ОСНОВНІ НАПРЯМКИ ВДОСКОНАЛЕННЯ ОСОБИСТОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНОГО СТУДЕНТА

Яценко Оксана Іванівна,
асистент кафедри комп'ютерних наук та інформаційних технологій
Житомирський державний університет імені Івана Франка
м. Житомир, Україна

В наш час цифрові технології використовуються практично у всіх сферах людської діяльності, і більшість із нас вже не уявляє свого життя без них. Сьогодні з їх можна проводити дослідження, здобувати освіту, вести бізнес та отримувати адміністративні послуги, здійснювати покупки, оплачувати товари та послуги через Internet, організовувати сумісну роботу фахівців над проектами, взаємодіяти з іншими користувачами мережі тощо. Цифрові технології ми використовуємо постійно і, на жаль, всі вони є потенційно вразливими. Саме тому, говорячи про розвиток суспільства, не можна забувати про таке важливе питання, як інформаційна безпека (ІБ), що, в результаті інформатизації суспільства і прискорення технічного розвитку, з кожним роком набуває все більшого значення як для країни загалом так і для пересічного користувача.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [1].

Питання забезпечення ІБ є дуже важливими для української держави на сучасному етапі, що обумовлено необхідністю протистояти протиправним посяганням на інформаційний простір України, збереження інформаційних ресурсів, захисту населення від негативного інформаційного впливу тощо [2].

Значна кількість організацій розробляють власні системи ІБ. Як правило, вони включають організаційні заходи: призначення осіб, відповідальних за ІБ, розробку правил та інструкцій для користувачів, впровадження політики резервного копіювання тощо. Сучасні організації використовують вимоги міжнародних стандартів для побудови систем управління ІБ та використання кращих світових практик [2].

Не менш актуальною та важливою є побудова особистої ІБ громадянина. Використання комп'ютерів, планшетів, смартфонів стало невід'ємною частиною життя кожного студента. Сучасне покоління легко освоює інформаційні технології але досить часто приділяє недостатньо уваги ризикам, що виникають при роботі в інтернеті, використанні знімних носіїв інформації і т. п. Іноді тільки втрата даних змушує звертати увагу на посилення засобів захисту і вивчення проблеми ІБ.

У повсякденному житті захист інформації в основному розглядається як захист від комп’ютерних вірусів. Комп'ютерний вірус – це тип шкідливого програмного забезпечення, що може створювати власні копії, вбудовуватися в код інших програм, завантажувальних секторів або областей системної пам'яті, а також поширювати власні копії по різних каналах зв'язку. Однак є і засоби протидії – антивірусні програми (антивіруси). Антивіруси – це спеціалізовані програми, призначені для виявлення, усунення і запобігання появи комп'ютерних вірусів та, за можливості, відновлення заражених (пошкоджених) вірусом файлів. Для того, щоб антивіруси могли виконувати свою функцію, потрібно їх вчасно оновлювати.

Ще однією з причин втрати даних може бути використання простих паролів чи паролів за замовчуванням. Так, наприклад, паролі, що складаються лише з невеликої кількості цифр (літер) на телефоні або в електронній пошті можуть призвести як до втрати особистих даних так і грошей. Щоб пароль був надійним, в ідеалі він повинен складатися з букв і цифр, містити не менше восьми символів, мати малі та великі літери, а також не збігатися з жодним словниковим словом.

Необхідно навчитися краще користуватися комп'ютером. Для комп'ютера найнебезпечнішим хакером є сам користувач. І якщо користувач планує надати доступ до персонального компютера сторонній особі, то він має бути впевнений в її компетентності та надійності. В іншому випадку особисті дані користувача можуть бути як втрачені, так і неправильно використані. Крім того потрібно використовувати лише надійні пристрої (сервіси) для зберігання даних. Якщо пристрій чужий і ви про нього нічого не знаєте, є ризик підключення пристрою з вірусом до комп'ютера.

Для того щоб убезпечити використання цифрових пристроїв, необхідно також пам'ятати про деякі моменти роботи в мережі Інтернет. Програмне забезпечення, включаючи браузер, слід періодично оновлювати. Досить небезпечним може бути перехід на підозрілі сторінки в Інтернеті чи на спливаючу рекламу. Ні в якому разі не можна вказувати власне ім'я, номер телефону, номер кредитної картки, адресу проживання, пароль тощо, якщо немає стопроцентної впевненості в достовірності та надійності ресурсу, що їх «запитує». Потрібно блокувати спам і рекламу, так як вони, в деяких випадках, також можуть бути джерелами вірусів.

Не менш важливою є проблема захисту персональних даних користувача в соціальних мережах. Соціальних мереж багато, і кожна з них, при реєстрації, запитує персональні дані (прізвище та ім’я, номер телефону, адресу проживання, та ін.). З одного боку, наявність особистих даних в соціальних мережах спрощує життя користувачів (онлайн покупки, оплата комунальних послуг, банківські перекази і т. п. – все це можна зробити, не виходячи з дому), але з іншого боку – користувачі не можуть бути повністю впевнені, що ці дані не використають без їх згоди. Зазвичай сервіси соціальних мереж, коли запитують дані, просять прочитати політику конфіденційності (на яку більшість користувачів не звертає увагу), але не це є основною проблемою. Проблема в тому, що користувачі, використовуючи окремі сервіси, погоджуються з тим, що частина їх особистих даних стає загальнодоступною. При цьому користувач несе відповідальність сам, не маючи можливості притягнути до

відповідальності третіх осіб (розробників соціальної мережі). Існує також ще одна проблема – проблема пошуку. Пошук в соціальних мережах дозволяє іншій людині отримати певну кількість інформації про конкретного користувача (навіть якщо останній максимально захищений вбудованими засобами від усіх незнайомих профілів). Його суть полягає в тому, що використовуються пошукові фільтри. Завдяки цим фільтрам можна дізнатися максимум з мінімуму, змінивши тільки запити на ті ж фільтри, будь то вік, рід занять, адреса і т. д. Відзначимо такі випадки, як аналіз профілів в соціальних мережах при прийомі на роботу, при підборі та показі контекстної реклами та ін.

Ще одним важливим питанням ІБ користувача є безпека при роботі з мобільними банківськими додатками. Найбільш поширеними засобами та каналами комунікації клієнта та банку, на думку Б. Кінга [4]: мобільні пристрої (20-30 разів на місяць); ПК (7-10 разів на місяць); банкомати (до 5 разів на місяць). Сьогодні клієнти спілкуються з банками використовуючи банк-клієнт або онлайн-банкінг через персональні комп'ютери, мобільні онлайн-додатки, соціальні мережі та ін. При цьому клієнт, спілкуючись з банком та проводячи транзакції, повідомляє персональні дані, і фактично, є досить вразливим. Потенційною вразливістю клієнта є злом паролів, несанкціоноване використання даних на банківських картах і рахунках, доступ до інформації про витрати і доходи.

Підсумовуючи зазначене вище, користувачеві для захисту особистих даних та фінансів можна порадити наступне:

– використовувати паролі різні паролі (паролі різної складності) для різних ресурсів та пристроїв;

– уважно перевіряти де і кому платить;

– не надсилати дані банківської картки, логіни та паролі в онлайн-сервіси на неперевірені сайти;

– не зберігати кошти на картці, за допомогою якої відбувається оплата через Інтернет;

– перевіряти (або передзвонювати в банк) при отриманні SMS-повідомлень із запитом на отримання фінансової інформації;

– при реєстрації на масових сайтах використовувати не основну адресу електронної пошти та номер телефону;

– не давати доступу до персональних цифрових пристроїв стороннім користувачам;

– вчасно оновлювати операційні системи, прикладне програмне забезпеченні та антивірусні програми.

Тільки використовуючи всі методи захисту по максимуму, користувачі створюють власну систему захисту інформації, яка дозволяє зберігати особисті дані, звести до мінімуму ризики несанкціонованого доступу до різного роду інформації. Важливо пам’ятати, що особисті інформаційна безпека громадянина є складовою інформаційної безпеки України і зміцнення інформаційної безпеки країни складається зі спільних злагоджених дій всіх державних органів та громадськості.

Список використаних джерел та літератури

1. Верховна Рада України. (2007, січ. 9). Закон № 537-V, Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16#Text (Дата звернення: 15.05.2022).

2. Солодка О. М., пріоритети удосконалення інформаційної безпеки України // Інформація і право /2015. – 2015. – № 3(15). – С. 36 - 4265

3. ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management [Електронний ресурс] // Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=56742 (Дата звернення: 15.05.2022).

4. Brett King. Bank 3.0: Why Banking Is No Longer Somewhere You Go but Something You Do, USA: Wiley, 2012