УДК 004.77
DOI https://doi.org/10.32782/IT/2022-3-1

Олександр В'ЮНЕНКО
кандидат економічних наук, доцент, доцент кафедри кібернетики і інформатики, Сумський національний аграрний університет, Суми, вул. Герасима Кондратьєва, 160, 40021
ut2ab@ukr.net
***ORCID:** 0000-0002-8835-0704*

Світлана ВИГАНЯЙЛО
кандидат економічних наук, доцент, доцент кафедри соціально-економічних наук, Сумська філія Харківського національного університету внутрішніх справ, Суми, вул. Миру, 24
vyganyaylosvitlana@ukr.net
***ORCID:** 0000-0001-5350-0728*

Бібліографічний опис статті: В'юненко, О., Виганяйло, С. (2022). Проблеми підвищення кібербезпеки систем електронного навчання. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 3, 3–10, doi: https://doi.org/10.32782/IT/2022-3-1

ПРОБЛЕМИ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

Навчання у вищих навчальних закладах країни на сьогоднішньому етапі передбачає дистанційне електронне навчання, оскільки університети проводять лекційні заняття, практичні та семінарські заняття, а також онлайн-курси, тренінги та інші освітні послуги для здобувачів різних напрямків освіти. Проте надання онлайн-освіти пов'язане зі своїми проблемами, включаючи забезпечення безпеки системи електронного навчання та її захист від кіберзагроз. Недавнє збільшення кібератак на університети підкреслило потребу в безпечній і надійній платформі для онлайн-освіти. У зв'язку з цим розглядається необхідність переходу системи дистанційного електронного навчання університету до роботи на хмарній платформі. Дослідження розглядає та аналізує проблеми, з якими стикаються університети під час надання онлайн-освіти, і переваги, які може надати хмарна система електронного навчання. Перехід на хмарну платформу може значно підвищити безпеку системи та забезпечити її захист від кіберзагроз. Дослідження містить огляд поточного стану систем електронного навчання, їхні виклики та переваги хмарних обчислень в освіті, також дослідження проблеми безпеки, з якими стикається середовище електронного навчання у вищих навчальних закладах, а також засоби захисту при загрозах інформаційній безпеці для забезпечення ефективного електронного навчального середовища. Адже хмарні платформи використовують розширені заходи безпеки, як-от шифрування, для захисту конфіденційних даних. Хмарні провайдери постійно оновлюють свої заходи безпеки, забезпечуючи належний рівень захисту, якого університети навряд чи змогли б досягти самостійно. Дотримується захищений механізм конфіденційності користувача, за рахунок методів аутентифікації, авторизації та доставки електронного контенту до користувачів.

Авторами надано рекомендації щодо подальшого розвитку системи дистанційного електронного навчання та зроблено висновок, що перехід на хмарну платформу є вирішальним для довгострокового успіху онлайн-освіти.

***Ключові слова:** інформаційна безпека, системи дистанційного електронного навчання, дистанційна освіта, хмарна система електронного навчання.*

Oleksandr VIUNENKO
Candidate of Economics Sciences, Associate Professor, Associate Professor of the Department of Cybernetics and Informatics, Sumy National Agrarian University, 160 Gerasyma Kondratyeva Street., Sumy, 40021
ut2ab@ukr.net
***ORCID:** 0000-0002-8835-0704*

Svitlana VYHANIAILO
Candidate of Economics Sciences, Associate Professor, Associate Professor of the Department of Socio-Economic Disciplines, Sumy Branch of Kharkiv National University of Internal Affairs, Sumy Street Peace, 24, 40000
vyganyaylosvitlana@ukr.net
***ORCID:** 0000-0001-5350-0728*

To cite this article: V'yunenko, O., Viganyajlo S. (2022). Problemi pi`dvishhennya ki`berbezpeki sistem elektronnogo navchannya [Problems of increasing the level of cyber security of electronic learning systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 3, 3–10, doi: https://doi.org/10.32782/IT/2022-3-1

PROBLEMS OF INCREASING THE LEVEL OF CYBER SECURITY OF ELECTRONIC LEARNING SYSTEMS

Education in the country's higher education institutions currently involves distance e-learning, as universities provide lectures, practical and seminar classes, as well as online courses, trainings and other educational services for students of various fields of study. However, the provision of online education comes with its own challenges, including ensuring the security of the e-learning system and protecting it from cyber threats. The recent increase in cyberattacks on universities has emphasized the need for a safe and reliable platform for online education. In this regard, the need to transition the university's distance e-learning system to a cloud-based platform is considered. The study examines and analyzes the challenges that universities face in delivering online education and the benefits that a cloud-based e-learning system can provide. Moving to a cloud-based platform can significantly improve the security of the system and ensure its protection against cyber threats. The study provides an overview of the current state of e-learning systems, their challenges, and the benefits of cloud computing in education, as well as a study of the security challenges faced by the e-learning environment in higher education institutions, and the means of protecting against information security threats to ensure an effective e-learning environment. After all, cloud platforms use advanced security measures, such as encryption, to protect sensitive data. Cloud providers are constantly updating their security measures, providing an adequate level of protection that universities could hardly achieve on their own. A secure mechanism for user privacy is observed, due to the methods of authentication, authorization and delivery of electronic content to users.

The authors provide recommendations for the further development of the distance e-learning system and conclude that the transition to a cloud platform is crucial for the long-term success of online education.

Key words: *information security, distance e-learning systems, distance education, cloud-based e-learning system.*

Актуальність проблеми. Останні події в соціальному та політичному житті українського суспільства та у всьому світі, а також високий рівень розвитку інформаційних технологій потребує переорієнтації сучасної освіти та перерозподілу напрямків її розвитку з використанням дистанційного електронного навчання. Проте надання онлайн-освіти пов’язане зі своїми проблемами, включаючи забезпечення безпеки системи електронного навчання та її захист від кіберзагроз. Недавнє збільшення кібератак на університети підкреслило потребу в безпечній і надійній платформі для онлайн-освіти. Це дослідження має на меті дослідити проблеми безпеки, з якими стикається середовище електронного навчання у вищих навчальних закладах, а також засоби захисту при загрозах інформаційній безпеці для забезпечення ефективного електронного навчального середовища (Толбатов, В., 2019).

Аналіз останніх досліджень і публікацій. Останні дослідження в галузі безпеки електронного навчання акцентують увагу на наступних аспектах:

1. Захист персональних даних студентів: Дослідження виявили, що велика кількість електронних систем навчання мають недостатній рівень захисту персональних даних студентів, що може призвести до зловживання даними.

2. Безпека мережі: Електронні системи навчання можуть стати об'єктом кібератак, що може призвести до витоку конфіденційної інформації та порушення роботи системи навчання. Останні дослідження показують, що багато систем навчання мають недостатній рівень захисту від кібератак.

3. Автентифікація користувачів: Цей аспект стає все більш важливим в електронному навчанні. Останні дослідження зосереджуються на розробці та вдосконаленні методів автентифікації користувачів, таких як біометрична ідентифікація, двофакторна автентифікація тощо.

4. Боротьба з плагіатом: Електронні системи навчання можуть стати джерелом плагіату, що може вплинути на якість навчання та оцінювання.

За останні роки дослідження зосереджуються на розробці та вдосконаленні програмних засобів для виявлення плагіату в електронних текстах та завданнях, і лише деякі з численних досліджень та публікацій на тему безпеки електронних систем дистанційного навчання. Закордонні автори, що зосереджуються на безпеці електронного навчання, включають таких дослідників, як: Zafar Aasim, Alghazzawi D., Hamid Syed, які у своїй статті «Системи електронного навчання та їх безпека» намагаються продемонструвати поєднання трьох технологій,

а саме стандартів безпеки системи, мультиагентів і систем електронного навчання. Методи, орієнтовані на агентів, які сприятимуть покращенню концептуалізації багатоагентних систем, оскільки вони вже почали включати стандарти FIPA для загальної безпеки (Zafar, Aasim & Alghazzawi, D. & Hamid, Syed., 2014). Авторb Chen Yong, He Wu у публікації «Ризики та захист безпеки в онлайн-навчанні» намагається визначити, наскільки постачальники онлайн-навчання усвідомлюють потенційні ризики безпеці та заходи захисту, які їх зменшать. Результати опитування підтверджують, що постачальники онлайн-навчання та практики не вважали безпеку своїм головним пріоритетом. (Chen Yong, He Wu, 2013). Автори Dima A, Bugheanu A-M, Boghian R, Madsen D. У своєму дослідженні на тему «Картування аналізу області знань в системах електронного навчання на основі хмарних обчислень» проводять оцінки наукової продукції у сфері електронного навчання та хмарних технологій за допомогою кількісного підходу методу бібліометричного аналізу з метою всебічного огляду та аналізу теми. (Dima A, Bugheanu A-M, Boghian R, Madsen DØ, 2023).

Тема безпеки електронних систем дистанційного навчання цікавить і українських авторів. Так автор Кухаренко у роботі «Розробка сучасної системи електронного навчання в університеті» визначає основні елементи, які створюють глобальну систему електронного навчання, і визначити структуру системи для використання в навчальних закладах. Показує, що на першому етапі дистанційні курси відігравали роль доставки навчальних матеріалів до студента. Розробка web 2. 0 технології та поява LMS змінили спосіб навчання. Педагогічні теорії, педагогічна навчальна модель ADDIE та використання таксономії Блума дозволили студентам співпрацювати та активно спілкуватися. (Кухаренко В.М., 2020).

Визначення мети дослідження. У вищих навчальних закладах середовище електронного навчання використовується для забезпечення якісної освіти є все більш затребувaним. Воно може включати в себе використання відео- та аудіо-матеріалів, онлайн-курсів, тестів, інтерактивних платформ, форумів для обговорення матеріалів та багато іншого. Однак, збільшення використання електронного навчання вищих навчальних закладів також створює загрози для інформаційної безпеки студентів та викладачів. Мета нашого дослідження полягає у визначенні та класифікації існуючих та потенційних загроз, визначенні різних засобів захисту, та пропозиції і аргументації вирішення даної проблеми.

Основна частина. Однією з найбільших проблем, з якою стикаються університети під час надання онлайн-освіти, є забезпечення безпеки їхніх систем електронного навчання. Такі кіберзагрози, як хакерство, фішинг і атаки зловмисного програмного забезпечення, становлять значний ризик для безпеки платформ електронного навчання. У нещодавньому звіті Агентства з кібербезпеки та безпеки інфраструктури (CISA) виявлено, що кібератаки на університети значно зросли за останні роки: більшість університетів повідомляють про значне збільшення кількості інцидентів порівняно з попередніми роками. Зокрема, можуть бути використані хакерські атаки, шпигунство, крадіжки особистих даних та інші загрози. Для захисту від таких загроз вищі навчальні заклади можуть використовувати різні засоби захисту, такі як:

1. Криптографічні методи: використовуються для захисту конфіденційної інформації шляхом шифрування даних.

2. Фізичний захист: включає в себе захист комп'ютерів, мереж та інших пристроїв, що використовуються для електронного навчання.

3. Програмне забезпечення для захисту: використовується для захисту від вірусів, шпигунського програмного забезпечення, зловмисних програм та інших загроз.

4. Політики безпеки: включають у себе правила та процедури, які встановлюються для захисту конфіденційної інформації.

5. Аудит безпеки: використовується для перевірки наявності потенційних загроз та слабких місць у системах електронного навчання.

Взагалі, забезпечення інформаційної безпеки є важливим аспектом використання середовищ електронного дистанційного навчання.

Щоб вирішити ці проблеми, університети звертаються до хмарних систем електронного навчання, які забезпечують більш безпечну та надійну платформу для онлайн-освіти. Хмарні обчислення пропонують низку переваг, включаючи покращену масштабованість, гнучкість і безпеку. Використовуючи хмарну платформу, університети можуть забезпечити захист своїх систем електронного навчання від кіберзагроз, оскільки постачальник платформи несе відповідальність за забезпечення безпеки інфраструктури.

Однією з ключових переваг хмарних обчислень в освіті є можливість забезпечити безпечну та надійну платформу для онлайн-освіти. Хмарні платформи використовують розширені заходи безпеки, як-от шифрування, для захисту конфіденційних даних і створені для високої безпеки та стійкості до кібератак. Крім того, хмарні провайдери постійно оновлюють свої

заходи безпеки, щоб не відставати від загроз, що розвиваються, забезпечуючи рівень захисту, якого університети не змогли б досягти самостійно.

Ще однією перевагою хмарних обчислень в освіті є можливість масштабувати систему електронного навчання відповідно до вимог студентів і викладачів. Хмарні платформи мають високу масштабованість, що дозволяє університетам швидко й легко додавати нових користувачів і ресурси за потреби. Це особливо важливо в освітньому секторі, де кількість студентів може сильно коливатися протягом року.

Конфіденційність користувача та його особистість є найважливішим питанням єдиної електронної системи. Більше того, методи аутентифікації, авторизації та доставки електронного контенту до користувачів потребують захищеного механізму. Окрім автентифікації та авторизації, недоступність системи чи її електронного вмісту для слухачів в необхідний для них проміжок часу є однією з головних загроз для електронної системи навчання. Якщо електронна система недоступна, вона викликає розчарування та деморалізацію від процесу електронного навчання. Крім того, традиційні методи аутентифікації, такі як логін, пароль тощо є небезпечними та ненадійними.

Автентифікація слухачів є складною проблемою, оскільки будь-яка людина легко може отримати доступ від імені зареєстрованого користувача. Отже, щоб впоратися з подібними проблемами аутентифікації, може бути реалізована біометрична автентифікація за допомогою відбитків пальців, розпізнавання очей чи обличчя, як це реалізовано на сучасних смартфонах. Отже, сучасна електронна система вимагає розгортання служб безпеки, таких як контроль доступу, шифрування, аутентифікація, керування користувачами та їхніми привілеями. Більше того, передача даних між системою та адміністраторами або операторами контенту і користувачами повинна використовувати шифрування. Також безпечна платформа навчання повинна не тільки включати всі ці аспекти безпеки, але й робити більшість процесів прозорими та легшими для викладача та користувача, щоб вона стала привабливою для всіх зацікавлених сторін.

Безпека є однією з найбільш серйозних проблем у сфері освіти, де ІКТ - це спосіб передачі знань, відомий як електронне навчання. Загалом виділяють чотири основні зацікавлені сторони в системах електронного навчання - розробники, інструктори, адміністратор та користувачі/студенти. Розробники розробляють інструкції, які також називаються Learning Objects (LOs), та завантажують їх на сервери у вигляді веб-утиліт. LOs можна визначити як сутність в електронному вигляді, це може бути текст, аудіо, відео, презентація для онлайн-курсів, які також можуть бути визнані продуктом електронного навчання. Адміністратор підтримує матеріали на сервері та контролює послуги. Користувачі отримують доступ до LOs через мережу. Основна функція безпеки парадигми електронного навчання полягає у забезпеченні безпечної передачі інформації між користувачами та системою електронного навчання. Тому основні питання мережевої безпеки та web-безпеки, такі як доступність, конфіденційність, цілісність, повинні бути зосереджені на досягненні ефективного рівня електронної безпеки, крім цього існують інші фактори, які сприяють безпечному електронному навчанню:

1. Різноманітний доступ по місцерозташуванню. Особливою характеристикою системи електронного навчання є те, що кілька користувачів можуть одночасно отримувати доступ до неї з різних місць та ресурсів. Ці фактори ускладнюють безпеку системи e-learning, крім цього існує багато місць для взаємодії всередині системи електронного навчання, які можуть надати численні можливості зловмисникам, оскільки велика кількість користувачів можуть одночасно отримувати доступ до системи електронного навчання з різних місць. Це збільшує ризик для безпеки даних електронного навчання, хоча такі ризики для безпеки можна зменшити, обмеживши точку входу до систем електронного навчання.

2. Конфіденційність. Користувачам дуже важливо відчувати конфіденційність під час роботи в середовищі електронного навчання, тобто передача інформації між користувачем та електронною системою повинна бути у тому форматі, в якому вона була передбачена.

3. Аутентифікація. Для безпечного спілкування необхідно підтвердити джерело інформації. Кожен користувач має унікальну ідентифікацію, яку слід захищати та перевіряти перед доступом та передачею даних. Захист ідентичності студентів є вирішальним у кіберпросторі. Отже, надійна ідентифікація користувача є одним із важливих факторів середовища електронного навчання, оскільки вона є основою для контролю доступу. Після того, як користувач буде ідентифікований, необхідно перевірити, чи він саме та особа, яка претендує на свій статус. Кожна особистість у середовищі електронного навчання унікальна завдяки специфічним характеристикам та уподобанням.

4. Авторизація. Авторизація зазначає, що легальні користувачі можуть отримати доступ до інформації відповідно до визначених привілеїв. Система електронного навчання знаходиться в розподіленій системі, і багато користувачів отримують доступ до неї з різних місць, тобто необхідно ідентифікувати користувача з його особистістю. Тому існує потреба у захищеному механізмі аутентифікації, який не тільки розпізнає користувача, але й визначає права доступу користувачів у системі електронного навчання, служби авторизації підтверджують, чи має автентифікована особа привілей на доступ до потрібного вмісту електронної системи чи ні. Усі зацікавлені сторони, такі як студенти, викладачі, розробники тощо, отримують доступ до системи електронного навчання відповідно до своїх обов'язків. Зазвичай тільки адміністратор системи реєструє користувачів та присвоює їм права доступу.

5. Конфіденційність. Захист активів електронної системи від несанкціонованого доступу називається конфіденційністю, тобто це стан збереження даних від несанкціонованого доступу та змін. Користувачі потребують впевненості, що дані та інформація в електронній системі залишаються безпечними та приватними і ніколи не будуть доступними стороннім особам, пристроям чи системам. Контроль доступу до ресурсів може допомогти досягти конфіденційності електронної системи, що може забезпечити безпечну доставку вмісту в мережі та надійне зберігання даних. Конфіденційність є однією з головних проблем зареєстрованих користувачів, а це означає, що подані ними завдання, документи, інформація будуть доступні лише відповідним екзаменатором або експертам. Користувач повинен мати доступ лише до авторизованого вмісту, а ті особи, які не є законними користувачами, взагалі не повинні мати доступ до електронної системи.

6. Цілісність. Цілісність даних визначає доступність, надійність, правильність та високу якість збережених даних. Цілісність - це впевненість, що лише авторизовані користувачі чи програми мають право змінювати дані чи програми. Отже, забезпечення цілісності даних та інформації є однією з головних цілей щодо безпеки електронної системи навчання. Цілісність залежить від контролю доступу та вимагає розпізнавати всіх користувачів, які намагаються отримати доступ до електронної системи, більше того, студенти системи e-learning мають бути впевненими, що відповідні особи (екзаменатор, інструктор, адміністратор тощо) отримають подані ними матеріали (завдання, документи тощо) у своєму первісному та нередагованому стані.

7. Доступність. Доступність можна пояснити як ступінь, при якому система доступна та функціонує і може бути використана студентами, коли це їм потрібно. Крім того, вона безпосередньо впливає на постійність, живучість, а також стосується атак типу «відмова від обслуговування» (DoS) та вірусів, які видаляють файли. Є два основні аспекти порушення доступності: розподілена атака типу «відмова в обслуговуванні» (DDoS) та втрата можливостей обробки даних, де DDoS-атака є кореневою атакою для недоступності даних. Отже в системах e-learning, важливо підтвердити, що інформаційно-комунікаційні ресурси завжди доступні при підвищенні попиту, щоб дозволені користувачі могли подати свої завдання, коментарі, замітки або документи протягом визначеного часу. Якщо користувач не в змозі отримати доступ до потрібного матеріалу чи електронного вмісту вчасно, вони можуть втратити інтерес або навіть відмовитись користуватися системою електронного навчання.

8. Безвідмовність. Безвідмовність змушує легальних користувачів не відмовлятися від виконання певних операцій. Наприклад, якщо студент має подати свою роботу, він не повинен відмовляти у поданні своїх матеріалів. Отже, необхідно мати с системі e-learning систематичний і формальний механізм, щоб не допустити зареєстрованим користувачам відмовлятися від роботи або змінах, які вони виконали в системі електронного навчання.

Для подальшого розвитку системи дистанційного електронного навчання в університеті важливо продовжувати інвестувати в хмарні обчислення та тісно співпрацювати з постачальниками хмарних технологій, щоб переконатися, що платформа відповідає потребам університету. Крім того, університети повинні зосередитися на навчанні та підтримці для викладачів і студентів, щоб допомогти їм максимально використати нову платформу та забезпечити її ефективне використання.

Перехід до хмарної системи електронного навчання на сьогодні має вирішальне значення для довгострокового успіху онлайн-освіти. Забезпечуючи безпечну та надійну платформу, університети можуть гарантувати, що їхні системи електронного навчання захищені від кіберзагроз і здатні задовольняти вимоги студентів і викладачів. Перехід на хмарну платформу є важливим кроком у постійному розвитку системи дистанційного електронного навчання університету та допоможе забезпечити її довгостроковий успіх та сталість.

Крім того, для університетів важливо регулярно оцінювати безпеку своїх хмарних систем електронного навчання та впроваджувати найкращі методи кібербезпеки, такі як автентифікація користувачів і контроль доступу, мережева безпека, резервне копіювання та відновлення даних. Це допоможе зменшити ризик кібератак і гарантуватиме захист конфіденційних даних і інформації університету. Відповідні заходи можуть включати механізм контролю доступу за допомогою брандмауера, цифрового підпису та біометричної автентифікації. Крім цього, використання SMS-повідомлень мобільних пристроїв може забезпечити безпечну аутентифікацію та авторизацію для забезпечення цілісності та конфіденційності системи e-learning (Farid S., 2017). Загалом можна виділити наступні механізми безпеки, які можуть ефективно застосовуватися в системах електронного навчання:

1. Контроль доступу (брандмауери). Найпростіший спосіб забезпечити контроль доступу - це використання брандмауерів. Для забезпечення безпеки весь трафік зсередини назовні або навпаки повинен проходити через нього для перевірки, тобто він виступає захисним шаром. Тому весь доступ до системи повинен бути фізично заблокований, а авторизований трафік повинен дозволяти лише проходити через нього, щоб забезпечити безпеку системи електронного навчання. Брандмауери давно доступні на ринку та використовуються для зв'язку через мережу Internet, тому достатньо включити такі міжмережеві екрани для підвищення рівня безпеки систем електронного навчання.

2. Біометрична аутентифікація. На сьогодні практично застосовуються різні методи аутентифікації, такі як паролі, смарт-карти, цифрові сертифікати та цифровий підпис. Але навіть у цих випадках не можна гарантувати, що користувачі не зможуть надати стороннім свій пароль під час завантаження електронного вмісту, подання завдань, отримання/створення документів тощо. Використання пароля - це давнє і широко використовується, але існує шанс викрасти або підробити пароль. Біометрична автентифікація - найкращий вибір для заміни перевірки відповідності паролів. Отже, механізм біометричної автентифікації може забезпечити порівняно кращу та безпечну обстановку, оскільки користувач ніколи не може втратити свої біометричні дані, а біометричний сигнал важко вкрасти або підробити. ВНЗ можуть зобов’язати студентів надавати їм одну чи більше біологічних характеристик, таких як обличчя, почерк, відбитки пальців, характеристики очей або голосу, які зберігаються в базі даних з метою автентифікації відповідного користувача. Для впровадження цієї методики потрібен біометричний пристрій, але такі пристрої, як пристрій розпізнавання відбитків пальців на основі смартфонів, легко доступні на ринку за доступною ціною. Ці факти свідчать про те, що автентифікація біометрики є можливим рішенням для систем електронного навчання.

3. Автентифікація SMS. Смартфони можуть успішно використовуватися ВНЗ, які пропонують систему електронного навчання для цілей аутентифікації користувачів. Пропонується використовувати SMS для безпечного доступу до системи e-learning. Можлива процедура може бути розділена на два етапи. На першому кроці студент подає ідентифікатор користувача та пароль через свій мобільний телефон. У відповідь на цю систему електронного навчання генерується спеціальний код та надсилається його на зареєстрований телефон користувача SMS-повідомленням, який фактично є ключем для поточного сеансу. На другому кроці студент вводить цей код, щоб підтвердити свою особу та безпечно отримати доступ до системи електронного навчання. Цю методику можливо поліпшити додавши криптографічний алгоритм, який приймає ім'я користувача та пароль як вхідні дані та забезпечує вихід у вигляді випадкового/унікального коду доступу. Цей код надсилається на зареєстрований мобільний телефон користувача не тільки для ідентифікації, але і для автентифікації та надання дозволу всім користувачам із попередньо наданими привілеями.

4. Криптографія. Криптографія - одна з принципово рекомендованих методик, які застосовуються для забезпечення безпеки в Internet для передачі інформації. Криптографічні алгоритми поділяють на три основні типи: алгоритм із секретним ключем (симетричний), алгоритм відкритого ключа (асиметричний) та хеш-функції. Криптографія корисна для захисту даних від крадіжок чи змін під час передачі, а також у сховищах/архівах, а також може виконувати аутентифікацію користувачів.

5. Аутентифікація сесії. Перехват сеансу чи викрадення файлів cookie – все це засоби неправомірного використання легального комп'ютерного сеансу. Зловмисник може перехопити сеанс, щоб мати несанкціонований доступ до комп'ютерної системи e-learning. Методи аутентифікації не є надійними та безпечними і завдання полягає в розробці такої електронної системи, яка б ідентифікувала справжнього користувача під час занять або через визначені часові інтервали. Двоетапний метод аутентифікації є більш безпечним,

ніж метод одиночної аутентифікації. Спочатку потрібно ввійти в систему за допомогою ідентифікатора та паролів, а після цього потрібно підтвердити автентифікацію надсиланням електронного листа або короткого повідомлення/ SMS. Цей тип повторної аутентифікації успішно реалізований різними захищеними системами веб-додатків, такими як електронний банкінг і можуть бути успішно застосовані в системах електронного навчання.

6. Пристрої фізичної безпеки. Захист можна організувати за допомогою USB-пристроїв. Студенти можуть зареєструвати ключ захисту у своєму обліковому записі, щоб наступного разу увійти в систему e-learning після активації доступу на цьому пристрої. За допомогою таких пристроїв фізичної безпеки може бути організовано ефективний захист від фішингу, оскільки користувачеві не потрібно вводити код самостійно.

Ще однією важливою перевагою хмарних обчислень є їх економічна ефективність. Завдяки хмарним обчисленням університетам не потрібно інвестувати в дороге обладнання та програмне забезпечення для підтримки своїх систем електронного навчання. Натомість вони можуть орендувати необхідну обчислювальну потужність і простір для зберігання даних у хмарних провайдерів, що набагато економічніше, ніж купувати та підтримувати власну інфраструктуру.

Можливо, найголовніше те, що хмарні обчислення забезпечують підвищену безпеку систем онлайн-освіти. Зберігаючи дані та програми на віддалених серверах, університети можуть захистити свої конфіденційні дані від кіберзагроз, таких як хакерство, зловмисне програмне забезпечення та витік даних (Alharbi et al., 2019). Це особливо важливо для університетів, які обробляють велику кількість конфіденційних даних студентів, таких як особиста інформація та фінансові записи.

Дослідження, проведене Alharbi et al. виявили, що хмарні обчислення забезпечують ряд переваг безпеки для систем електронного навчання. Ці переваги включають покращену конфіденційність і безпеку даних, покращений контроль доступу та автентифікацію, а також покращені можливості аварійного відновлення. Дослідження також виявило, що використання хмарних обчислень у системах електронного навчання допомагає зменшити ризик кібератак і витоку даних.

Крім того, для університетів дуже важливо вибрати надійного постачальника хмарних послуг для своєї системи електронного навчання. Не всі хмарні провайдери однакові, тому для університетів важливо ретельно розглянути політику безпеки та конфіденційності кожного провайдера, перш ніж приймати рішення. Рекомендується, щоб університети вибирали хмарного постачальника, який має перевірену історію безпеки та конфіденційності та відповідає відповідним нормам і стандартам, наприклад, таким як Загальний регламент захисту даних (GDPR) і стандарт ISO/IEC 27001:2013 для менеджменту інформаційної безпеки (CIS, 2020) .

Окрім вибору правильного хмарного постачальника, університети також повинні запровадити суворі політики та процедури безпеки, щоб забезпечити захист своїх систем електронного навчання. Це може включати регулярні аудити безпеки, регулярні оновлення програмного забезпечення та навчання співробітників найкращим практикам кібербезпеки (CIS, 2020). Здійснюючи ці проактивні кроки, університети можуть допомогти зменшити ризики кіберзагроз і забезпечити постійний успіх і сталість своїх онлайн-освітніх програм.

Висновки.

Перехід до хмарної системи електронного навчання має важливе значення для захисту конфіденційних даних та інформації, а також для подальшого успіху та стабільності онлайн-освіти. Вибравши надійного хмарного постачальника, впровадивши жорсткі політики та процедури безпеки, а також регулярно оцінюючи та налаштовуючи свої системи, університети можуть гарантувати, що їхні системи електронного навчання залишаються безпечними, ефективними та актуальними. Нарешті, університети повинні регулярно оцінювати та коригувати свої системи електронного навчання, щоб переконатися, що вони продовжують відповідати потребам студентів і викладачів. Це може включати впровадження нових технологій, інтеграцію нових інструментів навчання та впровадження нових політик і процедур для підвищення безпеки та конфіденційності системи. Регулярно оцінюючи та налаштовуючи свої системи електронного навчання, університети можуть гарантувати, що їхні системи залишаються актуальними, ефективними та безпечними.

ЛІТЕРАТУРА:

1. Толбатов, В., Толбатов, С., Толбатов, А., Вьюненко, А. 2019. Актуальные вопросы использования технологии BLOCKCHAIN в учреждениях высшего образования. Modern engineering and innovative technologies. 2, 09-02 (окт. 2019), 47-52. DOI:https://doi.org/10.30890/2567-5273.2019-09-02-037.

2. Zafar, Aasim & Alghazzawi, D. & Hamid, Syed. (2014). E-Learning Systems and their Security. Magnt Research Report. 2. 83-92.

3. Chen Yong, He Wu Security Risks and Protection in Online Learning: A Survey. International Review of Research in Open and Distance Learning, v14 n5 p108-127 Dec 2013

4. Dima A, Bugheanu A-M, Boghian R, Madsen DØ. Mapping Knowledge Area Analysis in E-Learning Systems Based on Cloud Computing. Electronics. 2023; 12(1):62.

5. Кухаренко В.М. Розробка сучасної системи електронного навчання в університеті. Український журнал інформаційних технологій 2, вип. 1 (2020): 95–102.

6. Alharbi, M., Alghamdi, M., Alotaibi, K., & Alqubisi, A. (2019). Cloud computing security issues in e-learning systems. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1171-1183.

7. Farid S., Alam M. Qaisar, G., Haq, A.A.A., Itmazi J. Security Threats and Measures in E-learning in Pakistan: A Review. Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan 2017. Vol. 22 No. 3 P. 98-107.

8. CIS (2020). 20 Critical Security Controls for Effective Cyber Defense. The Center for Internet Security. https://www.cisecurity.org/controls/

REFERENCES:

1 1. Tolbatov, V., Tolbatov, S., Tolbatov, A., V`yunenko, A. 2019. Aktual`ny`e voprosy` ispol`zovaniya tekhnologii BLOCKCHAIN v uchrezhdeniyakh vy`sshego obrazovaniya. Modern engineering and innovative technologies. 2, 09-02 (okt. 2019), 47-52. DOI:https://doi.org/10.30890/2567-5273.2019-09-02-037.

2. Zafar, Aasim & Alghazzawi, D. & Hamid, Syed. (2014). E-Learning Systems and their Security. Magnt Research Report. 2. 83-92.

3. Chen Yong, He Wu Security Risks and Protection in Online Learning: A Survey. International Review of Research in Open and Distance Learning, v14 n5 p108-127 Dec 2013

4. Dima A, Bugheanu A-M, Boghian R, Madsen DØ. Mapping Knowledge Area Analysis in E-Learning Systems Based on Cloud Computing. Electronics. 2023; 12(1):62.

5. Kukharenko V.M. Rozrobka suchasnoi systemy elektronnoho navchannia v universyteti. Ukrainskyi zhurnal informatsiinykh tekhnolohii 2, vyp. 1 (2020): 95–102.

6. Alharbi, M., Alghamdi, M., Alotaibi, K., & Alqubisi, A. (2019). Cloud computing security issues in e-learning systems. Journal of Ambient Intelligence and Humanized Computing, 10(3), 1171-1183.

7. Farid S., Alam M. Qaisar, G., Haq, A.A.A., Itmazi J. Security Threats and Measures in E-learning in Pakistan: A Review. Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan 2017. Vol. 22 No. 3 P. 98-107.

8. CIS (2020). 20 Critical Security Controls for Effective Cyber Defense. The Center for Internet Security. https://www.cisecurity.org/controls/