

4. Пелех І. Війна та емоційні переживання вагітних жінок: аспект статі. *Вісник Львівського університету. Серія психологічні науки*. 2023. Вип. 18. С. 76–82.

5. Шевчук М. Вплив воєнного стану на психологічний стан та репродуктивні установки жінок. *Особистість і суспільство: психосоціальні виміри ковітальної взаємодії*: матеріали IV Всеукр. науково-практ. конф. молодих вчених (Тернопіль, 30 квітня 2026 року). Тернопіль, 2026. С. 612-614.

DOI <https://doi.org/10.36059/978-966-397-651-8-14>

ІНСТРУМЕНТИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ, КІБЕРБЕЗПЕКА ТА ЗАХИСТ ДАНИХ В ОСВІТНЬОМУ ПРОЦЕСІ В УМОВАХ ВОЄННОГО СТАНУ

Вейландє Лілія Вольдемар-Вікторівна

кандидат педагогічних наук, доцент,

завідувач кафедри педагогічної освіти та соціальної реабілітації

Одеський національний університет імені І.І. Мечникова

м. Одеса, Україна

Повномасштабна військова агресія проти України кардинально змінила архітектуру вітчизняного освітнього простору, створивши безпрецедентні виклики для всіх його суб'єктів. Постійні безпекові загрози, повітряні тривоги та руйнування інфраструктури зробили вимушений перехід до масового дистанційного та змішаного навчання єдиним дієвим механізмом збереження безперервності здобуття освіти. Утім, стрімка цифровізація навчального процесу в умовах воєнного стану викрила гостру суперечність між необхідністю оперативної організації онлайн-взаємодії та забезпеченням належного рівня безпеки інформаційного середовища. Освітній сектор перетворився на одну з мішеней ворожих кібератак, де цілеспрямований деструктивний вплив спрямований не лише на дестабілізацію роботи цифрових інфраструктури навчальних закладів, а й на незаконний доступ до персональних даних учнів, студентів та педагогів. Гострота цієї проблеми зумовлена необхідністю одночасного вирішення двох складних завдань: з одного боку, збереження високої якості та доступності освітніх послуг за умов нестабільного зв'язку та блекаутів, а з іншого – побудови надійного контуру кіберзахисту для запобігання витоку чутливої інформації та несанкціонованого втручання в освітній

процес. процесу. Також, практична реалізація дистанційного та змішаного навчання під час війни вимагає фундаментального перегляду традиційних підходів до організації освітнього процесу. Ключовим фактором стійкості закладів освіти стала стандартизація цифрового інструментарію через розгортання та активне використання сучасних систем управління навчанням (LMS). Платформи на кшталт Google Workspace for Education, Microsoft Teams та Moodle забезпечують єдине безпечне цифрове середовище, де структуровано зберігаються навчальні матеріали, фіксується відвідуваність та здійснюється перевірка знань. Синхронний формат взаємодії, реалізований через відеоконференції, є критично важливим для підтримання живого емоційного контакту, проте в умовах воєнного стану він виявився досить вразливим.

Постійні загрози блекаутів, пошкодження критичної інфраструктури та нестабільний інтернет-зв'язок змусили освітян змістити фокус у бік асинхронного навчання та гнучких освітніх траєкторій. Практична адаптація до цих умов полягає у формуванні автономного освітнього контенту, який здобувачі освіти можуть завантажити заздалегідь та опрацювати за відсутності мережі. Педагоги все частіше відходять від громіздких текстових лекцій на користь коротривалих аудіопояснень (подкастів), конспективно структурованих інфографік, інтерактивних PDF-документів та стислих відеорозборів складної тематики. Такий підхід гарантує рівний доступ до знань для всіх студентів та учнів, незалежно від їхнього поточного географічного розташування чи локальних аварійних відключень електроенергії.

Оновлені умови життєдіяльності висунули нові вимоги й до цифрової дидактики. Класична академічна лекція у форматі монологу в режимі онлайн остаточно втратила свою ефективність, оскільки за умов загального стресу здобувачам освіти важко утримувати тривалу концентрацію. На перший план вийшов метод «перевернутого класу», за якого базовий теоретичний матеріал засвоюється самостійно в асинхронному режимі, а короткі синхронні зустрічі присвячуються виключно дискусіям, розв'язанню практичних кейсів та відповідям на запитання. Паралельно активно впроваджуються концепції мікронавчання, що передбачають розбиття навчального матеріалу на невеликі, логічно завершені блоки тривалістю 5–10 хвилин. Для підтримання згасаючої мотивації та емоційного залучення учасників процесу педагоги застосовують елементи гейміфікації, формувальне оцінювання через швидкі інтерактивні опитування та інструменти сумісної роботи у реальному часі. Цифрова дидактика воєнного часу орієнтується не на формальне відпрацювання годин, а на гнучкість, точкову практичну цінність та збереження психологічного ресурсу здобувачів освіти.

Перехід освітніх закладів у онлайн-простір в умовах воєнного стану зробив їх вразливою ціллю для системних кібератак. Специфіка загроз для освітнього сектору під час війни має як деструктивно-пропагандистський, так і шпигунський характер. Найбільш поширеними залишаються масові фішингові розсилки, спрямовані на заволодіння обліковими записами викладачів та адміністраторів, DDoS-атаки на сервери університетів та цифрові журнали, а також випадки стороннього втручання в онлайн-уроки («Zoom-бомбінг») з метою зриву навчального процесу та поширення ворожого контенту. Особливу небезпеку становить витік геопросторових даних навчальних закладів, а також персональної інформації про місця перебування, контакти та графіки здобувачів освіти і педагогів, що в умовах активних бойових дій створює пряму фізичну загрозу життям людей.

Забезпечення захисту цифрового освітнього середовища вимагає суворого дотримання Закону України «Про захист персональних даних» та стандартів інформаційної безпеки, а також впровадження чітких технічних регламентів на рівні кожного навчального закладу. Для мінімізації кіберризиків та захисту цифрової інфраструктури закладам освіти необхідно впроваджувати комплекс взаємопов'язаних практичних заходів. Насамперед це стосується впровадження суворої політики автентифікації, що передбачає обов'язкове включення двофакторної автентифікації для всіх корпоративних акаунтів та чітке розмежування прав доступу між студентами, викладачами й адміністраторами. Паралельно має здійснюватися захист мережевих каналів шляхом передачі даних виключно через зашифровані протоколи HTTPS та використання VPN-з'єднань для доступу до внутрішніх баз даних закладу. Особливої уваги потребує безпосередня регламентація проведення синхронних занять. Для запобігання несанкціонованому втручанню варто використовувати закритий доступ до кімнат відеоконференцій за корпоративними акаунтами, застосовувати функцію залу очікування, обмежувати права здобувачів освіти на демонстрацію екрана без дозволу лектора та блокувати вхід після початку уроку. Захист від втрати даних забезпечується регулярним автоматичним резервним копіюванням баз даних LMS, електронних журналів та методичних матеріалів на безпечні хмарні сховища або відокремлені сервери. Наостанок, критично важливим є жорстке обмеження публікації чутливої інформації, що вимагає вилучення з відкритого доступу списків груп із контактами, місцями проживання чи точними географічними координатами укриттів. Побудова такої багаторівневої системи гарантує збереження критично важливих даних та мінімізує ризики в умовах гібридної агресії.

У критичних умовах сьогодення дотримання правил кібергігієни перетворюється з додаткової цифрової навички на базову елементарну потребу та обов'язковий складник загальної безпеки кожного учасника освітнього процесу. Формування цифрової та кібергігієнічної компетентності педагогів і здобувачів освіти передбачає не лише знання технічних аспектів захисту інформації, а й розвиток критичного мислення, здатності розпізнавати соціальну інженерію, фішингові пастки, психологічні маніпуляції та ворожі дезінформаційні кампанії. Системно відповідальну роль у цьому процесі має відігравати безпосередньо заклад освіти, перетворюючись на осередки формування культури цифрової безпеки. Замість формального ознайомлення з правилами, навчальним закладам необхідно організувати постійно діючу систему підготовки. Вона має включати проведення регулярних коротких інструктажів і практичних тренінгів із кібергігієни для педагогічного колективу та здобувачів освіти, розробку та розповсюдження зрозумілих покрокових інструкцій щодо дій у разі виявлення підозрілої активності чи спроб зламу акаунтів, а також затвердження чітких внутрішніх регламентів використання цифрових сервісів. Запровадження таких комплексних заходів дозволяє мінімізувати ризики людського фактора, який залишається найпоширенішою ланкою у ланцюгу кіберінцидентів, та створює безпечне, свідоме й захищене цифрове освітнє середовище.

Сьогодні цифрова трансформація освітньої сфери в умовах воєнного стану перетворилася з тимчасового вимушеного заходу реагування на кризу на фундаментальну основу дальшої стратегічної модернізації всієї системи освіти України. Головним завданням такої стратегії є реалізації комплексного підходу, який поєднує нормативно-технічні заходи захисту інформації (впровадження двофакторної автентифікації, шифрування каналів зв'язку, регулярне резервне копіювання, обмеження доступу до чутливих геопросторових і персональних даних) із системним підвищенням рівня цифрової та кібергігієнічної компетентності всіх учасників освітнього процесу. Перспективи подальших наукових розробок у цьому напрямі полягають у дослідженні правових та етичних аспектів впровадження інструментів штучного інтелекту в дистанційне навчання, а також у створенні автоматизованих систем моніторингу та швидкого реагування на кіберінциденти в освітньому секторі.

Література

1. Гелеш А.В., Матійців Б.О. Актуальні питання кібербезпеки у професійній освіті: методи захисту інформації. *Академічні візії*. 2025. Вип. 42. С. 1-5. DOI: <https://doi.org/10.5281/zenodo.15376086>

2. Савченко, В., Маклюк О. Кібербезпека як фактор ефективності функціонування закладів вищої освіти. *Економіка та суспільство*. 2025. (60). DOI: <https://doi.org/10.32782/2524-0072/2024-60-24>

3. Швардак М.В. Кібербезпека у цифровому освітньому середовищі. *Науковий журнал Хортицької національної академії. Scientific Journal of Khortytsia National Academy*. 2025. Випуск 1(12). С. 26-33. DOI: <https://doi.org/10.51706/2707-3076-2025-12>

4. Яценко О., Яценко О. Особливості організації захисту інформації в цифровому освітньому середовищі закладу освіти. *Grail of Science*. 2022. (16), С. 206–210. DOI: <https://doi.org/10.36074/grail-of-science.17.06.2022.037>

DOI <https://doi.org/10.36059/978-966-397-651-8-15>

ПРАВОВІ МЕХАНІЗМИ ЗБЕРЕЖЕННЯ НАУКОВОГО ПОТЕНЦІАЛУ ТА АКАДЕМІЧНОЇ СТІЙКОСТІ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Волошанівська Тетяна Володимирівна

*доктор юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін,
Інститут права та безпеки Одеського державного
університету внутрішніх справ
м. Одеса, Україна*

Повномасштабна збройна агресія російської федерації проти України істотно змінила умови функціонування національної системи науки та вищої освіти. Воєнні ризики впливають не лише на матеріальну інфраструктуру закладів вищої освіти і наукових установ, а й на відтворення наукових шкіл, сталість дослідницьких колективів, академічну мобільність, міжнародну кооперацію, можливості проведення експериментальних досліджень та професійні траєкторії молодих учених. За таких обставин збереження наукового потенціалу держави набуває значення самостійного напрямку забезпечення національної стійкості, оскільки здатність суспільства продукувати нові знання, технології та експертні рішення безпосередньо визначає його спроможність протидіяти воєнним загрозам і здійснювати повоєнне відновлення.

Масштаб проблеми підтверджується емпіричними даними. За дослідженням UNESCO 2025 року, понад 40 закладів вищої освіти або