КІБЕРБЕЗПЕКА ЯК СКЛАДОВА БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ ЗАКЛАДІВ ОСВІТИ

Гончарова І.П., *старший викладач кафедри технології навчання, охорони праці та дизайну Білоцерківського інституту неперервної професійної освіти ДЗВО «Університет менеджменту освіти» НАПН України*

Пандемія коронавірусу COVID-19, відкритий воєнний напад Росії на Україну обрушили звичні умови життєдіяльності, докорінно змінила наше життя і прискорило перехід на нові цифрові технології та онлайн-сервіси. Протягом останніх років Україна визначила цифрову трансформацію як пріоритетну політику. У 2019 році виконавча влада України презентувала план розвитку цифрової економіки країни, який закликає до прискореного розвитку для переведення української економіки в цифровий формат [1]. Значна увага питанню цифрової трансформації приділена у затвердженій Кабінетом міністрів України Державній стратегії регіонального розвитку на 2021-2027 роки.

Поняття «цифрова трансформація» визнано як найбільш узагальнююче серед таких як: «успішне підприємництво, безпечне середовище для життя, здоров'я та благополуччя громадян» тощо. Міністерство цифрової трансформації до 2024 року визначило наступні цілі [1]:

– переведення 100 % соціально значимих послуг у електронний вигляд;

– 95 % транспортної інфраструктури, населених пунктів та їхні соціальні об’єкти мають мати доступ до високошвидкісного Інтернету;

– 6 млн. українців мають бути залучені до програми розвитку цифрових навичок;

– доля ІТ-продукту у ВВП країни має складати не менше 10 %.

Особлива увага в системі освіти приділяється цифровій трансформації освітнього процесу, як провідному напряму підвищення результативності навчання, одному з основних факторів підвищення якості освіти. Стрімкий розвиток цифрових технологій та нового інструментарію призвело до їх активного впровадження в освітній процес та професійну практику викладача. Сучасні педагогічні технології навчання висувають на перше місце не тільки

задачі інформування, навчання здобувачів освіти, але й їх здатність вирішувати проблеми безпеки життєдіяльності у навчальних та життєвих ситуаціях.

Проблеми безпеки життєдіяльності людини – одні з найактуальніших проблем людства, у світі цифрових технологій безпосередньо пов'язані з його виживанням в умовах цифрового технологічного прогресу. Новий інструментарій у вигляді Інтернету, комп'ютера, приладів мобільного зв'язку таїть у собі численні небезпеки та ризики. Кожен користувач глобальної мережі повинен розуміти, що робота в цифровому просторі несе в собі певний ризик. Усвідомлення цього факту дозволяє уникнути багатьох проблем.

Відомо, що в інтернеті давно не існує такого поняття, як анонімність. Тому правоохоронні структури з легкістю можуть визначити місцезнаходження будь-якого користувача соціальних мереж, знаючи IP-адресу комп'ютера, з якого надіслано повідомлення про «замінування будівлю, аеропорт тощо». Ще одна з небезпек, яка може підстерігати в мережі – це кібербулінг, цькування за допомогою відкритих коментарів недоліків особистості користувача, показ злісних тролів, нав'язування платних ігор тощо. Захоплення комп'ютерними іграми може спричинити небезпечні для суспільства проблеми кримінального характеру, коли в людей не вистачає грошей на гру, і вони йдуть на злочин. Щоб подібних ризиків не допустити, зі здобувачами освіти потрібно проводити заняття з кібербезпеки, на яких потрібно навчити їх відрізняти фейкові відомості від правдивих і негайно закривати спливаючі вікна. Високий рівень розвитку кіберпростору потребує такого ж високого рівня культури користування цим, без перебільшення, науково-технологічним досягненням. Цифрова безпека є викликом сучасності. Розвиток кіберкультури та кібергігієни здобувачів освіти дозволить попередити кібернебезпеку, може допомогти педагогічній та батьківській громадськості сформулювати ефективні заходи у відповідь.

У сучасних реаліях володіння базовими правилами інформаційної безпеки так само необхідно, як, наприклад, знання основ здорового життя чи пожежної безпеки. Причому формувати навички так званої кібергігієни потрібно з раннього віку. Розповідати дітям про правила безпечної поведінки в інтернеті потрібно, як тільки юні користувачі отримують доступ до цифрового пристрою.

Подібно до того, як дитина дізнається про правила безпечного переміщення містом, коли вона починає самостійно ходити до школи. В кіберпросторі необхідно використовувати ті самі правила безпеки життєдіяльності, що й в звичайному житті. Наприклад, мити руки, не спілкуватися з незнайомими людьми, не смітити, бути ввічливими, перевіряти інформацію перед тим, як купувати продукти харчування тощо. Знаходячись у кіберпросторі потрібно пам'ятати, що доступність до людини як об'єкта збільшилася. Тобто, з одного боку, утворився новий цікавий простір, а з іншого – доступність для всіх.

Програму вивчення в школі предмету «Основи здоров'я», у закладах професійної освіти предмету «Охорона праці та безпека життєдіяльності» необхідно розширити розділом вивчення основ кібербезпеки. Значимість інформаційної безпеки постійно зростає вже кілька років. Після атак на енергооб'єкти та урядові сайти, після витоків з оборонного сектору та масштабних хакерських атак на банки та великі компанії ні в кого не залишилося сумнівів, що ця сфера безпеки не поступається значущості. Шахраї активно використовують різні методи соціальної інженерії для крадіжки персональних даних, здійснення фінансових шахрайств. Загальносвітовий інтерес до цієї теми дозволив заразити сотні тисяч комп'ютерів через фішингові сайти та розсилки. Маса інформаційних фейків теж несе у собі загрозу безпеці. Ніщо так не вчить фінансової грамотності, як втрата грошей, і ніщо так не вчить кіберграмотності, як витік персональних даних, зламування акаунту і знову ж таки втрата грошей.

Всі учасники освітнього процесу повинні розуміти вплив кіберпростору на свою особистість, розуміти відповідальність перед собою та суспільством за власну поведінку та її (можливі) глобальні наслідки, знання та розуміння небезпек кіберпростору [3].

Як визначається Законом «Про основні засади забезпечення кібербезпеки України» [4], «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних».

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.

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.

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 вводити в освітні програми курс з основ кібербезпеки. Нормою є працювати не навздогін, а на випередження. І пам’ятаймо, безпека – понад усе.

Список використаних джерел

1. Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному? Поліський фонд міжнародних та регіональних досліджень, 2020 р. URL: http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf (дата звернення 22.10.2022).

2. Державної стратегії регіонального розвитку на 2021-2027 роки https://zakon.rada.gov.ua/laws/show/695-2020-%D0%BF#Text (дата звернення 24.10.2022).

3. Горбенко А. А. Кібербезпека освітнього середовища в умовах карантину URL: https://conf.ztu.edu.ua/wp-content/uploads/2020/05/94.pdf (дата звернення 23.10.2022).

4. Закон No 2163-VIII «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради), No 45, с. 403, 2017.

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 24.10.2022).