DOI 10.31392/UDU-nc.series2.2025.24(31).07
УДК: 378.091.21:004.946.5.056

Злагодух Костянтин Олександрович
Аспірант І курсу спеціальності 011 Освітні, педагогічні науки (ІКТ в освіті)
Українського державного університету імені Михайла Драгоманова, м. Київ, Україна
ORCID ID: 0009-0000-2401-2418
k.o.zlahodukh@udu.edu.ua

ФОРМУВАННЯ КІБЕРГІГІЄНИ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ: ОРГАНІЗАЦІЙНО-ПЕДАГОГІЧНІ ПІДХОДИ ТА ПРАКТИЧНІ СТРАТЕГІЇ

Анотація. Стаття присвячена аналізу організаційно-педагогічних засад формування кібергігієни у закладах вищої освіти (ЗВО) в умовах зростання кіберзагроз. Актуальність зумовлена інтенсивною цифровізацією освіти, що супроводжується поширенням кіберінцидентів, таких як фішинг, витік даних і атаки на інформаційні системи ЗВО. Метою є розроблення концептуальних підходів до формування кібергігієни з урахуванням організаційних і педагогічних чинників для забезпечення безпечного цифрового середовища. Дослідження базується на змішаній методології, що включає якісні методи та кількісні. Проаналізовано теоретичні основи кібергігієни, зокрема психологічні та поведінкові аспекти, такі як когнітивні упередження та недооцінка ризиків, що підвищують вразливість до кіберзагроз. Вивчено сучасний стан впровадження кібергігієни в ЗВО України, де брак ресурсів, фрагментарність нормативної бази та низька мотивація учасників освітнього процесу ускладнюють системний підхід. Проведено порівняння з зарубіжним досвідом, зокрема пострадянськими країнами, як-от Естонія, де кібергігієна інтегрована через державно-приватне партнерство, та країнами ЄС і США. Запропоновано практичні стратегії: організаційні заходи, педагогічні підходи, співпраця з ІТ-компаніями для доступу до сучасних інструментів і проведення інформаційних кампаній для підвищення обізнаності. Розроблено поетапну модель формування кібергігієни: оцінка потреб, створення адаптованих матеріалів, навчання студентів, викладачів і персоналу, моніторинг ефективності. Результати можуть бути використані для розроблення навчальних програм, методичних рекомендацій і нормативних документів, що підвищать кібербезпеку в освіті. Перспективи подальших досліджень – емпірична перевірка стратегій у ЗВО України, оцінка їх впливу на безпеку освітнього процесу та масштабування моделі на інші рівні освіти, зокрема середню. Стаття наголошує на необхідності міждисциплінарного підходу, що поєднує організаційні, педагогічні та технологічні аспекти.

Ключові слова: кібергігієна, кібербезпека, вища освіта, педагогічні стратегії, організаційні заходи, гейміфікація, цифрова грамотність

Вступ. Сучасний етап розвитку суспільства вирізняється інтенсивною цифровізацією всіх сфер життєдіяльності, серед яких освіта посідає особливе місце. Заклади вищої освіти дедалі активніше інтегрують інформаційно-комунікаційні технології (ІКТ) у свої процеси – від впровадження платформ дистанційного навчання до використання хмарних сервісів для зберігання й опрацювання даних. Застосування ІКТ відкриває значні перспективи для підвищення якості освітнього процесу, зокрема через забезпечення гнучкості та доступності навчальних ресурсів. Проте водночас це породжує суттєві виклики, пов’язані з кіберзагрозами. Зокрема, за даними Державної служби спеціального зв’язку та захисту інформації України [1], в країні спостерігається щорічне зростання кількості кіберінцидентів, таких як фішингові атаки, компрометація персональних даних і поширення шкідливого програмного забезпечення. У контексті вищої освіти ці загрози набувають особливої гостроти, оскільки вразливість окремого учасника освітнього процесу може спричинити порушення функціонування цілих інформаційних систем – наприклад, електронних журналів чи баз даних студентів.

Одним із ключових бар’єрів на шляху до безпечного використання цифрових технологій у закладах вищої освіти України залишається недостатній рівень кібергігієни серед студентів, викладачів та адміністративного персоналу. Під кібергігієною в цьому дослідженні розуміється комплекс знань і практичних навичок, спрямованих на безпечне поводження з ІКТ [4]. На жаль, у державних закладах вищої освіти ця проблема часто недооцінюється. Типові прорахунки включають використання слабких паролів, нехтування регулярними оновленнями програмного забезпечення та необережне поводження з електронною поштою,

що створює сприятливі умови для кібератак [6]. Разом із тим системне формування кібергігієни ускладнене відсутністю належно розроблених організаційних механізмів і педагогічних стратегій, адаптованих до специфіки вищої освіти. Як зазначають дослідники, освіта є стратегічно важливою сферою для впровадження принципів кібербезпеки, адже саме тут закладаються основи професійної компетентності майбутніх фахівців, які працюватимуть у цифровому середовищі [7].

Аналіз останніх досліджень і публікацій. Кібергігієна є складовою цифрової грамотності. NIST акцентує на важливості двофакторної автентифікації та оновлення програмного забезпечення [6], ENISA підкреслює роль людського фактора в кіберінцидентах [4]. В Україні Дія.Освіта пропонує базові курси з кібергігієни [2], але системний підхід до її інтеграції в освітні процеси відсутній. Нерозв'язаним залишається питання адаптації кібергігієни до специфіки вищої освіти.

Метою написання статті є аналіз теоретичних засад і розроблення концептуальних підходів до формування кібергігієни в закладах вищої освіти з урахуванням організаційно-педагогічних чинників. Серед завдань дослідження – огляд наукових джерел з питань кібергігієни, узагальнення зарубіжного досвіду та формулювання практичних пропозицій, які можуть стати основою для подальших емпіричних досліджень. У статті не ставиться за мету презентувати результати власного емпіричного аналізу, а радше виконується роль підготовчого етапу, окреслюючи перспективні напрями для вивчення проблеми. Теоретичне осмислення організаційних і педагогічних аспектів формування кібергігієни сприятиме створенню безпечного цифрового середовища у закладах вищої освіти, що є необхідною умовою їх ефективного функціонування в умовах глобальної цифровізації. У довгостроковій перспективі розроблені концептуальні підходи можуть бути використані для створення навчальних програм і нормативних документів, спрямованих на підвищення рівня кібербезпеки та кібергігієни в академічній спільноті.

Теоретичні основи формування кібергігієни. Формування кібергігієни у закладах вищої освіти становить собою багатогранний процес, що вимагає ретельного аналізу теоретичних засад і їх адаптації до специфіки освітнього середовища. У рамках цього дослідження кібергігієна трактується як сукупність знань, умінь і практичних навичок, спрямованих на забезпечення безпечного та відповідального використання цифрових технологій учасниками освітнього процесу [1]. Цей концепт охоплює захист персональних даних, протидію кіберзагрозам – зокрема фішингу чи шкідливому програмному забезпеченню, – а також дотримання етичних норм у цифровому просторі [4]. У вищій освіті кібергігієна набуває особливого значення через активне застосування онлайн-ресурсів, платформ дистанційного навчання та хмарних технологій, що суттєво підвищує вразливість до кіберінцидентів.

Психологічні та поведінкові аспекти кібергігієни. Формування кібергігієни в ЗВО вимагає врахування психологічних і поведінкових факторів, які впливають на сприйнятливість учасників освітнього процесу до кіберзагроз. Згідно з ENISA, когнітивні упередження, такі як надмірна впевненість у власній безпеці чи недооцінка ризиків, часто призводять до помилок, як-от відкриття фішингових листів чи використання слабких паролів [4]. Наприклад, студенти можуть ігнорувати попередження про оновлення програмного забезпечення через брак часу чи хибне відчуття безпеки. Соціальна інженерія, яка використовує психологічні маніпуляції, експлуатує довіру до офіційних джерел чи бажання швидко вирішити проблему, що особливо небезпечно в академічному середовищі [10]. Дослідження Furnell та Vasileiou підкреслює, що низька обізнаність про кіберзагрози часто поєднується з браком критичного мислення, що робить студентів і викладачів вразливими до атак [11]. Інтеграція кібергігієни в рамки цифрової грамотності передбачає використання освітніх моделей, орієнтованих на мотивацію. Модель самоспрямованого навчання Knowles наголошує на важливості внутрішньої мотивації дорослих, що актуально для студентів ЗВО [5]. Навчальні програми з кібергігієни мають демонструвати практичну користь, наприклад, захист особистих даних чи уникнення фінансових втрат. Такий підхід сприяє формуванню стійкої поведінки, спрямованої на

безпечне використання ІКТ, і підвищує ефективність навчання. Наприклад, програми, які підкреслюють зв'язок між кібергігієною та кар'єрними перспективами, можуть мотивувати студентів до активного освоєння цих навичок.

Організаційні аспекти формування кібергігієни потребують системного підходу, який інтегрує управлінські, технічні та нормативні складові. Ключову роль тут відіграє адміністрація закладів вищої освіти, на яку покладається відповідальність за розроблення внутрішніх політик і процедур, що гарантують безпечне функціонування інформаційно-технічної інфраструктури. Наприклад, зарубіжні джерела, такі як NIST, акцентують на доцільності впровадження двофакторної автентифікації та регулярного оновлення програмного забезпечення як базових захисних заходів. В Україні ці практики лише починають набувати обрисів: у стратегічних документах Міністерства освіти і науки України [3] підкреслюється важливість розвитку цифрових компетентностей, однак конкретні кроки до інтеграції кібергігієни в управлінські механізми ЗВО залишаються фрагментарними. Зарубіжний досвід – зокрема співпраця фінських університетів із агентствами кібербезпеки [4] – переконливо демонструє, що організаційна підтримка є визначальною умовою для системного впровадження кібергігієнічних практик.

Педагогічні підходи до формування кібергігієни ґрунтуються на принципах андрагогіки, які враховують особливості навчання дорослої аудиторії [5]. Оскільки студенти закладів вищої освіти уже володіють певним рівнем самостійності, навчання кібергігієні має бути орієнтованим на практичні результати та внутрішню мотивацію. У цьому контексті оптимальним є компетентнісний підхід, використання якого передбачає розвиток не лише теоретичних знань, а й конкретних навичок – наприклад, уміння розпізнавати фішингові атаки чи створювати надійні паролі [2]. Ефективність такого підходу посилюється за умови використання інтерактивних методів, таких як симуляції кіберінцидентів чи аналіз реальних прикладів, що сприяють кращому засвоєнню матеріалу [7]. Водночас важливо заохочувати самонавчання, адже стрімка еволюція кіберзагроз вимагає від учасників освітнього процесу постійного вдосконалення своїх знань.

Аналіз наукових джерел засвідчує, що кібергігієна є складовою ширшої концепції цифрової грамотності, яка дедалі частіше розглядається як невід'ємна частина сучасної освіти. Прикладом може слугувати британська програма "Cyber Essentials" [8], адаптована для закладів освіти і збагачена модулями з кібергігієни, що потенційно могло б стати орієнтиром для України. Натомість в українському контексті проблема нерідко сприймається як суто технічна, а не педагогічна, що суттєво звужує можливості її комплексного вирішення [2]. Порівняльний аналіз зарубіжного та вітчизняного досвіду виокремлює прогалини в нормативному регулюванні та педагогічній підготовці, які потребують подальшого теоретичного осмислення.

Теоретичні засади формування кібергігієни у вищій освіті синтезують організаційні механізми (нормативна база, інфраструктурне забезпечення) та педагогічні стратегії (компетентнісний підхід, інтерактивність). Такий синтез створює концептуальну основу для розроблення практичних підходів, адаптованих до українських реалій. У перспективі доцільним буде емпіричне тестування запропонованих ідей у конкретних закладах освіти для оцінювання їх ефективності та практичної цінності.

Методологічні підходи. Дослідження організаційно-педагогічних засад формування кібергігієни у закладах вищої освіти вимагає ретельно продуманих методологічних підходів, які б ураховували як теоретичні аспекти, так і практичні потреби всіх, хто залучений до освітнього процесу. Оскільки кібергігієна є міждисциплінарною темою, що перетинає кібербезпеку, педагогіку та організаційний менеджмент, доцільним є поєднання якісних і кількісних методів. Використання такого підходу дає змогу охопити як об'єктивні показники – скажімо, рівень знань про кіберзагрози, – так і суб'єктивні оцінки, наприклад, як студенти чи викладачі ставляться до навчання кібергігієни. Це цілком узгоджується з принципами андрагогіки, де акцент робиться на практичній користі та внутрішній мотивації [5].

Серед методів, які видаються перспективними, варто виокремити анкетування. Воно могло б стати інструментом для оцінювання базових кібергігієнічних компетентностей студентів, викладачів і працівників адміністрації. Анкети, наприклад, могли б містити запитання про те, як часто люди користуються цифровими інструментами, чи знають вони, як створювати надійні паролі, чи вміють розпізнавати фішингові атаки, а також чи готові вчитися чомусь новому в цій сфері. Для аналізу даних доцільно залучити статистичні програми, такі як PSPP або R (з RStudio), які допомогли б простежити зв'язки між рівнем обізнаності та такими факторами, як вік, спеціальність чи досвід роботи з інформаційними технологіями [7]. Це дало б змогу висунути припущення про те, що саме впливає на формування кібергігієни.

Для поглибленого вивчення кібергігієни доцільно використовувати змішаний методологічний підхід, який поєднує кількісні та якісні методи. Анкетування може базуватися на структурованій анкеті, що включає питання про частоту використання двофакторної автентифікації, розпізнавання фішингових листів та готовність до навчання. Наприклад, анкета може містити запитання: "Чи оновлюєте ви паролі щоквартально?" або "Чи можете ви відрізнити фішинговий лист від легітимного?". Для аналізу даних пропонується застосовувати регресійний аналіз у програмах, таких як R, щоб виявити кореляції між рівнем кібергігієни та демографічними факторами (вік, спеціальність, досвід) [7]. Додатково перспективним є метод кейс-стаді, який передбачає тестування стратегій у реальних умовах ЗВО. Наприклад, пілотне дослідження в УДУ імені Михайла Драгоманова могло б оцінити ефективність тренінгів із кібергігієни, залучаючи студентів і викладачів різних факультетів. OSCE рекомендує кейс-стаді для аналізу організаційних бар'єрів, таких як брак ресурсів чи недостатня координація, що перешкоджають впровадженню кібербезпеки [7]. Таке дослідження могло б включати впровадження навчального модуля з кібергігієни та оцінку його впливу через повторне анкетування.

Щоб доповнити цифри живою картиною, пропонується звернутися до якісних методів, зокрема глибинних інтерв'ю з адміністрацією та викладачами. Напівструктурований формат таких бесід дозволив би з'ясувати, що заважає на організаційному рівні – чи то брак ресурсів, чи то недостатня підготовка, – а також які педагогічні труднощі виникають, наприклад, чому студенти не завжди "горять" цією темою. Аналіз відповідей можна було б провести через контент-аналіз, як це радять у проєктах OSCE, щоб виокремити основні проблеми й теми, які потребують уваги.

Не менш важливим елементом методології є аналіз нормативної бази та стратегій – приміром, "Концепції розвитку цифрових компетентностей" від Міністерства освіти і науки України [3] чи зарубіжних практик, описаних у звітах ENISA [4]. Це допомогло б зрозуміти, наскільки кібергігієна вже «вплетена» в освітні політики, і підказало, як їх можна вдосконалити. Для порівняння корисним буде звернутися до міжнародного досвіду, наприклад, до рекомендацій NIST щодо оцінювання кіберкомпетентностей в академічному середовищі, що могло б слугувати орієнтиром для наших реалій.

Таким чином, методологічні підходи до вивчення кібергігієни у вищій освіті спираються на комбінацію кількісних методів (анкетування, статистичний аналіз) і якісних технік (інтерв'ю, аналіз документів). Запропонована схема є концептуальною основою, яку ще належить перевірити на практиці в українських закладах вищої освіти. Саме це могло б стати наступним кроком для подальших досліджень.

Сучасний стан кібергігієни у закладах вищої освіти. Сучасний стан кібергігієни у закладах вищої освіти відображає глобальні тенденції цифровізації, які приносять як нові можливості, так і серйозні виклики. В українському контексті ця проблема набуває особливої гостроти через стрімке зростання кіберзагроз і недостатню підготовленість освітніх інституцій до їхнього подолання. Зокрема, за даними Державної служби спеціального зв'язку та захисту інформації України [1], у 2022 році зафіксовано понад 2,5 тисячі кіберінцидентів, значна частка яких зачепила державні установи, включно з освітніми. Такі загрози, як фішинг, витік даних чи атаки на платформи дистанційного навчання, стають дедалі частішими, що лише

підкреслює необхідність системного формування кібергігієни серед усіх учасників освітнього процесу.

На міжнародному рівні дослідження вказують на те, що кібергігієна в закладах освіти залишається слабким місцем. Наприклад, звіт ENISA [4] наголошує, що близько 60% кіберінцидентів у європейських університетах пов'язані з людським фактором – необізнаністю чи необережністю користувачів. Типові помилки, такі як слабкі паролі, ігнорування оновлень програмного забезпечення чи незнання основ соціальної інженерії, зокрема фішингових атак, лише погіршують ситуацію [6]. Ці спостереження переконують мене в тому, що кібергігієна – це не лише технічне питання, а й педагогічна проблема, яка вимагає комплексного підходу до навчання та підвищення свідомості.

В Україні ситуація ускладнена кількома специфічними чинниками. По-перше, брак ресурсів суттєво обмежує можливості ЗВО для впровадження сучасних систем захисту чи регулярних тренінгів. Як зазначають у Дія.Освіта [2], лише незначна частина студентів і викладачів проходить базове навчання з кібергігієни, яке зазвичай зводиться до разових акцій. По-друге, нормативна база, зокрема "Концепція розвитку цифрових компетентностей" від Міністерства освіти і науки України [3], декларує важливість цифрової грамотності, але, на жаль, не пропонує конкретних механізмів для інтеграції кібергігієни в освіту. Це різко контрастує з зарубіжними підходами, де такі питання детально прописані – наприклад, у британській програмі "Cyber Essentials" [8], яка встановлює чіткі стандарти для закладів освіти, включно з тренінгами та сертифікацією.

Порівняльний аналіз з іншими пострадянськими країнами, зокрема Естонією, демонструє суттєві відмінності. Естонія, відома своєю розвинутою кібербезпековою інфраструктурою, інтегрує кібергігієну в освітні програми через державно-приватне партнерство, що забезпечує доступ до сучасних ресурсів і експертизи [4]. Наприклад, естонські університети співпрацюють із національним центром кібербезпеки для розробки навчальних модулів і проведення тренінгів. В Україні такі ініціативи обмежені через брак фінансування та координації. Геополітичні фактори, зокрема зростання кібератак в умовах війни, додатково ускладнюють ситуацію. За даними Держспецзв'язку, у 2022 році освітні установи стали мішенню цілеспрямованих атак, таких як витік даних студентів чи компрометація платформ дистанційного навчання [1]. Це підкреслює нагальну потребу в посиленні кібергігієнічних практик у ЗВО України для захисту інформаційної інфраструктури.

Організаційні перешкоди в Україні також пов'язані з недостатньою взаємодією між адміністрацією ЗВО і державними структурами у сфері кібербезпеки. Зарубіжний досвід, як-от співпраця фінських університетів із національними агентствами [4], показує, що партнерство з державою може значно посилити ефективність кібергігієнічних заходів. В Україні подібні ініціативи лише зароджуються, хоча проєкти на кшталт "Посилення спроможностей у сфері кібергігієни" від OSCE дають надію на поступовий прогрес [7].

Педагогічні труднощі, у свою чергу, зумовлені низькою мотивацією студентів і викладачів до освоєння кібергігієни. Як зазначають експерти, багато хто сприймає кібербезпеку як суто технічну сферу, що не стосується їхньої основної роботи чи навчання [2]. Це підтверджують і міжнародні джерела: NIST підкреслює, що без педагогічної підтримки навіть найкращі технічні рішення втрачають ефективність [6]. У США, наприклад, цю проблему вирішують через інтеграцію кібергігієни в навчальні плани – від окремих курсів до коротких модулів у межах інших дисциплін. В Україні такі практики поки рідкість, хоча окремі ЗВО, як-от Київський політехнічний інститут, уже роблять перші кроки, пропонуючи факультативні заняття з кібербезпеки, а УДУ імені Михайла Драгоманова співпрацюють з Кіберполіцією та проводять зустрічі-лекції з кібергігієни для бажаючих учасників освітнього процесу.

Позитивні зрушення в Україні все ж помітні. Інформаційні кампанії, як-от "Місяць кібербезпеки" [1], спрямовані на підвищення обізнаності, показують, що залучити студентів і викладачів можливо. Проте ці заходи мають епізодичний характер і не забезпечують системності. Порівняння з американськими програмами, такими як "Cybersecurity Awareness

Training" [6], лише підкреслює потребу в більш структурованому підході, який би поєднував організаційні та педагогічні зусилля.

Отже, сучасний стан кібергігієни у закладах вищої освіти в Україні характеризується низкою проблем – від недостатньої обізнаності й обмежених ресурсів до браку педагогічних стратегій. Водночас аналіз літератури та зарубіжного досвіду відкриває перспективи для вдосконалення, які потребують подальшого теоретичного осмислення й емпіричної перевірки в наших умовах.

Практичні стратегії формування кібергігієни. Формування кібергігієни у закладах вищої освіти вимагає розробки практичних стратегій, які б гармонійно поєднували організаційні заходи та педагогічні підходи. Оскільки емпіричні дані для оцінки їхньої дієвості в українських умовах поки відсутні, ці стратегії мають концептуальний характер і спираються на аналіз літератури, зарубіжний досвід та логічні міркування. Їхньою основною метою є створення безпечного цифрового середовища у ЗВО, підвищення обізнаності учасників освітнього процесу та формування у них стійких навичок протидії кіберзагрозам.

Організаційні заходи. На організаційному рівні доцільно зосередитися на системному підході до впровадження кібергігієни в діяльність закладів вищої освіти. Першим кроком могло б стати розроблення внутрішніх політик кібербезпеки, які б чітко регулювали використання інформаційно-технічних ресурсів. Наприклад, NIST рекомендує застосовувати двофакторну автентифікацію для доступу до електронних систем ЗВО – від журналів до платформ дистанційного навчання. В українських реаліях такі заходи могли б бути оформлені через накази адміністрації та включені до стратегічних планів розвитку закладів, що узгоджується з положеннями "Концепції розвитку цифрових компетентностей" [3].

Другим важливим напрямом є створення у вишах спеціалізованих центрів або груп із кібербезпеки, які б відповідали за координацію навчальних ініціатив, моніторинг загроз і реагування на інциденти. Зарубіжний досвід, зокрема співпраця американських університетів із Національним інститутом стандартів і технологій [6], свідчить, що такі структури значно підвищують ефективність превентивних заходів. В Україні подібне могло б реалізуватися через залучення місцевих ІТ-фахівців і партнерство з державними структурами, як-от Держспецзв’язок [1], який уже пропонує базові навчальні матеріали в рамках "Місяця кібербезпеки".

Педагогічні стратегії. Педагогічні стратегії, враховуючи тематику статті, мають базуватися на принципах андрагогіки, враховуючи мотивацію та практичні потреби дорослої аудиторії [5]. Одним із перспективних рішень є введення модулів із кібергігієни до навчальних програм. У Великій Британії, наприклад, програма "Cyber Essentials" [8] пропонує короткі курси для студентів і викладачів, що охоплюють основи кібербезпеки. В українських ЗВО це могло б втілитися через факультативні заняття або інтеграцію теми в дисципліни, пов’язані з інформаційними технологіями чи професійною етикою.

Інтерактивні тренінги виглядають ще одним дієвим інструментом для підвищення залученості та результативності навчання. Симуляції кібератак – наприклад, фішингових кампаній чи спроб злому паролів – дозволяють учасникам на практиці відпрацьовувати свої дії в умовах загрози. Такі методи успішно застосовуються в програмах OSCE і могли б бути адаптовані для України з використанням доступних онлайн-ресурсів, як-от платформа Дія.Освіта. Додавання гейміфікації, наприклад балів за виконання завдань, могло б додатково стимулювати студентів, особливо враховуючи їхню часто низьку зацікавленість у темі кібербезпеки.

Гейміфікація у навчанні кібергігієни. Для підвищення мотивації студентів доцільно використовувати гейміфікацію. Наприклад, віртуальний "кібер-квест", де учасники розпізнають фішингові листи чи створюють надійні паролі для "проходження рівнів", може зробити навчання цікавим і ефективним. Такі методи, за OSCE, підвищують залученість і сприяють засвоєнню матеріалу [7]. Гейміфікація може бути реалізована через платформи, як-от Дія.Освіта, з елементами змагальності, наприклад, балами за правильні дії. Прикладом

може бути гра, де студенти "розблоковують" рівні, ідентифікуючи підозрілі листи чи налаштовуючи двофакторну автентифікацію, що сприяє практичному закріпленню навичок.

Співпраця з ІТ-компаніями. Партнерство з приватними ІТ-компаніями може значно посилити ресурси ЗВО для впровадження кібергігієни. Фінський досвід показує, що співпраця університетів із технологічними фірмами забезпечує доступ до експертизи та сучасних інструментів [4]. В Україні подібні ініціативи могли б включати залучення компаній до розробки навчальних матеріалів чи проведення тренінгів. Наприклад, партнерство з локальними ІТ-фірмами могло б забезпечити ЗВО безкоштовними ліцензіями на антивірусне ПЗ чи платформи для симуляцій кібератак, що зменшило б фінансове навантаження на заклади.

Не менш важливим є підтримка викладачів. Організація семінарів чи онлайн-курсів із кібергігієни – наприклад, на основі матеріалів Держспецзв'язку – могла б покращити їхню готовність працювати зі студентами. Водночас розробка методичних рекомендацій для «вплетення» (додавання) кібергігієни в різні дисципліни додала б процесу системності. Приклад Фінляндії, де тренінги для викладачів стали основою успіху [4], лише підтверджує, що професійний розвиток педагогів є критично важливим для таких ініціатив.

Кампанії з підвищення обізнаності. Доповнити формальне навчання могли б інформаційні кампанії, орієнтовані на всіх учасників освітнього процесу. Плакати, вебінари чи електронні розсилки з практичними порадами – наприклад, "Як створити надійний пароль" чи "Як розпізнати фішинг" – є простими, але ефективними інструментами. В Україні подібні заходи вже реалізуються в рамках "Місяця кібербезпеки" [1], але їхній потенціал можна розширити на локальний рівень ЗВО, залучаючи студентські організації до створення цікавого й доступного контенту.

Технологічні інструменти для підтримки кібергігієни в ЗВО. У контексті зростання кіберзагроз і активної цифровізації освітнього процесу ЗВО потребують сучасних технологічних інструментів для підтримки формування кібергігієни. Такі інструменти не лише сприяють підвищенню безпеки інформаційних систем, але й відіграють ключову роль у навчанні студентів, викладачів і адміністративного персоналу. Їхнє використання дозволяє автоматизувати певні аспекти кібербезпеки, спрощувати моніторинг загроз і створювати інтерактивне середовище для практичного освоєння кібергігієнічних навичок.

Одним із основних інструментів є програмне забезпечення для симуляції кібератак, яке дозволяє учасникам освітнього процесу відпрацьовувати реакцію на типові загрози, такі як фішинг чи компрометація даних. Наприклад, платформи на кшталт KnowBe4 або Proofpoint, які широко застосовуються в європейських університетах [4], пропонують симуляції фішингових кампаній, де користувачі вчаться розпізнавати підозрілі листи та уникати їхньої взаємодії. В Україні подібні інструменти можуть бути адаптовані через співпрацю з локальними ІТ-компаніями або використання відкритих платформ, таких як Дія.Освіта, яка вже пропонує базові модулі з кібергігієни [2]. Такі симуляції не лише підвищують обізнаність, але й дозволяють оцінити рівень підготовки учасників через аналітику їхніх дій.

Іншим важливим інструментом є системи управління паролями, які допомагають створювати та зберігати надійні паролі. Програми, такі як LastPass або 1Password, рекомендовані NIST [6], можуть бути інтегровані в інформаційні системи ЗВО для забезпечення безпечного доступу до платформ дистанційного навчання чи електронних журналів. В українських реаліях, де ресурси часто обмежені, доцільно використовувати безкоштовні альтернативи, як-от Bitwarden, які пропонують базові функції для створення складних паролів і їх захисту. Впровадження таких інструментів супроводжується навчальними сесіями, де студенти та викладачі ознайомлюються з принципами їхньої роботи, що сприяє формуванню стійких кібергігієнічних звичок.

Апаратні засоби ідентифікації, такі як USB-токени чи смарт-карти, також відіграють важливу роль у забезпеченні кібербезпеки. Згідно з дослідженням Василя Михайловича Франчука [9], такі пристрої забезпечують надійний захист завдяки шифруванню та прив'язці до конкретних робочих станцій, що особливо актуально для адміністративного персоналу

ЗВО, який працює з чутливими даними. Наприклад, використання токенів YubiKey для двофакторної автентифікації може значно знизити ризик несанкціонованого доступу до баз даних студентів чи викладачів. Хоча впровадження таких рішень вимагає початкових інвестицій, їх ефективність виправдовує витрати, особливо в умовах зростання кібератак, зафіксованих Держспецзв'язком [1].

Аналітичні інструменти для моніторингу кіберзагроз також є важливим елементом. Системи на основі штучного інтелекту, такі як Splunk або QRadar, дозволяють ЗВО відстежувати підозрілу активність у реальному часі, наприклад, спроби несанкціонованого доступу до платформ дистанційного навчання. Для українських ЗВО, де бюджет може бути обмеженим, доцільно розглядати відкриті рішення, такі як ELK Stack, які забезпечують базовий аналіз логів і можуть бути адаптовані для потреб вишу. Такі інструменти не лише підвищують безпеку, але й можуть використовуватися в навчальних цілях, дозволяючи студентам технічних спеціальностей аналізувати реальні дані в рамках практичних занять.

Інтеграція технологічних інструментів у навчальний процес також передбачає використання гейміфікованих платформ. Наприклад, платформа Hack The Box, популярна в європейських ЗВО [4], дозволяє студентам у ігровій формі вирішувати задачі з кібербезпеки, такі як захист від атак або аналіз вразливостей. В Україні подібний підхід може бути реалізований через створення локальних гейміфікованих модулів, які інтегруються в навчальні програми. Наприклад, студенти могли б отримувати бали за виконання завдань, таких як правильне налаштування двофакторної автентифікації чи розпізнавання фішингових листів, що мотивувало б їх до активного навчання.

Використання технологічних інструментів потребує координації з організаційними та педагогічними заходами. Наприклад, адміністрація ЗВО має забезпечити технічну підтримку для впровадження програмного забезпечення, а викладачі – інтегрувати ці інструменти в навчальні курси. Зарубіжний досвід, зокрема співпраця фінських університетів із технологічними компаніями [4], показує, що партнерство з IT-сектором може значно полегшити доступ до таких рішень. В Україні подібна співпраця могла б реалізуватися через залучення локальних IT-компаній до надання безкоштовних ліцензій чи консультацій для ЗВО.

Таким чином, технологічні інструменти, такі як симуляційні платформи, менеджери паролів, апаратні засоби ідентифікації та аналітичні системи, створюють міцну основу для підтримки кібергігієни в ЗВО. Їхнє впровадження потребує адаптації до українських реалій, зокрема через використання доступних і відкритих рішень, але може значно підвищити безпеку освітнього середовища та ефективність навчання. Подальші дослідження мають оцінити практичну ефективність таких інструментів у контексті українських ЗВО.

Концептуальна модель. На основі аналізу літератури та зарубіжного досвіду пропонується поетапну модель формування кібергігієни у вищій освіті:

1. *Оцінка потреб*: Визначення поточного рівня обізнаності та виявлення вразливостей через опитування чи тестування.
2. *Розроблення модулів*: Підготовка навчальних матеріалів, адаптованих до специфіки конкретного вишу.
3. *Навчання*: Проведення тренінгів і курсів для студентів і викладачів.
4. *Моніторинг*: Оцінка прогресу через регулярні перевірки та зворотний зв'язок. Ця модель спирається на рекомендації OSCE [7], і має гіпотетичний характер та потребує емпіричної апробації, але вже зараз може слугувати орієнтиром для практичних кроків.

Перспективи реалізації. Використання запропонованої стратегії враховують як глобальні тенденції (інтерактивність, системність), так і локальні особливості України (обмежені ресурси, низька мотивація). Їх сильна сторона – у гнучкості: ці підходи можна адаптувати до потреб різних ЗВО залежно від їхнього профілю та можливостей. Проте для остаточного підтвердження їхньої ефективності необхідні подальші дослідження, які б оцінили вплив цих заходів на рівень кібергігієни в реальних умовах українських закладів освіти.

У рамках запропонованої концептуальної моделі формування кібергігієни у закладах вищої освіти ключовими компонентами є розробка навчальних модулів і організація навчання. Розробка модулів передбачає створення адаптованих навчальних матеріалів, які відповідають специфіці вишу та сучасним викликам кібербезпеки. Окрім базового змісту, рекомендованого Державною службою спеціального зв'язку та захисту інформації України [1], модулі мають включати теми, присвячені протидії соціальній інженерії, такій як фішинг, що використовує маніпуляції людською психологією для отримання доступу до даних [8]. Студенти повинні ознайомитися з методами перевірки ідентичності запитів і правилами нерозкриття паролів [8]. Також модулі мають охоплювати різні методи ідентифікації користувачів, зокрема апаратну (смарт-карти, USB-токени), біометричну та багатофакторну, з акцентом на створенні надійних паролів через комбінацію букв, цифр і символів [10]. Такі матеріали можуть включати практичні завдання, як-от аналіз підозрілих електронних листів або тестування надійності паролів.

Навчання у межах моделі передбачає проведення тренінгів і курсів, які формують практичні навички кібергігієни. Відповідно до рекомендацій NIST [6], тренінги мають бути інтерактивними, наприклад, через симуляції фішингових атак, що допомагають розпізнавати підозрілі запити на зміну паролів або розкриття даних [8]. Учасники також можуть опановувати використання апаратних засобів ідентифікації, таких як USB-токени, які забезпечують високу надійність завдяки шифруванню та прив'язці до робочих станцій [9]. Для викладачів доцільно організувати заняття з розробки політик безпеки, що включають чіткі інструкції щодо поводження з відвідувачами та захисту паролів як власності організації [8]. Такі тренінги підвищують обізнаність і сприяють формуванню культури кібербезпеки в ЗВО.

Отже, практичні стратегії формування кібергігієни охоплюють організаційні заходи (політики, центри кібербезпеки), педагогічні підходи (модулі, тренінги, підтримка викладачів) і кампанії з підвищення обізнаності. Ці ідеї, підкріплені літературою, створюють концептуальну основу для забезпечення безпечного цифрового середовища у вищій освіті.

Висновки та перспективи подальших досліджень. Проведений аналіз теоретичних засад і сучасного стану кібергігієни у закладах вищої освіти підкреслює її критичну важливість в умовах цифровізації. Зростання кіберзагроз – фішингу, витоку даних, атак на системи дистанційного навчання – свідчить про нагальну потребу в системному підході до розвитку кібергігієнічних компетентностей серед студентів, викладачів і адміністративного персоналу. Теоретичні основи, розглянуті в статті, спираються на поєднання організаційних механізмів (нормативне регулювання, інфраструктура) і педагогічних стратегій (компетентнісний підхід, інтерактивність, гейміфікація), що відповідає принципам андрагогіки та закордонному досвіду [4], [5]. Це створює міцний фундамент для розроблення практичних рішень, адаптованих до потреб вищої освіти.

Сучасний стан кібергігієни, як в Україні, так і глобально, характеризується низкою викликів: недостатньою обізнаністю, обмеженими ресурсами та фрагментарністю нормативного забезпечення [1], [6]. Водночас зарубіжні практики, наприклад "Cyber Essentials" у Великій Британії [8], демонструють переваги системного підходу, який міг би стати прикладом для України. Практичні стратегії, запропоновані в статті, – від внутрішніх політик і центрів кібербезпеки до навчальних модулів, тренінгів і гейміфікації – обґрунтовані літературою [2], [7] і є концептуальними ідеями, які ще потребують емпіричної перевірки.

Значення цього дослідження полягає в тому, що воно окреслює теоретичну базу та практичні напрями для формування кібергігієни, сприяючи створенню безпечного цифрового середовища у вищій освіті. Запропонована поетапна модель (оцінка потреб, розробка модулів, навчання, моніторинг) може стати основою для системних змін, хоча її впровадження, та я переконаний, що вона потребує доопрацювання. Для адміністрацій ЗВО ці напрацювання пропонують орієнтири для розроблення політик, для викладачів – ідеї для інтеграції кібергігієни в освітній процес, а для студентів – поштовх до саморозвитку в цій сфері.

Перспективи подальших досліджень пов'язані з емпіричною перевіркою запропонованих ідей. Зокрема, доцільно провести анкетування та інтерв'ю для оцінки

реального рівня кібергігієни в українських ЗВО, а також протестувати ефективність інтерактивних тренінгів чи навчальних модулів у контрольованих умовах. Іншим цікавим напрямом могло б стати вивчення впливу кібергігієни на академічну успішність чи розробка спеціалізованих програм для студентів різних спеціальностей – наприклад, технічних чи гуманітарних. Такі дослідження, дозволять перейти від теоретичних напрацювань до практичних рішень, які матимуть відчутний вплив на безпеку освітнього процесу.

Список використаних джерел:

[1]. Державна служба спеціального зв'язку та захисту інформації України. Місяць кібербезпеки: матеріали для навчання. 2023. URL: https://www.cip.gov.ua/ua/news/v-ukrayini-rozpochavsya-misyac-kiberbezpeki

[2]. Базові знання з кібергігієни: онлайн-курс. Мінцифри України; платформа Дія.Освіта. Київ, 2023. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene

[3]. Міністерство освіти і науки України. Концепція розвитку цифрових компетентностей. Київ, 2024. URL: https://mon.gov.ua/

[4]. European Union Agency for Cybersecurity (ENISA). Cybersecurity Skills Development in the EU [Розвиток навичок кібербезпеки в ЄС]. Athens, 2021. URL: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

[5]. Knowles M. S. The Modern Practice of Adult Education: From Pedagogy to Andragogy [Сучасна практика освіти дорослих: від педагогіки до андрагогіки]. Cambridge: Cambridge Adult Education, 1980. 400 с.

[6]. National Institute of Standards and Technology (NIST). Cybersecurity Awareness Training Guidelines [Керівні принципи навчання обізнаності з кібербезпеки]. Gaithersburg, MD, 2020. URL: https://csrc.nist.gov/pubs/sp/800/50/final

[7]. Organization for Security and Co-operation in Europe (OSCE). Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки. 2022. URL: https://www.osce.org/uk/project-coordinator-in-ukraine

[8]. UK National Cyber Security Centre. Cyber Essentials Scheme [Схема кібероснов]. London, 2018. URL: https://www.ncsc.gov.uk/cyberessentials

[9]. Франчук В. М. Захист даних. Засоби парольної ідентифікації та адміністрування. Науковий часопис НПУ імені М. П. Драгоманова. Серія № 2. Комп'ютерно-орієнтовані системи навчання. 2017. № 19 (26). с. 170–174.

[10]. Франчук В. М. Захист даних. Соціальна інженерія. Науковий часопис НПУ імені М. П. Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання. 2015. № 17 (24). с. 20–26.

[11]. Furnell S., Vasileiou I. Security education and awareness: A behavioral perspective [Освіта та обізнаність з безпеки: поведінкова перспектива]. Computers & Security. 2019. Vol. 87. 101586. DOI: 10.4018/978-1-5225-7847-5. URL: https://doi.org/10.4018/978-1-5225-7847-5

FORMATION OF CYBER HYGIENE IN HIGHER EDUCATION INSTITUTIONS: ORGANIZATIONAL AND PEDAGOGICAL APPROACHES AND PRACTICAL STRATEGIES

Kostiantyn Zlahodukh

Abstract. The article is dedicated to analyzing the organizational and pedagogical foundations of forming cyber hygiene in higher education institutions (HEIs) amid the growing cyber threats. The relevance is driven by the intensive digitalization of education, accompanied by an increase in cyber incidents such as phishing, data leaks, and attacks on HEI information systems. The aim is to develop conceptual approaches to forming cyber hygiene, considering organizational and pedagogical factors to ensure a secure digital environment. The study is based on a mixed methodology, including qualitative and quantitative methods. It analyzes the theoretical foundations of cyber hygiene, particularly psychological and behavioral aspects. The current state of cyber hygiene implementation in Ukrainian HEIs is examined, where resource shortages, fragmented regulatory frameworks, and low motivation among educational process participants hinder a systematic approach. A comparison is made with international experiences, including post-Soviet countries like Estonia, where cyber hygiene is integrated through public-private partnerships, and EU and US countries. Practical strategies are proposed: organizational measures, pedagogical approaches, collaboration with IT companies. A phased model for cyber hygiene formation is developed: needs assessment, creation of tailored materials, training of students, faculty, staff, and effectiveness monitoring. The results can be used to develop training programs, methodological guidelines, and regulations to enhance cybersecurity in education. Future research prospects include empirical testing of the strategies in Ukrainian HEIs, evaluating their impact on educational process security, and scaling the model to other educational levels, such as secondary education.

The article emphasizes the need for an interdisciplinary approach combining organizational, pedagogical, and technological aspects.

Keywords: cyber hygiene, cybersecurity, higher education, pedagogical strategies, organizational measures, gamification, digital literacy

References (translated and transliterated)

[1]. Derzhavna Sluzhba Spetsialnoho Zviazku ta Zakhystu Informatsii Ukrainy, Misiats Kiberbezpeky: Materialy dlia Navchannia [Cybersecurity Month: Training Materials], Kyiv, Ukraine, 2023. [Online]. Available: https://www.cip.gov.ua/ua/news/v-ukrayini-rozpochavsya-misyac-kiberbezpeki. (In Ukrainian)

[2]. Mintsyfry Ukrainy, Bazovi Znannia z Kibergigiieny: Onlain-Kurs [Basic Knowledge of Cyber Hygiene: Online Course], Kyiv, Ukraine: Diia.Osvita Platform, 2023. [Online]. Available: https://osvita.diia.gov.ua/courses/cyber-hygiene. (In Ukrainian)

[3]. Ministerstvo Osvity i Nauky Ukrainy, Kontseptsiia Rozvytku Tsyfrovykh Kompetentnostei [Concept of Digital Competencies Development], Kyiv, Ukraine, 2024. [Online]. Available: https://mon.gov.ua/ (In Ukrainian)

[4]. European Union Agency for Cybersecurity (ENISA), Cybersecurity Skills Development in the EU, Athens, Greece, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union. (In English)

[5]. M. S. Knowles, The Modern Practice of Adult Education: From Pedagogy to Andragogy, Cambridge, UK: Cambridge Adult Education, 1980, 400 p. (In English)

[6]. National Institute of Standards and Technology (NIST), Cybersecurity Awareness Training Guidelines, Gaithersburg, MD, USA, 2020. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/50/final (In English)

[7]. Organization for Security and Co-operation in Europe (OSCE), Posylennia Spromozhnostei Ukrainskykh Derzhavnykh Orhaniv u Sferi Kibergigiieny ta Kiberbezpeky [Strengthening the Capabilities of Ukrainian State Bodies in Cyber Hygiene and Cybersecurity], Vienna, Austria, 2022. [Online]. Available: https://www.osce.org/uk/project-coordinator-in-ukraine. (In Ukrainian)

[8]. UK National Cyber Security Centre, Cyber Essentials Scheme, London, UK, 2018. [Online]. Available: https://www.ncsc.gov.uk/cyberessentials. (In English)

[9]. V. M. Franchuk, “Zakhyst Danykh. Zasoby Parolnoi Identyfikatsii ta Administruvannia” [Data Protection. Means of Password Identification and Administration], Naukovyi Chasopys NPU imeni M. P. Drahomanova. Seriia № 2. Kompiuterno-Oriientovani Systemy Navchannia, no. 19 (26), pp. 170–174, 2017. (In Ukrainian)

[10]. V. M. Franchuk, “Zakhyst Danykh. Sotsialna Inzheneriia” [Data Protection. Social Engineering], Naukovyi Chasopys NPU imeni M. P. Drahomanova. Seriia № 2. Kompiuterno-Oriientovani Systemy Navchannia, no. 17 (24), pp. 20–26, 2015. (In Ukrainian)

[11]. S. Furnell and I. Vasileiou, “Security education and awareness: A behavioral perspective,” Computers & Security, vol. 87, 101586, 2019, doi: 10.4018/978-1-5225-7847-5. [Online]. Available: https://doi.org/10.4018/978-1-5225-7847-5. (In English)