УДК 37.018.43:004.056 **doi: 10.32620/reks.2020.4.08**

А. Г. ТЕЦЬКИЙ, О. І. МОРОЗОВА

Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Україна

АСПЕКТИ КІБЕРБЕЗПЕКИ ПЛАТФОРМ ДИСТАНЦІЙНОГО НАВЧАННЯ

Предметом *вивчення в статті є платформи, що використовуються для організації навчального процесу в умовах дистанційного навчання. Серед таких платформ виділено наступні: використання систем керування освітнім вмістом (системи з відкритим вихідним кодом та індивідуального розроблення), використання сервісу Google Classroom, використання електронної пошти і хмарних сховищ даних. Показано об'єкти навчального процесу, для яких має бути забезпечений стан захищеності. Такими активами є файли (лекції, завдання на лабораторні роботи), банк питань (загальна множина питань, з яких створюються тести для контролю знань) та оцінки (за лабораторні роботи та модульний контроль знань).* ***Метою*** *роботи є порівняльний аналіз платформ дистанційного навчання в аспекті кібербезпеки. Основними загрозами є порушення доступності та конфіденційності даних навчального процесу. Також можлива модифікація оцінок унаслідок експлуатації вразливостей системи чи отримання доступу до функцій адміністратора системи керування освітнім вмістом. Імовірність компрометації даних вище, ніж імовірність модифікації, це підтверджується інформацією з баз даних вразливостей про численні вразливості систем керування освітнім вмістом. Порушення доступності є наслідком відмови в обслуговуванні, тобто ресурс, на якому розміщено необхідні файли, стає недоступним для користувачів. Використовується* ***метод*** *експертного оцінювання зі змінними нечіткої логіки. У* ***результаті*** *аналізу виявлено, що найбільш гнучкою та зручною платформою є система керування освітнім вмістом індивідуального розроблення, у той же час вона є найменш безпечною серед розглянутих платформ. Більш безпечною платформою через наявність світової спільноти, здатної виявляти проблеми безпеки раніше зловмисників, є система керування освітнім вмістом з відкритим вихідним кодом. Використання сервісу Google Classroom та використання електронної пошти і хмарних сховищ даних є більш безпечним, але ці підходи поступаються у зручності та функціональних можливостях.* ***Висновки.*** *Вибір платформи дистанційного навчання – це пошук компромісу між безпекою та зручністю у вигляді широкої функціональності системи. При розгортанні централізованої системи керування освітнім вмістом важливо пам'ятати, що ця система є об'єктом критичної інформаційної інфраструктури, і для неї повинні виконуватися вимоги до критичних систем.*

Ключові слова: *дистанційне навчання; системи керування освітнім вмістом; кібербезпека; критична інформаційна інфраструктура.*

Вступ

Застосування сучасних технологій в навчальному процесі дозволяє зменшити одноманітність освітнього середовища і знизити часові витрати на супутні процеси. Простим прикладом такого процесу є звіт студента про виконання лабораторної роботи. До недавніх пір студенти повинні були витрачати час і гроші на друк звітів, викладач після завершення аудиторного заняття повинен був виконати роботу по переміщенню прийнятих звітів у викладацьку. До кінця семестру збиралася велика кількість звітів, які мають бути передані відповідним чином на зберігання. Рішенням цієї проблеми стали електронні звіти. Використання систем керування освітнім вмістом (англ. «Learning Content Management System», LCMS) надає можливість централізованого збору звітів [1]. Використовуючи свої облікові записи, студенти завантажують звіти через вебінтерфейс, викладач їх оцінює, студент бачить свої оцінки в електронному журналі. На кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» системи керування освітнім вмістом використовуються понад вісім років, у даний момент паралельно працюють системи Sakai і MOODLE. З самого початку ці системи користувалися особливою популярністю у молодих викладачів, які гідно оцінили переваги використання таких ресурсів в освітньому процесі.

Найпростішим способом передачі електронного звіту від студента до викладача є відправлення листом електронною поштою. Такий підхід є незручним, оскільки звіти не структуруються у сховищі, викладачеві потрібно повідомити оцінку студенту шляхом відправлення листа у відповідь.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Також у період пандемії отримав велику популярність Google Classroom – безкоштовний вебсервіс, розроблений Google для шкіл, який покликаний спростити створення, поширення й оцінювання завдань [2].

Під час онлайн-навчання збільшилась кількість кіберінцидентів за участі ресурсів, що використовуються для організації освітнього процесу. «Лідером» стало програмне забезпечення Zoom, яке дає змогу створювати онлайн-конференції. Основним вектором атак є встановлення шкідливого програмного забезпечення під виглядом програми Zoom від оригінального постачальника. На другому місці виявилась система керування освітнім вмістом MOODLE, де основним вектором атак стало розсилання електронних листів з посиланнями на фішингові сторінки для авторизації [3].

Як і будь-які веб-ресурси, системи керування освітнім вмістом можуть бути об'єктом кібератак [4]. Усі вищезгадані платформи дистанційного навчання мають свої особливості, у тому числі й у плані кібербезпеки. Метою роботи є порівняльний аналіз платформ дистанційного навчання в аспекті кібербезпеки.

Аналіз платформ

Для початку визначимо активи навчального процесу і відповідні загрози. Основними активами є такі:

– файли (лекції, завдання на лабораторні роботи тощо);

– банк питань (загальна множина питань, з яких створюються тести для контролю знань);

– оцінки (лабораторні роботи та модульний контроль знань).

Активом називається об'єкт, для якого забезпечується стан захищеності [5].

Далі визначимо можливі загрози для зазначених активів.

Порушення доступності є наслідком відмови в обслуговуванні [6]. Простіше кажучи, ресурс, на якому розміщені потрібні файли, стає недоступним для користувачів. Студенти не можуть отримати завдання, завантажити звіт або пройти тестування. Викладач не може додати нові файли або перевірити раніше завантажені звіти. Фактично така проблема є критичною для навчального процесу.

Компрометація банку питань може виникнути шляхом експлуатації вразливостей системи або шляхом отримання доступу до панелі адміністратора системи [7]. Сценарії таких атак розглянуті в [8]. Банк питань містить питання, варіанти відповідей і правильні відповіді, якщо такі є.

Модифікація оцінок з лабораторних робіт і модулів з'являється у порушника з тих же причин, що і компрометація банку питань.

Платформами, які розглядаються, є:

– системи керування освітнім вмістом з відкритим вихідним кодом;

– системи керування освітнім вмістом індивідуального розроблення;

– сервіс Google Classroom;

– електронна пошта і хмарні сховища.

Звісно ж, це не всі платформи, які можуть бути використані для дистанційного навчання. Вибір саме цих платформ зумовлений їх популярністю у всьому світі, усі вони використовуються на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».

Системи керування освітнім вмістом з відкритим вихідним кодом представляють клас систем, які дозволяють розгортати веб-ресурси для здійснення освітнього процесу. Прикладами таких систем є MOODLE і Sakai, кількість їх інсталяцій вимірюється сотнями тисяч [9]. Особливістю таких систем є наявність спільноти, яка виявляє проблеми безпеки і може виявити проблеми швидше зловмисників. Розробники системи сповіщаються про знайдену проблему, яка усувається шляхом випуску нової версії або установки патча для існуючої версії. Для коректного функціонування при великій кількості активних користувачів система вимагає досить велику кількість ресурсів, тому доцільно такі системи розгортати на окремому сервері. Хостинг-провайдери не рекомендують (а іноді й забороняють) встановлення таких систем на спільному хостингу.

Основною відмінністю в аспекті безпеки систем керування освітнім вмістом індивідуального розроблення є відсутність великої спільноти, здатної виявити проблеми безпеки. Дуже велику роль грає рівень професіоналізму розробників такої системи, оскільки ризик написання небезпечного коду у розробників-початківців набагато вище. Оскільки така система належить класу «mission critical», логічним і обґрунтованим є виконання тестування на проникнення як етапу життєвого циклу програмного забезпечення [10, 11].

Сервіс Google Classroom є безкоштовним, дозволяє розміщувати освітні матеріали й керувати учасниками освітнього процесу. Особливістю є те, що для створення нового ресурсу немає необхідності у використанні додаткової сторонньої інформаційної інфраструктури. Сервіс має набагато меншу гнучкість, ніж системи керування освітнім вмістом, які дозволяють розширювати функціональність шляхом встановлення різних модулів.

Електронну пошту і хмарні сховища складно назвати повноцінною платформою для дистанційної освіти, проте цей підхід також використовується через свою простоту. При цьому гнучкість і зручність користування є мінімальними серед розглянутих платформ.

Нижче наведено таблицю 1 з експертними оцінками загроз для платформ у вигляді змінних нечіткої логіки. Оцінки відображають суб'єктивну думку авторів статті, засновану на багаторічному досвіді адміністрування системи керування освітнім вмістом, розроблення веб-ресурсів і тестування їх на проникнення.

Припущенням є те, що системи керування освітнім вмістом розгорнуті на веб-сервері традиційним способом – без балансувальника навантаження і без можливості динамічного масштабування в межах інфраструктури. Також припущенням є рівнозначність критеріїв оцінювання, але також є можливим використання підходу зі зваженими коефіцієнтами.

Різні оцінки ймовірності порушення доступності різних платформ обумовлені особливостями реалізації – перші дві платформи, як правило, створюються у вигляді централізованого ресурсу, інші дві платформи реалізовані на децентралізованій інфраструктурі.

Відмінності в можливості модифікації і компрометації даних обумовлені можливими вразливостями в платформах. LCMS з відкритим вихідним кодом мають оцінки нижче, ніж LCMS індивідуального розроблення через те, що перші, як правило, мають велику спільноту, яка здатна виявляти проблеми безпеки швидше, ніж зловмисники. Імовірність компрометації даних вище, ніж імовірність модифікації, що підтверджується інформацією з баз даних вразливостей про численні вразливості систем керування освітнім вмістом [12]. Розглядаючи атаки, пов'язані з модифікацією запитів до бази даних (SQL-ін'єкція), проблема частіше зустрічається в запитах на отримання даних, ніж у запитах на вставлення й оновлення.

Для представлених в таблиці 1 платформ справедливим є такий порядок (у порядку збільшення ймовірності реалізації загроз):

– електронна пошта і хмарні сховища;
– сервіс Google Class;
– LCMS (відкритий вихідний код);
– LCMS (індивідуального розроблення).

Висновки

Представлений вище порядок був заснований лише на аспекті кібербезпеки платформ. Цей же порядок є справедливим для сортування платформ за гнучкістю і зручністю використання – найбільш зручна система є найнебезпечнішою. Проблема вибору – це пошук компромісу між безпекою та зручністю у вигляді широкої функціональності системи. При розгортанні системи керування освітнім вмістом важливо пам'ятати, що ця система є об'єктом критичної інформаційної інфраструктури, і для неї повинні виконуватися вимоги до критичних систем, зокрема використовуватися механізми створення резервних копій, повинні бути розроблені схеми максимально швидкого відновлення робочого стану.

Подальші дослідження можуть бути спрямовані на дослідження проблем безпеки у межах одного класу систем керування освітнім вмістом з відкритим вихідним кодом.

Література

1. Sejzi, A. A. Learning Management System (LMS) and Learning Content Management System (LCMS) at Virtual University [Text] / A. A. Sejzi, B. Arisa // Proc. 2nd International Seminar on Quality and Affordable Education, 2018. – P. 216-220.

2. Iftakhar, S. Google classroom: what works and how [Text] / S. Iftakhar // Journal of Education and Social Sciences. – 2016. – Vol. 3, No. 1. – P. 12-18.

3. Digital Education: The cyberrisks of the online classroom [Electronic resource] – Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf. – 11.10.2020.

4. Barhoom, T. S. Enhance MOODLE security against XSS vulnerabilities [Text] / T. S. Barhoom, R. J. Azaiza // International Journal of Computing and Digital Systems. – 2016. – Vol. 5, No. 5. – P. 421-430.

Таблиця 1

Оцінки загроз для платформ дистанційного навчання

Загрози / Платформи	LCMS (відкритий вихідний код)	LCMS (індивідуального розроблення)	Сервіс Google Class	Ел. пошта і хмарні сховища
Порушення доступності	Високий	Високий	Низький	Низький
Можливість модифікації даних	Низький	Середній	Нижче середнього	Низький
Можливість компрометації даних	Середній	Високий	Нижче середнього	Низький

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

5. Craigen, D. Defining cybersecurity [Electronic resource] / D. Craigen, N. Diakun-Thibault, R. Purse // Technology Innovation Management Review. – 2014. – Vol. 4, No. 10. – Available at: https://timreview.ca/article/835. – 11.10.2020.

6. Internet denial of service: attack and defense mechanisms (Radia Perlman Computer Networking and Security) [Text] / J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher. – Prentice Hall, 2004. – 400 p.

7. Flow-based web application brute-force attack and compromise detection [Text] / R. Hofstede, M. Jonker, A. Sperotto, A. Pras // Journal of network and systems management. – 2017. – Vol. 25, No. 4. – P. 735-758.

8. Тецкий, А. Г. Применение деревьев атак для оценивания вероятности успешной атаки web-приложения [Текст] / А. Г. Тецкий // Радіоелектронні і комп'ютерні системи. – 2018. – № 3 (87). – С. 74-79. DOI: 10.32620/reks.2018.3.08.

9. Learning Management System Usage Distribution on the Entire Internet [Electronic resource]. – Available at: https://trends.builtwith.com/cms/learning-management-system/traffic/Entire-Internet. – 11.10.2020.

10. Классификация критичности информационных систем [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/512556/. – 11.10.2020.

11. Web Application Security Assessment [Electronic resource]. – Available at: https://www.whitehatsec.com/glossary/content/web-application-security-assessment. – 11.10.2020.

12. National Vulnerability Database [Electronic resource]. – Available at: https://nvd.nist.gov/. – 11.10.2020.

References

1. Sejzi, A. A., Arisa, B. Learning Management System (LMS) and Learning Content Management System (LCMS) at Virtual University. *Proc. 2nd International Seminar on Quality and Affordable Education*, 2018, pp. 216-220.

2. Iftakhar, S. Google classroom: what works and how. *Journal of Education and Social Sciences*, 2016, vol. 3, no. 1, pp. 12-18.

3. *Digital Education: The cyberrisks of the online classroom.* Available at: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2020/09/04113558/education_report_04092020_2.pdf (accessed 11.10.2020).

4. Barhoom, T. S., Azaiza, R. J. Enhance MOODLE security against XSS vulnerabilities. *International Journal of Computing and Digital Systems*, 2016, vol. 5, no. 5, pp. 421-430.

5. Craigen, D. Diakun-Thibault, N., Purse, R. Defining cybersecurity. *Technology Innovation Management Review*, 2014, vol. 4, no. 10. Available at: https://timreview.ca/article/835 (accessed 11.10.2020).

6. Mirkovic, J., Dietrich, S., Dittrich, D., Reiher, P. *Internet denial of service: attack and defense mechanisms (Radia Perlman Computer Networking and Security)*. Prentice Hall, 2004. 400 p.

7. Hofstede, R., Jonker, M., Sperotto, A., Pras, A. Flow-based web application brute-force attack and compromise detection. *Journal of network and systems management*, 2017, vol. 25, no. 4, pp. 735-758.

8. Tetskiy, A. G. Primenenie derev'ev atak dlya otsenivaniya veroyatnosti uspeshnnoi ataki web-prilozheniya [Applying of attack trees for estimation the probability of a successful attack of the web-application]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2018, no. 3 (87), pp. 74-79. DOI: 10.32620/reks.2018.3.08.

9. *Learning Management System Usage Distribution on the Entire Internet*. Available at: https://trends.builtwith.com/cms/learning-management-system/traffic/Entire-Internet (accessed 11.10.2020).

10. *Klassifikatsiya kritichnosti informatsionnyh sistem* [Criticality classification of information systems]. Available at: https://habr.com/ru/post/512556/ (accessed 11.10.2020).

11. *Web Application Security Assessment*. Available at: https://www.whitehatsec.com/glossary/content/web-application-security-assessment (accessed 11.10.2020).

12. *National Vulnerability Database*. Available at: https://nvd.nist.gov/ (accessed 11.10.2020).

Надійшла до редакції 12.10.2020, розглянута на редколегії 16.11.2020

АСПЕКТЫ КИБЕРБЕЗОПАСНОСТИ ПЛАТФОРМ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

А. Г. Тецкий, О. И. Морозова

Предметом изучения в статье являются платформы, используемые для организации учебного процесса в условиях дистанционного обучения. Среди таких платформ выделены следующие: использование систем управления образовательным содержимым (системы с открытым исходным кодом и индивидуальной разработки), использование сервиса Google Classroom, использование электронной почты и облачных хранилищ данных. Показано объекты учебного процесса, для которых должно быть обеспечено состояние защищенности. Такими активами являются файлы (лекции, задания на лабораторные работы), банк вопросов (общее множество вопросов, из которых создаются тесты для контроля знаний) и оценки (за лабораторные работы и модульный контроль знаний). **Целью** работы является сравнительный анализ платформ дистанционного обучения в аспекте кибербезопасности. Основными угрозами являются нарушение доступности и конфиденциальности данных учебного процесса. Также возможна модификация оценок вследствие эксплуатации

уязвимостей системы или получения доступа к функциям администратора системы управления образовательным содержимым. Вероятность компрометации данных выше, чем вероятность модификации, это подтверждается информацией из баз данных уязвимостей о многочисленных уязвимостях систем управления образовательным содержимым. Нарушение доступности является следствием отказа в обслуживании, то есть ресурс, на котором размещены необходимые файлы, становится недоступным для пользователей. Используется **метод** экспертного оценивания с переменными нечеткой логики. В **результате** анализа выявлено, что наиболее гибкой и удобной платформой является система управления образовательным содержимым индивидуальной разработки, в то же время она является наименее безопасной среди рассмотренных платформ. Более безопасной платформой из-за наличия мирового сообщества, способной выявлять проблемы безопасности быстрее злоумышленников, является система управления образовательным содержимым с открытым исходным кодом. Использование сервиса Google Classroom и использование электронной почты с облачными хранилищами данных является более безопасным, но эти подходы уступают в удобстве и функциональных возможностях. **Выводы.** Выбор платформы дистанционного обучения – это поиск компромисса между безопасностью и удобством в виде широкой функциональности системы. При развертывании централизованной системы управления образовательным содержимым важно помнить, что эта система является объектом критической информационной инфраструктуры, и для нее должны выполняться требования к критическим системам.

Ключевые слова: дистанционное обучение; системы управления образовательным содержимым; кибербезопасность; критическая информационная инфраструктура.

CYBERSECURITY ASPECTS OF E-LEARNING PLATFORMS

A. Tetskyi, O. Morozova

The **subject** of study in the article is the platforms used to organize the educational process in the context of distance learning. The following platforms are selected: learning content management systems (open source systems and individual development), Google Classroom service, e-mail, and cloud data storage. The objects of the educational process for which the security state must be provided are shown. Such assets are files (lectures, tasks for laboratory work), a bank of questions (a total set of questions from which tests are created to control knowledge), and grades (for laboratory work and modular control of knowledge). The **goal** of the work is a comparative analysis of distance learning platforms in the aspect of cybersecurity. The main threats are a violation of the availability and confidentiality of data in the educational process. It is also possible to modify marks due to the exploitation vulnerabilities of the system or gaining access to the functions of the learning content management system administrator. The probability of data being compromised is higher than the probability of modification, as evidenced by information from vulnerability databases about numerous vulnerabilities in learning content management systems. An accessibility violation is a result of a denial of service, that is, the resource on which the necessary files are located becomes inaccessible to users. The **method** of expert evaluation with variables of fuzzy logic is used. As a **result** of the analysis, it was revealed that the most flexible and convenient platform is the learning content management system of individual development, at the same time it is the most unsecure among the platforms considered. An open-source learning content management system is a more secure platform due to the presence of a global community that can identify security problems faster than attackers. Using Google Classroom and using email with cloud storage is safer, but these approaches are inferior in usability and functionality. **Conclusions.** Choosing a distance-learning platform is about finding a compromise between security and convenience in the form of a wide functionality of the system. When deploying a centralized learning content management system, it is important to remember that this system is an object of critical information infrastructure, and the requirements for critical systems must be met for it.

Keywords: distance learning; learning content management systems; cybersecurity; critical information infrastructure.

Тецький Артем Григорович – канд. техн. наук, асист. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Морозова Ольга Ігорівна – д-р техн. наук, доц., доц. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Tetskyi Artem Grygorovych – Candidate of Technical Science, Assistant Lecturer of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: a.tetskiy@csn.khai.edu, ORCID: 0000-0003-1745-2452.

Morozova Olha Ihorivna – Doctor of Technical Science, Associate Professor of Dept. of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine, e-mail: o.morozova@csn.khai.edu, ORCID: 0000-0001-7706-3155.