Роман ВЛАСЕНКО,
курсант 4 курсу, здобувач першого (бакалаврського) рівня вищої освіти
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут (м. Київ)
e-mail: vlasenkoroman05@gmail.com
Олександр ЖАДАН,
курсант 4 курсу, здобувач першого (бакалаврського) рівня вищої освіти
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут (м. Київ)
e-mail: sanyazadan11@gmail.com

Науковий керівник:
Ольга МИРОНЕНКО,
старший викладач кафедри фундаментальних дисциплін
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут (м. Київ)

ЦИФРОВА БЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ ЗАКЛАДІВ ОСВІТИ В УМОВАХ ВОЄННОГО СТАНУ

У 2025 році команда CERT-UA опрацювала 5927 кіберінцидентів, на 37,4 % більше, ніж у 2024 році. Серед головних загроз року Національний координаційний центр кібербезпеки називає фішинг із генеративним штучним інтелектом і масову компрометацію облікових записів, а основним джерелом атак лишаються російські хакерські угруповання [1]. Ті самі методи зловмисники застосовують проти закладів освіти. З 2022 року викладачі ведуть значну частину занять у Moodle, Google Workspace і Microsoft 365, тож через скриньку одного працівника нападник дістається журналів оцінок і хмарних дисків кафедри. Водночас заклад як володілець персональних даних тисяч людей, серед них неповнолітніх, зобов’язаний ці дані захищати [2].

У листопаді 2025 року CERT-UA розслідувала атаку угруповання UAC-0241 на один із закладів вищої освіти Сумщини. Зловмисники розіслали закладам освіти і органам влади лист «Наказ № 332» зі справжньої Gmail-скриньки університету, на якій не було двофакторної автентифікації. Ярлик із вкладеного архіву через штатні mshta.exe і PowerShell встановлював програми для викрадення паролів і файлів та бекдор GAMYBEAR. Перше

зараження сталося ще 26 травня, коли користувач закладу відкрив лист нібито від Управління ДСНС у Сумській області. Пів року керівництво не знало, що сторонні мають доступ до комп'ютерів університету й можуть атакувати з них інші організації. CERT-UA пов'язує такі випадки з тим, що відповідальні особи нехтують базовими налаштуваннями захисту Windows і не повідомляють команду про інциденти [3].

Антивірус і складний пароль зменшують шанс проникнення, проте нічого не підказують керівникові, коли нападник уже в мережі. Для такої ситуації NIST пропонує поняття кіберстійкості: здатності системи передбачати несприятливі події, витримувати атаки, відновлюватися після них і пристосовуватися до нових умов [4, p. 1]. Український закон теж відносить до кіберзахисту відновлення сталості та надійності роботи систем після атак [5, ст. 1]. Для закладу освіти кіберстійкість означає, що заняття тривають і після шифрування сервера чи зламу пошти.

Будувати таку роботу керівнику зручно за NIST Cybersecurity Framework 2.0. Документ ділить кіберзахист на шість функцій: урядування (Govern), ідентифікацію, захист, виявлення, реагування та відновлення [6]. Функцію Govern розробники додали у версії 2.0, і вона закріплює відповідальність за кіберризики за керівництвом організації.

В. Биков, О. Буров і Н. Дементієвська вважають найнебезпечнішою загрозою для учасників освітнього процесу соціальну інженерію [7, с. 313]. І. Вербовський та О. Шелуха серед типових проблем українських закладів освіти називають низьку цифрову культуру персоналу та відсутність стандартних протоколів реагування на інциденти [8, с. 316]. З огляду на це пропонуємо п'ять заходів, які не потребують великого бюджету.

1) Увімкнути двофакторну автентифікацію для всіх службових облікових записів, у першу чергу для пошти та адміністраторів LMS. М. Швардак вважає її обов'язковою для викладачів і керівництва [9].

2) Заборонити звичайним користувачам запуск mshta.exe, файлів HTA і JS, Windows Script Host і PowerShell. Адміністратор налаштовує це груповими політиками Windows без витрат, а CERT-UA радить такі обмеження понад два роки [3].

3) Зберігати резервні копії журналів, курсів і баз персональних даних за правилом 3-2-1 з однією копією поза мережею закладу та раз на семестр перевіряти відновлення. План відновлення після кібератаки доцільно

поєднати з планом на випадок тривалого знеструмлення: в обох сценаріях керівник вирішує, де й на чому викладач продовжить заняття.

4) Призначити наказом відповідального за кіберзахист і прописати порядок повідомлення CERT-UA про інциденти. У 2025 році держава запровадила посади керівників з кіберзахисту в органах влади [1]; закладу освіти вистачить одного працівника з цими обов'язками.

5) Раз на квартал проводити для працівників коротке заняття з кібергігієни на реальних прикладах, як-от лист «Наказ № 332». Курсанти та студенти спеціальності «Кібербезпека» могли б вести такі заняття в школах і коледжах свого міста як частину навчальної практики.

Отже, фішинг у 2025 році став основним способом початкового проникнення в мережі українських організацій [1], і сумський інцидент теж почався з листа. Тому двофакторна автентифікація та навчання персоналу дають закладу освіти найбільший результат за найменших витрат. Кіберстійкість закладу залежить від керівника так само, як від адміністратора: керівник затверджує план відновлення і призначає відповідального.

Список використаних джерел:

1. Огляд національної системи кібербезпеки України 2025 : аналітичне дослідження / Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України. Київ, 2026. 61 с. URL: https://rnbo.gov.ua/files/2026/NATIONAL_CYBER_SCC/kiber_2025.pdf (дата звернення: 07.10.2026).

2. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 07.10.2026).

3. Кібератака UAC-0241 у відношенні навчального закладу на сході України з використанням програмного засобу GAMYBEAR (CERT-UA#18329). CERT-UA. 2025. URL: https://cert.gov.ua/article/6286219 (дата звернення: 07.10.2026).

4. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST, Special Publication 800–160, Vol. 2, Rev. 1. Gaithersburg, MD : National

Institute of Standards and Technology, 2021. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 07.10.2026).

6. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg : National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29.

7. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання.* 2019. № 2, т. 70. С. 313–331. DOI: https://doi.org/10.33407/itlt.v70i2.2876 (дата звернення: 07.10.2026).

8. Вербовський І., Шелуха О. Управління кіберризиками в освітньому середовищі. *Економіка. Управління. Інновації.* 2025. № 2 (37). С. 316–336. DOI: https://doi.org/10.35433/ISSN2410-3748-2025-2(37)-19 (дата звернення: 07.10.2026).

9. Швардак М. В. Кібербезпека у цифровому освітньому просторі. *Науковий часопис Хортицької національної академії*. 2025. Вип. 1 (12). С. 26–33. DOI: https://doi.org/10.51706/2707-3076-2025-12-2 (дата звернення: 07.10.2026).