Т1. №1(33)'2023 https://doi.org/10.31474/2786-9024/v1i1(33).299636

Інформаційна безпека

БЕЗПЕКА ТА ЗАХИСТ НАВЧАЛЬНИХ LMC СИСТЕМ

Н.О. Маслова[1], О.М. Любименко[1]

[1] Department of Applied Mathematics and Informatics, Donetsk National Technical University, Lutsk, Ukraine
E-mail: olena.liubymenko@donntu.edu.ua

Отримано 31.12.2023
Прийнято до публікації 19.01.2024
Опубліковано 01.04.2024

АНОТАЦІЯ

Інформаційні технології відіграють значну роль у навчальному процесі й забезпеченні якісних результатів навчання в умовах дистанційної освіти. Сучасною тенденцією є розвиток інтерактивних систем, які включають елементи аудіо- та відео- матеріалів, графіки, презентацій, інтернет посилань, матеріали з різних джерел та у різних форматах. Додавання інтерактивного контенту до в навчальних систем підвищує ризики інформаційної безпеки сучасних системах LMC. Акцент в роботі зроблено на необхідності забезпечення захисту програмного забезпечення систем, розміщеного в них освітнього контенту, результатів навчання та персональних даних учасників. Створюючи захист, слід звертати увагу на потенційні загрози, такі як несанкціонований доступ, недосконале програмне забезпечення, неякісні плагіни оновлення, копіювання матеріалів, шахрайство та кібератаки. Проаналізовано вразливості найбільш поширених сучасних LMC систем. Приділено увагу можливостям використання хмарних технологій для розміщення модулів систем, навчальних матеріалів й результатів навчання на хмарних сервісах. Застосування хмар гарантує постійний доступ до навчальної системи, надійне зберігання матеріалів, додатковий захист конфіденційної та персональної інформації. Тому для забезпечення ефективного та безпечного навчання з урахуванням сучасних інтерактивних підходів до подання учбових матеріалів, важливо розвивати системи та застосовувати технології, які забезпечують постійний доступ до освітнього контенту, надійний захист даних (у тому числі й персональних), збереження цілісності інформації та дотримання принципів конфіденційності.

***Ключові слова**: системи LMC, інтерактивне навчання, уразливості систем дистанційного навчання, захист, хмарні технології, конфіденційність, доступність, цілісність, надійність, інформація, персональні дані, освітній контент.*

ВСТУП

Бурхливий розвиток інформаційних технологій сприяв становленню багатьох сучасних технологій, які застосовуються у виробництві, медицині, навчанні. ІТ-технології, штучний інтелект, інтерактивні методи навчання є звичною дійсністю, без якої складно уявити процес надання знань й сьогодні дистанційні системи є невід'ємною частиною учбового процесу. Ці системи не тільки забезпечують доступ до знань у будь-якій точці світу, але й створюють унікальні можливості для взаємодії, адаптації до індивідуальних потреб та розвитку навчального процесу в інтерактивному ключі.

При експлуатації систем постійно зростають вимоги до технічних засобів й їх оновлення в процесі експлуатації, програмного забезпечення, яке не є простим в застосуванні та обслуговуванні, до створення й зберігання навчального контенту, який є однією з складових частин навчальної системи. Бази даних вимагають кваліфікованого супроводу, поповнення, розвитку, що складно здійснювати у разі великої кількості користувачів й мінімальної кількості (як правило) супроводжуючого персоналу.

Одночасно зі зростанням популярності й розповсюдженості дистанційної форми навчання, зростає розуміння у необхідності надійного захисту навчальних систем, приділяється увага захищеності контенту, програмного забезпечення, персональних даних учасників учбового процесу.

Навчальні системи мають конфіденційну інформацію, таку як особисті дані студентів та викладачів. А тому недостатні заходи безпеки можуть призвести до:

– несанкціонованого доступу до інформації, що зафіксована в системах;
– копіювання матеріалів, розміщених в навчальних системах, порушення авторських прав;
– шахрайства під час проведення тестів та іспитів (підміна користувача);
– ураження й порушення цілісності даних при проведенні кібератак та порушень безпеки;
– несанкціонованого доступу до навчальних матеріалів або систем, що може порушити конфіденційність даних.

Ці проблеми стають все більш актуальними в контексті розвитку електронної та дистанційної освіти. Одна з основних проблем використання систем навчання полягає в недостатньому рівні захисту систем та контенту, що в них розміщується та застосовується, особливо в умовах, коли кількість загроз постійно зростає.

АНАЛІЗ ЛІТЕРАТУРНИХ ДАНИХ ТА ПОСТАНОВКА ПРОБЛЕМИ

З розвитком технологій віртуальної та доповненої реальності, штучного інтелекту та онлайн-платформ, інтерактивні системи стали засобом для ефективного навчання. Інтерактивні системи являють собою інноваційні засоби, для їх створення використовують сучасні технології динамічного та захопливого освітнього досвіду.

Засоби проведення інтерактивного навчання розподіляють на чотири великі групи [1]. Це базові платформи для створення онлайн-курсів (Moodle, Canvas, Blackboard, Schoology), середовища віртуальної та доповненої реальності (Unity3D, A-Frame, ARCore та ARKit), системи для створення освітнього контенту з елементами гейміфікації (Kahoot!, Classcraft, Quizziz), інструменти для створення інтерактивних мультимедійних матеріалів (Adobe Captivate, Articulate Storyline) та спеціалізовані адаптивні освітні платформи (Smart Sparrow, Microsoft Teams, Knewton, Edpuzzle, Google Classroom), які дозволяють застосовувати інтерактивний контент, включати його в освітній контент.

Перелічені системи включають поширені й унікальні функції, побудовані з застосуванням різноманітних підходів до навчання, їх вибір залежить від конкретних потреб та цілей навчального процесу. Ці інструменти надають викладачам і розробникам освітніх матеріалів можливість створення інтерактивних систем, що сприяють активній участі студентів і підвищенню ефективності навчання. По-суті, це LMS (Learning Management System) системи, системи управління навчанням, в яких для підвищення ефективності навчання застосовують нестандартні форми представлення знань - ігри, графічні редактори, CAD-CAM системи, інтегровані середовища, аудіо та відео-записи й багато іншого. Це програмне забезпечення, найчастіше хмарне, яке дає змогу створювати освітні продукти в електронному вигляді та організовувати онлайн-заняття, включати в них інтерактивні елементи.

Галузь дистанційного навчання є на даний момент достатньо розвиненою та сталою. Відомими й широко застосовними є системи Moodle, Canvas, Webtutor, ILIAS та інші. Але під час створення цих систем проблеми захисту контенту, персональних даних, програмного забезпечення не були оголошені як першочергові. Це привело до необхідності розв’язування питань захисту існуючих систем в умовах їх активної експлуатації.

Перші застереження й спроби дослідження необхідності захисту систем дистанційного навчання виникли у першому десятиріччі поточного століття. Так, у роботі [2] автори наголосили на недостатній увазі, яку приділяють розробники навчальних систем до питань безпеки своїх продуктів. У роботі [3] проведено аналіз та класифікацію загроз порушення безпеки систем дистанційного навчання. Автори зробили висновок, що незалежно від архітектури системи, слід виділити дві групи загроз: загальні та специфічні.

До загальних автори віднесли загрози доступності, dos-атаки, проблеми переповнення буферів, впливу SQL-ін’єкцій, спроби підбору паролів, та інші, характерні для автоматизованих інформаційних систем взагалі. Ці загрози достатньо відомі й можуть бути нейтралізовані використанням методів та засобів захисту інформації загального призначення. А в якості специфічних для

ISSN 2786-9024

 https://doi.org/10.31474/2786-9024/v1i1(33).299636

систем дистанційного навчання автори називають загрози, які зумовлені взаємодією суб'єктів та об'єктів навчального процесу.

Частково проблеми захищеності розглянуті й в інших дослідженнях. Так, в [4] автори роблять акцент на організаційно-адміністративних методах забезпечення захисту однієї з найбільш популярних систем дистанційного навчання – системі Moodle. У роботі [5] показано особливості забезпечення захисту інформації, яка міститься в системі дистанційного навчання Moodle й розглянуто основні характеристики операційної системи CentOS, яка застосовується для забезпечення навісного захисту системи, показано особливості проведення захисту інформації при роботі з цією операційною системою. У роботі [6] увага акцентована на необхідності застосування систем шифрування в процесі отримання та зберігання даних.

Робота [7] наближена до сучасних вимог та стандартів захисту інформаційних систем. В ній детально проаналізовані базові проблеми захисту інформації в сучасних системах дистанційного навчання та загрози з точки зору інформаційної безпеки для таких систем, перелічені основні цілі, які може переслідувати зловмисник при реалізації атак на системи дистанційного навчання (СДН) та уразливості через які він здійснює атаки. Здійснено порівняння найбільш поширених LMC за такими ключовими параметрами, як загрози хибної реєстрації та автентифікації, загрози порушення достовірності результатів контролю знань та загрози впровадження шкідливого програмного забезпечення. Основну увагу приділено підходам до захисту СДН від загроз підміни користувача, загроз використання програмних ботів і скриптів, а також загроз використання лекцій, електронних довідників та інших сторонніх навчальних матеріалів. Запропоновано механізм захисту від загроз, й автори наголошують, що алгоритм дій може бути використаний у будь-якій системі дистанційного навчання для захисту від загроз порушення достовірності знань.

У [8] показано, що найбільш уразливими з точки зору інформаційної безпеки є процеси:

– передачі ідентифікаційних і аутентифікаційних даних користувача;
– обмін даними між браузером віддаленого користувача і веб-сайтом навчальної системи;
– авторизації користувача (на сервері системи дистанційного навчання і в інформаційно- комунікаційній системі навчального закладу);
– витяг і запис даних в бази навчального закладу;
– обмін даними між сервером СДН і сервером ІС навчального закладу.

Вказано, що зловмисник може бути як зовнішнім, так і внутрішнім, перелічені цілі, котрі він переслідує та уразливості, які застосовує. Це, зокрема – уразливості в веб-додатку і сервісах СДН; слабкі паролі і недоліки процесу автентифікації користувачів на сервері СДН; помилки в конфігурації і адмініструванні СДН; шкідливе програмне забезпечення (віруси, троянські програми, програмні бомби і закладки); слабкості системи захисту інформації.

Таким чином, до основних проблем захисту електронних навчальних систем слід віднести:

– недостатню захищеність від несанкціонованого доступу;
– ризики несанкціонованого копіювання та плагіату;
– порушення достовірності результатів контролю знань;
– безпеку даних під час розміщення та передачі даних;
– проблеми управління доступом;
– порушення конфіденційності.

Одним із актуальних шляхів розвитку освітніх систем є використання хмарних технологій. Хмарні технології є надзвичайно популярними, кількість їх застосувань у різних сферах стрімко зростає. Їх впровадженню й активному розповсюдженню сприяють такі фактори, як:

1. можливість постійного доступу до навчального контенту;
2. збереження матеріалів та результатів навчання на віддалених серверах в центрах обробки, завдяки чому з користувача знімається проблема обслуговування технічної частини навчальної системи;
3. наявність засобів безпеки при передачі, прийманні та збереженні інформації, що гарантується самою технологією хмарних структур;
4. додаткова ідентифікація користувачів в процесі отримання доступу до хмарного ресурсу з фіксацією й контролем адреси входу.

Проблеми захисту неможливо розв'язати без адаптації архітектури та конфігурації навчальних систем до існуючих технологій. Тому слід приділити увагу не тільки проблемам й особливостям так званого навісного захисту існуючих систем, а й дослідженню можливостей зниження ризиків інформаційної безпеки при експлуатації навчальних LMC систем при активному застосуванні сучасних хмарних технологій. Й об'єднати фактори гарантованої працездатності апаратного забезпечення, постійної доступності, сертифікованої захищеності, можливостей відокремленого збереження,

 https://doi.org/10.31474/2786-9024/v1i1(33).299636

послуг копіювання даних й антивірусного захисту, які надають хмарні сервіси з перевагами LMC систем в сфері надання освітніх послуг в сучасних реаліях.

Враховуючи вищенаведене, об'єктом дослідження є методології захисту LMC систем й засобів створення учбового контенту та навчального електронного ресурсу з огляду на сучасні погляди забезпечення безпеки учасників.

Предметом дослідження є вразливості навчального середовища при взаємодії користувача із інтерактивними та навчальними ресурсами.

Метою роботи є дослідження проблем захищеності сучасних LMC систем з урахуванням вразливостей програмного забезпечення, навчального контенту, результатів навчання та персональних даних учасників освітнього процесу, вплив хмарних технологій на безпеку систем, а також надання рекомендацій для підвищення захищеності навчальних електронних ресурсів.

Для досягнення мети необхідно виконати наступні задачі:

- виявити та проаналізувати загальні проблеми захисту систем LMC з урахуванням сучасних загроз інформаційній безпеці;
- обрати найбільш поширені системи дистанційної освіти й системи керування навчанням;
- дослідити вразливості поширених систем LMC й можливості застосування сучасних інформаційних технологій, зокрема, хмарних, для зниження ризиків порушення безпеки.

МАТЕРІАЛИ ТА МЕТОДИ ДОСЛІДЖЕНЬ

В роботі використано методи структурного і порівняльного аналізу, з інформаційним і аналітичним підходом розглянуто наукову та методичну літературу, а також онлайн ресурси.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

А. ДОСЛІДЖЕННЯ СИСТЕМ LMC ЗА ПАРАМЕТРАМИ БЕЗПЕКИ

У 2024 році сайт ahaslides.com [9] опублікував огляд, у якому проаналізовані сучасні системи LMS. Розглянемо п'ять з них у пропонованій в статті послідовності. Доповнимо огляд платформою інтеграції Edpuzzle, яка дозволяє об'єднувати популярні рішення. Й проаналізуємо рішення щодо захищеності й інформаційної безпеки ресурсів, на яких наголошують розробники на відповідних сайтах.

Називаючи найбільш поширеною та застосовною систему Google Classroom, автори, тим, не менш, перелічили її основні недоліки: обмежена інтеграція з іншими програмами, відсутність розширених (спеціалізованих для організації класу) функцій, необхідність конвертації своїх файлів у формат Google, відсутність автоматизованих вікторин чи тестів, вікові обмеження (студенти до 13 років можуть використовувати Classroom лише з обліковими записами Google Workspace for Education або Workspace for Nonprofits) й, найголовніший для даного дослідження недолік - Google відстежує поведінку користувачів і дозволяє рекламу на їхніх сайтах, що слід ідентифікувати як порушення конфіденційності.

Google Classroom, як і інші продукти Google, розміщена на хмарі. Google використовує свої власні хмарні інфраструктури, відомі як Google Cloud Platform, для забезпечення інфраструктури, потрібної для функціонування Google Classroom. Дані, включаючи інформацію про користувачів, завдання, матеріали та інше, зберігаються на серверах Google, які розташовані у різних частинах світу.

Іншою сучасною системою є платформа інтеграції систем Edpuzzle [9]. Edpuzzle – це проста у використанні, сучасна платформа, яка працює з відео- аудіо, текстовими, презентаційними матеріалами й дозволяє додавати до них власні запитання або записи, контролювати й керувати процесом навчання, відслідковувати прогрес учнів.

Edpuzzle [10] пропонує об'єднання на спеціалізованій платформі декількох існуючих систем дистанційного навчання з метою уніфікації застосування різнорідних систем, взаємообміну даними між ними, допомагає заощадити час і зусилля на експорт/імпорт даних між різними системами, завдяки єдиному інтерфейсу спрощує роботу з системою. Викладач може підключити відому йому й наповнену систему до Edpuzzle й транслювати завдання через новий, сучасний засіб, перенести контент в нове навчальне середовище, об'єднати декілька блоків навчальних матеріалів при їх попередньому розміщенні на різних ресурсах в єдине ціле.

Зараз Edpuzzle інтегрується з системами Google Classroom, Microsoft Teams, Canvas, Schoology, Moodle, Blackboard, Blackbaud, PowerSchool, Clever, D2L Brightspace.

Edpuzzle – достатньо безпечне середовище, яке дозволяє будувати повноцінні, сучасні навчальні курси, з застосуванням звичних користувачам середовищ. Edpuzzle серйозно ставиться до безпеки та конфіденційності. Ресурс нагороджено кількома сертифікатами безпеки та відповідності вимогам захисту конфіденційності. Edpuzzle - може бути розміщена на

ISSN 2786-9024

 https://doi.org/10.31474/2786-9024/v1i1(33).299636

хмарних серверах, однак недостатня захищеність приєднуваної системи може стати загрозою безпеці всього інтегрованого середовища.

Canvas LMS (https://www.instructure.com/canvas) – це хмарно - орієнтована система керування навчанням. Він відомий своїм зручним інтерфейсом, надійністю та повним набором функцій, призначених для зручного викладання і навчання.

Безпека вбудована безпосередньо в хмарну платформу, інфраструктуру та процеси, відповідно до стандартів SOC 2 і ISO 27001. Дані розміщуються в хмарі Instructure та доставляються через Amazon Web Services (AWS). Користувачі можуть входити за допомогою облікових даних облікового запису Google Cloud, використовуючи мову розмітки декларації безпеки (SAML). Canvas гарантує 99.99% часу безперебійної роботи і цілодобове функціонування платформи для всіх користувачів, тож Canvas вважається однією з надійних LMS.

Edmodo (офіційна web-сторінка - https://www.edmodo.com) - це освітній сайт, який являє собою усічену соціальну мережу за типом Facebook, яка дозволяє спілкуватися вчителям та учням, об'єднавшись навколо процесу навчання у школі.

Edmodo може бути розміщена на хмарних серверах. Використання хмарної інфраструктури дозволить Edmodo швидко впроваджувати оновлення та нові функції, забезпечуючи користувачам доступ до оновлень без необхідності вручну оновлювати програмне забезпечення. Крім того, хмарна інфраструктура може забезпечити резервне копіювання даних й покращити захист та відновлення даних в разі виникнення проблем.

Edmodo – це захищена освітня мережа, яка наголошує на суворому контролі безпеки для повідомлень і для всіх інших комунікацій на платформі.

Moodle - одна з найпопулярніших систем управління навчанням у світі, є модульним об’єктно-орієнтованим динамічним навчальним середовищем з відкритим вихідним кодом, система керування навчанням (LMS). Система Для створення персоналізованого навчального простору, Moodle пропонує власну послугу хостингу MoodleCloud. Хоча Moodle вважається достатньо надійною та захищеною для користувачів та контенту, захист інформації щодо конфіденційності, цілісності та доступності потребує використання різних методів та заходів[11].

Щоб забезпечити роботу Moodle, потрібні три складові: веб-сервер, база даних і поштовий сервер. Хостинги, які використовуються для розміщення серверів Moodle, повинні бути обладнані автоматизованими системами захисту від DDOS-атак та антивірусним програмним забезпеченням для захисту програмних файлів від різних видів порушень безпеки. [12].

Окрім того з метою захисту інформаційних ресурсів в системі передбачено:

– використання паролів для доступу до інформаційних ресурсів;

– політики розмежування прав доступу, що дозволяє призначати різний рівень повноважень для студентів, викладачів та адміністраторів;

– автоматизація виконання системних дій, включаючи доступ до тестів та обмеження настроювань без адміністративних прав;

– створення резервних копій системи;

– IP-блокатори для перевірки вхідних Інтернет-адрес і блокування небажаних IP-адрес;

– наявність безпечного http-з’єднання для сторінок входу до системи;

– вбудований антивірус «Clam AV», для перевірки всіх завантажених файлів та навчальних матеріалів на наявність вірусів;

– налаштування показу особистих даних користувачів (уподобання);

– комплексний захист інформації в базі даних, який забезпечує обмежений доступ до неї та розміщення інформації для тестів в різних таблицях..

В системі управління навчанням «Moodle» в будь-якому освітньому закладі використовується інформаційне середовище, що є сукупністю навчальних матеріалів, засобів підтримки навчального процесу, представлених в електронному вигляді, а також різні засоби, методи та форми комунікації між суб’єктами освітнього процесу.

Таким чином, можна наголосити, що система дистанційного навчання «Moodle» має достатній рівень захищеності інформації. На сайті [13] розміщена велика кількість інформаційно-довідникових матеріалів щодо організації й особливостей побудови безпеки системи Moodle. Але вразливим місцем системи вважаються слабкі паролі (пароль може обрати або змінити користувач), невірна конфігурація доступу або недостатня організація користувацьких прав. Це може створювати ризики для безпеки даних у Moodle. Система не оновлюється автоматично. Несвоєчасне встановлення плагінів можуть бути використані зловмисниками для отримання доступу до системи, внесення змін у інформацію або виконання інших злочинних дій. Крім того, широкі можливості застосування в якості навчальних матеріалів різноманітного контенту (відео, презентації, інтернет-посилання), не перевіреного або недостатньо перевіреного з точки зору безпеки контенту також можуть послабити захист системи.

 https://doi.org/10.31474/2786-9024/v1i1(33).299636

Moodle може бути розміщена як у хмарі, так і на локальних серверах, в залежності від вибору організації та її потреб у забезпеченні безпеки, доступності та масштабованості.

AhaSlides (https://ahaslides.com/ru/features/) – хмарна платформа, яка дає змогу презентувати та проводити інтерактивні заходи. Вона вважається аналогом PowerPoint.

У політиці безпеки AhaSlides реалізовано вимоги конфіденційності, управління доступом та контролю користувача. Резервні копії даних розміщені на платформі Amazon Web Services, яка відповідає стандартам ISO/IEC 27001:2013, 27017:2015 та 27018:2014, сертифікована як постачальник послуг PCI DSS 3.2 рівня 1 і проходить SOC 1, SOC 2 та SOC3. Копії зберігаються на Amazon RDS з використанням повного диска, стандартного шифрування AES ARS з унікальним ключем для кожного сервера. Файлові вкладення у презентації AhaSlides зберігаються у службі Amazon S3 з унікальними посиланнями, доступними через захищене з'єднання HTTPS.

AhaSlides використовує промисловий стандарт безпеки транспортного рівня (TLS) зі 128-бітним шифруванням AES для всіх з'єднань, а паролі хешуються та шифруються за допомогою алгоритму PBKDF2 (з SHA512).

На сайті опубліковано план перегляду безпеки та процес управління інцидентами для виявлення та реагування на них. Платформа дотримується сучасних стандартів безпеки та відкрита для перевірки.

AhaSlides може бути розміщена на хмарних серверах для швидкого впровадження оновлень та резервного копіювання даних.

Microsoft Teams називають робочим середовищем для спільної роботи.

Microsoft Teams використовує хмарну інфраструктуру Microsoft Azure. Це означає, що дані, повідомлення, файли, календарі, відеоконференції та інші, зберігаються на серверах Microsoft у різних місцях світу. Що підвищує їх надійність.

Використання хмарної інфраструктури дозволяє забезпечити високу доступність, масштабованість та безпеку продукту, оскільки Microsoft має великий досвід у сфері хмарних технологій і активно вдосконалює заходи безпеки. Ці заходи включають шифрування даних у спокої, заходи фізичної та мережевої безпеки, а також системи виявлення та запобігання вторгненням.

Недоліком Teams є підвищені ризики небезпеки, пов’язані з тим, що кожен може створити команду або вільно завантажувати на канал файли з конфіденційною інформацією [10]. Крім того, невірна настройка конфігурації Teams, помилки у встановлені налаштування конфіденційності чи доступу, може призвести до небажаних витоків інформації або несанкціонованого доступу.

Б. СИСТЕМАТИЗАЦІЯ РЕЗУЛЬТАТІВ

В огляді [9] пропонуються й інші системи, як то Classcraft та Excalidraw. Але вони не є повноцінними навчальними середовищами, а тільки варіаціями інструментів, які можуть бути застосовані для організації дистанційного навчання, й можуть впливати на загальну захищеність навчального середовища при їх застосуванні, але у цій статті не розглядаються.

За даними [9], найбільша кількість вразливостей, які використовуються зловмисниками при атаках з зовнішньої мережі на LMC системи, виявлена в прикладних програмах, що активно застосовуються при підготовці матеріалів для наповнення систем дистанційного навчання. Ці програми включають в себе браузери, які використовуються користувачами СДН для доступу до веб-сайтів, а також Adobe Reader, Adobe Flash Player і Oracle Java, які використовуються для виконання скриптів і обробки документів та мультимедійних файлів.

Систематизуємо проблеми можливих порушень безпеки систем LMC (таблиця 1) і запропонуємо заходи захисту від найбільш активних погроз безпеки.

Таблиця 1. Проблеми захисту LMC - систем

№	Вразливості	LMC- системи						
		Google Classroom	*Edpuzzle*	*Canvas*	*Edmodo*	*Moodle*	*AhaSlides*	*Teams*
1	Несанкціонований доступ до акаунтів	+	+	+	+	+	+	+
2	Витік конфіденційної інформації	+		+				
3	Віруси та шкідливе програмне забезпечення	+				+		+
4	Неякісні практики захисту даних	+	+	+	+	+	+	+
5	Атаки з перехопленням (слабке шифрування)	+						
6	Вразливості програмного забезпечення		+	+	+	+	+	+
7	Застарілі версії			+		+	+	

ISSN 2786-9024

 https://doi.org/10.31474/2786-9024/v1i1(33).299636

8	Помилки в конфігурації							+
9	Недостатній контроль доступу		+	+	+		+	
10	Втрати даних		+	+	+		+	
11	Порушення правил безпеки користувачами					+	+	

Наведемо розшифровку вразливостей, перелічених в таблиці.

Несанкціонований доступ до акаунтів може включати вторгнення в акаунти користувачів, використання слабких паролів або злам паролів, а також атаки фішингу. Несанкціонований доступ може призвести до витоку конфіденційної інформації, такої як персональні дані учнів та викладачів.

Якщо дані захищено недостатньо й вони потрапляють до неправомірних рук, це може призвести до *витоку особистої інформації*, оцінок, завдань або іншої конфіденційної інформації.

Шкідливе програмне забезпечення може заражати пристрої користувачів, які використовують LMC – системи, поширювати конфіденційні дані або завдати шкоди комп’ютерам користувачів.

Під неякісними практиками захисту даних розуміємо недостатні заходи безпеки, такі як слабкі паролі, використання незахищених мереж Wi-Fi, недостатня організація користувацьких прав або невірна обробка конфіденційної інформації, які можуть підвищити ризик порушення безпеки.

Атаки з перехопленням. Можливість їх реалізації створюються, якщо дані, що передаються від користувача в систему (або канали передачі даних) не мають належного шифрування. Це може створити ризик перехоплення чутливої інформації в мережі.

Вразливості програмного забезпечення – це помилки в самих системах (характерно для нових або «свіже оновлених» розробок) й недостатньо перевірених плагінах можуть бути використані зловмисниками для отримання доступу до системи, внесення змін у інформацію або виконання злочинних дій.

Відсутність автоматичного оновлення систем, використання застарілих версій систем, або невчасне встановлення патчів можуть залишити систему вразливою до відомих атак та загроз безпеки.

Помилки в конфігурації, невірно встановлені налаштування конфіденційності чи доступу, може призвести до небажаних витоків інформації

+ *Неадекватно налаштований контроль доступу* до курсів та матеріалів може призвести до неправомірного доступу до конфіденційної інформації.

Втрати даних - непередбачені ситуації, такі як вірусні атаки або технічні проблеми, можуть призвести до втрати або пошкодження даних, які зберігаються в системі.

Таким чином, проблема безпеки LMC систем э комплексною та багатоаспектною задачею.

Заходи з захисту систем LMC (Language Model-based Conversational systems) повинні включати наступні процедури.

1. *Обов’язкове проведення аутентифікації та авторизації*. Слід відслідковувати й забезпечувати механізми аутентифікації користувачів, щоб вони могли взаємодіяти з системою лише після підтвердження своєї ідентичності. Права доступу користувачів повинні бути налаштовані таким чином, щоб забезпечувати обмеження доступу до адміністративного функціоналу системи.
2. *Регулярне оновлення програмного забезпечення*, що допоможе виявленню та усуненню вразливостей, які можуть бути застосовані зловмисниками для порушення безпеки LMC системи.
3. *Регулярні резервні копії* даних запобігають втраті інформації в разі кібератаки або технічних проблем.
4. *Шифрування даних*. Слід використовувати алгоритми надійного шифрування для захисту конфіденційної інформації, яка передається між користувачем і системою, а також для зберігання даних на сервері.
5. *Дотримання вимог щодо захисту* особистих даних користувачів та вимог законодавства щодо захисту даних дозволить запобігти витоку персональних даних.
6. *Захист від кібератак*. Рекомендується вживайте різноманітні заходи безпеки, такі як використання мережевих брандмауерів, систем виявлення вторгнень (IDS), і системи запобігання вторгненням (IPS) для захисту системи від різних видів кібератак, таких як DDoS або SQL ін'єкції.
7. *Аудит безпеки*. Регулярні аудити безпеки дозволять виявляти потенційні вразливості системи та вживати заході для їх усунення.
8. *Інструктажі користувачів систем*. Цей захід допоможе залучити учасників навчального процесу до розпізнавання потенційних загроз безпеки та активно реагувати на них. Тренінги з кібербезпеки слід проводити для всіх учасників, які користуються системою LMC.
9. *Доступ до даних слід обмежити* діючою політикою та розробленою й функціонуючою системою доступу.

Це загальні рекомендації. Їх реалізація для користувачів системи значно спрощується у випадку розміщення LMC системи на хмарних хостингах. Хмарні технології дозволяють вирішити практично всі вищезазначені проблеми та забезпечують захист, надійність, доступність та конфіденційність усіх складових складних і спеціалізованих структур, якими є навчальні системи та сучасні модулі управління освітнім контентом.

Аутентифікація й авторизація, створення резервних копій даних, налагодження автоматичного оновлення програмного забезпечення систем, стандартне, високоякісне шифрування даних, які зберігаються, накопичуються та обробляються в системі, шифрування даних при прийманні й передаванні, антивірусний контроль з залученням міжнародно сертифікованих пакетів, це лише короткий перелік переваг розміщення навчальних систем на хмарах. Тож першим питанням навчального закладу при обранні системи для організації навчального процесу повинно бути питання безпеки й пошук ресурсу, який цю безпеку гарантує.

Таким чином, застосування хмарних технологій в освітніх системах сприяє покращенню процесу навчання, захисту накопиченої в системах інформації, доступності освітніх заходів.

А способи розподілу ресурсів LMC систем з урахуванням вимог безпеки та гарантування підтримки високого рівня захищеності планується розглянути в наступних роботах авторів.

ВИСНОВКИ

Впровадження сучасних інформаційних технологій у навчанні дозволяє досягти запланованих результатів тільки за умови надійної, безпечної та продуктивної роботи всієї IT-інфраструктури. До неї пред'являються всі зростаючі вимоги підвищення продуктивності, надійності та захищеності при постійному збільшенні обсягів інформації, що обробляється.

У роботі досліджено проблеми захищеності сучасних LMC систем з урахуванням вразливостей програмного забезпечення, навчального контенту, результатів навчання та персональних даних учасників освітнього процесу, а також надання рекомендацій для організації захисту навчального електронного ресурсу.

Виявлено та проаналізовано проблеми захисту систем LMC з урахуванням сучасних загроз інформаційній безпеці.

Для семи найбільш поширених систем дистанційного навчання й систем керування навчанням виділено й з точки зору інформаційної безпеки систематизовано вразливості, характерні для систем.

Показано, що практично всі системи LMC, які входять в топ-7 найбільш поширених освітніх систем мають можливість встановлення на хмарних платформах. Застосування цих можливостей повинно сприяти підвищенню безпеки навчальних систем, уніфікації процедур захисту, доступності й надійності роботи й, як наслідок, підвищенню якості навчального процесу.

Але LMC системи - це складні структури. Застосування принципів розподілу й відокремлення різних частин систем з їх розміщенням на різних хмарних ресурсах є темою подальших досліджень.

ЛІТЕРАТУРА

[1] M. Averkina, Y. Lykhosherstova, “Digital platforms in interactive learning”, *Modeling the development of the economic systems*, vol. 2023, no. 1, pp. 128-132, 2023.

[2] Yong Chen, Wu He, “Security Risks and Protection in Online Learning: A Survey”, *The International Review of Research in Open and Distance Learning*, vol. 14, no. 5, pp. 108-127, 2013. DOI: 10.19173/irrodl.v14i5.1632

[3] О.О.Будік, В.Ф. Чекурін, “Специфічні загрози інформаційній безпеці систем електронного навчання”, *Вісник Національного університету "Львівська політехніка" Автоматика, вимірювання та керування*, no. 741, pp. 71-76, 2012. [Онлайн]. URL: http://surl.li/rlaos Дата звернення: 10.01.2024 .

[4] Kassid Asmaa, Elkamoun Najib, “E-Learning Systems Risks and their Security”, *International Journal of Computer Science andInformation Security (IJCSIS)*, vol. 14, no. 7, pp. 194-200, 2016.

[5] С.Жовтя, О. І. Полотай, “Програмний захист інформації в системі дистанційного навчання Moodle на основі операційної системи CentOS”, LSULS Digital Repository: Програмний захист інформації в системі дистанційного навчання Moodle на основі операційної системи CentOS (ldubgd.edu.ua). – 2015

[6] N. H. Phuoc Dai, A. Kerti, and Z. Rajnai, “ E-Learning Security Risks and Countermeasures”, *Emerging Research and Solutions in ICT*, vol. 1, no. 1, pp. 17-25, 2020. DOI: 10.20544/ERSICT.01.16.P02.

[7] O.Harasymchuk, I. Opirskyy, Y.Sovyn, I. Tyshyk, Y. Shtefaniuk, “Організація захисту результатів контролю знань в системах дистанційного навчання”, *Кібербезпека: освіта, наука, техніка*, vol. 2, no. 10, pp. 144-157, 2020. Doi: 10.28925/2663-4023.2020.10.144157.

[8] F. Schwarz, “E-Learning in den Ingenieurwissenschaften – Entwicklung”, Anwendung und Evaluation einer internetbasierten Lernumgebung: Doktor Ingenieur, 2009.

[9] Сім найкращих альтернатив Google Classroom, 2024. [Онлайн]. URL: http://surl.li/rlasn/. Дата звернення: 10.01.2024.

[10] Що таке Edpuzzle, 2024. [Онлайн]. URL: http://surl.li/rlatq. Дата звернення: 10.01.2024.

[11] О. Бєлов, М.М. Делембовський, Організація захисту і безпеки в системі «Moodle» Київський національний університет будівництва і архітектури, 2024. [Онлайн]. URL: http://surl.li/rlaum. Дата звернення: 10.01.2024.

ISSN 2786-9024

[12] Інформація з безпеки Moodle.org, URL, 2024. [Онлайн]. URL: http://surl.li/rlavn. Дата звернення: 10.01.2024.

SECURITY AND PROTECTION OF EDUCATIONAL LMC SYSTEMS

Nataliia Maslova, Olena Liubimenko

Information technologies play a significant role in the educational process and ensuring quality learning outcomes in the context of distance education. A modern trend is the development of interactive systems, which include elements of audio and video materials, graphics, presentations, internet links, materials from various sources, and in different formats. The addition of interactive content to educational systems increases the risks of information security in modern LMC systems. Emphasis is placed on the need to ensure the protection of software in systems, educational content hosted within them, learning outcomes, and participants' personal data. When building protection, attention should be paid to potential threats such as unauthorized access, flawed software, poor plugin updates, material copying, fraud, and cyber-attacks. Vulnerabilities of the most widespread modern LMC systems are analyzed. Attention is given to the possibilities of using cloud technologies to host system modules, educational materials, or learning outcomes on cloud services. Cloud application guarantees constant access to the learning system, reliable storage of materials, additional protection of confidential and personal information. Therefore, to ensure effective and safe learning considering modern interactive approaches to presenting educational materials, it is important to develop systems and implement technologies that provide constant access to educational content, reliable data protection (including personal data), information integrity, and compliance with confidentiality principles.

Keywords: *LMC systems, interactive learning, vulnerabilities of distance learning systems, protection, cloud technologies, confidentiality, accessibility, integrity, reliability, information, personal data, educational content.*

REFERENCES

[1] M. Averkina, Y. Lykhosherstova, “Digital platforms in interactive learning”, *Modeling the development of the economic systems*, vol. 2023, no. 1, pp. 128-132, 2023.

[2] Yong Chen, Wu He, “Security Risks and Protection in Online Learning: A Survey”, *The International Review of Research in Open and Distance Learning*, vol. 14, no. 5, pp. 108-127, 2013. DOI: 10.19173/irrodl.v14i5.1632.

[3] O.O.Budik, V.F. Chekurin, “Spetsyfichni zahrozy informatsiinii bezpetsi system elektronnoho navchannia”, Visnyk Natsionalnoho universytetu "Lvivska politekhnika" Avtomatyka, vymiriuvannia ta keruvannia, no. 741, pp. 71-76, 2012. [Online]. URL: http://surl.li/rlaos. Accessed: 10.01.2024. (In Ukranian).

[4] Kassid Asmaa, Elkamoun Najib, “E-Learning Systems Risks and their Security”, *International Journal of Computer Science andInformation Security (IJCSIS)*, vol. 14, no. 7, pp. 194-200, 2016.

[5] S.Zhovtia, O. I. Polotai, “Prohramnyi zakhyst informatsii v systemi dystantsiinoho navchannia Moodle na osnovi operatsiinoi systemy CentOS”, LSULS Digital Repository: Prohramnyi zakhyst informatsii v systemi dystantsiinoho navchannia Moodle na osnovi operatsiinoi systemy CentOS (ldubgd.edu.ua), 2015. (In Ukranian).

[6] N. H. Phuoc Dai, A. Kerti, and Z. Rajnai, “ E-Learning Security Risks and Countermeasures”, *Emerging Research and Solutions in ICT*, vol. 1, no. 1, pp. 17-25, 2020. DOI: 10.20544/ERSICT.01.16.P02.

[7] O.Harasymchuk, I. Opirskyy, Y.Sovyn, I. Tyshyk, Y. Shtefaniuk, “Orhanizatsiia zakhystu rezultativ kontroliu znan v systemakh dystantsiinoho navchannia”, *Kiberbezpeka: osvita, nauka, tekhnika*, vol. 2, no. 10, pp. 144-157, 2020. Doi: 10.28925/2663-4023.2020.10.144157. (In Ukranian).

[8] F. Schwarz, “E-Learning in den Ingenieurwissenschaften – Entwicklung”, Anwendung und Evaluation einer internetbasierten Lernumgebung: Doktor Ingenieur, 2009.

[9] Сім найкращих альтернатив Google Classroom, 2024. [Online]. URL: http://surl.li/rlasn/. Accessed: 10.01.2024.

[10] Shcho take Edpuzzle, 2024. [Online]. URL: http://surl.li/rlatq. Accessed: 10.01.2024. (In Ukranian).

[11] O. Bielov, M.M. Delembovskyi, Orhanizatsiia zakhystu i bezpeky v systemi «Moodle» Kyivskyi natsionalnyi universytet budivnytstva i arkhitektury, 2024. [Online]. URL: http://surl.li/rlaum. Accessed: 10.01.2024. (In Ukranian).

[12] Informatsiia z bezpeky Moodle.org, URL, 2024. [Online]. URL: http://surl.li/rlavn. Accessed: 10.01.2024. (In Ukranian).