Оксана Яценко,
Асистент кафедри комп'ютерних наук та інформаційних технологій,
oksana@zu.edu.ua
(Житомирський державний університет імені Івана Франка)

ІНФОРМАЦІЙНА БЕЗПЕКА: СУЧАСНІ РЕАЛІЇ

В наш час цифрові технології (ЦТ) використовуються практично у всіх сферах людської діяльності, і більшість із нас вже не уявляє свого життя без них. Сьогодні з допомогою ЦТ 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. ЦТ 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, що, в результаті інформатизації суспільства і прискорення технічного розвитку, з кожним роком набуває все більшого значення як для пересічного користувача так і для багатьох галузей економіки.

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].

Багато організацій будують власні системи інформаційної безпеки, проводять перевірки та аналіз безпеки даних. Це стосується як персональних даних клієнтів і персоналу, так і інформації про поточну діяльність, фінансовий стан. Як правило, реалізація заходів захисту включає, перш за все, організаційні заходи: призначення осіб, відповідальних за інформаційну безпеку, розробка правил та інструкцій для користувачів, впровадження політики резервного копіювання тощо. Сучасні організації використовують вимоги міжнародних

стандартів для побудови систем управління інформаційною безпекою та використання кращих світових практик [2].

Незалежно від того, в якій формі зберігається інформація, як вона використовується, необхідно вжити адекватних заходів захисту. Кожен керівник повинен об'єктивно оцінити поточний стан інформаційних систем, побачити і зрозуміти потреби в інформаційній підтримці і існуючі інформаційні проблеми. Саме з цією метою організація повинна навчати відповідальних осіб і користувачів роботі з даними, в тому числі і з основами інформаційної безпеки. Саме тому встановлюються засоби захисту програмного забезпечення, програмне забезпечення, регулярно оновлюються антивірусні програми, програми шифрування даних. Для поліпшення захисту даних організації модернізується локальна комп’ютерна мережа, встановлюється додаткове обладнання – відеокамери, додаткові сервери, джерела безперебійного живлення і т. д. Завдяки заходам захисту значно знижуються ризики витоку ділової інформації, ризики різного роду впливів, що викликають збої в роботі інформаційних систем, таких як шахрайські програми, хакерські атаки тощо.

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

У повсякденному житті захист інформації в основному розглядається як захист від вірусних програм, або вірусів. Комп'ютерний вірус – це тип шкідливого програмного забезпечення. Він здатний 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. Їх називають антивірусами. Антивіруси – це

спеціалізовані програми, призначені для виявлення, усунення і запобігання появи комп'ютерних вірусів. Також однією з функцій антивіруса є відновлення заражених вірусом файлів. Для того, щоб антивірусні програми 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 «0000» на телефоні або «parol1» 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, мати не менше 8 символів, містити як великі, так і великі літери, а також не збігатися з жодним словниковим словом.

Необхідно навчитися краще користуватися комп'ютером. Для вашого комп'ютера найнебезпечнішим хакером є ви самі. І якщо хтось інший збирається працювати з вашими даними, ви повинні бути впевнені в його компетентності та надійності. В іншому випадку ваші особисті дані 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 комп'ютера, необхідно також пам'ятати про деякі моменти роботи в інтернеті. ПЗ, включаючи браузер, слід періодично оновлювати. Досить небезпечним може бути перехід на підозрілі сторінки в інтернеті та на спливаючу рекламу. Ні в якому разі не можна давати в інтернеті своє ім'я, номер телефону, номер кредитної картки, адресу проживання, пароль і т. д., якщо немає 100% впевненості в достовірності джерела. Потрібно блокувати спам і рекламу, так як вони, в деяких випадках, також можуть бути джерелами вірусів.

Не менш важливою є проблема захисту персональних даних в соціальних мережах. У сучасному світі людина, яка користується Інтернетом, зазвичай присутня в соціальних мережах. Соціальних мереж багато, і кожна з них, при реєстрації, запитує персональні дані. Цей факт можна розглядати з двох сторін. З одного боку, наявність персональних даних в соціальних мережах максимально

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. Звичайно, кожен раз, коли сервіси соціальних мереж запитують дані, вони просять прочитати політику конфіденційності (на яку більшість користувачів не звертає увагу), але н 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, контекстна реклама і багато інших.

Ще одним важливим питанням інформаційної безпеки користувача є безпека при роботі з мобільними банківськими додатками. Сьогодні клієнти спілкуються з банками використовуючи такі сервіси як: банк-клієнт або онлайн-банкінг через персональні комп'ютери; мобільні онлайн-додатки; соціальні мережі та месенджери. При цьому клієнт проводить транзакції, повідомляє персональні дані, і фактично, є досить вразливим. Найбільш поширеними засобами та каналами комунікації клієта та банку, на думку Б. Кінга [3]: мобільні пристрої (20-30 разів на місяць); ПК (7-10 разів на місяць); банкомати (до 5 разів на місяць);

Потенційною вразливістю клієнта є злом паролів, несанкціоноване використання даних на банківських картах і рахунках, доступ до інформації про

витрати і доходи, отримання інформації про паролі. Поради для клієнтів тут наступні:

– не використовуйте паролі в Інтернеті та для онлайн-банкінгу, що вже задіяні в інших сервісах;

– уважно перевірте, де і кому ви платите;

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

– не зберігайте кошти на картці, за допомогою якої ви платите через Інтернет;

– не використовуйте платежі на сторонніх сайтах;

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

– при реєстрації на масових сайтах використовуйте не основну адресу електронної пошти та номер телефону.

Використовуючи різні 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.

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. 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).

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