

людьми справді використовують найпопулярніші соціальні медіа-платформи, а також додатки для знайомств і форуми для відгуків. Спроби вербування також часто відбуваються в групах спільнот у соціальних мережах, які створюються на основі географічного походження тих, хто шукає послуги та країни призначення [5].

Отже, зважаючи на потребу в удосконаленні правоохоронної діяльності щодо протидії торгівлі людьми в умовах воєнного стану, Національна поліція України запроваджує передовий досвід діяльності правоохоронних органів зарубіжних країн та міжнародних поліцейських організацій Інтерполу й Європолу стосовно використання новітніх технологій у боротьбі зі злочинами, пов'язаними з торгівлею людьми, у практичну діяльність підрозділів міграційної поліції та навчальний процес закладів вищої освіти МВС.

Література

1. Злочини, вчинені військовими РФ під час повномасштабного вторгнення в Україну (станом на 21.11.2023). URL: <https://www.npu.gov.ua/news/zlochyny-vchyneni-viiskovymy-rf-pid-chas-povnomasshtabnoho-vtorhnennia-v-ukrainu-standom-na-21112023>
2. «Від початку війни рівень злочинності в Україні знизився», – Ігор Клименко в інтерв'ю Reuters. URL: <https://www.npu.gov.ua/news/vid-pochatku-viiny-riven-zlochynnosti-v-ukraini-znyzyvsia-igor-klymenko-v-interviu-reuters>
3. Міграційна поліція під егідою ЄВРОПОЛ створює міжнародну інформаційну платформу для запобігання торгівлі людьми серед українських біженців. URL: <https://www.npu.gov.ua/news/torgivlya-lyudmi/migracijnapolicziya-pid-egidoyu-Jevropol-stvoryuje-mizhnarodnu-informacijnuplatformu-dlya-zapobigannya-torgivli-lyudmi-sered-ukrajinskix-bizhencziv/>
4. «Возз'єднати Україну»: Нацполіція запустила новий мобільний додаток із пошуку зниклих дітей. URL: <https://www.npu.gov.ua/news/vozziednaty-ukrainu-natspolitsiia-zapustyla-novyi-mobilnyi-dodatok-iz-poshuku-znyklykh-ditei>
5. Цільовий: торговці людьми, які заманюють жертв в Інтернеті. URL: <https://www.europol.europa.eu/media-press/newsroom/news/targeted-human-traffickers-luring-victims-online>

Мороз А. О.

курсант факультету №4 Харківського національного університету внутрішніх справ

Лучик В. Є.

професор кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ, доктор економічних наук

СТРАТЕГІЇ ЗАХИСТУ ОСОБИСТОЇ КОНФІДЕНЦІЙНОСТІ ТА ДАНИХ КОРИСТУВАЧІВ В ОНЛАЙН СЕРЕДОВИЩІ

В онлайн-середовищі користувачі стикаються з постійними загрозами для їхньої особистої приватності та даних. Ці загрози можуть надходити від хакерів, державних органів і навіть від самих компаній, які збирають дані користувачів.

Щоб захистити себе в онлайн-середовищі, користувачі можуть використовувати різні стратегії. Деякі з них використовують надійні паролі та двофакторну автентифікацію. Паролі повинні бути складною комбінацією букв, цифр і символів. Двофакторна

автентифікація додатково захищає обліковий запис, надсилаючи код на мобільний телефон користувача.

Особливо потрібно бути обережним з інформацією, яка розміщується в Інтернеті. Ні в якому випадку не можна розголошувати конфіденційну інформацію, а, саме: імена, адреси, номери телефонів, кредитних карток тощо. Анонімні сервіси не вимагають від користувачів реєстрації та не зберігають дані.

Слід також оновлювати програмне забезпечення. Виробники програмного забезпечення регулярно випускають оновлення безпеки, які виправляють вразливості, що можуть бути використані хакерами. Не завадить встановлювати антивірусне програмне забезпечення. Антивірусне програмне забезпечення допомагає захистити комп'ютери від шкідливого програмного забезпечення, яке краде дані користувачів.

Збереження особистої інформації в інтернеті є складним завданням у світі постійних кіберзагроз. Використання унікальних паролів для кожного облікового запису є першим кроком до ефективного захисту, оскільки це ускладнює доступ до всіх аккаунтів при можливому зламі лише одного паролю. Важливо не зберігати паролі у браузері, оскільки отримання доступу до комп'ютера може привести до несанкціонованого входу у всі облікові записи.

Використання VPN на публічних Wi-Fi мережах забезпечує шифрування трафіку, запобігаючи можливе перехоплення даних хакерами. Обережність при встановленні додатків на мобільні пристрої та відмова від програм від невідомих розробників є важливими кроками для запобігання потенційним загрозам.

Ознайомлення з політикою конфіденційності веб-сайтів та додатків перед їх використанням дозволяє розуміти, яким чином дані будуть використовуватися. Необхідно мати на увазі, що жоден метод захисту не є абсолютно надійним, проте дотримання вищезазначених порад може значно знизити ризики витоку особистої інформації та даних в онлайн-середовищі.

Дослідження доводять, що більшість користувачів Інтернету усвідомлюють загрози для своєї приватності, проте не всі вживають належних заходів безпеки. Лише 30% використовують надійні паролі та двофакторну автентифікацію, 50% не приділяють уваги своїм особистим даним в мережі, а 20% не користуються анонімними сервісами, що може привести до загроз для їхньої приватності та безпеки.

Висновки. З метою підвищення рівня захисту особистої приватності та даних користувачів в онлайн-середовищі рекомендується розробити та впровадити ефективні закони та підзаконні акти щодо захисту особистого життя та даних користувачів, підвищувати рівень обізнаності користувачів про існуючі загрози, впроваджувати технічні заходи захисту, які ускладнюють доступ хакерів до особистої інформації та даних користувачів. Окремі стратегії захисту, такі як використання складних паролів, двофакторної автентифікації, уважність при обміні особистою інформацією, оновлення програмного забезпечення та використання антивірусних програм можуть значно зменшити ризики витоку даних та загрози для приватності.

Література

1. Впроваджуємо цифрові інструменти для фіксації воєнних злочинів росії. URL: <https://shtab.net/news/view/vprovadzhuemo-cifrovi-instrumenti-dlya-fiksaciji-v/>.
2. Дія. Доказ. Як повідомити про воєнний злочин проти українців? URL: <https://www.facebook.com/diia.gov.ua/photos/a.196543131750045/767598614644491/?type=3>.
3. Закон України від 1 червня 2010 року № 2297-VI «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/go/2297-17>.

4. Звіт Європейського агентства з питань мереж та інформаційного суспільства (ENISA) про кібербезпеку в Європі (2023). URL: <http://zpd.inf.ua/page12.html>.
5. Опитування інтернет-користувачів, проведене Інститутом кібербезпеки України, 2023 рік. URL: https://ela.kpi.ua/bitstream/123456789/59588/1/Shpotia_bakalavr.docx.

Мрачковський О. М.

курсант Львівського державного університету внутрішніх справ

КВАНТОВА ТЕХНОЛОГІЯ: ПЕРСПЕКТИВИ РОЗВИТКУ

Квантова технологія - це галузь науки та техніки, яка використовує властивості квантової механіки для створення нових продуктів та послуг. Квантові технології мають потенціал кардинально змінити наш світ, у тому числі в таких сферах, як комп'ютерні науки, хімія, матеріалознавство, медицина та телекомунікації.

Основи квантової технології

Квантова механіка - це теорія, яка описує поведінку матерії та енергії на атомному та субатомному рівнях. Квантові технології використовують такі квантові властивості, як суперпозиція, запутаність та квантова телепортація.

Суперпозиція – це властивість квантових об'єктів перебувати в двох або більше станах одночасно. Наприклад, електрон може перебувати одночасно у двох різних точках простору або мати два різних значення спіну.

Запутаність – це властивість квантових об'єктів, за якої їхні стани тісно пов'язані один з одним. Зміна стану одного об'єкта миттєво впливає на стан іншого, навіть якщо вони знаходяться на значній відстані один від одного.

Квантова телепортація – це процес передачі інформації з одного місця в інше без використання фізичного переносу інформації. Квантова телепортація використовує запутаність для передачі квантового стану одного об'єкта в інший.

Застосування квантових технологій

Квантова технологія має потенціал змінити наш світ у багатьох сферах. Ось деякі приклади можливих застосувань квантових технологій:

- Квантові комп'ютери – це комп'ютери, які використовують квантові принципи для обробки інформації. Квантові комп'ютери можуть вирішувати деякі завдання набагато швидше, ніж традиційні комп'ютери. Наприклад, квантові комп'ютери можуть бути використані для розробки нових ліків, моделювання клімату та створення нових матеріалів.
- Квантові сенсори – це сенсори, які використовують квантові принципи для вимірювання фізичних величин. Квантові сенсори можуть бути набагато точнішими та чутливішими, ніж традиційні сенсори. Наприклад, квантові сенсори можуть бути використані для виявлення хімічних речовин, виявлення витоків і моніторингу стану навколишнього середовища.
- Квантова криптографія – це метод шифрування даних, який використовує квантові принципи для забезпечення безпеки. Квантова криптографія є набагато безпечнішою, ніж традиційна криптографія, оскільки вона не може бути зламана навіть найпотужнішими комп'ютерами.