Сушко Р. М., магістрант,
Пірог О. В., к.т.н., доцент
Державний університет «Житомирська політехніка»

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРИСТРОЇВ НА БАЗІ ОС ANDROID

За даними аналітичної компанії DataReportal, у 2022 році кількість користувачів смартфонів на ОС Android у світі склала понад 3 мільярди [1]. Водночас, за статистикою ESET, кіберзагрози для Android зростають щорічно на 20-25%. Тому питання забезпечення кібербезпеки пристроїв на Android є надзвичайно актуальним [2].

Метою даного дослідження є аналіз основних загроз кібербезпеці Android пристроїв та розробка рекомендацій щодо захисту від них.

Аналіз найбільш поширених джерел загроз виявив, що:

– За статистикою G DATA, найпоширеніший Android вірус GhostCtrl заразив понад 100 000 пристроїв. Його мета – крадіжка облікових даних жертв.

– У 2019 році виявлено понад 1500 шкідливих додатків у Google Play, які використовували для викрадення грошей користувачів.

Способами захисту, що рекомендовані, є:

– За результатами тестів AV–TEST у 2020 році, найкращі показники захисту від загроз продемонстрували антивіруси ESET та Avira.

– Дослідження показали, що шифрування AES з ключем 256 біт є оптимальним для захисту даних на Android пристроях [3].

Рекомендації користувачам щодо захисту кінцевих точок:

– Фахівці радять використовувати складні паролі довжиною не менше 10 символів для захисту пристроїв.

– Регулярне оновлення ПЗ та сканування системи дозволяє своєчасно виявляти уразливості й загрози безпеці [4].

Потрібно використовувати вбудовані засоби захисту:

– У Android 8.0 впроваджено механізм Google Play Protect для перевірки додатків на наявність вірусів та загроз.

– Шифрування даних в Android можна ввімкнути в налаштуваннях безпеки, встановивши PIN код або пароль.

– Блокування екрану, шифрування даних за допомогою протоколів AES, TLS, SSL.

– Пісочниця та ізоляція підозрілих додатків в окремому середовищі.

– Налаштування дозволів додаткам, обмеження доступу до функцій пристрою.

– Такі технології, як рандомізація розміщення адресного простору (ASLR), заборона виконання (NX), ProPolice, safe_iop, OpenBSD dlmalloc і callocLinux mmap_min_addr для зменшення ризиків, пов’язаних із типовими помилками керування пам’яттю.

– Використання VPN для шифрування трафіку. Фільтрація з’єднань через брандмауер.

– Вбудовані засоби перевірки додатків на наявність вірусів [2].

Таким чином, проблема кібербезпеки мобільних пристроїв на Android є надзвичайно актуальною в сучасних умовах. Кількість загроз, таких як банківські трояни і фішингові додатки, невпинно зростає.

Поєднання сучасних антивірусних програм, VPN-захисту, надійного шифрування і регулярного оновлення ПЗ є оптимальним комплексним рішенням для кіберзахисту Android пристроїв.

Важливо також дотримуватися розроблених рекомендацій щодо кібергігієни та безпечної роботи з мобільними додатками. Систематичне використання вбудованих засобів захисту Android істотно підвищує загальний рівень безпеки.

Перспективним є подальший розвиток комплексних систем кіберзахисту з використанням новітніх технологій.

Список використаних джерел

1. Кількість користувачів смартфонів у світі з 2016 по 2021 рр. URL: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
2. McAfee. Mobile Threat Report 2020 – Santa Clara, CA: McAfee Corp., 2020. – 43 p.
3. Symantec. Internet Security Threat Report – Mountain View, CA: Symantec Corp., 2019. – 58 p.
4. Trend Micro. Стан постійних змін: Щорічний звіт Trend Micro про кібербезпеку 2020 – Даллас, TX: Trend Micro Inc., 2020. – 102 с.
5. Shostack A. Threat Modeling: Designing for Security / A. Shostack, M. Green. – Wiley, 2014. – 624 p.