М. В. Тарасюк

ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ КАТЕГОРИРОВАННЫХ СЕТЕЙ С СЕТЯМИ ОБЩЕГО ПОЛЬЗОВАНИЯ

Повышению эффективности любой организации или ведомства в значительной степени способствует предоставление оперативного доступа ее сотрудников к любым данным, имеющим отношение к их служебной деятельности. Если вся необходимая информация обрабатывается в пределах территории, контролируемой одной администрацией (контролируемой зоны), для решения данной задачи используют традиционные сетевые и телекоммуникационные технологии, объединяющие все ресурсы организации в единую корпоративную сеть с общей политикой безопасности, правилами создания, распределения и использования конфиденциальных данных. На практике часто возникает необходимость доступа пользователей (абонентов) корпоративной сети к ресурсам внешних сетей общего пользования.

В [1] представлена модель нарушителя и структура поля угроз ИТ, учитывающая возможность внедрения в защищенные сети деструктивных программ с целью компрометации данных, циркулирующих в категорированных сетях. Потенциальными источниками угроз, которые следует принимать во внимание при принятии решения о предоставлении доступа в открытые сети для абонентов категорированных сетей, являются следующие факторы:

1) Ошибки пользователей — могут приводить к непреднамеренной (случайной) выдаче информации в открытую сеть;

2) Уязвимости программного обеспечения — могут приводить к несанкционированному доступу в категорированную сеть непосредственно нарушителей из внешней сети либо вызвать случайную утечку информации в открытую сеть (например, к числу уязвимостей данного вида относятся всевозможные варианты некорректной обработки программами входных данных);

3) Программные закладки и деструктивные программы — могут быть заранее внедрены в защищенную сеть. При определенных условиях они могут активизироваться и передать информацию во внешнюю сеть под видом запросов легальных пользователей.

4) При внедрении программных закладок в категорированную сеть утечка информации может осуществляться путем ее встраивания в параметры запросов доступа (адреса, типы протоколов, команды инициализации модемов и т. д.) либо за счет манипуляции параметров запросов доступа в открытой сети, когда разные комбинации разрешенных параметров образуют кодовые символы для передачи данных программой-нарушителем.

Уровень требований безопасности для доступа к открытой сети может быть установлен исходя из анализа модели нарушителя — описания возможностей, которые могут использоваться для компрометации конфиденциальной информации.

Рассмотренная модель нарушителя такова, что одновременная работа пользователя в категорированной сети и в открытой сети не обеспечивает гарантированную защиту информации от утечки, в связи с чем в России действует указ президента (№ 351 от 2008 г.), запрещающий подключение категорированных сетей, обрабатывающих информацию, составляющую государственную тайну, к сетям общего доступа.

Как правило, для предоставления доступа к ресурсам открытых сетей в организациях, где требуется доступ к таким сетям, разворачиваются две физически независимые локальные сети: одна — для обработки конфиденциальной (секретной) информации, а другая — для доступа к ресурсам открытых сетей. Данное решение, хотя и не налагает каких-либо ограничений на

работу пользователей, тем не менее очень затратное (по всем статьям расходов — проектирование объектов, закупка технических средств, эксплуатационное обслуживание). Кроме того, необходимы дополнительные помещения для размещения абонентских пунктов.

В качестве альтернативного решения можно использовать односторонние шлюзы взаимодействия с адаптивно настраиваемой таблицей ссылок на ресурсы открытой сети. Для каждого пользователя задается перечень разрешенных для доступа ссылок, динамически пополняемый перекрестными и внутренними ссылками (гиперссылками), извлекаемыми из HTML-страниц, передаваемых абонентам. Конструктивное исполнение такого шлюза целесообразно выполнить в виде комплекса, состоящего из трех составных частей, называемых далее сервером доступа, модулем контроля запросов доступа (МКЗД), шлюзом сопряжения.

Схематично системная архитектура рассматриваемого шлюза показана на рис. 1. Сервер доступа и шлюз сопряжения строятся на базе стандартной аппаратно-программной платформы с двумя сетевыми интерфейсами, один из которых служебный (используется для взаимодействия с МКЗД), а другой — для соединения с терминальным оборудованием абонентов (сервер доступа) и узлами открытой сети.

МКЗД представляет собой специализированную одноплатную ЭВМ или (лучше) аппаратный модуль, так как при этом оказывается проще обосновать защищенности устройства.

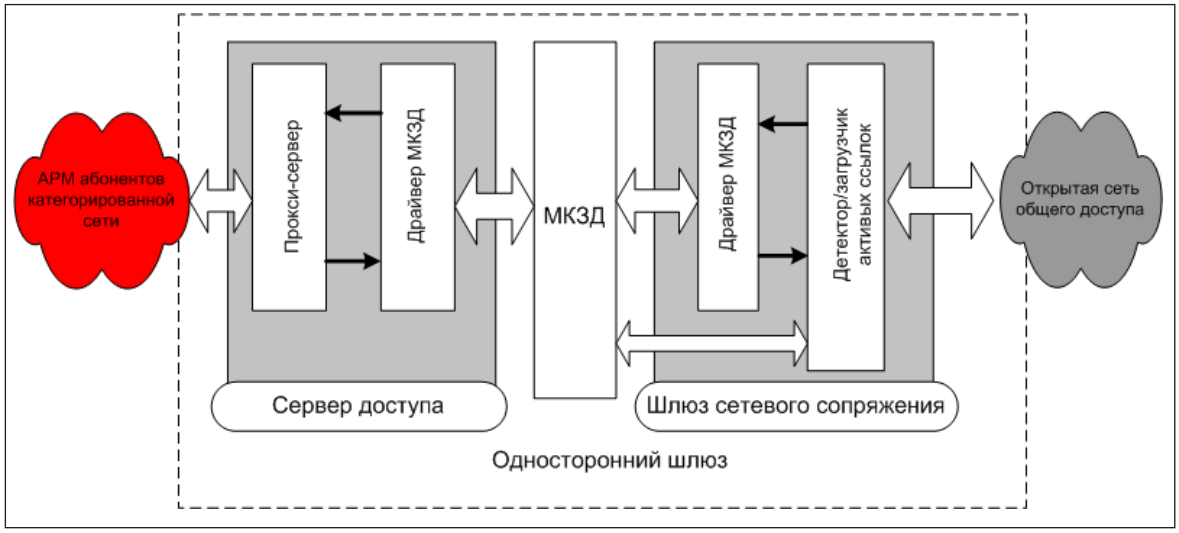

Рис. 1. Системная архитектура шлюза взаимодействия

В состав шлюза взаимодействия, как показано на рис. 1, входят следующие функциональные компоненты:

- прокси-сервер, обеспечивающий прием и обработку запросов со стороны пользователей абонентов категорированной сети путем реализации политики безопасности в части идентификации и подотчетности доступа к ресурсам;
- драйвер МКЗД, реализующий протокол взаимодействия с МКЗД и предназначенный для передачи через МКЗД запросов в открытую сеть (фактически ссылок на сайты открытой сети) и передачи в обратном направлении извлеченных данных;
- детектор/загрузчик ссылок на ресурсы, предназначенный для сканирования загружаемых ресурсов (страниц) сети Интернет, извлечения из них перекрестных и внутренних ссылок и выдачи в МКЗД для последующего использования.

Примечание: предполагается, что функции IP-маршрутизации и фильтрации сетевых потоков реализуются средствами операционной системы шлюза сопряжения.

С учетом принятой модели нарушителя организация доступа в открытую сеть через односторонний шлюз характеризуется возможностью возникновения канала утечки, вызванного навязыванием алфавита модуляции со стороны нарушителей внешней сети. Смысл угрозы заключается в том, что пользователь, осуществляя загрузку из внешней сети HTML-страницы, содержащей ссылки на другие ресурсы (страницы), обновляет данные конфигурации МКЗД (перечень разрешенных ссылок), давая, таким образом, возможность программе нарушителя (внедренной в объект) использовать данные ссылки для построения схемы сигнального алфавита.

Для оценки пропускной способности канала утечки информации удобно представить сегмент открытой сети, являющийся объектом доступа со стороны корпоративных пользователей, в виде случайного графа, в вершинах которого находятся ссылки на информационные ресурсы (они прозрачно передаются через МКЗД). Вершины графа предполагаются случайным образом связанными между собой. Вероятность такой связи (далее – P) иногда называют коэффициентом кластеризации сети, поскольку он определяет способность к образованию отдельных связанных подграфов и задает, в конечном счете, «близость» двух произвольно выбранных вершин. Кроме того, далее будем полагать, что в составе сервера доступа реализован буферный кэш, исключающий возможность в течение близких моментов времени выдавать запросы доступа на одну и ту же страницу сети. Это исключит из предлагаемой схемы модуляции замкнутые циклы перехода по ссылкам. При этом факт повторного использования одной и той же ссылки не может быть обнаружен нарушителем.

Различным информационным символам будем сопоставлять последовательности запросов обращения к внешним ссылкам, которые фиксирует нарушитель за границами контролируемой зоны. В соответствии с принятыми нами ограничениями для оценки мощности алфавита необходимо найти общее число траекторий (возможных последовательностей внешних ссылок), исходящих из заданного множества вершин. Для простоты будем полагать, что для пользователя в начальный момент времени разрешен доступ для работы только по одной (корневой) ссылке. При сделанных допущениях число незамкнутых траекторий в полносвязанном графе, соединяющих корневую вершину (ссылку) и любые другие доступные через нее ссылки, можно вычислить как сумму числа размещений из n элементов по всем возможным длинам траекторий. С учетом того, что в случайном графе вероятность наличия траектории длины i есть P^i, среднее число искомых траекторий Q можно вычислить по формуле:

$$Q = \sum_{i=0}^{n} \frac{n!}{(n-i)!} P^i \,. \qquad (1)$$

Поскольку нас интересует верхняя оценка пропускной способности (вероятности использования различных траекторий, применяемых для кодирования символов скрытого канала, должны быть одинаковыми), информативность запроса (средняя пропускная способность канала утечки на один запрос) можно вычислить по формуле W = Log(Q)/n. Для практического использования оценка опасности канала должна исходить из неограниченного n, поскольку, используя ссылки на ресурсы, можно за относительно небольшое число шагов достигнуть любого ресурса открытой сети. Данное свойство присуще так называемым моделям «малого мира». Таким образом, для больших значений n можно преобразовать формулу (1) к виду:

$$Q = n! \cdot P^n \sum_{i=0}^{n} \frac{P^{-(n-i)}}{(n-i)!} \approx n! \cdot P^n \cdot e^{\frac{1}{P}} \,.$$

Для дальнейшего упрощения можно воспользоваться формулой Стирлинга для приближенной аппроксимации факториала, в результате чего для информативности запроса W (в двоичных единицах измерения количества информации) получим выражение:

$$W = \frac{1}{2n} Log(2\pi) + \frac{Log(n)}{2n} + \frac{1}{Pn} + Log(n) + Log(P) - 1 \,,$$

где функция логарифма вычисляется по основанию 2. Поскольку для больших значений n первый и второй члены формулы будут стремиться к нулю, можно окончательно записать:

$$\lim_{n\to\infty}[W] = \frac{1}{Pn} + Log(Pn) - 1.$$

Для иллюстрации информативности запросов на рис. 2 приведены графики зависимостей точной и приближенной оценок W от коэффициента кластеризации сети (P), построенные при n = 20.

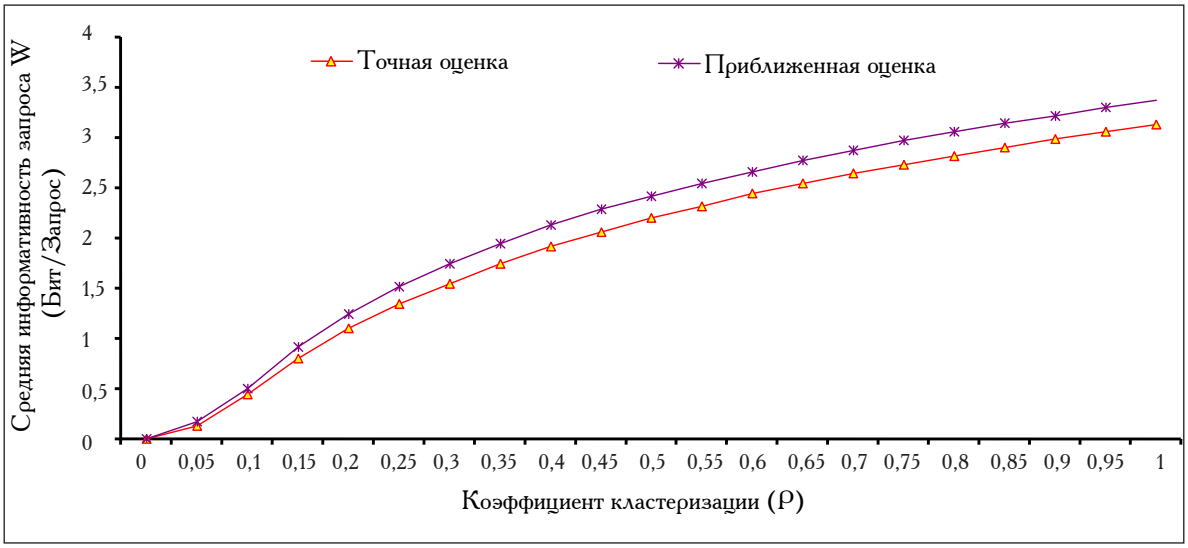

Рис. 2. Оценки информативности запросов к открытой сети

Произведение nP в вышеприведенной формуле дает оценку для среднего количества ресурсов открытой сети, связанных с другими ресурсами (доступными по ссылкам). Значение nP для сегментов открытой сети можно оценить, анализируя структуру реальных сайтов.

Угроза утечки, построенной по рассмотренной схеме кодирования, базируется на принятии достаточно жесткого предположения, а именно на этапе внедрения программной закладки в категорированную сеть нарушителю должна быть известна информация о множестве корневых ссылок, загруженных в шлюз, и о ресурсах открытой сети, доступных для работы абонентов. При этом модель канала утечки предполагает обращение к ссылкам в строго заданной последовательности, определяющейся порядком следования информационных символов. В противном случае информационные символы будут переставлены местами и передаваемая информация будет полностью или частично разрушена.

В качестве мер противодействия скрытой утечке информации через односторонний шлюз можно предложить следующее:

1. Установка в составе сервера доступа прикладных фильтров, ограничивающих область ресурсов открытой сети, доступных для работы абонентов. Эта мера позволяет снизить мощность алфавита, исключив его неконтролируемое расширение.

2. Генерация и передача ложных запросов доступа в открытую сеть, создающих помеху для ведения скрытого информационного обмена. Интенсивность ложных запросов должна определяться исходя из текущих значений параметра n (число «незасвеченных» в МКЗД ссылок) и заданных норм защиты. В качестве таких норм могут быть использованы, например, показатели защищенности информации от утечки по каналам ПЭМИН [2].

3. Проектирование подсетей доступа в открытые сети, обеспечивающее концентрацию телекоммуникационной нагрузки от возможно большего числа абонентских пунктов (увеличение числа пользователей, использующих для работы один шлюз). В этом случае для канала скрытой

передачи данных создается дополнительная помеха, вызванная одновременной обработкой запросов от многих абонентов.

Каждый из предложенных методов обладает своими достоинствами и недостатками. Ограничение области доступа в открытую сеть потребует тщательной работы администратора, но при этом не создает дополнительных накладных расходов при обмене данными. Маскировочная нагрузка не требует участия администратора, в то же время позволяя снизить информативность запросов до любого заданного значения, однако при этом создается дополнительная, весьма ощутимая нагрузка на каналы и ресурсы внешней сети, снижающая вероятностно-временные характеристики обслуживания абонентов. Концентрация нагрузки в одной точке доступа обладает низким уровнем гарантий безопасности, так как часто оказывается возможным найти время, когда шлюз простаивает и скрытая передача информации может быть выполнена без помех.

Могут использоваться и другие меры, снижающие опасность рассмотренных каналов утечки. Например, хорошей практикой является принятие организационных мер, предотвращающих или затрудняющих внедрение деструктивных программ в категорированную сеть (запрет использования внешних носителей, конфигурация прав доступа, исключающая разработку и отладку кода в терминальном оборудовании абонентов), ведение журналов и средств их анализа, выявляющих аномалии трафика, свидетельствующие о возможных проблемах безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Тарасюк М. В.* Защищенные информационные технологии. Вопросы проектирования и применения. М.: Солон пресс, 2004.
2. *Тарасов И. В., Тарасюк М. В.* Выбор норм эффективности защиты от утечки информации по скрытым каналам модуляции трафика в средствах сетевого шифрования // Информационные технологии. 2006. № 8.