Быть или не быть?

Безмалый В.Ф.

MVP Consumer Security

Microsoft Security Trusted Advisor

Быть или не быть шифрованию на вашем мобильном устройстве? Если шифровать, то почему? Если шифровать – то чем? На эти вопросы я постараюсь ответить в данной статье.

О необходимости шифрования мобильных устройств в корпоративной среде написано много. Я не хотел бы повторяться. В данной статье мы постараемся с вами задуматься над вопросом, а нужно ли шифровать мобильные устройства обычному пользователю? И вообще, как быть? Если шифровать, то чем? Где хранить ключи? Как восстановиться в случае аварии?

В дальнейшем, говоря о мобильных устройствах, я буду иметь ввиду как ноутбуки и смартфоны, так и обычные внешние USB-носители (флешки и жесткие диски). Там где речь будет идти о конкретном подклассе, об этом будет заявлено дополнительно.

Итак, давайте задумаемся, а что же хранят ваши устройства? Странный вопрос, не правда ли? На самом деле ваши устройства хранят все что угодно. В частности это могут быть пароли к социальным сетям, форумам, которыми вы пользуетесь, к вашей почте, а то и данные вашей кредитной карты, да и просто ваши письма. Неужели вы думаете, что это никому не интересно? А зря…

Что касается вашего смартфона, то здесь картина еще «веселее». На самом деле вы даже не представляете, сколько интересного знает о вас ваш телефон. В своей статье «Раскрываем телефонные тайны» (Windows IT Pro/RE № 5 2011) я писал о том, сколько информации хранится в вашем телефоне. В частности, что же может извлечь специалист из вашего телефона.

Для этого воспользуемся программным обеспечением «Мобильный криминалист» (http://www.oxygen-forensic.com/ru/). Несмотря на то, что данное программное обеспечение позиционируется как продукт для проведения криминалистической экспертизы, никто не в силах помешать злоумышленнику использовать его для получения весьма интересных данных с вашего телефона. Что мы с вами можем извлечь из вашего телефона с помощью данного программного обеспечения? Посмотрим на таблицу.

Таблица 1

1	Основные данные памяти телефона и данные SIM-карты
2	Список контактов (включая номера мобильных и стационарных телефонов, факсов, почтовые адреса, фотографии контактов и прочую информацию о контактах
3	Пропущенные/входящие/исходящие звонки
4	Данные SIM-карты
5	Информация о группах абонентов
6	Органайзер (встречи, заметки, напоминания о звонках, годовщины, дни рождения, списки дел)
7	Текстовые заметки
8	Сообщения SMS (сообщения, журнал сообщений, папки, удаленные сообщения (с

	некоторыми ограничениями))
9	Временные файлы и закладки интернет-браузеров)
10	Сообщения MMS с вложениями
11	Сообщения электронной почты с вложениями
12	Журнал трафика и сессий GPRS, EFGE и Wi-Fi
13	Фотографии и картинная галерея
14	Видеоклипы, фильмы
15	Голосовые записи и аудиоклипы
16	Все файлы из памяти телефона, а также карты памяти включая установленные приложения и их данные
17	Базы данных радиостанций FM (как часть данных файлового браузера)
18	Данные журнала Lifeblog, содержащего список действий с телефоном с указанием географических координат (если смартфон поддерживает эту функцию)

Как видите, список того, чем может воспользоваться злоумышленник в случае, если он завладеет вашим смартфоном, достаточно велик.

Между тем, список украденных (утерянных) устройств непрерывно растет. Более того, впечатление такое, что пользователи просто не желают задумываться. Совсем!

Обратимся к цифрам

Июнь 20, 2011

Аналитический центр InfoWatch зарегистрировал крупную утечку персональных данных граждан Великобритании. По сообщению газеты «The Sun», из здания Государственной службы здравоохранения пропал портативный компьютер, в котором хранились медицинские документы более восьми миллионов пациентов.

Всего из хранилища London Health Programmes – медицинской исследовательской организации на базе Государственной службы здравоохранения Северной и Центральной части Лондона – пропало 20 компьютеров.

Данные не были зашифрованы.

Июнь 09, 2011

Аналитический центр InfoWatch сообщает, что в Торонто были потеряны 3 незашифрованных CD-ROM с персональными данными клиентов банка Scotiabank.

Вы можете возразить, мол, это же корпоративные данные.

Приведу пример из собственной практики.

Год назад мне довелось возвращаться из Сиэттла в Киев с пересадкой в Амстердаме. В Амстердаме в самолет садилась большая компания моряков, многие из которых были «навеселе». Трижды (!) в самолет заходили представители службы безопасности аэропорта, чтобы узнать, кто забыл на стойке безопасности ноутбук(!). Никто не отозвался. Нет, я, конечно, понимаю, что это вопиющий случай, и вы никогда не будете в настолько беспомощном состоянии, чтобы забыть ваш ноутбук. Надеюсь это так. А все же? А вдруг? А?

Другая вопиющая тема – хищение смартфонов. Практически каждый из нас сталкивался с тем, что у него (его друзей, знакомых) воровали телефоны. Вы стали после этого внимательнее? Шифруете ваши данные? Уверен, что нет. Увы…

Но хорошо. Вы все же решились использовать шифрование. Далее перед вами встает старый вопрос. Чем шифровать?

Если вы используете ноутбук под управлением Windows 7 Ultimate (Максимальная), то логическим продолжением является использование технологии BitLocker. Однако так ли все хорошо и гладко? С одной стороны – да. Ведь данная технология шифрования встроена в операционную систему. С другой – все не так очевидно. Давайте подумаем почему. На самом деле в спецификации ноутбука возможны два варианта:

1. Ваш ноутбук (нетбук, а сегодня уже и планшет) оборудован TPM (**Trusted Platform Module**— название спецификации, описывающей криптопроцессор, в котором хранятся криптографические ключи для защиты информации, а также обобщенное наименование реализаций указанной спецификации, например в виде «чипа TPM» или «устройства безопасности TPM» (Dell). Спецификация TPM разработана Trusted Computing Group. Текущая версия спецификации TPM — 1.2 ревизия 103, издание 9 июля 2007).
2. Ваш ноутбук не содержит TPM.

Рассмотрим эти ситуации подробнее.

Если ваш ноутбук содержит TPM и вы работаете под управлением Windows 7 Ultimate, то выбор BitLocker будет самым простым и в то же время, вероятно, самым безопасным решением. Естественно, вы будете использовать TPM с PIN-кодом, т.е. своего рода двухфакторную аутентификацию.

Если же ваш ноутбук не содержит TPM, а не забудем о том, что ввоз в Российскую Федерацию ноутбуков с TPM официально запрещен, то выбор BitLocker будет не так очевиден. Почему? Да потому что в этом случае вы, скорее всего, будете хранить ключ доступа к вашему ПК на USB-флеш и, увы, чаще всего, эта флешка будет храниться в той же сумке (том же рюкзаке) что и ваш ноутбук. Т.е. в случае его кражи (утери) вы сами отдаете ключи шифрования. Толку от этого, увы, никакого!

Что делать в этом случае? На самом деле в этом случае есть 2 рекомендации:

1. Ноутбук в сумку – флешку на шею (в карман). Но не вместе!
2. Воспользуйтесь ПО третьего производителя

Та же рекомендация (о ПО третьего производителя) может быть дана, если вы до сих пор используете Windows XP или Windows 7 более младших версий.

Какое это будет ПО? На самом деле такого ПО много, попробуем перечислить некоторые образцы:

1. Kaspersky KryptoStorage
2. TrueCrypt
3. Secret Disk 4

Этот список на самом деле можно продолжать и продолжать. Что из этого вы выберете, я, естественно, не знаю.

Выбор ПО для шифрования смартфонов также необычайно велик. Надеюсь в это многообразии вы тоже сможете выбрать себе что-то полезное.

«Подводные камни» шифрования

На самом деле хотелось бы, чтобы вы помнили, что устойчивость вашего шифрования определяет стойкость вашего пароля. Я надеюсь, что ваш пароль шифрования немного сложнее чем «1111».

Вместе с тем стойкий пароль шифрования порождает следующую проблему. Как его не забыть? Здесь можно дать массу советов, но прежде всего совет один. Сразу задумайтесь о том, где вы будете хранить ключ восстановления! От этого будет зависеть, сможете ли вы расшифровать ваш носитель в чрезвычайной ситуации!

Заключение

Что хотелось бы вам сказать в заключение? Помните, что безопасность ваших данных это прежде всего ваша задача и ваша проблема. Я очень хочу, чтобы вы хоть немного задумались после прочтения данной статьи!