енергетики та промисловості [1]. Еволюція кіберзагрози вимагає відмови від застарілих підходів щодо ізольованості мережевих мереж і переходу до комплексних систем активного захисту на базі принципів Zero Trust, глибокого моніторингу трафіку та регулярного аудиту вразливостей [3]. Подальші дослідження у цьому напрямі мають бути спрямовані на розробку інтелектуальних систем виявлення аномалій на основі штучного інтелекту, здатних запобігати деструктивним кібератакам у режимі реального часу.

Список використаних джерел

1. Кузнецов С. В., Бондаренко О. М. Кібербезпека критичної інфраструктури та автоматизованих систем управління : монографія. Київ : Техніка, 2024. 245 с.

2. Сдіховська О. Є., Бєлоусов В. С. Захист інформації в автоматизованих системах управління технологічними процесами. Системи управління, навігації та зв'язку. 2025. Вип. 2 (72). С. 112–118.

3. Guide to Operational Technology (OT) Security : NIST Special Publication 800-82 Rev. 3 / National Institute of Standards and Technology. 2023. 250 p.

4. Byres E., Lowe J. The Myths and Facts of Secure SCADA Networks. Proceedings of the 5th Annual IEEE Information Assurance Workshop. 2024. P. 38–45.

УДК 004.056

КІБЕРБЕЗПЕКА ТА ЦИФРОВА ГІГІЄНА

Максим Дякунчак

Миколаївський національний аграрний університет, м. Миколаїв, Україна

Науковий керівник: Л. О. Борян,
старший викладач Миколаївський національний аграрний університет

Цифрові технології стали невід’ємною частиною повсякденного життя людини. Інтернет використовується для навчання, спілкування, роботи, здійснення покупок, користування банківськими та державними сервісами. Водночас активне використання цифрових ресурсів супроводжується зростанням кількості кіберзагроз. Однією з найпоширеніших є фішинг - спосіб шахрайства, за якого зловмисники намагаються змусити користувача добровільно передати конфіденційну інформацію, зокрема паролі, коди підтвердження або банківські дані. Тому кібербезпека та цифрова гігієна мають бути важливою складовою поведінки кожного користувача.

Цифрова гігієна - це сукупність повсякденних правил і звичок, спрямованих на безпечне використання цифрових пристроїв, сервісів та інформації. Її основою є відповідальне ставлення до власних облікових записів і персональних даних. Насамперед користувачеві необхідно створювати складні та унікальні паролі для різних сервісів. Використання одного пароля на декількох сайтах збільшує ризик компрометації одразу кількох облікових записів. Для додаткового захисту доцільно використовувати багатофакторну автентифікацію, якщо вона доступна.

Важливою складовою цифрової гігієни є також своєчасне оновлення операційної системи, браузера та встановлених програм. Оновлення можуть містити виправлення вразливостей, які потенційно можуть бути використані зловмисниками. Не менш важливо встановлювати програми лише з надійних джерел, перевіряти дозволи, які надаються застосункам, та не відкривати підозрілі файли.

Особливу увагу слід приділяти протидії фішингу. Фішингові повідомлення можуть надходити електронною поштою, у соціальних мережах, месенджерах або у вигляді SMS. Зловмисники часто використовують повідомлення про нібито заблокований акаунт, проблеми з оплатою, необхідність підтвердити особу або отримати винагороду. Для підвищення довіри вони можуть копіювати логотипи, стиль оформлення та назви відомих компаній.

Перед переходом за посиланням потрібно перевірити адресу вебсайту та переконатися, що вона відповідає справжньому домену сервісу. Не слід вводити пароль, реквізити платіжної картки або

коди з SMS на сторінках, відкритих із підозрілих повідомлень. Якщо повідомлення викликає сильне відчуття терміновості, страх або обіцянку значної вигоди, це додатковий привід зупинитися та перевірити інформацію через офіційний сайт або інший незалежний канал зв'язку.

Безпека даних передбачає не лише захист паролів, а й обережне поводження з персональною інформацією. Не варто без потреби публікувати у відкритому доступі номер телефону, адресу проживання, документи, фотографії банківських карток та інші відомості, які можуть бути використані для шахрайства. Під час користування соціальними мережами варто перевіряти налаштування приватності та контролювати, яку інформацію можуть бачити сторонні люди.

Корисною практикою є регулярне резервне копіювання важливих файлів. Резервні копії дають змогу відновити інформацію у випадку втрати пристрою, пошкодження файлів або зараження шкідливим програмним забезпеченням. Важливі дані також бажано захищати блокуванням пристрою, шифруванням та іншими доступними засобами безпеки.

Освітнє середовище також є важливою сферою, у якій необхідно формувати навички цифрової безпеки. Під час навчання здобувачі освіти щодня використовують електронну пошту, освітні платформи, хмарні сховища, відеоконференції та месенджери. Злам облікового запису студента або викладача може призвести до втрати навчальних матеріалів, розголошення персональних даних чи поширення шкідливих посилань серед інших учасників освітнього процесу.

Для студентів особливо важливо вміти розпізнавати фішингові повідомлення, які можуть маскуватися під повідомлення адміністрації закладу освіти, викладача або електронної освітньої платформи. Наприклад, користувача можуть попросити терміново перейти за посиланням для підтвердження навчального акаунта, отримання оцінки, доступу до матеріалів або зміни пароля. Перед виконанням таких дій необхідно перевіряти адресу відправника та домен сайту, а сумнівні повідомлення — уточнювати через офіційні канали.

Важливу роль відіграє і цифрова культура закладу освіти. Студенти та працівники мають дотримуватися правил роботи з персональними даними, не передавати іншим особам паролі та коди підтвердження, використовувати блокування пристроїв і своєчасно встановлювати оновлення. Формування таких навичок у процесі навчання допомагає не лише захистити освітні ресурси, а й підготувати молодь до безпечної роботи з інформаційними технологіями у професійній діяльності.

Отже, кібербезпека значною мірою залежить не тільки від технічних засобів, а й від поведінки самого користувача. Дотримання правил цифрової гігієни, використання унікальних паролів і багатофакторної автентифікації, регулярне оновлення програм, обережність із посиланнями та повідомленнями, а також захист персональних даних дають змогу суттєво зменшити ризик стати жертвою кіберзлочинців. Формування таких звичок є простим і водночас важливим кроком до безпечного використання цифрового середовища.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України. Рекомендації щодо безпеки в цифровому середовищі : вебсайт. URL: https://cip.gov.ua (дата звернення: 08.10.2026).

2. Національний банк України. Правила безпечних безготівкових розрахунків та захисту платіжних даних : вебсайт. URL: https://bank.gov.ua (дата звернення: 08.10.2026).

3. CERT-UA. Рекомендації з кібербезпеки та протидії фішингу / Державний центр кіберзахисту : вебсайт. URL: https://cert.gov.ua (дата звернення: 08.10.2026).

4. Cybersecurity and Infrastructure Security Agency (CISA). Phishing Guidance: Stopping the Attack Cycle : website. URL: https://www.cisa.gov (accessed: 08.10.2026).