УДК 378.091-043.86:004.05
DOI: 10.24144/2524-0609.2025.56.45-50

**Гайович Євгенія Федорівна**
аспірантка
кафедра загальної педагогіки та педагогіки вищої школи
начальник відділу електронного навчання центру інформаційних технологій
ДВНЗ «Ужгородський національний університет», м.Ужгород, Україна
y.haiovych@uzhnu.edu.ua
http://orcid.org/0009-0008-3855-7476

**Тополянський Сергій Іванович**
старший викладач
кафедра соціології та соціальної роботи
ДВНЗ «Ужгородський національний університет», м.Ужгород, Україна
serhiy.topolyanskyy@uzhnu.edu.ua
http://orcid.org/0000-0002-3033-4015

# КІБЕРБЕЗПЕКА В СИСТЕМІ СУЧАСНОЇ ВИЩОЇ ОСВІТИ: РЕАЛІЇ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОГО РОЗВИТКУ

**Анотація.** Актуальність проблеми кібербезпеки в закладах вищої освіти зростає через постійне збільшення кількості атак на освітні мережі та цифрову інфраструктуру освіти. Кіберзлочинність може суттєво впливати на освітній процес, порушуючи роботу навчальних платформ, компрометуючи персональні дані студентів і викладачів, а також створюючи ризики для безпеки інформаційних систем. Метою дослідження є аналіз загроз кіберзлочинності в освіті та розробка пріоритетних заходів для їх запобігання. Методи дослідження включають науковий аналіз та синтез, порівняльний підхід, експертну оцінку, метод моделювання. Результати дослідження демонструють, що ключовими факторами успішного забезпечення кібербезпеки є рівень підготовки учасників освітнього процесу, їхня відповідальність і професійні навички, а також ефективність функціонування освітніх платформ. Запропоновані заходи включають удосконалення політики кіберзахисту, підвищення цифрової грамотності, кіберобізнаності та впровадження національної стратегії кібербезпеки. Реалізація цих заходів сприятиме стабільному функціонуванню закладів вищої освіти та зменшенню ризиків кіберзагроз.

**Ключові слова**: культура кібербезпеки, освітній сектор, кібербезпека, кіберобізнаність.

**Вступ.** Безпека власних інформаційних ресурсів є одним із важливих завдань, що постають перед закладами вищої освіти. Вартим уваги є підвищення рівня загроз у цифровому просторі та поширення кіберзлочинів різних видів. Тут потрібно акцентувати як освітніх послугах у галузі кібергігієни та кібербезпеки, які дозволяє належним чином надавати політика навчальних закладів, так і на здійсненні наукових досліджень.

Для збору даних про поведінку контингенту закладів вищої освіти зловмисниками використовується методологія соціальної інженерії та психології. Використовуючи отриману інформацію, кіберзлочинці отримують можливість проникати до внутрішніх електронних систем вишу, маніпулювати поведінкою користувачів та, як результат, за допомогою шахрайства отримувати доступ до цінних даних інформаційної системи ЗВО.

Маючи на меті протидіяти сьогоднішнім кіберзагрозам, освітні заклади є відповідальними за захист персональних даних абітурієнтів, здобувачів та співробітників установи, академічної інформації, науково-дослідницьких та дослідно-конструкторських розробок, напрацювань. Комплекс заходів, сформований на основі такого підходу, передбачає систематичне оновлення політики безпеки та аналіз архітектури комп'ютерних мереж, поряд із суттєвим обмеженням відкритого доступу до службової інформації, що потенційно можуть стати уразливими пунктами для атак з навколишнього інформаційного середовища.

Важливою складовою інформаційної безпеки є залучення здобувачів освіти і працівників університету до вивчення та практичного освоєння принципів кібергігієни, що дасть змогу мінімізувати ризики виникнення випадків шахрайства, викрадення даних та маніпулювання отриманою інформацією [2, с.48].

Закладам вищої освіти необхідно сформувати дієві механізми кіберзахисту, серед яких двофакторна аутентифікація, шифрування даних, заходи з моніторингу та оперативної ідентифікації підозрілої активності користувачів у мережі. Такий підхід посилить рівень захисту, допоможе адаптувати інформаційну систему до нових кібервикликів. Даний фактор є важливим у динамічному глобалізованому та інформатизованому світі. Реалії інформаційного простору вимагають розробки системи ефективних заходів та методів боротьби із кіберзлочинністю в освітній галузі.

В умовах політико-економічної нестабільності, безпека інформаційних систем та мереж закладів вищої освіти є особливо актуальною і важливою проблемою, вирішення якої є нагальним завданням. Вдосконалення та адаптація нової інформаційної реальності вимагають техніко-технологічні методи захисту від кібератак, які можуть серйозно загрожувати персональним даним студентів і викладачів, а також науковій інформації та адміністративним системам.

Створення інструментів для гнучкого пристосування освітнього процесу до змінних реалій є важливим завданням закладів освітньої сфери, особливо враховуючи дистанційне навчання та широке використання освітніх онлайн-ресурсів. В цьому контексті суттєвого значення набуває навчання студентів та викладачів безпечній взаємодії з інформаційними технологіями. Створення електронних систем для надійної перевірки та контролю за інформаційним трафікком, що забезпечують реалізацію функціонування ЗВО, також постає у вигляді нагальної потреби системи вищої освіти.

**Метою** дослідження є аналіз ключових загроз в результаті кібератак та знаходження можливих рі-

шень проблем, з ними пов'язаних, з урахуванням як національного, так і міжнародного досвіду боротьби із загрозами інформаційному простору освітніх інституцій.

**Методи дослідження.** У дослідженні використано комплексний підхід, що поєднує аналіз та синтез для оцінки кіберзагроз в освітньому середовищі, порівняльний метод для вивчення міжнародного та національного досвіду кібербезпеки, а також експертне оцінювання для визначення ефективності захисних заходів. Метод моделювання застосовано для прогнозування можливих атак і розробки механізмів їх запобігання. Використання цих методів забезпечило комплексне бачення проблеми та дало змогу сформувати практичні рекомендації для підвищення рівня кіберзахисту в освітньому просторі.

**Постановка проблеми в загальному вигляді.** *Сучасна система вищої освіти дедалі більше залежить від цифрових технологій, що впроваджуються в навчальні процеси, адміністративне управління та дослідницьку діяльність. З одного боку, це відкриває можливості для більш ефективної організації навчального процесу, з іншого – створює якісно нові виклики у сфері кібербезпеки. ЗВО стикаються з численними загрозами освітньому процесу: від фішингових атак і витоку особистих даних до викрадення інтелектуальної власності та порушення функціонування електронної платформи освітніх систем.*

*Структура закладів освіти, що формується з професорсько-викладацького та адміністративного контингенту і студентів різних років навчання, ускладнює забезпечення ефективного моніторингу кіберзагроз. Обмеженість матеріальних і нематеріальних ресурсів та недостатнє фінансування заходів кібербезпеки є поширеними проблемами для багатьох закладів освіти.*

*Недостатня увага до кібербезпеки може призвести до серйозних наслідків, серед яких витік персональних даних студентів і викладачів та неналежне функціонування, навіть злам систем дистанційного навчання. Дані загрози у великих системних масштабах можуть призвести до порушень належного функціонування національної освітньої системи.*

**Аналіз досліджень і публікацій.** Окремі фактори впливу на кібербезпеку закладів вищої освіти України та світу були предметом дослідження вітчизняних науковців.

Серед них на особливу увагу заслуговують дослідження В.Бикова та Н.Дементієвської [1], в роботі яких основний акцент дослідження робиться на проблемі безпеки кіберпростору: його аналіз проводиться не лише в розрізі техніко-технологічних аспектів захисту інформації. В комплексному розумінні поняття «кібербезпека», згідно з думками авторів, повинне включати в себе правові, технічно-інформаційні, організаційні та психологічні складові елементи.

У роботі Ю.Білявської [2] здійснено аналіз тенденцій на ринку цифрових технологій, що розглядається у контексті кібербезпеки та необхідності дотримання кібергігієни в управлінні електронними системами.

Наукова публікація О.Литвинова [3] присвячена дослідженню впливу кіберзлочинності на функціонування закладів вищої освіти, в ньому розглянуто можливі шляхи попередження і подолання кібератак. Особливу увагу зосереджено та тому факті, що поряд із численними перевагами використання комп'ютерних технологій, їх широкомасштабне використання також може становити причину додаткових загроз, пов'язаних зі складністю забезпечення безпеки та обслуговування великих обсягів даних.

У роботі І.Татомира [5] показано, яку роль відіграє кібербезпека для протидії фішинговим аферам, що є розповсюдженими в освітній сфері. Визначено та проведено структурне групування мотивів здійснення фішингових атак, а також способів їх виявлення і попередження.

Дослідження О.Трофименко [6] присвячене особливій зацікавленості представників кіберзлочинності до освітнього сектора. На основі проведених досліджень виявлено, що головною причиною цієї тенденції є інформаційні бази навчальних закладів, що мають інформацію про передові дослідження, технологічні інновації та інтелектуальну власність.

В статті Н.Фесьохи [7] на основі результатів теоретичних досліджень запропоновано математичну модель множин для забезпечення захисту інформації з повним перекриттям загроз, що можуть виникати зі сторони кіберзлочинців.

Комплексним розглядом питання кібербезпеки та окремих її аспектів займалися закордонні вчені.

Робота A.Adams [8] висвітлює аналіз використання двох аспектів кібербезпеки: механізмів автентифікації та конфіденційності користувачів освітніх онлайн-платформ. Розглядаються причини труднощів використання освітніх електронних ресурсів в зіткненні культурних традицій між неорієнтованою на користувача перспективою безпеки та інформацією культурного обміну електронними даними у сфері освіти.

D.Geer [9] зосереджує основну увагу дослідження на аспекті концентрації інформаційних ресурсів, що потенційно може створити ефект перерозподілу ризиків між користувачами. Великі операційні системи, платформи, протоколи та організації стають ціллю зловмисної інформаційної діяльності через масштабність власних електронних ресурсів.

Y.Ho [10] в своєму науковому дослідженні проводить дихотомічний аналіз двох типів кібератак: одночасного вторгнень із кількох електронних джерел та кіберзагрози, що надходять з одного інформаційного джерела. В останньому випадку аналіз ускладнюється наявністю лише часткових поведінкових даних зловмисників.

У роботі S.Mello [11] здійснюється дослідження потенційних загроз, що можуть призводити до витоків інформаційних даних про вищу освіту та аналізуються основні фактори, що підвищують рівень вразливості освітніх закладів та установ у цьому аспекті.

Одним зі специфічних аспектів дослідження V.Rakstiņš [12] є фактор іноземного втручання, що потенційно може призвести до несанкціонованого доступу до конфіденційних даних досліджень освітніх установ. Залежність від іноземних цифрових систем посилює ці ризики, включаючи потенційну втрату доступу до результатів проведених наукових досліджень, що тимчасово зберігаються в сторонніх «електронних хмарах».

**Виклад основного матеріалу.** Широка розповсюдженість кіберзлочинності у галузі вищої освіти пояснюється наявністю значних масивів персональних даних учасників освітнього процесу. Додатковим суттєвим фактором також є той факт, що велика кількість ЗВО проводять сучасні наукові дослідження, володіють інноваціями та інтелектуальною власністю, що також є об'єктом пильної уваги зловмисників.

Одним з найважливіших чинників, що впливають на кібербезпеку закладах вищої освіти, є кібератаки (рідше – «інформаційні атаки»), що являють собою [10] цілеспрямовані дії, здатні впливати на складові інформаційного середовища. З метою здійснення такого впливу використовуються апаратно-

програмні засоби, робота яких може призвести до порушення конфіденційності, цілісності та доступності даних.

Кібератаки можуть бути як віддаленими, так і локальними. У випадку здійснення віддаленої кібератаки зловмисник знаходиться за межами зони операційного контролю об'єкта, при локальних кібератаках – перебуває у безпосередньому фізичному контакті з об'єктом.

Наявність достатньо великого обсягу конфіденційної інформації зумовлює критичність інформаційного простору закладів вищої освіти [3, с.17]. До такого типу інформації належать:

– інформація персонального характеру: дані студентів, викладачів, службового персоналу та облік змін в контингенті закладу;

– службові дані та внутрішня документація: директиви, накази, розпорядження, інші нормативні акти, що перебувають в обмеженому доступі;

– інформація фінансового змісту для внутрішнього використання: електронні звіти та ресурси;

– інформація юридичного характеру: судові справи, матеріали розслідування;

– матеріали наукового змісту та освітнього спрямування: інтелектуальна власність, патенти та ліцензії, наукові дослідження, програми навчання, електронні журнали, курси навчальних дисциплін.

Наявність достатньої кількості технічних спеціалістів з кіберзахисту є важливим фактором для належного функціонування вітчизняного освітнього сектора. Причиною браку кваліфікованих кадрів може бути недостатнє фінансування, що може бути виділене на цифрову безпеку установи.

Ротація кадрів, щорічна вступна кампанія, наявність великої кількості взаємопов'язаних комп'ютерних лабораторій, перехід до електронного навчання та онлайн-викладання роблять дані всередині мереж значно більш відкритими для доступу та розпорядження ними. В ряді випадків незахищені електронні пристрої можуть ставати вразливішими для атак кіберзлочинців [1, с.320].

Шкідливе, небезпечне при використанні, програмне забезпечення відкриває повний доступ до операційної системи користувача; надає можливість контролювати його дії; призводити до видалення чи зміни конфіденційних даних. Головні типи кібератак та види прямих загроз, що вони становлять, представлені у Таблиці 1.

Таблиця 1

Типи кібератак та види загроз

| Тип кібератаки | Види загроз, представлених кібератакою певного типу |
|---|---|
| Фішинг (англ. fishing - риболовля) | З метою тиску на користувача використовуються його емоційні слабкості – в першу чергу, імпульсивність та надмірна емоційність. При використанні такого типу кібератаки засобами впливу є електронні листи зі шкідливими посиланнями, додатками чи файлами, SMS-атаки (SMiShing = SMS + fishing), голосові дзвінки (vishing = voice + fishing). |
| SQL-ін'єкція (англ. structured query language – мова структурованого запиту) | Застосування команд структурованого запиту (SQL) з метою впливу на базу даних сервера, що може дати доступ до чутливих даних або дозволити використання шкідливого коду програми. |
| XSS-атака (англ. cross-site scripting – міжсайтовий скриптинг) | Використання вразливих місць електронного джерела (сайту, серверу) з метою здійснення кібернападу на конкретний об'єкт. В процесі атаки на вебсторінки, які, ймовірно, відвідає об'єкт атаки, може бути інтегрований шкідливий код,. Такий алгоритм надає кіберзлочинцю доступ до авторизаційних параметрів, куки (англ. cookies - печиво) жертви. Вони використовуються для обходу захисту облікового запису, отримання несанкціонованого доступу до системи в цілому або необхідної інформації. |
| DoS-атака (англ. disk operating system – дискова операційна система) (відмова в обслуговуванні) | Метою дії такої кібер-атаки є вичерпання оперативної пам'яті та ресурсів процесора сервера. В результаті користувачі втрачають доступ до необхідного електронного ресурсу. Реалізація відбувається за допомогою перевантаженні цільової системи, при одночасному підключенні численні пристроїв-ботів |
| MITM-атака (англ. man in the middle – людина посередині, посередник) | Ситуацію, за якої криптоаналітик (атакувальник) має вільний доступ до матеріалу, його читання та видозміни повідомлень, якими обмінюються кореспонденти, причому жоден з останніх не може запідозрити про його присутність в каналі |
| Атака нульового дня (англ. zero-day attack) | Використання недоліків апаратно-програмного забезпечення, невідомих розробникам або користувачам. Цей факт дає можливість використовувати вразливості системи з власною метою до моменту їх виправлення. Наслідками кібератак такого типу є порушення конфіденційності користувачів, цілісності або загальної доступності інформаційного ресурсу. |
| Бекдори (англ. back door – чорний хід, задні двері) | Дефект алгоритму захисту системи, що може бути вмонтований до неї розробником чи зловмисником з метою подальшого вільного доступу до інформації користувачів. |

Джерело: складено автором на основі [5; 6]

Аналіз досліджень [12, с.77] продемонстрував, що найбільш розповсюдженими кібератаками на освітні ресурси навчальних закладів є атаки типу DoS. При їх здійсненні виникає порушення налагодженого навчального процесу та ускладнюється доступ до вільних електронних систем. Даний факт

продемонстрував, що кіберзагрози є реальною та необхідною для вирішення проблемою освітньо-наукової, організаційної діяльності закладів вищої освіти.

З початком воєнного стану заклади освіти часто стають мішенню фішингових атак через низьку кіберкультуру та недостатню кіберобізнаність студентів і викладачів. Брак знань про базові принципи безпеки, довіра до підозрілих листів і відсутність двофакторної автентифікації роблять освітні установи вразливими до кібершахрайства. Фішингові атаки можуть призводити до викрадення облікових даних, зламу корпоративних систем, витоку персональних даних і навіть блокування доступу до навчальних платформ. Без належної освіти в сфері кібербезпеки користувачі часто стають жертвами маніпуляцій, що ставить під загрозу не лише їхні особисті дані, а й роботу всієї установи. Підвищення рівня кіберобізнаності через тренінги, розробку внутрішніх політик безпеки та регулярне тестування на стійкість до атак є ключовими кроками для зниження ризиків.

Апаратна частина інформаційно-комунікаційного технологічного блоку та програмне забезпечення, що функціонує на даному матеріально-технічному базисі, нерозривно пов'язані між собою та утворюють єдину цілісну функціональну систему. Недостатність фінансування інфраструктури для розвитку власних розробок ускладнює створення конкурентоспроможних українських продуктів. В результаті такої невідповідності між можливостями промислових, інженерно-технічних потужностей та потребами освітнього сектору, виникає необхідність отримання програмних та апаратних засобів закордонного виробництва через відсутність вітчизняних необхідних аналогів.

Суттєвою відмінністю в обробці, зберіганні та розпорядженні інформацією між Україною та переважною більшістю розвинених країн світу є уніфікована база даних: Єдина державна електронна база з питань освіти [4] – автоматизована система збирання, сертифікації, оброблення, зберігання та захисту даних, у тому числі персональних, щодо надавачів та отримувачів освітніх послуг в Україні.

Більшість закладів вищої освіти не змінює (або змінює дуже незначною мірою) власну стратегію щодо кіберзахисту навіть після зламу інформаційної системи [9, с.11]. В результаті навіть при наявності у відкритому доступі ефективних засобів захисту від кібератак, інформаційна платформа навчального закладу може постраждати при повторних процедурах зламу.

Даний парадокс ставлення освітніх закладів до питання власної кіберзахищеності пояснюється тим, що незважаючи на тотальне зростання кількості засобів захисту від кіберзагроз, відбувається нехтування можливостями застосування нових заходів кіберзахисту при реалізації власної кіберполітики. Пояснення парадоксу полягає в наявності значного інформаційного поля, що складається зі «справжньої» інформації (несе в собі корисне змістове навантаження) та «інформаційного баласту» (може мати нейтральний чи шкідливий вплив). В результаті виявити, що справді є корисним для власної освітньої діяльності в інформаційному просторі, є складним, іноді неможливим, завданням.

Використання різноманітних технологій, навчання користувачів і підтримка спеціальних служб є складовими елементами ефективної системи захисту електронних ресурсів від кібератак (Таблиця 2). Використовуючи такий підхід до вирішення проблеми кіберзахисту можливо захистити інформацію від кіберзагроз та впровадити високий рівень безпеки даних.

Таблиця 2

Види механізмів захисту від кібератак та принципи їх дії

| Тип захисту від кібератаки | Суть механізму дії захисту |
|---|---|
| Багатофакторна автентифікація | Для захисту користувача вимагається використання кількох етапів автентифікації: пароль та додатковий код, який надіслано на мобільний телефон чи електронну пошту. |
| Криптографія (грец. κρυπτός – прихований і gráphein – писати) | Захист конфіденційності даних здійснюється за допомогою шифрування, що використовуються при перебуванні їх в дорозі від відправника до адресата та в сховищі даних. |
| Файрволи (англ. fire wall – вогняна стіна) | Перевірка і фільтрація вхідного і вихідного трафіку здійснюється за допомогою спеціально створених програмних та / або апаратних пристроїв, комп'ютерної мережі, налаштовується блокування доступу до певних сайтів або додатків |
| Оновлення безпеки | Використання патчів (англ. patch – пластир) безпеки дозволяє зменшувати рівень вразливості, що може бути використаний зловмисниками для зламу системи. Оновлення необхідно інсталювати якомога швидше після їх випуску з метою уникнення проникнення в систему заздалегідь розробленими програмами зламу. |
| Моніторинг безпеки | Процес безперервної перевірки електронної мережі та систем на наявність можливих загроз за допомогою спеціалізованих програм і пристроїв для відстеження і виявлення підозрілої діяльності та активності інших користувачів. |

Джерело: складено автором на основі [7]

Однією з основних проблем закладів вищої освіти є низька інформаційна узгодженість роботи навчальних відділів: кожен навчальний відділ або підрозділ часто відповідає за зберігання, обробку та захист виключно своїх даних [8, с.340].

Є принаймні два виміри цієї проблеми: політика та інструкції повинні адекватно описувати належне управління даними для адміністративних завдань та досліджень [11]. Крім того, технічні системи мають бути зручними та масштабованими належним чином захищені для обробки конфіденційних даних.

**Висновки.** Згідно з проведеним аналізом зовнішніх чинників, що впливають на кібербезпеку закладів вищої освіти, можна стверджувати про їх несистемний характер зі сторони самих ЗВО, що не піддаєть-

ся раціональному контролю. У зв'язку з цим виникає необхідність в удосконаленні внутрішніх заходів протидії зовнішнім впливам і забезпеченні ефективності функціонування кіберзахисту університетів та інститутів.

Створення ефективної системи кібербезпеки у закладах вищої освіти має ґрунтуватися на поєднанні між собою інфраструктури кібербезпеки, регулярного навчання та підвищення кваліфікації персоналу, чітко визначеної процедури управління ризиками, інформованості про загрози та належного рівня захищеності інформаційної інфраструктури закладу освіти.

Кібербезпека є невід'ємною складовою інформаційної безпеки закладів вищої освіти, враховуючи повномасштабну цифровізацію процесу навчання та викладання, широку розповсюдженість практики дистанційного навчання та всеосяжність масштабів електронного документообігу всередині інформаційної архітектури освітньої галузі. Не варто нехтувати умовами сьогодення, а саме війна, адже значна кількість атак здійснюється саме країною-агресором.

Неперервне в часі динамічне оновлення програмного забезпечення, що забезпечує освітній процес, має враховуватися закладами вищої освіти при здійсненні власної політики, спрямованої на забезпечення кібербезпеки науково-практичної діяльності. Логічна імплементація стратегії такого типу підвищить загальний рівень кіберзахисту, водночас забезпечуючи швидке та гнучке реагування інформаційної системи на нові загрози, що можуть виникати при неухильному зростанні впливу електронних технологій на процес надання та отримання вищої освіти.

Системно організоване забезпечення інформаційної безпеки, що враховує вплив зовнішніх і внутрішніх чинників діяльності, дозволить закладам вищої освіти значно вдосконалити захист даних та забезпечити власне ефективне функціонування й здійснення координованої співпраці в умовах динамічно змінюваних кіберризиків.

З метою ефективного протистояння глобальним кіберзагрозам та діяльності хакерських груп важливо здійснювати постійний моніторинг міжнародних тенденцій розвитку заходів з кібербезпеки та адаптації інтернальних процедур до нових міжнародних викликів, що формуються сьогоденням. Важливим є оперативно реагувати на поточні загрози, здійснювати прогностичну оцінку потенційних ризиків з метою аналізу ймовірності їх виникнення, запобігання можливим небажаним інцидентам, що можуть негативно вплинути на освітній процес.

Широко застосовуючи комплексний підхід до вирішення питань кібербезпеки, складовими елементами якого виступають техніко-технологічні, організаційно-правові та кадрові заходи, заклади вищої освіти можуть підвищити рівень кіберзахищеності власного інформаційного простору, забезпечити ефективну реалізацію навчального процесу, наукових досліджень та інноваційних впроваджень в умовах реальних та потенційних кіберзагроз.

У перспективи подальших досліджень варто включити низький рівень кіберобізнаності здобувачів освіти, викладачів та адміністративного персоналу. Саме людський фактор залишається головною вразливістю інформаційних систем, тому перспективним напрямом є розробка ефективних програм навчання та підготовки. Дослідження можуть зосереджуватися на таких аспектах, як визначення найефективніших методів підвищення кіберобізнаності в освітніх закладах (ігрові симуляції, онлайн-курси, інтерактивні тренінги), аналіз впливу різних підходів до навчання на здатність учасників освітнього процесу виявляти та запобігати кібератакам, створення спеціалізованих програм для викладачів та ІТ-персоналу щодо реагування на загрози, управління ризиками та впровадження безпекових політик.

Ще одним важливим напрямом є аналіз та впровадження міжнародного досвіду та його адаптація до українських реалій. Багато університетів у світі вже впровадили комплексні стратегії кіберзахисту, що охоплюють як технологічні, так і освітні аспекти. Дослідження в цьому напрямку можуть включати вивчення політик кібербезпеки у провідних університетах світу, оцінку ефективності міжнародних стандартів та програм навчання з кібербезпеки.

Поєднання підвищення рівня кіберобізнаності з адаптацією міжнародного досвіду створить стійку основу для розвитку ефективної системи кіберзахисту у закладах вищої освіти України.

**Конфлікт інтересів.** Автори підтверджують відсутність фінансових, особистих чи інших інтересів, що можуть розглядатися як потенційний конфлікт інтересів щодо публікації цієї статті.
**Фінансування.** Робота виконана за відсутності фінансової підтримки з боку будь-яких організацій.
**Доступність даних.** Це теоретичне дослідження не передбачає використання додаткових наборів даних.
**Використання штучного інтелекту.** Інструменти штучного інтелекту не використовувались при написанні цієї роботи.

## Список використаної літератури

1. Биков В.Ю., Буров О.Ю., Дементієвська Н.П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання.* 2019. Т.70. № 2. С.313–331.
2. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки.* 2022. № 3. С.47–59.
3. Литвинов О., Філіпенко Н., Лукашевич С., Палкова К. Кібербезпека як фактор ефективності закладів вищої освіти. *Пропілеї права та безпеки : наук. журнал.* Національний аерокосмічний університет ім. М.Є.Жуковського «Харківський авіаційний інститут», 2024. № 5. С.15–23.
4. Положення про Єдину державну електронну базу з питань освіти. URL: https://zakon.rada.gov.ua/laws/show/z1132-18#Text (дата звернення: 09.03.2025).
5. Татомир І. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс.* 2020. Вип.1. С.59–67.
6. Трофименко О.Г. Кібербезпека освітнього сектора. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права): у 2 т.: матеріали Міжнар. наук.-практ. конф. (м.Одеса, 17 червня 2022 р.) / за загальною редакцією С.В.Ківалова. Одеса: Видавничий дім «Гельветика», 2022. Т.1. С.698–700.
7. Фесьоха Н.О. Стан та тенденції розвитку кібербезпеки в епоху цифрової трансформації. *Вісник Херсонського національного технічного університету*, 2024. № 2 (89). С.235–241.

8. Adams, A.; Blanford, A. Security and Online Learning: To Protect and Prohibit. In Usability Evaluation Of Online Learning Programs; IGI Global: Hershey, PA, USA, 2003. P.331–359.
9. Geer D., Jardine E., Leverett E. (2020). On market concentration and cybersecurity risk. Journal of Cyber Policy. 2020. № 5. P.1–21.
10. Ho Y., Frinke D., Tobin D. Planning, Petri-Nets and Intrusion Detection. Taylor & Francis, 1998. 324 p.
11. Mello, S. Data Breaches in Higher Education Institutions. In Honors Theses and Capstones; University of New Hampshire: Durham, NH, USA, 2018. 31 p.
12. Rakstiņš V., Palkova K., Juļa L. and Filipenko N. (2024). Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law. 2024. No.1-29. P.75–79.

**References**

1. Bykov, V. Yu., Burov, O. Yu., & Dementiievska, N. P. (2019). Kiberbezpeka v tsyfrovomu navchalnomu seredovyshchi [Cybersecurity in the digital learning environment. Information technologies and learning tools]. *Informatsiini tekhnolohii i zasoby navchannia, 70 (*2), 313–331. [in Ukrainian]
2. Biliavska, Yu., & Shestak, Ya. (2022). Kiberbezpeka ta kiberhihiiena: nova era tsyfrovykh tekhnolohii [Cybersecurity and cyberhygiene: a new era of digital technologies]. *Tovary i rynky, 3,* 47–59. [in Ukrainian]
3. Lytvynov, O., Filipenko, N., Lukashevych, S., & Palkova, K. (2024). Kiberbezpeka yak faktor efektyvnosti zakladiv vyshchoi osvity [Cybersecurity as a factor in the effectiveness of higher education institutions]. *Propilei prava ta bezpeky, 5,* 15–23. [in Ukrainian]
4. Polozhennia pro Yedynu derzhavnu elektronnu bazu z pytan osvity [Regulations on the Unified State Electronic Database on Education]. URL: https://zakon.rada.gov.ua/laws/show/z1132-18#Text [in Ukrainian]
5. Tatomyr, I. (2020). Kiberbezpeka universytetiv yak sposib protydii fishynhovomu shakhraistvu [Cybersecurity of universities as a way to combat phishing fraud]. *Ekonomichnyi dyskurs, 1,* 59–67. [in Ukrainian]
6. Trofymenko, O.H. (2022, June). Kiberbezpeka osvitnoho sektora [Cybersecurity of the educational sector.]. *Proceedings of International conference Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv KhKhI stolittia* [Ukraine's European choice, the development of science and national security in the realities of large-scale military aggression and global challenges of the 21st century] (pp.698–700). Helvetyka. [in Ukrainian]
7. Fesokha, N.O. (2014). Stan ta tendentsii rozvytku kiberbezpeky v epokhu tsyfrovoi transformatsii [and trends in the development of cybersecurity in the era of digital transformation]. *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu, 2* (89), 235–241. [in Ukrainian]
8. Adams, A., & Blanford, A. (2003). Security and Online Learning: To Protect and Prohibit. *In Usability Evaluation Of Online Learning Programs* (pp.331–359). IGI Global: Hershey.
9. Geer D., Jardine E., & Leverett E. (2020). On market concentration and cybersecurity risk. *Journal of Cyber Policy*, 5, 1–21.
10. Ho Y., Frinke D., & Tobin D. (1998). *Planning, Petri-Nets and Intrusion Detection*. Taylor & Francis.
11. Mello, S. (2018). Data Breaches in Higher Education Institutions*.* University of New Hampshire.
12. Rakstiņš V., Palkova K., Juļa L., & Filipenko N. (2024) Improving cybersecurity measures in academic institutions to reduce the risk of foreign influence. *Socrates. Rīga Stradiņš University Faculty of Law Electronic Scientific Journal of Law,* 1-29, 75–79.

Статус статті:
Отримано: 28.03.2025 Прийнято: 30.04.2025 Опубліковано: 05.05.2025

**Haiovych Yevheniia**
PhD Student in Educational, Pedagogical Sciences (Specialty 011)
Department of General Pedagogy and High School Pedagogy
State University «Uzhhorod National University», Uzhhorod, Ukraine

**Topolyanskyy Serhiy**
Senior Lecturer
Department of Sociology and Social Work
State University «Uzhhorod National University», Uzhhorod, Ukraine

## CYBERSECURITY IN THE SYSTEM OF MODERN HIGHER EDUCATION: REALITIES AND PROSPECTS FOR FURTHER DEVELOPMENT

**Abstract.** The relevance of the problem of cybersecurity in higher education institutions is growing due to the constant increase in the number of attacks on educational networks and digital infrastructure. Cybercrime can significantly affect the educational process by disrupting the operation of learning platforms, compromising the personal data of students and teachers, and creating risks to the security of information systems. The purpose of the study is to analyze the threats of cybercrime in education and develop priority measures to prevent them. The research methods include scientific analysis and synthesis, comparative approach, expert evaluation, and modeling. The results of the study demonstrate that the key factors for successful cybersecurity are the level of training of participants in the educational process, their responsibility and professional skills, as well as the efficiency of educational platforms. The proposed measures include improving cybersecurity policy, increasing digital literacy, cyber awareness, and implementing a national cybersecurity strategy. The implementation of these measures will contribute to the stable functioning of higher education institutions and reduce the risks of cyber threats. The prospects for further research include the low level of cyber awareness among students, teachers, and administrative staff. The human factor remains the main vulnerability of information systems, so the development of effective training and education programs is a promising direction. Research can focus on such aspects as determining the most effective methods for increasing cyber awareness in educational institutions (game simulations, online courses, interactive trainings), analyzing the impact of different approaches to learning on the ability of participants in the educational process to detect and prevent cyber attacks, creating specialized programs for teachers and IT personnel on responding to threats, managing risks, and implementing security policies.

**Keywords:** cybersecurity culture, education sector, cybersecurity, cyber awareness.