АЛГОРИТМ АУТЕНТИФИКАЦИИ И ФОРМИРОВАНИЯ РАЗОВЫХ КЛЮЧЕЙ

в имитаторе лабораторного стенда 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,
А.Кравцов, старший научный сотрудник НИИЦ (Москва) ЦНИИ ВВКО,
Т.Никулина, студентка кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана

УДК 621.392, DOI: 10.22184/2070-8963.2019.79.2.62.68

Приведены алгоритмы аутентификации и формирования разовых ключей, предназначенных для обеспечения канального сквозного шифрования и целостности сообщений в имитаторе сети ПД категории специального назначения. При этом учитываются особенности объединенной структуры сети, включающей частные изолированные сети разных государственных ведомств, а также возможность предоставления соединений определенным оконечным пунктам частных сетей.

Введение

Настоящая статья является продолжением работ на кафедре "Информационная безопасность" МГТУ им. Н.Э.Баумана по созданию имитатора сети передачи данных (ПД) учебного лабораторного стенда (УЛС) для систем категории специального назначения (технология коммутации имитатора сети ПД построена на основе виртуальных каналов) и посвящена вопросам обеспечения их информационной безопасности (ИБ).

В предыдущих публикациях о создании такого имитатора не учитывалась сформулированная в работах [1,2] задача создания единой (объединенной) действующей отечественной сети ПД, предназначенной для организации информационного взаимодействия как внутри государственных структур, так и между ними (например, внутри ведомств МО и МВД РФ и между ними). Для этого необходимо создание в сети ПД нескольких частных (изолированных) сетей для каждого ведомства

и предоставление возможности устанавливать соединение некоторым оконечным пунктам частных сетей разных ведомств. Последние будем называть смешанными соединениями.

Решение задач обеспечения ИБ в сетях ПД категории специального назначения отечественными нестандартизированными механизмами возложено на специализированные отечественные научно-практические организации. В рамках учебного лабораторного стенда перед разработчиками имитатора сети ПД стоит задача составить основные положения ИБ сети ПД категории специального назначения с учетом особенностей создания объединенной сети. В настоящей статье изложены предложения по взаимной аутентификации и формированию разовых канальных ключей шифрования между всеми устройствами имитатора и сквозных ключей шифрования, контроля целостности в оконечном пункте источника пакета данных. В статье изложены основные положения обеспечения ИБ отечественной сети ПД специального назначения с учетом объединенной структуры ее построения. Для этого на имитаторе сети ПД в рамках УЛС потребовалось провести анализ и дать предложения по механизмам взаимной аутентификации устройств, аутентификации оконечных пунктов, управлению ключами.

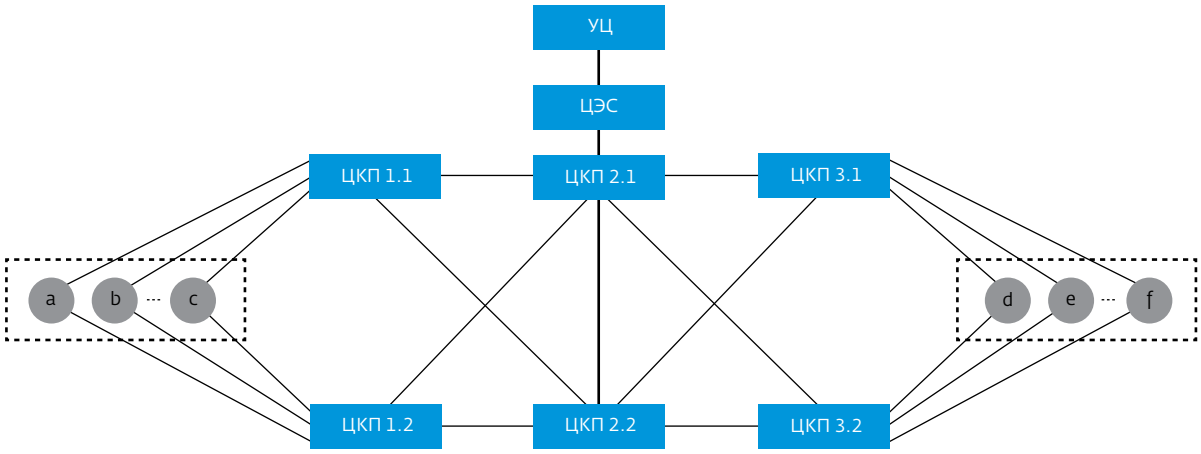
Рассмотрим алгоритмы аутентификации с учетом создания объединенной сети ПД категории специального назначения: алгоритм взаимной аутентификации всех смежных устройств имитатора сети ПД; алгоритм аутентификации оконечных пунктов (ОП) разных частных сетей ПД; алгоритм управления канальными и сквозными ключами. Алгоритм покажем на примере наличия трех частных сетей. На рисунке приведена конфигурация имитатора сети ПД в УЛС с центром эксплуатации сети (ЦЭС). Функции ЦЭС и приведенного Удостоверяющего центра (УЦ) будут приведены позже, при описании алгоритмов.

Конфигурация имитатора сети ПД в УЛС предусматривает создание пучка маршрутов между оконечными пунктами, состоящего из четырех путей маршрутизации. Каждый путь маршрутизации состоит из трех центров коммутации пакетов (ЦКП). К двум граничным ЦКП абонентского доступа в каждом пути маршрутизации (ЦКП 1.1 – адрес 11, ЦКП 3.1 – адрес 31 и ЦКП 1.2 – адрес 12, ЦКП 3.2 – адрес 32) подключены оконечные пункты, а ЦКП 2.1 – адрес 21 и ЦКП 2.2 – адрес 22 являются транзитными (или транспортными). Доступ оконечных пунктов (a, b … c и d, e … f) к граничным центрам коммутации пакетов удаленный. Оконечные пункты коммутируемых виртуальных каналов обмениваются данными одновременно по четырем путям маршрутизации. В работах [1, 2 и др.] в качестве примера приводятся пути маршрутизации для одного коммутируемого виртуального канала (КВК) одной частной сети (ЧС) без учета объединенной сети ПД с несколькими частными сетями и возможностью установления соединений между некоторыми оконечными пунктами (ОП) разных ЧС. Примем, что оконечные пункты a (ОПa) и f (ОПf) принадлежат частной сети 1 (ЧС1); оконечные пункты c (ОПc) и e (ОПe) принадлежат частной сети 2 (ЧС2), оконечные пункты b (ОПb) и d (ОПd) принадлежат частной сети 3 (ЧС3). Присвоим оконечным пунктам ЧС1 физические адреса от 1 до 999, ЧС2 – от 1001 до 1999, ЧС3 – от 2001 до 2999. Присвоим физический адрес 101 для ОПa, 601 – для ОПf, 1101 – для ОПc, 1601 – для ОПe, 2101 – для ОПb, 2601 – для ОПd. Номер частной сети обозначим как Z1.

Примером смешанного соединения может быть коммутируемый виртуальный канал (КВК) между принадлежащим ЧС1 оконечным пунктом ОПa и принадлежащим ЧС3 оконечным пунктом ОПd. Обозначим его СС13.

Алгоритм взаимной аутентификации всех смежных устройств имитатора сети ПД и аутентификации только оконечных пунктов

Необходимо взаимно аутентифицировать все смежные устройства имитатора сети, то есть между устройствами каждого абонентского доступа (оконечный пункт – ЦКП) и между смежными ЦКП. В работе по имитатору сети ПД [3], не рассматривающей объединенные частные сети, предлагается использовать алгоритмы взаимной аутентификации устройств имитатора сети ПД только на базе инфраструктуры открытых систем PKI. В работах по имитатору объединенной сети ПД категории специального назначения [1, 2] предлагаются использовать алгоритмы взаимной аутентификации устройств имитатора сети также только на базе PKI. Как показано в работе [4], по сетям связи в модернизированных энергосистемах smart grid таким алгоритмам на основе только PKI свойственен недостаток. При большом числе устройств в сети ПД для аутентификации необходим обмен большим числом сообщений, что вызывает недопустимые для smart grid задержки. Аналогичное положение имеет место и в объединенных сетях ПД категории специального назначения. Это вызвано экономической целесообразностью создания объединенных ведомственных сетей в сфере ОПК (т.е.



Конфигурация имитатора сети ПД в УЛС с центром эксплуатации сети

под каждую систему вооружения), МВД и других государственных структур [1, 2]. Для исключения указанного недостатка предлагается использовать принцип механизма взаимной аутентификации устройств сети ПД, который изложен в работе [4] для сетей ПД усовершенствованной инфраструктуры счета AMI модернизированной энергосистемы smart grid. Взаимная аутентификация здесь построена на использовании двух механизмов – PKI и механизма аутентификации на основе идентификатора устройств. Для использования этих механизмов в имитаторе сети ПД категории специального назначения используется приведенный на рисунке единый удостоверяющий центр (УЦ), который предоставляет центру эксплуатации сети ЦЭС каталог сертификатов всех устройств сети ПД. Удостоверяющий центр УЦ (CA, Certificate Authority) аутентифицирует ЦЭС и предоставляет ему функцию взаимной аутентификации всех смежных узлов имитатора сети ПД, а также аутентификацию оконечного пункта. Сертификат ЦЭС выдан этим УЦ, а сертификаты устройств имитатора сети могут быть выданы этим удостоверяющим центром.

Приведем последовательность операций по выполнению взаимной аутентификации между всеми смежными узлами на примере одной из пар смежных узлов имитатора сети ПД:

- создание и подключение к центру эксплуатации сети единого удостоверяющего центра УЦ (см. рисунок) имитатора сети ПД, включающего каталог из нескольких разных сертификатов для каждого устройства сети;
- УЦ аутентифицирует ЦЭС и пересылает ему указанный выше каталог сертификатов;
- аутентификация каждого устройства этой пары смежных устройств на основе их идентификатора и закрытого ключа сертификата предыдущей взаимной аутентификации;
- передача из ЦЭС в успешно аутентифицированные устройства этой пары новых сертификатов;
- взаимная аутентификация пары смежных устройств с использованием механизма PKI.

Приведенные первые два пункта относятся к первоначальной процедуре перед пуском имитатора сети ПД.

Аутентификация только оконечного пункта отличается от приведенной последовательности взаимной аутентификации:

- аутентификация только оконечного пункта абонентского доступа на основе идентификатора и закрытого ключа сертификата предыдущей аутентификации;
- передача нового сертификата из ЦЭС в успешно аутентифицированный оконечный пункт;
- аутентификация оконечного пункта с использованием сертификата граничного ЦКП абонентского доступа от последней взаимной аутентификации с другим ЦКП. При этом следует учесть, что смена сертификата граничного ЦКП при его взаимной аутентификации с другим ЦКП

проводится реже по сравнению с аутентификацией оконечного пункта.

Аутентификация ЦЭС:

- ЦЭС формирует запрос на его аутентификацию (зашифрованный открытым ключом идентификатор ЦЭС, его хэш, временное значение) $E_{ЦЭСЗ}$ [h(ЦЭСИД)||$T_{ЦЭС}$|| ЦЭСИД], где $E_{ЦЭСО}$ – открытый ключ ЦЭС, ЦЭСИД – идентификатор ЦЭС, $T_{ЦЭС}$ – отметка времени;
- ЦЭС отправляет это сообщение в УЦ;
- ЦЭС на приеме дешифрует принятое сообщение закрытым ключом ЦЭС $E_{ЦЭСЗ}$. Совпадение дешифрованного значения со значением запроса на аутентификацию [h(ЦЭСИД)||$T_{ЦЭС}$|| ЦЭСИД] означает аутентификацию ЦЭС;
- УЦ отправляет в ЦЭС каталог сертификатов и поручает использовать эти сертификаты для аутентификации устройств имитатора сети.

В имитаторе сети ПД категории специального назначения взаимная аутентификация между смежными ЦКП, оконечным пунктом и граничным ЦКП производится периодически. Частота для каждой пары смежных ЦКП определяется частной сетью с наиболее жесткими требованиями к ИБ. Частота для каждой пары узлов абонентского доступа определяется требованиями к ИБ частной сети. Аутентификация только оконечного пункта производится в зависимости от требований к ИБ частной сети либо периодически после установления нескольких КВК, либо при каждом установлении КВК.

Приведем основные положения этих алгоритмов на примере взаимной аутентификации между устройствами ЦКП 2.1 – ЦКП 1.1, устройствами ОПа (оконечный пункт а) – ЦКП 1.1. и аутентификации только оконечного пункта а. Указанные устройства относятся к ветви имитатора сети ОПа – ЦКП 1.1 – ЦКП 2.1. Идентификаторы, открытые и закрытые ключи устройств сети обозначим на основе их физических номеров. Например, идентификатор ЦКП 2.1–21ИД, открытый ключ ЦКП 2.1–$21_{O,}$ закрытый ключ ЦКП 2.1–$21_{З.}$

Взаимная аутентификация ЦКП 2.1 – ЦКП 1.1. Аутентификация на основе идентификатора ЦКП 2.1 и передача сертификата из ЦЭС осуществляются следующим образом: передача из ЦКП 2.1 в ЦЭС зашифрованного открытым ключом ЦЭС $E_{ЦЭСО}$ сообщения [h(21ИД)||T_{21}|| 21ИД]; дешифрация сообщения на приеме в ЦЭС закрытым ключом ЦЭС; ЦЭС проверяет 21ИД – принадлежит ли ЦКП 2.1; передача из ЦЭС сертификата ЦКП 2.1.

Аутентификация на основе идентификатора ЦКП 1.1 и передача сертификата из ЦЭС осуществляются следующим образом: передача из ЦКП 2.1 в ЦЭС зашифрованного открытым ключом ЦЭС $E_{ЦЭСО}$ сообщения [h(11ИД)||T_{21}|| 11ИД]; дешифрация сообщения на приеме в ЦЭС закрытым ключом ЦЭС; ЦЭС проверяет 11ИД – принадлежит ли ЦКП 1.1, передача из ЦЭС сертификата ЦКП 1.1.

Взаимная аутентификация ЦКП 2.1 – ЦКП 1.1 с использованием сертификатов осуществляется следующим образом: передача от ЦКП 2.1 его сертификата 21ИД|| 21_Oh[21ИД|| 21_O] в ЦКП 1.1, зашифрованного открытым ключом ЦКП 1.1 (11_O), то есть 11_O{21ИД|| 21_Oh[21ИД|| 21_O]}; дешифрация сертификата ЦКП 2.1 на приеме в ЦКП 1.1 закрытым ключом ЦКП 1.1 ($11_З$) – $11_З$ {21_O{21ИД|| 21_O h[21ИД|| 21_O]}} = {21ИД|| 21_O h[21ИД|| 21_O]}.

Убеждаемся в подлинности идентификатора 21ИД и ключей ЦКП 1.1: передача от ЦКП 1.1 его сертификата 11ИД||11_O h[11ИД|| 11_O] в ЦКП 2.1, зашифрованного открытым ключом ЦКП 2.1 (21_O), то есть 21_O{11ИД|| 11_O h[11ИД|| 11_O]}; дешифрация сертификата ЦКП 1.1 на приеме в ЦКП 2.1 закрытым ключом ЦКП 2.1 ($21_З$) – $21_З$ {21_O{11ИД|| 11_O h[11ИД|| 11_O]}} = {11ИД|| 11_O h[11ИД|| 11_O]}.

Убеждаемся в подлинности идентификатора 11ИД и ключей ЦКП 2.1: передача от ЦКП 2.1 в ЦЭС сообщения об успешной взаимной аутентификации ЦКП 2.1 – ЦКП 1.1.

Взаимная аутентификация ЦКП 1.1 – ОПа (обозначения: открытый ключ – a_o, закрытый ключ – $a_з$, идентификатор ОПа – 101ИД) осуществляется следующим образом:

- аутентификация на основе идентификатора ОПа и передача сертификата из ЦЭС: передача из ОПа в ЦЭС зашифрованного открытым ключом ЦЭС $E_{ЦЭСО}$ сообщения [h(101ИД) ||Ta|| 101ИД], дешифрация на приеме в ЦЭС закрытым ключом ЦЭС; ЦЭС проверяет 101ИД – принадлежит ли ОПа; передача из ЦЭС сертификата ОПа;
- взаимная аутентификация ЦКП 1.1 – ОПа с использованием сертификата ЦКП 1.1, полученного из ЦЭС: передача от ОПа в ЦКП 1.1 сертификата ОПа – 101ИД || a_o h[101ИД || a_o], зашифрованного открытым ключом 11_O, то есть 11_O {101ИД || a_o h[101ИД || a_o]}. Используется сертификат ЦКП 1.1, полученный из ЦЭС; дешифрация сертификата ОПа на приеме в ЦКП 1.1 осуществляется закрытым ключом $11_З$ – $11_З$ {11_O {101ИД || a_o h[101ИД || a_o]}} = {101ИД || a_o h[101ИД || a_o]}.

Убеждаемся в подлинности идентификатора 101ИД и ключей ЦКП 1.1: передача от ЦКП 1.1 его сертификата в ОПа, сертификат 11–11ИД || 11_O h[11ИД || 11_O], зашифрованный открытым ключом a_o, то есть a_o {11ИД|| 11_O h[11ИД || 11_O]}; дешифрация сертификата 11 на приеме в ОПа осуществляется закрытым ключом $a_з${ a_o {11ИД|| 11_O h[11ИД || 11_O]}} = {11ИД || 11_O h[11ИД || 11_O]}.

Убеждаемся в подлинности идентификатора 11ИД и ключей ОПа; далее следует передача от ЦКП 1.1 в ЦЭС сообщения об успешной взаимной аутентификации ЦКП 1.1 – ОПа.

Аутентификация ОПа. Алгоритм аутентификации оконечного пункта на примере ОПа на основе идентификатора: осуществляется передача из ОПа в ЦЭС зашифрованного открытым ключом ЦЭС $E_{ЦЭСО}$ сообщения [h(101ИД) ||Ta|| 101ИД], затем – дешифрация сообщения на приеме в ЦЭС закрытым ключом ЦЭС, после чего ЦЭС проверяет 101ИД – принадлежит ли ОПа. В зависимости от требований к ИБ к ЧС и конкретному КВК периодически выполняется взаимная аутентификация между ОПа и граничным маршрутизатором абонентского доступа при получении от ЦЭС сертификата ОПа и использовании сертификата граничного ЦКП (в приведенном выше примере ЦКП 1.1).

Алгоритм управления ключами в имитаторе сети ПД. Управление ключами (КМ, key management) является важной функцией в обеспечении ИБ объединенной сети ПД категории специального назначения.

Рассмотрим выполнение таких задач КМ, как генерация головного ключа, обмен (распределение) ключей, смена ключей; покажем пример управления ключами на абонентском доступе источника установления КВК. Для абонентского доступа такими ключами являются канальный ключ шифрования, сквозной ключ шифрования, сквозной ключ обеспечения целостности. Поскольку абонентский доступ окончания установления КВК может быть абонентским доступом источника установления КВК, для каждого абонентского доступа производится создание не только канальных ключей шифрования, но и всех сквозных ключей. Для участка между ЦКП таким ключом является только канальный ключ шифрования.

Выбор механизмов ИБ и управление ключами

Выбор канальных и сквозных механизмов шифрования и обеспечения целостности на абонентских участках и между смежными узлами коммутации определяется алгоритмом ассоциации безопасности SA (Security association). Подробный алгоритм приводится с помощью ЦЭС при описании установления КВК.

Генерация и распределение ключей на абонентском доступе установления КВК. Приведем основные положения управления ключами (на примере участков имитатора сети ПД, для которых выше показана взаимная аутентификация) – между смежными ЦКП 2.1 – ЦКП 1.1 и на абонентском участке оконечного пункта источника установления КВК ЦКП 1.1 – ОПа. Для этого абонентского доступа такими ключами являются канальный ключ шифрования, сквозной ключ шифрования, сквозной ключ обеспечения целостности.

Обозначим K_a – головной ключ в ОПа и ЦКП 1.1.

Сгенерированный в ОПа ключ K_a передается в ЦКП 1.1, зашифрованный открытым ключом ЦКП 1.1, то есть $11_O[K_a]$ с последующей дешифрацией закрытым ключом ЦКП 1.1, то есть $K_a = 11_З[11_O[K_a]]$.

В ОПа и ЦКП 1.1 создается разовый канальный ключ $K_{ак} = K_{101} = hash(K_a || 101ИД)$ для шифрования/дешифрации на абонентском доступе сообщений установления соединения КВК, заголовков информационных сообщений установленного КВК. Алгоритм установления канального ключа на абонентском доступе другого ОП этого КВК аналогичен приведенному для абонентского доступа источника установления КВК.

В ОПа частной сети и смешанного соединения создаются разовые сквозные ключи $K_{аинф1}$, $K_{аинф2}$ для шифрования/дешифрации в оконечном пользователе ОП информационной части передаваемого/принимаемого соответственно в прямом и обратном направлении пакета данных:

- $K_{аинф1} = K1_{101601} = hash(K_a || 101ИД || 1)$;
- $K_{аинф2} = K2_{101601} = hash(K_a || 101ИД || 2)$.

В ОПа частной сети и смешанного соединения создаются разовые сквозные ключи $K_{Цаинф1}$, $K_{Цаинф2}$ для проведения контроля в оконечном пользователе целостности информационной части пакета данных соответственно в прямом и обратном направлении:

- $K_{Цинф1} = K3_{101601} = hash(101ИД || K_a || 3)$;
- $K_{Цинф2} = K4_{101601} = hash(101ИД || K_a || 4)$.

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

Генерация и распределение ключей между смежными ЦКП. В конкретной паре смежных ЦКП число канальных ключей равно числу частных сетей, используемых в этой паре. Обозначим такой ключ $K(Z)_{И1И2}$ между двумя смежными ЦКП с идентификаторами И1 и И2 и номером частной

сети Z. $K(Z)_{И1И2}$ = hash($K_{И1И2}$ ||И1||И2||Z). Здесь $K_{И1И2}$ – сгенерированный ключ в одном из смежных ЦКП с идентификаторами И1 или И2, в частной сети Z. Таким образом, создаются канальные ключи для каждой частной сети в девяти каналах имитатора сети ПД – 1121, 1221, 3121, 3221, 2221, 1122, 1222, 3122, 3222. Две цифры названия канала обозначают физический адрес одного смежного ЦКП, другие две цифры – другого смежного ЦКП.

Приведем пример установления канальных ключей для трех подсетей на примере участка транспортной сети ЦКП 2.1 – ЦКП 1.1. По команде с ЦУС в одном из этих ЦКП производится генерация ключа. Обозначим R – сгенерированный ключ в ЦКП 2.1.

При использовании путей маршрутизации между ЦКП 2.1 и ЦКП 1.1 всех трех частных сетей в ЦКП 2.1 создаются канальные ключи для каждой частной сети – ЧС1, ЧС2, ЧС3:

- $K1_{1121}$ = hash(R ||11ИД||21ИД||1) для ЧС1,
- $K2_{1121}$ = hash(R ||11ИД||21ИД||2) для ЧС2,
- $K3_{1121}$ = hash(R ||11ИД||21ИД||3) для ЧС3.

Все эти ключи передаются в ЦКП 1.1 зашифрованным открытым ключом ЦКП 1.1, то есть $11_O[K1_{1121}]$, $11_O[K2_{1121}]$, 11_O $[K3_{1121}]$.

В ЦКП 1.1 производится их дешифрация закрытым ключом ЦКП 1.1, то есть $K1_{1121}$ =$11_З\{11_O$ $[K1_{1121}]\}$, $K2_{1121}$ = $11_З\{11_O$ $[K2_{1121}]\}$, $K3_{1121}$ = $11_З\{11_O$ $[K3_{1121}]\}$.

Эти ключи остаются без изменения при установлении каждого соединения в частной сети. Для того чтобы канальные ключи были разовыми для каждого соединения, они создаются для каждого нового устанавливаемого соединения с помощью номера коммутируемого виртуального канала – k:

- $K1_{1121K}$ = hash(11ИД||21ИД||1) для ЧС1,
- $K2_{1121K}$ = hash(11ИД||21ИД||2) для ЧС2,
- $K3_{1121K}$ = hash(11ИД||21ИД||3) для ЧС3.

Генерация и распределение ключей между ЦЭС и ЦКП 2.1. На участке между ЦЭС и ЦКП 2.1 необходим ключ шифрования/дешифрации сообщений обмена по коррекции таблицы маршрутизации, запроса таблиц маршрутизации от источника из ЦКП абонентских доступов при установлении КВК и других сообщений. Сгенерированный в ЦКП 2.1 ключ $K_{ЦЭС}$ передается в ЦЭС, зашифрованный открытым ключом ЦЭС с последующей дешифрацией закрытым ключом ЦЭС. В ЦЭС и ЦКП 2.1 создаются канальные ключи для каждой частной сети:

- $K1_{ЦЭС}$ = hash($K_{ЦЭС}$ ||0ИД||21ИД||1) для ЧС1,
- $K2_{1121}$ = hash($K_{ЦЭС}$ ||0ИД||21ИД||2) для ЧС2,
- $K3_{1121}$ = hash($K_{ЦЭС}$ ||0ИД||21ИД||3) для ЧС3,

где 0ИД – идентификатор ЦЭС.

Выводы

В рамках создания учебного лабораторного стенда имитатора сети ПД предложено с учетом особенностей создания объединенной сети категории специального назначения обеспечение ИБ в части: алгоритма взаимной аутентификации смежных устройств имитатора сети ПД на основе PKI и механизма идентификатора устройств; алгоритма аутентификации оконечного пункта на основе механизма идентификатора; формирования на абонентском доступе разового канального ключа; формирования на оконечном пункте источника установления соединения разовых сквозных ключей шифрования/дешифрации и контроля целостности сообщений; формирования в транспортной части имитатора сети ПД разового канального ключа каждого пути маршрутизации частной сети.

Планируется аппаратно-программная реализация этих предложений в имитаторе объединенной сети ПД студентами кафедры "Информационная безопасность" МГТУ им. Н.Э.Баумана. Эта работа ведется в соответствии с дисциплинами "Системы и сети передачи данных" и "Защищенные системы связи".

ЛИТЕРАТУРА:

1. **Бельфер Р.А., Басараб М.А., Кравцов А.В.** Алгоритмы коррекции таблицы маршрутизации в имитаторе сети ПД с обеспечением высокой надежности и безопасности // Электросвязь. 2018. № 6. С. 63–66.
2. **Матвеев В.А., Бельфер Р.А., Кравцов А.В.** Анализ технологий построения сети передачи данных с высокими требованиями по информационной безопасности, надежности и задержке // Электросвязь. 2017. № 5. С. 46–49.
3. **Басараб М.А., Бельфер Р.А., Глинская Е.В., Кравцов А.В.** Алгоритм ПО установления коммутируемого виртуального канала на абонентском доступе имитатора сети ПД с учетом обеспечения информационной безопасности // ПЕРВАЯ МИЛЯ. 2017. № 8. С. 64–69.
4. Lee Sangji, Bong Jinsuk, Shin Sunhee, Shin Yongtae. A security mechanism of Smart Gri d AMI network through smart devicemutual au thentication. The International Conference on Information Networking 2014 (ICOIN2014). 2014. P. 592–595.
5. Bouhafs F et al. Communication Challenges and Solutions in the Smart Grid? The Smart Grid in the Last Mile. 2014. P. 25–35.