Жакупов Жанат - магистрант
Казахский университет технологий и бизнеса,
г. Астана, Казахстан

К ВОПРОСУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Статья содержит обзор проблемы безопасности информации, обрабаты-ваемой средствами вычислительной техники и автоматизированными системами, способов и программ для несанкционированного доступа, вредоносных программ.

The article contains review of the problem of security of information elaborated by means of computer techniques and automated systems, ways and software for unauthorized access, maleficent programs.

Неправомерный доступ к информации – действия или процесс, в результате которых возможно неправомерное ознакомление с информацией, снятие копий с носителей информации или запись информации на носитель.

Несанкционированный доступ к информации (НСД) является наиболее широко распространенным способом неправомерного доступа к информации.

Наиболее часто термин «несанкционированный доступ» используется применительно к информации, обрабатываемой средствами вычислительной техники (СВТ) или автоматизированными системами (АС). При этом, под несанкционированным доступом к информации понимается доступ к информации, осуществляемый с нарушением установленных прав и (или) правил доступа к информации с применением штатных средств, предоставляемых СВТ или АС, или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам [4].

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Субъект доступа, осуществляющий несанкционированный доступ к информации называется нарушителем правил разграничения доступа.

Из определения «несанкционированного доступа» вытекает, что нарушитель осуществляет доступ к информации с использованием программного или микропрограммного обеспечения средств вычислительной техники или автоматизированных систем или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

Можно выделить два способа несанкционированного доступа: программно-технический (физический) и программный.

При программно-техническом (физическом) доступе нарушитель осуществляет несанкционированное вскрытие системного блока СВТ и изъятие HDD или изменение аппаратной части СВТ.

Изъятый HDD диск может быть подключен к специальной аппаратуре копирования (дублирования) диска или к другому компьютеру в виде локального диска с целью копирования как всего диска, так и интересующей нарушителя информации. Например, компактное устройство SuperSonix способно копировать информацию с жестких дисков с файловыми системами FAT 16/32, NTFS со скоростью до 8 ГБ в минуту.

Изменение аппаратной части СВТ производится с целью осуществления несанкционированного доступа к информации или копирования интересующей его информации на внешний носитель и может включать: отключение программно-аппаратных средств защиты информации или установку порта для внешнего устройства.

После изменения аппаратной части нарушитель осуществляет физический

взлом BIOS путем временного изъятия CMOS-батарейки из платы BIOS, а затем производит изменение приоритета последовательности загрузки дисков в подменю BIOS «Primary Master», осуществляет загрузку альтернативной ОС с внешнего носителя и копирование интересующей информации на flash-накопитель.

При реализации данного способа возможно также внедрение в СВТ электронного устройства перехвата информации (закладочного устройства) с целью перехвата защищаемой информации или получения необходимых данных для осуществления несанкционированного доступа (например, установка аппаратного кейлогера с целью получения логина и пароля пользователя).

Однако, на мой взгляд, закладочные устройства относятся именно к средствам перехвата информации, а не к средствам несанкционированного доступа, так как принципы их построения отличаются от принципов построения СВТ и они, как правило, не используют системные или сетевые ресурсы АС.

Выявить факт внедрения в СВТ закладочных устройств с использованием программных средств практически невозможно. Для этих целей используются специальные технические средства и методы.

При программном доступе нарушитель использует программное обеспечение, позволяющие реализовать несанкционированный доступ к информации без вскрытия системного блока или изменения аппаратной части СВТ.

Можно выделить следующие способы несанкционированного доступа с использованием программных средств [2, 3]:

– маскировка под зарегистрированного пользователя;

– непосредственное обращение к объектам доступа;

– использование программных средств, выполняющих обращение к объектам доступа в обход средств защиты;

– использование программных средств модификации средств защиты, позволяющих осуществить несанкционированный доступ;

– внедрение в АС вредоносных программ для осуществления несанкционированного доступа к информации или ее копирования.

При маскировке под зарегистрированного пользователя для входа в систему нарушитель использует логин и пароль зарегистрированного пользователя, который может быть перехвачен, например, с использованием программного кейлогера.

Непосредственное обращение к объектам доступа может осуществить нарушитель, имеющий санкционированный доступ к АС, но не имеющий доступа к защищаемой информации ограниченного доступа. При этом доступ к защищаемой информации осуществляется без «взлома» системы разграничения доступа с использованием специальных программ, например путем:

– восстановления удаленных файлов;

– восстановления временных файлов, хранящихся в папке «Temp»;

– просмотра файла подкачки Windows;

– сканирования диска с целью поиска на нем информации ограниченного доступа по словарю (списку) ключевых слов и т.д.

Несанкционированный доступ к защищаемой информации в обход средств защиты может осуществляться вследствие уязвимостей системы защиты или программного обеспечения АС. Основными причинами возникновения уязвимостей являются [1]:

– ошибки при проектировании и разработке программного обеспечения;

– преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного обеспечения;

– неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

– сбои в работе аппаратного и программного обеспечения, вызванные, например, сбоями в электропитании, и др.

Несанкционированный доступ к защищаемой информации может осуществляться путем внедрения в систему защиты АС программной закладки, под которой понимается преднамеренно скрытно внедренный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие, в том числе инициирование реализации недекларированных возможностей программного обеспечения [4]. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

Вредоносные программы могут быть внедрены не только в систему защиты АС, но и непосредственно в программное обеспечение АС, что также позволет осуществлять несанкционированный доступ к защищаемой информации.

Основными видами вредоносных программ, обеспечивающих несанкционированный доступ к защищаемой информации, являются:

– программные кейлоггеры (клавиатурные шпионы);

– программы подбора и вскрытия паролей (программы-взломщики паролей);

– программы для скрытого наблюдения за компьютером (типа Actual Spy);

– программы для скрытного удаленного управления и администрирования (троянские программы типа Back Orifice, Backdoor, штатные средства управления и администрирования компьютерных сетей типа Landesk Management Suite, Managewise и т.п.);

– программы для несанкционированного скрытого копирования файлов (типа USBDumper) и т.д.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_razd/_workinfo.htm.

2. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. - Москва: Стандартинформ, 2007. – 6 с.

3. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. [Электронный ресурс]. – Режим доступа: http://www.fstec.ru/_docs/doc_3_3_001.htm.

4. Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст . – Введ. 2006-06-01. – Москва: Стандартинформ, 2006. – 16 с.