электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 621.392

Сравнительный анализ риска нарушения конфиденциальности при различных технологиях сетей связи ограниченных пользователей

Дурдиева Д.А., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Бельфер Р.А., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru

Введение.

В соответствии со ст. 12 Федерального закона «О связи» в группу сетей связи ограниченного пользователя входят выделенные, технологические, а также сети связи специального назначения [1]. *Технологические сети связи* предназначены для обеспечения производственной деятельности организаций, управления технологическими процессами. Примерами операторов таких статей являются сети связи железнодорожного транспорта «Трансгелеком ТТК», «ЕЭС Телеком», сеть «Газпром связь». Со стороны заказчиков сетей связи ОгП обычно предъявляются более высокие требования по качеству функционирования сетей, чем к сетям связи общего пользования. Это относится в первую очередь и к обеспечению информационной безопасности сетей связи.

Обеспечению информационной безопасности (ИБ) для отечественного потребителя таких сетей большое внимание уделяет организация «Российская корпорация средств связи» (РКСС). Об этом сообщает заместитель генерального директора этой организации, член Экспертного совета Комитета Государственной думы по безопасности А.Ю. Бадалов. Он относит предприятия топливно-энергетического комплекса, обслуживаемые технологическими сетями связи, к предприятиям критической инфраструктуры [2]. РКСС является первой в нашей стране организацией, которая специализируется на разработке и производстве доверенного телекоммуникационного оборудования. Большое внимание информационной безопасности таких сетей уделяют китайские ученые. Одними из примеров таких работ могут быть [3-5].

Задачей настоящей работы является сравнительный анализ риска угроз нарушения конфиденциальности данных и анализа трафика в сетях связи ОгП для различных технологий их построения.

В настоящей работе сравнительному анализу с точки зрения обеспечения ИБ подлежат следующие технологии транспортных частей сетей ОгП (и их конфигурации).

1. Сети коммутации пакетов (КП), построенные на основе физических адресов (не на виртуальных каналах);

2. Сети КП на основе логических адресов без установления виртуальных частных сетей:

- сети, построенные на базе постоянных виртуальных каналов;
- сети, построенные на базе коммутируемых виртуальных каналов;
- сети, построенные на базе комбинированных (постоянных и коммутируемых) виртуальных каналов.

3. Сети КП на основе логических адресов с установлением виртуальных частных сетей:

- сети, построенные на базе постоянных виртуальных каналов;
- сети, построенные на базе коммутируемых виртуальных каналов;
- сети, построенные на базе комбинированных (постоянных и коммутируемых) виртуальных каналов.

К сетям ОгП со стороны заказчика могут предъявляться требования по предоставлению не только служб передачи данных, но и или мультисервисных служб (передача данных, речь и др.).

Высокие требования заказчиков по ИБ и надежности могут относиться не только к службе передачи данных, но и к службе телефонии, т.е. мультимедийной технологии проектируемой сети связи ОгП. Данные требования могут быть причиной проектирования таких сетей с резервированием соединения оконечных пунктов с помощью пучка независимых маршрутов (узлам коммутации и каналам связи) и резервированием каналов связи. Поэтому в настоящей работе рассматриваются особенности шифрования данных в сети связи ОгП пакетной коммутации при резервировании соединений между оконечными пунктами.

1. Общие положения по обеспечению конфиденциальности данных в сетях связи

В настоящем разделе приведены общие положения по обеспечению шифрования в сетях связи пакетной коммутации.

В общем виде последовательность работы механизмов обеспечения ИБ следующая.

1. На этапе установления соединения должна быть предусмотрена аутентификация источника сообщений между взаимодействующими пунктами, оконечными пунктами установленного соединения, между центрами коммутации пакетов (ЦКП), а также на участках между ЦКП и подключенным к нему оконечным пунктом.

2. После успешного прохождения аутентификации выполняются функция обмена ключами по созданию общего главного секретного ключа (мастер-ключа) и передача его на противоположный оконечный пункт.

3. Создается защищенный канал SA (Security Association) между взаимодействующими пунктами.

4. После установления соединения должно быть обеспечено шифрование сообщений.

В зависимости от конкретных требований заказчика сетей ОгП эта последовательность этапов уточняется. Например, может отсутствовать этап создания защищенного канала.

2. Шифрование в сети связи пакетной коммутации

В настоящем разделе для приведенных выше технологий сетей связи изложим принципы организации шифрования сообщений.

На рис. 1 приведена архитектура сети пакетной коммутации, включающая четыре центра коммутации пакетов ЦКП. К трем из этих ЦКП подключены оконечные устройства a_1, a_2, a_3. Для обеспечения ИБ в такой сети требуется шифрование сообщений установления соединений и сообщений данных, целостность сообщений данных, аутентификация оконечных пунктов и ЦКП. Здесь приведена упрощенная схема без учета необходимого резервирования (горячего или с разделением нагрузки) соединений для выполнения требований надежности и возможных требований к мультимедийной технологии сети, обеспечивающей передачу данных, телефонию или видео.

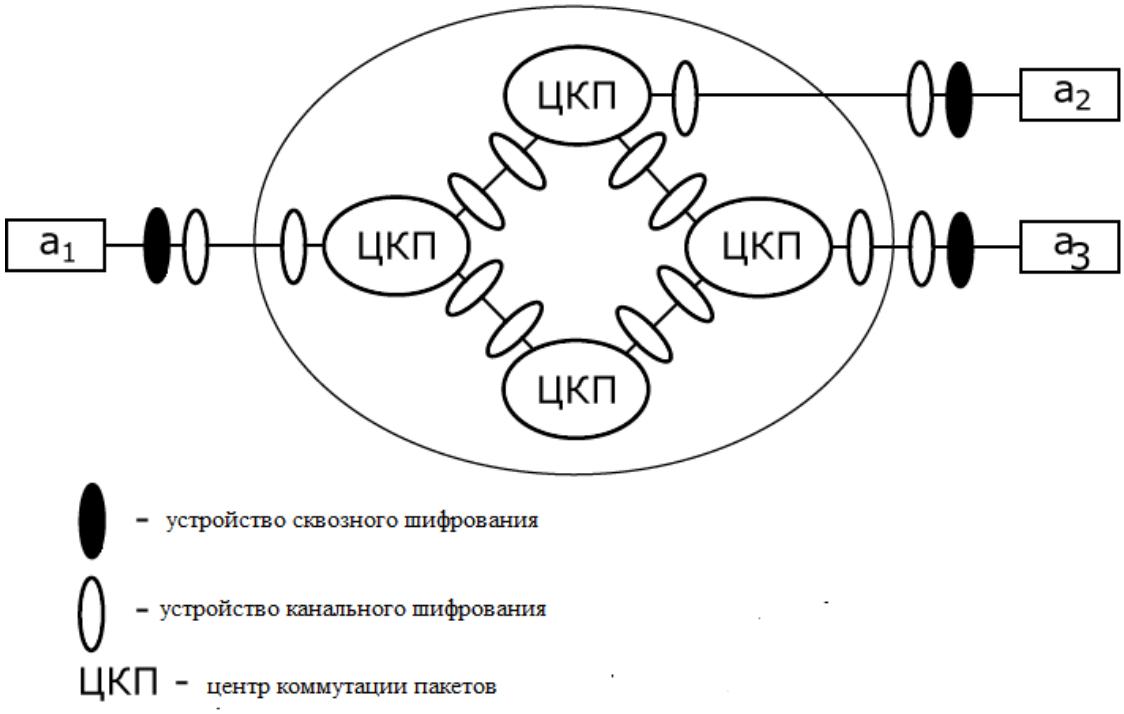


Рис. 1. Архитектура сети коммутации пакетов

В таких сетях предусмотрено два основных варианта обеспечения ИБ: канальное – между смежными устройствами сети и сквозное – между оконечными устройствами.

При канальном шифровании каждый уязвимый канал на сетевом уровне оборудуется устройствами аутентификации, целостности сообщений и шифрования на обоих концах. Таким образом, весь поток данных в канале оказывается защищенным. Недостатком канального шифрования является то, что сообщение должно расшифровываться каждый раз, проходя через коммутатор пакетов, поскольку коммутатор должен прочитать адрес в заголовке пакета, чтобы направить пакет по нужному направлению. Поэтому сообщение оказывается уязвимым в каждом коммутаторе.

При сквозном шифровании процесс шифрования выполняется на уровне выше третьего только в двух конечных станциях. Исходные данные шифруются в оконечном устройстве источника сообщений. Затем данные в шифрованном виде передаются без изменений через всю сеть получателю. Адресат использует тот же ключ, что и отправитель, и поэтому может дешифровать полученные данные. Эта схема кажется безопасной с точки зрения защиты от воздействий в канале связи или узлах коммутации пакетов. Однако и у такого

подхода есть слабое место.

Какую часть каждого пакета при сквозном шифровании должен шифровать

источник? Предположим, что шифрует весь пакет, включая заголовок. Но этого делать нельзя, так как выполнить расшифровку сможет только получатель. Промежуточный узел коммутации или распределитель сообщений (в сети без коммутации), получивший такой пакет, не сможет прочитать заголовок и поэтому не сумеет переслать пакет в соответствии с адресом. Отсюда следует, что отправитель должен шифровать только ту часть пакета, которая содержит данные пользователя, и оставить заголовок нетронутым.

Итак, при сквозном шифровании данные пользователя оказываются защищенными, чего нельзя сказать о самом потоке данных, поскольку заголовки пакетов передаются в открытом виде. Для некоторых сетей ОгП открытый адрес в сообщении может быть уязвимым местом для приводящей к большому ущербу атаки злоумышленника (передача в оконечный пункт нелегитимного сообщения, передача легитимного сообщения в непредназначенный для приема пункт назначения). Для некоторых сетей возможность несанкционированного изучения структуры потока по адресам проходящих пакетов также является угрозой информационной безопасности, которая называется “анализ трафика” [6]. Чтобы достичь более высокого уровня защищенности, необходима комбинация канального и сквозного шифрования, например, как показано на рис. 1, на котором приведена сеть коммутации пакетов с четырьмя центрами коммутации ЦКП. К трем из этих ЦКП подключены оконечные устройства a_1, a_2, a_3. Рассмотрим следующую ситуацию. Два оконечных устройства устанавливают соединение для передачи данных с использованием шифрования. Сообщения передаются пакетами, состоящими из заголовка и поля данных. Какую часть пакета должен шифровать оконечный пункт-источник сообщения?

При использовании обеих форм шифрования узел - источник шифрует на уровне выше сетевого пакет данных пользователя, используя ключ сквозного шифрования. Затем шифруется адресная часть пакета, используя ключи канального шифрования.

При движении пакета по сети каждый коммутатор сначала дешифрует адресную часть пакета с применением ключа шифрования соответствующего канала, а затем снова шифрует адресную часть пакета для передачи его по следующему каналу. Теперь весь пакет защищен почти все время – за исключением времени, когда он находится в памяти коммутатора пакетов, где адресная часть пакета оказывается открытым.

При использовании шифрования необходимо решать, что именно следует шифровать и на каком уровне эталонной модели OSI следует осуществлять защиту информации. На рис. 1 показано использование двух основных вариантов шифрования: канальное и сквозное шифрование.

Изложенный ниже в разделах 2.1-2.3 анализ и предложения по шифрованию данных в сети связи ОгП пакетной коммутации соответствуют конфигурации при отсутствии резервирования соединений между оконечными пунктами. Раздел 2.4 посвящен особенностям шифрования данных в сети связи ОгП пакетной коммутации при резервировании соединений между оконечными пунктами.

2.1. Сети КП на основе физических адресов

2.1.1. Шифрование между оконечными устройствами (сквозное шифрование)

В основу предлагаемого алгоритма аутентификации оконечных устройств предлагается использование сертификатов [7].

Возможно несколько методов создания общего главного секретного ключа между оконечными устройствами, которые сводятся к двум вариантам.

1. Метод ассиметричной криптографии. Для упрощения описание использования этого метода приводится на примере протокола RSA (реально должны быть использованы протоколы отечественных ГОСТов). Генерация осуществляется оконечным устройством, являющимся инициатором соединения с помощью виртуального канала. В данном примере им является оконечное устройство x. Этот ключ шифруется открытым ключом второго оконечного пункта (в данном случае оконечного пункта y) и передается от оконечного пункта x в оконечный пункт y.

2. Метод Диффи-Хеллмана. Оба оконечных пункта генерируют открытые ключи для алгоритма Диффи-Хеллмана. После обмена этими ключами каждое оконечное устройство устанавливаемого виртуального канала выполняет определенные вычисления по методу Диффи-Хеллмана. В результате каждое из этих устройств получает общий секретный ключ.

При создании защищенного канала должны договориться о применяемых протоколах шифрования, ключах шифрования сообщений, векторах инициализации, алгоритмах хеш-функций, а также о других параметрах (например, дата установления новых параметров данного соединения). Некоторые из этих параметров могут быть сгенерированы от главного секретного ключа (например, с использованием хеш-функций).

Шифрование полезного груза сообщений производится с помощью одного из выбранных на предыдущем этапе (разд. 4.1.1.3) механизмов криптографии.

2.1.2. Шифрование между смежными устройствами (канальное шифрование)

При канальном шифровании необходима взаимная аутентификация устройств коммутируемого канала:

- между оконечными устройствами и ЦКП, к которым они подключены;
- между двумя смежными ЦКП устанавливаемого виртуального канала.

Алгоритм взаимной аутентификации на участке оконечное устройство – ЦКП во многом аналогичен описанному выше алгоритму аутентификации при сквозном шифровании. В отличие от аутентификации на участке оконечное устройство – ЦКП аутентификация на участке между двумя смежными ЦКП может проводиться не при каждом установлении коммутируемого канала, а периодически (например, раз в сутки) при небольшой нагрузке в сети.

Создание общих главных секретных ключей между смежными устройствами и создание защищенного канала между ними также может проводиться не при каждом установлении соединения.

Шифрование адресной части заголовка сообщений или всего сообщения производится с помощью одного из выбранных с помощью защищенного канала протокола криптографии с общим ключом. Это шифрование необходимо как на этапе создания соединения, так и в процессе обмена сообщений по установленному соединению.

2.2. Сети КП на основе логических адресов без установления виртуальных частных сетей

Описание информационных процессов на сетевом уровне на примере сети КП на основе логических адресов без установления виртуальных частных сетей

передачи данных стандарта X.25 приводится в работе [8].

2.2.1. Шифрование между оконечными устройствами (сквозное шифрование)

Аутентификация оконечных устройств в сети КП на основе логических адресов без установления виртуальных частных сетей, создание защищенного канала между оконечными устройствами и установление параметров соединения, создание общего главного секретного ключа и шифрование сообщений на уровне выше сетевого между оконечными устройствами производится аналогично сети КП на основе физических адресов, приведенных выше в разделе 2.1.1. В некоторых случаях заказчик может не задавать требования на шифрование полезного груза после установления виртуального канала, поскольку в этих сообщениях отсутствуют физические адреса.

2.2.2. Шифрование между смежными устройствами (канальное шифрование)

Взаимная аутентификация устройств между оконечными устройствами, ЦКП и между смежными ЦКП устанавливаемого виртуального канала в сети КП на основе логических адресов без установления виртуальных частных сетей, создание защищенного

канала между оконечными устройствами и установление параметров соединения, создание общего главного секретного ключа и шифрование сообщений на уровне выше сетевого между оконечными устройствами производится аналогично сети КП на основе физических адресов, приведенных выше. В некоторых случаях заказчик может не задавать требования на шифрование полезного груза после установления виртуального канала, поскольку в этих сообщениях отсутствуют физические адреса.

Канальное шифрование осуществляется на этапе установления коммутируемого виртуального канала (КВК, SVC), при котором одновременно осуществляется аутентификация оконечных устройств. В обоих случаях необходимо шифровать/дешифровать физические адреса оконечных устройств виртуального канала. На этапе установления КВК эти адреса находятся в заголовке сообщений по установлению коммутируемого виртуального канала. В сети X.25 это физические адреса в пакетах «Запрос Вызова» и «Вызов Принят», выполняющие установление КВК. В сетях Frame Relay и ATM эти сообщения называются соответственно SETUP и CONNECT [8].

Поскольку адреса размещаются в нескольких байтах заголовка канальное шифрование можно осуществить либо с помощью криптографии с общим ключом либо с помощью криптографии с открытым ключом.

В последнем варианте шифрование осуществляется с помощью закрытого ключа отправителя, а дешифрование открытым ключом отправителя этих пакетов. Значения этих ключей определены на этапе аутентификации устройств при канальном шифровании, принципы которого изложены выше. В сетях Frame Relay и ATM логические адреса называются соответственно DLCI (Data Link Connection Identifier, идентификатор линий связи данных) и VPI (Virtual Path Identifier – идентификатор виртуального пути)/VCI (Virtual Channel, идентификатор виртуального канала) [8].

При установлении соединения с помощью постоянного виртуального канала (ПВК, PVC) между оконечными устройствами в зависимости от конкретных требований заказчика может отсутствовать необходимость в канальном шифровании. При установлении соединения с помощью коммутируемого постоянного виртуального канала (КПВК,SPVC) канальное шифрование осуществляется только между оконечными устройствами и ЦКП.

2.3. Сети КП на основе логических адресов с установлением виртуальных частных сетей

2.3.1. Виртуальная частная сеть КП на основе логических адресов

В настоящем разделе приведем описание виртуальной частной сети VPN,

построенной на сети КП с логическими номерами X.25 или Frame Relay (FR) [8]. В следующем разделе приводятся особенности шифрования VPN на базе сетей КП с логическими адресами. Виртуальная частная сеть в определенной степени воспроизводит свойства реальной частной сети, когда оборудование и каналы связи находятся в собственности владельца сети. VPN использует оборудование связи, которым владеет оператор публичной сети. Цель технологий VPN состоит в максимальной обособленности отдельных групп пользователей этой публичной сети. Технология VPN предназначена для выполнения двух задач. Одна из них заключается в обеспечении информационной безопасности в части защиты от несанкционированного доступа к пользователям такой виртуальной сетью. В качестве способов защиты от несанкционированного доступа понимается обеспечение конфиденциальности и целостности сообщений в сети, доступа к предоставляемым услугам связи и др. Другая задача VPN состоит в качестве обслуживания QoS пользователей связью. С помощью сети провайдера общего пользования может быть организовано много виртуальных частных сетей VPN, каждая из которых служит для определенной группы пользователей. Для построения VPN на базе сети FR используются постоянные виртуальные каналы ПВК, коммутируемые виртуальные каналы КВК или коммутируемого постоянного виртуального канала КПВК. Доступ предоставляется только к тем виртуальным каналам, которые зарезервированы для VPN.

2.3.2. Особенности шифрования в виртуальной частной сети КП на основе логических адресов

При установлении VPN с помощью постоянного виртуального канала ПВК коммутируемого виртуального канала КВК, коммутируемого постоянного канала КПВК может отсутствовать необходимость в канальном или сквозном шифровании. Это объясняется тем, что в этом случае при построении VPN выбираются специальные логические номера, что позволяет перемещаться пакетам данных по сети отдельно. Пакеты данных не могут попасть или быть доступны другим VPN. Незащищенным в отношении угроз перехвата данных остается участок соединения между пользователем и интерфейсом сети. В зависимости от требований заказчика здесь может потребоваться сквозное и/или канальное шифрование.

2.4. Особенности шифрования данных в сети связи ОгП пакетной коммутации при резервировании соединений между оконечными пунктами

Приведенный выше анализ и предложения по шифрованию данных в сети связи ОгП

пакетной коммутации соответствует конфигурации при отсутствии резервирования соединений между оконечными пунктами. Настоящий раздел посвящен анализу особенностей шифрования данных в сети связи ОгП пакетной коммутации при резервировании соединений между оконечными пунктами. При этом рассмотрению подлежат следующие два вида резервирования: передача одних и тех же данных по разным маршрутам между оконечными пунктами и распределение нагрузки по разным маршрутам между оконечными пунктами.

2.4.1. Пример резервирования соединения между оконечными пунктами в сети связи ОгП пакетной коммутации

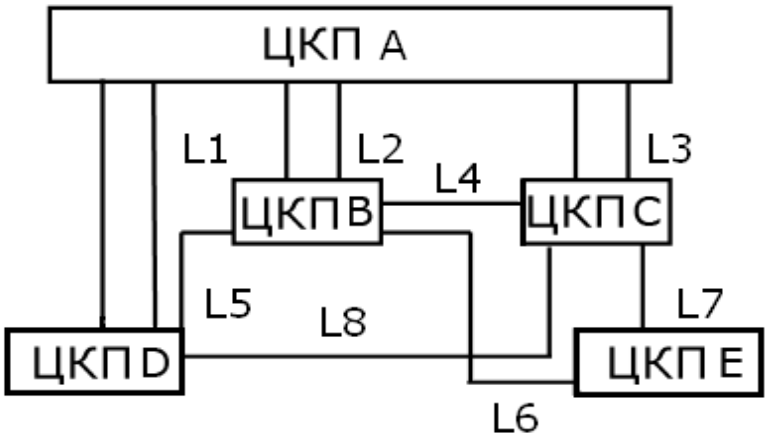


Рис. 2. Пример резервирования соединений между оконечными пунктами в сети связи ОгП пакетной коммутации

Как видно из рис. 2, пример структуры сети связи ОгП пакетной коммутации включает три ЦКП (ЦКП А, ЦКП Е, ЦКП D), два ЦКП (ЦКП В, ЦКП С) и пучки каналов связи (L1-L8). Некоторые из пучков каналов связи (L4-L8) состоят из одного канала, а остальные (L1-L3) из двух каналов связи (КС). В таблице маршрутизации введены следующие обозначения: Li, Lj: Li- нормальный пучок КС, Lj- резервный пучок КС; Li-Lj: разделение нагрузки между пучками КС Li и Lj. Каждая строка является таблицей маршрутизации для соответствующего пункта ЦКП (исходящего или транзитного).

Для примера приведем на основании таблицы маршрут сообщений подсистемы пользователя от ЦКП А в ЦКП Е в случае отсутствия отказов пучков КС.

1. Сообщения направляются с разделением нагрузки по пучкам КС L2 и L3 (см. строку таблицы маршрутизации для ЦКП А).
2. Сообщения из ЦКП В поступают на КС L6 и далее в КС Е.
3. Сообщения из ЦКП С поступают на КС L7 и далее в КС Е.

Таким образом, пучок маршрутов состоит из двух маршрутов, каждый из которых включает один транзитный пункт ЦКП:

1. ЦКП А-ЦКП В-ЦКП Е;
2. ЦКП А-ЦКП С-ЦКП Е.

В обратном направлении сообщения поступают по маршруту ЦКП Е-ЦКП С-ЦКП А.

При отказе каналов связи L3 и L6 пучок маршрутов состоит из одного резервного маршрута ЦКП А-ЦКП В-ЦКП С-ЦКП Е, который включает два транзитных пункта ЦКП через альтернативные каналы ЦКП второго приоритета. Обратный маршрут совпадает с прямым.

В некоторых случаях отказов КС для маршрутизации недостаточно только данных таблицы маршрутизации. В случае отказа L6, L7, L4 нет ни одного доступного маршрута сообщениям из ЦКП А в ЦКП Е. О недоступности ЦКП Е, ЦКП С и ЦКП В сообщают ЦКП А специальными сообщениями управления маршрутизацией. В таблице маршрутизации ЦКП А отмечается недоступность КС L2 и L3 по причине недоступности ЦКП Е.

Во время эксплуатации таких резервированных сетей пакетной коммутации требуется коррекция таблиц маршрутизации при неисправностях каналов связи, узлов коммутации, перегрузках. Это осуществляется с помощью специальных сообщений управления маршрутизацией. Необходима защита таких нелегитимных сообщений, отправляемых злоумышленником для нарушения функционирования сети.

2.4.2. Особенности шифрования в сети связи ОгП пакетной коммутации при отсутствии отказов в каналах связи

При отсутствии отказов в каналах связи канальное и сквозное шифрование производится по каждому маршруту пучка маршрутов между оконечными пунктами устанавливаемого соединения описанным выше методом. При наличии горячего резервирования каналов связи шифрование производится по основному каналу. При этом запоминаются все атрибуты шифрования для предоставления возможности перехода на резервный канал при неисправности основного. При резервировании каналов с помощью распределения нагрузки атрибуты шифрования устанавливаются, и шифрование производится по всем этим каналам.

4.4.3. Особенности шифрования в сети связи ОгП пакетной коммутации с учетом отказов каналов связи

Рассмотрению подлежит частный случай использования сети связи ОгП пакетной коммутации с установлением соединения на длительное время для выполнения технологических функций.

Особенность шифрования в такой сети связи ОгП пакетной коммутации с учетом отказов каналов связи заключается в ее уязвимости по отношению к злоумышленным атакам нарушения маршрутизации. При этом необходимо принимать меры защиты от нелегитимного управления сетью сигнализации по изменению таблицы маршрутизации в процессе эксплуатации - под предлогом изменения состояния каналов связи или узлов коммутации. Защита от такого рода угроз ИБ требует решать сложные задачи использования на эксплуатируемой сети механизмов аутентификации от атак DoS. О сложности такой задачи говорит тот факт, что по происшествии более 20 лет после разработки, по признанию разработчиков стандартов, эти задачи не удалось решить для ОКС№7. [Gerhard Rufa. Developments in Telecommunications. With a Focus on SS7 Network Reliability, Springer, 2008, P.283.]

2.5. Сравнительный анализ риска нарушения конфиденциальности при различных технологиях сетей связи ограниченных пользователей

Угрозы в сетях связи ОгП пакетной коммутации требуют применения метода оценки рисков ИБ на основе теории нечётких множеств. Этот математический аппарат позволяет определить количественные характеристики субъективным методом. В настоящей работе предложены модели анализа угроз на основе теории нечетких множеств для сетей связи ограниченных пользователей.

Основные этапы схемы нечеткого вывода представлены на рисунке 3 [9].

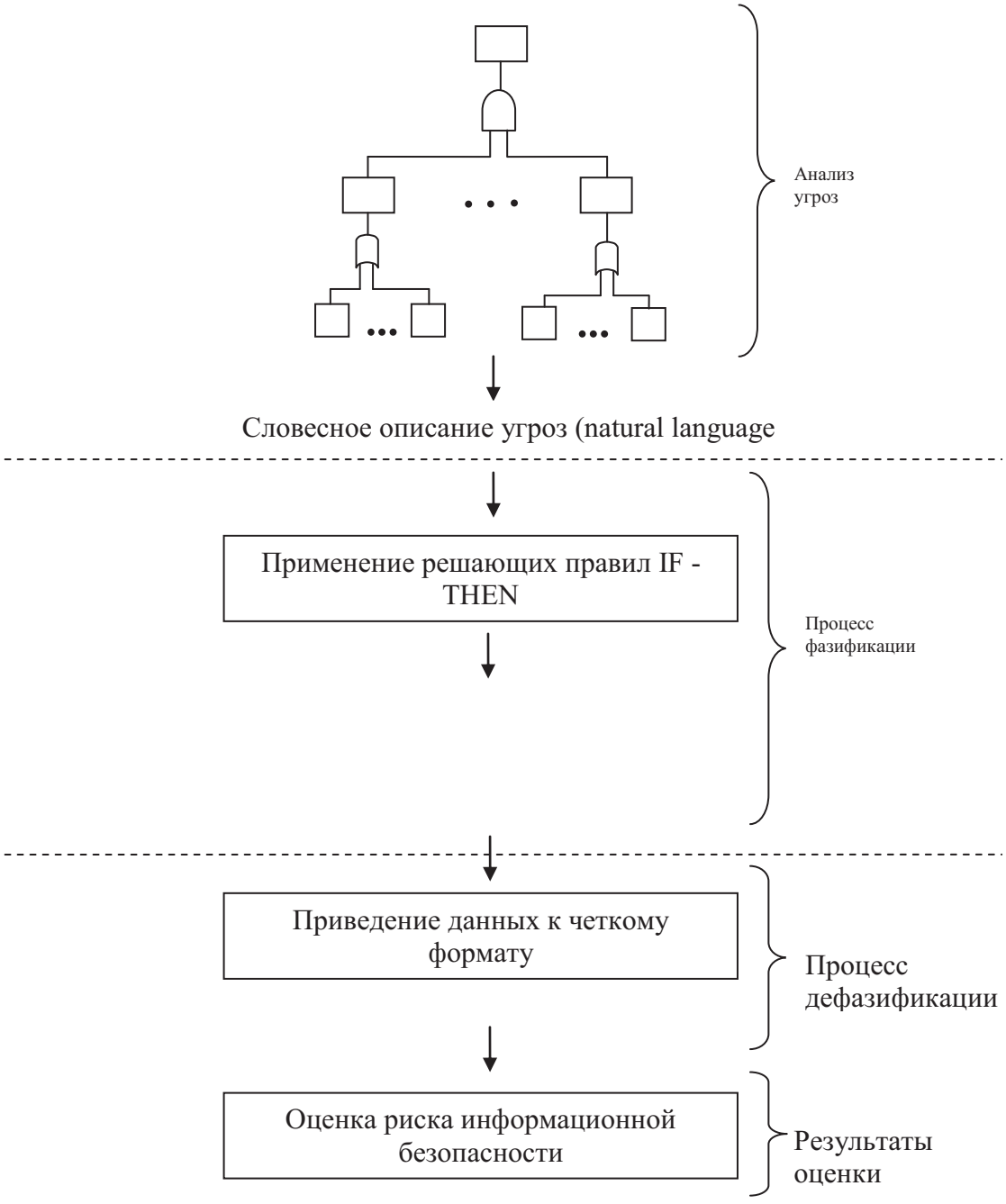
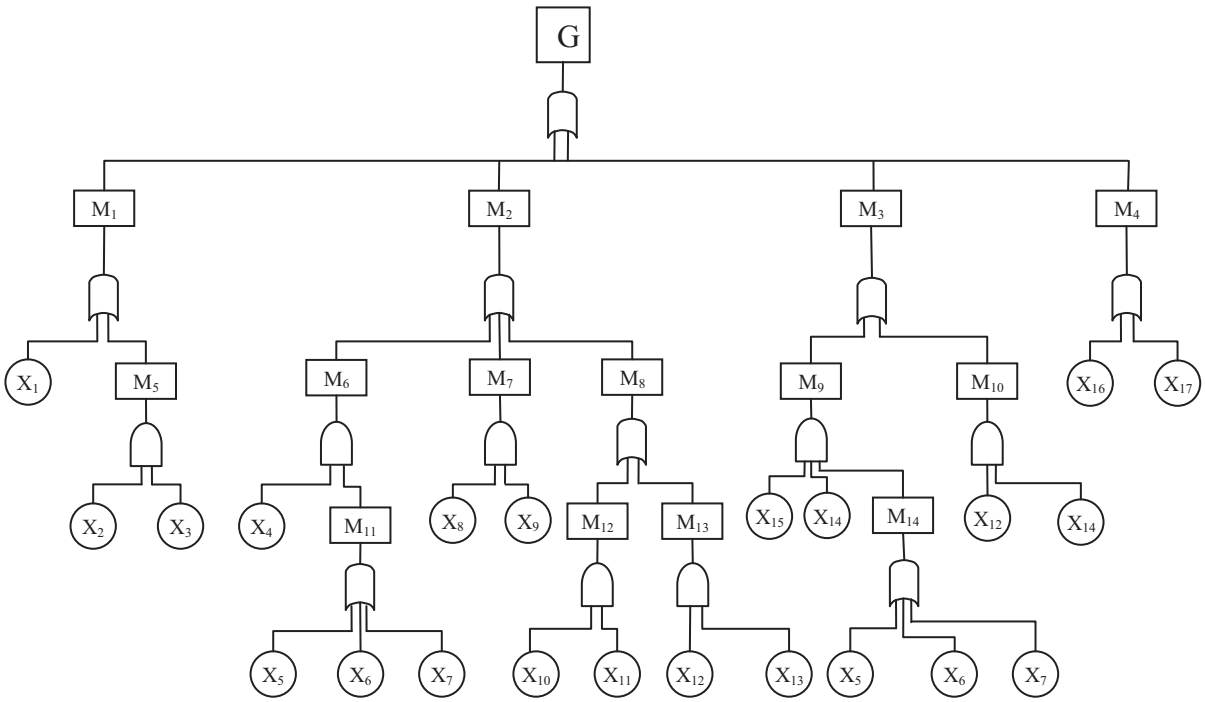


Рис. 3. Модель системы оценки риска на основе теории нечетких множеств

Важным этапом оценки риска информационной безопасности является анализ возможных угроз. В данной работе предлагается построение дерева угроз (attack tree). Вершина этого дерева – конечная цель нарушителя. После определения цели следует

анализ сети и выявление условий и событий, ведущих к реализации атаки. В соответствии с логическими связями между событиями, они могут быть соединены либо конъюнкцией, либо дизъюнкцией. Дизъюнкция используется в случае, если вышележащее событие реализуется, когда выполняется хотя бы одно из нижележащих условий. Соответственно конъюнкция используется, если для реализации вышележащего необходимо выполнение всех нижележащих событий.

Дерево атак для угрозы «Утечка приватной информации» [10] приведено на рисунке 4.



G – утечка приватной информации

M_1 – прямое воздействие

M_2 – прослушивание

M_3 – кража

M_4 – незаконное разглашение

M_5 – мошенничество

M_6 – прослушивание на физическом уровне

M_7 – прослушивание на MAC-уровне

M_8 – прослушивание на прикладном уровне

M_9 – физическая кража

M_{10} – кража с использованием вредоносного ПО

M_{11} – установка прослушивающего беспроводного устройства

M_{12} – подслушивание псевдонима

M_{13} – запуск прослушивающего ПО

M_{14} – кража автомобиля

X_1 – допрос

X_2 – поиск уязвимостей в механизме аутентификации

X_3 – подделка ID

X_4 – демонтаж устройства защиты от прослушивания

X_5 – сервис-провайдер автомобилей

X_6 – разрушение противоугонной системы автомобиля

X_7 – использование ошибок владельца

X_8 – анализ протокола взаимодействия на уязвимости

X_9 – сброс конфигурации

X_{10} – доступ к передатчику

X_{11} – анализ слабостей механизма присвоения псевдонимов

X_{12} – преодоления межсетевого экрана сети

X_{13} – знание слабостей механизмов защиты беспроводных сетей

X_{14} – дешифрование зашифрованных файлов

X_{15} – нарушение работы функции очищения памяти

X_{16} – получение данных от третьих лиц

X_{17} – утечка от официальных источников

Рис. 4. Дерево атак для реализации угрозы «Утечка приватной информации»

Сценарий атаки – это набор действий злоумышленника, которые привел к реализации его угрозы «Утечка приватной информации». Другими словами, $S_i = (X_{i1}, X_{i2}, \ldots, X_{in})$. В этом случае вероятность реализации конкретного сценария равна произведению входящих в него событий:

$$P(S_i) = P(X_1)*P(X_2)*...*P(X_n) \quad (1)$$

Применим правила булевой алгебры для получения всех возможных сценариев реализации рассмотренной атаки [10]:

$M_1 = X_1 \vee M_5 = X_1 \vee (X_2 \wedge X_3)$
$M_2 = M_6 \vee M_7 \vee M_8 = (X_4 \wedge M_{11}) \vee (X_8 \wedge X_9) \vee (M_{12} \vee M_{13}) = X_4 \wedge (X_5 \vee X_6 \vee X_7) \vee (X_8 \wedge X_9) \vee (X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13})$
$M_3 = M_9 \vee M_{10} = (X_{15} \wedge X_{14} \wedge M_{14}) \vee (X_{12} \vee X_{14}) = (X_{15} \wedge X_{14} \wedge (X_5 \vee X_6 \vee X_7)) \vee (X_{12} \wedge X_{14})$
$M_4 = X_{16} \vee X_{17}$
$G = M_1 \vee M_2 \vee M_3 \vee M_4 = X_1 \vee (X_2 \wedge X_3) \vee X_4 \wedge (X_5 \vee X_6 \vee X_7) \vee (X_8 \wedge X_9) \vee (X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13}) \vee (X_{15} \wedge X_{14} \wedge (X_5 \vee X_6 \vee X_7)) \vee (X_{12} \wedge X_{14}) \vee X_{16} \vee X_{17} = X_1 \vee X_2 \wedge X_3 \vee X_4 \wedge X_5 \vee X_4 \wedge X_6 \vee X_4 \wedge X_7 \vee X_8 \wedge X_9 \vee X_{10} \wedge X_{11} \vee X_{12} \wedge X_{13} \vee X_{15} \wedge X_{14} \wedge X_5 \vee X_{15} \wedge X_{14} \wedge X_6 \vee X_{15} \wedge X_{14} \wedge X_7 \vee X_{12} \vee X_{14} \vee X_{16} \vee X_{17}.$

Таким образом, были получены 14 различных сценариев реализации угрозы «Утечка приватной информации». Сценарии перечислены в таблице.

S_1	X_1	**S_8**	X_{12}, X_{13}
S_2	X_2, X_3	**S_9**	X_5, X_{14}, X_{15}
S_3	X_4, X_5	**S_{10}**	X_6, X_{14}, X_{15}
S_4	X_4, X_6	**S_{11}**	X_7, X_{14}, X_{15}
S_5	X_4, X_7	**S_{12}**	X_{12}, X_{14}
S_6	X_8, X_9	**S_{13}**	X_{16}
S_7	X_{10}, X_{11}	**S_{14}**	X_{17}

Выводы

Предложенная математическая модель позволяет произвести сравнительный анализ различных технологий построения сетей связи пакетной коммутации для категорий ограниченных пользователей (технологические и другие сети) по характеристике риска нарушения конфиденциальности в этих сетях.

Список литературы

1. Федеральный закон Российской Федерации №126-ФЗ от 7.07.2003 (редакция от 23.02.2011) «О связи».
2. А.Ю. Бадалов. Концепция доверенного оборудования как отражение воли рынка. – Электросвязь. – 2011. – № 8., с.3-5.
3. Hui-sheng Gao, Jing-xue Ran, Yi-qun Sun. Risk Evaluation of Communication Network of Electric Power Based on Restriction Coefficient Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference, p. 3127 – 3134.
4. Hui-sheng Gao (and others), Risk Evaluation of Communication Network of Electric Power Using logarithm Least, 7th World Congress on Intelligent Control and Automation, 2008, Chongqing, China. p. 5801-5806.
5. Hui-Sheng Gao; Jing-xue Ran; Yi-qun Sun Risk Evaluation of Communication Network of Electric Power Based on Improved FAHP, Fuzzy Systems and Knowledge Discovery, 2007. FSKD 2007. Fourth International Conference on Volume: 3, p. 653 - 659

6. Таненбаум Э. Д. Уэзеролл. Компьютерные сети, 5-е изд. СПБ.: Питер, 2012. 960с.
7. Бельфер Р.А. Сети и системы связи (технологии, безопасность): учебное пособие по дисциплине «Сети и системы связи»: электронное учебное издание. М.: ФГБОУ ВПО “ МГТУ им.Н.Э.Баумана, 2012, 738 с.
8. Бельфер Р.А. Сети и системы связи (технологии, безопасность): учебное пособие по дисциплине «Сети и системы связи»: электронное учебное издание: ФГБОУ ВПО “ МГТУ им. Н. Э. Баумана, 2012, 738 с.
9. Fakariah Hani Mohd Ali, Wan Mohd Nadzir Hadzril Wan Ismail. Network Security Threat Assessment Model Based on Fuzzy Algorithm, IEEE, no. 11, 2011.
10. Dandan.Ren, Suguo.Du, Haojin Zhu. A Novel Attack Tree Based Assessment Aproach for Location Privacy Preservation in the VANETs, IEEE ICC, no. 8, 2011.