

Автор:

Злагодух Костянтин Олександрович,
аспірант першого курсу
спеціальності 011 Освітні, педагогічні науки
(ІКТ в освіті)

Науковий керівник:

Франчук Василь Михайлович,
доктор педагогічних наук, доцент,
завідувач кафедри комп'ютерної та програмної
інженерії

РОЗВИТОК ЦИФРОВОЇ БЕЗПЕКИ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ: ПЕДАГОГІЧНІ ІНСТРУМЕНТИ ТА ОРГАНІЗАЦІЙНІ РІШЕННЯ

Анотація. У роботі досліджується проблема забезпечення цифрової безпеки в закладах вищої освіти через використання педагогічних інструментів та організаційних рішень. Метою дослідження є аналіз сучасних підходів до формування кібергігієни у освітньому процесі та розроблення рекомендацій для їх удосконалення. Об'єкт дослідження – система цифрової безпеки ЗВО, предмет – методи та інструменти її реалізації. Використані методи: аналіз літератури, порівняння, узагальнення. Результати свідчать, що інтеграція курсів із кібергігієни та внутрішніх політик безпеки підвищує рівень захищеності студентів і викладачів.

Ключові слова: цифрова безпека, кібергігієна, вища освіта, педагогічні інструменти.

Вступ. Сучасний розвиток інформаційних технологій супроводжується стрімким зростанням кіберзагроз, що робить проблему цифрової безпеки в закладах вищої освіти (ЗВО) надзвичайно актуальною. Незахищеність студентів і викладачів від кібератак може призвести до втрати конфіденційних даних, порушення приватності, а також суттєвого зниження якості освітнього процесу. Усе це вимагає пошуку ефективних рішень для створення безпечного цифрового середовища у ЗВО.

Постановка задачі. Необхідно визначити комплекс педагогічних інструментів та організаційних рішень, використання яких сприятимуть підвищенню рівня цифрової безпеки у ЗВО через формування кібергігієни. Особливу увагу слід приділити врахуванню специфіки освітнього процесу, а також обмеженості ресурсів, з якими часто стикаються заклади вищої освіти.

Мета роботи. Метою дослідження є розроблення практичних рекомендацій для інтеграції сучасних підходів до забезпечення кібергігієни у систему вищої освіти, що дозволить підвищити рівень цифрової безпеки та стійкості ЗВО до кіберзагроз.

Основна частина. Дослідження показало, що одним із найефективніших педагогічних інструментів є впровадження спеціалізованих курсів із кібергігієни, які мають бути доступними для студентів усіх спеціальностей. Такі курси повинні включати не лише теоретичні основи, але й практичні заняття, спрямовані на формування навичок розпізнавання фішингових атак, створення безпечних паролів, а також правильного використання хмарних сервісів і програмного забезпечення. Наприклад, у 2023 році в одному з українських ЗВО було проведено експериментальне навчання, яке охопило 150 студентів різних факультетів. У рамках цього проєкту учасники отримали базові знання про кіберзагрози та відпрацьовували практичні навички на симуляціях реальних атак. Результати показали зростання рівня обізнаності студентів на 35%, а також зменшення випадків успішного фішингу на 20% у порівнянні з контрольною групою [1, 45].

Окрім цього, важливим аспектом є залучення викладачів до процесу підвищення кваліфікації у сфері кібергігієни. Оскільки викладачі часто виступають прикладом для студентів, їхня обізнаність із сучасними кіберзагрозами та методами їх запобігання має бути на високому рівні. Для цього доцільно проводити регулярні тренінги та семінари, які б

охоплювали такі теми, як безпечне використання електронної пошти, захист персональних даних і правильна реакція на підозрілі інциденти.

Щодо організаційних рішень, у дослідженні підкреслюється необхідність розроблення та впровадження внутрішніх політик безпеки у ЗВО. Одним із базових заходів є обов'язкова двофакторна автентифікація для доступу до навчальних платформ, таких як Moodle чи Google Classroom, що значно ускладнює несанкціонований доступ до системи. Також важливим є регулярне оновлення програмного забезпечення на комп'ютерах і серверах закладів освіти, адже застарілі версії часто стають вразливими до атак. Для оперативного реагування на кіберінциденти пропонується створення спеціальних груп, які б склалися з ІТ-фахівців і представників адміністрації ЗВО. Такі групи могли б швидко локалізувати проблему, наприклад, витік даних чи атаку вірусу-шифрувальника, та мінімізувати її наслідки.

Для формування кібергігієни в ЗВО пропонується інтегрувати до навчальних програм модулі з розпізнавання атак соціальної інженерії, таких як фішинг, та навчання створення надійних паролів [4, 20-26]. Організаційні рішення включають впровадження політик безпеки, що передбачають перевірку ідентичності запитів на доступ до даних, використання багатофакторної ідентифікації (поєднання паролів і USB-токенів) та технічний аналіз електронної пошти для виявлення загроз. Такі заходи підвищують рівень захищеності інформаційних ресурсів ЗВО та сприяють формуванню культури цифрової безпеки [3, 170-174].

На міжнародному рівні подібні підходи вже демонструють ефективність. Наприклад, у США низка університетів запровадила обов'язкові курси з кібергігієни для першокурсників, що дозволило знизити кількість інцидентів, пов'язаних із кібератаками, на 15% протягом двох років [2, 72]. Цей досвід може бути адаптований до українських реалій із урахуванням місцевих особливостей, таких як обмежене фінансування та недостатня кількість кваліфікованих спеціалістів у сфері кібербезпеки.

Висновки. Інтеграція педагогічних інструментів, таких як навчальні курси з кібергігієни, та організаційних рішень, зокрема внутрішніх політик безпеки, дозволяє створити комплексний підхід до забезпечення цифрової безпеки у ЗВО. Для системного вирішення проблеми рекомендується впроваджувати ці заходи на державному рівні, залучаючи до співпраці Міністерство освіти і науки, а також провідні ІТ-компанії, які могли б надати експертну підтримку.

Список використаних джерел

1. Коваленко І.М. Кібергігієна в освіті: сучасні виклики та рішення. – К.: Видавництво НПУ, 2023. – 120 с.
2. Smith J. Cyber Hygiene in Higher Education: Trends and Strategies. – New York: Academic Press, 2022. – 95 p.
3. 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.
4. 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.