Актуальні питання кібербезпеки у професійній освіті: методи захисту інформації

Гелеш Анна Валентинівна[1], Матійців Богдан Орестович[2]

Опубліковано	Секція	УДК
30.04.2025	Освіта/Педагогіка	004.056:37.018.43

DOI: https://doi.org/10.5281/zenodo.15376086

Анотація. У статті розглядається актуальність кібербезпеки в професійній освіті, методи захисту інформації. Визначено основні загрози, такі як фішинг, шкідливе програмне забезпечення, атаки на сервери освітніх закладів та низький рівень цифрової грамотності користувачів. Проаналізовано технічні, організаційні та правові методи захисту інформації, включаючи використання антивірусних програм, навчання основам кібербезпеки та дотримання законодавства. Відзначено вагомість комплексного підходу до забезпечення кібербезпеки для захисту інформаційних ресурсів освітніх закладів та підвищення обізнаності учасників освітнього процесу щодо сучасних кіберзагроз.

Ключові слова: кібербезпека, професійна освіта, захист інформації, цифрова грамотність, кіберзагрози, фішинг, шкідливе програмне забезпечення, законодавство.

Cyber security in professional education: methods of information protection

Annotation. The modern world is rapidly developing in the direction of digital technologies, which makes the issue of cybersecurity relevant for all spheres of life, including vocational education. The process of digitalization of education has significantly accelerated with the advent of online learning in Ukraine. This transition became necessary due to the COVID-19 pandemic, and later due to military actions, which forced educational institutions to change the format of education. However, along with this, new threats have emerged: possible leakage of personal data, hacker attacks on educational platforms and unauthorized access to educational materials. Educational institutions accumulate a significant amount of confidential information: personal data of students and teachers, methodological materials, scientific developments, etc. Therefore, the issue of cybersecurity is becoming increasingly relevant, because the protection of student and teacher data is one of the key tasks for modern education.

The Law of Ukraine No. 2163-VIII “On the Basic Principles of Ensuring Cybersecurity in Ukraine” defines the legal and organizational framework for ensuring cybersecurity in the state, including the educational sphere. It establishes the principles of protecting information systems, preventing cyber threats, and liability for data security breaches. According to this law, educational institutions must also implement effective cyber security measures to protect information and digital infrastructure.

[1] кандидат історичних наук, доцент, доцент кафедри педагогіки та інноваційної освіти, Національний університет «Львівська політехніка», ORCID: https://orcid.org/0000-0002-0143-0518

[2] здобувач вищої освіти четвертого курсу навчання бакалаврського рівня вищої освіти спеціальності 015 Професійна освіта (Цифрові технології), Національний університет «Львівська політехніка», ORCID: https://orcid.org/0009-0008-4179-6603

The article examines the relevance of cybersecurity in vocational education in the context of digitalization and the transition to online learning in Ukraine. The main threats are identified, such as phishing, malware, attacks on educational institution servers, and low levels of digital literacy of users. Technical, organizational, and legal methods of information protection are analyzed, including the use of antivirus programs, training in the basics of cybersecurity, and compliance with the law. The need for a comprehensive approach to ensuring cybersecurity is emphasized to protect the information resources of educational institutions and raise awareness among participants in the educational process about modern cyber threats.

Keywords: cyber security, professional education, information security, digital literacy, cyber threats, phishing, malware, legislation.

Вступ

Постановка проблеми. Сучасний світ швидко розвивається в напрямі цифрових технологій, що робить питання кібербезпеки актуальним для всіх сфер життя, зокрема й професійної освіти. Процес цифровізації освіти значно прискорився з появою онлайн навчання в Україні. Цей перехід став необхідним через пандемію COVID-19, а згодом і через воєнні дії, які змусили заклади освіти змінювати формат навчання. Однак разом із цим виникли нові загрози: можливий витік особистих даних, хакерські атаки на навчальні платформи та несанкціонований доступ до освітніх матеріалів. У освітніх закладах накопичується значний обсяг конфіденційної інформації: персональні дані студентів і викладачів, методичні матеріали, наукові розробки тощо. Тому питання кібербезпеки стає все більш актуальним, адже захист даних студентів і викладачів є одним із ключових завдань для сучасної освіти.

Закон України No 2163-VIII «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення кібербезпеки в державі, включаючи освітню сферу. Він встановлює принципи захисту інформаційних систем, запобігання кіберзагрозам та відповідальність за порушення безпеки даних. Відповідно до цього закону, освітні заклади також повинні впроваджувати ефективні заходи кіберзахисту для захисту інформації та цифрової інфраструктури [4].

В умовах зростаючої кількості кіберзагроз та активного використання цифрових технологій в освітньому процесі постає нагальна потреба в розгляді методів захисту інформації. Хакерські атаки, фішингові схеми та несанкціонований доступ до даних можуть призвести до витоку конфіденційної інформації, що особливо небезпечно для освітніх закладів, які зберігають персональні дані студентів і викладачів. Тому важливо не лише використовувати сучасні технології кіберзахисту, а й підвищувати рівень цифрової грамотності всіх учасників освітнього процесу [3].

Аналізуючи тему кібербезпеки в професійній освіті: методи захисту інформації, доцільно розглянути визначення поняття інформації, інформаційного простору, а також кібератаки та кібербезпеки.

Інформація – це сукупність відомостей про події, явища та процеси, які передаються, зберігаються та обробляються за допомогою різних носіїв і технологій. Вона може мати різні форми, зокрема текстову, графічну, аудіо- та відеоінформацію, і є ключовим ресурсом у сучасному цифровому середовищі.

Інформаційний простір – це сукупність даних, інформаційних технологій, цифрових комунікацій та засобів їхнього зберігання, обробки та передачі. Він охоплює як матеріальні, так і нематеріальні складові, включаючи інформаційні ресурси, програмне забезпечення, мережеву інфраструктуру та засоби кіберзахисту. Інформаційний простір є невід'ємною частиною сучасного суспільства, що потребує ефективних механізмів безпеки для запобігання загрозам кіберзлочинності.

Кібератака – це будь-яка навмисна дія, спрямована на порушення функціонування комп'ютерних систем, крадіжку, зміну або знищення даних, використовуючи шкідливе

програмне забезпечення, соціальну інженерію чи інші методи. Такі атаки можуть бути спрямовані на організації, державні установи та окремих користувачів.

Кібербезпека – це сукупність технологій, процесів і практик, спрямованих на захист мереж, пристроїв, програм та даних від атак, пошкоджень або несанкціонованого доступу. Вона є ключовим елементом інформаційної безпеки та передбачає запобігання, виявлення та реагування на кіберзагрози. Вона охоплює технічні, організаційні та освітні аспекти безпечного використання цифрових ресурсів [5].

У сучасному цифровому світі інформація є одним із найцінніших ресурсів, який потребує надійного захисту. В умовах активного розвитку інформаційного простору освітні заклади все частіше стикаються з ризиками несанкціонованого доступу, витоку даних та інших загроз. Кібератаки можуть призвести до серйозних наслідків, зокрема втрати персональних даних студентів і викладачів, порушення функціонування освітніх платформ та компрометації навчальних матеріалів. Саме тому кібербезпека в професійній освіті є ключовим завданням, що потребує комплексного підходу: впровадження сучасних технологій захисту, підвищення цифрової грамотності користувачів та дотримання норм безпечного використання інформаційних ресурсів.

Аналіз останніх досліджень і публікацій. Проблема кібербезпеки в освіті активно досліджується як вітчизняними, так і зарубіжними науковцями. Серед українських дослідників значний внесок у вивчення питань цифрової безпеки зробили Іванченко О.М. та Петренко В.В., які аналізують методи захисту інформації у освітньому середовищі. Серед зарубіжних авторів слід відзначити роботи Андерсона Р., що висвітлюють загальні принципи кібербезпеки, та Шнайєра Б., який розглядає аспекти криптографічного захисту даних. В їхніх працях розглядаються методи захисту інформації, кіберзагрози та рівень цифрової грамотності користувачів освітніх платформ. Зокрема, в наукових статтях наголошується на важливості впровадження системних заходів кібербезпеки та підвищення обізнаності студентів і викладачів щодо сучасних загроз. Проблема кібербезпеки в освіті активно досліджується як вітчизняними, так і зарубіжними науковцями, в їхніх працях розглядаються методи захисту інформації, кіберзагрози та рівень цифрової грамотності користувачів освітніх платформ. Зокрема, в наукових статтях наголошується на важливості впровадження системних заходів кібербезпеки та підвищення обізнаності студентів і викладачів щодо сучасних загроз.

Метою статті є визначення актуальних методів захисту інформації для забезпечення безпеки освітнього процесу.

Результати

Відчуття безпеки в інформаційному просторі є основою довіри між особою і організацією. Люди хочуть бути впевненими, що їхні персональні дані надійно захищені, а організації повинні забезпечити, щоб ці дані не потрапили до рук третіх осіб або не були використані неналежним чином. Це вимагає не лише технічних заходів захисту, але й чіткої політики щодо обробки даних, прав і обов'язків усіх сторін. Важливо, щоб організації не тільки дотримувалися законодавчих норм, але й інвестували в сучасні засоби кіберзахисту та підвищували обізнаність своїх співробітників щодо ризиків у кіберпросторі.

Основні загрози кібербезпеці, які можуть зустрічатися в освітньому середовищі це фішинг та соціальна інженерія, віруси та шкідливе програмне забезпечення, атаки на сервери освітніх заладів, а також низький рівень цифрової грамотності користувачів. Фішинг та соціальна інженерія – атаки, спрямовані на отримання конфіденційної інформації через обманні електронні листи або сайти. Віруси та шкідливе програмне забезпечення – можуть призвести до втрати або викрадення даних. Атаки на сервери освітніх закладів – несанкціонований доступ до баз даних або злам інформаційних

систем. Низький рівень цифрової грамотності користувачів – студенти та викладачі можуть нехтувати базовими принципами безпеки [1, 2].

Загрози кібербезпеці в професійній освіті можуть мати серйозні наслідки як для студентів, так і для освітніх закладів. Освітні заклади зберігають велику кількість персональної інформації про студентів, викладачів та співробітників (наприклад, оцінки, платіжні дані, документи). Якщо ці дані потрапляють у руки кіберзлочинців, можуть виникнути проблеми з приватністю та використанням цих даних у зловмисних цілях. Це може призвести до втрати репутації та зменшення кількості студентів, що бажають навчатися в цьому закладі.

Атаки на системи зберігання даних можуть призвести до втрати важливих навчальних матеріалів, які використовуються в освітньому процесі. Це може порушити освітній процес і ускладнити доступ до необхідних ресурсів. В разі злому системи захисту можна отримати доступ до дипломних робіт, курсових проектів та інших академічних матеріалів студентів. Це може призвести до крадіжки інтелектуальної власності або підготовки фальшивих робіт.

Використання кіберзагроз для отримання фінансової інформації, наприклад, даних студентських карток або платіжних систем, може призвести до фінансових втрат і шахрайства.

У разі атак на платформи дистанційного навчання студенти та викладачі можуть втратити доступ до ресурсів, що порушить освітній процес. Атаки на відеоконференції або онлайн-засоби можуть створити додаткові труднощі в навчанні. У сучасному світі професійна освіта пов'язана з навчанням нових технологій та підготовкою до роботи з ними. Атаки на ці технології можуть сповільнити розвиток або ускладнити освітній процес [5].

Для зменшення цих загроз необхідно інвестувати в кібербезпеку, постійно оновлювати програмне забезпечення, проводити навчання для студентів та викладачів щодо основ захисту інформації та створювати надійні механізми для захисту даних.

До технічних методів захисту інформації слід віднести використання антивірусного програмного забезпечення, встановлення та регулярне оновлення антивірусних програм, використання міжмережевих екранів (фаєрволів) для блокування потенційно небезпечних з'єднань [1, 2].

Серед організаційних методів захисту інформації слід виділити навчання студентів і викладачів основам кібербезпеки, проведення тренінгів і семінарів щодо розпізнавання загроз, ознайомлення з методами захисту особистих даних та паролів.

Правові методи захисту інформації це ознайомлення з відповідним законодавством у сфері кібербезпеки та захисту персональних даних, а також забезпечення відповідності політики кібербезпеки закладу вимогам законодавства.

Інтеграція технічних, організаційних та правових методів захисту інформації в професійній освіті є необхідною для забезпечення комплексної кібербезпеки та стійкості освітніх установ до сучасних кіберзагроз.

Отже, важливо здійснювати контроль доступу до інформаційних ресурсів, використовувати багаторівневу автентифікацію, надавати права доступу лише тим, кому це необхідно, здійснювати резервне копіювання даних, зберігати резервні копії у безпечних місцях, зокрема в хмарних сховищах із шифруванням.

Висновки

Захист даних у професійній освіті є багатогранним завданням, що вимагає комплексного підходу, який включає технічні, організаційні та правові методи захисту інформації. Враховуючи досвід провідних освітніх установ, які активно впроваджують сучасні технології та практики кіберзахисту.

Технічні методи, такі як впровадження сучасних антивірусних програм, міжмережевих екранів та систем виявлення вторгнень, є першою лінією оборони проти кібератак. Ці засоби дозволяють виявляти та нейтралізувати загрози на ранніх етапах, запобігаючи можливим втратам даних та порушенням роботи інформаційних систем.

Організаційні методи включають розробку та впровадження політик безпеки, регулярне навчання персоналу та проведення аудитів безпеки. Наприклад, освітні програми з кібербезпеки, такі як ті, що пропонуються Міжрегіональною Академією Управління персоналом, забезпечують підготовку фахівців, здатних ефективно реагувати на сучасні кіберзагрози.

Правові методи, зокрема дотримання законодавства у сфері захисту інформації та кібербезпеки, встановлюють нормативну базу для забезпечення безпеки в освітніх закладах. Це включає виконання вимог щодо захисту персональних даних та конфіденційної інформації, що є критично важливим для підтримання довіри серед студентів та співробітників.

Отже, забезпечення кібербезпеки в професійній освіті вимагає системного підходу, що поєднує технічні, організаційні та правові заходи. Лише комплексне впровадження цих методів дозволить ефективно захистити інформаційні ресурси освітніх закладів та підготувати фахівців, здатних протистояти сучасним кіберзагрозам.

Список використаних джерел

1. Гончарова І.П. Кібербезпека як складова безпеки життєдіяльності закладів освіти. – 2022. Взято з: https://lib.iitta.gov.ua/id/eprint/733621/1/%D0%91%D0%96%D0%94.pdf (дата звернення: 07.03.2025).
2. Гончарова І.П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти: електронний навчальний курс. – 2022. Взято з: https://lib.iitta.gov.ua/id/eprint/733620/1/%D0%9A%D0%86%D0%91%D0%95%D0%A0%D0%91%D0%95%D0%97%D0%9F%D0%95%D0%9A%D0%90.pdf (дата звернення: 07.03.2025).
3. Горбенко А.А. Кібербезпека освітнього середовища в умовах карантину. Взято з: https://conf.ztu.edu.ua/wp-content/uploads/2020/05/94.pdf (дата звернення: 07.03.2025).
4. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII // Відомості Верховної Ради. – 2017. – № 45. – С. 403.
5. Основні правила захисту даних – кібергігієна для активного Інтернет-користувача. Взято з: https://eset.ua/ua/blog/view/38/osnovnyye-pravilazashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya (дата звернення: 07.03.2025).