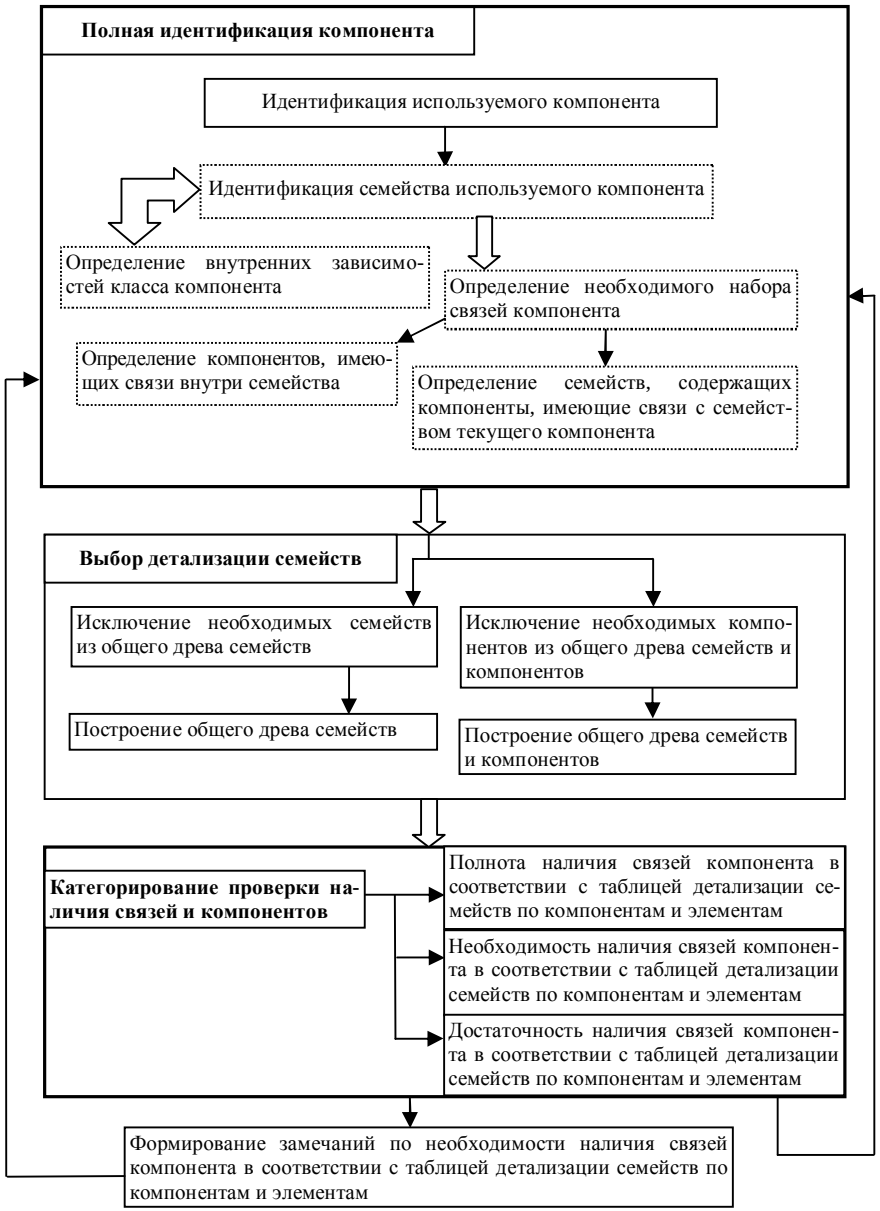

Обоснование должно обеспечивать детализацию до уровня выбранного на этапе выбора детализации семейств.

Формирование замечаний по необходимости наличия связей компонента в соответствии с таблицей детализации семейств по компонентам и элементам обеспечивает полноценное рассмотрение необходимых компонентов, что в свою очередь позволяет повысить уровень защищенности информации при разработке и использовании ПЗ или ЗБ.

Методика логического контроля формирует рекомендации, которые необходимы для выполнения. Они могут указывать как на недостаточность взаимосвязей компонента, обнаруженных на этапе идентификации, так и на избыточность.

Формирование замечаний по компоненту есть объединение замечаний по взаимосвязям компонента со сторонними семействами.

В случае абсолютного наличия всех необходимых компонентов и семейств – переход к полной идентификации следующего компонента.

Данную методику могут использовать разработчики профилей защиты, заданий по безопасности, систем ОБИ в КВСИИ, общей методики функционального анализа стандартов информационной безопасности, а также специалисты информационной безопасности в области ОБИ в КВСИИ.

А.М. Пановицын

О СОВРЕМЕННЫХ СРЕДСТВАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ ПРОГРАММ ЗАЩИТЫ ДАННЫХ

Сегодня далеко не во всех подразделениях органов внутренних дел сотрудниками уделяется должное внимание вопросам защиты информации. У большинства сотрудников, использующих в профессиональной деятельности персональные компьютеры, мероприятия по защите служебной информации сводятся исключительно к вводу пароля учетной записи операционной системы. В отдельных случаях сотрудники применяют программы маскировки данных, позволяющие скрывать диски, папки и файлы (Hide Folders, Folder Guard Pro, «Тайник» и т. п.), содержащие наиболее важную информацию.

Сегодня существует масса способов загрузки компьютеров с модулей памяти USB, CD/DVD в обход операционной системы, ее средств защиты и защиты любых программных продуктов, установленных в операционную систему. Как следствие, злоумышленник за считанные минуты получает доступ ко всей информации, хранящейся на жестком диске.

На жестком диске компьютера сохраняется вся информация о работе за ним. Получив доступ к компьютеру (или напрямую к жесткому диску), можно извлечь массу данных. Чтобы этого не произошло, необхо-

димо использовать набор специальных инструментов для защиты служебной информации и уничтожения следов работы за компьютером.

В сложившейся ситуации в качестве решения проблемы защиты информации вполне подойдет пакет утилит Steganos Security Suite, который включает в себя набор инструментов по защите компьютерных данных.

Служебные документы, как известно, принято хранить в сейфе. Для электронных документов разработчики Steganos Security Suite по аналогии создали виртуальный сейф, для которого на одном из жестких дисков выделяется область, используемая для создания виртуального диска. Количество виртуальных дисков может быть любым. После выделения места в системе появляется дополнительный диск, как если бы вы подключили модуль памяти USB или дополнительный винчестер. Каждый виртуальный диск может хранить до 256 Гбайт данных при использовании файловой системы NTFS и до 4 Гбайт при использовании файловой системы FAT32. Такой виртуальный диск целесообразно использовать для хранения служебных и секретных документов. При этом можно не беспокоиться, что кому-нибудь, кроме вас, удастся прочитать эту информацию. Все данные, записываемые на диск, кодируются «на лету» с использованием стойкого алгоритма шифрования, а после завершения работы виртуальный диск отключается от операционной системы.

В программе есть возможность использовать в качестве пароля последовательность изображений. Вы должны запомнить не только то, какие изображения в качестве пароля выбрали, но и их последовательность. Для хранения пароля можно использовать модуль памяти USB или флешкарту мобильного устройства. В этом случае не нужно запоминать пароль, главное – не потерять модуль памяти, который при подключении к компьютеру служит ключом для открытия виртуального сейфа.

В программный пакет входит утилита Portable Safe, которая обеспечивает сохранность данных при хранении информации на модулях памяти USB или CD/DVD. Для прочтения данных с таких носителей не требуется обязательная установка программы Steganos Security Suite, достаточно лишь подключить съемный носитель к компьютеру или вставить диск в привод.

Сотрудникам, по служебной необходимости использующим интернет, окажется полезным приложение Private Favorites, позволяющее хранить ссылки в специальной зашифрованной папке, просмотреть которые можно только после ввода пароля.

Утилита Password Manager предназначена для хранения личных паролей от сайтов и ящиков электронной почты. Для работы с программой достаточно запомнить один пароль. Если программа постоянно открыта, ввод пароля необходимо подтверждать через определенные промежутки времени. Таким образом программа защищает данные от возможной кражи третьими лицами, получившими доступ к компьютеру.

Пакет E-Mail Encryption дает возможность зашифровать текст электронного письма, чтобы в случае перехвата его содержимое осталось тайной. Текст письма можно вводить непосредственно в окне программы или же использовать для шифрования кнопку Encrypt, которая добавляется на панель инструментов в поддерживаемых почтовых приложениях (например, Outlook Express). Если ваша почтовая программа не поддерживается E-Mail Encryption, достаточно ввести текст письма в окне приложения для шифрования и сохранить текст в виде файла, который затем можно отправить по электронной почте. Шифровать можно текст, файлы и папки целиком. Для расшифровки сообщения получатель должен знать только пароль, наличие на его компьютере программы E-Mail Encryption не обязательно.

Steganos File Manager – это утилита, предназначенная для шифрования содержимого файлов и папок, а также для их скрытия от посторонних глаз. Используя ее, можно не просто зашифровать файлы, но и спрятать их в любом графическом или аудиофайле. При этом в файловом менеджере будет отображаться только файл-прикрытие, а настоящее содержимое графического или аудиофайла можно увидеть, только открыв его в программе File Manager и введя пароль.

Любой компьютер, а особенно ноутбук, имеет шансы быть украденным или утерянным. В Steganos Security Suite есть специальная утилита AntiTheft, которая может помочь отыскать пропажу. После активации программа назначает компьютеру уникальный идентификатор (AntiTheft ID) и через определенные промежутки времени отсылает данные о его IP-адресе на сервер разработчика. Эти данные сохраняются и в случае необходимости могут быть получены. Если, например, с украденного ноутбука выйдут в интернет, то подразделения, занимающиеся поиском устройства, могут легко отследить информацию об IP-адресе и принять соответствующие меры.

Приложение Internet Trace Destructor позволяет удалить временные файлы, список файлов, которые недавно открывались, и список программ, которые недавно запускались, файлы cookies и History браузера Internet Explorer и др. Программа работает с менеджерами загрузки (GetRight, Download Accelerator), интернет-пейджерами (ICQ, Trillian, Miranda), пиринговыми клиентами (eMule, Bittorent и пр.), проигрывателями мультимедиа файлов (Windows Media Player, Quicktime,

WinAmp, Realplayer), популярными графическими редакторами и по первому требованию удаляет все данные, которые могут вас скомпрометировать.

Для полного удаления данных с жесткого диска можно использовать приложение Shredder. Как известно, при стандартном удалении файлов и папок с винчестера данные на нем все равно остаются. Их можно с легкостью восстановить, используя специальное программное обеспечение (EasyRecovery Pro, Recover4all Professional, R-Studio Serials, RAR Recovery, O&O DiskRecovery и т. д.). После использования программы Shredder ни одна программа для восстановления не сможет показать наличие удаленных файлов и их содержимое. Для удаления данных программа может использовать одну из трех технологий, каждая из которых достаточно надежна. Например, один из предложенных методов удаления используется в Министерстве обороны США и предусматривает многократное беспорядочное перезаписывание данных внутри файла.

Сегодня не существует средств абсолютной защиты компьютерных данных, поэтому максимум, что можно сделать для безопасной работы на компьютере, это установить специальное программное обеспечение, которое если не предотвратит, то сведет к минимуму риск утраты служебной информации. В этом смысле Steganos Security Suite является достойным решением, программа уже в течение многих лет надежно оберегает секреты тысяч пользователей по всему миру. На рынке программного обеспечения существует достаточное количество программ по защите информации, успешно справляющихся со своей задачей. Очевидным преимуществом пакета Steganos Security Suite на ряду с надежным алгоритмом кодирования (AES/256 бит) является комплексный подход к решению задач по защите компьютерной информации. Очевидное удобство заключается в том, что многие приложения, входящие в состав Steganos Security Suite, можно приобрести отдельно, а полнофункциональную ознакомительную версию скачать с официального сайта производителя.

А.А. Ребковец, Д.Н. Михайловский, И.Н. Цырельчук

МЕЖСЕТЕВЫЕ ЭКРАНЫ

С развитием рыночных отношений информация все более приобретает качества товара, т. е. ее можно купить, продать, передать и, к сожалению, украсть. Поэтому проблема обеспечения безопасности информации с каждым годом становится все более актуальной. Одним из

возможных направлений решения данной проблемы является использование межсетевых (сетевых) экранов – комплексов аппаратных или программных средств, осуществляющих контроль и фильтрацию проходящих через них сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами.

Тем не менее поддерживаемый уровень сетевой модели OSI является основной характеристикой при классификации межсетевых экранов. Различают следующие типы межсетевых экранов:

управляемые коммутаторы (канальный уровень);

сетевые фильтры (сетевой уровень);

шлюзы сеансового уровня (circuit-level proxy);

посредники прикладного уровня (application-level proxy);

инспекторы состояния (stateful inspection), представляющие собой межсетевые экраны сеансового уровня с расширенными возможностями.

Коммутаторы среднего и старшего уровня Cisco, Bay Networks (Nortel), 3Com и других производителей позволяют привязывать MAC-адреса сетевых карт компьютеров к определенным портам коммутатора. Более того, немало коммутаторов предоставляет возможность фильтрации информации на основе адреса сетевой платы отправителя или получателя, создавая при этом виртуальные сети (VLAN). Другие коммутаторы позволяют организовать VLAN на уровне портов самого коммутатора. Таким образом, коммутатор может выступать в качестве межсетевого экрана канального уровня.

Следует заметить, что большинство специалистов по безопасности информационных систем редко относят коммутаторы к межсетевым экранам. Основная причина этого в том, что область фильтрующего действия коммутатора простирается до ближайшего маршрутизатора и поэтому не годится для регулирования доступа из интернета.

Кроме того, подделать адрес сетевой платы обычно не составляет труда (многие платы Ethernet позволяют программно менять или добавлять адреса канального уровня) и такой подход к защите является крайне ненадежным. Организация виртуальных сетей на уровне портов коммутатора более надежна, но, опять же, она ограничена рамками локальной сети.

Сетевые фильтры работают на сетевом уровне иерархии OSI. Сетевой фильтр представляет собой маршрутизатор, обрабатывающий пакеты на основании информации, содержащейся в заголовках пакетов. Сетевые фильтры существуют для сетей TCP/IP и IPX/SPX, но последние применяют в локальных сетях, поэтому они рассматриваться не будут.

При обработке пакетов ими учитывается следующая информация: IP-адрес отправителя и получателя, протокол (TCP, UDP, ICMP), номер программного порта отправителя, а также номер программного порта