8. **Петрухін А.В., Антонік В.І., Кулькова Т.М., Чепурний В.І., Гришко В.М.** та інші. Проведення комплексногоаналізу екологічного стану навколишнього природного середовища (НПС) Новолатівської сільської ради та розробка комплексної програми забезпечення екологічної безпеки території Новолатівської сільської ради на2017 – 2021 рр. Звіт НДР по темі 12-16 у 2-х т.- Кривий Ріг: НДГРІ, 2016.- 630 с.

9. **Антонік В.І., Антонік І.П.,** Екологічна характеристика стану водного басейну річки Інгулець // Сталий розвиток промисловості та суспільства. Матеріали міжнародної науково – технічної конференції / Редкол. Вілкул Ю.Г., Ступнік М.І., Азарян А.А. та ін. – Кривий Ріг : ВЦ ДВНЗ «КНУ» , 2014. С.112 – 113.

10. **Фатєєва А.І.**Фоновий вміст мікроелементів у ґрунтах України / За ред. **А.І.Фатєєва, Я.В.Пащенко**. – Харків, 2003. – 117 с.

Рукопис подано до редакції 14.04.17

УДК 004.056. 5: 004.738.5(045)

Е.А. МЕЛЕШКО, канд. техн. наук, доц., Е.С. БОЛОТНИКОВА, студентка
Национальный авиационный университ

ПРОБЛЕМЫ БЕЗОПАСНОСТИ МОБИЛЬНЫХ УСТРОЙСТВ, СИСТЕМ И ПРИЛОЖЕНИЙ В OS ANDROID

Цель работы. Повышение эффективности защиты информации с ограниченным доступом в мобильных устройствах путем разработки политик и регламентов использования мобильных устройств, анализа и выбора методов шифрования, ограничения использования вредоносного ПО. Систематизация и анализ корпоративных методов защиты внутренней информации. Минимизация корпоративных убытков за счет утечки информацию различного уровня (типа) конфиденциальности.

Методы исследования. Обзор и анализ факторов риска нарушения безопасности использования мобильных устройств. Анализ и систематизация методов зашиты информации на мобильных устройствах под управлением OS Android. Опытная проверка существующих способов защиты конфиденциальной информации на мобильном устройстве. Анализ алгоритмов установки стороннего ПО на устройства под управлением OS Android, поиск путей уязвимости и защиты внутренней информации.

Научная новизна. Выполнен анализ и систематизация угроз и способов воздействия на мобильные устройства. На основе выполненного анализа и систематизации разработан и практически проверен алгоритм использования методов защиты информации.

Результаты. На основании проведенных исследований уязвимости и методов защиты в OS Android установлено, что данная операционная система как собственные, внутренние средства защиты, так же может и поддерживать дополнительное, разработанное другими разработчиками. Встроенные внутренние средства защиты, достаточно удобными инструментами защиты данных на мобильных телефонах. Учитывая тип блокировки, выделяют различные виды безопасности. Они достаточно эффективны, но от внешних атак, то есть если кто-то хочет зайти на мобильный телефон и посмотреть какие-то определенные данные, то злоумышленник встречает препятствие в виде: пароля, рисунка, распознавание лица или PIN. Но от внутренних атак, вирусов, данные средства беспомощны. В то время как дополнительное программное обеспечение, может обеспечить, как безопасность от внутренних, так и от внешних атак.

Ключевые слова: OS Android; мобильные телефоны; безопасность информации; угрозы; конфиденциальность; целостность; доступность; средства защиты информации.

Проблема и ее связь с научными и практическими задачами. В настоящее время, практически у каждого есть такое устройство как мобильный телефон. Данная технология является полноценными вычислительными устройствами, поддерживающими большую часть функционала традиционных ЭВМ при значительно меньших размерах, что позволяет обрабатывать информацию удаленно и оперативно, сократив на этом время и усилия, затраты времени на перемещения к компьютеру. Учитывая тот факт, что хранящаяся информация может содержать в себе информацию различного уровня (типа) конфиденциальности, то потеря ее может нести большие убытки.

Анализ исследований и публикаций. Развитие высоких технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон/ зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента.

Сам аппарат многое может рассказать о своем владельце, ведь в его памяти хранятся: контакты коллег, друзей и близких с их персональными данными; журнал звонков; корпоративная переписка; параметры точек доступа Wi-Fi, которые расположены в пределах ареала обитания владельца; приложения социальных сетей (зачастую с сохраненными паролями); банковские реквизиты или мобильный/СМС банкинг, снимки, видеозаписи, заметки и пр.

Такая концентрация деловых и персональных данных приводит к тому, что абстрактная стоимость информации перевешивает цену самого устройства. Именно поэтому задача защиты телефона/планшета как от кибер угроз так и от банальной утери/выхода из строя является критически важной. К сожалению, часть пользователей осознает важность этих задач лишь постфактум.

Постановка задачи. Определить оптимальные методы защиты мобильных устройств, с помощью которых можно обеспечить безопасность хранящихся данных на устройстве.

Изложения материала и результаты. Итак, прежде чем перейти к содержательной части проблем безопасности объектов обозначенных в заголовке данной статьи, давайте конкретизируем основные понятия и определения интересующих нас именованных сущностей:

Мобильное устройство (*гаджет* – англ.) – это продукт информационно-коммуникационных технологий.

Мобильными считаются устройства, обладающие малыми габаритами и весом, как минимумом одним беспроводным интерфейсом доступа к Сети (мобильной связи или Интернет), встроенной (несъемной) памятью, операционной системой, не являющейся полноценной операционной системой настольных компьютеров и ноутбуков, возможностью установки приложений различными способами, имеющие встроенные средства синхронизации локально хранимых данных с удаленным источником. Кроме этого, устройство может обладать другими, необязательными свойствами, в частности, иметь не менее одного беспроводного персонального сетевого интерфейса типа Bluetooth или NFC, а также не менее одного беспроводного сетевого интерфейса для голосовой связи, например сотовый модуль;

Давайте разберемся от чего именно и каким образом можно (и нужно) защищать наши мобильные устройства, системы и приложения.

Угрозы и уязвимости мобильных устройств. Как правило, мобильные устройства должны обеспечивать решение нескольких задач информационной безопасности (триаду ИБ):

конфиденциальность – свойство информации, состоящее в том, что информация не может быть получена неавторизованным пользователем и процессом информационной системы. Информация сохраняет конфиденциальность, если придерживаются установленных правил ознакомления с ней;

целостность данных – свойство информации, которое определяется её пригодностью к использованию в разных отраслях целеустремленной деятельности человека;

доступность – возможность использования информации (данных), когда в этом возникает необходимость. Доступность так же характеризуется трудоспособностью информационной системы.

Прежде чем развертывать мобильные решения, компаниям и организациям стоит разработать модель рисков информационной безопасности, определив возможные уязвимые ресурсы, угрозы и средства обеспечения безопасности, вычислив вероятности успешных атак и их последствий, и т. п.

Мобильные устройства сотрудника обычно используются в местах, не контролируемых компанией, и даже если устройства используются внутри офиса, они переносятся с места на место, что создает угрозу утечки конфиденциальных данных. Смартфоны и планшеты могут быть потеряны или украдены, и данные, хранимые на них, подвергаются риску быть скомпрометированными.

При формировании политик и регламентов использования мобильных устройств необходимо учитывать, что такие устройства могут попасть в руки злоумышленников, которые попытаются получить конфиденциальные данные либо напрямую с устройства, либо используя их для удаленного доступа к ресурсам организации. Стратегия по смягчению последствий этого состоит из нескольких уровней.

Первый включает защиту конфиденциальных данных либо путем шифрования локального хранилища самого мобильного устройства, либо путем запрета локального хранения конфиденциальных данных.

Даже если мобильное устройство всегда находится при владельце, существуют другие угрозы безопасности - например, возможность подглядеть важные данные или процесс ввода пароля.

Использовать шифрование возможно только в том случае, если у пользователя установлена блокировка экрана с помощью пароля. С помощью шифрования пользователь может уберечь хранящиеся в памяти телефона.

У пользователя есть возможность зашифровать:

1. Учетная запись.
2. Параметры.
3. Загруженные и их данные.
4. Мультимедийные и другие файлы.

После шифрования устройства, при каждом его включении для расшифровки потребует PIN-код или пароль.

Необходимо учесть, что программа при этом не шифрует SD-карту. Шифрование может занять до 1:00, это зависит от объема памяти на смартфоне. В случае если пользователь забыл пароль, единственным вариантом разблокировки устройства, это сброс до заводских настроек. При этом все данные, которые хранились на устройстве будут потеряны.

Недостатки шифрования:

1. Данная услуга доступна в OS Android 4.0 и выше.
2. Доступно не на всех моделях смартфонов. Чаще всего эта функция встречается в телефонах от Samsung, HTC, Philips.
3. Пользователю необходимо постоянно вводить пароль, (6-10 символов) даже если нужно просто позвонить.
4. Если пользователь желает сняты защиту, то сделать это возможно только при полной перезагрузке телефона. Восстановил его к заводским настройкам.

3. Шифрование внешней SD-карты

Данная функция входит в стандартный набор пакета Android 4.1.1 и высших версиях. Она обеспечивает надежную защиту данных на внешний SD-карте. Здесь могут храниться только фотографии, текстовые файлы с информацией коммерческого и личного характера.

Позволяет зашифровать файл на SD-карте, не меняя ее названия, файловой структуры, с сохранением предварительного просмотра графических файлов (иконок). Файлы, зашифрованные на данном устройстве, можно использовать только на нем. При сбросе настроек до заводских, ключ для расшифровки будет удален. Пользователь не сможет пользоваться зашифрованным файлом на карте памяти SD, но незашифрованные файлы будут доступны и в дальнейшем. Функция требует установки длиной не менее 6 символов, имеет в себе не менее 1 цифра. При изменении пароля вслед идет автоматическое обновление шифра.

Второй уровень включает обязательную аутентификацию пользователя.

Как правило, у устройства имеется единственный идентификатор, поскольку предполагается только один владелец – следовательно, имя пользователя отсутствует, а есть только пароль, зачастую в виде простого PIN, что снижает защищенность. Поэтому нужны более надежные методы аутентификации, такие как аутентификация в домене, используемые вместо или в дополнение к встроенным возможностям устройства.

Многим мобильным устройствам, принадлежащим сотрудникам, которые они используют в своей производственной деятельности, не хватает, так называемых, «корней доверия», криптопроцессоров, которые давно уже встраиваются, например, в ноутбуки.

Организации должны придерживаться презумпции ненадежности мобильных устройств и предоставлять доступ с них к корпоративным данным и приложениями только после обеспечения безопасности, постоянно отслеживая состояние устройств в процессе их работы.

Есть несколько стратегий устранения рисков использования недоверенных мобильных устройств. Можно ограничить или запретить использование личных устройств и обеспечивать безопасность каждого корпоративного устройства, перед тем как выдавать его пользователю – это приводит устройство в наиболее безопасное состояние, и все отклонения от него могут

быть отслеживаемы и контролируемы. Как правило, у организаций, а тем более пользователей нет возможности контролировать безопасность сетей, используемых мобильными устройствами.

Мобильные устройства разрабатывались с целью упрощения поиска, получения, установки и использования приложений, что сразу создает очевидные риски безопасности, особенно на платформах, которые не ставят ограничений безопасности на публикацию сторонних приложений. Организации должны планировать защиту своих мобильных устройств исходя из предположения, что загружаемые пользователями сторонние приложения изначально опасны.

Есть несколько способов сократить риски, вызванные подобными приложениями, – например, запретить установку всех внешних приложений, составить списки разрешенных или запрещенных приложений, использовать безопасный контейнер изоляции корпоративных данных и приложений от всех прочих, имеющихся на устройстве. Еще одна общая рекомендация – оценивать риски, создаваемые тем или иным сторонним приложением, перед разрешением его использования на мобильных устройствах организации. Важно отметить, что даже если эти стратегии устранения рисков безопасности применяются, пользователи все равно через встроенный браузер будут иметь доступ к небезопасным веб-приложениям. Связанные с этим риски можно сократить, ограничивая или запрещая использование браузера.

Мобильные устройства могут взаимодействовать с другими системами для хранения и синхронизации данных. Локальное взаимодействие обычно включает в себя подключение мобильного устройства к настольному компьютеру или ноутбуку. Удаленное взаимодействие чаще всего включает автоматическое архивирование данных в облачном хранилище.

Если все компоненты находятся под контролем организации, то риски в целом приемлемы, но обычно как минимум один компонент оказывается внешним для организации: возможно подключение личного мобильного устройства к корпоративному ноутбуку; подключение корпоративного мобильного устройства к удаленному хранилищу; перенос вредоносного программного кода с одного устройства на другое. Стратегии сокращения рисков в этом случае зависят от типа соединения. Предотвращение синхронизации корпоративного устройства с личным компьютером требует наличия на мобильном аппарате средств выбора устройств, с которыми разрешено синхронизироваться. Если говорить о программном обеспечении, то существующие угрозы можно разделить на две группы:

Различное вредоносное ПО (вирусы, трояны) – обычно предназначено для хищения персональных данных, получения контроля над устройством или вывода его из строя;

Уязвимости (потенциальные ошибки) в прошивке или приложении, как правило, приводят к потенциальной практической возможности обхода аутентификации, искажения процессов обработки информации на устройстве.

Приведём несколько бытовых способов защитить свой телефон, планшет или иной гаджет:

Блокировка экрана и защита паролем.

Это самая важная защита, которую вы можете обеспечить своему устройству. Причем настроить ее можно за считанные минуты. Хотя такая зашита и не спасет от самых квалифицированных нарушителей (хакеров), но все же поможет избежать нежелательного просмотра информации в вашем телефоне. Рекомендуем также применить ее к программам, которые взимают плату за дополнительный контент, чтобы дети случайно не израсходовали ваш бюджет.

Существует несколько вариантов блокировки:

Прикосновение к экрану мобильного телефона (Слайдер)

Для разблокирования устройства, пользователь должен провести пальцем по экрану монитора, что и приводит к разблокированию прибора. Использование данного способа не обеспечивает сохранность вашей информации, потому что защита вообще отсутствует.

Распознавание лица (низкий уровень безопасности)

Данный способ обеспечивает низкий уровень безопасности, так как человек с похожим типом лица, может разблокировать данное устройство. Если же пользователь собирается использовать именно этот тип блокировки, то надо найти место с хорошим освещением и удерживать устройство на уровне глаз вдоль минуты. Тогда фронтальная камера зафиксирует контуре вашего лица (идентификационные данные), которые будут использованы для идентификации личности. Эти данные будут храниться в закрытом доступе.

Блокировка рисунком (средний уровень безопасности)

Блокировка рисунком считается системой среднего уровня защиты. Для его применения пользователь должен соединить в любом порядке не менее 4 точки, тем самым создавая свой уникальный ключ.

Введите PIN (средний или высокий уровень безопасности)

PIN - определенная последовательность цифр, минимальная длина которого 4 символа. Чем больше цифр, тем выше уровень защиты системы.

Введение пароля (высокий уровень безопасности)

Ввод пароля имеет наиболее высокий уровень безопасности. Поскольку в его состав входит не только цифры, но и буквы.

Программы защиты.

Для устройств Android можно загрузить специальные программы защиты:

Самая популярная программа защиты для устройств Android – это TrustGo Antivirus & Mobile Security: она включает средство сканирования вирусов, проверку программы и даже антиоранжевые инструменты, позволяющие в случае похищения заблокировать устройство и определить его местонахождение;

Подозрительные ссылки.

Согласно результатам исследования, пользователи мобильных устройств втрое чаще переходят по подозрительным ссылкам, чем пользователи компьютеров и ноутбуков. А причина довольно проста: небольшой размер экрана не позволяет должным образом распознать источник ссылки. Поэтому будьте бдительны, когда переходите на сайты, и проверяйте, надежен ли источник. А во время загрузки файлов необходима предельная осторожность. Проверенное правило такое: если не уверены в источнике, не переходите по ссылке.

Проверка программ.

Сначала трудно устоять перед искушением, чтобы не загрузить первые попавшиеся бесплатные программы. Однако всегда обращайте внимание, на какой сайт вы переходите. Загружайте файлы только из проверенных интернет-магазинов, таких как Google Play. Рекомендуем также сначала просмотреть отзывы других пользователей о необходимом продукте, чтобы убедится, что он не только широко используется, но и достаточно безопасен.

Важным аспектом безопасности является и тот факт, разрешает ли система устанавливать программы из неизвестных источников. Если да, веб-сайт может автоматически начать установку программы на ваш телефон. Если вы не уверенны в надежности источников, настройте телефон так, чтобы система запрещала установку таких программ.

Поэтому можете не волноваться, если вы пользуетесь одним из этих мобильных устройств.

Общие советы:

1. Просматривая сайты на ноутбуке, планшете или телефоне, помните о правилах политики безопасности, принятые в вашей организации, которые нужно соблюдать;

2. Будьте осторожны, открывая беспроводные точки доступа Wi-Fi;

3. Когда вы пользуетесь общим интернет-соединением (в том числе и через мобильное соединение через GSM или Wi-Fi), история вашего просмотра передается через сеть, к которой могут получить доступ находящиеся рядом люди.

Хотя это и нелегко, но все же возможно через это соединение получить доступ к вашему компьютеру. Поэтому не просматривайте важную информацию и не осуществляйте онлайн-платежи, если эта сеть ненадежная;

4. Желательно используйте устройство только по назначению;

5. Устройства иногда используются не только по назначению, но и в других целях, непредусмотренных их программированием.

6. В этом случае помните, что таким образом вы рискуете снизить степень защиты, что может повлечь за собой множество проблем и лишение гарантии;

7. Не включайте функцию сохранения и автозаполнения для пароля.

8. Защита паролем очень важна.

Настроить ее можно за считанные минуты. Однако она теряет всякую силу при автоматическом запоминании пароля на переносных устройствах. Не желая каждый раз вводить пароль вручную, вы применяете эту функцию для просмотра страниц, соцсетей, онлайн-платежей и оплаты, которая производится через программу. Однако делать этого не рекомендуется;

Выводы и направление дальнейших исследований. Итак, рассмотрев варианты защиты информации на смартфонах с платформой Android, можно подвести вывод. Данная операционная система как собственные, внутренние средства защиты, так же может и поддерживать дополнительное, разработанное другими разработчиками.

Встроенные внутренние средства защиты, достаточно удобными инструментами защиты данных на мобильных телефонах. Учитывая тип блокировки, выделяют различные виды безопасности. Они достаточно эффективны, но от внешних атак, то есть если кто-то хочет зайти на мобильный телефон и посмотреть какие-то определенные данные, то злоумышленник встречает препятствие в виде: пароля, рисунка, распознавание лица или PIN. Но от внутренних атак, вирусов, данные средства беспомощны. В то время как дополнительное программное обеспечение может обеспечить как безопасность от внутренних, так и от внешних атак.

Кроме того следует придерживаться определенных элементарных правил, а именно:

выключать Wi-Fi на телефоне, когда не пользуетесь Интернетом;

используйте сложные пароли;

загружайте приложения с умом.

Дополнительно, для большей надежности, уместно будет делать резервных копий и добавить удаленный доступ. Все эти советы позволят относительно безопасно пользоваться мобильными устройствами в быту.

Список литературы

1. **Якушин Петр**. Безопасность мобильного предприятия// Открытые системы № 01, 2013.

2. **Юдин А. К., Богуш В. М.** Информационная безопасность государства: Учебное пособие // Харьков: Консул. - 2005. - С. 38.

3. **Шетько Николай.** Взлом сотовых сетей GSM: расставляем точки над «i»// ET CETERA – серия цифровых журналов, распространяемых по подписке № 32, 2013.

4. **Белорусов Д.И.** Wi-Fi – сети и угрозы информационной безопасности/ Д.И. Белорусов, М.С. Корешков // СПЕЦИАЛЬНАЯ ТЕХНИКА № 6, 2009; с. 2-6.

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

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

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

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

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

Рукопис подано до редакції 14.04.17

УДК 532.58: 669.162.1

В.П. ТАРАСОВ, С.В. КРИВЕНКО, (ООО «Азовский технологический центр, Мариупольский государственный университет, г. Мариуполь)

ОБОСНОВАНИЕ ЗАКОНОМЕРНОСТИ КОЭФФИЦИЕНТА ГАЗОДИНАМИЧЕСКОГО СОПРОТИВЛЕНИЯ ПРИ ДВИЖЕНИИ ГАЗА В СЛОЕ ОКОМКОВАННОЙ АГЛОШИХТЫ

Газодинамические условия спекания агломерационных шихт оказывают существенное влияние на производительность процесса, качество агломерата и параметры работы газоотсосного оборудования, оптимизация которых возможна при обоснованном научном решении проблемы.

Наиболее часто исследователи при описании газодинамики зернистого слоя используют формулу Дарси-Вейсбаха, определяющую потери напора при развитом турбулентном течении несжимаемой жидкости [1,2]