Кільдішев В.Й.
кандидат технічних наук, доцент;
Стайкуца С.В.
кандидат філософських наук, доцент;
Овчаров В.О.
студент,
Одеська національна академія зв'язку імені О.С. Попова

АНАЛІЗ УРАЗЛИВОСТЕЙ ПЕРСОНАЛЬНИХ МОБІЛЬНИХ ПРИСТРОЇВ

Кількість мобільних пристроїв, якими користується людство, стрімко зростає. Так, за даними дослідження GSMA The Mobile Economy, яке було представлено на Всесвітньому мобільному конгресі в Барселоні, кількість унікальних користувачів мобільних пристроїв за наступні п'ять років зросте з 3,6 млрд чоловік до 4,6 млрд людей. Щорічне зростання складе 4%. Це означає, що до 2020 року 60% населення будуть володіти одним або більше мобільним пристроєм [1]. Згідно даних аналітичної компанії StatCounter, в минулому році кількість підключень до сайтів з мобільних пристроїв по всьому світу вперше перевищила використання інтернету зі стаціонарних комп'ютерів та ноутбуків і склало 51,3% від загального використання мережі Internet [2]. Мобільність, високі швидкості роботи з інформацією та зручна робота з контентом, великі обсяги інформації, яка передається, доступність багатьох сервісів, універсальність – це тільки частина критеріїв, які впливають на загальну динаміку. До найбільш поширених мобільних пристроїв відносяться смартфони, планшети, телефони, КПК, нетбуки, ноутбуки, розумні годинники, окуляри віртуальної реальності тощо.

Варто відзначити, що в умовах все більшого залучення смартфонів і планшетів в бізнес-процеси організацій управління мобільними пристроями стає найважливішим завданням. Рушійною силою «мобілізації» для більшості користувачів в першу чергу виступає можливість доступу до корпоративних інформаційних ресурсів організації. Прагнення керівництва задовольнити цю бізнес-потребу своїх співробітників породжує ряд проблем з точки зору інформаційної безпеки. Серед фахівців IT близько двох третин (64%) очікують збільшення числа інцидентів мобільної безпеки та стурбовані впливом інцидентів мобільної безпеки на бізнес-процеси компаній. Загальна статистика проблематики інцидентів мобільної безпеки представлена на рис. 1.

Витрати, пов'язані з усуненням наслідків інциденту інформаційної безпеки в результаті втрати або крадіжки інформації з мобільного пристрою, широко варіюються в залежності від включення в них робочого часу співробітників, витрат на юридичну підтримку, штрафи і процеси вирішення проблеми, а також інших витрат. Більшість професіоналів IT відзначають, що вартість усунення наслідків інциденту мобільної безпеки зростає. Розглянемо більш детально основні уразливості мобільних пристроїв.

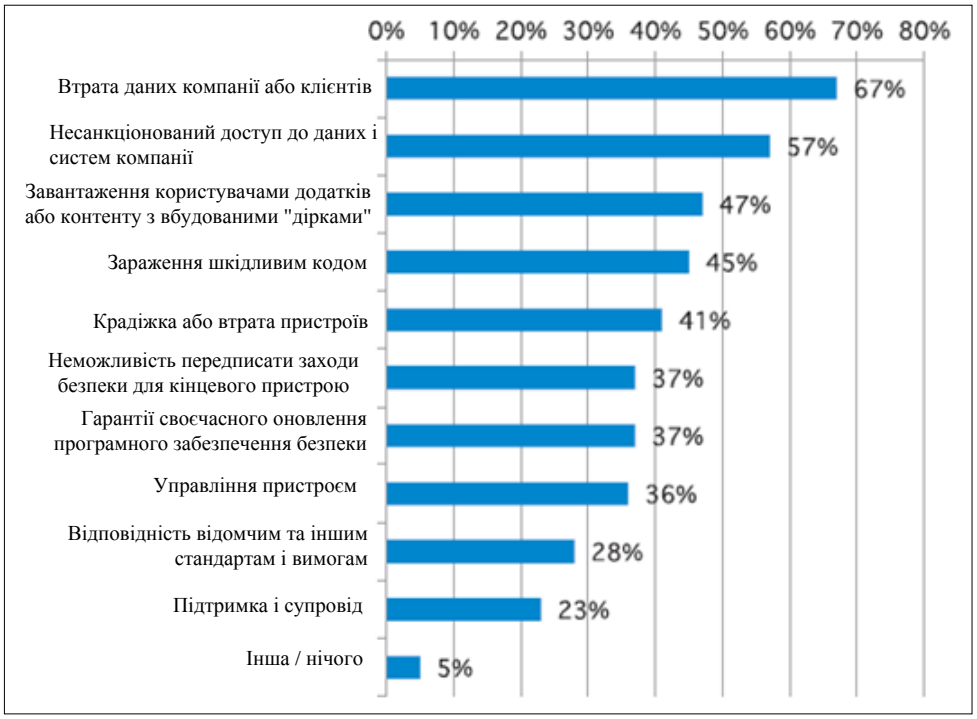

Рис. 1. Статистика найбільш небезпечних проблем, пов'язаних з використанням мобільних пристроїв

В даний час мобільні віруси є однією з найбільш поширених проблематик, з якою стикаються користувачі та виступає основою для формування класу програмних загроз [3]. Мобільний вірус – це програма, яка призначена для втручання в роботу мобільного пристрою за допомогою запису, пошкодження або видалення особистих даних. Поширюються мобільні віруси через типові канали зв'язку (SMS/MMS, Bluetooth, Wi-Fi, мережу Internet). Віруси можуть непомітно для користувача провести масову розсилку SMS і MMS, за яких абонентові доведеться платити та несанкціоновано дзвонити на платні номери, знищити дані користувача (телефонна книга, файли і т.д.) або викрасти конфіденційну інформацію, заблокувати функції телефону або апарат в цілому, розсилати від імені користувача заражені файли тощо. Більшість відомих вірусів для смартфонів відноситься до класу троянських програм і використовує для реалізації своєї функціональності уразливості операційних систем (як програмні помилки, так і функції, що передбачені при розробці ОС).

Згідно статистичних показників 2016-2017 років, ринок мобільних ОС розподілений між Android (84%), iOS (12%) і Windows Mobile (5%). Використання певного типу мобільної операційної системи позначається на параметрах захищеності самого мобільного пристрою. На це впливають різні критерії, наприклад, відкритість операційної системи, наявність вбудованих систем захисту інформації та функцій комплексної системи захисту інформації (КСЗІ), тип пристрою і т.д. Так, відкритість ОС Android робить її досить вразливою для проведення несанкціонованих дій – отримання зловмисником root-прав, використанні неофіційних прошивок, використанні помилок програмних модулів і уразливостей «нульового дня» [4].

Проте, не всі загрози безпеки виходять від зловмисників, які мають намір скомпрометувати або вкрасти критичні дані. Так, клас фізичних загроз створюється самим користувачем, як правило, за необачністю або халатністю. До цього класу загроз можна включити, насамперед, втрату пристрою, в результаті чого дані або контрольні повноваження можуть бути використані несанкціоновано. Також існує можливість несанкціонованого втручання на програмному або апаратному рівнях, що дозволить збирати або спотворювати дані як на рівні пристрою, так і на рівні організації. Взагалі, до класу фізичних загроз можуть бути включені такі дії, як:

- втрата пристрою;
- несанкціонований фізичний доступ;
- використання специфічних функцій пристрою;
- втручання в ланцюг постачання компонентів;
- використання зовнішнього обладнання.

До наступного класу загроз відносяться мережеві загрози, які здійснюються через мережу оператора зв'язку або мережеві протоколи, а також пристрої, додатки і дані, які постійно використовують мережу [5]. Загальна класифікація мережевих загроз представлена на рис. 2.

Рис. 2. Загальна класифікація мережевих загроз мобільних пристроїв

Інші класи загроз можуть включати до себе загрози з боку постачальника послуг, (як операторів зв'язку, так і постачальників мобільного програмного забезпечення), web-загрози (отримання мобільного коду, завантаження «на льоту» та використання уразливого браузера) тощо.

Отже, мобільні пристрої, які застосовуються як персонально, так і в корпоративному сегменті, схильні до цілої низки потенційних загроз. Для організації безпеки мобільних пристроїв користувачі повинні підвищувати рівень знань для формування «культури інформаційної безпеки», а також застосовувати вбудовані та додаткові методи і засоби захисту.

Список використаних джерел:

1. Нестерчук Я. К 2020 году количество мобильных пользователей вырастет до 4,6 млрд. человек [Електронний ресурс] / Яна Нестерчук // IGate. – 2015. – Режим доступу до ресурсу: http://igate.com.ua

2. Mobile and tablet internet usage exceeds desktop for first time worldwide [Електронний ресурс] // GlobalStats. – 2016. – Режим доступу до ресурсу: http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide.

3. В.Н.Конев, М.И. Фроимсон, Д.М.Михайлов, В.Л. Евсеев // Вирусные атаки на современные мобильные платформы.

4. Фроимсон М. И. Основные принципы построения защищенной операционной системы для мобильных устройств / М. И. Фроимсон, С. В. Кутепов, О. В. Тараканов. // Спецтехника и связь. – 2013. – №1. – С. 43–47.

5. Безопасность мобильных технологий в корпоративном секторе. Общие рекомендации. – Москва, 2015. – (АРСИБ), – 24 с.

Клекот Р.О.

бакалавр,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

«ІНФОРМАЦІЙНА ВІЙНА» – ФЕНОМЕН XXI СТ. СУЧАСНІ ВИКЛИКИ ДЛЯ УКРАЇНИ

Інформаційна війна стала різновидом бойових дій, у яких ключовим об'єктом впливу є інформація, що зберігається або циркулює в керуючих, державних, оборонних, розвідувальних, контррозвідувальних енергетичних, транспортних та інших важливих системах супротивника.

Інформаційна війна може вестись між людськими спільнотами, які мають власні системи влади, що володіють різними, в чомусь взаємовиключними, антагоністичними системами цінностей, включаючи ідеологію і систему влади. Такими групами є визнані і невизнані держави, союзи держав, сторони громадянської війни, екстремістські, у тому числі терористичні організації, які прагнуть до насильницького захоплення влади, сепаратистські, визвольні рухи тощо.

Варто погодитись з думкою багатьох вітчизняних аналітиків стосовно того, що загрози від проведення інформаційної війни спричинили появу серйозних викликів для України як цілісної, незалежної держави.