Це показує важливість та потребу у проведенні тренінгів, курсів або семінарів для покращення цифрової гігієни із дотриманням принципу наступності [1].

Формування безпечного інформаційного простору повинно включати не тільки технічні засоби, а також важливо, щоб самі користувачі усвідомлювали власну відповідальність за свою безпеку та проявляли ініціативу у здобутті базових знань і вмінь з кібергігієни.

Список використаних джерел

1. Барна О. В. Наступність у формуванні компетентностей учнів з питань безпеки в інтернеті: проблеми та шляхи їх вирішення. *Безпека дітей в Інтернеті: попередження, освіта, взаємодія* : збірник матеріалів ІІІ Всеукраїнської науково-практичної конференції (м. Кропивницький, 05–09 лютого 2024 року). С. 39–43.

2. Кравчук В. О. Зарубіжний досвід захисту персональних даних у соціальних мережах. Науковий вісник Ужгородського університету. Право. Ужгород, 2023. Т. 2, вип. 78. С. 49–53.

3. Прокопов С., Буцанова К. Проблеми персональної інформаційної безпеки в соціальних мережах. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали VI Міжнар. наук.-практ. конф. (м. Дніпро, 11 березня 2022 р.). Дніпро, 2022. С. 217–219.

4. Kemp S. Digital 2025 : Global Overview Report. Data Reportal. URL: https://datareportal.com/reports/digital-2025-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2025&utm_term=Isle_Of_Man&utm_content=Global_Promo_Block (дата звернення: 05.03.2025).

ТЕХНОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА РІШЕННЯ

Заяць Адам Олексійович
здобувач першого (бакалаврського) рівня вищої освіти спеціальності Середня освіта (Інформатика),
ернопільський національний педагогічний університет імені Володимира Гнатюка,
zayats_ao@fizmat.tnpu.edu.ua
Барна Ольга Василівна
кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
barna@tnpu.edu.ua

У XXI столітті бурхливий поступ цифрових інновацій суттєво трансформував інформаційний простір, одночасно породжуючи нові виклики в кібербезпеці. Збільшення кількості інтернет-користувачів, активне впровадження цифрових платформ у бізнес та державне управління зумовлюють збільшення обсягів конфіденційної інформації, яка потребує надійного захисту. На цьому фоні спостерігається посилення кібератак, які стають все складнішими, цілеспрямованішими та руйнівнішими. Порушення приватності, витоки даних, проникнення в корпоративні мережі – це лише деякі з сучасних загроз, з якими стикаються користувачі та організації. Актуальність проблеми загострюється недостатнім рівнем обізнаності користувачів щодо основних правил цифрової безпеки, зокрема двофакторної аутентифікації, а також відсутністю належної культури кіберзахисту в багатьох компаніях.

Відтак виникає необхідність у підвищенні рівня кіберграмотності, впровадженні сучасних технічних рішень та розбудові системи інформаційної безпеки на всіх рівнях. Для визначення ступеня поінформованості користувачів щодо базових принципів кібербезпеки серед студентів Тернопільського національного педагогічного університету імені Володимира Гнатюка було організовано опитування. В опитуванні взяли участь 62 студенти різного року здобуття вищої освіти. Його результати стали основою для аналізу поточних трендів та викликів у цій галузі.

Кібербезпека в епоху XXI століття – важливе питання, яке стосується державного, так і корпоративного рівнів. На сьогодні, світ стрімко перетворюється завдяки цифровій революції, що радикально змінює «обличчя» кібербезпеки. Сучасний стан свідчить про поглиблення складності атак, розширення спектра нових загроз та велику потрібно у розробці ефективних інструментів для захисту інформаційних активів. Тому, захист даних від несанкціонованого доступу є одним із пріоритетних завдань під час проєктування будь-якої інформаційної системи [1, с. 39].

Значну небезпеку мають кібератаки на бізнес-середовище. Компанії регулярно стикаються з фішинг-атаками, спроби проникнути у свої мережі, і були просочені випадки конфіденційної інформації. Нехтування заходами кібербезпеки може поставити під загрозу репутацію компанії, довіру клієнтів та фінансову стабільність, що робить її важливим компонентом сучасної бізнес-стратегії [2, с. 103–106]. Крім того, кібератаки також можуть призвести до фінансових втрат: примусове припинення роботи, відшкодування збитків або штрафи за недотримання правильного захисту даних.

Студенти також зазнавали різних загроз безпеки в цифровому середовищі. Оскільки вибірка респондентів буде деперсоналізована, охоплювала студентів різного віку та спеціальностей, то з високою достовірністю її результати можна поширити на користувачів інтернету віком 17–21 років (рис. 1).

Рис. 1. Рівень загроз кібербезпеці на студентство

Загрози, на які вказали респонденти, в переважній більшості стосувались фішингових атак та фінансового шахрайства з боку кіберзлочинців. У зв’язку із цим та за запитами студентів ми проаналізували рекомендації з забезпечення інформаційної безпеки від провідних фахівців. Виявлено, що для подолання ризиків використання соціальних мереж та різноманітних сервісів існують численні способи й інструменти захисту, котрі групують на технічні та організаційні.

Технічні методи та засоби захисту інформації містять в собі технологічні рішення, спрямовані на безпосередній захист інформаційних систем та даних:

Системи автентифікації та авторизації: забезпечують контроль доступу до інформаційних ресурсів шляхом перевірки особи користувача та надання прав доступу лише до дозволених ресурсів.

Антивірусний захист: призначений для виявлення та нейтралізації шкідливого програмного забезпечення (ШПЗ), такого як віруси, трояни, шпигунські програми тощо.

Системи захисту даних: забезпечують захист інформації від несанкціонованого доступу, модифікації, знищення або викрадення.

Системи виявлення та запобігання вторгненням (IDS/IPS): використовуються для виявлення спроб несанкціонованого доступу до комп'ютерних мереж та їх блокування.

Мережеві екрани (фаєрволи): здійснюють фільтрацію мережевого трафіку, пропускаючи лише авторизовані з'єднання та блокуючи небезпечні або небажані.

Системи криптографічного захисту: застосовують криптографічні методи для забезпечення конфіденційності, цілісності та автентичності даних [1, с. 52–53].

Слід зауважити, що серед тих, що взяли участь у нашому опитуванні 54,8 % респондентів використовують двофакторну аутентифікацію для захисту своїх акаунтів. Це говорить про те, що понад половину опитаних розуміє значення додаткової безпеки під час авторизації у мережах. Разом з цим, 17,7 % респондентів взагалі не використовують 2FA, що суттєво збільшує ризик зламу чи перехоплення особистої інформації (рис. 2).

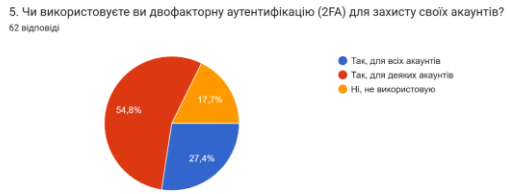

Рис. 2. Використання двофакторної аутентифікації.

Окрім цього 61,3 % респондентів змінюють паролі до своїх акаунтів після виникнення проблеми, тільки 11 % роблять це регулярно, згідно рекомендацій. Водночас 9,7 % змінюють раз у рік, а 17,7 % не змінюють ніколи. 40,3 % ніколи не перевіряють безпечність посилань перед тим, як перейти за ними.

Організаційні заходи передбачають створення чітких політик інформаційної безпеки, розробку планів реагування на кіберінциденти та впровадження внутрішнього контролю за дотриманням норм цифрової безпеки. До обов'язкових заходів належить регулярне оновлення програмного забезпечення, обмеження прав доступу до критичних систем, а також створення резервних копій важливих даних. Слід розуміти, що більшість кібератак відбувається через людський фактор, тому підвищення обізнаності користувачів щодо фішингу, соціальної інженерії та основ кібергігієни істотно знижує ризики. Варто відвідувати тренінги, здійснювати моделювання атак та способів їх усунення, тим самим тестувати власний рівень кіберготовності. На сьогодні розроблено цілий ряд додатків для вивчення основ кібербезпеки [3]. Одним з інструментів вимірювання результатів такого навчання є онлайн гра-симуляція від Української міжбанківської Асоціації членів платіжних систем ЄМА «Здолай шахрая!», де на гравців чекають симуляції

різноманітних видів платіжного шахрайства [4]. Окрім того, в ігровій формі можна дізнатись про наслідки прийнятих рішень, поради щодо виявлення шахрайства та дієві засоби захисту у кожній ситуації. У грі представлено 58 ситуацій, у яких безе участь ігровий агент. За проходження гри учаснику/ці нараховуються бонуси та відмітка про проходження завдання – «Здолано» (рис. 3).

Рис. 3. Фрагмент вікна гри «Здолай шахрая!»

Користувачі в коментарях високо оцінюють гру та її вплив на формування реальних практичних навичок уникнення кібершахрайства.

Проблема кібербезпеки залишається надзвичайно актуальною у час цифрових трансформацій у світі. Щороку збільшується не тільки частота кібератак, але і їх рівень складності. Поліпшення цифрової грамотності, періодичне оновлення систем безпеки та формування відповідального ставлення до захисту даних мусять бути пріоритетними у боротьбі з кіберзагрозами.

Список використаних джерел

1. Аль-Амморі А. Н., Дехтяр М. М., Іщенко Р. М., Клочан А. Є. Методи та засоби захисту інформації. *Системи управління, навігації та зв'язку*, Київ. 2024.

2. Бортник К. Я., Делявський М. В., Кузьмич О. І., Багнюк Н. В., Чернящук Н. Л. Основні загрози безпеці інформаційних систем. *Комп'ютерно-інтегровані технології : освіта, наука, виробництво.* Вип. 41. Луцьк, 2020. С. 137–142.

3. Барна О. В., Ворончак В. І. Ігрові додатки для навчання основ інтернет-безпеки. С. 21–25.

4. ЄМА. Здолай шахрая. URL: https://game.ema.com.ua (дата звернення: 01.04.2025).

ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ В УМОВАХ ДУАЛЬНОЇ ФОРМИ ЗДОБУТТЯ ОСВІТИ: ДОСВІД І ПЕРСПЕКТИВИ

Карабін Оксана Йосифівна
кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
karabin@tnpu.edu.ua
Скасків Ганна Михайлівна
асистент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
skaskiv@fizmat.tnpu.edu.ua

Важливим аспектом модернізації педагогічної освіти є вектор на практико-орієнтованого навчання, що забезпечується через впровадження дуальної форми здобуття освіти. Закон України «Про освіту» (2017), Закон України «Про фахову передвищу освіту» (2019), Закон України «Про вищу освіту» (2014, із змінами), а