ОКСАНА КРАВЧИНА
науковий співробітник
відділу компаративістики інформаційно-освітніх інновацій
Інститут цифровізації освіти НАПН України, м.Київ

МЕТОДИ КІБЕРГІГІЄНИ ДЛЯ ОРГАНІЗАЦІЇ БЕЗПЕЧНОГО ДИСТАНЦІЙНОГО НАВЧАННЯ У ШКОЛІ

Ключові слова: *цифрові технології, кібергігієна, безпека*

Впровадження та застосування цифрових технологій є важливим серед численних інноваційних напрямків розвитку навчання і освіти в цілому. Розробляється безліч інформаційних сервісів, які вчитель може впроваджувати і ефективно використовувати в навчальному процесі та для свого професійного розвитку. Багато шкіл користуються такими цифровими ресурсами, але не займаються питаннями захисту даних. Але захист інформації є дуже важливим, оскільки часто використовуються особисті дані учнів та вчителів, навчальні матеріали та результати навчання. Тому важливими для освітян є питання безпеки в інтернеті, що є особливим компонентом ширших ідей кібербезпеки та комп'ютерної безпеки, що включає в себе такі складові як: безпека браузера, поведінка в Інтернеті, безпека мережі. Оскільки на сьогодні існує багато ризиків, серед яких COVID-19 та військові дії, що спричинило запровадження дистанційної форми навчання, тобто значну частину свого часу освітяни

проводить в Інтернеті, і важливо розуміти, які загрози інтернет-безпеці існують. Серед таких загроз можна виділити такі, як:

- злом, це коли сторонні неавторизовані користувачі отримують доступ до комп'ютерних систем, облікових записів електронної пошти або веб-сайтів;
- віруси або зловмисне програмне забезпечення, що може нанести шкоду вашим даним або зробити системи вразливими до інших загроз;
- крадіжка особистих даних, коли злочинці викрадають особисті дані та фінансову інформацію.

Слід зауважити, що також існують різні види інтернет-атак, серед яких можна виділити такі як:

- фішинг – це кібератака, яка включає замасковані електронні листи, задача – обдурити людей, щоб вони передали свою особисту інформацію або завантажили шкідливе програмне забезпечення;
- злом і віддалений доступ, який хакери намагаються використати для викрадання конфіденційної інформації та даних користувачів, оскільки програмне забезпечення для віддаленого доступу дозволяє користувачам отримувати доступ до комп'ютера та керувати ним віддалено (актуально при пандемії та воєнному стані, коли багато людей працюють віддалено). Протокол, який дозволяє користувачам дистанційно керувати комп'ютером, підключеним до Інтернету, називається протоколом віддаленого робочого столу або RDP. Хакери використовують різні методи для використання вразливостей RDP, поки не отримають повний доступ до мережі та її пристроїв. Вони можуть здійснювати крадіжку даних самостійно або продавати облікові дані в темній мережі;
- шкідливе програмне забезпечення— це набір «зловмисного» та «програмного забезпечення» (віруси, хробаки, трояни тощо), які хакери використовують для руйнування та крадіжки конфіденційної

інформації. Будь-яке програмне забезпечення, призначене для пошкодження комп’ютера, сервера чи мережі, можна назвати шкідливим.

- зловмисна реклама — це онлайн-реклама, яка розповсюджує шкідливе програмне забезпечення, оскільки інтернет-реклама — це складна екосистема (включає веб-сайти видавців, біржі реклами, рекламні сервери, мережі ретаргетингу), яку зловмисники використовують для розміщення шкідливого коду у місцях, які видавці та рекламні мережі не завжди виявляють, а користувачі Інтернету, які взаємодіють із шкідливою рекламою, можуть завантажити шкідливе програмне забезпечення на свій пристрій або перенаправляються на шкідливі веб-сайти;
- програми-вимагачі – це зловмисне програмне забезпечення, яке не дозволяє вам використовувати свій комп’ютер або отримувати доступ до певних файлів на вашому комп’ютері, якщо не сплачено викуп (поширюється як троян);
- ботнет – це мережа комп’ютерів, які навмисно заражаються шкідливим програмним забезпеченням для виконання автоматизованих завдань в Інтернеті без дозволу чи відома власників комп’ютерів та може використовувати їх для здійснення шкідливих дій (створення підробленого інтернет-трафіку на сторонніх веб-сайтах для фінансової вигоди, використання потужності вашого комп’ютера для допомоги в атаках розподіленої відмови в обслуговуванні (DDoS) для закриття веб-сайтів, розсилка спаму мільйонам користувачів Інтернету, здійснення шахрайства та крадіжки особистих даних, атаки на комп’ютери та сервери);
- загрози Wi-Fi у громадських місцях та вдома, оскільки безпека в цих мережах – у кав’ярнях, торгових центрах, аеропортах, готелях, ресторанах тощо – часто слабка або відсутня, тобто кіберзлочинці та викрадачі

особистих даних можуть стежити за тим, що ви робите в Інтернеті, і викрадати паролі та особисту інформацію користувачів.

При дистанційному навчанні всі вищеперелічені загрози можуть виникнути, тому персонал навчального закладу має вміти захистити свої дані та інформацію про всіх учасників освітнього процесу в інтернеті. Розглянемо деякі шляхи забезпечення кібергігієни в інтернеті, серед яких можна виділити так як:

- багатофакторна автентифікація (MFA) – це метод автентифікації, який просить користувачів надати два або більше методів перевірки для доступу до облікового запису в Інтернеті (наприклад: додатковий одноразовий пароль, який сервери аутентифікації веб-сайту надсилають на телефон або адресу електронної пошти користувача; відповіді на питання особистої безпеки; відбиток пальця або інша біометрична інформація, як-от розпізнавання голосу чи обличчя тощо). Багатофакторна аутентифікація знижує ймовірність успішної кібератаки. Також можна використати програми аутентифікації, наприклад Google Authenticator і Authy;
- використання брандмауеру, програми чи пристрою, що здійснює захист комп'ютерних мереж, вони блокують небажаний трафік, а також можуть допомогти заблокувати шкідливе програмне забезпечення від зараження комп’ютера (часто ваша операційна система та система безпеки мають попередньо встановлений брандмауер, але бажано переконатися, що ці функції ввімкнено, а ваші налаштування налаштовані на автоматичний запуск оновлень, щоб максимально підвищити безпеку в Інтернеті);
- уважно вибраний браузер, який буде безпечним та захистить від злому даних;
- створення надійного паролю або використання безпечного менеджера паролів (надійний пароль має бути: довгим, щонайменше з 12 символів; поєднувати символи, тобто великі і малі літери, символи і цифри; уникати простого використання порядкових номерів («1234») або особистої

інформації, такої як дата вашого народження чи ім’я домашньої тварини; зберігати свої паролі конфіденційними та не повідомляйте їх іншим і не записувати їх; не використовувати один і той самий пароль для всіх своїх облікових записів і регулярно змінювати їх);

- застосовувати антивірусну програму та постійно оновлювати її, вона має вирішальне значення для забезпечення конфіденційності та безпеки в інтернеті, оскільки захищає від різних типів інтернет-атак і захищає дані в Інтернеті.

Необхідно зазначити також, що безпека в Інтернеті для дітей має вирішальне значення, оскільки вони мають бути захищені від шкідливого чи невідповідного вмісту та контактів, а також від шкідливого програмного забезпечення чи атак, а навчання дітей кібергігієні може допомогти захистити їх.

Щодо забезпечення кібергігієни для дистанційного навчання необхідно:

- мати чіткі вказівки, коли існує безліч інструментів електронного навчання, які можуть зацікавити вчителів необхідно переконатися, що будь-який навчальний ресурс, який використовується є безпечним;
- навчати учнів, вчителів та інших працівників школи безпечному поводженню в інтернеті;
- постійно оновлювати паролі та використовувати методи багатофакторної аутентифікації, щоб зменшити ризики викрадення паролів.
- визначити потенційні загрози, оскільки дистанційне навчання створює унікальні проблеми безпеки для навчання, а саме викладачі та учні використовують свої персональні пристрої вдома та існує ймовірність того,

що користувачі працюють у незахищеній мережі або забувають оновлювати свої пристрої та програмне забезпечення.

Слід зазначити, що кібергігієна має бути включена в плани дистанційного навчання. Це є запорукою безпеки та дотримання конфіденційності, які сприятимуть навчанню.

На сьогодні існують онлайн ресурси в Україні, які навчають кібергігієні. Одним з таких ресурсів є освітній серіал «Основи кібергігієни», який розміщено на Національній онлайн-платформі для розвитку цифрової грамотності «Дія.Цифрова Освіта**»** [1]. Серіал було створено в рамках проекту «Посилення спроможностей українських державних органів у сфері кібергігієни та кібербезпеки», що реалізується Координатором проектів ОБСЄ в Україні за підтримки Міністерства закордонних справ і міжнародного розвитку Великобританії та Федерального міністерства закордонних справ Німеччини та знайомить слухачів із базовими принципами кібергігієни та типовими алгоритмами дій у разі виявлення ознак інформаційних атак на реальних прикладах.

Наступним ресурсом є освітній онлайн-курс «Основи кібергігієни» [2] який проходить відповідно до Плану всеукраїнських і міжнародних організаційно-масових заходів з дітьми та учнівською молоддю на 2022 рік (за основними напрямами позашкільної освіти), затвердженого наказом Міністерства освіти і науки України від 15 грудня 2021 № 1379 Національним центром «Мала академія наук України» в рамках Всеукраїнського освітнього проекту «EduLab». Курс розраховано на здобувачів освіти 8-11 класів закладів загальної середньої освіти, вихованців закладів позашкільної освіти. Основна мета, це формування уявлення про небезпеки у віртуальному просторі та правила безпечного користування інтернетом. Курс знайомить з основними загрозами у віртуальному просторі; вразливістю програмного забезпечення; основними способами генерування та зберігання надійних паролів; правилами безпечного користування інтернетом, електронною поштою та месенджерами. Навчання

здійснюється з використанням дистанційних технологій у режимі онлайн на платформах «Google Classroom» і «Zoom».

Слід зазначити, що кібергігієна має бути включена в плани дистанційного навчання. Це є запорукою безпеки та дотримання конфіденційності, які сприятимуть навчанню.

Список використаних джерел:

1. Національна онлайн-платформа для розвитку цифрової грамотності «Дія. Цифрова Освіта». URL:https://osvita.diia.gov.ua/courses/cyber-hygiene
2. Онлайн-курс. «Основи кібергігієни». URL:https://cybereducation.org/
3. O. V. Ovcharuk, I. V. Ivaniuk, O. Y. Burov, M. V. Marienko, N. V. Soroko, O. O. Gritsenchuk, O. Y. Kravchyna, The practical experience of the use of digital learning resources by Ukrainian teachers to ensure the sustainable development and democratization of education process, in: S. Semerikov, V. Osadchyi, O. Kuzminska (Eds.), Proceedings of the Symposium on Advances in Educational Technology, AET 2020, University of Educational Management, SciTePress, Kyiv, 2022.