In work the review of a condition of economic crimes is carried out. In the analysis of data it is revealed that the main serious threat of economic security among the banking sector of economy is fraud with financial statements.

УДК 004.056.53

ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ ДАННЫХ НА ANDROID

Замалетдинова Р.Э., студентка 4 курса
экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновская ГСХА

Ключевые слова: *информационная безопасность, Android OS, персональные данные, графический ключ, шифрование.*

В статье рассмотрены встроенные средства защиты персональных данных на устройствах Android.

На сегодняшний день практически все смартфоны стали носителями важных персональных либо корпоративных данных. Наибольшей популярностью пользуются устройства под управлением операционной системы Android OS. Доля Android на рынке ОС в 2015г. составляла 82,8%, что значительно превышает долю iOS и Windows Phone. В связи с этим угрозы безопасности данной платформы являются наиболее актуальными.

Какую же информацию следует защищать в телефоне? В таблице 1 представлен перечень информационных ресурсов, в наибольшей степени подверженных утечке.

Утечка данных может произойти в результате потери или кражи устройства, в результате фишинговой атаки или атаки шпионских программ. Кроме этого, если информация на старом мобильном устройстве не стерта должным образом, следующий владелец может легко заполучить доступ к огромному количеству чужих персональных данных.

Способы защиты персональных данных на устройствах Android подразделяются на встроенные программы защиты, а также средства, которые предоставляются сторонними разработчиками.

Таблица 1 – Информационные ресурсы, подверженные утечке

Тип данных	Подробное описание данных
Данные о контактах	Номер телефона, ФИО, электронная почта, группа контакта, дата рождения контакта, почтовый адрес, сведения о работе, псевдоним, веб-сайт
Данные о совершенных звонках	Журнал входящих, исходящих, пропущенных вызовов
SMS-данные	Журнал сообщений, содержимое входящих, исходящих SMS и MMS, а также черновики сообщений
Данные аккаунтов электронной почты	Контакты, электронные адреса, вложенные сообщения и файлы
Данные из браузеров	Временные файлы, список посещенных страниц, закладки браузеров
Медиафайлы	Файлы (фото, видео-, аудиофайлы, документы), хранящиеся в памяти телефона
Данные SIM-карты	Номер SIM-карты; юридическое лицо, обслуживающее мобильные станции; тарифный план и др.
Данные с карты памяти	Файлы (фото, видео-, аудиофайлы, документы), хранящиеся в карте памяти

К встроенным средствам защиты относятся:

1. Экран блокировки с графическим ключом.

Графический ключ – это соединение точек в заданном порядке на дисплее, является особым методом блокировки мобильных устройств с сенсорным экраном. Во время активации защиты порядок последовательного соединения устанавливается пользователем.

Уровень безопасности в данном случае можно повысить путем увеличения поля ввода графического ключа, путем скрытия отображения точек графического ключа на экране смартфона, а также с помощью установления автоматической блокировки экрана после 1 минуты бездействия телефона.

2. Шифрование памяти телефона.

Данный способ предполагает шифрование внутренней памяти телефона, доступ к которой будет осуществляться только по паролю или PIN-коду. Шифрование позволяет сохранить данные пользователя, расположенные в памяти телефона, например, сведения о контактах, данные из браузеров, пароли, используемые в Интернете, фотографии и видео, полученные пользователем с помощью камеры и не переписанные на SD-карту.

Недостаток этого средства защиты заключается в том, что шифрование можно отключить только с помощью ресета и возврата заводских настроек телефона. При этом все пользовательские данные будут

стерты с устройства.

3. Шифрование внешней SD-карты памяти.

Функция входит в стандартный пакет Android 4.1.1 для планшетов, предназначена для надежной защиты информации на внешней SD-карте.

Карта памяти может содержать личные фотографии пользователя, текстовые файлы с данными коммерческого и личного характера. Шифрование внешней SD-карты памяти позволяет зашифровывать файлы без изменения их названия, структуры файла, с сохранением предварительного просмотра графических файлов (иконки).

Функция предполагает установку блокировочного пароля на дисплей длиной не менее 6 знаков. Существует возможность отмены шифрования. При изменении пароля происходит автоматическая перешифровка.

В случае потери пользователем карты памяти, зашифрованные файлы не могут быть прочтены через card-reader. Кроме этого, если карту памяти поставить на другое устройство с другим паролем, зашифрованные данные также не будут прочтены.

Таким образом, встроенные средства защиты данных на Android являются весьма надежными и удобными инструментами. Они позволяют обеспечить защиту данных о контактах пользователя, SMS-данных и данных о совершенных звонках, данных аккаунтов электронной почты, а также файлы и папки, находящиеся как в памяти телефона, так и на съемной SD-карте.

Библиографический список:

1. Альбекова, З.М. Уязвимость мобильной платформы Android / З.М. Альбекова, Р.Б. Дамиров // Вестник научных конференций. – 2015. – № 4-2 (4). – С. 14 – 15.

2. Гатиятуллин, Т.Р. Угрозы безопасности Android OS / Т.Р. Гатиятуллин, Д.Д. Николаев // Научный журнал. – 2016. – № 1 (2). – С. 18 – 19.

3. Гришко, И.С. Безопасность мобильных устройств на платформе Android / И.С. Гришко // Вестник магистратуры. – 2016. – № 2-1 (53). – С. 35 – 36.

BUILT-IN DATA PROTECTION TO ANDROID

Zamaletdinova R.E., Golubev S.V.

Key words: *information security, Android OS, personal data, graphical key encryption.*

The article describes the built-in protection of personal data on Android devices.