УДК 004.056.5

Віктор Миколайович КРАСНОЩОК,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

Людмила Миколаївна СКАЧЕК,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

КРАЇНА У СМАРТФОНІ – ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

В 2019 році влада України анонсувала впровадження концепції «Держава в смартфоні» – це концепція з переведення державних послуг у режим онлайн. «Держава у смартфоні» – це коли громадянин може вирішити будь-яку свою життєву чи бізнесову ситуацію онлайн в один клік і бажано зі смартфона. Така концепція надає багато переваг, а в умовах всесвітньої пандемії – є життєво необхідною. В ситуації обмеженого пересування громадян містом можливість онлайн замовити їжу, сплатити комунальні платежі, поповнити рахунки, розрахуватися за послуги, спілкуватися з колегами, проводити заняття та конференції – все це дозволяє продовжувати працювати навіть в умовах карантину.

Разом з тим, для плодотворної роботи необхідно багато персональних даних передати в загальне користування різним додаткам, які в свою чергу зберігають ці дані або в смартфоні, або в хмарних сервісах.

В Україні презентували мобільний додаток «Дія», який на сьогоднішній момент містить водійське посвідчення та техпаспорт та планується скоро додати цифрову ID-картку, біометричний закордонний паспорт та студентський квиток. Розробники додатку «Дія», представники компанії EPAM, стверджують, що "авторизація здійснюється через BankID, сам застосунок побудовано відповідно до кращих практик індустрії, усі дані передаються та зберігаються на смартфоні користувача виключно у зашифрованому вигляді, посилена процедура автентифікації між додатком та сервером".

В Міністерстві цифрової трансформації України декларують для зберігання даних про використання українського облака De Novo. Але разом з тим ір-адреса сайту diia.app вказує на німецький Франкфурт та містить в описі хмарні сервіси Amazon, які не мають українського атестату відповідності КСЗІ. Сама компанія EPAM (розробник «Дія») працює в 25 країнах світу, а міноритарний пакет акцій належить інвестиційному банку «ВТБ-Капітал» з головним офісом в Москві. «ВТБ-капітал» публічно називає EPAM своїм ключовим партнером [1].

В умовах карантину величезної популярності набувають онлайн конференції. Одним з лідерів на ринку програмного забезпечення для проведення відео-конференцій є компанія Zoom Video Communications. Її розробка Zoom – є доволі простою та зручною програмою для проведення відео-конференції. У січні 2020 р., після зросту популярності Zoom, команда дослідників Check Point опублікувала звіт, в якому довела, що сервіс відеоконференцій Zoom мав недоліки в області безпеки. Згідно з дослідженням, хакери могли прослуховувати виклики Zoom, генеруючи і вгадуючи випадкові числа, призначені URL-адресами конференції Zoom. Zoom був змушений усунути пролом в системі безпеки і змінити деякі функції безпеки, такі як обов'язковий захист запланованих конференцій паролем [2].

В сучасних смартфонах реалізована технологія NFC – це доволі безпечна технологія бездротового високочастотного зв'язку малого радіусу дії «в один дотик». Ця технологія дає можливість обміну даними між пристроями, насамперед смартфонами та безконтактними платіжними терміналами, що перебувають на відстані близько 10 см.

З використанням технологія NFC є можливість застосовувати технологію безконтактної оплати, яка була реалізована в Україні ще в 2011 році.

Технологія безконтактної оплати є максимально безпечною, оскільки має кілька ступенів захисту. Кожна транзакція захищена унікальною криптограмою або динамічним кодом. Використати безконтактну картку (смартфон) без згоди користувача практично неможливо.

Проаналізувавши три найбільш популярні дії, які роблять з використанням смартфонів сьогодні, можна зробити висновки, що перш за все треба використовувати загальні рекомендації щодо захисту гаджетів:

— здійснювати регулярне та своєчасне оновлення операційної системи та додатків;

- використовувати надійні паролі для запобігання несанкціонованого доступу до пристрою;
- завантажувати додатки тільки перевірених та відомих розробників, а також звертати увагу на відгуки про них, особливо негативні. Крім цього, спеціалісти ESET не рекомендують завантажувати невідоме програмне забезпечення або додаток з невеликою кількістю інсталяцій, оскільки така програма може мати ще певні помилки, а в гіршому випадку й шкідливий код;
- використовувати двофакторну аутентифікаціюдля покращення безпеки телефона за допомогою захисту облікових записів банківських додатків;
- уникати підключення до публічних Інтернет-мереж, які є менш захищеними та часто поширюють різні загрози;
- не переходьте за випадковими посиланнями та не натискайте на спливаючі вікна;
- уникати поширення конфіденційної інформації через електронну пошту та соціальні мережі;
- використовувати надійне рішення для безпеки телефона та захисту від різних загроз, зокрема фішингових атак, спрямованих на викрадення паролів, даних банківських карт, інформації для входу в облікові записи, а також програм-вимагачів, які блокують екрани пристроїв та вимагають викуп.

Список бібліографічних посилань

1. Лиховид И. Электронные документы в смартфоне – насколько надежна защита данных? // DATA.UA : сайт. 12.02.2020. URL: https://data.ua/news/top-tema/49570-elektronnie-dokumenti-v-smartfone-naskolko-nadezhna-zaschita-dannih (дата звернення: 04.04.2020).
2. Киберпреступники эксплуатируют возросшую популярность Zoom // КО. IT для бизнеса : сайт. 02.04.2020. URL: https://ko.com.ua/kiberprestupniki_jekspluatiruyut_vozrosshuyu_populyarnost_zoom_132478 (дата звернення: 04.04.2020).

Одержано 08.04.2020