers / Chief Editor O. P. Kivliuk. – Kyiv: "Hileya" Publishing House, 2019. – Vol. 13 (5): Pedagogical Sciences. – p. 20-31.