DOI: 10.17117/no.2014.01.022

Поступило в редакцию: 25.11.2014

<http://ucom.ru/doc/no.2014.01.022.pdf>

vka@mil.ru

Нечай А.А., Протоchanская Ю.Ю., Котиков П.Е. Анализ каналов утечки информации

Nechay A.A., Protochanska Yu.Yu., Kotikov P.E.
Analysis of the channels of leakage of information

Статья посвящена актуальной проблеме, совершенствованию средств защиты информации в экономических системах. Сегодня информация играет существенную роль в жизни любой компании. Сохранность информации приобретает определяющее значение. В статье рассмотрены каналы утечки информации, выполнен анализ их особенностей, возможностей закрытия каналов утечки. Показано, как одним из наиболее эффективных способов борьбы с сетевыми угрозами, в том числе с программными закладками, становится совершенствование методов и средств контроля доступа к сети

Ключевые слова: информация, утечка информации, каналы утечки информации, физические каналы утечки информации, технические каналы утечки информации, программный червь, программная закладка

The article is devoted to the urgent problem of improving the means of information protection in economic systems. Today, information plays a significant role in the life of any company. The security of information becomes crucial. In the article the channels of information leakage, the analysis of their features, capabilities closure leakage channels. Shows how one of the most effective ways of dealing with network threats, including software bookmarks, is the improvement of methods and tools to control access to the network

Key words: information, information leakage, leakage of information, physical-ski channels of information leakage, technical channels of information leakage, software worm, software tab

Нечай Александр Анатольевич

Преподаватель

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

Nechay Alexander Anatolievich

Teacher

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Протоchanская Юлия Юрьевна

Курсант

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

Protochanska Yulia Yurievna

Cadet

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Котиков Павел Евгеньевич

Кандидат технических наук, доцент

Военно-космическая академия им. А.Ф. Можайского
г. Санкт-Петербург, ул. Ждановская, 13

Kotikov Pavel Evgenievich

Candidate of Technical Sciences, associate Professor

Military space Academy Alexander Mozhaisky
St. Petersburg, Zhdanov st., 13

Все каналы утечки данных можно разделить на косвенные и прямые. Косвенные каналы не требуют непосредственного доступа к техническим средствам информационной системы. Прямые, соответственно требуют доступа к аппаратному обеспечению и данным информационной системы.

Примеры косвенных каналов утечки:

– Кража или утеря носителей информации, исследование не уничтоженного мусора;

– Дистанционное фотографирование, прослушивание;

– Перехват электромагнитных излучений.

Примеры прямых каналов утечки:

– Инсайдеры (человеческий фактор). Утечка информации вследствие несоблюдения коммерческой тайны;

– Прямое копирование.

Каналы утечки информации можно также разделить по физическим свойствам и принципам функционирования:

– акустические – запись звука, подслушивание и прослушивание;

– акустоэлектрические – получение информации через звуковые волны с дальнейшей передачей ее через сети электропитания;

– виброакустические – сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;

– оптические – визуальные методы, фотографирование, видео съемка, наблюдение;

– электромагнитные – копирование полей путем снятия индуктивных наводок;

– радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации “закладных устройств”, модулированные информативным сигналом;

– материальные – информация на бумаге или других физических носителях информации

1. Физические каналы утечки информации

Необходимость совершенствования средств физической защиты различных носителей информации является одной из главных задач любого объекта, будь то отдельно взятый индивид, или же некоторая организация. По статистике, главным источником утечки информации является человек. Для получения злоумышленником информации используются:

– сознательные действия сотрудников, обусловленные инициативным сотрудничеством с другой фирмой; продажей информации за взятку, под угрозой шантажа, в виде мести; переход на другую фирму на более высокую оплату (так называемая «кража мозгов»);

– обман (например, за счет создания ложной фирмы, в которую заманивают специалиста на собеседование, беседуют, выуживают сведения и затем отказывают в приеме);

– особенности характера сотрудника, например, его болтливость, желание показать себя более компетентным;

– слабое знание и невыполнение требований по защите информации и т.д.

Документы и публикации являются также одним из важных возможных каналов утечки информации. Документ имеет определенные этапы жизни: составление, оформление, размножение, пересылка, использование, хранение и уничтожение. На любом этапе возможна утечка информации.

Для уменьшения возможности утечки информации руководство организации предпринимает следующие действия:

- разработка перечня документов с грифом «Коммерческая тайна» (этот термин обозначает информацию, которая позволяет получать предприятию большую прибыль по сравнению с конкурентом);
- уточнение списка лиц, допускаемых к работе с документами;
- организация учета входящих, исходящих документов и правил работы с ними;
- определение правил хранения (инвентарный учет, номенклатура дел, наличие сейфов и т. д.) документов;
- определение правил уничтожения документов.

2. Технические каналы утечки информации

Для обеспечения технической деятельности компании или организации широко используются телефоны, радиотелефоны, компьютеры, принтеры, дисплеи, клавиатура, обычный речевой обмен информацией и т.д. Потеря информации возможна по акусто-преобразовательным, электромагнитным, визуальным и другим каналам.

Для нелегального съёма информации используются различные технические средства. Информация с объекта поступает злоумышленнику по следующим физическим каналам: акустическим каналам; вибрационному каналу колебаний конструкций здания; электромагнитным каналам; телефонным каналам; электросетевым каналам; визуальным каналам.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата сообщения, технические каналы утечки можно разделить на:

1) Электромагнитные, электрические и параметрические (для телекоммуникационной информации). Примерами вмешательства злоумышленника с использованием такого рода каналов являются перехват побочных электромагнитных излучений; перехват побочных электромагнитных излучений на частотах работы высокочастотных генераторов; перехват побочных электромагнитных излучений на частотах самовозбуждения усилителей низкой частоты.

2) Воздушные (прямые акустические), вибрационные (виброакустические), электроакустические, оптико-электронные и параметрические (для речевой информации);

На основании обработки данных по эксплуатации прослушивающих устройств крупными фирмами (2010 год) были сделаны следующие выводы: для снятия информации чаще всего используется электромагнитный канал (61%) с внедрением на объект "жучков", затем телефонный канал (15%) и далее проводные каналы и диктофоны (13%). Акустический канал с применением направленных микрофонов, вибрационный и электросетевой каналы используются редко.

Рис. 1. Типовая структура канала передачи информации

В общем виде под техническим каналом утечки информации понимают совокупность 1) источника опасного сигнала, 2) среды распространения – носителя опасного сигнала, 3) средства технической разведки. На рисунке 1 представлена обобщенная типовая структура канала передачи информации.

На вход канала поступает информация в виде первичного сигнала $i_{вх}$. Первичный сигнал поступает с некоторого носителя информации или с выхода предыдущего канала. В качестве источника сигнала выступают:

- объект наблюдения, отражающий электромагнитные и акустические волны,
- объект наблюдения, излучающий собственные (тепловые) электромагнитные волны в оптическом и радиодиапазонах,
- передатчик функционального канала связи,
- источник опасного сигнала (т.е. сигнала, который содержит информацию с ограниченным доступом),
- источник акустических волн, модулированных информацией.

Так как информация от источника поступает на вход канала на языке источника (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), то передатчик производит преобразование этой формы представления информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения. В общем случае он выполняет следующие функции:

- создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;
- производит запись информации на носитель (модуляцию информационных параметров носителя);
- усиливает мощность сигнала (носителя с информацией);
- обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.
- Приемник выполняет функции, обратные функциям передатчика. Он производит следующие действия:
 - выбор (селекцию) носителя с нужной получателю информацией;
 - усиление принятого сигнала до значений, обеспечивающих съём информации;
 - съём информации с носителя (демодуляцию, декодирование);
 - преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия [3].

Зона, в которой возможны перехват (с помощью разведывательного приёмника), побочных электромагнитных излучений и последующая расшифровка содержащейся в них информации, называется опасной зоной.

Как любой канал связи, канал утечки информации характеризуется следующими основными показателями: пропускной способностью, дальностью передачи информации.

Пропускная способность канала связи оценивается количеством информации, передаваемой по каналу в единицу времени с определенным качеством.

Перехват информационных сигналов по электрическим каналам утечки возможен путём непосредственного подключения к соединительным линиям вспомогательных технических средств и систем (это информационные системы, размещенные в помещениях обработки конфиденциальной информации) и посторонним проводникам. Для этих целей используют специальные средства радио- и радиотехнической разведки, а также специальная измерительная аппаратура.

Электронные устройства перехвата информации часто называют аппаратными закладками. Они представляют собой мини-передатчики, излучение которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация непосредственно передаётся по радиоканалу или сначала записывается на специальное запоминающее устройство, а уже затем по команде передаётся на запросивший её объект.

В воздушных (прямых акустических) технических каналах утечки информации средой распространения акустических сигналов является воздух.

Звуковые волны оказывают переменное давление на предметы, расположенные на их пути, вызывая механические колебания в твердом теле со звуковой частотой. В отдельных конструкциях эти колебания могут передаваться на значительные расстояния, почти не затухая, и вновь излучаться в воздух, как слышимый воздушный звук. Особенно хорошо излучают звук легкие строительные конструкции с большой площадью поверхности. Передаваемый звук носит название "структурный звук".

Рис. 2. Возникновение акустического канала утечки

Наиболее возможные каналы передачи структурного звука – стены, трубопроводы, каналы воздушной вентиляции помещений и т.д. Таким образом, злоумышленник, находясь даже на значительном расстоянии, может получить желаемую звуковую информацию. На рисунке 2 приведен пример возникновения канала утечки за счет сформированного структурного звука в стенах и перекрытиях здания.

Для перехвата акустической (речевой) информации используют следующие устройства:

- портативные диктофоны и проводные микрофонные системы скрытой звукозаписи;
- направленные микрофоны;
- акустические радиозакладки (передача по радиоканалу);
- акустические сетевые закладки (передача информации по сети питания 220 В);
- акустические инфракрасные-закладки (передача информации по оптическому каналу в инфракрасном диапазоне длин волн);
- акустические телефонные закладки (передача информации по телефонной линии на высокой частоте);
- акустические телефонные закладки типа “телефонное ухо” (передача информации по телефонной линии на низкой частоте).

В вибрационных (виброакустических) технических каналах утечки информации средой распространения акустических сигналов являются элементы конструкций зданий, сооружений (стены, потолки, полы), трубы водоснабжения, канализации и другие твёрдые тела. Воздушные волны человеческой речи воздействуют на строительные конструкции и приводят к колебаниям стен, стекол, батарей и т.д. Для съема информации со стен используется электронные стетоскопы, для съема информации со стекла – лазерные системы, для съема информации с воды трубопроводов – гидроакустические преобразователи. Распознавание информации зависит от материала конструкций, толщины конструкций, от шумов, образующихся в конструкции, от движения людей, транспорта, вибрации.

Данный канал утечки не имеет деконспирационных признаков, и, следовательно, представляется затруднительным технически определить, происходит ли утечка информации по этому каналу. Специалисты осуществляют оценку возможности утечки информации на основании изучения архитектурно-строительной документации на определенную часть объекта с последующей проверкой выводов с помощью стетоскопов. Если оказывается, что такой канал утечки возможен, то встаёт задача закрытия этого канала.

Для закрытия канала целесообразно применять искусственные источники помех – системы виброакустического зашумления (рисунок 3). Она состоит из генератора шума Г, формирующего помеху в диапазоне частот 0,2 – 5,0 кГц; усилителя мощности УМ, включаемого устройством управления УУ, которое включается голосом или вручную, и вибратора Вб (электромеханического преобразователя), обеспечивающего преобразование электрического сигнала в механические колебания конструкции. Генератор создает шум, который пода-

ется на усилитель мощности. Сигналом с устройства управления включается усилитель мощности, и сигнал с него поступает на вибратор. Вибратор начинает работать, и появляются колебания стены, которые зашумляют колебания стены от акустического сигнала.

Рис. 3. Структурная схема системы

Виброакустического зашумления.

Программные закладки класс программ с потенциально опасными последствиями, обязательно выполняющие следующие функции:

- разрушают код программы в памяти;
- сохраняют фрагменты информации из оперативной памяти в некоторой области внешней памяти прямого доступа;
- искажает произвольным образом, блокирует или подменяет выводимые во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ.

Программная реализация несанкционированного доступа к информации на основе использование программных закладок. Под несанкционированным доступом (НСД) к ресурсам компьютерной системы понимаются по использованию, изменению и уничтожению используемых данных указанной системы, производимые субъектом, не имеющие права на такие действия. Если компьютерная система содержит механизмы защиты от несанкционированного доступа, то несанкционированные действия могут быть вызваны:

- отключением или видоизменением защитных механизмов нелегальным пользователям;
- входом в систему под именем и с полномочиями реального пользователя.

В первом случае злоумышленник должен видоизменить программу, защитные механизмы в системе (например, отключить программу запросов пользователей), во втором – каким-либо образом выяснить или подделать идентификатор реального пользователя (например, подсмотреть или вычислить пароль, вводимый с клавиатуры).

В обоих случаях несанкционированный доступ можно представить моделью опосредованного доступа, когда проникновение в систему осуществляется на основе некоторого воздействия, произведенного предварительно внедренной в систему программой или несколькими программами.

Особый интерес представляют уязвимые места компьютерных систем, используемые для внедрения программных закладок.

Внедрение возможно на всех участках жизненного цикла программного обеспечения:

- эскизного и технического проектирования;
- рабочего проектирования;
- внедрения;
- эксплуатации, включая сопровождение и модернизацию.

Несанкционированный доступ к ресурсам компьютерной системы. Несанкционированный доступ к ресурсам компьютерной системы – действия по использованию, изменению и уничтожению используемых модулей и массивов данных, производимые субъектом, не имеющим права на такие действия.

Несанкционированное вмешательство в процесс обмена сообщениями между узлами связи локально вычислительных сетей. Осуществляется путем передачи следующих сообщений:

- разрушающих;
- искажающих;
- имитирующих;
- хаотических.

Под уязвимостью компьютерной системы понимается некоторая слабость системы безопасности, которая может послужить причиной нанесения компьютерной системе ущерба. Обычно слабые (уязвимые) места в компьютерной системе называются дырами, люками, брешами.

Люк – механизм внутри операционной системы (программное обеспечение), позволяющий программе злоумышленника получить привилегированную функцию. Умышленный люк может присутствовать в программе из-за того, что программист умышленно оставил его в программе, например:

- для обеспечения тестирования или выполнения оставшейся части отладки;
- в интересах облегчения окончательной сборки конечного программного продукта;
- с тем, чтобы иметь скрытое средство доступа к программе уже после того, как она вошла в состав конечного продукта.

В найденной брешу программа «разрывается», и туда дополнительно вставляют одну или несколько команд. Этот люк «открывается» по мере необходимости, а встроенные команды автоматически осуществляют свою задачу. Люк – это возможность получить управление системой в обход защиты.

Из всех известных угроз наиболее часто встречаются программные закладки типа «троянского коня» и «компьютерного червя».

«Троянский конь» – программа, имеющая законный доступ к системе. Но выполняющая и скрытые функции. Закладки типа «троянский конь» проявляют себя в различных в определенных условиях (по времени, ключевым сообщениям) и могут разрушать (искажать) информацию, копировать фрагменты конфиденциальной информации или пароли (ключи), засылать сообщения не по адресу или блокировать прием (отправку) сообщений.

В последние годы наиболее распространенным способом получения приватной информации стало использование программ – троянов – программ, выполняющих помимо заявленных некоторые дополнительные не афишируемые функции, направленные, например, на получение личной информации пользователя. Конечный пользователь получает их, как правило, по системе электронной почты под видом важного документа или давно разыскиваемой программы. После запуска программа прописывается в системном реестре для запуска при загрузке операционной системы и начинает собирать информацию. Ее целью могут быть файлы учетной записи пользователя, содержащие его пароль, скрипты удаленного доступа к Интернет или пароли электронной почты.

Возможна также ее работа в режиме подслушивания – в этом случае, например, все вводимые с клавиатуры символы записываются в отдельный файл, кроме того, «прослушиваться» может и передаваемая по сети информация. Далее вся собранная информация отправляется атакующему для дальнейшего анализа на предмет содержания ценной информации, такой как пароли или личная пользовательская информация.

Возможен также и самый простой способ: при работе пользователя на компьютере программа выводит на экран системное окно с предложением ввести имя пользователя и пароль, маскируясь под работу операционной системы. В результате пользователь «добровольно» сообщает злоумышленнику свой пароль, даже не подозревая о происшедшем. А если этим пользователем окажется ответственный сотрудник, то перед атакующим откроются огромные возможности.

«Программный червь» программа, маскирующаяся под системные средства поиска свободных вычислительных ресурсов в сети. Закладки типа компьютерного червя нацелены на проникновение в системы разграниченного доступа пользователей к ресурсам сети, к наущению работы всей сети в целом и системы разграничения доступа в частности.

Для того чтобы закладка смогла выполнить какие-либо функции по отношению к прикладной программе, она должна, получить управление на себя, т.е. процессор должен начать выполнять инструкции (команды), относящиеся к коду закладки. Это возможно только при одновременном выполнении двух условий:

– закладка должна находиться в оперативной памяти до начала работы программы, которая является целью воздействия закладки; следовательно, она должна быть загружена раньше или одновременно с этой программой;

– закладка должна активизироваться по некоторому общему как для закладки, так и для программы событию, т.е. при выполнении ряда условий в программно-аппаратной среде управление должно быть, передано на программу – закладку.

К способам задеирования программных закладок можно отнести:

1. запуск программы;
2. прерывания;
3. определенное сочетание входных данных;
4. определенное сочетание условий применения системы.

По времени пребывания программной закладки в оперативной памяти можно выделить следующие типы закладок:

– резидентного вида – находятся постоянно с некоторого момента до окончания сеанса работы персонального компьютера (включения питания или перезагрузке). Закладка может быть загружена в память при начальной загрузке ПЭВМ, загрузке операционной среды или запуске некоторой программы (которая по традиции называется вирусоносителем), а также запущена отдельно;

– нерезидентного вида – начинают работу по аналогичному событию, но заканчивают ее самостоятельно по истечении некоторого промежутка времени или некоторому событию, при этом выгружая себя из памяти целиком.

Помимо классификации программных закладок по времени пребывания в оперативной памяти их можно классифицировать еще по методу их внедрения и по типам вредоносного воздействия. Представленная на рисунке 2 классификация выполнена достаточно наглядно и дополнительного пояснения не требует.

Таким образом, программные закладки в настоящее время являются наиболее мощным и эффективным инструментом в реализации компьютерных угроз, защита от которых должна быть динамичной и постоянно совершенствования. Одним из наиболее эффективных способов борьбы с сетевыми угрозами, в том числе с программными закладками, является совершенствования методов и средств контроля доступа к сети.

Заключение

Обеспечение сохранности информации – одна из основных и наиболее сложных задач, которые необходимо решать каждому предприятию. Сегодня организация работы любого предприятия, будь оно частным или государственным, претендующего на успешное развитие, обязательно базируется на современных информационных технологиях. Поэтому необходимо обращать внимание на стандарты управления информационной безопасностью. Как правило, вопросы управления информационной безопасностью тем актуальнее, чем крупнее организация, чем шире масштаб ее деятельности и претензии на развитие, и, как следствие, выше ее зависимость от информационных технологий.

Деятельность по защите информационных ресурсов от утечки информации должна быть строго спланирована и состоять из нескольких этапов:

1 этап – постановка задачи. Составление списка сведений, которые несут наиболее важную информацию.

2 этап – оценка ущерба, если сведения из перечня будут известны конкуренту; определение времени, необходимого конкуренту для реализации добытой информации.

3 этап – определение источников и каналов утечки информации.

4 этап – определение возможностей предотвращения утечки информации.

5 этап – определение стоимости мероприятий по защите информации.

Список литературы:

1. Хорев А.А. Защита информации от утечки по техническим каналам. М.: НПЦ «Аналитика», 2008. С. 436-440.
2. Сидорин Ю.С. Технические средства защиты информации. СПб.: СПбГПУ, 2005. С. 4-6, 8-10, 12-15.
3. Андрианов В.И., Бородин В.А., Соколов А.В. Шпионские штучки и устройства для защиты объектов и информации. Справочное пособие. СПб.: Лань, 1997. С. 198-205.
4. Рыжиков Ю.И., Лохвицкий В.А. Расчет узла сети с отрицательными заявками // Информационные технологии в управлении (ИТУ-2012). 2012. С. 354-359.
5. Нечай А.А. Выявление недеklarированных возможностей аппаратно-программного обеспечения // Экономика и социум. 2014. № 1-2(10). С. 457-460.
6. Лохвицкий В.А., Калинин С.В., Нечай А.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации // Мир современной науки. 2014. № 2 (24). С. 8-12.

References:

1. Horev A.A. Protection of information from leakage through technical channels. M: research Analyst, 2008. P. 436-440.
2. Sidorin Y.C. Technical means of information protection. SPB.: SPbSPU, 2005. P. 4-6, 8-10, 12-15.
3. Andrianov C.I., Borodin C.A., Sokolov A.C. Spy stuff and device for protection of objects and information. Reference manual, SPB.: DOE, 1997. P. 198-205.
4. Ryzhikov Y.I., Lohvitski C.A. Calculation of node networks with negative customers // Information technologies in management (ITU-2012). 2012. P. 354-359.
5. Nechay A.A. Detection of undeclared capabilities of the hardware-software // Economy and society. 2014. № 1-2(10). P. 457-460.
6. Lohvitski C.A., Kalinichenko S.C., Nechay A.A. Approach to building a system for automated integration of data into a database for its timely update // Modern science. Publishing House. 2014. №2(24). P. 8-12.

© 2014, Нечай А.А., Проточанская Ю.Ю.,
Котиков П.Е.
Анализ каналов утечки информации

© 2014, Nechay A.A., Protochanska Yu.Yu.,
Kotikov P.E.
Analysis of the channels of leakage of information