Шуляк Богдан Андрійович,
студент н.гр. 102_СПД
ННІ права та психології НАВС

Науковий керівник:
Кудінов Вадим Анатолійович,
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ПОТЕНЦІЙНІ РИЗИКИ ДЛЯ ФІНАНСОВОЇ ДОКУМЕНТАЦІЇ В ЦИФРОВОМУ ФОРМАТІ ОСВІТНІХ УСТАНОВ СИСТЕМИ МВС УКРАЇНИ

Сьогодні спостерігається інтенсивна цифровізація середовища освітніх установ системи МВС України, яке, спираючись на відповідну нормативно-правову базу, активно діджиталізується. Активно впроваджуються різноманітні платформи для онлайн-навчання та ведення електронного документообігу, що підвищує ефективність освітнього процесу закладів вищої освіти (далі – ЗВО) та зменшує витрати часу/ресурсів на підтримку його функціонування.

Але цифровізація освітньої системи МВС України супроводжується новими ризиками. Серед ключових загроз виділяють:

1) вразливість цифрових платформ: більшість платформ, що використовуються в ЗВО, мають низький рівень кіберзахисту (не оновлене програмне забезпечення та слабкі алгоритми шифрування);
2) використання недостатньо захищених каналів для передачі даних між структурними підрозділами ЗВО. Тому стають можливими кібератаки типу «ransomware», які блокують доступ до баз даних, вимагаючи викуп за їх відновлення. Також серед ризиків – застосування фішингових схем, які спрямовані на отримання доступу до паролів або інших конфіденційних даних [1].

Таким чином, викрадення фінансової інформації може призвести до втрати коштів або їх використання для незаконних операцій, а розголошення персональних даних викликає репутаційні та юридичні ризики.

До ризиків слід також обов’язково віднести і можливі технічні збої – у такому разі відсутність резервного копіювання електронних баз даних може призвести до повної втрати інформації.

Отже, в сучасних реаліях хакерські атаки можуть завдати значної шкоди фінансовим процесам ЗВО. Вплив таких кібератак охоплює кілька аспектів:

1) економічні наслідки: втрата доступу до баз даних може спричинити затримки у виплаті заробітних плат, що вплине на якість роботи персоналу, а також існує ризик розкрадання коштів з рахунків ЗВО або благодійних фондів;

2) збої в управлінні: відсутність доступу до фінансових звітів унеможливлює оперативне прийняття рішень щодо витрат, а порушення звітності перед органами управління освітою може призвести до санкцій або призупинення фінансування;
3) репутаційні ризики: втрата довіри з боку персоналу та здобувачів вищої освіти освітньої установи, потенційних абітурієнтів, які можуть відмовитися від вступу на навчання до ЗВО, а також негативний імідж закладу освіти в інформаційному просторі.

Питання захисту освітніх баз даних у країнах ЄС, США, Канаді стало актуальним ще в середині 1990-х років, коли почали використовуватися перші автоматизовані програмні продукти для діловодства у закладах освіти, що відповідали стандартам FERPA (Family Educational Rights and Privacy Act) [2].

У Німеччині, Великобританії, Канаді та Австралії електронні журнали в освітній системі стали обов'язковими з 2000-х років, а в Швеції – з 2005 року [3]. Поряд з їх впровадженням завжди актуальним було питання гарантій захисту даних і наразі в країнах ЄС діють чіткі вимоги для роботи з освітніми платформами відповідно до регламенту GDPR (General Data Protection Regulation), а в скандинавських країнах всі навчальні заклади користуються інтегрованими державними платформами, які забезпечують збереження усієї звітності [4].

Таким чином, захист фінансових даних закладів вищої освіти системи МВС України є основою для забезпечення стабільної роботи освітньої системи, оскільки це дозволить уникнути непередбачуваних витрат, забезпечить відшкодування збитків у разі порушення роботи систем. Автоматизація фінансових процесів із захищеними системами забезпечує більшу прозорість та зручність управління.

Слід зазначити, що для підвищення рівня захисту інформації необхідно формувати цифрову компетентність з питань кібергігієни (уникнення підозрілих посилань, створення складних паролів тощо) науково-педагогічного складу, адміністрації та бухгалтерії закладів вищої освіти системи МВС України.

Список використаних джерел:

1. Бендер Ю. В. Вплив кіберзлочинності на фінансову сферу: проблеми та можливі рішення. Економіка і фінанси. 2017. № 6. С. 112-120.

2. Власенко С. Ю. Основи кіберстрахування: теорія та практика: книга для фахівців з фінансів та ІТ. 2020.

3. Броннер Д. Захист даних у цифрових платформах: принципи та підходи до страхування. Економіка та інновації. 2020. № 3(8). С. 65-70.

4. Огляд Європейського агентства з кібербезпеки: безпека електронних платформ для закладів освіти. ENISA : [сайт]. URL: http://www.enisa.europa.eu (дата звернення: 18.10.2025).