Н.Г. Панько

БГЭУ, ФФБД, группа ДФФ-1, 1 курс

ЗАЩИТА ДАННЫХ НА USB ФЛЭШКЕ

В условиях формирования демократического правового государства и основ гражданского общества, рыночной экономики важное значение приобретает четкое и всестороннее регулирование информационных отношений.

Самый распространенный аксессуар у современного бизнес-пользователя — компактный модуль флэш-памяти. Полностью запретить использование флэшек нереально — USB-порты есть у подавляющего числа современных компьютеров. ИТ-подразделениям компаний разной величины остается только внедрять системы контроля и безопасности, учитывающие особенности этих персональных систем — такие, как высокие риск заражения вирусами и вероятность потери самих носителей.

При этом специального антивирусного ПО для данного вида устройств не существует, с этой задачей без проблем справляются стандартные антивирусные продукты, однако некоторые из них могут работать с внешними модулями памяти более эффективно, например запрещать с них автоматический запуск приложений, блокировать операции записи-чтения или ограничивать пользователей в эксплуатации только определенных типов присоединяемых устройств памяти.

Повсеместное использование флэш-накопителей, устройств iPod делает их хорошим инструментом для скрытого проникновения зловредного ПО в ИТ-системы - под угрозой оказываются все компьютеры предприятия, оснащенные USB-портом.

Самый простой вариант защиты переносимой на флэшке информации — пароль для идентификации пользователя. Существуют также программы двухуровневой аутентификации.

Защита флэш-памяти паролем или шифром — это только часть общей системы безопасности мобильных устройств у корпоративных пользовате-

лей. Существуют флэшки с системой уничтожения записанной на ней информации, которая активируется при попытке несанкционированного доступа.

Интересным решением в виде персонального компактного сейфа является Pin Pad USB Stick — это флэш-накопитель, оснащенный небольшой числовой клавиатурой для ввода пароля доступа к данным.

Некоторые устройства оснащаются кроме встроенного ПО миниатюрным сканером отпечатков пальцев.

К изделиям компании MXI Security, которая специализируется на решениях с мощной защитой данных, относятся флэш-накопители Stealth MXP, выполненные в металлическом корпусе, весьма мало подверженные механическим повреждениям. В случае пропажи такой флэшки владельцу не придётся особенно переживать, что его данные попадут в чужие руки: доступ к ним можно получить лишь пройдя проверку биометрическим сканером, который при транспортировке прячется внутрь корпуса Stealth MXP (кроме этого пользователь может добавить защиту данных с помощью пароля). На одном накопителе свои раздельные безопасные зоны могут создавать до пяти пользователей.

Еще одно решение предлагает компания NERO — продукт АБС EF, который представляет собой высокоскоростное USB запоминающее устройство для хранения любого типа информации с возможностью мгновенного физического уничтожения носителя, причем, как отмечают представители компании-производителя, данные, содержавшиеся на носителе, восстановлению не подлежат.

Литература

1. http://forum.ixbt.com/topic.cgi?id=27:7636
2. http://www.pcweek.ru/themes/detail.php?ID=115551
3. http://forum.ladoshki.com/viewtopic.php?t=32254