УДК 004.62+004.77

А. В. Платоненко

ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ КОРИСТУВАЧІВ СУЧАСНИХ МОБІЛЬНИХ ПРИСТРОЇВ ТА ЗАСОБИ ЇХ ЗАХИСТУ

Розглянуто вразливості сучасних мобільних пристроїв з використанням високошвидкісних мобільних мереж, адже кожен третій житель України має смартфон з сенсорним екраном, а висока швидкість передачі даних є зручною не тільки для користувача, а і для зловмисника, що несе за собою небезпеку для інформації, яка зберігається та передається з використанням мобільних пристроїв.

Ключові слова: інформаційна безпека, загрози інформаційної безпеки, збитки від кіберзлочинів, захист мереж від несанкціонованого доступу, захист мобільних пристроїв.

Вступ

Сучасні мобільні пристрої стали невід'ємною частиною нашого життя, але окрім зручності та багатьох технічних можливостей, вони несуть за собою все більшу небезпеку для інформації, яка в них зберігається та передається [1]. Швидкість передачі даних у мережах 4G, яка може досягати до 1 Гбіт/с (в 6 разів більше у порівнянні з найшвидшими мережами 3G), а в мережах 5G швидкість передачі даних може досягати до 5 Гбіт/с (в 80 разів більше ніж заявлена максимально можлива швидкість в мережах 3G-операторів України). З використанням високошвидкісних мобільних мереж нового покоління, загрози інформаційної безпеки для державних та приватних установ збільшуються, адже для зловмисників відкриваються більші технічні можливості, оскільки працівники все частіше використовують мобільні пристрої для віддаленої роботи, а не тільки для спілкування [2].

Основна частина

Кожен третій житель України (33%) має смартфон з сенсорним екраном, а серед людей у віці 18-50 років – половина (50%). Порівняно з 2015 роком простежується зростання частки таких людей – з 26% до 33% у випадку загального населення і з 41% до 50% у випадку осіб до 50 років. Якщо серед молоді 65% користуються смартфонами (рис. 1), то серед осіб літнього віку – 5%. Типовий користувач смартфонів – це молода особа не старше 40 років з вищою освітою, яка проживає у середніх і великих містах України. Більшість (66%) користуються операційною системою Android, а 68% користувачів смартфонів мають досвід встановлення додатків. Найбільш популярними є соціальні мережі (73%), ігри (61%), навігація (51%), месенджери (49%) [3].

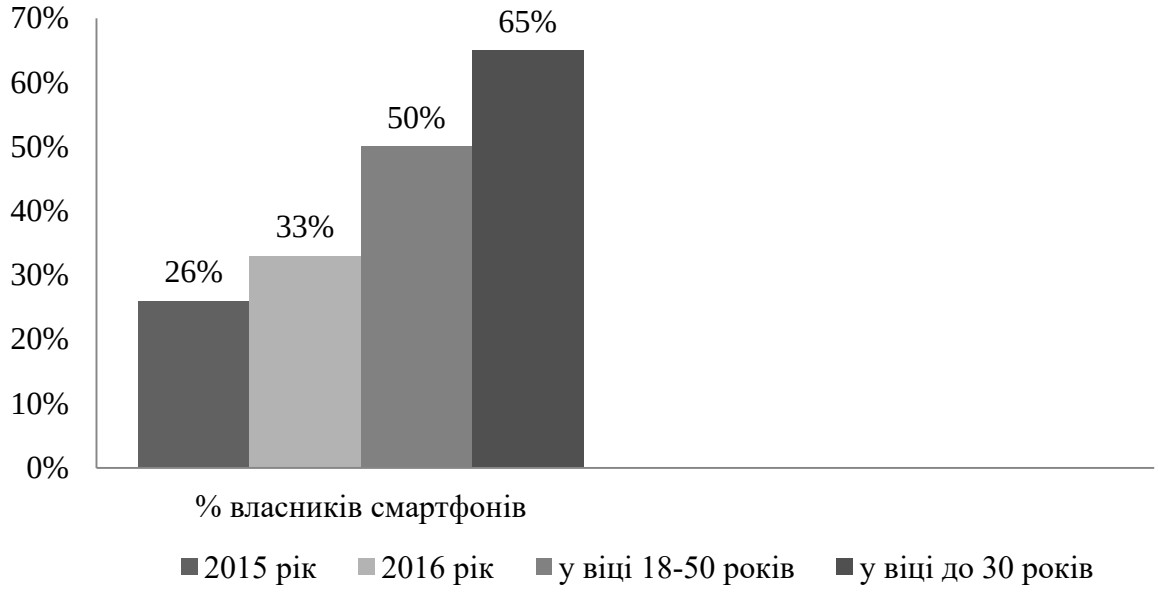

Рис. 1. Кількість власників смартфонів серед жителів України

Нажаль неуважні, або недосвідчені користувачі мобільних пристроїв встановлюють і зловмисне програмне забезпечення, яке може нанести особисту шкоду, чи принести збитки організації, в якій вони працюють. Зловмисник може отримати доступ до соціальних мереж, особистої та корпоративної пошти, даних платіжних карток, списку контактів, вимагати гроші заблокувавши мобільний пристрій, чи використовувати його для мережевих атак. Враховуючи швидкість передачі даних, його можливості збільшуються в рази.

Небезпеку для інформації несуть і відкриті Wi-Fi мережі, адже кожен має змогу до них підключитись та виконувати необхідні зловмисні дії. Також небезпечними можна вважати і умовно захищені мережі в публічних місцях чи організаціях, до яких можна підключитись прочитавши пароль з чеку чи дізнавшись його у працівника. Дані проблеми захисту інформації в бездротових мережах є актуальними та поширеними.

Ненадійні паролі зазвичай стають причиною хакерських атак. Після того як зловмисник підключиться до мережі, після проникнення він отримує доступ абсолютно до всіх підключених пристроїв. Крім того, якщо ненадійний або стандартний пароль використовується для панелі налаштувань, то всі пристрої також піддаються ризику хакерської атаки.

30% користувачів використовують в якості пароля слово з топ - 10 000 паролів. Збільшення словника до 10 000 000 дасть приріст всього до 33% всіх паролів [4, 5]. Третина всіх паролів, що використовуються, зламуються шляхом банального перебору варіантів зі словника. Список найбільш часто використовуваних паролів зазнав незначних змін за минулі кілька років. Знання користувачів в області інформаційної безпеки дуже обмежені, значне їх число не збирається приділяти час захисту своїх даних: майже 17% облікових записів були захищені паролем «123456» (рис. 2).

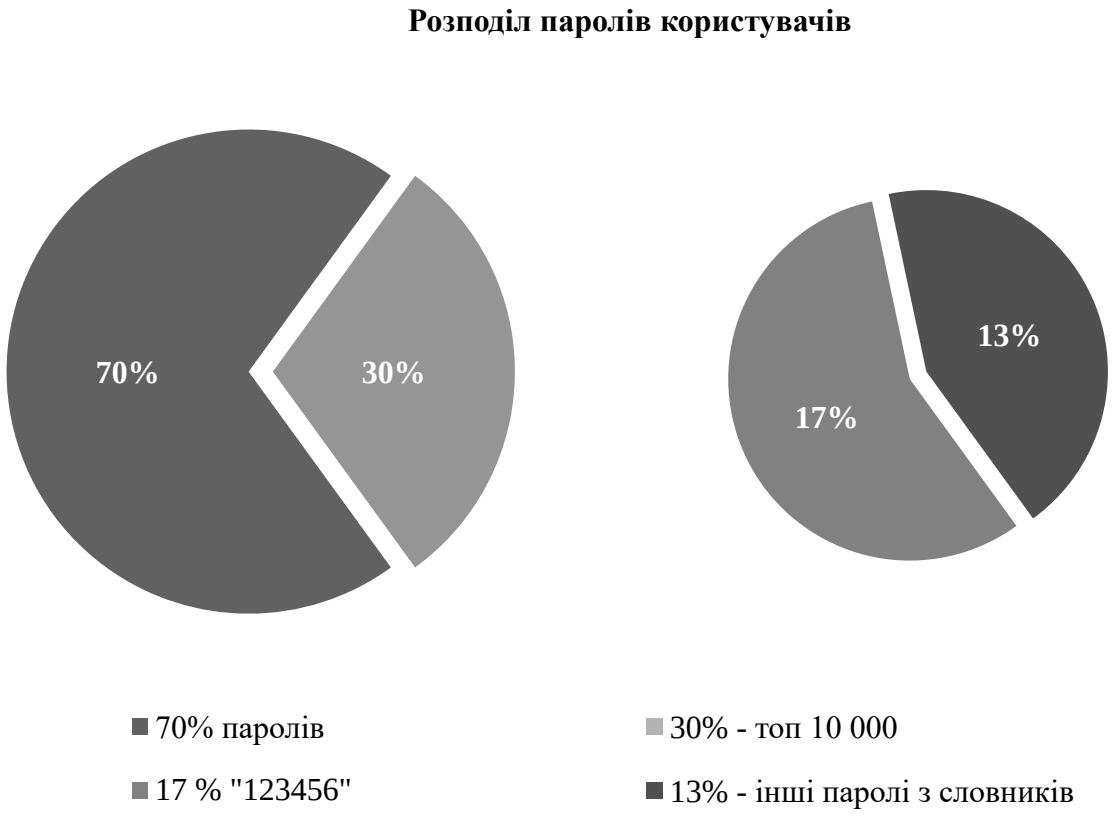

Рис. 2. Розподіл паролів користувачів

При цьому паролі розподілені наступним чином:
• 0.5% користувачів використовують в якості пароля password;
• 0.4% користувачів використовують в якості пароля password або 123456;
• 0.9% користувачів використовують в якості пароля password, 123456 або 12345678;
• 1.6% користувачів використовують в якості пароля слово з топ 10 паролів;
• 4.4% користувачів використовують в якості пароля слово з топ 100 паролів 100;
• 9.7% користувачів використовують в якості пароля слово з топ 500 паролів;
• 13.2% користувачів використовують в якості пароля слово з топ 1000 паролів;
• 30% користувачів використовують в якості пароля слово з топ 10 000 паролів.

Застосування таких паролів як «1q2w3e4r» і «123qwe» показує, що деякі користувачі намагаються використовувати непередбачувані поєднання символів для створення захищених паролів, проте їх зусилля як мінімум недостатні. Програми для злому паролів, засновані на словниках, в першу чергу аналізують такі поширені варіації. У кращому випадку, це збільшить час злому буквально на кілька секунд.

При умові підбору в 10 000 паролів за секунду, якщо за приклад словника паролів взяти перелік можливих мобільних телефонів, при форматі + 380 YY XXX XX XX (YY код регіону або мобільного оператора, де є 16 кодів оператора, або 48 кодів регіонів та операторів України, XXX XX XX номер телефону), то:

- для перебору мобільних номерів потрібно 4 години 26 хвилин,
- для кодів регіонів та операторів України потрібно вже 13 годин 20 хвилин.

В стійких паролів ситуація зовсім інша. Для комбінації, що можуть складатись з 63 символів у паролі для Wi-Fi мережі, які обираються з множини у 88 знаків, час для їх перебору буде становити більше 19 млрд. років!

Хакерська група, яка раніше інфікувала цілу «армію» пристроїв зі сфери Інтернету речей, цілеспрямовано заразила 3,2 мільйона домашніх Wi-Fi-маршрутизаторів за допомогою шкідливого програмного оновлення. Вони встановили сервер, який автоматично підключається до уразливих маршрутизаторів і відправляє інфіковане оновлення. Такий підхід надає їм постійний доступ до пристрою і можливість заблокувати обліковий запис власника, а також відповідні дії інтернет-провайдера і виробника обладнання [6].

Рівень розкриття кіберзлочинів в Україні становить в середньому 50%, при цьому 80% постраждалим вдається відшкодувати збитки, яких вони зазнали внаслідок дій злочинців.

За даними опитування у якому взяли участь 502 експерта в області інформаційної безпеки та IT-фахівців, у найближчі три роки інформаційна безпека матиме найбільший вплив на IT-стратегію компаній.

Рис. 3. Основні загрози інформаційної безпеки для організацій

Основною перешкодою для захисту компаній від кіберзагроз 65,1% вважають дефіцит бюджету, 47% - брак фахівців з IT-безпеки.

• Основні загрози інформаційній безпеці організацій (рис. 3) несуть забезпечення мобільності співробітників (51%) та Інтернет речей (20%) ;

• 4,2% організацій на сьогодні захищені максимально надійно;

• 49,7% - фахівців оцінюють захист на три бали з можливих п'яти.

Більше половини опитаних за останній рік мали проблеми з атаками, а саме: зараження шкідливим ПЗ - (70,2%), спам, фішинг і різні види інтернет-шахрайства (52,5%), DOS-атаки (37,4%), шпигунські атаки (20%), програми-вимагачі (18, 5%), спрямовані атаки хакерів (15,1%) і ботнети (12,5%).

Більша кількість компаній виявляють проблему протягом одного дня (37,3%). Протягом години це вдається зробити в 11,5% організацій, близько тижня потрібно для 31,5% фірм. Іншим компаніям потрібно більше часу.

Збиток, нанесений в результаті кібератаки, виражається переважно в збої системи (58,4%), втрата даних і неавторизований доступ до них також поширені: 25,2% і 14,9% відповідно. Крім того, в результаті дій зловмисників фахівці втрачали час, не могли скористатися необхідним обладнанням, втрачали доступ до зашифрованих зловмисниками даних, несли репутаційні втрати [7].

В свою чергу, кількість сім-карт на ринку України продовжує зменшуватись, незважаючи на продаж великої кількості смартфонів на дві сім-картки (більше 90%) можна зробити висновок, що користувачі стали більше приділяти увагу економії у використанні ресурсів мережі та більш сумлінно відноситись до можливостей своїх пристроїв [8].

Висновки

Інформаційна безпека не несе за собою можливості заробітку, оскільки потребує певних витрат, але завдяки цим витратам можливо захистити установи від значних майбутніх збитків.

Враховуючи розвиток та поширення сучасних мобільних пристроїв, зростання їх апаратних можливостей, а також швидкості передачі даних в мережах мобільного зв’язку, для більш ефективного захисту треба бути уважнішим, використовувати перевірене програмне забезпечення, різні паролі для облікових записів, блокування пристрою (пін-код, пароль, тощо), віддалене управління на випадок втрати.

Необізнаність користувачів та адміністраторів мереж, що призводить до великої ймовірності перехоплення інформації вирішується навчанням правилам інформаційної безпеки. Ймовірність перехоплення інформації можна зменшити шляхом використання засобів захисту в повному обсязі, але проблема відсутності коректного налаштування може залишатись, через використання нестійких паролів.

Використовуючи спеціалізоване програмно-апаратне забезпечення є можливість підвищити рівень захисту мереж від зловмисних дій, а правильне налаштування та відповідальне використання особистої техніки допоможе ефективно та безпечно використовувати можливості сучасних мобільних пристроїв.

Таким чином важливо поєднувати зусилля в підвищенні обізнаності користувачів фахівцями у галузі інформаційної безпеки, виробниками мобільних пристроїв, провайдерами послуг та технічного забезпечення, адже більшість користувачів, нажаль навіть не замислюється над можливістю того, що їх пристрої можуть піддаватись загрозам.

Література

1. Засоби інформаційної безпеки для мобільних пристроїв у корпоративних мережах/ А. В. Платоненко. Матеріали Науково-технічної конференції «Світ телекомунікації та інформатизації». – ДУТ. – 2015 р.

2. Сучасні загрози інформаційної безпеки для державних та приватних установ України / А. В. Платоненко, Київ, ДУТ, Сучасний захист інформації. Науковий журнал. – 2015. – № 4, с. 86 – 90.

3. Використання смартфонів в Україні [Електронний ресурс] – Режим доступу: http://lead9.com/slide/slide.pdf (20.02.2017).

4. Некоторые интересные факты о подборе паролей [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153530 (20.02.2017).

5. Опубликованы наиболее часто используемые пароли 2016 года [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153680 (20.02.2017).

6. Hacker Claims To Push Malicious Firmware Update to 3.2 Million Home Routers [Електронний ресурс] – Режим доступу: https://motherboard.vice.com/en_us/article/hacker-claims-to-push-malicious-firmware-update-to-32-million-home-routers (20.02.2017).

7. Cisco исследовала основные тенденции в сфере информационной безопасности на украинском рынке [Електронний ресурс] – Режим доступу: http://www.pcweek.ua/themes/detail.php?ID=153526 (20.02.2017).

8. Украинцы постепенно отказываются от лишних SIM-карт [Електронний ресурс] – Режим доступу: http://itc.ua/news/ukraintsyi-postepenno-otkazyivayutsya-ot-lishnih-sim-kart (20.02.2017).

Надійшла 10.03.2017 р. Рецензент: д.т.н., проф. Шевченко В.Л.