И.Г. Книтор

ПРИКЛАДНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

На современном этапе развития белорусского государства одним из важных аспектов деятельности правоохранительных органов является внедрение информационных технологий во всех структурных подразделениях.

Процессы информатизации общества потребовали от сотрудников правоохранительных органов овладения новейшими технологиями обработки и анализа информации, способов обеспечения надежности и безопасности информационных систем. Вместе с тем ни для кого не секрет, что большинство сотрудников ОВД в основном знакомо только с работой в текстовых и табличных процессорах.

Типичный состав программного обеспечения компьютерной системы, получившей наибольшее распространение в ОВД, – это ОС MS Windows, офисный пакет MS Office, антивирусное программное обеспечение и брандмауэр. Также могут использоваться клиенты корпоративной электронной почты и интернет-браузер для доступа к банкам данных по технологии клиент – сервер. Перечисленное программное обеспечение при грамотном использовании способно оказать сотруднику ОВД существенную помощь в организации и практическом осуществлении правоохранительной деятельности.

Как правило, информационное и техническое обеспечение подразделений ОВД централизованно осуществляется специальными службами, которые обеспечивают поддержание на должном уровне надежности и безопасности информационных систем, сетевой инфраструктуры и персональных компьютеров сотрудников. Однако на практике, бывают ситуации, когда по каким-либо причинам нормальная работа персонального компьютера нарушается. И по известному закону Мэрфи происходит это в самый неподходящий момент.

В случае аппаратного сбоя необходим ремонт. Но если проблема в программном обеспечении, то возможность восстановления работоспособности системы существует при надлежащем отношении к организации сохранности персональных данных на резервных носителях и небольшой модификации способа загрузки операционной системы. Резервирование и дублирование программных и аппаратных ресурсов любой компьютерной системы – залог ее надежного функционирования. Что касается аппаратного резервирования – его мы рассматривать не будем, так как оно требует дополнительного финансирования. А вот

с программным обеспечением не все так плохо, как может показаться на первый взгляд.

Простое решение – иметь на одном компьютере две независимые копии рабочей системы с возможностью выбора очередности загрузки. В случае сбоя одной системы – выбираем для загрузки другую и продолжаем работу дальше. Но в этом, казалось бы, очевидном решении есть нюансы.

1. Стоимость лицензионного программного обеспечения компании Microsoft в комплектации усредненного компьютерного рабочего места сотрудника ОВД составляет 1500 долларов США: Windows Vista Business – 299 долларов США, Microsoft Office Standard 2007 – 399 долларов США, прибавим стоимость антивируса и брандмауэра, умножим на два.

2. В случае возникновения программного сбоя системы по причине инфицирования вирусом или другим вредоносным программным обеспечением время работы в исправной копии операционной системы при совместном использовании пользовательских данных будет ограничено повторным заражением и последующим сбоем работы копии.

3. Не всегда существует возможность копирования пользовательских данных на внешний носитель с зараженной системы. Если существует, то приведет к распространению вирусного или другого вредоносного кода и заражению следующей системы. Такое положение возможно при нерегулярности обновления антивирусных баз и отставании писателей антивирусов от ваятелей вирусного кода. Антивирус новые вирусы ловит не сразу, а работать нужно сейчас.

4. Дальнейшее самовосстановление работоспособности системы становится невозможным и требует специальных знаний и специального программного обеспечения, что в условиях ОВД не всегда осуществимо.

Выше приведенные аргументы доказывают неэффективность предложенного способа при использовании программного обеспечения Microsoft. Ситуация коренным образом меняется, если в качестве резервной операционной системы используется какой-либо клон ОС UNIX, например Линукс Ubuntu 9.10.

Особенность данного решения в том, что Линукс имеет другой формат исполняемых файлов. Это не позволяет вирусам мешать нормальной работе системы. Линукс имеет другую организацию файловой системы и развитые собственные средства работы с документами, интернетом, почтой, т. е. имеет полный функциональный набор приложений для использования в качестве автоматизированного рабочего места сотрудника правоохранительных органов. И это по цене одного DVD-диска.

Графический интерфейс Линукса также интуитивно понятен пользователю как и интерфейс Windows. Операционная система Линукс позволяет монтировать различные типы файловых систем, в том числе и NTFS, FAT32. Это свойство Линукс позволяет получать доступ к файлам пользователя в случае заражения вирусами или после сбоя файловой системы Windows с выдачей «синего экрана смерти».

Важные вопросы обеспечения информационной безопасности реализованы в Линуксе на самом высоком уровне. Данное свободное программное обеспечение поставляется с исходными кодами, что при необходимости позволяет специалисту убедиться в отсутствии закладок, черных ходов, «пасхальных яиц», чем любят баловаться программисты от Microsoft. Бесплатная замена MS Office – это офисный пакет OpenOffice от фирмы SUN – старейшего производителя ПО и аппаратного обеспечения для профессионалов.

В чем же состоит предлагаемый способ повышения надежности и безопасности компьютерной системы сотрудника ОВД?

Сокращенный алгоритм действий следующий:

1. Купить DVD-диск Ubuntu 9.10 или бесплатно скопировать из интернета по ссылке www.ubuntu.com/download.

2. Сохранить пользовательские данные на флэш или DVD и проверить наличие свободного места на жестком диске 10–15 гигабайт.

3. Загрузить компьютер с DVD-диска Ubuntu 9.10

4. Создать раздел под Ubuntu размером 10–15 гигабайт.

5. Инсталлировать Ubuntu 9.10 в версии «Рабочий стол».

6. Выбрать установку загрузчика Grub2 и добавить опцию загрузки Windows (можно установить пароль и время для его ввода).

7. Создать образ системного раздела Windows в файловую систему Ubuntu: dd if=/dev/sda1 of=/home/windows/winXP_dump.

8. Настроить сетевое подключение, если в сети не используется протокол DHCP.

9. Для непосредственного запуска программ Windows из среды Ubuntu установить приложение Wine.

10. Проверить последовательно загрузку систем после включения компьютера.

11. Продолжить работу в среде Windows.

Самое интересное начинается при вирусном заражении компьютера или возникновении программных сбоев ОС Windows и приложений MS Office. В этом случае следует выбрать при загрузке операционную систему Линукс. После загрузки получаем доступ к разделу Windows и пользовательским файлам. Пакет OpenOffice позволяет работать с пользовательскими документами Word, Excel, PowerPoint и сохранять

их в нужных форматах, выводить на печать, посылать по электронной почте. В это время можно сохранить пользовательские файлы на внешний диск (чтобы избежать утери) или в файловую систему Линукс.

Может быть после пробного использования Линукса в экстремальной ситуации сотрудник больше не захочет рисковать своими данными и терять время на восстановление работы Windows. Но это дело пользователя и его предпочтений, а также требований ведомственных инструкций и приказов.

Для восстановления Windows нужно из терминала Ubuntu выполнить команду:

if==/home/windows/winXP_dump of=/dev/sda1

Для Windows раздела размером 10 гигабайт время восстановления составит около 10 минут, при этом система восстановит свое состояние на момент создания образа. После перезагрузки система Windows работоспособна, без повреждений и вирусов. Затем следует обновить антивирусную программу и переписать пользовательские данные, предварительно проверив носитель антивирусом.

Для того чтобы подготовиться к возможной нештатной ситуации, следует знать, что в интернете (www.sun.com) существует бесплатная полнофункциональная версия пакета OpenOffice для Windows.

В заключение отметим, что использование Линукс в информационном обеспечении ОВД улучшит безопасность и надежность компьютерных систем, что незамедлительно отразится на оперативности и качестве правоохранительной деятельности.

В.В. Козловский

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Основу электронного документооборота составляет вопрос целостности и подлинности документа. В ряде случаев требуется конфиденциальность документа между получателем и отправителем.

Вопрос целостности и подлинности электронного документа решают средства электронно-цифровой подписи, а вопрос его конфиденциальности – средства шифрования.

Для рассмотрения угроз информационной безопасности при использовании электронного документооборота выделяют применяемые средства и выполняемые ими функционалы:

1) средства электронно-цифровой подписи:

процедура генерации открытого и закрытого ключей электронно-цифровой подписи;