УДК 004.056

А.А. Костырин[1]
А.А. Тихомирова[2]

РЕАЛИЗАЦИЯ УГРОЗ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ РАЗЛИЧНЫХ КАНАЛОВ УТЕЧКИ

Статья посвящена актуальному вопросу. Дается характеристика каналов утечки информации, их перечень и способы съема информации. Также ценным в этой статье является описание способов съема информации как через традиционные каналы утечки информации, так и по каналам утечки информации непосредственно из компьютерных систем.

Ключевые слова: *канал утечки, специальные технические средства, съем информации, закладные элементы, компьютерные вирусы, уязвимости системы.*

A.A. Kostyrin
A.A. Tikhomirova

THREATS TO INFORMATION BY USING A VARIETY OF LEAK CHANNELS

The article is devoted to the topical issues. It contains the characteristic of information leake channels, their list and information retrieval methods. Just valuable in this article is to describe the methods of information retrieval, both through the traditional information leak channels, and directly from the computer systems.

Keywords: *channel leakage, special equipment, information retrieval, fitting pieces, computer viruses, system vulnerabilities.*

Под каналами утечки информации понимают методы и пути утечки информации из информационной системы; паразитная (нежелательная) цепочка носителей информации, один или несколько из которых являются (могут быть) злоумышленниками или его специальной аппаратурой.

Объективное существование данных каналов утечки предполагает их возможное использование злоумышленниками для несанкционированного доступа к информации, ее модификации, блокированию и иных неправомерных манипуляций.

Каналы утечки информации целесообразно условно классифицировать на традиционные каналы утечки информации и каналы утечки информации непосредственно из компьютерных систем.

Наличие первых предопределяет широкое использование их с применением специальных технических средств, среди которых выделяют следующие основные группы:

– радиомикрофоны и микрофоны;
– оптические системы;
– устройства перехвата телефонных сообщений;
– видеосистемы записи и наблюдения;
– системы определения местоположения контролируемого объекта;
– устройства приема, записи, управления.

Контактное подключение к электронным устройствам является простейшим способом съема информации. Чаще всего оно реализуется непосредственным подключением к линии связи.

Бесконтактное подключение может осуществляться за счет электромагнитных наводок или с помощью сосредоточенной индуктивности.

Встроенные микрофоны, видео- и радиозакладки могут быть установлены в элементы интерьера, строительные конструкции, теле- и радиоприемники, розетки, телефонные аппараты, калькуляторы, замаскированы под канцелярские принадлежности, элементы одежды и т.д. Они обладают дальностью действия от 50 до 1000 м при сравнительно небольшой стоимости.

Рассмотрим общий принцип действия таких технических средств.

[1] Преподаватель, Военно-космическая академия им. А.Ф. Можайского.

[2] Кандидат экономических наук, заведующая кафедрой, Санкт-Петербургский государственный педиатрический медицинский университет.

Принцип действия съема акустической информации при помощи лазерных устройств с отражающих поверхностей основан на моделировании по амплитуде и фазе отраженного лазерного луча от окон, зеркал и т.д. Отраженный сигнал принимается специальным приемником. Дальность действия – до нескольких сотен метров. На эффективность применения подобных устройств сильное влияние оказывают погодные условия.

Оптический дистанционный съем видеоинформации может осуществляться через окна помещений с использованием длиннофокусного оптического оборудования в автоматическом или в ручном режиме работы.

Для съема аудиоинформации применяются высокочувствительные микрофоны с очень узкой диаграммой направленности. Узкая диаграмма направленности позволяет указанным устройствам избежать влияния посторонних шумов. Узконаправленные микрофоны могут быть использованы совместно с магнитофонами и диктофонами.

Утечка информации по цепям заземления, сетям громкоговорящей связи, охранно-пожарной сигнализации, линиям коммуникаций и сетям электропитания возможна за счет существования гальванической связи проводников электрического тока с землей.

При организации каналов утечки информации через сигнализации различного назначения злоумышленники используют «микрофонный эффект» датчиков. Подобные каналы утечки получили название параметрических каналов. Они формируются путем «высокочастотной накачки» (ВЧ-облучения, ВЧ-навязывания) электронных устройств с последующим переизлучением электромагнитного поля, промодулированного информационным сигналом. Промодулированные ВЧ-колебания могут быть перехвачены и демодулированы соответствующими техническими средствами.

Аналогичным образом могут быть созданы высокочастотные каналы утечки информации в бытовой и иной технике.

Утечка может произойти за счет плохой звукоизоляции стен и перекрытий. Съем информации может происходить с применением как простейших приспособлений (фонендоскоп), так и достаточно сложных технических устройств, например специализированных микрофонов.

Средой распространения акустических волн являются трубы газо- и водоснабжения, конструкции зданий. Акустическая информация может, например, восприниматься при помощи пьезоэлектрических датчиков, затем усиливаться и фиксироваться при помощи магнитофонов либо передаваться в эфир.

Возможны утечки информации через персонал. Сотрудники могут уничтожать или искажать информацию, писать компьютерные вирусы, похищать информацию.

Широкое внедрение компьютерной техники и телекоммуникаций в производственную, хозяйственную, финансовую деятельность предприятий, учреждений, организаций значительно повышает эффективность их работы.

Обратной стороной глобальной информатизации явилось появление компьютерной преступности.

Утечка информации из компьютерных систем зачастую происходит за счет:

– введения программно-аппаратных закладок;

– побочного электромагнитного излучения и наводок (ПЭМИН);

– съема информации с принтера и клавиатуры;

– модификации, уничтожения или блокирования информации с использованием компьютерных вирусов;

– утери носителей информации;

– инициализации злоумышленником каналов утечки, вызванных несовершенством программного либо аппаратного обеспечения, а также систем защиты.

В настоящее время в основе производства технических средств и программного обеспечения вычислительных систем лежат комплектующие изделия зарубежного производства. При этом появляется угроза внедрения программно-аппаратных закладок, что приводит к утечке информации, а также управляемого выведения из строя средств вычислительной техники. Подобные устройства могут быть установлены негласным образом и впоследствии при эксплуатации компьютерных систем. Применение закладных элементов представляется реальной и опасной угрозой при использовании вычислительной техники.

Аппаратные закладные элементы могут быть реализованы в аппаратуре персональных компьютеров и периферийных устройств. При этом возможны утечки информации, искажение вычислительного процесса, а также управляемый выход из строя вычислительной системы.

Программные закладные элементы могут быть представлены в виде модификации ком-

пьютерной программы, в результате которой данная программа способна выполняться несколькими способами в зависимости от определенных обстоятельств. При работе программные закладные элементы могут никак не проявляться, однако при определенных условиях программа работает по алгоритму, отличному от заданного (подобно компьютерным вирусам).

Существует классификация закладных элементов по следующим критериям:

– способу размещения;

– способу активизации;

– пути внедрения в систему;

– разрушающему действию.

При функционировании компьютерных систем возникают побочные электромагнитные излучения и наводки, несущие обрабатываемую информацию. ПЭМИН излучаются в пространство клавиатурой, принтером, монитором, кабелями. Утечка данных обусловлена излучением сигналов при перемене данных. Перехват ПЭМИН осуществляется радиоприемными устройствами, средствами анализа и регистрации информации. При благоприятных условиях с помощью направленной антенны можно осуществлять перехват на расстоянии до 1-1,5 км.

Утечки за счет съема информации с принтера и клавиатуры по акустическому каналу позволяют перехватывать и декодировать акустические колебания, распространяющиеся в воздушной среде.

Технически возможен перехват и декодирование кодов клавиш клавиатуры. Дальность действия подобных перехватов ограничена мощностью источника акустических и электромагнитных колебаний.

Утечка, модификация, уничтожение или блокирование информации возможны при использовании компьютерных вирусов, обладающих собственными отличительными признаками.

Последствия вирусной модификации могут быть различными – от незначительных помех до полного уничтожения данных и программ. Вирусы, использующиеся злоумышленниками для программного уничтожения, разрушают информацию в зависимости от определенных логических или временных условий.

Попадание вирусов в компьютерную систему возможно различными способами: от высокотехнологичного несанкционированного подключения до основанного на обмане, выполняемом оператором системы, при котором умышленно переписываются заранее зараженные файлы и сервисные программы для вывода компьютерной системы из строя. Вирус может попасть в систему и при неумышленных действиях операторов ЭВМ – при обмене флешками, CD-дисками, файлами.

Существует большое разнообразие вирусных программ. Некоторые из них занимаются сбором информации как с отдельных с компьютеров, так и из компьютерных сетей. Их объединяют под общим названием «троянский конь».

«Троянский конь» – это вирусы, скрытые в файлах данных (например, сжатых файлах или документах). Чтобы избежать обнаружения, некоторые разновидности «троянских коней» размещаются и в исполняемых файлах. Эти программы могут располагаться и в программных файлах, и в файлах библиотек, пришедших в сжатом виде. Чаще «троянские кони» содержат только подпрограммы вируса. «Троянский конь» скрывается под видом безобидного приложения, например архиватора, игры или программы обнаружения и уничтожения вирусов. После установки на компьютер вирус передает данные с зараженного компьютера злоумышленнику, который его создал.

Полиморфные вирусы – это вирусы, которые зашифровывают свое тело и благодаря этому могут избежать обнаружения путем проверки сигнатуры вируса. Прежде чем приступить к работе, такой вирус расшифровывает себя с помощью специальной процедуры расшифровки. Процедура расшифровки превращает зашифрованную информацию в обычную. Чтобы расшифровать тело вируса, процедура расшифровки захватывает управление машиной.

Еще одна возможность для злоумышленников использования каналов утечки – атаки на компьютерные системы, вызванные несовершенством программного либо аппаратного обеспечения. Под атакой подразумевается любая попытка преодоления систем защиты. Любые атаки нарушителей реализуются путём активизации той или иной уязвимости, которая присутствует в системе. Примерами уязвимостей могут служить некорректно составленная политика безопасности, отсутствие определённых средств защиты или ошибки в используемом программном обеспечении.

Рассмотрим наиболее распространенные атаки.

Анализ сетевого трафика – вид атаки, направленный в первую очередь на получение пароля и идентификатора пользователя путем «прослушивания сети». Реализуется такой вид атаки с помощью sniffer – специальной программы-

анализатора, перехватывающей все пакеты, идущие по сети. Если протокол, например FTP или TELNET, передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя.

Сканирование сети – данная атака заключается в сборе информации о топологии сети, об открытых портах, используемых протоколах и т.п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных.

Угроза выявления пароля – целью атаки является преодоление парольной защиты и получение доступа к чужой информации. Существуют различные методы кражи пароля: простой перебор всех возможных значений пароля, перебор с помощью специальных программ (атака словаря), перехват пароля с помощью программы-анализатора сетевого трафика.

Угроза подмены доверенного объекта сети и передачи по каналам связи сообщений от его имени с присвоением его прав доступа. Доверенный объект – это элемент сети, легально подключенный к серверу.

Такой вид угрозы эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.

Выделяют две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет злоумышленнику вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений.

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к информации, установленные его пользователем для доверенного абонента.

Навязывание ложного маршрута сети – данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP), таких, как слабая аутентификация маршрутизаторов. Суть атаки состоит в использовании злоумышленником уязвимости протоколов, внесении несанкционированных изменений в маршрутно-адресные таблицы.

Внедрение ложного объекта сети – атака, при которой изначально объекты сети не имеют информации друг о друге. В этом случае для построения адресных таблиц и последующего взаимодействия используется механизм запроса (как правило, широковещательного) и ответа с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети и выдать себя за легального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника.

Существует большое количество различных типов каналов утечек информации, потенциальное использование которых злоумышленниками может нанести непоправимый ущерб. Однако любая потенциальная атака может быть предотвращена при условии своевременного выявления и устранения имеющихся утечек. Такие мероприятия должны носить не единичный, а систематический комплексный характер. Только в этом случае возможно минимизировать вероятность успешной атаки на защищаемый объект или компьютерную систему.

Литература

1. Каторин Ю., Разумовский А., Спивак А. Защита информации техническими средствами. – СПб. : НИУ ИТМО, 2012.

2. Климентьев К. Компьютерные вирусы и антивирусы: взгляд программиста. – М. : ДМК Пресс, 2013.

3. Партыка Татьяна, Попов Игорь. Информационная безопасность. – 3-е издание. – М. : Форум, 2010.

4. Меньшаков Ю. Основы защиты от технических разведок. – М. : МГТУ им. Н.Э. Баумана, 2011.

5. Яковлев В.А. Шпионские и антишпионские штучки. – М. : Наука и техника, 2015.

6. Першина И.В. Программные методы сокрытия информации / И.В. Першина, А.А. Нечай // Экономика и социум. – 2015. – № 1–4 (14). – С. 196–199.

7. Нечай А.А. Методика комплексной защиты данных, передаваемых и хранимых на различных носителях информации / А.А. Нечай, П.Е. Котиков // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». – 2015. – Вып. 1. – С. 94–98.

8. Котиков П.Е. Репликация данных между серверами баз данных в среде геоинформационных систем / П.Е. Котиков, А.А. Нечай // Вестник Российского нового университета. Серия «Сложные системы: модели, анализ и управление». – 2015. – Вып. 1. – С. 90–94.