УДК 004.056.55:378
DOI https://doi.org/10.11603/m.2414-5998.2025.2.15490

А. В. Чорномидз
ORCID https://orcid.org/0000-0001-5479-8298

Тернопільський національний медичний університет імені І. Я. Горбачевського МОЗ України

ІНФОРМАЦІЙНА БЕЗПЕКА ВИКЛАДАЧІВ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ В УМОВАХ ВОЄННОГО СТАНУ: ВИКЛИКИ ТА ПРАКТИЧНІ РЕКОМЕНДАЦІЇ

A. V. Chornomydz

Ivan Horbachevsky Ternopil National Medical University of the Ministry of Health of Ukraine

FACULTY INFORMATION SECURITY IN HIGHER EDUCATION INSTITUTIONS AMIDST MARTIAL LAW: CHALLENGES AND PRACTICAL GUIDELINES

Анотація. У статті висвітлено актуальне питання забезпечення інформаційної безпеки викладачів закладів вищої освіти в умовах воєнного стану, що триває в Україні. Розглянуто вплив війни на цифрове освітнє середовище, а також на рівень загроз, з якими щоденно стикаються викладачі у своїй професійній діяльності. Акцентовано увагу на кіберзагрозах (фішинг, шкідливе програмне забезпечення, DDoS-атаки), ризиках розголошення особистої інформації, використанні соціальних мереж як інструменту пропаганди та дезінформації, а також на психологічних чинниках, які впливають на здатність викладача зберігати інформаційну стійкість. Теоретичною основою аналізу слугували концепції тріади CIA (конфіденційність, цілісність, доступність), моделі управління інформаційною безпекою (зокрема ISO/IEC 27001), а також підходи до оцінки ризиків та врахування людського фактору. Окреслено типові ситуації ризику, з якими може зіткнутися викладач, і подано рекомендації щодо індивідуального та організаційного рівнів захисту. Особливу увагу приділено психологічному аспекту інформаційної безпеки, включно з інформаційною втомою, емоційним вигоранням та потребою в підтримці цифрового самоконтролю. Запропоновано комплекс практичних порад і стратегій саморегуляції. Матеріали статті можуть бути корисними для адміністрацій ЗВО, викладачів, ІТ-фахівців та науковців, що досліджують освітню безпеку в умовах кризових ситуацій.

Ключові слова: інформаційна безпека; викладачі; кіберзагрози; заклади вищої освіти; воєнний стан.

Abstract. This article addresses the urgent issue of ensuring information security for university educators during the period of martial law in Ukraine. It explores the impact of wartime conditions on the digital educational environment and highlights the spectrum of threats that educators face daily in their professional activities. Particular attention is paid to cyber threats (phishing, malware, DDoS attacks), risks of personal data exposure, the role of social media in propaganda and disinformation, as well as psychological factors influencing educators' ability to maintain informational resilience. The theoretical framework includes the CIA triad (confidentiality, integrity, availability), information security management models (notably ISO/IEC 27001), risk assessment approaches, and user behavior theories. Typical risk situations are outlined, and recommendations are provided for both individual and institutional levels of protection. Special focus is placed on the psychological dimension of information security, including information fatigue, emotional burnout, and the need for digital self-regulation and peer support. The study offers a comprehensive set of practical tips and self-regulation strategies tailored to the educational context. The materials presented in this paper can be useful for university administrations, academic staff, IT specialists, and researchers in the field of educational safety and crisis-response pedagogy.

Key words: Information security; educators; cyber threats; higher education institutions; martial law.

Вступ. В умовах воєнного стану, що триває в Україні, питання інформаційної безпеки набуває особливої гостроти як на рівні державних інституцій, так і в повсякденному житті громадян. Особливу вразливість у цьому контексті демонструють науково-педагогічні працівники, які, окрім виконання своїх основних обов'язків із навчання та наукової діяльності, активно залучені до цифрової комунікації, управління освітнім процесом і взаємодії в онлайн-середовищі. Викладачі стикаються із цілою низкою загроз: від фішингових атак, витоку конфіденційної інформації до впливу дезінформаційних кампаній і психологічного тиску, спричиненого інформаційним перевантаженням. Паралельно зростає соціальне значення викладача як лідера думок та публічної особи, чия присутність у медіапросторі може бути використана як ціль для інформаційних маніпуляцій [2].

Актуальність дослідження інформаційної безпеки викладачів у контексті війни зумов-

лена потребою в захисті особистої і професійної інформації, стабільності освітнього процесу, а також збереженні психоемоційної стійкості працівників освіти. Водночас, попри дедалі більшу увагу до кібербезпеки загалом, питання саме педагогічної інформаційної безпеки ще недостатньо висвітлене в сучасній науковій літературі.

Метою статті є систематизація основних загроз інформаційній безпеці викладачів у воєнний період, аналіз відповідних практик захисту, а також формулювання практичних рекомендацій, що сприятимуть підвищенню інформаційної грамотності, цифрової стійкості та безпеки в освітньому середовищі.

Теоретичні основи інформаційної безпеки викладача. У контексті дослідження інформаційної безпеки викладача в умовах воєнного стану ключовим є розуміння базових понять, моделей і концепцій, що формують наукове підґрунтя теми. Так, інформаційна безпека – це багатовимірне поняття, що охоплює захист конфіденційності, цілісності та доступності інформації незалежно від її форми – електронної, паперової чи усної. Особливої актуальності воно набуває в умовах війни, коли зростають ризики втручання, маніпуляцій та компрометації інформаційних ресурсів. Своєю чергою, кібербезпека є підсистемою інформаційної безпеки, зосередженою на захисті інформаційних систем, мереж і цифрових даних від кіберзагроз [2].

У контексті освітнього середовища поняття інформаційної безпеки викладача пов’язане не лише з технічним захистом персональних даних, а й з формуванням інформаційної культури, цифрової етики та стійкості до впливу дезінформації.

Воєнний стан та інформаційна війна. Воєнний стан в Україні створює кризовий контекст, що характеризується нестабільністю, невизначеністю та зростанням ризиків. У таких умовах інформаційна війна – один із ключових інструментів впливу. Вона містить кіберзлочинність, психологічні операції, пропаганду, поширення фейків і спрямована як на дестабілізацію супротивника, так і на мобілізацію підтримки серед населення.

Класичною основою інформаційної безпеки є модель CIA – Confidentiality, Integrity, Availability [1], яка передбачає основні три принципи:

1. Конфіденційність. Захист чутливої інформації викладача (персональні дані, списки студентів, службова інформація) від несанкціонованого доступу. У воєнних умовах витік таких даних може мати небезпечні наслідки [4].

2. Цілісність. Гарантія незмінності даних. Для викладача це означає захист навчальних матеріалів, оцінок, електронної переписки від викривлення або підробки.

3. Доступність. Забезпечення постійного доступу до навчальних ресурсів, навіть у разі кіберінцидентів або перебоїв зі зв’язком.

Ці принципи реалізуються через шифрування, контроль доступу, резервне копіювання, цифрові підписи, та інші технічні й організаційні заходи [4].

Ефективне забезпечення безпеки передбачає управління ризиками: ідентифікацію загроз, виявлення вразливостей і розробку контрзаходів. У період війни спектр ризиків суттєво зростає: кібератаки, цілеспрямовані фейкові кампанії, проникнення через соціальну інженерію тощо.

Найбільш вразливим елементом у системі безпеки залишається користувач. У випадку викладача, стрес, перевантаження, брак технічної підготовки можуть призводити до критичних помилок.

Міжнародні моделі та стандарти. До найважливіших системних підходів, які можна застосовувати в освітньому середовищі навіть під час війни, належать:

ISO/IEC 27001 – міжнародний стандарт управління інформаційною безпекою [1];

Defense in Depth – концепція глибокоешелонованого захисту: кілька рівнів безпеки, кожен з яких блокує потенційний прорив;

Risk Assessment Frameworks – дають змогу системно оцінювати ризики та планувати заходи з урахуванням їх критичності.

Межі цифрової компетентності викладача (зокрема, DigCompEdu) містять модулі, пов’язані з інформаційною безпекою: захист пристроїв, управління даними, дотримання етичних норм онлайн-взаємодії, формування критичного ставлення до інформаційного контенту.

Так, теоретичне осмислення інформаційної безпеки викладача в умовах воєнного стану потребує міждисциплінарного підходу, що поєднує технічні, правові, педагогічні та психологічні складники. Ключовими поняттями є тріада CIA, інформаційна війна, кібербезпека, управління ризиками та поведінкові моделі користувачів. В умовах дедалі більших загроз критично важливо, щоб викладачі не лише володіли технічними навичками захисту інформації, а й формували високий рівень інформаційної культури та цифрової стійкості [1].

Знання основних міжнародних стандартів (ISO/IEC 27001), принципів багаторівневого захисту (Defense in Depth) та поведінкових моделей дає змогу ефективніше адаптувати стратегії захисту до реалій воєнного часу. Саме на цьому підґрунті будується подальший аналіз практичних викликів та ризиків, з якими стикається викладач у кризових умовах [1].

Особливості діяльності викладача в умовах воєнного стану. Воєнний стан в Україні кардинально трансформував освітній простір, змінивши формати взаємодії, цифрові практики та рівень інформаційної загрози. Викладач опинився в умовах не лише професійного, а й особистого виклику, коли кожен цифровий крок може мати реальні наслідки.

Зміна інформаційного середовища. З початком повномасштабного вторгнення викладачі масово перейшли до дистанційного або гібридного навчання. Це означає: зростання залежності від цифрових сервісів (Zoom, Moodle, Google Workspace, Microsoft Teams тощо); інтенсифікацію комунікації через соціальні мережі та месенджери (Viber, Telegram, Signal); появу нових каналів взаємодії зі студентами, батьками, адміністрацією.

Водночас цифрове середовище стало полем для кіберзагроз – від фішингових листів до вторгнень у відеозустрічі та викрадення персональних даних [2].

Інформаційні ризики в щоденній роботі викладача. В умовах воєнного стану інформаційний простір є не лише важливим каналом обміну знаннями, а й полем ризиків – технічних, поведінкових і психологічних. Особливо це стосується викладачів, які є публічними особами, володіють чутливою інформацією й постійно взаємодіють із цифровими системами.

Серед найбільш поширених викликів:

Кіберзагрози, фішинг. У період тривожності й інформаційного перевантаження фішинг стає одним із найефективніших інструментів кіберзлочинців. Зловмисники активно використовують такі теми [2]: «термінове оновлення облікових записів», «зміни у процедурі евакуації», «фінансова допомога від держави чи волонтерів».

Наприклад: викладач отримує e-mail, замаскований під лист від ректорату, з проханням «підтвердити дані акаунту для збереження доступу». Перехід за посиланням веде до фальшивої сторінки авторизації.

Шкідливе програмне забезпечення (malware). Злочинці поширюють трояни або програми-вимагачі через підроблені документи (інструкції, списки евакуації, новини), заражені архіви в групах викладачів, компрометовані сайти зі зниженими рівнями безпеки. Наприклад: файл «пам'ятка з виживання під час блекауту» містить шкідливий скрипт, який краде збережені паролі в браузері викладача.

DDoS-атаки [2]. Хоча такі атаки рідко спрямовані особисто на викладачів, вони виводять з ладу онлайн-платформи, порушують проведення занять, руйнують довіру до цифрової стабільності навчального процесу.

Загрози, пов'язані з розголошенням особистої інформації. Воєнний стан підвищує вразливість до використання особистих даних у ворожих цілях. Особливо небезпечними є публікації з геолокацією (фото з місця перебування); згадка в соцмережах про маршрути, переміщення, участь у гуманітарних місіях; поширення номерів, адрес, інформації про дітей, родину. Наприклад: після допису у Facebook з хештегом #Чернігів викладач стає об'єктом дзвінків із погрозами або маніпуляціями.

Використання соціальних мереж та месенджерів. Соцмережі є не лише каналом комунікації, а й вразливим місцем. Серед найчастіших проблем є злам акаунтів викладачів: поширення фейків або компрометаційних дописів; масовані інформаційні атаки через Telegram-канали, TikTok, псевдопатріотичні сторінки. Месенджери можуть бути каналами впливу: маніпулятивні листи або запрошення до «неофіційних груп студентів» із фейковим адміністратором. Наприклад: акаунт викладача у Facebook використовують для поширення фальшивої «заяви МОН про припинення навчання в регіоні».

Дезінформація та пропаганда [5]. Дезінформаційні кампанії підривають довіру до офіційних рішень, створюють паніку серед викладачів і студентів, спрямовані на деструкцію авторитету науки та освіти. Викладачі як інтелектуальні лідери особливо вразливі до маніпулятивних «аналітичних звітів», фальсифікованих інтерв'ю, спотворених цитувань. Наприклад: у Twitter поширюється цитата, вирвана з контексту онлайн-лекції викладача, з метою дискредитації ЗВО.

Небезпеки психологічного характеру. Воєнний стрес поєднується з інформаційною втомою, емоційним вигоранням, почуттям відповідальності за студентів і колег. Постійний потік тривожної інформації, часті повітряні тривоги, відсутність світла чи зв'язку – усе це створює емоційне напруження, що знижує здатність до критичного мислення та підвищує вразливість до фейків.

Виклики організаційного характеру. Відсутність чітких інструкцій щодо кібербезпеки в деяких ЗВО.

1. Обмеженість ресурсів (немає VPN, недостатній захист Wi-Fi у гуртожитках тощо).

2. Необхідність самостійно шукати способи захисту, часто без належної технічної підтримки.

Типологія загроз показує, що викладач як інформаційний агент, лідер думок і цифровий користувач стає багатовимірною мішенню. Тому важливо не лише знати про загрози, а й уміти їх розпізнавати, критично аналізувати та вчасно реагувати.

Методи та інструменти захисту інформаційної безпеки викладача. З огляду на складність сучасного інформаційного середовища, ефективна безпека викладача вимагає комплексного підходу: від базових навичок цифрової гігієни до впровадження міжнародних стандартів безпеки в освітніх установах.

Технічні інструменти. Двофакторна автентифікація (2FA). Забезпечує додатковий рівень безпеки при вході до акаунтів. Рекомендується використовувати через застосунки (Google Authenticator, Authy), а не SMS.

Менеджери паролів. Наприклад: Bitwarden, KeePass, 1Password. Дозволяють створювати й зберігати складні, унікальні паролі для кожного сервісу.

VPN та шифрування [4]. VPN (ProtonVPN, NordVPN) захищає з'єднання у відкритих мережах (кафе, гуртожитки). Шифрування файлів (VeraCrypt, BitLocker) – для захисту локальної інформації [4].

Резервне копіювання. Хмарне (Google Drive, OneDrive) або локальне (на зовнішні носії). Рекомендовано зберігати копії матеріалів щонайменше у двох місцях.

Поведінкові та етичні практики. Критичне мислення щодо інформації [5]: уникати поширення неперевірених повідомлень, відстежувати першоджерела новин, користуватися платформами фактчекінгу (StopFake, VoxCheck).

Цифрова етика: обережно поводитися з конфіденційною інформацією студентів і колег; уникати емоційних коментарів у соціальних мережах, які можуть бути неправильно інтерпретовані.

Приватність у соцмережах: закрити доступ до особистих даних, використовувати окремі акаунти для навчання й особистого життя, не ділитися точним місцеперебуванням у режимі реального часу.

Організаційні заходи в навчальному закладі. Впровадження політик безпеки: чітко прописані правила збереження паролів, розмежування доступів, поводження з електронною поштою; підписання угод про відповідальне використання ІКТ.

Підвищення цифрової грамотності: курси з кібергігієни для викладачів, регулярні симуляції фішинг-атак із подальшим аналізом помилок. [2]

Підтримка ІТ-відділу: надання офіційних інструкцій щодо безпечної роботи, оперативне реагування на повідомлення про інциденти.

Адаптація до умов воєнного часу: підготовка до втрати зв'язку: попереднє завантаження лекцій, інструкцій, завдань; альтернативні канали комунікації: резервні чати у Signal, офлайн-доступ до Google Docs; підготовка інформаційних матеріалів про безпечну поведінку для студентів.

Інформаційна безпека викладача не є справою лише ІТ-фахівців. Це відповідальність кожного освітянина, що потребує не стільки складних знань, скільки щоденної уважності, звички до безпечної поведінки та підтримки з боку колективу. В умовах воєнного стану ці навички перетворюються з рекомендацій на засоби виживання.

Психологічна безпека як частина інформаційної безпеки викладача. У контексті війни поняття інформаційної безпеки набуває глибшого значення, включно не лише з технічним, а й із психологічним компонентом. Викладачі, як лідери освітнього процесу, опиняються під подвійним тиском: з одного боку, цифрові ризики, з іншого – емоційне виснаження, спричинене невизначеністю, інформаційним перевантаженням і постійними загрозами.

Інформаційна втома і когнітивне перевантаження. Війна призвела до безперервного потоку новин, часто тривожного чи суперечливого характеру. Постійне відстеження ситуації сприяє появі таких явищ:

– **інформаційне виснаження** – зниження здатності обробляти й аналізувати інформацію;

– **«інформаційний шум»** – втрата концентрації під час підготовки чи проведення занять;

– **зниження критичності мислення** – підвищена вразливість до дезінформації.

Наприклад: викладач постійно перевіряє стрічку новин, водночас намагаючись готуватися до пари – у результаті зростає тривожність і знижується якість роботи.

Емоційні атаки в інформаційному середовищі. Інформаційна війна часто має на меті **викликати емоційну реакцію** – страх, гнів, розгубленість. Педагоги можуть ставати об'єктами: публічних обговорень чи осуду в соцмережах; інформаційних провокацій; персональних атак через фейкові профілі. Такі ситуації не лише дестабілізують психологічний стан, а й знижують готовність до конструктивної професійної комунікації.

Стрес, викликаний інформаційною відповідальністю. Викладач у кризовий період – це не просто фахівець, а людина, яка має утримувати освітній процес, підтримувати студентів, бути джерелом стабільності. Це породжує відчуття постійного тиску («я не можу дозволити собі помилитися»), втому від високих очікувань, ризик емоційного вигорання.

Стратегії психологічної саморегуляції. Власна інформаційна гігієна: встановити чіткий час для перевірки новин (наприклад, не більше 2–3 разів на день); обирати перевірені джерела, уникати «сенсацій» та емоційних заголовків; дотримуватися принципу «менше – краще» щодо інформаційного шуму.

Підтримка з боку колег і середовища: внутрішні спільноти викладачів, групи психологічної підтримки; обговорення викликів у колективі, спільний пошук рішень.

Техніки зняття напруги: дихальні вправи, мікропаузи під час занять; вправи на усвідомлення (grounding), щоденники вдячності; психологічні консультації онлайн – зокрема, через сервіси, які підтримують освітян.

Так, психологічна безпека – це не додатковий, а необхідний компонент інформаційної безпеки в умовах воєнного стану. Емоційна стійкість, здатність протистояти паніці та маніпуляції, критичне мислення – усе це вимагає турботи про себе, підтримки спільноти й практик саморегуляції. [5]

Практичні рекомендації для викладачів в умовах воєнного стану. Щоб ефективно протидіяти інформаційним загрозам у період воєнного стану, викладачам необхідно дотримуватися

базових принципів цифрової гігієни, зберігати емоційну стійкість та впроваджувати прості, але надійні захисні практики. Серед ключових рекомендацій: використання складних паролів і двофакторної автентифікації, уважне ставлення до електронних листів та повідомлень, уникнення сумнівних посилань і файлів, регулярне резервне копіювання навчальних матеріалів.

Також важливо зберігати критичне ставлення до інформації, яку отримуєш чи поширюєш, обмежувати публікацію особистих даних у соцмережах, а також налаштовувати приватність акаунтів. Окрему увагу варто приділяти психологічній саморегуляції: обмеження споживання тривожних новин, створення підтримувального професійного середовища, використання перевірених джерел інформації та, за потреби, звернення до фахових консультантів. Інформаційна обережність і внутрішня стійкість – це не лише захист для себе, а й приклад для студентів.

Висновки. Інформаційна безпека викладача в умовах воєнного стану – це не лише питання технічного захисту акаунтів чи запобігання фішингу. Це багатовимірне явище, що охоплює технічні, поведінкові, психологічні та організаційні аспекти. В умовах гібридної війни викладач стає не лише транслятором знань, а й ціллю для інформаційних атак, носієм критичного мислення та лідером інформаційної стійкості. Проаналізовані загрози – від фішингових листів до дезінформаційних кампаній і емоційних атак – показують, що найефективнішим захистом є поєднання цифрової грамотності, особистої обачності та психологічної зрілості. Освіта потребує не лише модернізації технічних систем, а й формування інформаційної культури, що включає навички критичного аналізу, цифрову етику та вміння діяти в кризових ситуаціях.

У час, коли слово може бути сильнішим за зброю, роль викладача набуває особливої ваги. Тому безпечне освітнє середовище починається з безпеки самого педагога – обізнаного, уважного та стійкого до викликів сьогодення.

Перспективи подальших досліджень. Подальші дослідження доцільно спрямувати на розробку спеціалізованих програм з кібергігієни для викладачів, оцінку ефективності інформаційно-психологічної підтримки в освітньому середовищі та створення інституційних політик безпеки у ЗВО. Також перспективним є вивчення реальних кейсів порушень інформаційної безпеки в освітній сфері, аналіз поведінкових моделей викладачів у кризових ситуаціях та розвиток цифрових інструментів швидкого реагування на загрози. У міждисциплінарному контексті важливо поглибити співпрацю між педагогами, ІТ-фахівцями й психологами для формування стійкого освітнього інформаційного середовища.

References

1. Kovalchuk, I.V. (2020). Informatsiina bezpeka v umovakh hibrydnoi viiny [Information security in conditions of hybrid warfare]. *Naukova dumka.* [in Ukrainian].

2. Petrenko, O.M. (2021). Kiberzahrozy ta zakhyst informatsii v osvitnomu seredovyshchi [Cyber threats and information protection in the educational environment]. *Journal "Education and Security", 3(12),* 45–52 [in Ukrainian].

3. Brown, A. (2020). The Role of Educators in Combating Disinformation. *International Journal of Education, 8(1),* 15–22.

4. Johnson, L., & Wang, M. (2021). Protecting Personal Data in the Digital Age. *Information Security Journal, 10(2),* 89–95.

5. Smith, J. (2022). Cybersecurity in Higher Education: Challenges and Solutions. *Journal of Educational Technology, 15(4),* 233–240.

Отримано 11.05.2025

Електронна адреса для листування: chornomydz@tdmu.edu.ua