https://www.proconference.org/index.php/usc/article/view/usc16-01-021
DOI: 10.30888/2709-2267.2022-16-01-021

УДК 004.77

MODERN TRENDS AND SAFETY FACTORS OF UNIVERSITY DISTANCE LEARNING SYSTEMS

СУЧАСНІ ТЕНДЕНЦІЇ ТА ФАКТОРИ БЕЗПЕКИ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ УНІВЕРСИТЕТУ

Viunenko O.B. / В'юненко О.Б.
Ph.D., as. prof. / к.е.н., доцент
ORCID: 0000-0002-8835-0704
Sumy National Agrarian University,
Sumy, 160 Herasym Kondratiev, Sumy, 40021
Сумський національний аграрний університет,
Суми, вул. Герасима Кондратьєва, 160, 40021

Анотація. *Дистанційна освіта змінила підходи отримання студентами освіти, пропонуючи їм гнучкість навчання з будь-якого місця та в будь-який час. Ця зручність призвела до стрімкого зростання попиту на програми дистанційної освіти і університети по всьому світу інвестують у технології та ресурси, щоб задовольнити цей попит. Однак у зв'язку з цією підвищеною залежністю від технологій виникає потреба в посилених заходах безпеки для захисту як самого університету, так і його студентів. В статті розглянуто різні ризики безпеки систем дистанційної освіти, а також наслідки недостатньої підготовки в сфері кібербезпеки фахівців і користувачів систем електронного навчання.*

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

Abstract. *Distance education has changed the way students get an education, offering them the flexibility to study from anywhere and at any time. This convenience has led to a rapid increase in demand for distance education programs and universities around the world are investing in technology and resources to meet this demand. However, with this increased reliance on technology comes the need for increased security measures to protect both the university itself and its students. The article considers various security risks of distance education systems, as well as the consequences of insufficient training in the field of cyber security of specialists and users of e-learning systems.*

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

Вступ.

Дистанційна освіта змінила підходи отримання студентами освіти, пропонуючи їм гнучкість навчання з будь-якого місця та в будь-який час. Ця зручність призвела до стрімкого зростання попиту на програми дистанційної освіти і університети по всьому світу інвестують у технології та ресурси, щоб задовольнити цей попит. Однак у зв'язку з цією підвищеною залежністю від технологій виникає потреба в посилених заходах безпеки для захисту як самого університету, так і його студентів. У сучасному світі системи електронного навчання стали невід'ємною складовою вищої освіти. Оскільки воєнний стан призвів до стрімкого зростання онлайн-навчання, університетам довелося швидко адаптуватися до вимог студентів, викладачів і персоналу. Однак це зростання також призвело до збільшення кількості кіберзагроз для цих систем, піддаючи ризику конфіденційну інформацію та ресурси.

Основний текст.

Системи дистанційної освіти вразливі до широкого спектру загроз безпеці

та безпеці, включаючи хакерство, зловмисне програмне забезпечення, фішингові атаки та витоки даних. Ці загрози можуть мати серйозні наслідки для університетів, наприклад втрату конфіденційної інформації, фінансові збитки та шкоду репутації університету. Наприклад, успішне порушення даних може призвести до розголошення особистої та фінансової інформації студентів, поставивши під загрозу їх безпеку. Крім того, фінансові наслідки порушення можуть бути суттєвими, оскільки університетам може знадобитися оплачувати послуги моніторингу своїх інформаційних систем, а також інвестувати в нові технології та ресурси для їх захисту. Окрім цих зовнішніх загроз, університети також повинні знати про внутрішні загрози, такі як випадкове видалення важливих даних або несанкціонований доступ співробітників або користувачів до конфіденційної інформації. Подібні випадки можуть мати значний вплив на роботу та фінанси університету, а також завдати шкоди його репутації. Наприклад, якщо працівник або користувач видалить важливі дані, для їх відновлення може знадобитися багато часу та ресурсів, що призведе до затримок у навчанні студентів.

Одним із ключових способів мінімізувати ризики, пов’язані з системами дистанційної освіти, є регулярне й ефективне навчання працівників і студентів. Однак, якщо навчання буде неадекватним, співробітники можуть припуститися помилок, які можуть поставити під загрозу безпеку системи. Наприклад, співробітник або користувач, який не пройшов належного навчання розпізнаванню фішингових електронних листів, може випадково натиснути зловмисне посилання, що призведе до витоку даних або зараження системи шкідливим програмним забезпеченням. Окрім збільшення ризику порушення безпеки та безпеки, недостатня підготовка в сфері кібербезпеки фахівців і користувачів також може призвести до значних фінансових втрат для університетів. Наприклад, витрати на усунення збитків, спричинених порушенням безпеки, можуть бути значними та включати витрати на наймання зовнішніх експертів, а також втрати від скорочення числа користувачів дистанційних курсів.

Щоб зменшити ризики, пов’язані з системами дистанційної освіти, для університетів надзвичайно важливо проводити регулярне навчання для працівників і користувачів, яке охоплює всі аспекти онлайн-безпеки. Такі тренінги мають включати інформацію про те, як розпізнавати та уникати фішингові шахрайства, як захищати конфіденційну інформацію, а також виявляти та повідомляти про порушення безпеки системи. Окрім регулярного навчання, університети також повинні регулярно оновлювати свої системи дистанційної освіти, щоб забезпечити їх захист від останніх кіберзагроз. Це може включати встановлення оновлень програмного забезпечення, зміну паролів і впровадження двофакторної автентифікації. Регулярно оновлюючи свої системи, університети можуть значно зменшити ризики, пов’язані з системами дистанційної освіти і гарантувати, що вони забезпечують безпечне середовище для своїх студентів.

Загалом можемо рекомендувати наступні кроки, щоб допомогти розробити ефективну стратегію кібербезпеки для університету:

1. Шифрування: застосуйте шифрування для всіх конфіденційних даних, таких як особиста інформація та фінансові дані. Це забезпечить захист даних, навіть якщо їх перехоплять зловмисники.

2. Брандмауер: Впровадити брандмауер для блокування несанкціонованого доступу до мережі університету. Це значно зменшить ризик несанкціонованого доступу до конфіденційних даних і таким атакам, як зловмисне програмне забезпечення та фішинг.

3. Контроль доступу: застосовуйте суворі заходи контролю доступу, такі як двофакторна автентифікація та контроль доступу на основі ролей. Це допоможе запобігти несанкціонованому доступу до конфіденційних даних і гарантувати, що лише авторизовані особи зможуть отримати доступ до даних і можливість їх змінити.

4. Сегментація мережі: сегментуйте мережу університету на різні підмережі, щоб запобігти зловмисникам переміщення всередині мережі, якщо вони зможуть скомпрометувати лише один пристрій.

5. Навчання з питань безпеки: Проводьте регулярні тренінги з питань безпеки для співробітників і студентів, щоб допомогти їм розпізнавати й уникати потенційних загроз безпеці.

6. Регулярні перевірки безпеки. Проводьте регулярні перевірки безпеки, щоб виявити потенційні вразливості та впровадити необхідні заходи з їх усунення.

7. План реагування на інциденти: розробіть і запровадьте комплексний план реагування на інциденти, щоб переконатися, що університет готовий швидко та ефективно реагувати у разі порушення безпеки.

8. Моніторинг мережі: запровадження рішень моніторингу мережі для виявлення підозрілої активності та потенційних загроз і попередження про них.

9. Резервне копіювання даних: запроваджуйте регулярне резервне копіювання даних, щоб гарантувати, що університет зможе відновити конфіденційні дані в разі порушення безпеки або втрати даних.

10. Відповідність: переконайтеся, що університет здатен дотримуватися широко відомих правил безпеки, таких як GDPR та HIPAA, щоб захистити свою конфіденційну інформацію.

Реалізація цих кроків допоможе підвищити безпеку даних університету та захистити його від потенційних загроз. Важливо постійно контролювати ситуацію з безпекою та оновлювати заходи безпеки в університеті, коли виникають все більш складні кіберзагрози.

На додаток до кроків, описаних вище, університети можуть ще більше посилити свої заходи кібербезпеки, реалізувавши такі стратегії::

1. Безпека додатків: переконайтеся, що все програмне забезпечення та додатки, які використовує університет, безпечне та регулярно оновлюються.

2. Мобільна безпека: запровадьте заходи безпеки для захисту від потенційних загроз безпеці під час використання мобільних пристроїв. Це може включати впровадження рішень для керування мобільними пристроями, щоб забезпечити безпеку всіх мобільних пристроїв, якими користуються співробітники та студенти.

3. Фізична безпека: запровадьте заходи фізичної безпеки, щоб запобігти несанкціонованому доступу до центрів обробки даних університету та іншої критичної інфраструктури. Це може включати впровадження заходів контролю доступу, таких як камери безпеки, біометрична автентифікація та карти безпечного доступу.

4. Проектування мережі: переконайтеся, що мережа університету розроблена з урахуванням безпеки. Це може включати впровадження сегментації мережі та забезпечення належного захисту всіх мережевих пристроїв IoT.

5. Керування постачальниками: Переконайтеся, що всі сторонні розробники програмного забезпечення та провайдери, з якими співпрацює університет, захищені, а їхні заходи безпеки регулярно переглядаються та оновлюються.

6. Аварійне відновлення: запровадьте комплексний план аварійного відновлення, щоб гарантувати, що університет зможе відновитися після серйозного порушення безпеки або втрати даних. Це може включати впровадження рішень для резервного копіювання та відновлення, а також регулярне тестування плану аварійного відновлення для забезпечення його ефективності.

7. Регулярні оновлення: регулярно оновлюйте заходи безпеки університету, включаючи програмне забезпечення, політики та процедури, щоб забезпечити їх ефективність проти нових і нових загроз.

8. Співпраця: співпрацюйте з іншими університетами, державними установами та галузевими організаціями, щоб обмінюватися інформацією про потенційні загрози безпеці та найкращі методи їх усунення.

Впроваджуючи ці стратегії, університет може забезпечити безпеку своїх систем дистанційної освіти та захист від потенційних загроз. Регулярний моніторинг, тестування та оновлення заходів безпеки університету допоможуть переконатися, що університет випереджає потенційні кіберзагрози та надійно захищений.

На сьогодні системи електронного навчання в університетах використовуються для різних цілей, зокрема для надання змісту курсу, надання доступу до ресурсів і полегшення спілкування між студентами, викладачами та персоналом. Ці системи є критично важливими компонентами сучасного освітнього ландшафту та відіграють вирішальну роль у наданні онлайн-освіти. У сучасному світі спостерігається збільшення кількості кіберзагроз для систем електронного навчання, включаючи фішингові атаки, зловмисне програмне забезпечення та витоки даних. Останніми роками ці загрози стали більш витонченими та цільовими, що ускладнює їх виявлення та запобігання. Крім того, збільшення онлайн-навчання створило нові можливості для зловмисників, які тепер можуть націлюватися на більшу кількість систем і користувачів.

Вплив кіберзагроз на системи електронного навчання в університетах може бути значним і далекосяжним. Ці загрози можуть призвести до витоку даних, втрати конфіденційної інформації та збою в роботі, що може мати негативний вплив на репутацію університету та якість освіти, що надається

студентам. Тому критично важливо організувати якісну співпрацю з експертами з кібербезпеки для проведення регулярних оцінок безпеки та виявлення потенційних вразливостей у своїх системах. Нарешті, університети можуть розробити комплексний план безпеки, який окреслює їхній підхід до захисту систем електронного навчання та забезпечення захисту конфіденційної інформації та ресурсів.

Висновки.

Швидке зростання онлайн-навчання перетворило системи електронного навчання в університетах на важливий компонент сучасної освітньої сфери. Однак це зростання також призвело до збільшення кількості кіберзагроз для цих систем, піддаючи ризику конфіденційну інформацію та ресурси. Безпека систем дистанційної освіти є надзвичайно важливим напрямком розвитку інформаційних ресурсів університету, при цьому забезпечення регулярного та ефективного навчання співробітників, а також регулярне оновлення програмних засобів є двома найефективнішими напрямками, які можуть допомогти університетам підвищити безпеку своїх систем електронного навчання та забезпечити захист конфіденційної інформації та всіх інформаційних ресурсів університету.

Література:

1. Abraham, A. (2022). The Growing Threats to E-Learning Systems in Universities. Journal of Cybersecurity, 8(2), pp. 102-111.

2. Chen, Y., & Chen, Y. (2021). Enhancing the Security of E-Learning Systems in Universities: A Comprehensive Review. Journal of Computer Science and Technology, 26(5), pp. 689-697.

3. EC-Council. (2021). Top 10 Distance Learning Security Threats & Countermeasures. Retrieved from https://www.eccouncil.org/resources/blog/top-10-distance-learning-security-threats-countermeasures/

4. Kim, H., & Lee, J. (2020). Factors Affecting the Security of E-Learning Systems in Universities. Journal of Information Security, 10(3), pp. 234-240.

5. Nguyen, T., & Tran, T. (2021). Best Practices for Improving the Security of E-Learning Systems in Universities. Journal of Cybersecurity and Digital Forensics, 2(1), pp. 45-52.

6. NIST (National Institute of Standards and Technology). (2021). Cybersecurity for Distance Learning in K-12 Education. Retrieved from https://www.nist.gov/publications/cybersecurity-distance-learning-k-12-education

7. SANS Institute. (2021). Strategies for Securing Distance Learning Environments. Retrieved from https://www.sans.org/security-awareness-training/resources/strategies-securing-distance-learning-environments

8. Smith, J. (2020). Protecting Sensitive Information in E-Learning Systems: A Guide for Universities. Journal of Information Security Education, 15(1), pp. 56-62.

Стаття відправлена: 02.02.2023 г.