ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА БЕЗПЕКА

Інформаційно-комунікаційна (ІК) безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації.

Ризики – ймовірність, що хтось/щось скористається недосконалістю захищеності системи обробки і зберігання даних.

Захист комп'ютерної інформації — це комплекс організаційних, етичних, правових, технічних і програмних засобів, методів і заходів, спрямованих на попередження як навмисного, так і випадкового несанкціонованого доступу до комп'ютерної інформації, а також її модифікації і знищення. Такий комплекс заходів зазвичай спрямовують на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення.

Все нагальнішою постає необхідність зберігати, контролювати доступ на будь-яких видах ґаджетів до персональних даних, знайдених чи створених. У інформації, що вирує інтернетом, питому вагу займають персональні дані бібліотечних акаунтів: контакти, фото, документи, акаунти тощо. Зростає значення вмінь не тільки створювати, але захищати особисту інформацію. У цьому допомагатиме дотримання інформаційно-комунікаційної безпеки у мультимедійному просторі.

Основну небезпеку для функціонування інформаційних систем представляє несанкціонований доступ до комп'ютерної інформації, під яким слід розуміти доступ, здійснюваний із порушенням встановлених вітчизняним законодавством правил розмежування доступу.

Несанкціонований доступ до інформації в електронному форматі здійснюється таким чином:

- ✓ копіюванням конфіденційної інформації сторонньою особою;

- ✓ спостереженням за діями користувача, внесенням ним персональних даних або введенням конфіденційної інформації;
- ✓ маскуванням під зареєстрованого користувача за допомогою викрадання паролів і інших реквізитів розмежування доступу;
- ✓ маскуванням несанкціонованих запитів під запити операційної системи (містифікація);
- ✓ використанням програмних пасток, а також навмисним виведенням з ладу механізмів захисту;
- ✓ несанкціонованою зміною/викривленням програмного забезпечення.

Ризики несанкціонованого доступу, ймовірність, що зловмисник може отримати доступ до бібліотечних ресурсів (пошти, соцмереж, комп'ютера, банківського рахунку тощо) можлива завжди. Щоб передбачити це, необхідно: визначити, що є найвразливішим та найважливішим, зосередити на ньому увагу, посилити рівень безпеки. Стосовно інших даних варто особливо ретельно визначити, які можуть бути наслідки отримання до них доступу зловмисником та оцінити ступінь ймовірної шкоди, а також рівень зручності користування даними у разі підвищення ступеню захисту. Трапляється, що підвищення рівня захисту привносить значний дискомфорт у користуванні. В такому випадку варто переоцінити важливість даних, частоту та якість користування ними. Іноді, аналізуючи цифрову безпеку персональних даних, доводиться робити вибір між безпекою та зручністю користування. Необхідно пам'ятати також, що неможливо одного разу налаштувати безпеку і постійно нею користуватись – цифрова безпека потребує регулярного корегування, уточнення, внесення змін, удосконалення

чи навпаки спрощення рівню захисту. Цифрова безпека – це не продукт чи стан, це процес.

Якщо ж загроза є досить реальною, а дані варті захисту та збереження, рекомендується здійснити цикл дій, спрямованих на запобігання несанкціонованому доступу до персональних даних. Основними заходами є наступні:

- ✓ використовувати унікальні, складні паролі, що містять не менше восьми символів, серед яких є літери та цифри. У паролях не можна використовувати персональні дані. За необхідності рекомендується використовувати як пароль фразу, вигадану, а не поширену цитату. Не рекомендується зберігати паролі на пристроях, особливо на власних. На різні облікові записи слід встановлювати різні паролі, за необхідності ставити паролі на пристрій та на режим очікування. Наприклад, через систему Have I Been Pwned можна перевірити, чи не було обліковий запис вкрадено і чи не було пароль підібрано зловмисниками. Для генерування та кращого запам'ятовування паролів рекомендується використовувати сервіси 1Password, LastPass та KeePass. Для захисту від потрапляння паролів до третіх осіб варто створювати неординарні способи відновлення паролів, а сайтами користуватись тільки надійними, перевіреними;

- ✓ для входу до облікових записів рекомендується використовувати двофакторну автентифікацію. Щоб покращити захист, варто налаштовувати сповіщення про вхід до акаунту, закривати доступ з незнайомих пристроїв, не використовувати функцію «довірений пристрій». Корисним та безпечним буде розмежовування пошт: одна – для листування, інша – для створення та керування акаунтами;

- ✓ підтримувати базові налаштування на ґаджетах: регулярно оновлювати програми, використовувати надійну антивірусну програму, застосовувати тільки ліцензійне програмне забезпечення. Оновлення програм варто здійснювати тільки через надійні джерела, власноручне автоматичне оновлення не рекомендується. Крім того, оновленням чи завантаженням краще не надавати можливість автоматично відтворюватись, цим також можуть скористатись програми-шкідники.

Безпечне користування мультимедійним простором включає в себе також регулярну перевірку дозволів, які мають інстальовані додатки, програми на ПК, використання у роботі тільки надійних перевірених сервісів, пошт, соціальних мереж, месенджерів, гіперпосилань, ігнорування підозрілих гіперпосилань, систематичне очищення кешу, історії серфінгу інтернетом. У разі використання ПК на робочому місці доречною буде робота під обліковим записом «Користувач», під час якої право на внесення змін до ПЗ має тільки користувач під записом «Адміністратор». Ця дія збереже внесення змін на ПК вірусними програмами, заборонить шпіонаж стороннім програмам.

Іноді у роботі, щоденному житті доводиться звертатись до стороннього, не персонального пристрою. У такому випадку важливим постає вихід з облікових записів, закриття робочих сесій, видалення даних про них із пам’яті браузера, сайта.

Певні нюанси цифрової безпеки у мультимедійному просторі виникають при користуванні смартфонами чи іншими ґаджетами цього типу. Персональні пристрої зберігають безліч конфіденційної інформації про свого користувача. Це фото, відео, нотатки, повідомлення, геолокація, контакти, мобільний банкінг і т. і. Захистити їх можна дотримуючись наступних простих кроків: пароль на вхід або цифровий, надійний, або біопароль (відбитки пальців чи скан обличчя); регулярне оновлення додатків; контроль додатків, яким дозволено виводити сповіщення на екран. З метою

збереження даних рекомендується створювати копії за допомогою хмарних технологій, а паролі до акаунтів не записувати на цьому ж самому пристрої. Варто також користуватись функцією «Знайти пристрій», який автоматично працює, якщо у ґаджеті активований Google-акаунт. З її допомогою можна не тільки дізнатись, де знаходиться пристрій, але і заблокувати його чи видалити всі дані. З цією ж метою можна активувати програму Find my device, яка дозволить знайти пристрій, дистанційно змінити на ньому пароль, встановити чи видалити контакти тощо.

На смартфони встановлюються певні додатки, які роблять життя легшим, оперативнішим, зручнішим. Додатки постійно є активними: вони взаємодіють між собою, звертаються до мережі, весь час здійснюють обмін даними. Щоб додатки коректно працювали, їм необхідно надавати доступ до даних, що містяться на пристрої. Найпростіші кроки для захисту даних при користуванні ґаджетом такі: контроль доступів, систематична ревізія доступів, складні паролі, завантаження даних тільки з надійних джерел (для смартфонів на системі Android – Google Play, якщо операційна система від Apple – з Play Store).

Комунікація з появою інтернету не тільки збільшилась в обсягах, але й набула великої активності. На смартфонах, стаціонарних телефонах встановлено різноманітні месенджери, які часто використовуються для оперативної взаємодії з користувачами бібліотеки, колегами. Безпека у їх використанні також важлива. Щоб зловмисники не отримали доступ до персональної кореспонденції, рекомендується особливо важливі чати робити секретними, створювати їх копії у хмарних сховищах. І навпаки, неважливі або вже не потрібні бесіди варто видаляти. Надійним способом контролю акаунту в месенджерах є двофакторна автентифікація, налаштування сповіщення про вхід, контроль відкритих сесій та створення надійних способів відновлення паролів.

Особливо популярною в останній час формою заволодіння персональними даними є фішінгова атака, тобто дії зловмисників, які мають за мету дізнатись особисті дані, паролі тощо. Найпопулярнішою формою фішінгової атаки є фішінгові листи, які містять посилання, схожі на популярні, відомі сайти з пропозицією швидко скористатись ними, ввести чи змінити пароль, власноруч залишити конфіденційно дані. Якщо користувач робить ці дії, зловмисники отримують доступ до користувацьких акаунтів, облікових даних. Найголовніше, що рекомендують фахівці з ІК безпеки – ніколи не переходити лінками, що надіслані з ненадійних, незнайомих адрес, використовувати двофакторну автентифікацію та пам'ятати, що офіційні сервіси не розсилають листів з проханнями повідомити свої облікові дані, пароль та інше і бути пильним – перед зломом чи проникненням завжди здійснюється розвідка.

Фахівці бібліотек Харкова активно навчаються та навчають користувачів і колег дотримуватись інформаційно-комунікаційної безпеки. Для цього проводяться відповідні заходи. Протягом 2018/2019 рр. для бібліотечних фахівців були проведені такі заходи: тренінг з інформаційно-комунікаційних технологій для неурядових організацій (НУО) від ресурсного центру «Гурт», бліц-презентація «ІК безпека по-бібліотечному», секція на Форумі молодих бібліотекарів, воркшоп «Віртуальні продукти бібліотек: how to». На постійній основі діють курси для формування навичок з ІК безпеки для користувачів у клубах «КЛІК», «Онлайн», курс для вимушених переселенців та інших користувачів бібліотек, заняття при Регіональному тренінговому центрі (РТЦ).

На тренінгу з інформаційно-комунікаційних технологій для НУО харківські бібліотекарі досліджували чек-лист для управлінця, моделювали потреби та проблеми безпеки в організаціях, знаходили рішення їх усунення, відшукували оптимальні шляхи подолання цифрової нерівності, долучились до секретів корпоративних рішень засобами хмарних технологій, дізнались

про можливість отримання пільгового програмного забезпечення від партнерів програми TechSoup та Office 365. Організаторами тренінгу були Ресурсний центр «Гурт» та громадська організація «Лабораторія цифрової безпеки».

У межах тренінгу «Шістка креативних бібліотекарів: оптимізуємо, модернізуємо, просуваємо», що проводився на базі Центральної міської бібліотеки імені В. Г. Бєлінського, відбулась бліц-презентація «ІКТ безпека по-бібліотечному». Слухачами були фахівці публічних бібліотек Харкова, які в інтерактивному режимі навчались захищати свої ґаджети від ймовірних ризиків.

Під час IV Міжнародного форуму молодих бібліотекарів УБА представлено доповіді, присвячені кібербезпеці у межах секції «Технології». Учасники навчалися як працювати з ризиками, як їх визначати та запобігати; як захищати дані від кібершахрайств, уникати неприємних ситуацій у мережі, як контролювати функціонування бібліотечних онлайнових електронних ресурсів (сайтів, блогів, електронних каталогів) та працювати з ризиками під час роботи із хмарними технологіями.

Бібліотекарі закладів професійної (професійно-технічної) освіти м. Харкова та області опановували онлайн-сервіси для створення бібліотечно-журналістських медіа та оволодівали ІК безпекою на воркшопі «Віртуальні продукти бібліотек: how to».

До найбільших заходів, спрямованих на поглиблення знань з ІК безпеки, серед громади належать постійно діючі клуби при ХДНБ ім. В. Г. Короленка («КЛІК», онлайн-інтернет-клуб); курс для вимушених переселенців та інших користувачів бібліотеки; заняття у РТЦ, що працюють на регулярній основі у ХОУНБ. Учасники клубів та слухачі занять вивчають ІК безпеку під час користування ґаджетами, серфінгу в інтернеті, користування соціальними мережами, месенджерами та ін.

Зростає необхідність постійного удосконалення навичок зі збереження та захисту персональних, корпоративних даних. Досліджувати проблему ІК захисту, навчатись протистояти зловмисникам, мінімізувати ризики атаки є надважливим завданням. Тому заходи з ІК безпеки, які проводяться у бібліотеках Харківщини для бібліотечних фахівців та для користувачів, є актуальними як ніколи.

Джерела

1. Безкоштовні заняття з основ комп'ютерної грамотності та роботи в інтернет для початківців**:** курс для вимушених переселенців та інших користувачів бібліотеки // Харківська державна наукова бібліотека імені В. Г. Короленка : сайт. URL : http://korolenko.kharkov.com/novyny-ta-podii/1041.html.

2. Віртуальні продукти бібліотек: HOW TO // Харківська державна наукова бібліотека імені В. Г. Короленка : сайт. URL : http://korolenko.kharkov.com/novyny-ta-podii/2298.html.

3. Інформаційна безпека в мережі Інтернет // Харківська державна наукова бібліотека імені В. Г. Короленка : сайт. URL : http://korolenko.kharkov.com/novyny-ta-podii/1470.html.

4. Клуб «Клік» Харківська державна наукова бібліотека імені В. Г. Короленка : сайт. URL : http://korolenko.kharkov.com/50+/klik.html.

5. Кушнір Антон. За тобою, як за стіною // Куншт : сайт українського науково-популярного журналу. URL : https://kunsht.com.ua/messengers/?fbclid=IwAR0DazHmbHwgHsx5luqoZkLqSeajHrnPMA1UKmpbW1iNa7w0YIul6jngBC8.

6. Леонычев Юрий. Безопасность мобильных приложений для Android. Теория и практика // Компьютерные науки : канал на YouTube. URL: https://www.youtube.com/watch?v=4-D3ai-RtyA.

7. Тренинг «Шестерка креативных библиотекарей: оптимизируем, модернизируем, продвигаем!» // Центральна міська бібліотека імені В. Г. Бєлінського : сайт. URL : http://belinskogo.kh.ua/news/2659.html.

8. Цифрова грамотність актуальна у любому віці // Харківська обласна універсальна наукова бібліотека : сайт URL : http://library.kharkov.ua/library/events/?events=6314&fbclid=IwAR2ON0UrQONbN2bKMO7eE44IX9Hn3IxO-t80URs4XoIlwdVCHVVKJLi7Rs8.

9. Як проходив IV Міжнародний форум молодих бібліотекарів УБА // Сайт Молодіжної секції Української бібліотечної асоціації. URL : https://kunsht.com.ua/messengers/?fbclid=IwAR0DazHmbHwgHsx5luqoZkLqSeajHrnPMA1UKmpbW1iNa7w0YIul6jngBC8.

10. Як? Практичні поради з цифрової безпеки : сайт проєкту. URL : https://yak.dslua.org/.

Тіщенко Антоніна Анатоліївна

Статтю створено 27.03.2020