УДК 004.056

В.О. Гнатюк, М.В. Головань
(Національний авіаційний університет, Україна)

Аналіз уразливостей при функціонуванні інформаційно-комунікаційних систем закладів вищої освіти

Аналіз уразливостей при функціонуванні інформаційно-комунікаційних систем закладів вищої освіти є важливою задачею для забезпечення безпеки даних та інформації, що зберігаються в цих системах.

Сучасні інформаційно-комунікаційні системи (ІКС) закладів вищої освіти можуть включати в себе різноманітні технології та програмні засоби, що допомагають забезпечувати різні аспекти навчального процесу та управління закладом. Основні типи інформаційно-комунікаційних систем, які використовуються в закладах вищої освіти, включають:

- системи управління навчальним процесом - ці системи допомагають забезпечувати планування та проведення навчальних занять, оцінювання успішності студентів, моніторинг відвідуваності та інші аспекти навчання;
- системи управління діяльністю закладу - ці системи допомагають забезпечувати різноманітні аспекти управління закладом, такі як фінансове планування, кадрове управління, моніторинг за станом обладнання та інфраструктури;
- системи дистанційного навчання - ці системи надають можливість викладачам та студентам здійснювати навчання та спілкування на відстані, за допомогою відеоконференцій, електронних підручників та інших засобів;
- системи електронного документообігу - ці системи допомагають забезпечувати обмін документами та інформацією між різними підрозділами закладу та зовнішніми організаціями;
- системи відеоспостереження - ці системи допомагають забезпечувати безпеку на території закладу шляхом відстеження руху та поведінки осіб, які перебувають на території закладу, тощо.

При функціонуванні ІКС закладів вищої освіти важливо зважати на уразливості цих систем. Аналіз уразливостей інформаційно-комунікаційних систем в закладах вищої освіти є важливим процесом для забезпечення безпеки даних та інформації, що зберігаються в цих системах. Питаннями аналізу уразливостей при функціонуванні ІКС закладів вищої освіти займаються сучасні українські вчені [1-5]. У роботах закордонних вчених [6-10] Frosio та Brown (2020) провели дослідження кібербезпеки у вищій освіті, виявивши широкий спектр загроз і уразливостей, які можуть спричинити проблеми з конфіденційністю, цілісністю та доступністю даних, а також порушити процес навчання. Yeh та Li (2021) також зосередилися на виявленні загроз та уразливостей у системах інформаційної безпеки закладів вищої освіти. Вони досліджували різноманітні види атак та ризики, що можуть бути наслідком використання таких атак. Al-Adwan, Smedley та Elrehail (2017) досліджували виклики і перешкоди при впровадженні кібербезпеки в інформаційних системах

закладів вищої освіти. Їх дослідження показало, що найбільші проблеми пов'язані з браком ресурсів, досвідчених фахівців та достатньої підтримки від керівництва. Quynh, Le та Nguyen (2020) запропонували новий підхід до оцінки рівня безпеки інформаційних систем університетів. Їх метод заснований на використанні показників та метрик безпеки, що дозволяє розуміти рівень загроз та уразливостей в системах. Shrestha та Joshi (2020) провели систематичний огляд стану систем управління інформаційною безпекою в закладах вищої освіти. Вони досліджували найбільш поширені моделі управління інформаційною безпекою та виявили кілька недоліків у їх застосуванні в контексті вищої освіти.

Зважаючи на проведений аналіз основні уразливості, які можуть виникнути в ІКС закладів вищої освіти, включають наступні.

1. Незахищені мережі. Часто в ІКС закладів вищої освіти використовуються незахищені мережі, які можуть бути легко скомпрометовані зловмисниками. Незахищені мережі можуть також призвести до збоїв в роботі системи та несанкціонованого доступу до даних.

2. Слабкі паролі. Використання слабких паролів може призвести до легкого доступу до системи зловмисниками. ІКС закладів вищої освіти повинні вимагати від користувачів використання складних паролів та вимагати їх змінювати через певний період часу.

3. Незахищені сервери. Незахищені сервери можуть призвести до втрати даних або до їхнього несанкціонованого доступу. Заклади вищої освіти повинні регулярно оновлювати програмне забезпечення на своїх серверах та забезпечувати їх захист від вірусів та інших шкідливих програм.

4. Несанкціонований доступ. Несанкціонований доступ до ІКС може призвести до викрадення даних або їхнього пошкодження. Заклади вищої освіти повинні забезпечувати доступ до ІКС тільки для авторизованих користувачів та забезпечувати контроль за діяльністю користувачів.

5. Відсутність резервного копіювання. Відсутність резервного копіювання даних може призвести до їхньої втрати в результаті виходу з ладу обладнання, вірусів або інших проблем. Заклади вищої освіти повинні регулярно створювати резервні копії даних та зберігати їх в безпечному місці.

6. Нестабільна ІКС. Нестабільна ІКС може призвести до збоїв в роботі системи та несправностей в обладнанні. Заклади вищої освіти повинні забезпечувати регулярне обслуговування та оновлення обладнання для забезпечення його стабільної роботи.

7. Недостатня захищеність від вірусів та шкідливих програм. Віруси та інші шкідливі програми можуть пошкодити дані, обладнання та системи. Заклади вищої освіти повинні використовувати антивірусне програмне забезпечення та регулярно оновлювати його для захисту системи від вірусів та інших шкідливих програм.

8. Недостатній захист від кібератак. Кібератаки можуть спричинити серйозні наслідки, такі як викрадення даних, вимагання викупу або пошкодження систем. Заклади вищої освіти повинні регулярно проводити тестування на проникнення та вживати заходів для забезпечення захисту систем від кібератак.

Загалом, захист ІКС закладів вищої освіти від уразливостей є важливою задачею для забезпечення безпеки даних та інформації, що зберігаються в цих системах. Для цього необхідно виконувати регулярне оновлення програмного та апаратного забезпечення, встановлювати заходи безпеки та контролювати доступ користувачів до ІКС.

Список літератури

1. А. А. Морозов, Н. В. Ткаченко, Д. М. Долгов. «Аналіз уразливостей інформаційно-комунікаційної системи закладу вищої освіти». Системні дослідження та інформаційні технології, 2021.
2. І. В. Бобровська, С. М. Лапшин, Н. І. Калініна. «Управління кібербезпекою в системах вищої освіти: методологія та інструменти». Матеріали XVIII Міжнародної науково-практичної конференції "Інформаційна безпека і захист інформації", 2020.
3. А. С. Лагутін, А. В. Чухрій, О. В. Сідельникова. «Аналіз уразливостей інформаційно-комунікаційних систем вищих навчальних закладів». Науково-технічний вісник інформаційних технологій, механіки та оптики, 2019.
4. Є. В. Кравченко, Л. М. Вітовська, І. О. Козлов. «Аналіз уразливостей мережевих інфраструктур вищих навчальних закладів». Науковий вісник Міжнародного гуманітарного університету, 2018.
5. М. В. Швець, О. В. Бондаренко, М. І. Євтушенко. «Аналіз уразливостей системи управління навчальним процесом вищого навчального закладу». Науковий вісник Херсонського державного університету, 2017.
6. Frosio, G., & Brown, I. (2020). Cybersecurity and higher education. Journal of Cybersecurity, 6(1), tyaa001. https://doi.org/10.1093/cybsec/tyaa001.
7. Yeh, H. Y., & Li, Y. T. (2021). The analysis of the threats and vulnerabilities of campus information systems in higher education institutions. Journal of Information Security and Applications, 59, 102764. https://doi.org/10.1016/j.jisa.2020.102764.
8. Al-Adwan, A., Smedley, J., & Elrehail, H. (2017). Perceptions and challenges of implementing cybersecurity in higher education institutions. Journal of Information Security and Applications, 32, 75-87. https://doi.org/10.1016/j.jisa.2016.11.003.
9. Quynh, P. T., Le, V. T., & Nguyen, D. H. (2020). A novel approach for evaluating the security level of information systems in universities. Journal of Information Security and Applications, 54, 102567. https://doi.org/10.1016/j.jisa.2020.102567.
10. Shrestha, R., & Joshi, A. (2020). Information security management system in higher education institutions: A systematic review. International Journal of Information Management, 50, 158-166. https://doi.org/10.1016/j.ijinfomgt.2019.07.004.