УДК 004.056.5:004.738.5(045) **О.О. Мелешко, О.С. Болотнікова**

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В МОБІЛЬНИХ ПРИСТРОЯХ ВІД ВИТОКУ

Основним завданням даної статті є пошук способів захисту інформації з обмеженим доступом, що зберігається на мобільному пристрої від злому, крадіжки й просто втрати смартфону. Визначити та розглянути найпоширеніші та більш надійні варіанти захисту інформації на мобільному пристрої. При цьому визначити які дані можна віднести до інформації з обмеженим доступом.

***Ключові слова*:** мобільні телефони, безпека інформації, засоби захисту інформації, смартфон, пароль.

Вступ

На сьогоднішній день проблема захисту інформації з обмеженим доступом у мобільних телефонах стає дедалі актуальнішою. Адже на даний момент мобільний телефон є майже у кожного. Дана технологія є повноцінним обчислювальним пристроєм, що підтримує більшу частину функціоналу традиційних електронно обчислювальної машини (ЕОМ) при значно менших розмірах, що дозволяє обробляти інформацію віддалено й оперативно, скоротивши на цьому час і зусилля, витрати часу на переміщення до комп'ютера, адже мобільний пристрій знаходитися практично завжди при собі. Враховуючи той факт, що інформація яка зберігається може містити в собі даны різного рівня (типу) конфіденційності, тому втрата її може нести великі збитки.

Об'єктами захистує інформація, що міститься та обробляється на мобільному телефоні, права власника цієї інформації та власника мобільного пристрою, права користувача.

Доступ до інформації, яка зберігається, обробляється і передається в мобільному пристрої, здійснюється лише згідно з дозволу наданим власником інформації чи уповноваженою ним особою.

Без дозволу власника доступ до інформації, яка зберігається, здійснюється лише у випадках, передбачених чинним законодавством.

Постановка проблеми

Сьогодні мобільний телефон використовується не лише для дзвінків й СМС, але й для виходу до мережі Інтернет. Люди використовують смартфони для завантаження нових ігор, гаджетів, перегляду сторінок у соціальних мережах, таких як ВКонтакте, Facebook. Адже мобільні оператори не обмежують своїх користувачів у вільному доступі до мережі.

Враховуючи на всі свої плюси, смартфони мають й недоліки, а саме своїми можливостями зберігати, передавати інформацію вони зацікавлюють зловмисників. Тому потенційною жертвою злому й атак хакерів може стати будь-який смартфон, незалежно від марки чи статусу власника.

З цього всього можна зробити висновок, що цінну інформацію (документи, фото, відео) легко втратити, завжди існують різні варіанти: злому, крадіжки, втрати мобільного пристрою. Виникає питання, як захистити мобільний телефон?

Постановка завдання

Завданням даної статті є пошук способів захисту інформації, що зберігається на мобільному пристрої від злому, крадіжки й просто втрати смартфону. Визначити та розглянути найпоширеніші та більш надійні варіанти захисту інформації на мобільному пристрої.

Аналіз досліджень і публікацій

Розглянемо типові дані, що зберігаються на смартфоні, які можуть бути корисні для зловмисника і тому потребують захисту.

1. Доступ до пошти і поштової скриньки.

Як правило, доступ до поштових сервісів і синхронізація пошти налаштовуються на мобільному пристрої одноразово, і у разі втрати або викрадення смартфону зловмисники дістають доступ до усього листування, а також до усіх сервісів, що прив'язані до цієї поштової скриньки.

2. Jabber-клієнт.

Skype, Icq, Jabber - усе це спостерігається в сучасних мобільних пристроях, внаслідок чого і усе листування цієї конкретної людини, і його співрозмовника можуть бути під загрозою.

3. Документи, замітки.

Як було сказано раніше, на даний момент мобільні телефони можуть стати місцем зберігання, редагування яких-небудь документів, так само як і різні замітки і події в календарі. Місткість сучасних пристроїв настільки велика, що вони могли б замінити usb-накопичувачі, а документи і файли на них цілком здатні зацікавити зловмисників. Як правило, в смартфонах звичайні користувачі зберігають взамітках, чи інших текстових редакторах, паролі, електронні адреси тощо.

4. Історія СМС – листування і телефонна книга.

Іноді відомості про певних людей коштують дуже дорого.

5. Мережеві засоби.

Використання смартфону або планшета для віддаленого доступу до робочого місця за допомогою TeamViewer і інших засобів віддаленого адміністрування вже не рідкість. Тому втративши свій телефон, користувач піддає сумніву захист інформації не лише на пристрої, а й на комп’ютері, до якого може під’єднатися.

6. Мобільний банкінг.

Якщо користувач використовує на своєму мобільному пристрої систему Дистанційного банківського обслуговування (ДБО), що дає даному клієнту можливість зробити самостійний вибір в певних видах послуг. Сучасні браузери цілком дозволяють здійснювати подібний вид діяльності і цей же мобільний пристрій прив'язаний до банку для отримання sms- паролів і сповіщень. Нескладно здогадатися, що уся система ДБО може бути скомпрометована втратою одного пристрою.

7. Карта пам'яті.

Як правило, накарті зберігають фото і відео зйомку.

Викладка основного матеріалу дослідження

Для вирішення питання щодо захисту інформації на мобільному пристрої існує кілька варіантів, а саме:

1. Вимикати Wi-Fi і Bluetooth на телефоні, коли не користуєтеся Інтернетом.

Контроль за бездротовими мережами і злом телефону через Wi-Fi - улюблена "забава" хакерів. Якщо ці функції у Вас весь час включені, стороннім значно легше проникнути в ваш телефон. Це можна пояснити на прикладі наступної ситуації: на мобільному пристрої весь час активні Wi-Fi та Bluetooth, побачивши це зловмисник може визначити до яких саме мереж було здійснено підключення, потім зімітувати їх, в результаті чого ваш телефон підключиться до пристроїв, що належить зловмиснику (така атака називається «злий двійник»). Після з'єднання з пристроєм, зловмисники атакують його за допомогою спеціальних програм, викрадаючи дані, або можуть почати стежити за вами. Причому ви цього навіть не помітите.

2. Користуйтеся двоетапною автентифікацією для входу.

Автентифікація - процедура встановлення належності користувачеві інформації всистемі, шляхом перевірки введеного паролю і логіну, із паролем і логіном у відповідній базі даних [6]. Але один пароль не гарантує достатній захист телефону. Паролі від пошти постійно зламують. Тому для того щоб забезпечити максимальну безпеку, багатопоштових

сервісів і соціальні мережі пропонують додатковий рівень захисту: автентифікацію з двох кроків.

Двоетапна аунтифікація являє собою використання для входу різних методів паролів: текст, одноразовий код, смс-повідомлення, відбиток пальця тощо. Звичайно, пароль зловмисники можуть отримати різним шляхом, але вони не зможуть прочитати одноразового коду у смс-повідомленні, що прийде на певний номер, для підтвердження.

1. Використовуйте складні паролі

Прості паролі легко запам'ятати, такі як: дата народження, «1111», але вони навряд будуть надійні. Пристрій можна вважати більш захищеним при наявності пароля довжиною 6-8 символів, що складаються з символів кирилиці, цифр та, якщо є можливість, символів «*,!,@,$».

2. Встановіть антивірусні програмні забезпечення

На сьогоднішній день існує багато програмних засобів «антивірусів», що виконують аналогічні функції на смартфонах, як на ПК. До їх задач входить перехоплення вірусів й інших шкідливих пакетів, що можуть нести загрозу.

3. Завантажуйте додатки з розумом

Будь-які додатки можуть зробити ваш смартфон вразливим. Завантажуйте лише ті додати, що дійсно вам потрібні й з надійних джерел (офіційних магазинів додатків для вашої платформи) таких як Google Play маркет, Marketplace, ITunes. При цьому завжди потрібно звертати увагу на то, які саме дані цей додаток потребує при встановленні. Дуже часто користувачі погоджуються та без питань надають свою інформацію для встановлення додатків, яка по суті в дійсності там не потрібна, таким чином надаючи її третій особі.

3. Створення резервних копій даних

Більшість смартфонів мають функцію синхронізації даних з їх хмарними сервісами зазвичай це робиться вручну або автоматично. Синхронізуйте дані зі своїм домашнім комп'ютером або ноутбуком з періодичністю 1 раз на тиждень чи навіть частіше, залежно від того, наскільки висока важливість інформації та контенту на вашому телефоні .

Синхронізація - необхідна для того щоб на всіх ваших пристроях були необхідні дані і випадку втрати або блокування телефону, ви змогли швидко відновити їх. Витративши один раз час, в подальшому ви будете його економити, налаштувавши синхронізацію, можна миттєво налаштувати пристрій, щоб на вашому телефоні відразу були всі ваші контакти і налаштування. Дана процедура є на всіх сучасних смартфонах: Iphone, Android 4.4, Windows Phone.

4. Віддалений доступ

Цей спосіб дозволяє мати обмежений доступ до пристрою. Він є зручним у випадку крадіжки чи втрати мобільного. Найчастіше він застосуємо до телефонів або смартфонів, але можливе використання його також з планшетами.

З функцій, доступних користувачеві в цьому способі, можна відзначити можливість відстежити місцезнаходження телефону, зателефонувати на нього і заблокувати доступ до нього (рис. 1).

Ще можна налаштувати скидання даних. Для того щоб ці можливості були доступні, необхідно мати акаунт в Google, а також зробити певні настройки всамому смартфоні, а саме включити у кладці «Безпека» - «Віддалений пошук пристрою», «Дистанційне блокування і скидання налаштувань». Активувавши дані функції ви запустите віддалений доступ.

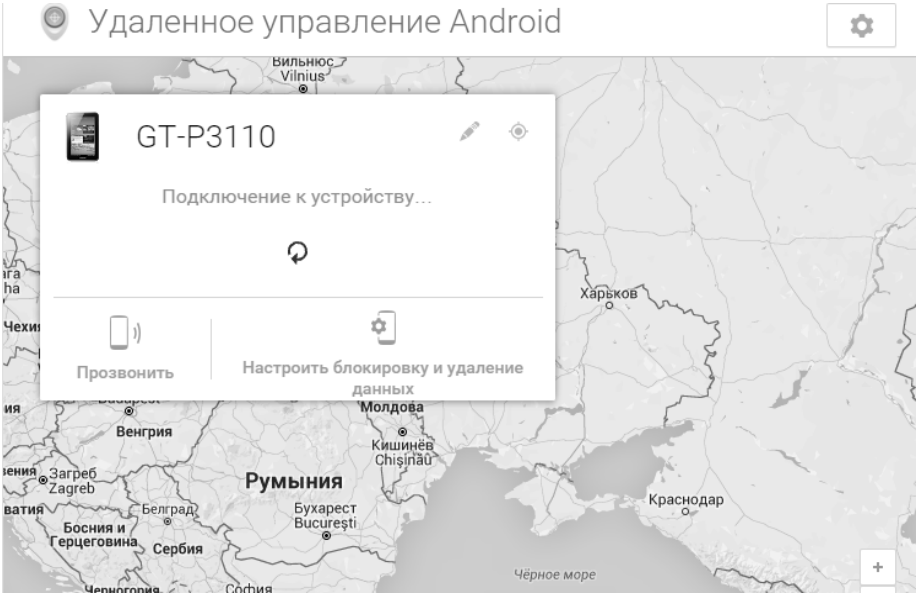

Рис. 1. Функції, доступні користувачеві при використані віддаленого доступу

Також є можливість запустити дану функцію й через додаткові програмні додатки, що з'єднують комп'ютер з смартфоном.

Висновки

Визначивши інформацію, яку ми можемо віднести до інформації з обмеженим доступом та розглянувши варіанти захисту інформації на смартфонах, можна підвести висновок. Для захисту інформації від зловмисників треба дотримуватись певних елементарних правил, а саме: вимикати Wi-Fi і Bluetooth на телефоні , коли не користуєтеся Інтернетом; використовувати складні паролі; завантажувати додатки з розумом.

Додатково, для більшої надійності, доречно буде робити резервні копії та додати віддалений доступ. Таким чином, інформація з обмеженим доступом, що зберігається на мобільному пристрої буде у більшій безпеці від злому та втрати.

Література

1. Михайлов Д. М., Жуков И. Ю., Ивашко А. М. Защита мобильных телефонов от атак М.: Фойлис, 2011. - 192 с.

2. Якушин Петр. Безопасность мобильного предприятия/ П.Якушин// Открытые системы – 2013 - № 1 (187) – с. 22-27.

3. Панасенко А. Влияние мобильных устройств на безопасность информации – [Електронний ресурс] – Режим доступу: http://www. anti-malware.ru/node/12301, 2013.

4. Гилмор Дж., Бирдмор П. Безопасность мобильных устройств для «Чайников» М.: John Wiley & Sons Ltd, Chichester, West Sussex, England (Англия), 2013. – 54 с.

5. Ванг Й., Стрефф К., Раман С. Проблемы безопасности смартфонов//ОТКРЫТЫЕ СИСТЕМЫ. СУБД, М: Издательство «Открытые системы», 2013. - 27-31 с.

6. Мельников Д. А. Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА. – 2013.

Надійшла 30.01.2016 р. Рецензент: д.т.н., проф. Шелест М.Є.