АЛГОРИТМ БЕЗОПАСНОГО УСТАНОВЛЕНИЯ/ РАЗЪЕДИНЕНИЯ СОЕДИНЕНИЯ на транспортном участке объединенной сети ПД спецназначения

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 / glinskaya-ju8@rambler.ru,

А.Кравцов, начальник отдела НИИЦ (Москва) ЦНИИ ВКС / skyak78@gmail.com

УДК 621.392, DOI: 10.22184/2070-8963.2020.87.2.62.68

Рассматривается объединенная сеть, включающая несколько изолированных (частных) сетей передачи данных специального назначения для разных ведомств. На примере двух частных сетей имитатора сети передачи данных учебного лабораторного стенда кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана предлагаются следующие алгоритмы: установление в транспортной части сети коммутируемого виртуального канала, разъединение соединения. Решения предусматривают обеспечение надежности и информационной безопасности.

ВВЕДЕНИЕ

Разработке алгоритма защищенного соединения в имитаторе объединенной сети ПД специального назначения была посвящена статья [1]. В ней говорилось об установлении соединения только на абонентском доступе, включающем окончательный пункт источника запроса на установление коммутируемых виртуальных каналов (КВК). Сейчас

речь пойдет об алгоритмах функций завершения установления двух соединений КВК разных частных сетей передачи данных (ПД) объединенной сети категории специального назначения. Это относится к установлению КВК в транспортной части сети между смежными центрами коммутации пакетов (ЦКП) и на абонентском доступе окончательного пункта назначения. После успешного

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

завершения этих процедур выполняются алгоритмы подтверждения – установления соединения КВК.

На рис.1 показана конфигурация имитатора объединенной сети ПД, краткое описание которой дано в [1]. В табл.1, 2 приведены сформированные в этой работе в ЦКП 1.1 и ЦКП 1.2 таблицы маршрутизации по логическим адресам КВК частной сети 1 (ЧС1) и КВК ЧС3 (в скобках).

Исходное состояние очередей свободных номеров в ЦКП 2.1, ЦКП 2.2, ЦКП 3.1, ЦКП 3.2 имитатора сети (для упрощения описания алгоритмов

очереди свободных номеров в ЦКП 2.1 и ЦКП 2.2, в ЦКП 3.1 и ЦКП 3.2 приняты одинаковыми):

- в ЦКП 2.1 и ЦКП 2.2. ЧС1. $O_{1\text{свн}2122}$: 924; 922; 905; 921; 927; 919; 918; 929; 953; 930; 941, 942, 923; 925; 926; 947; 948; 904; 907... 901; 903; ЧС3. $O_{3\text{свн}2122}$: 2924; 2922; 2905; 2921; 2927; 2919; 2918; 2929; 2953; 2930; 2941, 2942, 2923; 2924; 2925; 2926; 2947; 2948; 2904; 2907... 2901; 2903;
- в ЦКП 3.1 и ЦКП 3.2. ЧС1. $O_{1\text{свн}3132}$: 714; 722; 715; 720; 717; 719; 727; 728; 729; 730; 731; 732; 733; 734; 709... 701; 703; ЧС3. $O_{3\text{свн}3132}$: 2714; 2722; 2715; 2720; 2717; 2719;

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		
		Адрес источн. сообщ. в ЦКП 1.1	LCN	$O_{\text{свн}}$	Адрес поступлен. сообщ. из ЦКП 1.1	LCN	$O_{\text{свн}}$
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

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		
		Адрес источн. сообщ. в ЦКП 1.2	LCN	О _{свн}	Адрес поступлен. 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

2718; 2723; 2724; 2726; 2727; 2728; 2729; 2730; 2731; 2732; 2733; 2734; 2709... 2701; 2703.

А. АЛГОРИТМ УСТАНОВЛЕНИЯ КВК В ТРАНСПОРТНОЙ ЧАСТИ СЕТИ МЕЖДУ СМЕЖНЫМИ ЦКП

Первое: следует зашифровать канальным ключом K_{1121} (между смежными ЦКП имитатора ЦКП 1.1 и ЦКП 2.1) сообщение "Запрос вызова" (ЗВ) коммутируемого виртуального канала (КВК) частной сети 1 (ЧС1), канальным ключом K_{3121} – сообщение ЗВ КВК частной сети 3 (ЧС3) первого пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA (Security Association) соответственно ЧС1 и ЧС3) между ЦКП 1.1 (адрес 11) и ЦКП 2.1 (адрес 21). В ЦКП 2.1 этими ключами дешифруется ЗВ, принятый от ЦКП 1.1. Алгоритм создания канального ключа (для каждой частной сети) между смежными ЦКП в имитаторе сети ПД приведен в [2]. Согласование канальных механизмов обеспечения информационной безопасности между смежными ЦКП в имитаторе сети выполняется не с каждым установлением соединения, а периодически по команде из центра эксплуатации сети (ЦЭС).

Затем нужно зашифровать канальным ключом K_{1122} между смежными ЦКП имитатора ЦКП 1.1 и ЦКП 2.2 (адрес 22) сообщение ЗВ КВК ЧС1, канальным ключом K_{3122} – сообщение ЗВ КВК ЧС3 третьего пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 1.1 и ЦКП 2.2. В ЦКП 2.2 производится дешифрация ЗВ этими ключами. В зависимости от требований к информационной безопасности ЧС1 и ЧС3 в

результате этих процедур между одними и теми же смежными ЦКП могут быть приняты разные алгоритмы ИБ.

Зашифровать канальным ключом K_{1122} сообщение ЗВ КВК ЧС1, канальным ключом K_{3122} – сообщение ЗВ КВК ЧС3 второго пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 1.2 (адрес 12) и ЦКП 2.2. В ЦКП 2.2 этими ключами дешифруется ЗВ.

Зашифровать канальным ключом K_{1121} сообщение ЗВ КВК ЧС1, канальным ключом K_{3121} – сообщение ЗВ КВК ЧС3 четвертого пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 1.2 и ЦКП 2.1. В ЦКП 2.1 этими ключами дешифруется ЗВ.

Второе: в маршрутизаторах ЦКП 2.1 и ЦКП 2.2 (на основании входящих значений в ЗВ) следует сформировать строки таблиц маршрутизации по логическим адресам КВК ЧС1 и КВК ЧС3. Строки создаются для каждого пути маршрутизации. В табл.3 приведены строки таблицы маршрутизации ЦКП 2.1 по логическим адресам КВК ЧС1 для первого и четвертого пути маршрутизации, в табл.4 – строки таблицы ЦКП 2.2 второго и третьего пути маршрутизации КВК ЧС1. В скобках табл.3 указаны строки таблицы маршрутизации ЦКП 2.1 по логическим адресам КВК ЧС3 для первого и четвертого пути маршрутизации, в скобках табл.4 – строки таблицы ЦКП 2.2 второго и третьего пути маршрутизации КВК ЧС3.

В приведенных табл.3 и 4 установлены значения LCN из ЗВ. В верхней строке таблицы для входящего сообщения в ЦКП 2.1 и ЦКП 2.2 LCN = 802 для

Таблица 3. Маршрутизация КВК ЧС1 и ЧС3 по логическим адресам в ЦКП 2.1

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 2.1			Исходящее сообщение из ЦКП 2.1		
		Адрес источн. сообщ. в ЦКП 2.1	LCN	О _{свн}	Адрес поступлен. сообщ. из ЦКП 2.1	LCN	О _{свн}
1	1	11	802 (2802)	Нет	31	924 (2924)	Да
	1	31	924 (2924)	Да	11	802 (2802)	Нет
	4	12	802 (2802)	Нет	32	924 (2924)	Да
	4	32	924 (2924)	Да	12	802 (2802)	Нет

КВК ЧС1 и LCN = 2802 для КВК ЧС3. Для подготовки к передаче сообщения ЗВ от транзитных ЦКП 2.1 и ЦКП 2.2 в ЦКП 3.1 (адрес 31) и ЦКП 3.2 (адрес 32) абонентских доступов окончных пунктов назначения следует заменить в сообщении ЗВ КВК ЧС1 LCN = 802 на LCN = 924, стоящий первым в приведенном выше О_{1свн2122}, а в ЗВ КВК ЧС3 LCN = 2802 на LCN = 2924, стоящий первым в указанном выше О_{3свн2122}. Откорректировать очереди О_{1свн2122}, О_{3свн2122} и их характеристики. В верхней строке таблицы для исходящего сообщения из ЦКП 2.1 и ЦКП 2.2 LCN = 2802 для КВК ЧС3.

Третье: зашифровать канальным ключом К1₂₂₃₁ сообщение ЗВ КВК ЧС1, канальным ключом К3₂₁₃₁ – сообщение ЗВ КВК ЧС3 первого пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между

ЦКП 2.1 и ЦКП 3.1. В ЦКП 3.1 этими ключами производится дешифрация ЗВ, принятого от ЦКП 2.1. Запомнить установленные в ЗВ КВК ЧС1 и ЧС3 соответствующие логические адреса LCN = 924 и LCN = 2924.

Канальным ключом К1₂₂₃₁ зашифровать сообщение ЗВ КВК ЧС1, канальным ключом К3₂₂₃₁ – сообщение ЗВ КВК ЧС3 третьего пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 2.2 и ЦКП 3.1. В ЦКП 3.1 этими ключами дешифруется ЗВ.

Зашифровать канальным ключом К1₂₂₃₂ сообщение ЗВ КВК ЧС1, канальным ключом К3₂₂₃₂ – сообщение ЗВ КВК ЧС3 второго пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 2.2 и ЦКП 3.2.

Таблица 4. Маршрутизация КВК ЧС1 и ЧС3 по логическим адресам в ЦКП 2.2

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 2.2			Исходящее сообщение из ЦКП 2.2		
		Адрес источн. сообщ. в ЦКП 2.2	LCN	О _{свн}	Адрес поступлен. сообщ. из ЦКП 2.2	LCN	О _{свн}
1	2	12	802 (2802)	Нет	32	924 (2924)	Да
	2	32	924 (2924)	Да	12	802 (2802)	Нет
	3	11	802 (2802)	Нет	31	924 (2924)	Нет
	3	31	924 (2924)	Да	11	802 (2802)	Да

Таблица 5. Маршрутизация КВК ЧС1 и ЧС3 по логическим адресам в ЦКП 3.1

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 3.1			Исходящее сообщение из ЦКП 3.1		
		Адрес источн. сообщ. в ЦКП 3.1	LCN	О _{свн}	Адрес поступлен. сообщ. из ЦКП 3.1	LCN	О _{свн}
1	1	21	924 (2924)	Нет	601 (2601)	714 (2714)	Да
	1	601 (2601)	714 (2714)	Да	21	924 (2924)	Нет
	3	22	924 (2924)	Нет	601 (2601)	714 (2714)	Да
	3	601 (2601)	714 (2714)	Да	12	924 (2924)	Нет

В ЦКП 3.2 этими ключами выполняется дешифрация ЗВ.

Канальным ключом K_{12132} зашифровать сообщение ЗВ КВК ЧС1, канальным ключом K_{32132} – сообщение ЗВ КВК ЧС3 четвертого пути КВК согласованными алгоритмами шифрования (полученными с помощью процедур Ассоциации безопасности SA соответственно ЧС1 и ЧС3) между ЦКП 2.1 и ЦКП 3.2. В ЦКП 3.2 этими ключами дешифруется ЗВ.

Б. Алгоритм установления КВК на абонентском доступе оконечного пункта назначения

Первое: необходимо согласовать алгоритмы канальной безопасности (шифрования, аутентификации и др.) между ОП_ф (физический адрес 601) в ЧС1 и граничными ЦКП 3.1, ЦКП 3.2 абонентского доступа; в ЧС3 – между ОП_д (физический адрес 2601) и ЦКП 3.1, ЦКП 3.2. Снять стоящие первыми в приведенных выше очередях свободных номеров $O_{1свн3132}$ ЧС1 и $O_{3свн3132}$ ЧС3 соответственно LCN = 714 и LCN = 2714. Назначить логический адрес LCN = 714 ОП_ф КВК ЧС1, LCN = 2714 ОП_д КВК ЧС3. Заменить в ЦКП 3.1 и ЦКП 3.2 ЗВ КВК ЧС1 LCN = 924 на LCN = 714 и ЗВ КВК ЧС3 LCN = 2924 на LCN = 2714. Откорректировать очереди и их характеристики $O_{1свн3132}$ и $O_{3свн3132}$ для использования при установлении других КВК этих частных сетей.

Второе: в ОП_ф, ОП_д, ЦКП 3.1 и ЦКП 3.2 следует создать канальные ключи абонентских доступов соответственно КВК ЧС1 $K_{601} = \text{hash}(K_f \parallel 601\text{ИД})$ и ЧС3 $K_{2601} = \text{hash}(K_d \parallel 2601\text{ИД})$ для шифрования/дешифрации на абонентском доступе сообщений установления соединения КВК, заголовков информационных сообщений установленного КВК. Здесь

K_f и K_d – это сгенерированные ключи соответственно в ОП_ф, ОП_д и переданные в граничные маршрутизаторы ЦКП 3.1 и ЦКП 3.2 с помощью открытого и закрытого ключей этих маршрутизаторов. Зашифрованные в ЦКП 3.1 и ЦКП 3.2 ключом K_{601} сообщения ЗВ четырех путей маршрутизации КВК ЧС1 нужно отправить в ОП_ф. Зашифрованные в ЦКП 3.1 и ЦКП 3.2 ключом K_{2601} сообщения ЗВ четырех путей маршрутизации КВК ЧС3 следует отправить в ОП_д. Дешифруются эти ЗВ соответствующими ключами K_{601} и K_{2601} . В результате при отсутствии помех в каналах получаем расшифрованные в ОП_ф (ЧС1) LCN = 714, механизмы и ключи сквозного шифрования и контроля целостности информационной части пакетов данных. В ОП_д (ЧС3) получаем LCN = 2714, механизмы и ключи сквозного шифрования, контроля целостности информационной части пакетов данных.

Третье: в маршрутизаторах ЦКП 3.1 и ЦКП 3.2 необходимо сформировать строки таблиц маршрутизации по логическим адресам КВК ЧС1 и КВК ЧС3. В табл.5 приведены строки таблицы маршрутизации ЦКП 3.1 по логическим адресам КВК ЧС3 для первого и третьего пути маршрутизации, в табл.6 – строки таблицы ЦКП 3.2 второго и четвертого пути маршрутизации КВК ЧС3.

Как видно из табл.5 и 6, все входящие значения получены из сообщений ЗВ. Логические адреса LCN в верхней строке таблиц каждого пути маршрутизации КВК во входящих сообщениях в ЦКП 3.1 и ЦКП 3.2 устанавливаются из дешифрованных ЗС, полученных из ЦКП 2.1 и ЦКП 2.2 (пункт третий раздела А). Логические адреса LCN в верхней строке таблиц каждого пути маршрутизации КВК в исходящих сообщениях из ЦКП 3.1 и

Таблица 6. Маршрутизация подсети КВК ЧС1 и ЧС3 по логическим адресам в ЦКП 3.2

Номер КВК	Номер пути маршрутизации	Входящее сообщение в ЦКП 3.2			Исходящее сообщение из ЦКП 3.2		
		Адрес источн. сообщ. в ЦКП 3.2	LCN	О _{свн}	Адрес поступлен. сообщ. из ЦКП 3.2	LCN	О _{свн}
1	2	22	924 (2924)	Нет	601 (2601)	714 (2714)	Да
	2	601 (2601)	714 (2714)	Да	22	924 (2924)	Нет
	4	21	924 (2924)	Нет	601 (2601)	714 (2714)	Да
	4	601 (2601)	714 (2714)	Да	21	924 (2924)	Нет

ЦКП 3.2 устанавливаются из дешифрованных ЗС, полученных в этих ЦКП (пункт первый раздела Б).

В. АЛГОРИТМ ПОДТВЕРЖДЕНИЯ УСТАНОВЛЕНИЯ КВК

Алгоритм подтверждения установления КВК выполняется путем передачи по сети сообщений "Вызов принят" (ВП) по всем четырем путям маршрутизации от оконечного пункта назначения установления КВК в оконечный пункт источника установления соединения КВК. Для подтверждения установления КВК ЧС1 ВП передается в ЧС1 от ОП_ф в ОП_а, в ЧС3 – от ОП_д в ОП_б. Формат сообщений ВП состоит из трех полей: тип сообщения, логический адрес LCN, номер пути маршрутизации. Коммутация ВП производится по нижней строке таблиц маршрутизации логических адресов (табл.1–6). На абонентских доступах и в транспортной части имитатора сети ПД сообщение ВП подлежит шифрованию/дешифрации теми же канальными ключами и механизмами, что и при передаче сообщения ЗВ.

Поступление ВП с LCN = 809 в ОП_а, совпадающем с LCN в этом ОП, означает подтверждение установления КВК в ЧС1. Поступление ВП с LCN = 2809 в ОП_б, совпадающем с LCN в этом ОП, указывает на установление КВК в ЧС3.

Г. АЛГОРИТМ РАЗЪЕДИНЕНИЯ КВК

Приведем алгоритм разъединения установленных КВК в ЧС1 и ЧС3. Источником разъединения примем оконечный пункт ОП_ф. Будем считать, что отказы в каналах отсутствуют.

Шаг 1. Составить в ОП_ф сообщение "Запрос разъединения" (ЗР), в которое входят следующие поля:

тип сообщения М = 4, номер пути маршрутизации, LCN = 714 оконечного пункта. Разъединение КВК осуществляется путем передачи по всем путям маршрутизации сети ПД защищенного сообщения ЗР от оконечного пункта инициатора разъединения в другой оконечный пункт соединения. Шифрование/дешифрация сообщения ЗР производится теми же канальными ключами и механизмами, которые использовались при установлении КВК и передаче пакетов данных. Коммутация сообщений ЗР на участках абонентских доступов и в транспортной сети выполняется по нижним строкам таблиц маршрутизации логических адресов (табл.1–6).

Шаг 2. Зашифровать ЗР ЧС1 ключом К₆₀₁, ЗР ЧС2 ключом К₂₆₀₁ оконечного пункта ОП_ф и отправить в ЦКП 3.1 и ЦКП 3.2 по всем четырем путям маршрутизации КВК: по первому и третьему пути по адресу 31, по второму и четвертому – по адресу 32.

Шаг 3. Дешифровать ЗР ключом К₆₀₁. Сменить в сообщении ЗР ЧС1 логический номер LCN = 714 на LCN = 924, в сообщении ЗР ЧС3 – логический номер LCN = 2714 на LCN = 2924 (согласно табл.5 и 6), предварительно установив в ЦКП 3.1 и ЦКП 3.2 LCN = 714 в конец очереди свободных номеров О_{1свн3132}, а LCN = 2714 – в конец очереди свободных номеров О_{3свн3132}.

В результате в ЦКП 3.1 и ЦКП 3.2 очередь ЧС1 О_{1свн3132}: 722; 715; 720; 717; 719; 718; 723; 724; 726; 727; 728; 729; 730; 731; 732; 733; 734; 709; 703, 714. Затем следует откорректировать характеристику очереди О_{1свн3132} и по аналогии очередь ЧС3 О_{3свн3132}.

Шаг 4. Зашифровать сообщения ЗР ЧС1 с LCN = 924 всех четырех путей маршрутизации соответствующими

канальными ключами (K_{12131} , K_{12231} , K_{12232} , K_{12132}), а сообщения ЗР ЧСЗ – канальными ключами (K_{32131} , K_{32231} , K_{32232} , K_{32132}). Используются те же канальные ключи, что и при установлении КВК (шаг 3).

Шаг 5. В соответствии с табл.5, 6 отправить сообщение ЗР в транзитные ЦКП 2.1 и ЦКП 2.2 по всем четырем путям маршрутизации.

Шаг 6. Стереть все строки таблиц маршрутизации (табл.5 в ЦКП 3.1 и табл.6 в ЦКП 3.2) сбрасываемых КВК ЧС1 и ЧСЗ.

Шаг 7. Дешифровать соответствующими канальными ключами ЧС1 (K_{12131} , K_{12231} , K_{12232} , K_{12132}) и ЧСЗ (K_{32131} , K_{32231} , K_{32232} , K_{32132}) принятые ЗР в ЦКП 2.1 и ЦКП 2.2 по четырем путям маршрутизации сообщений. Сменить в сообщении ЗР ЧС1 логический номер LCN = 924 на LCN = 802, а в сообщении ЗР ЧСЗ – логический номер LCN = 2924 на LCN = 2802 (согласно табл.3 и 4), предварительно установив LCN = 924 ЗР ЧС1 в конец очереди свободных $O_{1свн2122}$ в ЦКП 2.1 и ЦКП 2.2.

В результате в ЦКП 2.1 и ЦКП 2.2 $O_{свн2122}$: 922; 905; 921; 927; 919; 918; 929; 953; 930; 941; 942; 923; 925; 926; 947; 948; 904; 907; 924. Откорректировать характеристику очереди $O_{свн2122}$ и аналогично очередь ЧСЗ $O_{3свн3132}$.

Шаг 8. Зашифровать сообщения ЗР ЧС1 с LCN = 802 всех четырех путей маршрутизации соответствующими канальными ключами (K_{1121} , K_{1122} , K_{11221} , K_{11222}), а сообщения ЗР ЧСЗ – канальными ключами (K_{31121} , K_{31122} , K_{31222} , K_{31221}). Используются те же канальные ключи, что и при установлении КВК (шаг 3).

Шаг 9. В соответствии с табл.3, 4 отправить сообщение ЗР в ЦКП абонентского доступа ЦКП 1.1 и ЦКП 1.2 по всем четырем путям маршрутизации.

Шаг 10. Стереть все строки таблиц маршрутизации (табл.3 в ЦКП 2.1 и табл.4 в ЦКП 2.2) сбрасываемых КВК ЧС1 и ЧСЗ.

Шаг 11. Дешифровать соответствующими канальными ключами ЧС1 (K_{1121} , K_{1122} , K_{11222} , K_{11221}) и ЧСЗ (K_{31121} , K_{31122} , K_{31222} , K_{31221}) принятые ЗР в ЦКП 1.1 и ЦКП 1.2 по четырем путям маршрутизации сообщений. Сменить в сообщении ЗР ЧС1 логический номер LCN = 802 на LCN = 809, а в сообщении ЗР ЧСЗ – логический номер LCN = 2802 на LCN = 2809 (согласно табл.1 и 2), предварительно установив эти LCN ЗР ЧС1 в конец очереди свободных $O_{1свн2122}$, LCN = 2802 ЗР ЧСЗ – в конец очереди свободных $O_{3свн2122}$ (в ЦКП 1.1 и ЦКП 1.2).

В результате в ЦКП 1.1 и ЦКП 1.2 очередь ЧС1 $O_{1свн1112}$: 805; 814; 815; 816; 817; 818; 819; 820; 821; 822; 823; 824; 825; 826; 827; 828; 804; 807; 809; 802. Откорректировать характеристику очереди $O_{свн2122}$ и по аналогии очередь ЧСЗ $O_{3свн1112}$.

Шаг 12. Зашифровать сообщения ЗР ЧС1 с LCN = 809 канальным ключом оконечного пункта K_{101} (в примере оконечный пункт а), ЗР ЧСЗ с LCN = 2809 канальным ключом оконечного пункта K_{2101} (в примере оконечный пункт d) и отправить эти сообщения ЗР в соответствующие оконечные пункты.

Шаг 13. Дешифровать ЗВ ключами оконечных пунктов КВК ЧС1 и ЧСЗ. Убедиться в совпадении LCN = 809 КВК ЧС1 и LCN = 2809 КВК ЧСЗ, расшифрованных в ЗР и присвоенных оконечным пунктам при установлении КВК. Стереть все строки таблиц маршрутизации (табл.1 в ЦКП 1.1 и табл.2 в ЦКП 1.2) сбрасываемых КВК ЧС1 и ЧСЗ.

Выводы

В продолжение разработки алгоритмов защищенного установления соединения в имитаторе объединенной сети ПД спецназначения [1] в транспортной части сети и на удаленном абонентском доступе оконечного пункта соединения, алгоритма разъединения соединения предложены алгоритмы защищенной передачи пакета данных по установленному коммутируемому виртуальному каналу в каждой из двух изолированных частных сетей. Эти сети передачи данных входят в имитатор объединенной сети ПД категории специального назначения. Представленные алгоритмы предусматривают обеспечение высоких требований как по информационной безопасности, так и по надежности. При этом учтены особенности канального шифрования в транспортной части сети по сравнению с абонентским доступом в [1]: сообщения установления КВК в транспортной части сети ПД выполняют функцию установления КВК нескольких ЧС между смежными узлами коммутации с различными канальными ключами шифрования в них; сквозные механизмы безопасности не формируются.

ЛИТЕРАТУРА

1. Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В. Алгоритм установления защищенного соединения на абонентском доступе имитатора объединенной сети ПД специального назначения // ПЕРВАЯ МИЛЯ. 2019. № 8. С. 46–51.
2. 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.

**21-23
МАЯ**

БЕЗОПАСНОСТЬ. IT-ТЕХНОЛОГИИ

**ВЫСТАВКА НОВЫХ ТЕХНОЛОГИЙ
ДЛЯ БИЗНЕСА И ЭКОНОМИКИ**

**ЧЕЛЯБИНСК
ЛА «ТРАКТОР»**

+7 992 511-35-55

При поддержке Национального
антитеррористического комитета

27–29 мая
КРАСНОЯРСК 2020

АНТИ ТЕРРОР

XVI ВСЕРОССИЙСКИЙ
СПЕЦИАЛИЗИРОВАННЫЙ
ФОРУМ-ВЫСТАВКА

современные системы
безопасности

- Технические средства и системы безопасности
- Инженерно-технические средства физической защиты
- Пожарная безопасность
- Аварийно-спасательное оборудование. Транспорт
- Экипировка. Индивидуальные средства защиты
- Информационная безопасность

Более **11 000** посетителей и **97** экспонентов в 2019 году!

КРАСНОЯРСКИЙ
КРАЙ
ПРАВИТЕЛЬСТВО

МВДЦ «Сибирь», ул. Авиаторов, 19
тел. (391) 200-44-28
famenko@krasfair.ru
www.krasfair.ru