Дерипаско А.
студентка юридичного факультету
Західноукраїнського національного університету.
Науковий керівник: доктор юридичних наук, доцент,
професор кафедри теорії права та конституціоналізму
Західноукраїнського національного університету
Колесніков А. П.

КІБЕРЗАГРОЗИ ТА ЕФЕКТИВНІ СПОСОБИ ЗАХИСТУ ОСОБИСТИХ ДАНИХ У СУЧАСНОМУ ЦИФРОВОМУ ПРОСТОРІ

У епоху глобальної цифровізації, коли інформаційні технології проникли в усі сфери людської життєдіяльності – від особистого спілкування та навчання до банківських операцій і державного управління – безпека віртуального простору набула статусу одного з найважливіших елементів загальної безпеки особистості. Персональні дані перетворилися на надцінний ресурс, який у сучасному світі часто прирівнюють до цифрової валюти. Відповідно, стрімко зростає і кількість загроз, спрямованих на викрадення, компрометацію або несанкціоноване використання цієї інформації. Розуміння природи кіберзагроз, механізмів їхньої дії та методів протидії їм є базовою вимогою для кожної людини, яка користується перевагами цифрового суспільства.

Кіберзагрози постійно еволюціонують, стаючи дедалі витонченішими, масованішими та складнішими для виявлення. Зловмисники використовують широкий спектр технічних і психологічних інструментів для отримання доступу до приватних систем користувачів. Сьогодні можна виділити кілька ключових категорій загроз, які становлять найбільшу небезпеку для пересічних громадян та професійних спільнот.

Соціальна інженерія є одним із найефективніших методів атаки, оскільки вона спрямована не на технічні вразливості програмного забезпечення, а на людський фактор – неуважність, довіру, страх або цікавість. Найпоширенішим її проявом є фішинг, зловмисники створюють точні копії легітимних сайтів (банківських установ, поштових сервісів, державних платформ або соціальних мереж) і змушують користувача ввести туди свої логіни, паролі чи дані платіжних карток. Це може відбуватися через фейкові електронні листи, SMS-повідомлення (смішинг) або повідомлення в месенджерах із закликами терміново «підтвердити акаунт», «отримати фінансову допомогу» чи «скасувати підозрілу транзакцію». До цієї групи входить широкий спектр шкідливих програм, кожна з яких виконує специфічні завдання в системі жертви. Особливе місце посідають віруси-вимагачі (Ransomware), які шифрують усі файли на пристрої та вимагають викуп у криптовалюті за надання ключа дешифрування. Не менш небезпечними є шпигунські програми (Spyware), які непомітно збирають інформацію про дії користувача,

фіксують натискання клавіш та передають конфіденційні дані на сервери зловмисників, а також троянські програми, які маскуються під робоче середовище, але відкривають хакерам повний віддалений доступ до системи.

Також використання публічних, незахищених Wi-Fi мереж у кафе, готелях, транспорті чи парках створює ідеальні умови для проведення атак типу «людина посередині» (Man-in-the-Middle). Хакери можуть перехоплювати весь незашифрований трафік, який проходить через таку точку доступу, отримуючи доступ до особистих повідомлень, паролів та сесій авторизації в реальному часі.

Статистичні дослідження у сфері кібербезпеки свідчать, що понад 85% успішних зламів та витоків інформації пов'язані саме з людським фактором – низьким рівнем цифрової грамотності, використанням простих паролів або банальною неуважністю при роботі з електронними ресурсами.

Для побудови надійного захисту необхідно чітко усвідомлювати, які саме слабкі місця у нашій повсякденній цифровій поведінці стають мішенню для кіберзлочинців. Зазвичай успіх атаки зумовлений комбінацією кількох факторів, а саме- використання одного й того самого пароля (або його незначних варіацій) для десятка різних сайтів призводить до того, що злам одного другорядного форуму відкриває хакерам доступ до основної пошти, соціальних мереж та навіть онлайн-банкінгу жертви через метод підбору облікових даних. Розробники операційних систем (Windows, Android, iOS) та додатків регулярно випускають патчі безпеки, які закривають виявлені технічні вразливості. Відтермінування оновлень залишає «діри» в системі, які зловмисники можуть експлуатувати автоматизовано. Якщо захист облікового запису тримається лише на комбінації логін-пароль, то будь-який витік бази даних сайту автоматично означає втрату контролю над акаунтом користувача.

Користувачі часто публікують у соцмережах інформацію, яка використовується для підтвердження особи або як відповіді на секретні питання (дівоче прізвище матері, кличка першої домашньої тварини, локації, дати народження родичів), що полегшує завдання для цільового фішингу. Захист особистих даних не повинен бути одноразовою дією, це – безперервний процес, що вимагає формування стійких навичок цифрової гігієни. Сучасні стандарти безпеки пропонують чіткий алгоритм дій для мінімізації ризиків.

Надійний пароль повинен складатися щонайменше з 12-16 символів, включати великі та малі літери, цифри та спеціальні знаки. Оскільки запам'ятати десятки таких комбінацій неможливо, стандартною практикою є використання менеджерів паролів (наприклад, Bitwarden, Keepass, 1Password), які надійно шифрують базу даних. Обов'язковим кроком є активація двофакторної автентифікації (2FA). При цьому варто надавати перевагу спеціальним додаткам-автентифікаторам (Google

Authenticator, Microsoft Authenticator) або апаратним ключам безпеки (YubiKey), оскільки перехоплення кодів через SMS є технічно можливим через атаку на SIM-карту. На кожному персональному пристрої має бути активоване автоматичне оновлення операційної системи та встановлений надійний, ліцензійний антивірусний захист з актуальними базами даних. При підключенні до будь-яких публічних Wi-Fi мереж критично важливо використовувати надійні VPN-сервіси (Virtual Private Network), які створюють зашифрований тунель для всього інтернет-трафіку, унеможливлюючи його перехоплення третіми особами.

Також на рівні пристроїв варто вимикати функції автоматичного підключення до відкритих мереж Wi-Fi та Bluetooth, коли вони не використовуються.

Кожен користувач повинен виробити в собі здоровий цифровий скептицизм. Перед кліком по будь-якому посиланню в листі чи повідомленні необхідно ретельно перевіряти адресу відправника (зловмисники часто змінюють одну літеру в домені, наприклад, corn-bank замість core-bank). Якщо повідомлення містить елементи психологічного тиску (погрози заблокувати рахунок, вимоги терміново переказати кошти), варто самостійно зв’язатися з організацією через її офіційні контакти, вказані на офіційному сайті, а не використовувати номери чи посилання з отриманого повідомлення. Одним із найефективніших засобів нейтралізації наслідків атак вірусів-вимагачів чи технічних збоїв є регулярне створення резервних копій важливої інформації. Рекомендується дотримуватися класичного правила «3-2-1»: зберігати щонайменше 3 копії даних, на 2 різних типах носіїв (наприклад, локальний жорсткий диск та хмарне сховище), причому 1 копія повинна зберігатися географічно в іншому місці або на повністю ізольованому від мережі фізичному носії, який підключається лише на час копіювання.

Кіберзагрози є невід’ємною частиною сучасної цифрової реальності, і повністю уникнути взаємодії з ними неможливо. Проте рівень безпеки особистих даних майже на сто відсотків залежить від культури поведінки самого користувача в Інтернеті. Впровадження базових інструментів захисту – складних унікальних паролів, двофакторної автентифікації, регулярних оновлень програмного забезпечення та резервного копіювання у поєднанні з постійним розвитком критичного мислення та цифрової грамотності – дозволяє створити потужний багаторівневий захист, здатний успішно протистояти переважній більшості сучасних кібератак.

Список використаних джерел

1. Департамент кіберполіції Національної поліції України : офіційний сайт. URL: https://cyberpolice.gov.ua

2. Колесніков А.П. Legal tech в Україні в умовах глобальної диджиталізації. *Наукові записки. Серія: Право*. 2024. № 16. С. 98-102.

3. Колесніков А.П., Зяйлик М.Ф. Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею. Актуальні проблеми правознавства. 2017. № 5. С. 26-29.
4. Команда реагування на комп'ютерні надзвичайні події України (CERT-UA) : офіційний сайт / Держспецзв’язку. URL: https://cert.gov.ua
5. Cybersecurity and Infrastructure Security Agency (CISA) : official website. URL: https://www.cisa.gov
6. The NIST Cybersecurity Framework (CSF) 2.0 : Special Publication 1299 / National Institute of Standards and Technology. 2024. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf