Гончарова Ірина Петрівна,
старша викладачка кафедри технологій навчання, охорони праці та дизайну Білоцерківського інституту неперервної професійної освіти

АКТУАЛЬНІ АСПЕКТИ ФОРМУВАННЯ БЕЗПЕЧНИХ ЦИФРОВИХ ПОТОКІВ, ЯК ЛОГІСТИЧНИХ ЕЛЕМЕНТІВ СУЧАСНОГО ОСВІТНЬОГО СЕРЕДОВИЩА

Сучасну освіту неможливо уявити без використання засобів цифрових технологій. Водночас інформаційно-освітнє середовище має потенційні загрози для всіх учасників освітнього процесу, зокрема через наявність у ньому можливостей маніпуляції свідомістю, впливу на психічні та фізіологічні структури особистості, доступності сайтів терористичного та екстремістського характеру тощо. Таким чином, потрібні спеціальні заходи щодо захисту освітнього цифрового середовища від зовнішніх негативних чинників.

Забезпечення цифрової безпеки держави є актуальною задачею сьогодення. Закон України «Про основні засади забезпечення кібербезпеки України», прийнятий Верховною Радою України 5 жовтня 2017 року, визначає онлайн-безпеку (кібербезпеку) як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [1]. Сьогодні у світі вже виникло розуміння того, що проблема безпеки цифрових потоків – це задача, що вимагає скоординованого рішення на всіх рівнях: від сім'ї, закладу освіти, громади до регіонального та міжнародного. Розмаїття небезпек і загроз зростає постійно, зачіпаючи всі можливі дії людини в мережі. Найбільшу загрозу мають приховані активні небезпеки [2, с. 319]. Таке поняття як кібергігієна є надзвичайно актуальним для сьогодення, адже саме розвиток кіберкультури та кібергігієни здобувачів освіти

дозволить попередити небезпеку цифрових потоків інформації, зможе допомогти педагогічній спільноті сформулювати ефективні заходи у відповідь.

Через воєнний стан в Україні більшість здобувачів освіти навчаються дистанційно. Це несе із собою певні кібернебезпеки. До початку активної фази війни, ми постійно бачили в мережі інформацію про взломи сайтів, про крадіжку персональних даних, про постійне відбиття кібератак. Наразі таких повідомлень майже немає в інформаційному полі, однак це зовсім не означає, що кібератаки зупинилися. Російські хакери полюють на нашу особисту інформацію, на персональні дані як наші, так і тих осіб, до яких ми маємо доступ. Тому кібергігієна – це те, про що ми не маємо забувати кожного дня, адже наше життя тісно пов'язане з використанням мережі інтернет [3].

Під кібергігієною розуміють сукупність навичок та знань, що зменшують ризики перебування у мережі. Кожен користувач повинен розуміти, що робота в цифровому просторі несе в собі певний ризик. Усвідомлення цього факту дозволяє уникнути багатьох проблем. Високий рівень розвитку кіберпростору потребує такого ж високого рівня культури користування цим, без перебільшення, науково-технологічним досягненням.

Щоб здобувачі освіти з легкістю засвоювали базові правила цифрової безпеки інформаційних потоків, важливо їм показати, що кібербезпека дійсно є цікавою і важливою, а головне – вона стосується кожного з нас. Для досягнення цієї мети дієво стають у пригоді інструменти індустрії розваг.

У процесі навчання кіберграмотності саме у відеоіграх здобувачі освіти зіткнуться з правдоподібними ситуаціями та будуть поставлені перед тими ж виборами, які доводиться робити і в реальному житті, що безпосередньо вплине на рівень захищеності користувача від кіберзагроз. Це такі актуальні питання, як доцільність використання VPN, підключення до Wi-Fi у громадських місцях, збереження паролів до важливих ресурсів безпосередньо у веб-браузерах, листування з незнайомими дорослими тощо. Прикладом таких ігор може бути Cyber Manhunt (розробник: Aluba Studio) або Hacknet (розробник: Team Fractal Alligator). Подібні ігри успішно виконують свою основну функцію:

демонструють дії зловмисників, вказуючи нас слабкі ланки захисту від таких дій, знайомлять із тим набором навичок, які застосовуються у сфері безпеки інформаційних цифрових потоків.

Онлайн-тренажери створюють ситуації, які максимально наближені до «бойових». Так, у серпні 2022 року кіберполіція Сумщини спільно з громадськими та урядовими організаціями регіону презентували онлайн-гру для дітей «Чемпіони кібербезпеки». Відповідаючи на питання у форматі вікторини, користувачі мають змогу покращити знання з цифрової безпеки та підвищити власний рівень кібергігієни.

Кібергігієна – це фундамент безпеки у цифровому середовищі. Саме тому, з метою підвищення рівня обізнаності учнівської молоді щодо кібербезпеки, формування навичок безпечної поведінки у кіберпросторі ГО «Всеукраїнський громадський центр «Волонтер» спільно з Управлінням протидії кіберзлочинам у м. Києві Департаменту кіберполіції Національної поліції України за підтримки Представництва Дитячого фонду ООН (ЮНІСЕФ) в Україні розроблено онлайн курс для молодих людей, які хочуть знати, як захистити себе та свою інформацію у кіберпросторі (https://cyber.volunteer.kiev.ua/#/). В межах курсу здобувачі освіти знайомляться з поняттям «кібербезпека», захистом персональних даних, дізнаються про лайфхаки щодо убезпечення особистих даних, про те, як з'являється фейкова інформація, які існують фейки, про способи і техніки, що допомагають відрізнити фейкову інформацію від правдивої, про алгоритми самозахисту у цифровому просторі. Під час навчання здобувачі освіти не тільки знайомляться з інформацією, а також виконують практичні завдання.

За даними Cyberedge Group, у 2019 році 78% IT-фахівців повідомляли про кібератаки. Опитування The Myers-Briggs Company дає цифру 64% [4]. Всесвітній економічний форум у 2019 році назвав кібератаки та мережеве шахрайство серед головних проблем, з якими стикається суспільство. 82% опитаних аналітиками форуму погодилися з тим, що витік даних завдає серйозних збитків для їхніх компаній [4].

Для забезпечення захисту персональних даних під час роботи в Інтернет-мережі спеціалісти ESET (міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки для корпоративних і домашніх користувачів) рекомендують дотримуватися основних правил кібергігієни [5]: перевірка безпеки вже існуючих облікових записів електронної пошти та акаунтів в соцмережах (такі веб-сайти як haveibeenpwned.com та breachalarm.com допоможуть з'ясувати, чи був пароль до електронної пошти викрадений зловмисниками); аналіз програм; своєчасне оновлення операційної системи та окремих додатків; створення надійних паролів; використання двофакторної аутентифікації; регулярне резервне копіювання інформації на зовнішній жорсткий диск або у хмару; використання надійного рішення для захисту комп'ютера чи смартфона від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак. Ці основні правила кібергігієни допоможуть користувачам цифрового простору своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації.

Отже, формування основ кібергігієни – процес тривалий і складний, але важливий і необхідний. Інтернет може бути як всесвітньою енциклопедією, яка об'єднує цифрові інформаційні ресурси в усьому світі, так і руйнівним чинником, що таїть у собі конкретні ризики. Завданням педагогів є формувати різнобічну інтелектуальну особистість, високий моральний рівень якої буде гарантією її безпеки в цифровому потоці інформації. Для цього необхідно підвищувати кваліфікацію педагогів з питань цифрової безпеки, щоб вони вміли не тільки оперативно орієнтуватися в цифровому кіберпросторі, а й орієнтували здобувачів освіти на відповідну безпеку перебування в ньому. Нормою є працювати не навздогін, а на випередження. І пам'ятаймо, безпека – понад усе.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України, Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 07.10.2022)

2. В. Ю. Биков, О. Ю. Буров, Н. П. Дементієвська. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, 2019, Том 70, №2, С. 313 – 331.
3. Основні правила кібергігієни. URL: https://erepublic.org.ua/news/osnovni-pravila-kibergigiyeni/ (дата звернення: 07.10.2022)
4. Кибербезопасность с человеческим лицом: как донести проблему до каждого. URL: https://trends.rbc.ru/trends/industry/5fa460199a7947a946d4b37e (дата звернення: 06.10.2022)
5. Основні правила захисту даних — кібергігієна для активного Інтернет-користувача. URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya (дата звернення: 06.10.2022)