УДК 004.056:316.77

ФОРМУВАННЯ КУЛЬТУРИ ЦИФРОВОЇ ГІГІЄНИ

Косенко М.А., Пронюк Г.В.
e-mail: mykola.kosenko@nure.ua
Харківський національний університет радіоелектроніки, кафедра БІ
м. Харків, Україна

In the modern digital world, cybersecurity is essential for protecting personal information. This article explores common cyber threats such as phishing, malware, password breaches, and DDoS attacks. It highlights key cybersecurity measures, including two-factor authentication, strong passwords, antivirus software, encryption, and regular updates. The importance of digital hygiene practices is also emphasized. Additionally, international cybersecurity regulations, including GDPR, HIPAA, and Ukrainian cybersecurity laws, are discussed.

Сучасний світ неможливо уявити без цифрових технологій. Ми спілкуємося в соціальних мережах, здійснюємо покупки онлайн, працюємо у віддаленому форматі та зберігаємо важливі документи в хмарних сховищах. Проте разом із комфортом цифрового простору приходять і ризики. Кібербезпека стає ключовою умовою захисту особистої інформації, а дотримання правил цифрової гігієни набуває статусу необхідності [1].

Однією з найпоширеніших загроз у кіберпросторі є фішинг — метод шахрайства, за допомогою якого зловмисники створюють підроблені сайти чи надсилають електронні листи, що імітують офіційні запити [2]. Користувач, не підозрюючи небезпеки, вводить свої персональні дані, які одразу потрапляють у руки злочинців. Так само небезпечними є шкідливі програми (малвар), які можуть проникнути на пристрої, викрасти дані або навіть заблокувати доступ до них із метою вимагання викупу.

Ще одним вектором атак є злам паролів [2]. Використання слабких або повторюваних паролів на різних платформах створює ідеальні умови для кібератак. Крім того, методи соціальної інженерії дозволяють зловмисникам маніпулювати людьми, змушуючи їх самостійно передавати особисті дані. Не можна ігнорувати й DDoS-атаки, коли хакери навмисно перевантажують сервери, виводячи з ладу сайти та онлайн-сервіси.

Для протидії таким загрозам існує низка ефективних методів кібербезпеки. Двофакторна аутентифікація (2FA) забезпечує додатковий рівень захисту, вимагаючи підтвердження входу за допомогою SMS або спеціального застосунку. Створення складних та унікальних паролів для кожного сервісу значно ускладнює роботу зловмисників. Використання антивірусного програмного забезпечення та файрволів дозволяє вчасно виявляти та блокувати загрози. Надійне шифрування даних гарантує конфіденційність інформації навіть у разі її перехоплення. Важливу роль

відіграє й регулярне оновлення програмного забезпечення, оскільки кожна нова версія усуває можливі вразливості.

Однак, окрім технічних засобів, важливо дотримуватися цифрової гігієни. Це сукупність правил, що допомагають мінімізувати ризики кібератак. Зокрема, необхідно бути обережними під час відкриття електронних листів від невідомих відправників та уникати переходу за підозрілими посиланнями. Використання різних паролів для кожного облікового запису та їхнє регулярне оновлення допомагає запобігти компрометації акаунтів. Регулярне резервне копіювання важливих даних дозволяє уникнути їхньої втрати у разі атак. Використання VPN при підключенні до публічних Wi-Fi-мереж забезпечує захист переданих даних від перехоплення.

На рівні міжнародного законодавства існують документи, що регулюють питання кібербезпеки. Одним із ключових нормативних актів є Загальний регламент про захист даних (General Data Protection Regulation, GDPR), прийнятий Європейським Союзом у 2016 році [3]. Він встановлює суворі вимоги до обробки персональних даних і передбачає значні штрафи за порушення. У США діє Закон про портативність і підзвітність медичного страхування (HIPAA), який регулює захист конфіденційної медичної інформації. У сфері фінансової безпеки важливу роль відіграє Директива ЄС PSD2, що впроваджує заходи для захисту онлайн-платежів. В Україні діє Закон "Про основи забезпечення кібербезпеки України", який визначає правові засади кіберзахисту на державному рівні.

Таким чином, кібербезпека є невід’ємною складовою цифрової гігієни. Використання сучасних методів захисту, обачливість у мережі та знання основних принципів безпеки допомагають зменшити ризики та захистити особисті дані. Дотримання основних принципів безпеки в мережі дозволяє мінімізувати ризики та зберігати конфіденційність інформації у цифровому просторі. Важливо не тільки використовувати технічні засоби захисту, а й формувати культуру безпечного користування цифровими ресурсами, що є ключовим фактором у боротьбі з кіберзлочинністю в сучасному інформаційному суспільстві.

Список використаних джерел:

1. Збітнєв Д.С., кер. Пронюк Г.В. Інтернет безпека: як захистити свої данні та своє життя в онлайн просторі // 27-го Міжнарод. Молодіж. форум «Радіоелектроніка та молодь у XXI столітті», 10-12 травня 2023. – Т.2. – С. 130-131.

2. European Union Agency for Cybersecurity (ENISA). Cyber Hygiene Practices. [Електронний ресурс]. – Режим доступу: https://www.enisa.europa.eu/topics/cyber-hygiene.

3. General Data Protection Regulation (GDPR) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/eli/reg/2016/679/oj.