Ковтун В.В., ст. викладач
Державний університет «Житомирська політехніка»

КІБЕРБЕЗПЕКА В ДИСТАНЦІЙНІЙ ОСВІТІ

Кіберпростір згідно ЗУ «Про основні засади забезпечення кібербезпеки України» – це середовище, що надає шляхи взаємодії та реалізації суспільних відносин, утворене в результаті функціонування сумісних комунікаційних систем та забезпечення електронних комунікацій з використанням Інтернету або інших мереж передачі даних.

У зв'язку з подіями останніх кількох років (пандемія, повномасштабне вторгнення російської федерації в Україну), кіберпростір став незамінною альтернативою очному навчанню, що забезпечує безперервний доступ до освіти учням та студентам ВНЗ [3]. Окрім того, сучасних дітей змалку оточують гаджети, комп'ютерні мережі, тощо. У сучасному світі це цілком природне середовище.

Однак у цьому просторі присутня низка загроз, що потребують швидкого реагування та вдосконалення систем захисту. Існує багато різних підходів до типологізації загроз, що виникають з інформаційно-комунікаційних мереж, на думку автора основні загрози кібербезпеці у дистанційній освіті наступні:

1. Вразливості освітніх платформ. Навчальні платформи, такі як Moodle, Google Classroom, Zoom, Microsoft Teams, можуть містити недоліки у захисті, що дозволяє зловмисникам здійснювати атаки типу "людина посередині" (MITM), ін'єкційні атаки (SQL injection), атакувати через міжсайтові скрипти (XSS) або отримувати доступ до конфіденційних даних через недостатній захист автентифікації.
2. Кібератаки на мережеву інфраструктуру. Університетські мережі можуть стати об'єктами DDoS-атак, спрямованих на блокування доступу до навчальних сервісів. Крім того, зловмисники можуть здійснювати перехоплення даних у відкритих Wi-Fi-мережах або експлуатувати слабкі місця у VPN-з'єднаннях, що використовуються для дистанційного доступу до навчальних ресурсів.
3. Недостатній рівень кібергігієни Багато студентів та викладачів нехтують основними правилами кібербезпеки, зокрема використанням слабких паролів, повторним використанням паролів, відсутністю двофакторної аутентифікації (2FA) або встановленням ненадійного програмного забезпечення. Це підвищує ризик компрометації облікових записів та витоку даних.

Оскільки навчальні процеси дедалі більше переходять у цифрове середовище, забезпечення безпеки в Інтернеті під час дистанційного навчання є надзвичайно важливим. Захист автентифікації та доступу є ключовим заходом [5, с. 80]. Багатофакторна автентифікація (MFA) значно ускладнює несанкціонований доступ до облікових записів викладачів і студентів. Сучасні методи ідентифікації, такі як біометрична автентифікація та апаратні ключі безпеки, такі як YubiKey або Google Titan, покращують захист доступу. Розмежування прав доступу до навчальних ресурсів залежно від рівня довіри та ролі користувачів у системі також є важливим.

Протоколи TLS/SSL гарантують безпечне зв'язок між користувачами та серверами навчальних платформ. Наскрізне шифрування (E2EE) доцільно використовувати для захисту комунікацій під час відеоконференцій і обміну навчальними матеріалами. Усі дані в хмарних освітніх сервісах також мають бути зашифровані, щоб запобігти витоку та несанкціонованому доступу. Постійний моніторинг та аналіз кібербезпеки є необхідними для виявлення потенційних загроз. Системи виявлення та запобігання вторгненням (IDS/IPS) можна використовувати для виявлення та усунення незвичайних дій у мережах університетів. Дозволяє оперативно реагувати на інциденти завдяки централізованому аналізу кіберзагроз SIEM [2, с. 200]. Допомагає запобігти потенційним атакам шляхом регулярного сканування навчальних платформ на наявність вразливостей за допомогою спеціалізованого програмного забезпечення (наприклад, Nessus, OpenVAS, Qualys).

Кібербезпека в дистанційній освіті потребує комплексного підходу, який включає в себе освітні, організаційні та технічні заходи. Сучасні технології шифрування, багатофакторної автентифікації, моніторингу загроз і навчання користувачів дозволяють створювати безпечне цифрове освітнє середовище, яке відповідає сучасним викликам кіберпростору.

Для забезпечення безпеки слід приділяти більшу увагу організаційним підходам, які базуються на дослідженнях відомих компаній у кіберпросторі. Наприклад, у щомісячному моніторинговому звіті за вересень 2020 року Fidelis Threat Intelligence Team, лідер у США з пошуку та блокування кібер-небезпек, застерігає від використання Internet Explorer, особливо версій IE11, а також Adobe Flash, який часто використовується в навчальному процесі [7].

Кібербезпека у вищій дистанційній освіті потребує комплексного підходу, що включає як технічні, так і організаційні методи захисту. Найефективніші стратегії включають багатофакторну автентифікацію, шифрування даних, використання сучасних систем моніторингу загроз та впровадження програм підвищення обізнаності студентів і викладачів. Подальші дослідження у сфері кібербезпеки освіти можуть бути спрямовані на вдосконалення адаптивних механізмів реагування на кіберзагрози та впровадження штучного інтелекту для їх автоматизованого виявлення.

Список використаних джерел:

1. Дистанційне навчання в системі професійно-технічної освіти. Монографія / авт. кол. В. В. Ягупов, Л. М. Петренко, С. Г. Кравець та ін. За наук. ред. В. В. Ягупова. Житомир. Полісся. 2019. 234 с. URL: https://lib.iitta.gov.ua/id/eprint/721757/1/Дистанц_монограф.pdf (дата звернення: 10.03.2025).
2. Інформаційна та кібербезпека. Підручник / за ред. В. В. Бурячка. Суми. СумДПУ імені А. С. Макаренка. 2019. 200 с. URL: https://duikt.edu.ua/uploads/p_303_79299367.pdf (дата звернення: 10.03.2025).
3. Інформаційні технології в контексті міжнародних відносин. Кібербезпека як один із викликів сучасної цифрової епохи. Національний університет «Києво-Могилянська академія». 2024. URL:

https://ekmair.ukma.edu.ua/bitstreams/4705dd15-6aa1-4493-b206-2c2e94b7553d/download (дата звернення: 10.03.2025).

4. Кібербезпека № 10/2023. Аналітичний дайджест. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». Національна бібліотека України ім. В. І. Вернадського. Київ. 2023. 320 с. URL: https://ippi.org.ua/sites/default/files/2023-10_0.pdf (дата звернення: 10.03.2025).

5. Кібербезпека в цифровому освітньому середовищі. БІНПО ДЗВО «УМО» НАПН України. 2022. 80 с. URL: https://lib.iitta.gov.ua/id/eprint/733620/1/KIBERBEZPEKA.pdf (дата звернення: 10.03.2025).

6. Освітньо-професійна програма «Кібербезпека». Одеський національний політехнічний університет. 2020. URL: https://op.edu.ua/sites/default/files/files/opscans/proj/proekt_op_2020_125_bak.pdf (дата звернення: 10.03.2025).

7. Тези доповідей Студентської Конференції Інформаційна, Функційна і Кібербезпека. I Scientific and Practical Conference. 2023. URL: https://www.researchgate.net/publication/375792766_Tezi_dopovidej_Studentskoi_Konferencii_Informacijna_Funkcijna_i_Kiberbezpeka (дата звернення: 10.03.2025).