УДК 004.056.5: 004.738.5(045)

О.О. МЕЛЕШКО, канд. техн. наук, доц., О.С. БОЛОТНІКОВА, студентка,
Національний авіаційний університет
К.В. ГЕРАСИМОВА, канд. техн. наук, доц., Криворізький національний університет

СПОСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В МОБІЛЬНИХ ПРИСТРОЯХ В КОРПОРАЦІЇ ВІД ВИТОКУ

У даній статі визначено, що основним завданням є пошук способів захисту інформації з обмеженим доступом у корпораціях, що зберігається на мобільному пристрої від злому, крадіжки й просто втрати смартфону.

Виявлено, що на сьогоднішній день концепція BYOD (Bring Your Own Device) стає все далі актуальнішою, адже вона досить вигідна як для робітників, так і для керівників компанії. Адже використовуючи особисті пристрої в роботі, компанія чекає збільшення продуктивності праці і зниження витрат, пов'язаних з мобільними пристроями. Але як і будь-який пристрій мобільні пристрої та планшети мають свої слабкі місця, у зв'язку з цим розглядається ряд проблем, що можуть з'явитись з точки зору інформаційної безпеки.

Визначено та розглянуту три різні рівня захисту, що можуть залежати від того які саме пристрої використовуються в компанії. Розглянуто різні варіанти розмежування доступу до особистих й корпоративних даних на одному пристрої таких як: MDM - «Mobile Device Management», розробка контейнерів інформації та віртуалізація.

Для вирішення питання щодо захисту інформації на мобільних пристроях розглянуто декілька легких, але в той же час й ефективні загальноприйняті варіантів, а саме: двоетапна аутентифікація, складні паролі, віддавлений доступ до пристрою, створення резервних копій та інші.

У результаті автори надають поради, що до оптимального захисту мобільного пристрою(планшету), для оптимального використання його для роботи в офісі, корпорації тощо.

Проблема та її зв'язок з науковими та практичними завданнями. За останні роки використання мобільних пристроїв в корпоративному середовищі набирає все більшої популярності. 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

Проникнення особистих мобільних пристроїв в корпоративну мережу, перш за все, пов'язано з позитивними очікуваннями від BYOD (BYOD (Bring Your Own Device) - "Візьми Своє Власне Пристрій на роботу"), як з боку власників бізнесу так і співробітників. Використовуючи особисті пристрої в роботі, компанія чекає збільшення продуктивності праці і зниження витрат, пов'язаних з мобільними пристроями. Дійсно видавати всім корпоративні пристрої і підтримувати їх - це дороге задоволення [1].

Надавши можливість використовувати особисті пристрої і дозволяючи доступ до корпоративних ресурсів ззовні, компанія знімає з себе необхідність забезпечення їх підтримки та закупівлі, при цьому очікує підвищення ефективності праці та оперативності дій співробітників. Тому перехід користувачів і бізнесу на мобільні пристрої практично неминучий.

Враховуючи той факт, що дані які зберігається можуть містити в собі інформацію різного рівня (типу) конфіденційності, то втрата її може нести великі збитки як для однієї особи, так і для всієї компанії.

Об'єктами захисту є 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.

З огляду на той фактор, що на сьогоднішній момент залучення смартфонів і планшетів досить таки добре розвивається, розглянемо ряд проблем, які можуть з'явиться в подальшому з точки зору інформаційної безпеки порушення конфіденційності інформації в результаті крадіжки або втрати пристрою;порушення конфіденційності інформації в результаті доступу сторонніх осіб до пристрою, залишеному без нагляду; доступ до конфіденційної інформації

зовнішніх порушників за допомогою використання шкідливого програмного коду; розкрадання інформації працівником, який має легітимний доступ до інформації і зберігає цю інформацію на своєму пристрої (шляхом відправки через особисту пошту та ін.) [2,3].

Проблема посилюється так само тим, що значна кількість використовуваних пристроїв є особистими, а це означає, що працівник може звертатися з ним як завгодно.

У реальності особисті мобільні пристрої приносять некерованість мобільного середовищем користувачів і втрату безпеки. Фактично використання мобільних гаджетів для компанії різко змінює карту ризиків, де на перше місце виходять такі проблеми як зберігання важливих даних на мобільних пристроях і забезпечення контролю використовуваних корпоративних ресурсів. Як наслідок постає питання серйозних інвестицій на забезпечення інформаційної безпеки мобільних користувачів в рамках BYOD.

Аналіз досліджень і публікацій. У реальності, особисті мобільні пристрої приносять некерованість мобільного середовищем користувачів. Задача забезпечення захисту мобільних співробітників складається з створення політики забезпечення безпеки при віддаленому доступі і обробці даних, а також перевірки на їх основі мобільного пристрою, принесеного в корпоративну мережу. Такий підхід для компанії вибудовується в комплексну стратегію захисту мобільних співробітників.

Компанії неминуче стикаються з питанням, а що конкретно треба захищати і як це можна зробити. Експерти виділяють три різних рівня захисту в залежності від того які пристрої використовуються в компанії [3,4]:

1. Захист пристроїв (для корпоративних пристроїв):

впровадження технології управління пристроями (MDM - «Mobile Device Management»); запровадження суворих політик безпеки для пристроїв; локальне шифрування даних на пристрої; створення захищених розділів (контейнерів) на пристроях.

2. Захист додатків (для різнорідної середовища з великим парком рішень):

тісний зв'язок з розробниками додатків на предмет безпеки; безпечне поширення і оновлення програм.

3. Захист даних (для особистих мобільних пристроїв):

контроль зліпків пристроїв (fingerprint); шифрування каналу передачі даних; віртуалізація і віддалений робочий стіл; забезпечення цілісності даних (контроль життєвого циклу даних).

Фактично використання мобільних гаджетів для компанії різко змінює карту ризиків, де на перше місце виходять такі проблеми як зберігання критичних даних на мобільних пристроях і забезпечення контролю використовуваних корпоративних ресурсів. Як наслідок постає питання серйозних інвестицій на забезпечення інформаційної безпеки мобільних користувачів в рамках BYOD.

Постановка завдання. Завданням даної статті є пошук способів захисту інформації, що зберігається на мобільному пристрої від злому. Визначити та розглянути най поширеніші та більш надійні варіанти захисту інформації на мобільному пристрої.

Викладення матеріалу та результати. Актуальним питанням стає захист корпоративних даних, а саме як вони будуть зберігатись та використовуватись на пристрої співробітників. Основна мета, це зручність та розмежування доступу до особистих й корпоративних даних на одному пристрої. це можливо реалізувати за допомогою різних засобів, всі вони розвиваються поетапно.

Спочатку для цих цілей застосовувалися рішення MDM, які програмними засобами розмежовували доступ до даних на мобільному пристрої. При цьому даний підхід застосовувався саме для пристроїв, якими володіла сама компанія, так як він вимагав не тільки установки додаткового програмного забезпечення, але і налаштування прав доступу через засоби централізованого управління. На жаль, даний підхід зажадав кардинальної зміни політик безпеки стосовно до особистих пристроїв і концепції BYOD, так як він фокусувався на захист самого пристрою, а не даних.

В результаті на зміну класичним MDM рішень прийшли продукти з підтримкою захищених контейнерів, які жорстко розділили функціонал MDM і захист даних. З одного боку, засобами централізованого управління забезпечувався контроль відповідності пристрою вимогам політик безпеки, з іншого, окремий програмний компонент в рамках MDM рішення створював зашифрований контейнер для роботи з даними. Більшість розробників MDM рішень сьогодні розви-

вають свої продукти саме за рахунок захищених контейнерів. Тим самим користувач при роботі з даними завжди працює в створеному просторі, яке в статичному вигляді завжди зашифровано і повністю виключає втрату даних у відкритому вигляді. Недоліком такого підходу стало те, що такого роду рішення шифрування даних працюють далеко не з усіма додатками (частіше всього обмеження створюються саме самим розробником і списком програм, які підтримуються).

Тобто подібного роду рішення незручно використовувати для корпоративних додатків, тільки якщо компанія сама не готова інтегрувати подібний функціонал.

Наступним логічним кроком в забезпечення безпеки корпоративних даних є технологія віртуалізації. Віртуалізація мобільних пристроїв - це технологія, що дозволяє запускати кілька операційних систем одночасно на одному і тому ж мобільному пристрої. Подібний підхід повністю відповідає вимогам роботи з особистими і корпоративними даними в рамках концепції BYOD. Фактично при роботі користувача з даними створюється кілька рівноправних і паралельно працюючих наборів програмного забезпечення, доступних з одного і того ж пристрою, але для різних профілів: корпоративного й персонального.

Існує три види віртуалізації [8]:

віртуальний робочий стіл;

принцип аналогічний стандартним рішенням для корпоративної інфраструктури з тонкими клієнтами, коли користувач працює з віддаленим робочим столом, не маючи можливості зберегти щось на свій локальне робоче місце;

хмарна віртуалізація.

Даний підхід має являє собою хмарний сервіс, коли на кінцевому пристрої користувача присутні лише ярлики для доступу до додатків, як зі своєї особистої операційної системи, так і з окремої оболонки, що створює візуальне подібність незалежного робочого столу або всієї операційної системи. При цьому всі дані зберігаються і обробляються на стороні хмарного хостингу, в якому відбувається також розмежування доступу до додатків і управління користувачами.

Для таких рішень є два підходи в реалізації.

Перша - це послуга з хмарного хостингу самого розробника рішення, де компанії надається лише платформа для побудови політик і вибору з готового списку додатків для співробітників

Другим є продукт для приватної хмарної інфраструктури, що дозволяє створювати не тільки політики для поширених додатків, але і додавати власні додатки для доступу з пристроїв співробітників

Даний вид рішень по віртуалізації мобільних пристроїв зараз набирає обертів на заході і подає великі надії, так як вимагає мінімальних змін на особистих мобільних пристроях.

Розглянемо віртуалізацію на самому пристрої. Технологія реалізує пряме виконання віртуального середовища на кінцевому пристрої користувача. Такий підхід включає в себе створення двох незалежних доменів на одному пристрої з можливістю швидкого перемикання між ними. При цьому є кілька принципово різних варіантів реалізації такого функціоналу:

створення паралельно працюють віртуальних доменів на єдиній апаратній платформі;

створення віртуального домену всередині реальної операційного середовища мобільного пристрою.

Для вирішення питання щодо захисту інформації на мобільному пристрої існує ще декілька загальноприйнятих варіантів, а саме :

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

Контроль за бездротовими мережами і злом телефону через wifi - 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 побачити 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 аутентифікацією для входу

Автентифікація - процедура встановлення належності користувачеві інформації в системі, 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, багато поштових сервісів і соціальні мережі пропонують додатковий рівень захисту : аутентифікацію 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.

3. Використовуйте складні паролі [7].

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

4. Установіть 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.

5. Завантажуйте додатки з розумом.

Будь-які додатки можуть зробити ваш смартфон вразливим. Завантажуйте лише ті додатки, 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.

6. 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.

7. 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).

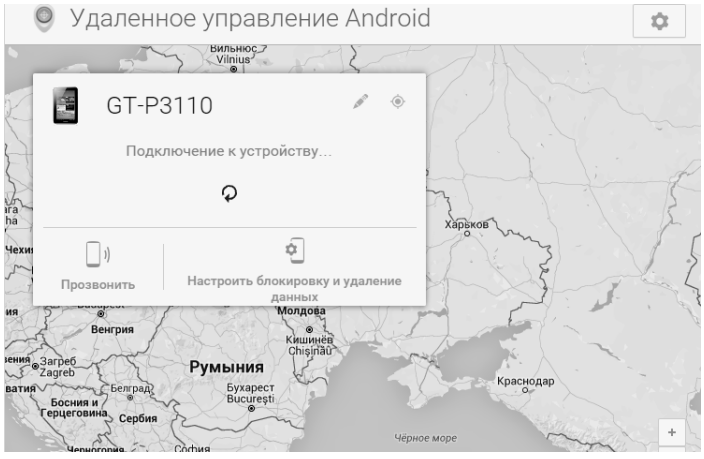

Рис. 1. Функції, що доступні користувачеві при використані віддаленого доступу

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

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

Висновки та напрямок подальших досліджень. Сьогодні концепція BYOD стає все далі актуальнішою, адже вона досить вигідна як для робітників, так і для керівників компанії. Адже співробітники можуть використовувати свої власні пристрої (мобільні, планшети) й працювати як в офісі, так й вдома, тим самим підвищуючи виробництво. Керівництво ж, вигідно заощаджує на закупівлі нового обладнання (додаткових комп'ютерів). Для захисту інформації від зловмисників треба дотримуватись певних елементарних вимог, а саме: створення віртуалізації; вимикати Wi-Fi і Bluetooth на телефоні, коли не користуєтеся Інтернетом; використання складних паролів; завантаження додатків з розумом.

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

Список літератури

1. **Гайкович В. Ю.** Проблема корпоративной мобильности/ **Гайкович В. Ю** // Защита информации. INSIDE – 2012 - №4 – С.2-5

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

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

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

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

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

7. **Мельников Д. А.** Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА, 2013.

8. **Дзюндзюк В. Б.** Віртуальні співтовариства: потенційна загроза для національної безпеки //Державне будівництво, 2011. – №. 1.

Рукопис подано до редакції 15.04.16

УДК 681.5: 622.2

В.С. МОРКУН, д-р техн. наук, проф,
Н.В. МОРКУН, В.А. ДВОРНИКОВ, И.В. КАСАТКИНА, кандидаты техн. наук, доц.
Криворожский национальный университет

АНАЛИЗ МЕТОДОВ ОПРЕДЕЛЕНИЯ ГРАНУЛОМЕТРИЧЕСКОГО СОСТАВА ТВЕРДОЙ ФАЗЫ ПУЛЬПЫ С ИСПОЛЬЗОВАНИЕМ ОБЪЕМНЫХ УЛЬТРАЗВУКОВЫХ ВОЛН

Известные методы ультразвукового контроля параметров пульпы позволяют определить две ее основные характеристики - плотность и гранулометрический состав. Для измерения этих параметров используются объемные и поверхностные ультразвуковые волны, а также их сочетания [1-4]. Ниже рассмотрены методы ультразвуковой гранулометрии на основе объёмных волн.

Пульпа представляет собой случайно неоднородную гетерогенную среду, содержащую в воде твердые частицы различного размера с распределением, описываемым функцией $F(r)$, где r - радиус частиц. Содержание частиц в пульпе может быть задано либо через концентрацию

$$n = N \cdot V^{-1},$$

либо через их объемную долю W. Амплитуда ультразвуковой волны частоты ν, прошедшей в среде расстояние Z, описывается зависимостью