АЛГОРИТМ УСТАНОВЛЕНИЯ ЗАЩИЩЕННОГО СОЕДИНЕНИЯ на абонентском доступе имитатора объединенной сети ПД специального назначения

М.Басараб, д.ф.-м.н., заведующий кафедрой

"Информационная безопасность" МГТУ им. Н.Э.Баумана,

Р.Бельфер, к.т.н., доцент кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана /
a.belfer@yandex.ru,

Е.Глинская, ст. преподаватель кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана,
А.Кравцов, начальник отдела НИИЦ (Москва) ЦНИИ ВВКО

УДК 621.392, DOI: 10.22184/2070-8963.2019.85.8.46.51

Рассматривается объединенная сеть, включающая несколько изолированных (частных) сетей передачи данных (ПД) специального назначения для разных ведомств. На гипотетической конфигурации имитатора сети ПД учебного лабораторного стенда кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана предложен алгоритм установления коммутируемых виртуальных каналов разных частных сетей. В алгоритме предусмотрено обеспечение надежности и информационной безопасности.

ВВЕДЕНИЕ

Настоящая статья является развитием работ [1, 2 и др.] по созданию имитатора объединенной сети ПД категории специального назначения, проводимых в рамках учебного лабораторного стенда УЛС на кафедре "Информационная безопасность" МГТУ им. Н.Э.Баумана совместно с Научно-исследовательским испытательным центром ЦНИИ Войск ВВКО МО РФ. В ФЗ "О связи" отмечено, что сети специального назначения предназначены для нужд органов

государственной власти, обороны страны, безопасности государства и обеспечения правопорядка. Под объединенной сетью понимается создание единой сети, включающей несколько изолированных (частных) сетей ПД специального назначения для разных ведомств из указанных в категории сетей специального назначения. Это соответствует резолюции IV конференции "Информационные технологии на службе оборонно-промышленного комплекса России-2015" [3] и предложению распространения

Рис.1. Конфигурация имитатора объединенной сети ПД с центром эксплуатации сети и единым удостоверяющим центром

объединения на сети специального назначения других ведомств [4]. В [1, 2] приводится, соответственно, алгоритм аутентификации и формирования разовых ключей в имитаторе объединенной сети, алгоритм формирования архитектуры очередей таблиц маршрутизации этого имитатора сети ПД категории специального назначения. В настоящей статье приводятся укрупненные алгоритмы установления на удаленном абонентском доступе двух соединений коммутируемых виртуальных каналов (КВК) разных частных сетей ПД объединенной сети категории специального назначения. Рассматривается только один из абонентских доступов соединения, включающий конечный пункт источника запроса на установление КВК. Составлению остальных алгоритмов установления КВК в объединенной сети будет посвящена другая статья в ближайших номерах журнала.

ОБЩИЕ ПОЛОЖЕНИЯ УСТАНОВЛЕНИЯ КВК В ИМИТАТОРЕ ОБЪЕДИНЕННОЙ СЕТИ ПД СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Приведенная на рис.1 конфигурация имитатора объединенной сети ПД в рамках учебного лабораторного стенда (УЛС) позволяет создавать пучок маршрутов между конечными пунктами, состоящий из четырех путей маршрутизации. Каждый путь маршрутизации включает три центра коммутации пакетов (ЦКП). К двум конечным

ЦКП в каждом пути маршрутизации (ЦКП 1.1, ЦКП 3.1 и ЦКП 1.2, ЦКП 3.2) подключены конечные пункты, а ЦКП 2.1 и ЦКП 2.2 являются транзитными. Доступ конечных пунктов (a, b, ..., c и d, e, ..., f) к центру коммутации пакетов удаленный.

Конфигурация имитатора сети ПД в УЛС предусматривает создание пучка маршрутов из четырех путей маршрутизации одного соединения между конечными пунктами. К двум граничным ЦКП абонентского доступа в каждом пути маршрутизации (ЦКП 1.1 – адрес 11, ЦКП 3.1 – адрес 31, ЦКП 1.2 – адрес 12, ЦКП 3.2 – адрес 32) подключены конечные пункты, а ЦКП 2.1 – адрес 21 и ЦКП 2.2 – адрес 22 являются транзитными (или транспортными). Имитатор сети ПД представляет объединение частных (изолированных) сетей, каждая из которых предназначена для определенных функций ОПК, МВД и некоторых других государственных ведомств.

Примем, что конечные пункты a (ОП_a) и f (ОП_f) принадлежат частной сети 1 (ЧС1); конечные пункты c (ОП_c) и e (ОП_e) принадлежат частной сети 2 (ЧС2), конечные пункты b (ОП_b) и d (ОП_d) принадлежат частной сети 3 (ЧС3). Присвоим конечным пунктам ЧС1 физические адреса от 1 до 999, ЧС2 – от 1001 до 1999, ЧС3 – от 2001 до 2999. Присвоим физический адрес 101 для ОП_a, 601 – для ОП_f, 1101 – для ОП_c, 1601 – для ОП_e, 2101 – для ОП_b, 2601 – для ОП_d.

В настоящей статье приводится описание укрупненных алгоритмов защищенного установления КВК в имитаторе объединенной сети на примере двух частных сетей ПД (частной сети 1 – ЧС1 и частной сети 3 – ЧС3). Допустим, что ЧС1 относится к одному роду войск МО, а ЧС3 – к другому. Приведем последовательность операций алгоритма защищенного установления двух КВК имитатора объединенной сети ПД: в ЧС1 – между оконечным пунктом а (ОП_а) и f (ОП_f), в ЧС3 – между оконечным пунктом b (ОП_b) и d (ОП_d).

Установлению КВК предшествует выполнение с определенной периодичностью предложенных в [1] алгоритмов: взаимная аутентификация на основе сертификатов Удостоверяющего Центра (УЦ) смежных ЦКП, оконечного пункта и ЦКП, аутентификация оконечного пункта и центра эксплуатации сети (ЦЭС); формирование ключей шифрования и обеспечения целостности сообщений.

Алгоритм установления КВК в частной сети состоит из трех последовательно выполняемых алгоритмов: на абонентском доступе оконечного пункта источника установления соединения (в настоящем примере – ОП_а и ОП_b); в транспортной части сети между смежными ЦКП; на абонентском доступе оконечного пункта назначения (в настоящем примере – ОП_f и ОП_d).

После успешного завершения выполнения процедур этих алгоритмов следует последовательное выполнение алгоритмов подтверждения установления соединения КВК: на абонентском доступе оконечного пункта назначения; в транспортной части сети между смежными ЦКП; на абонентском доступе оконечного пункта источника установления соединения. Принятое в статье обозначение АИД означает идентификатор устройств, физический адрес которого А. В ЦКП используется одна общая очередь свободных номеров для всех частных сетей, использующих этот ЦКП для установления соединения.

Примем исходное состояние очередей свободных номеров в ЦКП 1.1 и ЦКП 1.2 ЧС1 и ЧС3 имитатора объединенной сети (для упрощения описания алгоритмов очереди свободных номеров приняты одинаковыми). Тогда в ЧС1 – О_{1свн1112}: 809; 802; 805; 814; 815; 816; 817; 818; 819; 820; 821; 822; 823; 824; 825; 826; 827; 828; 804; 807... 801; 803. В ЧС3 – О_{3свн1112}: 2809; 2802; 2805; 2814; 2815; 2816; 2817; 2818; 2819; 2820; 2821, 2822, 2823; 2824; 2825; 2826; 2827; 2828; 2804; 2807... 2801; 2803.

АЛГОРИТМ УСТАНОВЛЕНИЯ КВК НА АБОНЕНТСКОМ ДОСТУПЕ ИСТОЧНИКА УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ

Первое: нужно согласовать алгоритмы канальной безопасности (шифрование, аутентификация и др.) между ОП_а (физический адрес 101) в ЧС1 и граничными ЦКП 1.1 и ЦКП 1.2 абонентского доступа (ассоциация безопасности Security Association, SA), в ЧС3 – между ОП_b (физический адрес 2101) и ЦКП 1.1 и ЦКП 1.2; снять стоящие первыми в приведенных выше очередях свободных номеров О_{1свн1112} ЧС1 и О_{3свн1112} ЧС3 – соответственно LCN = 809 и LCN = 2809. Затем назначить логический адрес LCN = 809 (Logical Channel Number) оконечному пункту источника соединения ОП_а КВК ЧС1 [1] и LCN = 2809 оконечному пункту источника соединения ОП_b КВК ЧС3. Откорректировать очереди и характеристики очередей О_{1свн1112} и О_{3свн1112} с целью использования при установлении этого и других КВК частных сетей.

Второе: в ОП_а, ОП_b, ЦКП 1.1 и ЦКП 1.2 создаются канальные ключи абонентских доступов, соответственно КВК ЧС1 и ЧС3, – $K_{101} = \text{hash}(K_a || 101\text{ИД})$, $K_{2101} = \text{hash}(K_b || 2101\text{ИД})$ – для шифрования/дешифрации на абонентском доступе сообщений установления соединения КВК, заголовков информационных сообщений установленного КВК [1]. Здесь K_a и K_b – сгенерированные ключи соответственно в ОП_а, ОП_b, переданные в граничные маршрутизаторы с помощью открытого и закрытого ключей этих маршрутизаторов. Зашифрованное в ЦКП 1.1 и ЦКП 1.2 ключом K_{101} сообщение согласованных алгоритмов канальной безопасности КВК ЧС1 (п.1) и LCN ОП_а отправить в ОП_а. Зашифрованное в ЦКП 1.1 и ЦКП 1.2 ключом K_{2101} сообщение согласованных алгоритмов канальной безопасности КВК ЧС3 (п.1) и LCN ОП_b отправить в ОП_b.

Третье: в ОП_а и ОП_b создаются разовые сквозные ключи соответственно КВК ЧС1 и ЧС3 $K_{\text{аинф1}}$, $K_{\text{аинф2}}$ и $K_{\text{бинф1}}$, $K_{\text{бинф2}}$ для шифрования/дешифрации в оконечном пользователе ОП_а и ОП_b информационной части передаваемого/принимаемого соответственно в прямом и обратном направлении пакета данных:

$K_{\text{аинф1}} = K_{1101601} = \text{hash}(K_a || 101\text{ИД} || 1)$; $K_{\text{аинф2}} = K_{2101601} = \text{hash}(K_a || 101\text{ИД} || 2)$,

$K_{\text{бинф1}} = K_{121012601} = \text{hash}(K_b || 2101\text{ИД} || 1)$; $K_{\text{бинф2}} = K_{21012601} = \text{hash}(K_b || 2101\text{ИД} || 2)$.

В ОП_а и ОП_b создаются разовые сквозные ключи $K_{\text{цаинф1}}$, $K_{\text{цаинф2}}$, $K_{\text{цбинф1}}$, $K_{\text{цбинф2}}$ для проведения контроля в оконечном пользователе целостности информационной части пакета

данных соответственно в прямом и обратном направлениях:

$K_{\text{Цаинф1}} = K_{3_{101601}} = \text{hash}(101\text{ИД} \parallel K_a \parallel 3)$; $K_{\text{Цаинф2}} = K_{4_{101601}} = \text{hash}(2101\text{ИД} \parallel K_a \parallel 4)$,

$K_{\text{Цбинф1}} = K_{3_{21012601}} = \text{hash}(2101\text{ИД} \parallel K_b \parallel 3)$; $K_{\text{Цбинф2}} = K_{4_{21012601}} = \text{hash}(2101\text{ИД} \parallel K_b \parallel 4)$.

Алгоритм защищенной доставки сквозных ключей на другой оконечный пункт КВК использует ЦЭС и приводится при описании алгоритма установления КВК.

Четвертое: нужно составить в ОП_а и ОП_б сообщения на установление соединения (УС); привести поля сообщения УС и ключи на примере только для ЧС1 (УС включает поля: тип (установление КВК), физический адрес оконечного пункта источника соединения (ОП_а), физический адрес оконечного пункта назначения f (в примере – 601)); зашифровать сообщение УС, сквозные ключи шифрования и целостности – $K_{1_{101601}}$, $K_{2_{101601}}$, $K_{3_{101601}}$, $K_{4_{101601}}$ канальным ключом K_{101} (передача всех этих зашифрованных сообщений в ЦКП 1.1 и ЦКП 1.2); дешифровать сообщение УС и сквозные ключи шифрования и контроля целостности $K_{1_{101601}}$, $K_{2_{101601}}$, $K_{3_{101601}}$, $K_{4_{101601}}$ канальным ключом K_{101} ; сформировать в ЦКП 1.1 и ЦКП 1.2 сообщения запроса цепочек маршрутизации (ЗЦМ), шифрование/дешифрация их при передаче в ЦЭС.

Пятый шаг: нужно составить в ЦКП 1.1 и ЦКП 1.2 два сообщения (для ЧС1 и ЧС3), запрос цепочек маршрутизации (ЗЦМ) – тип сообщения, физический адрес ЦКП абонентского доступа оконечного пункта источника установления КВК, физический адрес оконечного пункта абонентского доступа назначения установления КВК ОП_г и ОП_д, путь маршрутизации сообщений ЗЦМ в ЦЭС, дублированный путь маршрутизации сообщений ЗЦМ ЦКП 1.1 – ЦКП 2.1 – ЦЭС и ЦКП 1.2 – ЦКП 2.1 – ЦЭС. Затем передать в ЦКП 2.1 зашифрованное ЗЦМ ЧС1 и ЗЦМ ЧС3 в ЦКП 1.1 и ЦКП 1.2 соответственно канальными ключами $K_{1_{1121}}$ и $K_{3_{1121}}$, дешифровать эти сообщения в ЦКП 2.1 [1]. Алгоритм шифрования определяется ассоциацией безопасности.

Сообщения ЗЦМ ЧС1 и ЧС3 передаются в ЦЭС с использованием шифрования/дешифрации соответствующими канальными ключами $K_{1_{\text{ЦЭС}}}$ и $K_{3_{\text{ЦЭС}}}$ [1].

Шаг шестой: на основании полученных сообщений ЗЦМ в ЦЭС формируются сообщения цепочек маршрутизации (ЦМ) для КВК ЧС1 и ЧС3, включающие: тип сообщения; текущий номер устанавливаемого КВК; принадлежность КВК определенной частной сети; механизмы сквозного шифрования и контроля целостности

пакета данных устанавливаемого КВК; пути их маршрутизации в граничные маршрутизаторы ЦКП 1.1 и ЦКП 1.2, которые являются обратными путям маршрутизации сообщения ЗЦМ в ЦЭС; цепочки маршрутизации первого пути (11-21-31) и третьего пути (11-22-31) в ЦКП 1.1; цепочки маршрутизации второго пути (12-22-32) и четвертого пути (12-21-32). На каждом из участков между смежными ЦКП с помощью канальных ключей производится шифрование/дешифрация сообщений. Примем для упрощения одинаковыми цепочки маршрутизации всех четырех путей маршрутизации КВК ЧС1 и ЧС3.

Седьмой и восьмой шаги: из граничных маршрутизаторов ЦКП 1.1 и ЦКП 1.2 отправить в ОП_а и ОП_б полученные из ЦЭС механизмы сквозного шифрования и контроля целостности информации передаваемых пакетов данных после установления КВК ЧС1 и КВК ЧС3. В граничных маршрутизаторах ЦКП 1.1 и ЦКП 1.2 формируются два сообщения "Запрос вызова" (ЗВ) (для КВК ЧС1 и ЧС3), включающие соответствующие устанавливаемым КВК их текущие номера; физические адреса ОП_а и ОП_б; номера путей маршрутизации, полученные из ЦЭС цепочки физических адресов ЦКП каждого пути маршрутизации от ОП_а и ОП_б; номер частной сети; полученные из ЦЭС механизмы сквозного шифрования и контроля целостности информационной части передаваемых по установленным КВК ЧС1 и КВК ЧС3 пакетов данных, ключи сквозного шифрования и контроля целостности.

Наконец, это формирование в граничных маршрутизаторах ЦКП 1.1 и ЦКП 1.2 (на основании входящих значений в ЗВ) строк таблиц маршрутизации по логическим адресам КВК ЧС1 и КВК ЧС3. Эти строки создаются для каждого пути маршрутизации. В табл.1 приведены строки маршрутизации ЦКП 1.1 по логическим адресам КВК ЧС1 для первого и третьего пути маршрутизации, в табл.2 – строки ЦКП 1.2 второго и четвертого пути маршрутизации КВК ЧС1. В скобках этих таблиц приведены значения для КВК ЧС3.

Каждая приведенная таблица состоит из двух частей – для входящего сообщения в ЦКП и исходящего сообщения из этого ЦКП. Мы видим, что в верхней строке входящего в ЦКП сообщения таблицы маршрутизации каждого пути приведены следующие характеристики: адрес источника сообщения, поступившего в ЦКП 1.1 или ЦКП 1.2 (в примере – ОП_а с адресом 101 для КВК ЧС1 и ОП_б с адресом 2101 для КВК ЧС3); LCN этого сообщения (809 для КВК ЧС1 и 2809 для КВК ЧС3); производилось ли

Таблица 1. Маршрутизация КВК ЧС1 и ЧС3 по логическим адресам в ЦКП 1.1

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 1.1			Исходящее сообщение из ЦКП 1.1		
		Адр. источн. сообщ. в ЦКП 1.1	LCN	О _{свн}	Адрес поступл. сообщ. из ЦКП 1.1	LCN	О _{свн}
1	1	101(2101)	809 (2809)	Да	21	802 (2802)	Да
	1	21	802 (2802)	Да	101	809 (2809)	Да
	3	101(2101)	809 (2809)	Да	22	802 (2802)	Да
	3	22	802 (2802)	Да	101	809 (2809)	Да

назначение этого LCN в данном ЦКП (в данном случае – да). Это необходимо учесть в алгоритме разъединения КВК. В том случае, если это имело место, необходимо при разъединении это значение LCN установить в очередь свободных номеров.

В результате выполнения первого пункта данного алгоритма первые в очереди – О_{1свн1112} LCN=802 для КВК ЧС1 и О_{3свн1112} LCN = 2802 для КВК ЧС3. Если снять из О_{1свн1112} и О_{3свн1112}, соответственно LCN=802 и LCN=802, и запомнить их, то в результате О_{1свн1112}: 805; 814; 815; 816; 817; 818; 819; 820; 821; 822; 823; 824; 825; 826; 827; 828; 804; 807... 801; 803; О_{3свн1112}: 2805; 2814; 2815; 2816; 2817; 2818; 2819; 2820; 2821; 2822; 2823; 2824; 2825; 2826; 2827; 2828; 2804; 2807... 2801; 2803.

Теперь следует откорректировать очереди О_{1свн1112} и О_{3свн1112} и их характеристики. Для подготовки к передаче сообщения ЗВ от ЦКП абонентских доступов (в примере ЦКП 1.1 и ЦКП 1.2) в транзитные ЦКП 2.1 и ЦКП 2.2 нужно заменить в сообщении ЗВ КВК ЧС1 LCN = 809 на LCN = 802, а в ЗВ КВК ЧС3 LCN = 2809 на LCN = 2802.

В верхней строке исходящего из ЦКП сообщения таблицы маршрутизации каждого пути приведены следующие характеристики: адрес поступления из ЦКП сообщения (в зависимости от пути маршрутизации ЦКП 2.1 или ЦКП 2.2); LCN этого сообщения (802 для КВК ЧС1 и 2802 для КВК ЧС3); производилось ли назначение этого LCN в данном ЦКП (в данном случае – да).

Приведенные таблицы маршрутизации и последующие таблицы в остальных ЦКП имитатора объединенной сети ПД составляют при установлении КВК для маршрутизации в сети ПД по логическим адресам служебных сообщений (при подтверждении установления или разъединения КВК и др.), при передаче пакетов данных.

Верхние строки пути маршрутизации таблиц по логическим адресам обеспечивают передачу сообщений только в одном направлении – от оконечного пункта источника установления КВК во второй оконечный пункт (в примере от ОП_а в ОП_г КВК ЧС1, от ОП_б в ОП_д КВК ЧС3). Для передачи

Таблица 2. Маршрутизация КВК ЧС1 по логическим адресам в ЦКП 1.2

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 1.2			Исходящее сообщение из ЦКП 1.2		
		Адр. источн. сообщ. в ЦКП 1.2	LCN	О _{свн}	Адрес поступл. сообщ. из ЦКП 1.2	LCN	О _{свн}
1	2	101(2101)	809 (2809)	Да	22	802 (2802)	Да
	2	22	802 (2802)	Да	101	809 (2809)	Да
	4	101(2101)	809 (2809)	Да	21	802 (2802)	Да
	4	21	802 (2802)	Да	101	809 (2809)	Да

сообщений в противоположном направлении в таблицы маршрутизации для каждого пути вводится еще одна строка (нижняя). Как видно из таблиц, эта строка для другого направления составляется на основе верхней строки. Создание строк таблиц маршрутизации для передачи сообщений противоположного направления производится при установлении КВК во всех ЦКП сети ПД.

ЗАКЛЮЧЕНИЕ

Изложены общие положения установления КВК объединенной сети ПД категории специального назначения; разработан алгоритм установления КВК на одном из удаленных абонентских доступов в каждой из двух изолированных частей сетей ПД, входящих в объединенную сеть. В алгоритме предусмотрено обеспечение высоких требований по информационной безопасности и надежности. Составлению остальных алгоритмов установления КВК в имитаторе объединенной сети будет посвящена другая статья в ближайших номерах журнала. Эти работы являются составной частью подготовки студентов кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана к участию в создании

предприятиями страны отечественной объединенной сети ПД специального назначения.

ЛИТЕРАТУРА

1. Басараб М.А., Бельфер Р.А., Кравцов А.В., Никулина Т.П. Алгоритм аутентификации и формирования разовых ключей в имитаторе лабораторного стенда объединенной сети ПД специального назначения // ПЕРВАЯ МИЛЯ. 2019. № 2. С. 62–68.
2. Басараб М.А., Бельфер Р.А., Кравцов А.В. Архитектура очередей таблиц маршрутизации объединенной сети ПД категории специального назначения // Электросвязь. 2019. № 2. С. 33–37.
3. Резолюция конференции "Информационные технологии на службе оборонно-промышленного комплекса России 2015" // Connect. 2015. № 9. С. 78–88.
4. Матвеев В.А., Басараб М.А., Бельфер Р.А., Кравцов А.В., Мерзляков Д.И. Алгоритм функционирования УЛС защищенной сети ПД на базе виртуальных каналов с высокими требованиями к качеству обслуживания // "Электросвязь". 2017. № 8. С. 57–62.

АПК «Безопасный город»

ИСКРАУРАЛТЕЛ

Решения для автоматизации РСЧС

- Единый центр оперативного реагирования;
- Система 112;
- Комплекс средств оповещения;
- Портал взаимодействия городских служб и населения;
- Система диспетчеризации;
- eCall/ГЛОНАСС.

www.iskrauraltel.ru