Комунальний заклад «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»
Комунальний заклад «Житомирський обласний інститут післядипломної педагогічної освіти» Житомирської обласної ради
Комунальний заклад вищої освіти «Вінницька академія безперервної освіти»
Комунальний заклад «Запорізький обласний інститут післядипломної педагогічної освіти» Запорізької обласної ради
Тернопільський національний педагогічний університет імені Володимира Гнатюка
Центральноукраїнський національний технічний університет
Центральноукраїнський інститут розвитку людини Університету «Україна»
Донецький державний університет внутрішніх справ
Кіровоградський науково-дослідний експертно-криміналістичний центр МВС України
Центр «Адвокат дитини» Вищої школи адвокатури Національної асоціації адвокатів України

III Всеукраїнська науково-практична конференція

«БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ, ОСВІТА, ВЗАЄМОДІЯ»

05-09 лютого 2024 року

Сайт конференції

Сторінка матеріалів учасників конференції

Відеозапис пленарного засідання конференції

Кропивницький
2024

УДК 004 (06)

Безпека дітей в Інтернеті: попередження, освіта, взаємодія: збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції, м. Кропивницький, 05-09 лютого 2024 року / уклад. С.М. Єфіменко; за заг. ред. Г.В.Скрипки. Кропивницький: КЗ «КОІППО імені Василя Сухомлинського», 2024. 140 с.

Друкується за рішенням вченої ради
комунального *закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»*
(від 14 лютого 2024 року, протокол №2)

Рецензенти:
Сергій БУРТОВИЙ, кандидат педагогічних наук, заступник директора з науково-дослідної діяльності та міжнародного співробітництва комунального закладу «Кіровоградський обласний інститут післядипломної педагогічної освіти імені Василя Сухомлинського»;
Олександр УЛІЧЕВ – кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Відповідальний за випуск – Віталій ДМИТРУК

Збірник матеріалів конференції містить основні результати науково-практичних пошуків освітян, правоохоронців, представників громадських організацій та державних органів різних областей України щодо осмислення, виявлення та поширення ефективних практик, які сприяють забезпеченню безпеки дітей в Інтернеті, а також розвитку кіберграмотності педагогічної спільноти.

Матеріали опубліковані в авторській редакції.

ЗМІСТ

повинні не лише покращити свої навички у сфері кіберграмотності, а й успішно інтегрувати їх у освітній процес.

На цьому шляху важливо враховувати конкретні напрями:

- навчання, зосереджене на безпечному використанні онлайн-ресурсів, сучасних методах пошуку інформації, критичному аналізі;
- активне впровадження інноваційних методик у професійну практику;
- самоосвіта та постійний професійний розвиток.

Відповідальне використання педагогом інтернет-простору є ключовим чинником для забезпечення високої ефективності та надійності онлайн-середовища в освітній сфері. Це впливає на якість освіти та створює сприятливі умови для подальшого прогресивного розвитку освітньої системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гончарова І. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти / електронний навчальний курс. Біла Церква, 2022 URL: http://surl.li/mxthz.

2. Бондаренко В. Умови та засоби формування навичок інформаційної безпеки майбутніх учителів. *Інформаційні технології і засоби навчання*, 2019. Том 74, № 6. URL: http://surl.li/qebjf.

3. Правила кібергігієни: 7 кроків для покращення захисту даних. Eset : вебсайт. URL: http://surl.li/mdzrt

ВИКЛИКИ КІБЕРБЕЗПЕКИ В УМОВАХ ДИСТАНЦІЙНОГО НАВЧАННЯ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Ганна СКАСКІВ

Основні положення щодо організації питань безпеки у кіберпросторі викладено у Законі України «Про основні засади забезпечення кібербезпеки України». Закон регулює основні напрямки та принципи політики держави у сфері кібербезпеки, координує основні положення державних органів та установ щодо захисту інтересів громадян у міжнародному цифровому просторі [1].

Однак відкритими залишаються питання про виклики освітнього кіберпростору під час організації навчання в онлайн-форматі у закладах вищої освіти.

Мета статті: подати огляд найважливіших викликів кібербезпеки, які мають відношення до системи вищої освіти в умовах організації освітнього процесу в дистанційній або змішаній формі.

У діджиталізованому освітньому онлайн-просторі однією з найбільших загроз є соціальна інженерія, що охоплює і шахрайські атаки. Кіберзлочинці отримують користь від облікових даних для отримання доступу до шкільної або університетської мережі. Найпоширенішим способом отримання таких облікових даних є успішна спроба фішингу.

Організація безпечної дистанційної роботи у вищій школі є своєрідним викликом у мирних умовах, що значно ускладнюється в умовах воєнного стану, оскільки доступ до освітніх платформ здійснюється через Інтернет [2] великою кількістю користувачів через різні мережі, які характеризуються стандартною архітектурою.

Сучасні цифрові технології, що використовуються у закладах вищої освіти України, забезпечують для студентів нові можливості для формування базових знань, практичного досвіду та розвитку ключових компетентностей. Однак значна кількість систем електронного навчання, зокрема і Moodle, є великими за обсягом, містять багато інформації та передбачають різні способи взаємодії та обміну даними. І основною проблемою стає захист, підтримка конфіденційності користувачів, збереження цілісності контенту та авторського права з забезпеченням однакових можливостей і рівнів доступу до освітніх послуг усіх користувачів.

Проведений аналіз забезпечення якості надання освітніх послуг та визначення загроз інформаційної безпеки в умовах навчання онлайн у Центрі дистанційного навчання Тернопільського національного педагогічного університету імені Володимира Гнатюка (ТНПУ) дає можливість визначити наступні виклики з проблем кібербезпеки:

1. Атаки програм-зловмисників (вірусів, макросів);
2. Помилки ППЗ (збої у функціоналі програмного забезпечення);
3. Технічні збої (проблеми з кодуванням та декодуванням даних);
4. Несанкціонований доступ (шпигунські та хакерські атаки);
5. Несанкціоноване використання контенту (стороннє втручання сторонніх осіб, порушення авторського права);
6. Проблеми з електропостачанням (тривалі відключення електроенергії, проблеми з послугами WAN);
7. Зношеність техніки (використання застарілого обладнання, яке складно підтримувати та оновлювати в умовах війни) [3].

З огляду на визначення подібних загроз, для успішної реалізації дистанційного навчання в умовах війни заклади вищої освіти визначають чіткі лінії передачі даних, встановлюють брандмауери та оновлюють антивірусне програмне забезпечення, проводять постійну перепідготовку фахівців з організації безпеки та онлайн-комунікації, удосконалюють рівні доступу, авторизації та ідентифікації користувачів.

Безпека даних у закладах вищої освіти – це практика захисту даних від несанкціонованого доступу, від маніпулювання та несанкціонованого розповсюдження інформації. Тому рівні безпеки включають фізичні заходи, такі як замки та паролі для запобігання зловмисному доступу, а також цифрові засоби захисту, такі як шифрування та брандмауери для захисту від хакерів. Вона також охоплює політику та процедуру для належного поводження з конфіденційною інформацією.

Безпека даних набуває все більшого значення в освіті. Університети та школи повинні захищати не лише власну інформацію, але й інформацію про

студентів чи учнів, батьків, викладачів чи учителів, персоналу та інших зацікавлених сторін.

Зі збільшенням обсягу даних, що зберігаються в електронному вигляді в освітянських мережах, зростає і потреба в безпечній практиці їх передачі, яка ніколи не була такою важливою. Коли справа доходить до безпеки в Інтернеті, усі учасники освітнього процесу повинні бути особливо обережними. Сьогодні існує безліч сайтів, які зберігають персональні дані та використовують їх у зловмисних цілях – наприклад, для отримання коштів або навіть викрадення людей. Ось чому важливо інформувати молодь про небезпеку надання особистої інформації на підозрілих сайтах.

Умови успішного подолання викликів у сфері кібербезпеки, які впроваджуються у ТНПУ:

1. Захист конфіденційних даних.

У ТНПУ обробляють та зберігають велику кількість конфіденційної інформації, включаючи інформацію про студентів, фінансову звітність, результати досліджень тощо. Важливо, щоб ці дані зберігалися у безпеці, щоб захистити конфіденційність залучених осіб і забезпечити доступ до них лише уповноваженому персоналу.

2. Забезпечення нормативно-правової відповідності.

Дотримання вимог регуляторних органів, які висувають до закладів вищої освіти щодо керування безпекою даних. Невиконання цих вимог може призвести до великих штрафів або інших санкцій, які можуть зашкодити репутації закладу, а також його фінансовому стану.

3. Уникнення втрати даних.

Незахищені дані піддаються ризику крадіжки або випадкової втрати через людські помилки або технічні збої, що може мати серйозні наслідки. Тому з метою захисту регулярно проводиться резервного копіювання інформації на віддалених захищених серверах, щоб уникнути будь-яких потенційних втрат.

4. Захист інтелектуальної власності.

Кожен ЗВО часто володіє цінною інтелектуальною власністю, яку потрібно захистити від несанкціонованого використання або розголошення. Тому заходи безпеки даних можуть допомогти захистити цю інтелектуальну власність, щоб вона залишалася безпечною та конфіденційною.

5. Запобігання кібератакам.

Кіберзлочинці все частіше націлюються на вищі навчальні заклади через цінну інформацію, яку вони містять, що робить ефективні заходи безпеки даних необхідними для захисту від цих атак.

6. Мінімізація репутаційних втрат.

Витік даних може зашкодити репутації установи, а також її фінансовому стану, з довгостроковими наслідками для кількості студентів, відносин з донорами тощо. Впровадження надійних заходів безпеки може допомогти запобігти подібним інцидентам.

Навчальні заклади повинні демонструвати свою прихильність до безпеки своїх студентів, викладачів, співробітників та інших зацікавлених сторін,

впроваджуючи надійну політику та процедуру захисту даних. Це допоможе захистити всіх від будь-яких потенційних ризиків, пов'язаних з витоком даних.

Щоб забезпечити безпеку в освіті, слід дотримуватися деяких найкращих практик [3]. Встановлення чітких правил і процедур, пов'язаних з використанням технологій, онлайн-сховищ і цифрових комунікацій, може допомогти захистити конфіденційні дані навчального закладу. Ці правила повинні включати вказівки щодо прийнятного використання пристроїв і мереж; налаштування конфіденційності; протоколів управління паролями; процедур затвердження нових програмних додатків тощо.

Усі дані, що зберігаються, мають бути зашифровані, щоб запобігти несанкціонованому доступу. Шифрування робить інформацію нечитабельною для будь-кого, хто не має ключа для її розшифрування. Також важливо регулярно перевіряти, хто має доступ до конфіденційної інформації. Це допоможе виявити потенційні загрози та спроби несанкціонованого доступу.

Вживаючи необхідних заходів для захисту своїх даних, вищі навчальні заклади можуть краще захистити конфіденційну інформацію. Таким чином, вони можуть продемонструвати високий рівень безпеки та відповідність до вимог законодавства [1]. Безпека даних має важливе значення для захисту від будь-яких потенційних загроз. Завдяки налагодженій роботі у сфері кібербезпеки заклади вищої освіти, навіть в умовах воєнного стану, можуть продовжувати надавати якісні освітні послуги без перебоїв або втрати даних у форматі дистанційного чи змішаного навчання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 01.02.2024).
2. Про електронні комунікації Закон України від 30 вересня 2020 року. URL: https://dslua.org/publications/zakon-pro-elektronni-komunikatsii-universalnyy-dostup-subsydii-na-internet-zakhyst-personalnykh-danykh-ta-ryzyk-shatdauniv-v-zoni-ato/ (дата звернення: 01.02.2024).
3. Chen Y. and He W. Security and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 2013. URL: http://www.irrodl.org/index.php/irrodl/article/view/1632/2712.

Матеріали III Всеукраїнської науково-практичної конференції «БЕЗПЕКА ДІТЕЙ В ІНТЕРНЕТІ: ПОПЕРЕДЖЕННЯ, ОСВІТА, ВЗАЄМОДІЯ»

(м. Кропивницький, 05-09 лютого 2024 року)

Відповідальний редактор: Скрипка Г.В.
Укладач: Єфіменко С. М.

Підписано до друку 11.03.2024 р.
Формат 60х84 1/16. Папір офсетний. Гарнітура «Times New Roman».
Друк – принтер. Тираж 100 прим.
Зам. № 434

КЗ «КОІППО імені Василя Сухомлинського», вул. Велика Перспективна, 39/63, м. Кропивницький, 25006.