НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ "ЗАХИСТ ІНФОРМАЦІЇ" №4, 2003

УДК 621

А.В. Зайчук

Основные пути утечки информации и несанкционированного доступа в корпоративных сетях

Корпоративная сеть (КС) – система, обеспечивающая передачу информации между различными приложениями, используемыми в корпорации. Исходя из этого вполне абстрактного определения, рассмотрим назначение и значимость передаваемой информации в корпоративных сетях и всевозможные пути утечки информации.

1. Определение корпоративной сети и ее назначение

Корпоративная сеть является *базовой несущей конструкцией современной организации* вне зависимости от того, является ли данная организация коммерческой (торговой, промышленной, многопрофильной) или относится к государственному сектору.

Корпоративная Сеть - это инфраструктура организации, поддерживающая решение актуальных задач и обеспечивающая достижение ее целей (то есть выполнение миссии организации). Она объединяет в единое пространство информационную систему (ИС) всех объектов Корпорации. КС создается в качестве системно-технической основы ИС, как ее главный системообразующий компонент, на базе которого конструируются другие подсистемы.

С функциональной точки зрения КС - это эффективная среда передачи актуальной информации, необходимой для решения задач корпорации. С системно-технической точки зрения Сеть представляет собой целостную структуру, состоящую из нескольких взаимосвязанных и взаимодействующих уровней: интеллектуальное здание; компьютерная сеть; телекоммуникации; компьютерные платформы; программное обеспечение (ПО) промежуточного слоя (middleware); приложения.

С точки зрения системной функциональности КС выглядит как единое целое, предоставляющее пользователям и программам набор полезных в работе услуг (сервисов), общесистемных и специализированных приложений, обладающее набором полезных качеств (свойств) и содержащее в себе службы, гарантирующие нормальное функционирование КС[1].

Практически вся информация связанная с деятельностью крупных предприятий обрабатывается, анализируется и передается с помощью КС. Следовательно, этот аргумент наводит на мысль о необходимости защиты информации, то есть руководитель предприятия должен понять всю остроту проблемы утечки, потери и уничтожения информации и позаботиться о создании системы защиты. Перед началом создания системы защиты необходимо разобраться и понять ряд элементарных понятий, связанных с каналами утечки информации. Этот вопрос более детально раскрыт и рассмотрен в следующем пункте данной статьи.

2. Особенности современных каналов утечки и несанкционированного доступа к информации

Для того чтобы построить эффективную систему информационной безопасности, необходимо в первую очередь определить реальные и потенциальные угрозы, каналы несанкционированного доступа и утечки информации. Рассмотрим более подробно особенности каналов утечки и несанкционированного доступа к информации.

Одним из основных требований интегральной защиты является системный подход, поэтому при выявлении технических каналов утечки информации необходимо рассматривать всю совокупность элементов защиты, включающую основное

оборудование технических средств обработки информации (ТСОИ), оконечные устройства, соединительные линии, распределительные и коммутационные устройства, системы электропитания, системы заземления и т. п.

Наряду с основными техническими средствами, непосредственно связанными с обработкой и передачей конфиденциальной информации, необходимо учитывать и вспомогательные технические средства и системы (ВТСС), такие, как технические средства открытой телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрофикации, радиофикации, часофикации, электробытовые приборы и др.

В качестве каналов утечки большой интерес представляют вспомогательные средства, выходящие за пределы контролируемой зоны, а также посторонние провода и кабели, к ним не относящиеся, но проходящие через помещения, где установлены основные и вспомогательные технические средства, металлические трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции.

В зависимости от способов перехвата, от физической природы возникновения сигналов, а также среды их распространения технические каналы утечки информации можно разделить на электромагнитные, электрические и параметрические.

Для электромагнитных каналов утечки характерными являются побочные излучения:

- *электромагнитные излучения элементов ТСОИ* (носителем информации является электрический ток, сила тока, напряжение, частота или фаза которого изменяются по закону информационного сигнала);
- *электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС* (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство);
- *электромагнитные излучения на частотах самовозбуждения усилителей низкой частоты ТСОИ* (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автогенерации сигналов, причем сигнал на частотах самовозбуждения, как правило, оказывается промодулированным информационным сигналом).

Возможными причинами возникновения **электрических каналов утечки** могут быть:

- *наводки электромагнитных излучений ТСОИ* (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС);
- *просачивание информационных сигналов в цепи электропитания* (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала);
- *просачивание информационных сигналов в цепи заземления* (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы контролируемой зоны, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);
- *съем информации с использованием закладных устройств* (представляют собой минипередатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами контролируемой зоны).

Параметрический канал утечки информации формируется путем "высокочастотного облучения" ТСОИ, при взаимодействии электромагнитного поля которого с

элементами ТСОИ происходит переизлучение электромагнитного поля, промодулированного информационным сигналом.

Анализ возможных каналов утечки и несанкционированного доступа показывает, что существенную их часть составляют технические каналы утечки акустической информации, носителем которой являются акустические сигналы. В зависимости от среды распространения акустических колебаний, способов их перехвата и физической природы возникновения информационных сигналов технические каналы утечки акустической информации можно разделить на воздушные, вибрационные, электроакустические, оптико-электронные и параметрические.

В **воздушных** технических каналах утечки информации средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные и направленные микрофоны, которые соединяются с диктофонами или специальными минипередатчиками. Подобные автономные устройства, объединяющие микрофоны и передатчики, обычно называют закладными устройствами или акустическими закладками. Перехваченная этими устройствами акустическая информация может передаваться по радиоканалу, по сети переменного тока, соединительным линиям, посторонним проводникам, трубам и т. п. В этом случае прием осуществляется, как правило, на специальные приемные устройства. Особого внимания заслуживают закладные устройства, прием информации с которых можно осуществить с обычного телефонного аппарата. Для этого их устанавливают либо непосредственно в корпусе телефонного аппарата, либо подключают к телефонной линии в телефонной розетке. Подобные устройства, конструктивно объединяющие микрофон и специальный блок коммутации, часто называют "телефонным ухом". При подаче в линию кодированного сигнала или при дозвоне к контролируемому телефону по специальной схеме блок коммутации подключает микрофон к телефонной линии и осуществляет передачу акустической (обычно речевой) информации по линии практически на неограниченное расстояние.

В отличие от рассмотренных выше каналов в **вибрационных**, или **структурных**, каналах утечки информации средой распространения акустических сигналов является не воздух, а конструкции зданий (стены, потолки, полы), трубы водо- и теплоснабжения, канализации и другие твердые тела. В этом случае для перехвата акустических сигналов используются контактные, электронные (с усилителем) и радиостетоскопы (при передаче по радиоканалу).

Электроакустические каналы утечки информации обычно образуются за счет электроакустических преобразований акустических сигналов в электрические по двум основным направлениям: путем "высокочастотного навязывания" и путем перехвата через ВТСС. Технический канал утечки информации путем **высокочастотного навязывания** образуется путем несанкционированного контактного введения токов высокой частоты от ВЧ-генератора в линии, имеющие функциональные связи с элементами ВТСС, на которых происходит модуляция ВЧ-сигнала информационным. Наиболее часто подобный канал утечки информации используют для перехвата разговоров, ведущихся в помещении, через телефонный аппарат, имеющий выход за пределы контролируемой зоны. С другой стороны, ВТСС могут сами содержать электроакустические преобразователи. К таким ВТСС относятся некоторые датчики пожарной сигнализации, громкоговорители ретрансляционной сети и т. д. Используемый в них эффект обычно называют **микрофонным эффектом**. Перехват акустических колебаний в этом случае осуществляется исключительно просто. Например, подключая рассмотренные средства к соединительным линиям телефонных аппаратов с электромеханическими звонками, можно при положенной трубке прослушивать разговоры, ведущиеся в помещениях, где установлены эти телефоны.

При облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей, таких, как стекла окон, зеркал, картин и т. п., создается

оптико-электронный, или **лазерный,** канал утечки акустической информации. Отраженное лазерное излучение модулируется по амплитуде и фазе и принимается приемником оптического излучения, при демодуляции которого выделяется речевая информация. Для перехвата речевой информации по данному каналу используются локационные системы, работающие, как правило, в ближнем инфракрасном диапазоне волн и известные как "лазерные микрофоны". Дальность перехвата составляет несколько сотен метров.

Параметрический канал утечки информации образуется в результате воздействия акустическою поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т. п., что приводит к изменениям параметров сигнала, например модуляции его информационным сигналом. Промодулированные высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены и детектированы соответствующими средствами. Параметрический канал утечки информации может быть создан и путем "высокочастотного облучения" помещения, где установлены полуактивные закладные устройства, имеющие элементы, параметры которых (добротность, частота и т. п.) изменяются по закону изменения акустического (речевого) сигнала.

Необходимо отметить, что акустический канал может быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с принтера или клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

Особый интерес представляет **перехват информации при ее передаче по каналам связи**. Это вызвано тем, что в этом случае обеспечивается свободный несанкционированный доступ к передаваемым сигналам. Единственным гарантированным методом защиты информации в этом случае является криптографическая защита. В зависимости от вида каналов связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Этот **электромагнитный канал** перехвата информации широко используется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

Электрический канал перехвата информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. Этот канал наиболее часто используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называются телефонными закладками.

Однако непосредственное электрическое подключение аппаратуры перехвата является компрометирующим признаком. Поэтому чаще используется **индукционный канал** перехвата, не требующий контактного подключения к каналам связи. Современные индукционные датчики, по сообщениям открытой печати, способны снимать информацию с кабелей, защищенных не только изоляцией, но и двойной броней из стальной ленты и стальной проволоки, плотно обвивающих кабель.

В последнее время стало уделяться большое внимание утечке **видовой информации,** получаемой техническими средствами в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения обычно используются

соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры, телекамеры, приборы ночного видения, тепловизоры и т. п.

Для документирования результатов наблюдения проводится съемка объектов, для чего используются фотографические и телевизионные средства, соответствующие условиям съемки. Для снятия копий документов используются электронные и специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют видеозакладки.

Наиболее динамично развиваются в последнее время методы съема компьютерной информации. Несмотря на то что в этом направлении также используются различные аппаратные закладки, основные возможности несанкционированного доступа обеспечиваются специальным математическим обеспечением, включающим в себя такие составляющие, как компьютерные вирусы, "логические бомбы", "троянские кони", программные закладки и т. п.. Современные компьютерные вирусы обладают широкими возможностями враждебного воздействия, начиная от безобидных шуток и кончая серьезными повреждениями аппаратуры. Бороться с подобными вирусами, как и с подавляющим большинством других, можно, к сожалению, лишь после его появления.

Рассмотренные выше методы получения информации основаны на использовании внешних каналов утечки. Однако необходимо остановиться и на внутренних каналах утечки информации, тем более что обычно им не придают должного внимания и много теряют. Внутренние каналы утечки связаны, как правило, с администрацией и обслуживающим персоналом, с качеством организации режима работы. Из них в первую очередь можно отметить такие каналы утечки, как хищение носителей информации, съем информации с ленты принтера и плохо стертых дискет, использование производственных и технологических отходов, визуальный съем информации с дисплея и принтера, несанкционированное копирование и т. п.[2].

На рисунке 1 приведены результаты анализа возможных направлений утечки информации и путей несанкционированного доступа (как прямого, так и косвенного) в каналах корпоративных сетей.

В заключении можно дополнить, что в силу своей специфики информация о возможных каналах утечки и несанкционированного доступа длительное время была недоступна широкому пользователю, что, безусловно, способствовало росту злоумышленных воздействий. Совершенно очевидно, что для успешной защиты своей информации пользователь должен иметь абсолютно ясную картину о возможных каналах утечки, чтобы соответствующим образом предпринять контрмеры по пресечению несанкционированного доступа (усилить программную защиту, использовать антивирусные программы, сменить алгоритм закрытия, усилить пароли и т.п.).

Необходимо отметить, что особую опасность в настоящее время представляет проблема компьютерного вируса, так как с учетом большого числа его модификаций надежной защиты против него не удалось разработать. Все остальные пути несанкционированного доступа поддаются надежной блокировке при правильно разработанной и реализуемой на практике системе обеспечения безопасности. Независимо от того, насколько хорошо разработаны технические и организационные меры безопасности и соблюдения конфиденциальности, они в конце концов основываются на человеческой деятельности, в которой возможны ошибки и злой умысел. Если отдельный сотрудник обманет доверие, то никакая система безопасности не сможет предотвратить утечку информации.

Для обеспечения уверенности в том, что данная организация успешно поддерживает функционирование системы безопасности, необходимо применять различные методы проверки. Это регулярные независимые инспекции и ревизии, а также проверочные комиссии, состоящие из представителей всех лиц, участвующих в работе с конфиденциальной информацией.

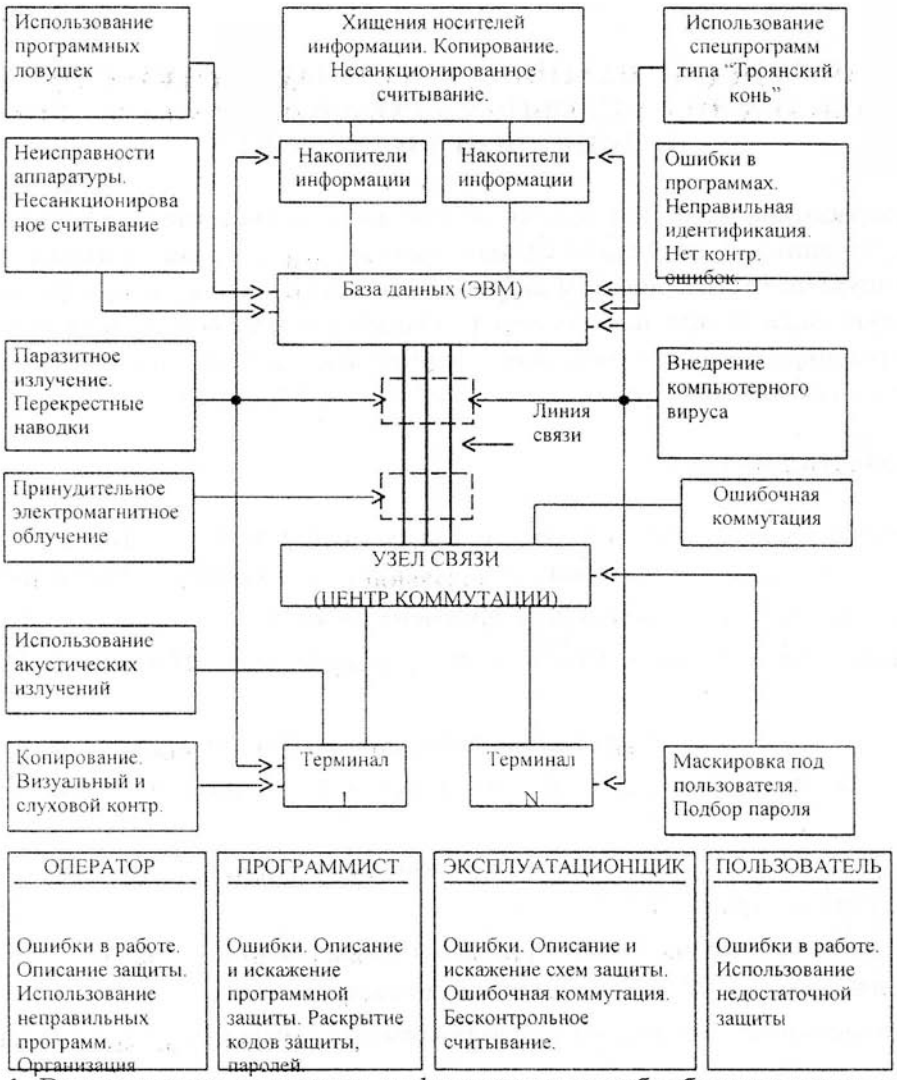

Рис. 1. Возможные пути утечки информации при обработке и передаче данных в каналах корпоративных сетей

Так как ни одна из форм не является идеальной, то общий контроль за деятельностью системы защиты и ее функционированием должен осуществлять высший орган руководства организации, предприятия через специальные подразделения обеспечения безопасности.

Литература:

1. Т. И. Иванова Корпоративные сети связи. – М.: Эко-Трендз, 2001.
2. В. С. Барсуков Безопасность: технологии, средства, услуги. – М.: КУДИЦ – ОБРАЗ, 2001 – 496 с.

Поступила 22.04.2003
После доработки 12.06.2003