Віталій МАСИЧ,
курсант 4 курсу,
здобувач першого (бакалаврського) рівня вищої освіти
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут,
м. Київ
e-mail: masych.vitaliy@gmail.com
Богдан КОСТЮК,
курсант 4 курсу,
здобувач першого (бакалаврського) рівня вищої освіти
Військового інституту телекомунікацій та інформатизації
імені Героїв Крут (м. Київ)
e-mail: bohdansteam2000@gmail.com

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

ФОРМУВАННЯ КІБЕРГІГІЄНИ ТА НАВИЧОК БЕЗПЕКИ ДАНИХ У ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Повномасштабна військова агресія російської федерації проти України остаточно деконструювала класичні межі збройного конфлікту, перетворивши цифровий та інформаційний простір на повноцінний театр воєнних дій. Сучасна гібридна війна інтегрує конвенційні бойові операції, високотехнологічні кібератаки та цілеспрямовані когнітивні кампанії, спрямовані на дестабілізацію критичної інфраструктури, публічних інституцій і деморалізацію суспільства [1, с. 14]. У цій архітектурі вітчизняні заклади вищої освіти (ЗВО) є стратегічними мішенями для ворожих спецслужб та підконтрольних їм кіберугруповань (Advanced Persistent Threat – APT) [2, с. 48]. Здобувачі вищої освіти виступають активними суб’єктами цифрового середовища, залученими до волонтерських зборів, кіберопору та наукових досліджень. Водночас статус «цифрових аборигенів» (digital natives) формує оманливу ілюзію захищеності: побутова активність молоді часто поєднується з безтурботністю та відсутністю

культури безпеки даних, що створює критичні вразливості для проникнення супротивника в університетські комп'ютерні мережі [3, с. 88].

Фундаментальні засади функціонування систем кібербезпеки та протидії кіберзагрозам висвітлено у працях О. Корченка, В. Гнатюка, В. Богуша, К. Захарова, Ю. Сєрих та І. Дзюби [1, с. 18; 4, с. 102]. Педагогічні аспекти розвитку цифрової грамотності майбутніх фахівців ґрунтовно досліджували В. Биков, М. Дорош, В. Шеломовська та О. Спірін [5, с. 42; 6, с. 183]. Міжнародний досвід розбудови кіберстійкості узагальнено у стандартах ENISA [7, с. 12], керівних принципах NIST [8, с. 15] та рекомендаціях NATO CCDCOE [9, с. 24]. Разом із тим, у вищій школі потребує розв'язання проблема практичного формування культури кібергігієни у студентів нетехнічних спеціальностей в умовах воєнного стану. Метою дослідження є теоретичне обґрунтування компонентної структури кібергігієни, систематизація векторів загроз на основі аналізу практичних кейсів і емпіричних спостережень, а також розробка матриці компетентностей безпеки даних у здобувачів вищої освіти.

Для верифікації реального рівня безпекової культури студентської молоді нами проведено пілотне діагностичне анкетування 54 здобувачів вищої освіти Тернопільського національного педагогічного університету імені Володимира Гнатюка (гуманітарних, природничих та педагогічних спеціальностей). Результати засвідчили гострий розрив між суб'єктивною самооцінкою цифрової обізнаності та реальними діями студентів: 72,2% опитаних використовують однакові або спрощені паролі для особистих і навчальних акаунтів (Moodle, Google Workspace); 63,0% респондентів свідомо уникають використання багатофакторної автентифікації (MFA/2FA), вважаючи її обтяжливою; 57,4% здобувачів зізналися, що переходили за сумнівними посиланнями через емоційні тригери виплат чи сесії; 81,5% регулярно користуються публічним Wi-Fi без VPN, а 75,9% студентів мають хибне переконання, що їхні пристрої не становлять інтересу для ворожих кібератак.

Академічний сектор перебуває під постійним прицілом ворожих кіберугруповань Gamaredon (UAC-0010), Sandworm (UAC-0082) та APT28 [2, с. 52]. Домінантними векторами загроз є: 1) таргетований соціальний інжиніринг (Spear Phishing). Навчально-практичним кейсом є розсилання фішингових листів від імені деканату з темою «Терміново: оновлення

наказів щодо стипендій та військового обліку на осінній семестр» із домену-спуфера («decanat@tnpu-edu.online»), де перехід за посиланням на клон сторінки входу веде до викрадення єдиного облікового запису (SSO) студента та компрометації реєстрів ЗВО [7, с. 28]; 2) інфікування шкідливим ПЗ класу Infostealer (RedLine, Vidar, LummaC2) через поширення у студентських чатах зламаного софту для лабораторних робіт (SPSS, AutoCAD, компіляторів), що призводить до викрадення браузерних паролів і сесійних токенів [4, с. 108]; 3) ризики розвідки на основі відкритих джерел (OSINT) через публікацію фотографій корпусів і геолокацій [3, с. 94].

Кібергігієна здобувача розглядається нами як багатовимірний комплекс, що інтегрує: когнітивний компонент (знання законодавства України [10], розуміння мережевих загроз, тактик соціальної інженерії та методів ІПСО); операційно-технологічний (застосування менеджерів паролів із наскрізним шифруванням, апаратних та застосункових TOTP-генераторів, повнодискового шифрування та бекапування «3-2-1»); поведінково-рефлексивний (інтерналізація принципу «Zero Trust» – «ніколи не довіряй, завжди перевіряй», імунітет до маніпуляцій, негайне інформування IT-підрозділу ЗВО про інциденти [8, с. 21]); та ціннісно-мотиваційний компонент (інформаційна відповідальність, академічна доброчесність і повна відмова від використання програмного забезпечення держави-агресора), що деталізовано у відповідній матриці компетентностей (табл. 1).

Формування практичної культури кібергігієни у ЗВО вимагає реалізації комплексу заходів [5, с. 49; 6, с. 185]: 1) впровадження наскрізного мікромодуля «Кібергігієна в умовах воєнного стану» для всіх спеціальностей на засадах мікронавчання (Microlearning) по 15 хвилин із кейс-стаді; 2) проведення регулярних симуляцій фішингу (Phishing Simulation Awareness) із обов’язковим подальшим дебрифінгом [7, с. 45]. Методологія дебрифінгу виключає покарання здобувачів, фокусуючись на психолого-педагогічному аналізі маркерів підробки та відпрацюванні дій при компрометації даних; 3) впровадження змагань у форматі Academic CTF (Capture The Flag) за адаптованими сценаріями: «OSINT-розслідувач» (пошук метаданих EXIF на фотографіях), «Детектив підозрілих посилань» (перевірка URL через VirusTotal) та «Аудитор паролів» [4, с. 115]; 4) нормативне закріплення обов’язкової двофакторної автентифікації на

базі FIDO2 для сервісів ЗВО, регламентація політики безпеки власних пристроїв (BYOD) та повна заборона софту і сервісів держави-агресора.

Таблиця 1

Матриця кібербезпекових компетентностей здобувача вищої освіти в умовах гібридної війни

Рівень загрози	Вектор гібридної атаки	Необхідні компетентності здобувача	Технологічний та організаційний
Індивідуальний	Таргетований фішинг (Spear Phishing), підроблені чат-боти деканату, діпфейки керівництва ЗВО	Верифікація цифрових сертифікатів (SSL/TLS), аналіз службових заголовків листів (SPF, DKIM, DMARC), критичне декодування емоційних тригерів	Багатофакторна автентифікація (FIDO2/WebAuthn), апаратні ключі доступу, антифішингові фільтри, захищені DNS-сервіси (Cloudflare 1.1.1.2)
Локальний / Апаратний	Інфостілери (RedLine, LummaC2), шпигунське ПЗ, небезпечні публічні Wi-Fi мережі, заражені знімні USB-носії	Контроль цілісності операційної системи, розділення особистого й навчального профілів пристрою, санітарія знімних накопичувачів	Повнодискове шифрування (FileVault, BitLocker), перевірені протоколи VPN (WireGuard), блокування автозапуску знімних накопичувачів
Академічний	Компрометація платформ LMS (Moodle, Teams), витік персональних баз даних студентів, OSINT-деанонімізація	Дотримання регламентів безпечного обміну даними, мінімізація цифрового сліду, неухильне дотримання протоколів реагування на кіберінциденти	Менеджери паролів із Zero-Knowledge архітектурою (Bitwarden, KeePass), наскрізне шифрування, регулярний аудит активних веб-сесій
Когнітивно-державний	ІПСО супротивника, дезінформація про навчальний процес і ЗСУ, штучна деморалізація студентства	Розвинена інформаційна медіаграмотність, практичні навички фактчекінгу, імунітет до когнітивних маніпуляцій ворожих джерел	Офіційні верифіковані державні канали комунікації, інструменти OSINT-верифікації першоджерел, платформи спростування фейків

Висновки та перспективи подальших наукових розвідок. В умовах повномасштабної гібридної війни формування кібергігієни та розвинених навичок безпеки даних у здобувачів вищої освіти є критичним чинником захисту суверенітету та стійкості вищої школи України. Здобувач освіти має розглядатися як свідомий суб'єкт кібероборони держави. Запропонована компонентна структура та матриця компетентностей, підкріплені аналізом реальних кейсів, емпіричними даними та прикладними педагогічними технологіями, створюють надійну основу для модернізації освітнього процесу ЗВО. Перспективи подальших розвідок полягають у розробці адаптивних алгоритмів діагностики кібервразливості студентів із використанням моделей машинного навчання.

Список використаних джерел:

1. Гнатюк В. П., Дзюба І. В., Сєрих Ю. І. Кібергігієна як базовий елемент системи національної кібербезпеки в умовах воєнного стану. *Сучасний захист інформації.* 2023. № 2 (54). С. 12–21.

2. Богуш В. М., Юдін О. К., Корченко О. Г. Управління інцидентами інформаційної безпеки та кіберзагрозами в критичних інфраструктурах : монографія. Київ : НАУ, 2022. 312 с.

3. Дорош М. В., Горовий В. М. Цифрова стійкість та інформаційна безпека людини в умовах гібридної війни. *Інформаційна безпека людини, суспільства, держави.* 2023. № 1–2 (33–34). С. 84–97.

4. Корченко О. Г., Іванченко Є. В. Методи протидії шкідливому програмному забезпеченню та соціальній інженерії в освітніх мережах. *Захист інформації.* 2023. Т. 25, № 2. С. 101–118.

5. Биков В. Ю., Спірін О. М. Цифрова компетентність учасників освітнього процесу в кризових умовах: безпековий вимір. *Інформаційні технології і засоби навчання.* 2022. Т. 88, № 2. С. 40–55.

6. Шеломовська В. О., Захаров К. В. Формування цифрової компетентності та культури безпеки даних майбутніх фахівців в умовах цифровізації освіти. *Науковий вісник Ужгородського університету. Серія: «Педагогіка. Соціальна робота».* 2023. Вип. 2 (53). С. 182–187.

7. ENISA Threat Landscape 2023 / European Union Agency for Cybersecurity. Luxembourg : Publications Office of the European Union, 2023. 138 p.

8. The NIST Cybersecurity Framework (CSF) 2.0 / National Institute of Standards and Technology. Gaithersburg : NIST, 2024. 32 p.

9. NATO CCDCOE. Cyber Hygiene: Principles and Educational Frameworks. Tallinn : NATO CCDCOE, 2023. 64 p.

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII (ред. від 28.07.2023). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.10.2026).