УДК 004.056.53

# ЗАЩИТА ИНФОРМАЦИИ

Л. М. Савченко
Научный руководитель – Т. Г. Долгова

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: qcva@yandex.ru

*Научная мысль развивается быстрыми темпами и предоставляет как обычному пользователю, так и программисту широкий набор возможностей защитить персональную информацию от несанкционированного доступа. Существуют как аппаратные, так и программные средства защиты, каждое из которых имеет свои преимущества.*

*Ключевые слова: информационная безопасность, ПСКЗИ ШИПКА, USB-токен, антивирусные программы, HASP.*

# INFORMATION SECURITY

L. M. Savchenko
Scientific supervisor – T. G. Dolgova

Reshetnev Siberian State Aerospace University
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
E-mail: qcva@yandex.ru

*Scientific thought is growing in quick tempo and provides as a standard user and the programmer a broad range of options to protect information from unauthorized access. There are hardware and software means of protection, all of them has its advantages.*

*Keywords: Information security, PSKZI SHIPKA,USB-токен, антивирусные программы, HASP.*

В настоящее время почти все данные переходят в электронный вид. Вместе с переходом информации в цифровую среду совершенствуются и методы несанкционированного доступа к ней. Поэтому сейчас стремительно развивающейся отраслью становится разработка и производство средств обеспечения безопасности данных. Но так как способов нелегального проникновения существует великое множество, то и способы защиты не должны ограничиваться только аппаратными или программными.

Чтобы избежать утечки информации в организации, необходимо обеспечить персональный доступ каждого сотрудника исключительно к тем данным и техническим средствам, с которыми он непосредственно работает. Одним из решений такого ограничения являются USB-устройства. В свою очередь они делятся на электронные ключи HASP, средства криптографической защиты и USB-токены [1].

HASP: Это аппаратно-программная система защиты информации от нелегального доступа и распространения. Была разработана компанией Aladdin Knowledge System Ltd. Систему защиты составляют: электронный ключ HASP (представляет собой USB-накопитель), специальное ПО для защиты данных, также схемы и методы защиты [2]. Принцип работы системы это закрепление за определенным человеком USB-ключа, который будет необходим для доступа к данным и подтверждения легальности копии.

Средства криптографической защиты: ПСКЗИ ШИПКА – персональное средство криптографической защиты информации (шифрование, идентификация, подпись, коды аутентификации). Это специализированное USB-устройство на основе микропроцессора. Использование микропроцессора, а не микросхемы, позволяет создавать продукты с различным набором функционала, что отражается на широком выборе для пользователя, которому даются возможности выбора действительно необходимого продукта и не переплачивать за ненужный функционал. ПСКЗИ ШИПКА дает возможности:

шифровать подписи файлов электронной цифровой подписью, автоматически заполнять WEB-формы и хранить для них пароли, предоставляет услуги идентификации и аутентификации пользователя на ПК при загрузке ОС.

USB-токены: Это аналог смарт-карты (карта со встроенной микросхемой – микропроцессором и ОС), представляет собой USB-ключ или USB-брелок (отличается от USB-ключа лишь тем, что имеет вид брелка, который можно закрепить, например, на ключ). Позиционируется устройство как средство строгой аутентификации – двухфакторной или трехфакторной. Двухфакторная аутентификация подразумевает под собой использование пароля, ПИН-кода и физического ключа, магнитной карты или электронного ключа. В трехфакторной аутентификации используются предыдущие два признака и также биометрических характеристики – голос, рисунок сетчатки глаза или отпечаток пальца [4].

Далее перейдем к прикладному программному обеспечению. Учитывая, что кража информации может производиться не только из памяти компьютера, но также, сейчас это особенно становится актуально, и из памяти смартфона или планшета. Вдобавок ко всему многие крупные компании собирают данные о пользователях, собирают информации о программном обеспечении, которое установлено на их компьютерах, причем такие действия со стороны фирм не афишируются. Поэтому чтобы обезопасить накопители информации, как от шпионажа, так и от взлома, было придумано множество программ и утилит, которые могут защищать компьютер в целом, как например антивирусные программы, но и, например, исключительно работать с трафиком и другое.

Распространённой защитой являются антивирусные программы. Сейчас без них не обходится ни один компьютер. Яркие представители этого сегмента рынка программного обеспечения это ESET NOD 32, Антивирус Касперского, Dr. Web и другие. В основном эти продукты ориентированы на защиту компьютеров, хотя вслед за современными тенденциями производители адаптируют антивирусные программы и для смартфонов.

Последние модели смартфонов созданы на базе операционных систем iOS, Android, Windows 8.1, Windows Mobile. Для этих операционных систем разработаны также и свои защитные средства от кражи и шпионских программ.

Одна из первых разработанных антивирусных программ для операционной системы Android это Lookout Mobile Security. Данный продукт после установки на смартфон моментально производит сканирование файловой системы устройства и других программ. Также пользователь сам может задать расписание сканирования своего устройства или же настроить функцию поиска, если смартфон потеряется. При включении этой функции пользователь самостоятельно при помощи компьютера с подключенным Интернетом может определить местоположение смартфона на карте, причем не обязательно, чтобы на устройстве был активирован GPS-модуль.

Из бесплатных приложений можно уделить внимание GuardX Antivirus – занимается исключительно защитой гаджета и отличается «спартанским» количеством настроек. NQ Mobile Security – достойное антивирусное приложение, кроме защиты от вирусов и шпионских программ также доступна опция «черного списка» контактов, которая будет блокировать входящие звонки и SMS от абонентов, занесённых в него. Trust Go Antivirus & Mobile Security – в широкий набор функций этого антивирусного приложения входит ещё и возможность создания резервных копий необходимой информации на удаленном сервере. AVG Antivirus – данная программа, после инсталляции, сама предлагает рекомендуемые параметры безопасности, но пользователь может в любое время внести свои корректировки [5].

На данный момент операционная система iOS считается самой надежной, чего нельзя сказать об Android, которая в свою очередь, – самой не защищенной. Windows Mobile, также не отстает от iOS, и имеет свою защиту уже внутри операционной системы. Но это справедливо только в том случае, если пользователь использует исключительно те продукты, которые предоставляет ему производитель. В противном случае, используя сторонние программные продукты, существует вероятность занести на устройство вирус или шпионскую программу. Для предостережения таких атак предлагается продукт ESET NOD32 Mobile Security. Он предоставляет возможности: блокировки нежелательных SMS и MMS сообщений, защиты от потери персональных данных, удаления данных при помощи SMS-команд [6]. Также существует программный продукт Dr. Web Mobile Security. Программа проверяет самостоятельно все файлы, передаваемые на устройство, дает возможность создать «черный список» контактов, чтобы блокировать входящие вызовы и SMS и многое другое [7].

Так как антивирусные программы для защиты компьютера или ноутбука – избитая тема, то стоит рассказать о программах для защиты отдельных компонентов – интернет-браузеров, электронной почты, социальных сетей, WI-FI.

Организация Network Advertising Initiative поддерживает работу online средство, которое позволяет обнаружить тех, кто собирает о пользователе какую-либо информацию. В качестве примера, тех, кто занимается слежкой, можно назвать такие фирмы как Criteo или AppNexus.

Если говорить об электронной почте, то такие протоколы как POP3, SMTP, IMAP – оставляют данные открытыми, что дает удобную лазейку для нарушителей закона и не только. Как известно, из сведений предоставленных Эдвардом Сноуденом всему миру, агенство национальной безопасности США при помощи программы Stellar Wind накапливала метаданные по электронной почте. В связи с этой сенсационной новостью Джон Каллас, сотрудник компании Silent Circle, которая занимается шифровкой связи через электронную почту, рассказал о намереньях создать новую службу, которая будет называться Darl Mail, для защиты как электронных писем, так и метаданных. Также к разработке присоединится служба защиты электронной почты Lavabir, свернувшая работу своего сервера по причине требований со стороны ФБР все ключи шифров, защищающих сайт.

К сожалению, довольно просто перехватить данные, транслируемы через сеть Wi-Fi. Злоумышленник, использую даже недорогое программное обеспечение, может записывать пакеты данных 802.11 (IEEE 802.11 – набор стандартов связи для работы в беспроводной локальной сетевой зоне), курсирующих между компьютерами и устройством Wi-Fi. Можно попробовать установить программное обеспечение Tor (система прокси-серверов, которая позволяет создать анонимное сетевое соединение), но, как известно, идеальной защиты не бывает [8].

В заключении можно сделать вывод о том, что как бы быстро не развивались технологии защиты персональной информации – никогда не будет рецепта идеальнее, чем затворничество в темной комнате и ограничение всех связей с внешним миром. Но, все-таки, обезопасить себя можно. И самым эффективным средством будет использование как технических, так и программных средств защиты.

**Библиографические ссылки**

1. Конявская С. // Журнал сетевых решений LAN. № 11 [Электронный ресурс]. URL: http://www.osp.ru/lan/2007/11/4592946/ (дата обращения: 07.04.2015).

2. HASP // Материал из Википедии – свободной энциклопедии – 20.10.2014. [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/HASP (дата обращения: 07.04.2015).

3. Сергеев Ю. // CNews [Электронный ресурс]. URL: http://www.cnews.ru/reviews/free/security2006/articles/usb/ (дата обращения: 07.04.2015).

4. Седов С. // Мой android: новости, советы, слухи. 9.02.2013. [Электронный ресурс]. URL: http://myandroid.ru/zashhita-android-ot-virusov-i-shpionskix-programm-10-antivirusnyx-prilozhenij (дата обращения: 07.04.2015).

5. ESET NOD 32 [Электронный ресурс]. URL: http://www.esetnod32.ru/home/products/mobile-security/windows-mobile/ (дата обращения: 07.04.2015).

6. Dr. WEB Антивирус [Электронный ресурс]. URL: http://products.drweb.com/mobile/?lng=ru (дата обращения: 07.04.2015).

7. Элб Д. Цифровая оборона // Популярная механика. 2014. № 3(137). С. 50–53.