127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство Криптографической Защиты Информации

КриптоПро CSP Версия 5.0 KC1 1-Base Описание реализации КриптоПро IPsec

ЖТЯИ.00101-01 90 02
Листов 41

2019 г

Содержание

Список определений и сокращений

AH	Authentication Header (Аутентифицирующий заголовок)
CMAK	Connection Manager Administration Kit (Пакет администратора диспетчера подключений)
CSP	Cryptographic Service Provider (Криптопровайдер)
EAP-TLS	Extensible Authentication Protocol-Transport Level Security
ESP	Encapsulating Security Payload (Инкапсуляция зашифрованных данных)
GPMC	Group Policy Management Console (Редактор управления групповыми политиками)
IAS	Internet Authentication Service (Служба проверки подлинности в Интернете)
IKE	Internet Key Exchange (протокол Обмена ключами)
IPsec	IP Security (протокол Защиты IP-трафика)
IPsec SA	Security Associations (Безопасное соединение)
ISA Server	Internet Security and Acceleration Server
NAT	Network Address Translation (Преобразование сетевых адресов)
NPS	Network Policy Server (Сервера политики сети)
OCSP	Online Certificate Status Protocol (Протокол получения статуса сертификата в реальном времени)
PEAP	Protected Extensible Authentication Protocol (Защищённый Расширяемый Протокол Аутентификации)
PSK	Предварительно согласованный ключ
RADIUS	Remote Authentication in Dial-In User Service (Протокол для реализации аутентификации, авторизации и учета)
SAN	Subject Alternative Name (Альтернативное имя субъекта)
TMG	Threat Management Gateway
UPN	User Principal Name (Основное имя пользователя)
ААУ	Аутентификация, авторизация и учет
БД	База данных
МЭ	Межсетевой экран
ПАК	Программно-Аппаратный Комплекс
СКЗИ	Средство криптографической защиты информации
УЦ	Удостоверяющий центр

Аннотация

Настоящий документ содержит описание реализации и вариантов использования программного модуля КриптоПро IPsec, предназначенного для защиты данных, передаваемых в IP-сетях.

В настоящем документе описаны особенности применения КриптоПро IPsec для:
- защиты VPN;
- защиты соединения site-to-site VPN;
- организации изоляции домена

на базе ключевых систем:
- PSK;
- сертификаты.

Документ также содержит руководство по установке и конфигурации КриптоПро IPsec под управлением ОС Windows. Сценарии пошаговой настройки вариантов использования КриптоПро IPsec (в том числе для МЭ) приводятся в приложении.

Порядок использования API для реализации протоколов IPsec под управлением ОС семейств Windows и Linux описан в «КриптоПро IKE, ESP, AH. Руководство разработчика» (`ikespah_ipsec50.chm`).

1 Назначение и условия эксплуатации

КриптоПро IPsec предназначен для защиты открытой информации в информационных системах общего пользования и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах, и обеспечивает:

- аутентичность сторон взаимодействия, указанных в политике IPsec (правилах IPsec), при использовании совместно с МЭ;
- конфиденциальность и аутентичность передаваемой по VPN или ЛВС конфиденциальной информации в режиме мандатного шифрования без применения дополнительных МЭ;
- конфиденциальность и аутентичность передаваемой по VPN или ЛВС конфиденциальной информации между некоторыми, выделенными, сторонами взаимодействия при встраивании в состав МЭ или приложений;
- аутентичность сторон голосовых или видеоконференций, в которых нет обмена конфиденциальной информации.

Использование КриптоПро IPsec для обеспечения конфиденциальности голосовых или видеоконференций без проведения дополнительных исследований запрещается.

Встраивание КриптоПро IPsec в МЭ или в другие защищаемые информационные системы должно производиться в соответствии с Положением ПКЗ-2005 организациями, имеющими лицензию на право проведения таких работ.

При встраивании КриптоПро IPsec в прикладное программное обеспечение должны выполняться требования раздела 7 документа «ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть», документа «ЖТЯИ.00101-01 96 01. Руководство программиста» и п. 1.5 документа «ЖТЯИ.00101-01 30 01. Формуляр».

Соединения, построенные с использованием режимов и алгоритмов IPSec, отличных от описанных в настоящей документации, должны рассматриваться как незащищенные соединения. При этом должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с КриптоПро IPsec по требованиям информационной безопасности.

2 Программно-аппаратные среды функционирования

КриптоПро IPsec функционирует в программно-аппаратных средах:

Windows 7/8.1/10/Server 2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016/2019 (x64).

Со сроками эксплуатации указанных операционных систем можно ознакомиться по адресу:

https://support.microsoft.com/ru-ru/lifecycle/search

Для работы КриптоПро IPsec необходима предварительная установка компонентов КриптоПро CSP (подробнее см. разд. 6).

Порядок использования API для реализации протоколов IPsec под управлением ОС семейств Windows и Linux описан в «КриптоПро IKE, ESP, AH. Руководство разработчика» (`ikespah_ipsec50.chm`).

3 Описание протоколов КриптоПро IPsec

Для защиты данных, передаваемых по открытым каналам связи, принято использовать так называемую «технологию защищенного канала», в котором должны быть обеспечены:

- взаимная аутентификация взаимодействующих сторон;
- конфиденциальность передаваемых данных;
- целостность и аутентичность передаваемых данных с защитой от повторов.

Защищенный канал может быть реализован путем организации виртуальной частной сети (Virtual Private Network, VPN). Суть подхода состоит в том, чтобы внутри открытой сети, доступ к которой не ограничен различным категориям пользователей, создать собственную, изолированную, доверенную среду обмена данными. В этой среде смогут работать только допущенные пользователи, а для остальных пользователей трафик защищенного канала будет зашифрован на ключе пользователя, без обладания которым передаваемая информация будет недоступна на чтение. Кроме того, пакет защищен кодом аутентификации, что обеспечивает невозможность модификации, переадресации и DoS-атак.

Среди наиболее распространенных VPN-протоколов можно выделить L2TP/IPSec и SSTP. Не рекомендуется использовать протокол PPTP для защиты сети, т.к. на сегодняшний день он не отвечает минимальным требованиям безопасности.

КриптоПро IPsec позволяет создавать защищенные каналы передачи данных в IP-сетях с использованием шифрования. В зависимости от решаемых задач, данный продукт может быть использован в составе уже имеющихся решений, в новой инфраструктуре, на отдельно стоящих компьютерах или в составе всех защищаемых объектов сети. КриптоПро IPsec предназначен для установки на сетевые объекты, такие как межсетевые экраны, серверы удаленного доступа, контроллеры домена, а также на компьютеры пользователей домена и удаленных пользователей, которые работают под управлением поддерживаемых ОС (см. разд. 2).

Возможно применение КриптоПро IPsec в 3 базовых сценариях:

- «точка-сеть» («точка-точка», «подключение удаленного доступа», «client-to-site»), когда клиент подключается к серверу удаленного доступа, связь между которым и локальной сетью назначения идет через сеть общего доступа (см. рис. 1);
- «сеть-сеть» («маршрутизатор-маршрутизатор», «site-to-site»), когда две (или более) доверенные сети обмениваются внутренними данными через общедоступную, сеть (например, «Интернет»), но при этом риск, связанный с нарушением конфиденциальности передаваемых данных, их подмены, искажения сводится к допустимому минимуму (см. рис. 2);
- «изоляция группы» компьютеров или всего домена в локальной сети (см. рис. 3).

VPN-подключение типа «точка-сеть» дает пользователям возможность получать доступ к сетевым ресурсам своей организации с использованием общедоступной сети передачи данных. При этом, реальная инфраструктура общедоступной сети не имеет никакого значения, так как передача данных организована подобно тому, как если бы они передавались по выделенному (т.е. недоступному посторонним лицам, частному) каналу (см. рис. 1).

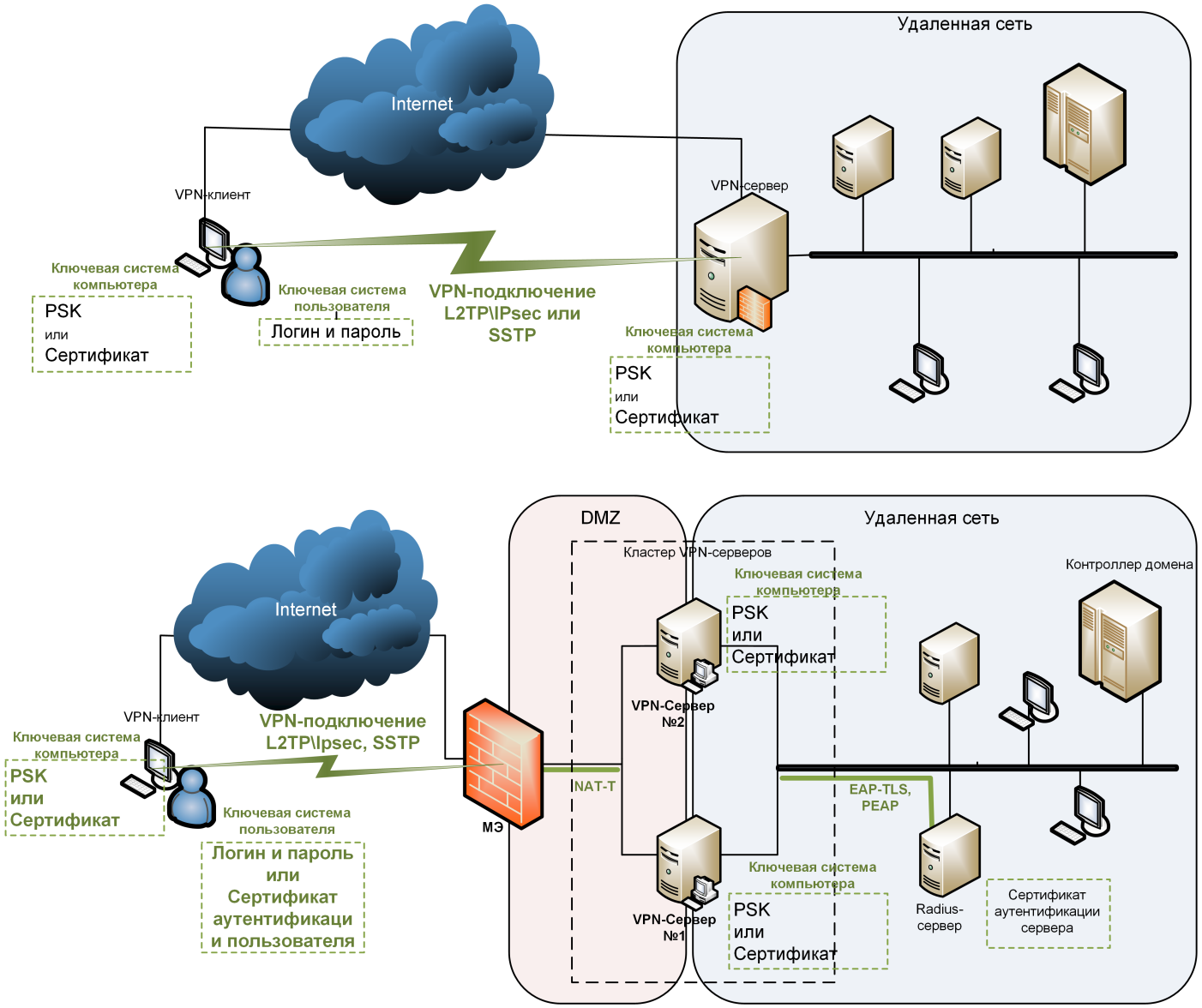

Рисунок 1. Варианты подключения «точка-сеть»

При соединении типа «сеть-сеть» протоколы безопасности применяются только к пакетам, выходящим из локальной сети, и прекращают свое действие при входе пакета в другую удаленную локальную сеть, т.е. внутри локальных сетей пакеты не защищены (не зашифрованы, не содержат данных для проверки целостности). При таком соединении один VPN-сервер обеспечивает маршрутизируемое подключение к сети, которая находится за другим VPN-сервером. Сервер, инициирующий VPN-соединение, т.е. по сути VPN-клиент, проходит проверку подлинности на отвечающем сервере (VPN-сервере), а затем уже отвечающий сервер проходит проверку подлинности на вызывающем сервере с целью обеспечения взаимной проверки подлинности взаимодействующих сторон (см. рис. 2).

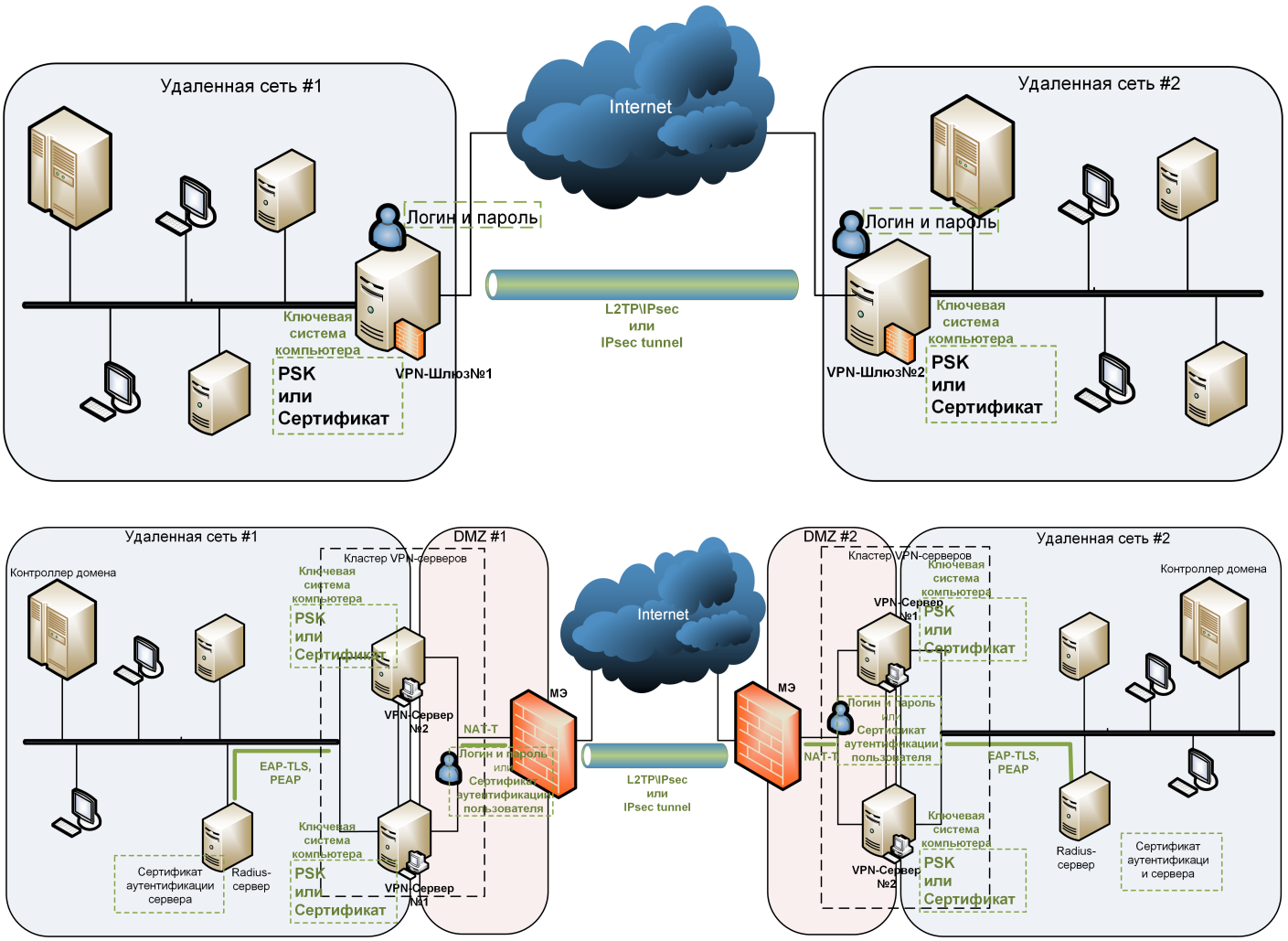

Рисунок 2. Варианты подключения «сеть-сеть»

Кроме того, КриптоПро IPsec поддерживает **Правила** и **Политики IPsec**, что позволяет сегментировать локальную сеть на изолированные логические сети с разными уровнями безопасности. Можно в имеющейся физической сети создать логическую, в которой компьютеры будут использовать общий набор правил и политик безопасного обмена данными (см. рис. 3).

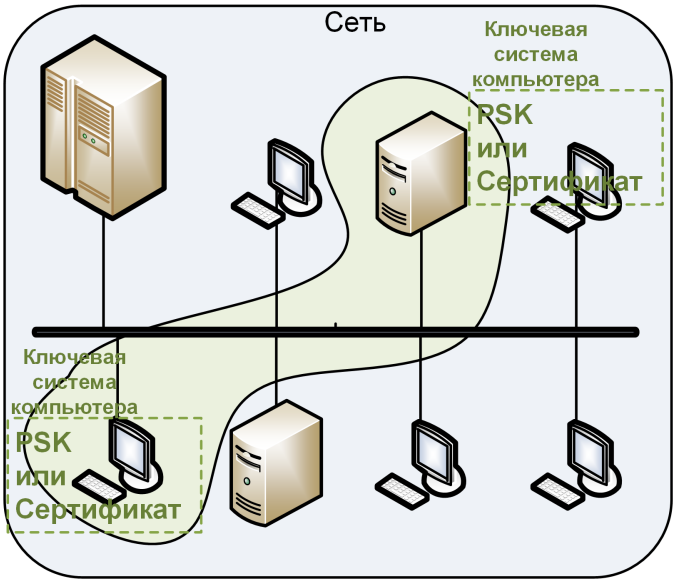

Рисунок 3. Политики и правила IP-безопасности

С точки зрения правила, любой IP-пакет, подходящий по совокупности критериев (фильтров) к данному правилу, должен быть обработан. Существует 3 варианта обработки пакетов: применить IPsec к пакету, заблокировать или пропустить пакет. Таким образом, существует возможность управлять тем или иным типом трафика с помощью настройки правил, что в результате позволяет защищать с помощью IPsec необходимый диапазон IP-пакетов.

Перечисленные выше сценарии применения КриптоПро IPsec основаны на низкоуровневом («сетевой уровень» №3 модели OSI) протоколе IPsec, что исключает необходимость внесения изменений в топологию сети и в существующие приложения.

IPsec можно условно разделить на три группы протоколов:

• Протокол **IKE** отвечает за согласование параметров и выработку ключевой информации, работает в режиме пользователя на транспортном уровне, использует для транспорта протокол UDP порт 500 (4500 в случае NAT-Traversal).

• Протоколы **ESP** и **AH** обеспечивают защиту непосредственно передаваемых данных, на основе параметров и ключей, полученных на этапе работы IKE, работают в режиме ядра на сетевом уровне.

• Протоколы **L2TP** и **EAP-TLS**, **PEAP** обеспечивают контроль регламента подключаемого к сети клиента (пользователя).

Протокол IKE содержит две фазы работы. Фаза 1 предназначена для организации основы для дальнейшего взаимодействия, она согласует параметры работы протокола IKE, вырабатывает ключевой материал криптографической защиты данных вложений и обеспечивает аутентификацию сторон (основанием подлинности может быть сертификат или PSK). После того как стороны подтвердили свою подлинность, фаза 1 считается завершенной.

Фаза 2 создается на основе фазы 1 и предназначена для выработки согласованных параметров и новой ключевой информации для протокол ESP, завершается созданием IPsec SA. На основе одной фазы 1 может быть создано несколько фаз 2. Одна успешно завершенная фаза 2 по умолчанию создает две IPsec SA (для входящих и исходящих пакетов), они содержат весь необходимый набор правил и криптографических ключей для обработки пакетов в рамках протокол ESP.

Соединение по IPsec — это безопасное соединение типа точка-точка. Поэтому для установки соединения по IPsec между любыми двумя участниками должны быть успешно пройдены IKE фазы 1 и 2 для выработки

актуальных IPsec SA. После этого фаза 1 переходит в режим ожидания, фаза 2 считается завершенной и освобождается с появлением IPsec SA. Пока IPsec SA актуальны, соединение по IPsec может быть использовано. С течением времени и трафика IPsec SA могут утратить актуальность (ключи требуют периодического обновление). Обновление IPsec SA происходит автоматически при повторном прохождении новой IKE фазы 2 или полного цикла 1 и 2 фазы IKE, аналогичного начальному. При появлении нового участника в обмене каждый должен установить с ним отдельное соединение по IPsec описанным выше образом.

Важно помнить, что соединение по IPsec является инструментом защиты канала. Как только канал установлен, дальнейшая логика работы в канале зависит от используемых приложений и протоколов транспортного и других уровней взаимодействия.

4 Структура КриптоПро IPsec

Структуру КриптоПро IPsec следует представлять как надстройку над механизмами реализации IPsec в ОС. На рис. 4 изображена схема взаимодействия компонентов КриптоПро IPsec с компонентами ОС. Все компоненты, за исключением фильтра КриптоПро, встроены в реализацию IPsec ОС и обеспечивают выполнение расширенного функционала. Фильтр КриптоПро находится на канальном уровне и обеспечивает дополнительный контроль корректности применения шифрования. В случае применения режима мандатного шифрования фильтр также обеспечивает блокировку выхода в канал всех незашифрованных пакетов (исключением являются пакеты базовых сетевых служб, таких как DHCP, DNS, а также пакеты IKE и UDP порт 4500 для работы IPsec в режиме NAT-Traversal).

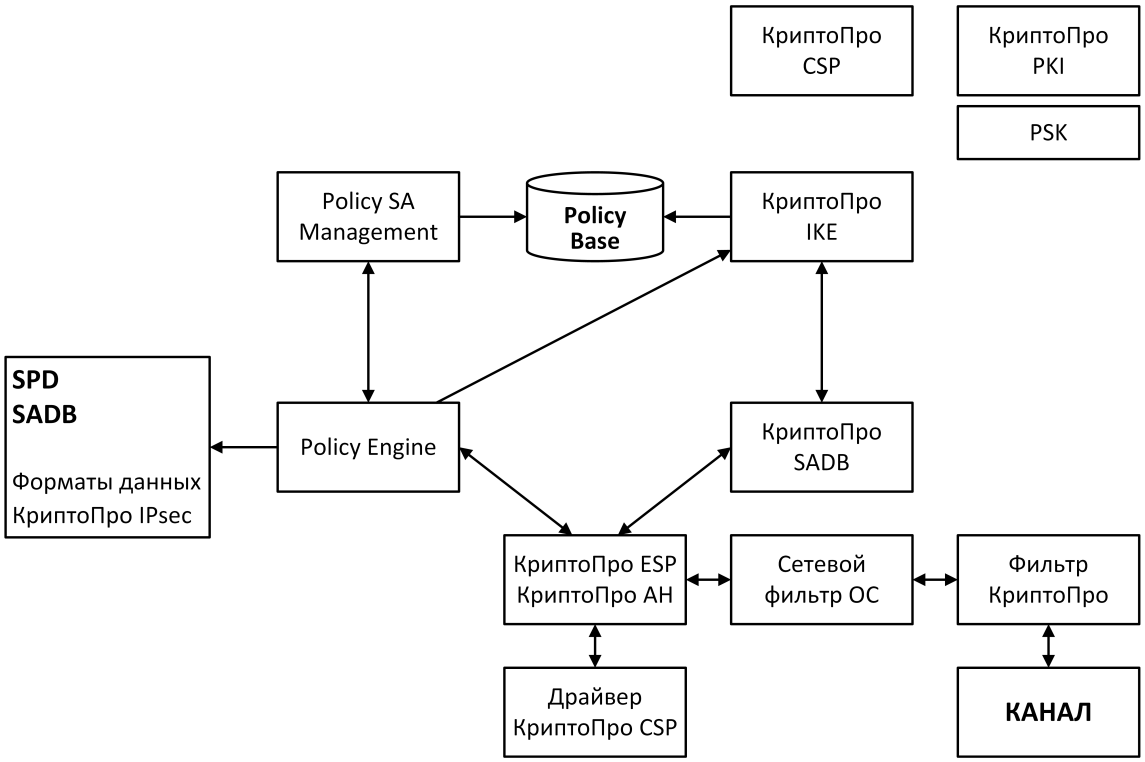

Рисунок 4. Схема взаимодействия компонентов КриптоПро IPsec и ОС

5 Ключевая система

Под ключевой системой КриптоПро IPsec понимается совокупность данных, необходимых для аутентификации участника, устанавливающего соединение по IPsec. В это понятие входят сертификаты компьютера и пользователя, PSK, имя пользователя и пароль. Ключевая система в зависимости от вариантов использования может представлять собой ограниченный набор, например, только сертификат компьютера или только PSK. Для корректного функционирования ключевой системы требуется обеспечить каждому участнику обмена соответствующие механизмы получения, хранения, обновления, исключения, удаления ключевого материала. Для сертификатов это обеспечивается внедренной инфраструктурой открытых ключей. Для PSK — утилитой `genpsk` и организационными методами. Для имени пользователя и пароля — администрированием учетных записей пользователей в ОС.

Использование того или иного варианта ключевой системы зависит от выбора реализуемого варианта использования. Следует различать сертификат компьютера и пользователя.

Вариант использования **VPN** предполагает несколько вариантов ключевых систем:

1) (рекомендуется) Наличие сертификата компьютера и сертификата пользователя; допустимо объединение сертификатов в один сертификат двойного назначения компьютера-пользователя. Сертификат компьютера необходим для аутентификации в рамках IKE, сертификат пользователя — для аутентификации пользователя на удаленном сервере. В этом варианте серверу необходимо иметь только сертификат компьютера. При этом инфраструктура открытых ключей (ИОК) должна находиться как внутри сети, так и снаружи.

2) Использование PSK и учетной записи пользователя (символьные имя пользователя и пароль). В этом случае PSK используется для аутентификации в рамках IKE, имя пользователя и пароль — для аутентификации пользователя на удаленном сервере. При использовании PSK для аутентификации машин пользователя в рамках IKE требуются дополнительные организационные меры защиты в случае стационарных компьютеров. В случае мобильных компьютеров данный вариант не рекомендуется к использованию ввиду повышенной вероятности компрометации PSK.

Вариант использования **Site-to-site VPN** предполагает использование PSK и учетных записей серверов (символьные имя пользователя и пароль). Так как данный вариант использует соединение по IPsec исключительно между серверами, то, как правило, не требуются дополнительные организационные меры по предотвращению НСД, и сервера находятся в оперативном доступе администратора. Таким образом, достаточно пройти процедуру аутентификации по PSK в рамках IKE и аутентификацию по имени пользователя и паролю сервера инициатора на удаленном сервере. Ввиду обоснованной простоты, данная ключевая система рекомендуется к использованию при Site-to-site VPN.

Вариант использования **Изоляция домена** предполагает использование инфраструктуры открытых ключей внутри домена. В этом варианте все участники домена должны иметь сертификат компьютера для аутентификации в рамках IKE, аутентификация в домене происходит штатными средствами данного домена и не включается в требования к ключевой системе КриптоПро IPsec.

Примечание. Использование PSK возможно только после проведения исследований в соответствии с п. 1.5 ЖТЯИ.00101-01 30 01. Формуляр. Без дополнительных исследований допускается использовать PSK только в тестовом режиме.

5.1 Pre-Shared Key (PSK)

Генерация, распространение, плановая схема и действия при компрометации PSK определяются установленным регламентом.

Для генерации КриптоПро PSK применяется утилита genpsk. Утилита реализована в виде исполняемого файла genpsk.exe. После установки КриптоПро IPsec по умолчанию утилита доступна по пути %ProgramFiles%\Crypto Pro\IPsec.

Для запуска утилиты необходимо выполнить следующую команду:

[путь]genpsk [<команда> [<опции>]]

путь путь к месторасположению программы

genpsk имя исполняемого файла

команда одна из допустимых команд:

-f GenPSK – генерация PSK

-f CreateBasePSK – генерация закрытого ключа

-f DeleteBasePSK – удаление закрытого ключа

-f chkpsk – проверка PSK

опции параметры команды

Для формирования PSK запуск утилиты производится с параметром **-f GenPSK**:

[-f GenPSK] [-n <PSKId>] [-D <NetName>] [-d <FilePath>] [-v <Version>] [-P <PrintType>] [-S <on/off>] [-m <PSK time to live>] [-N <Stations List>]

-n <PSKId> Идентификатор PSK

-D <NetName> Имя сети связи (направления связи). Кроме того, используется как заголовок при печати ключей

-d <FilePath> Путь к файлам результирующих списков ключей. Должен завершаться символом '\'. Полные имена файлов: FilePath|NetName_0, FilePath|NetName_1. Если отсутствует, то печать в файлы не производится.

-v <Version> Версия PSK. Если не задан, то в качестве версии используется случайное число

-P <PrintType> Форма вывода на печать:
- по признаку "Net" осуществляется печать PSK в двух частях;
- по признаку "CMAK" осуществляется печать единым массивом.

-S <on/off> Если установлен, то производится вывод на экран

-m <PSK time to live> Срок действия PSK в месяцах (не более 6 месяцев)

-N <Stations List> Список узлов связи

Пример:

```
genpsk -D TestNet -n 02.06.18 -v 2 -m 6 -f GenPSK -P CMAK -S -N ForOffice ForClient
```

```
02.06.18,ForOffice,FPH90HEKY2WDWPR1W2VLAZD603C1

02.06.18,ForClient,UKUX0QYGM52EPPEPG5HZ09URUU41
```

Для создания PSK может быть использован контейнер закрытого ключа. Применение контейнера упрощает генерацию и сохраняет возможность расширения списка PSK без перегенерации всех PSK.

```
[-f GenPSK] [-n <PSKId>] [-D <NetName>] [-d <FilePath>] [-v <Version>] [-P <PrintType>]
[-S <on/off>] [-m <time to live>] [-k <Container>] [-p <PIN>] [-N <Stations List>]
```

-k <Container> Имя ключевого контейнера, использующегося как хранилище ключа

-p <PIN> Пароль (PIN) на ключевой контейнер

Пример:

```
genpsk -D TestNet -n 02.06.11 -f GenPSK -k Cont -p 123456 -m 6 -P CMAK -S -N ForOffice
ForClient
```

```
02.06.18,ForOffice,DH8BPT8XA40HYCX8FXPM87FWRM5H

02.06.18,ForClient,GAAYM6ETF10ZUC2Z9LQFWRVD3TBH
```

Для создания контейнера закрытого ключа genpsk запускается с параметром **–f CreateBasePSK**:

```
[-f CreateBasePSK] [-k <Container>] [-p <PIN>] [-m <time to live>]
```

Пример:

```
genpsk -D TestNet -n 02.06.11 -f CreateBasePSK -k MainCont -p 123456 -m 6
```

Для удаления контейнера закрытого ключа genpsk запускается с параметром **–f DeleteBasePSK**:

```
[-f DeleteBasePSK] [-k <Container>] [-p <PIN>] [-m <time to live>]
```

Пример:

```
genpsk -f DeleteBasePSK -k MainCont -p 123456
```

Для проверки PSK genpsk нужно запустить с параметром **–f chkpsk**:

```
[-f chkpsk] [-n <PSKId>] [-D <NetName>] [-v <Version>] [-K <checking PSK>] [-N <Stations
List>]
```

-K <checking PSK> Значение проверяемого PSK

Пример:

```
genpsk -n 02.06.18 -D TestNet -v 2 -f chkpsk -K FPH90HEKY2WDWPR1W2VLAZD603C1 -N ForOffice
```

```
PSK FPH90HEKY2WDWPR1W2VLAZD603C1 OK, TTL_EXPIRED: UTC Fri Dec 01 00:00:00 2018
```

5.2 Сертификаты открытого ключа

Запрос, выпуск, распространение, плановая схема сертификатов и действия при компрометации определяются установленными регламентами ИОК (УЦ) в ИС.

Все сертификаты должны соответствовать стандарту X.509. Кроме того, в зависимости от назначения к сертификату предъявляются дополнительные требования. При использовании одного сертификат для разных назначений требования к нему совмещаются.

Сертификаты IPsec (аутентификация компьютера в IKE) должны удовлетворять следующим требованиям:

- находиться в хранилище Личное локального компьютера с привязкой к закрытому ключу (рис. 6);
- быть действительными (рис. 6);
- содержать назначение **«IKE-посредник IP-безопасности»** (1.3.6.1.5.5.8.2.2) (рис. 7);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись» (рис. 7);
- содержать открытый ключ ГОСТ Р 34.10-2012, для которого имеется соответствующий контейнер закрытого ключа компьютера с кэшированным паролем или без пароля (рис. 8).

Сертификаты могут применяться при проверке подлинности пользователя в VPN-подключениях с использованием протоколов EAP-TLS, PEAP. В зависимости от типа проверки подлинности, настроенного для метода проверки подлинности, сертификаты используются для проверки подлинности клиента и сервера или только сервера.

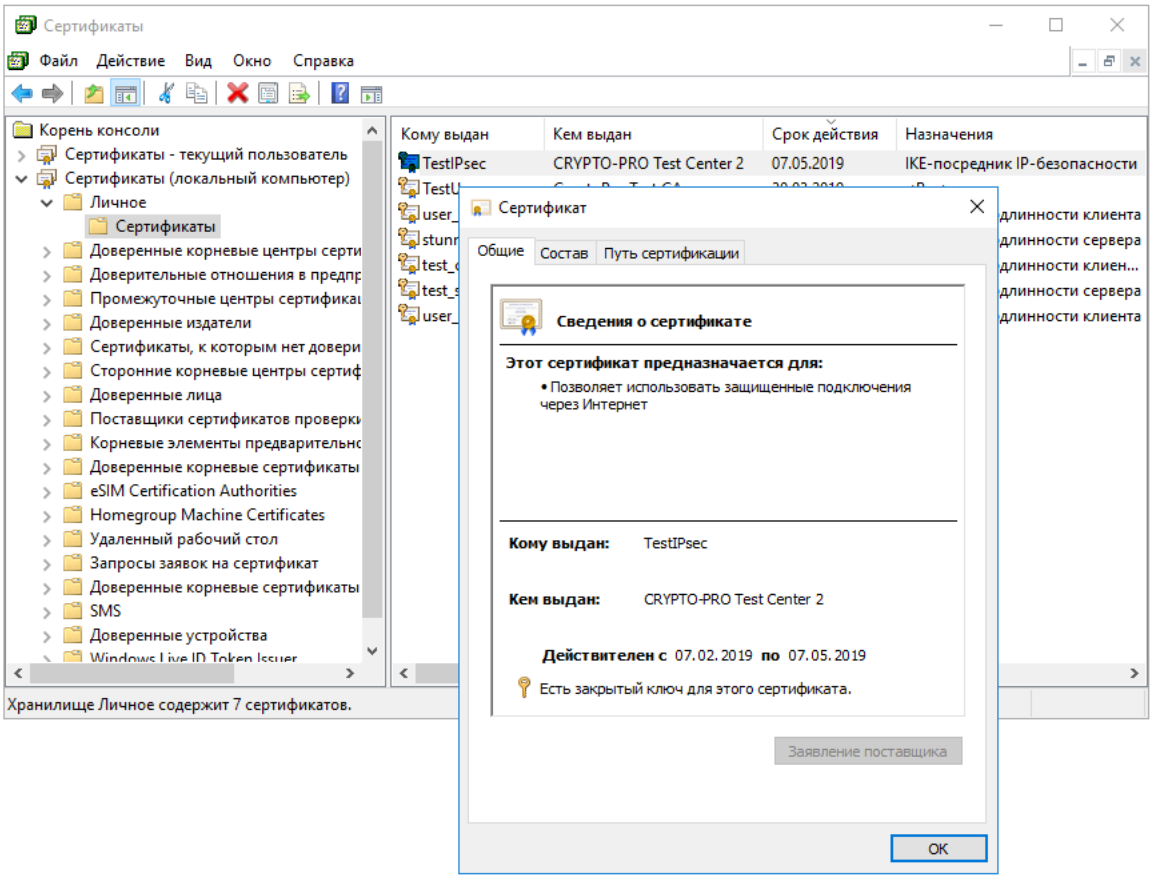

Рисунок 5. Сертификат в хранилище Личное локального компьютера

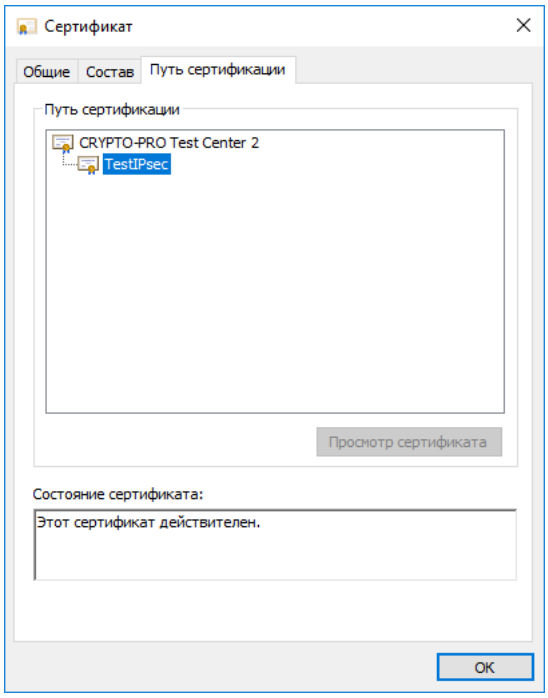

Рисунок 6. Действительный сертификат

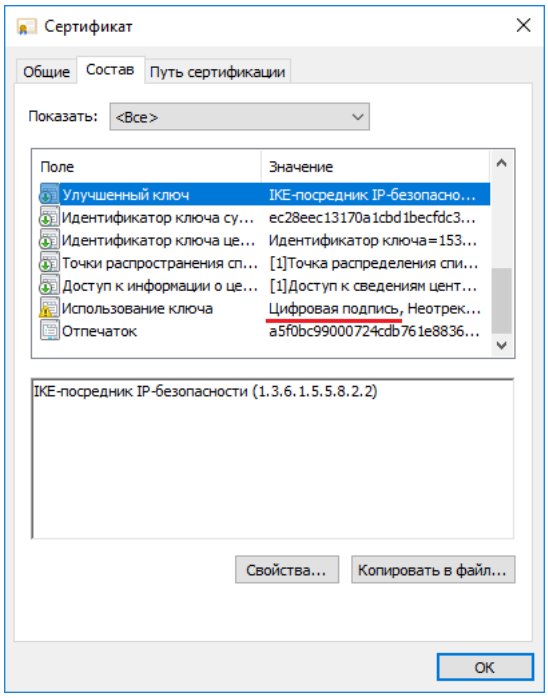

Рисунок 7. Назначение сертификата

Сертификаты аутентификации клиента должны удовлетворять следующим требованиям:

- находиться в хранилище Личное локального компьютера с привязкой к закрытому ключу;
- быть действительными;
- содержать назначение **«Проверка подлинности клиента»** (1.3.6.1.5.5.7.3.2);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись»;
- содержать открытый ключ ГОСТ Р 34.10-2012, для которого имеется соответствующий контейнер закрытого ключа пользователя с кэшированным паролем или без пароля.

Сертификаты аутентификации сервера должны удовлетворять следующим требованиям:

- находиться в хранилище Личное локального компьютера с привязкой к закрытому ключу компьютера;
- быть действительными;
- содержать назначение **«Проверка подлинности сервера»** (1.3.6.1.5.5.7.3.1);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись»;
- содержать открытый ключ ГОСТ Р 34.10-2012, для которого имеется соответствующий контейнер закрытого ключа компьютера с кэшированным паролем или без пароля.

Возможно использование смарт-карт для хранения ключей аутентификации пользователя.

Сертификаты аутентификации по смарт-карте должны удовлетворять следующим требованиям:

- находиться в контейнере по умолчанию на одной из поддерживаемых КриптоПро CSP смарт-карте, подключенной к поддерживаемому считывателю;
- быть действительными;
- содержать назначение **«Вход со смарт-картой»** (1.3.6.1.4.1.311.20.2.2.);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись»;
- содержать открытый ключ ГОСТ Р 34.10-2012.

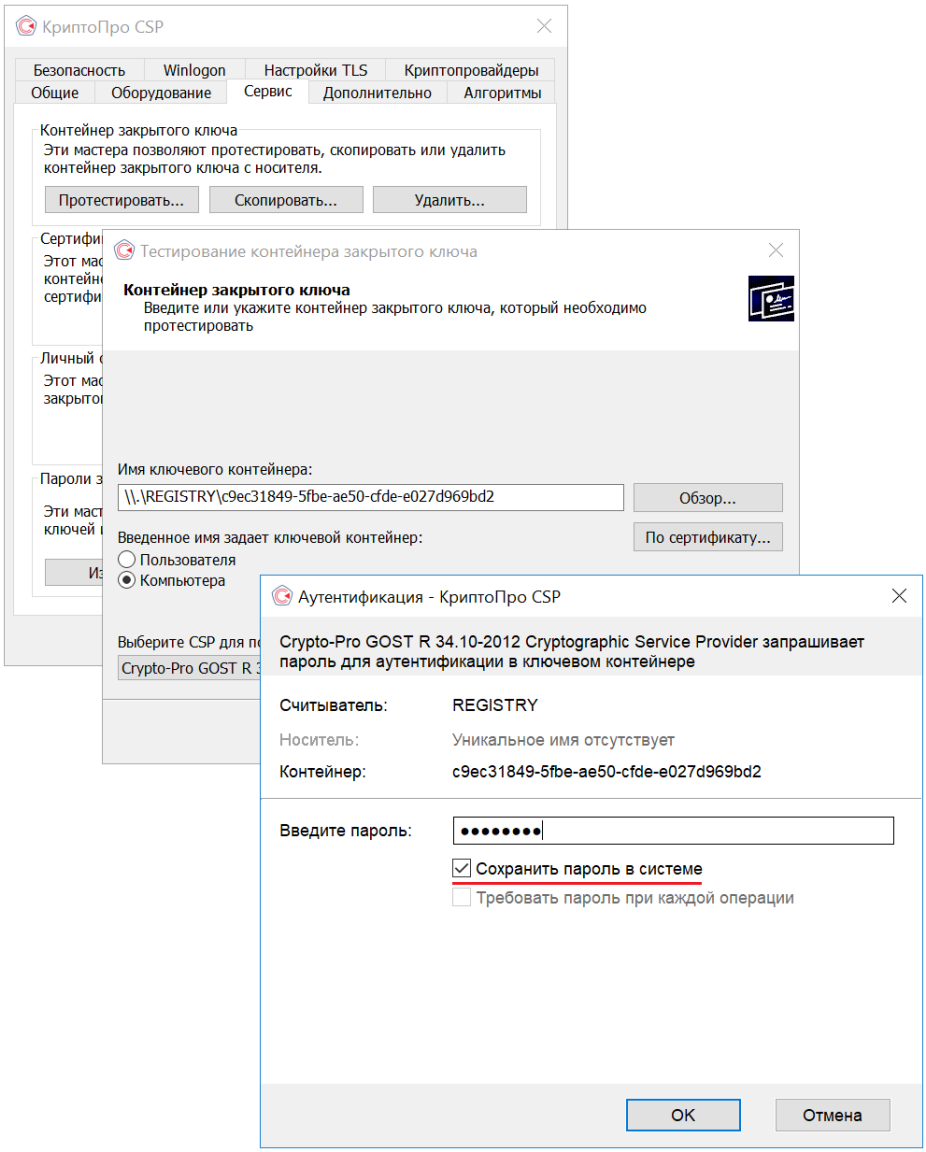

Рисунок 8. Кэширование пароля на контейнер закрытого ключа

6 Установка КриптоПро IPsec

Для начала установки КриптоПро IPsec запустите MSI-пакет, соответствующий используемой ОС. Откроется Мастер установки КриптоПро IPsec (см. рис. 9). Нажмите кнопку **Далее**.

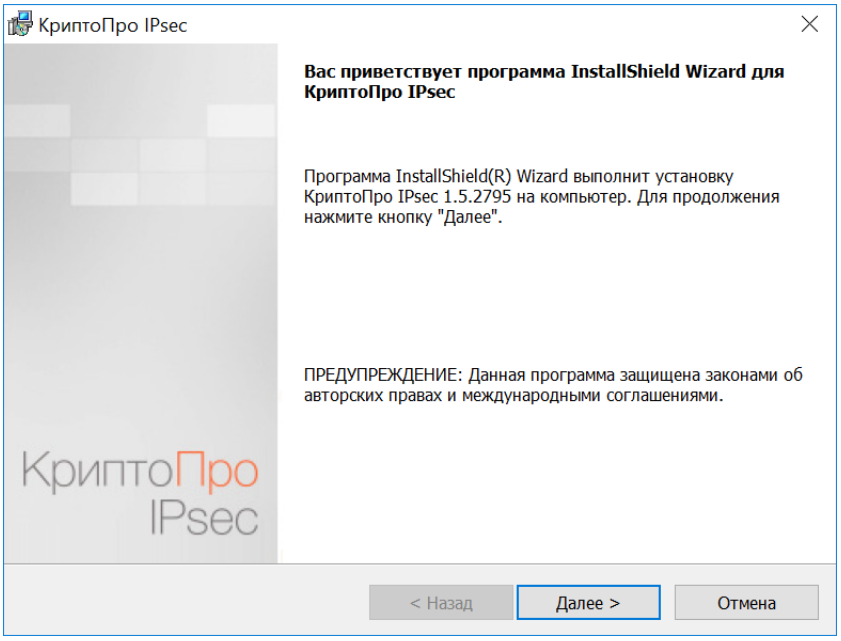

Рисунок 9. Мастер установки КриптоПро IPsec

Примечание. Перед началом установки КриптоПро IPsec необходимо установить КриптоПро CSP (в частности, должны быть установлены компоненты «Расширенная совместимость с продуктами Microsoft» и «Криптопровайдер уровня ядра ОС»). При попытке установки КриптоПро IPsec без установленного КриптоПро CSP отобразиться окно с предупреждением о невозможности установки (см. рис. 10).

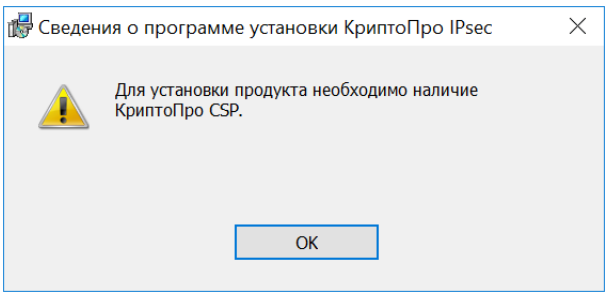

Рисунок 10. Ошибка установки КриптоПро IPsec

В следующем окне мастера установки внимательно ознакомьтесь с лицензионным соглашением на использование КриптоПро IPsec. Если Вы согласны со всеми пунктами соглашения, выделите пункт **Я принимаю условия лицензионного соглашения**, и нажмите **Далее** (см. рис. 11).

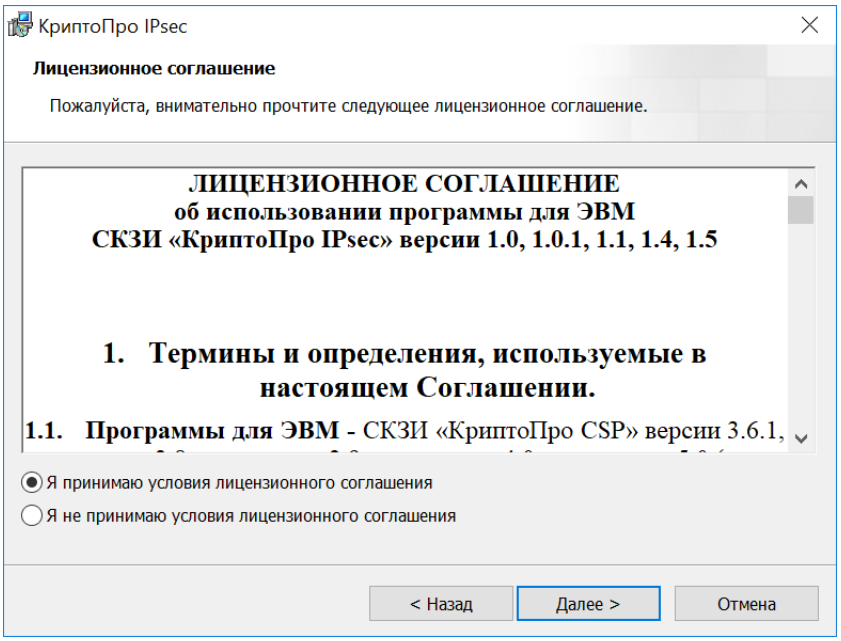

Рисунок 11. Лицензионное соглашение

В следующем окне выберите вид установки программы (см. рис. 12). Возможны два вида установки: полная и выборочная. Использование выборочной установки позволяет сменить папку для установки.

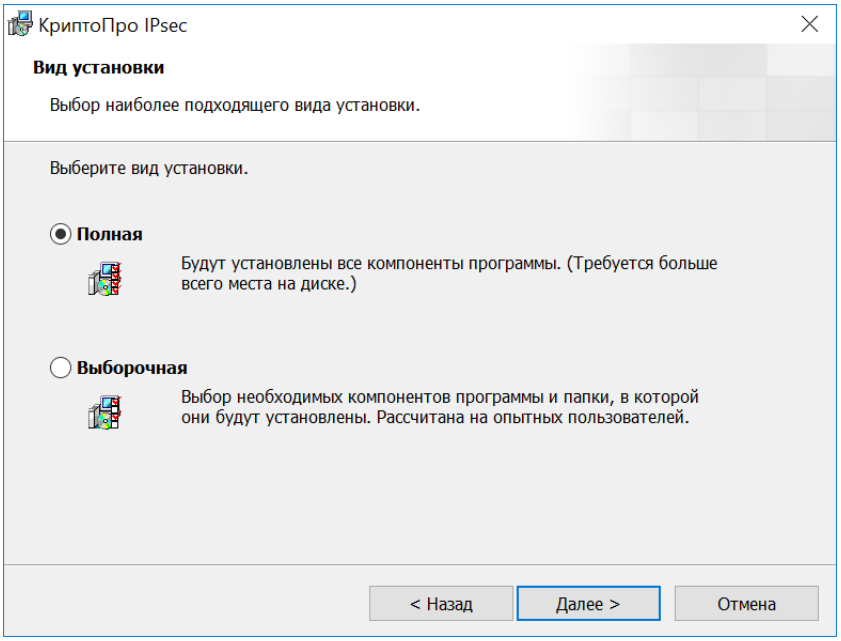

Рисунок 12. Вид установки

Для установки КриптоПро IPsec необходимо наличие компонентов КриптоПро CSP «Расширенная совместимость с продуктами Microsoft» и «Криптопровайдер уровня ядра ОС». Если данные компоненты отсутствуют, то продолжить установку КриптоПро IPsec невозможно. Чтобы автоматически установить данные компоненты, нажмите на кнопку **Настроить КриптоПро CSP** (см. рис. 13).

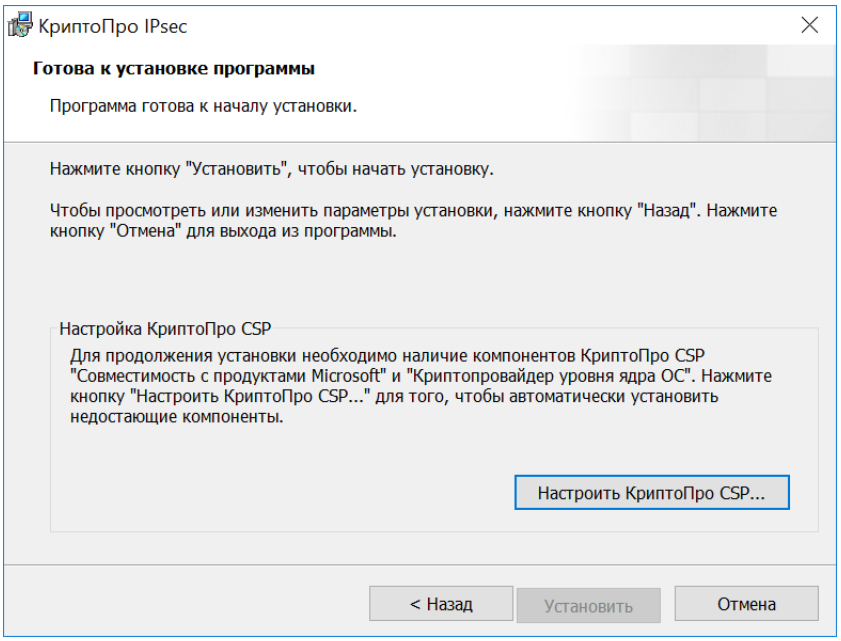

Рисунок 13. Установка отсутствующих компонентов КриптоПро CSP

Если все необходимые компоненты КриптоПро CSP установлены, для подтверждения установки КриптоПро IPsec нажмите кнопку **Установить** (см. рис. 14).

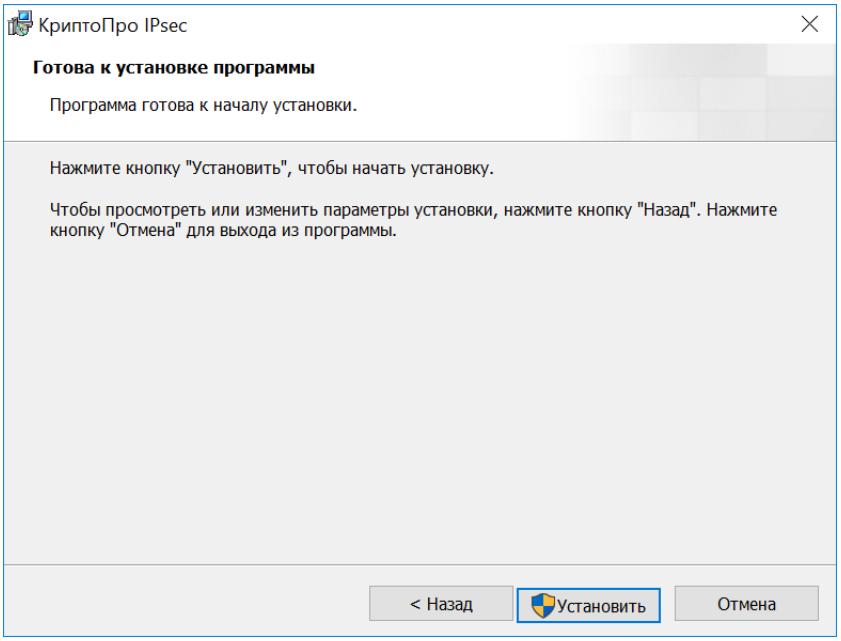

Рисунок 14. Подтверждение установки

В окне Мастера установки будет отображено текущее состояние процесса установки КриптоПро IPsec (см. рис. 15).

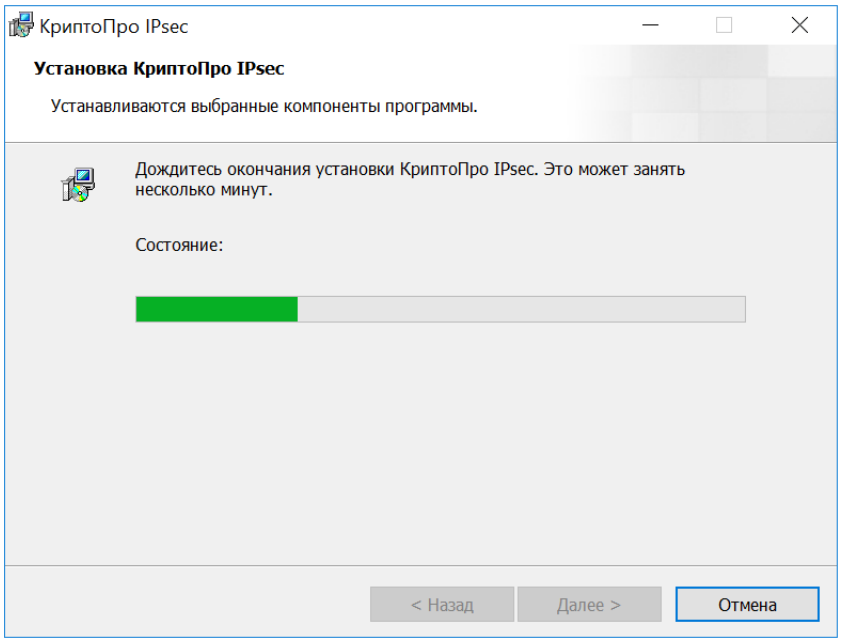

Рисунок 15. Процесс установки

В случае успешной установки всех компонентов КриптоПро IPsec будет отображено окно завершения работы Мастера установки. Нажмите кнопку **Готово** для выхода из программы (см. рис. 16).

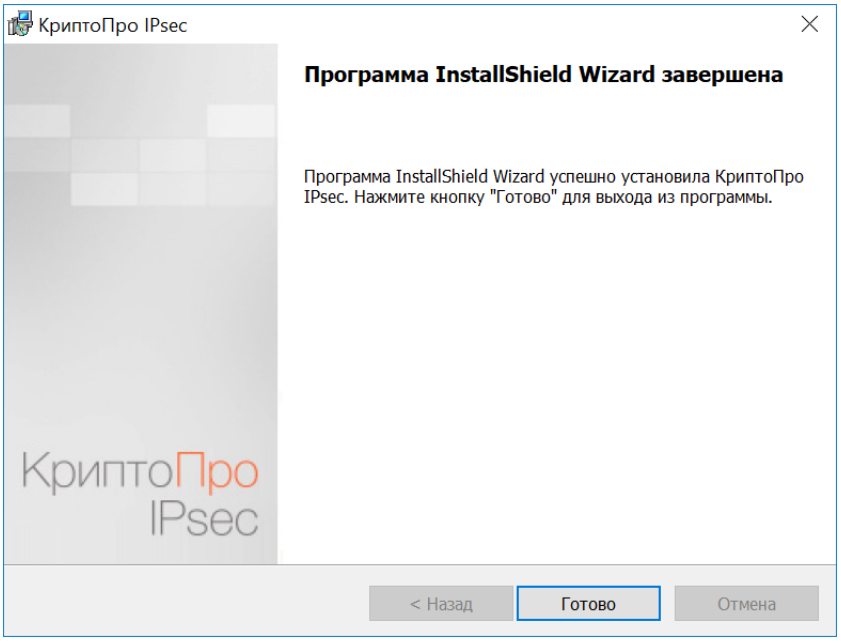

Рисунок 16. Завершение установки

Если программой установки будет предложена перезагрузка компьютера (см. рис. 17), нажмите кнопку **Да** для корректного завершения установки и применения изменений в настройках ОС.

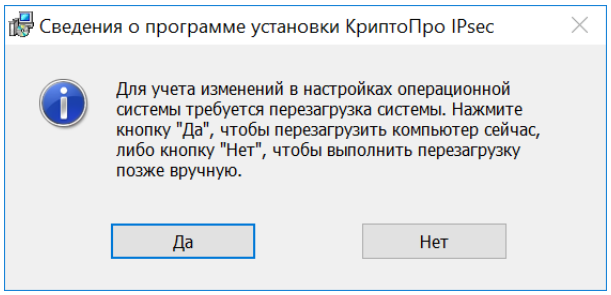

Рисунок 17. Подтверждение перезагрузки компьютера после установки

7 Настройка и мониторинг КриптоПро IPsec

Под первичной настройкой понимается настройка IPsec средствами ОС, не включающей понятия КриптоПро IPsec. Предполагается, что администратор проводит данную настройку самостоятельно до установки КриптоПро IPsec на основе знаний об IPsec в ОС.

Статическая настройка заключается в управлении набором неизменяемых при активной работе параметров КриптоПро IPsec, сюда включаются набор параметров алгоритмов и способ аутентификации.

Динамическая настройка подразумевает управление набором изменяемых в процессе работы параметров, включая управление мандатным шифрованием и лицензией.

В мониторинг, помимо средств мониторинга IPsec в ОС, включено приложение для просмотра общего состояния КриптоПро IPsec, информации об ошибках и состояния соединений КриптоПро IPsec (`%ProgramFiles%\Crypto Pro\IPsec\cp_ipsec_info.exe`).

7.1 Настройка параметров фильтра драйвера

Настройка параметров КриптоПро IPsec осуществляется с помощью приложения `cp_ipsec_info` (по умолчанию устанавливается в `%ProgramFiles%\Crypto Pro\IPsec`).

Запустите приложение `cp_ipsec_info` от имени администратора. После запуска в правом нижнем углу Панели задач Windows появится значок КриптоПро IPsec (см. рис. 18).

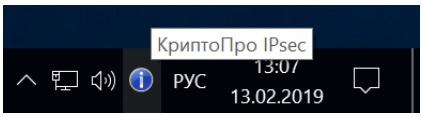

Рисунок 18. Доступ к настройкам КриптоПро IPsec

Примечание. В случае запуска приложения cp_ipsec_info от имени пользователя выбор протоколов, участвующих в фильтрации, и настройка параметров недоступна (см. рис. 19).

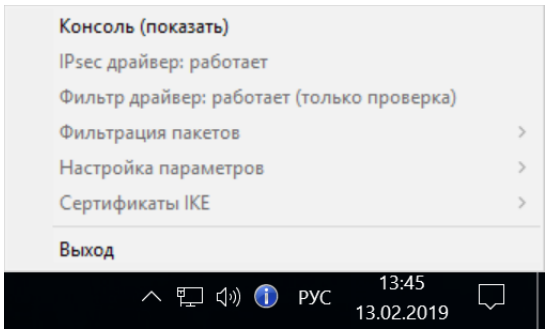

Рисунок 19. Окно КриптоПро IPsec в режиме пользователя

Нажмите на значок КриптоПро IPsec. В открывшемся окне отображаются сообщения о статусе работы драйвера IPsec и фильтра драйвера (см. рис. 20).

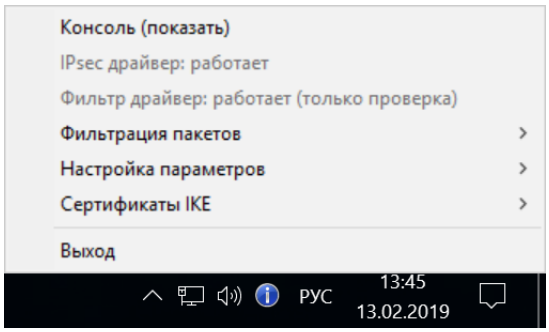

Рисунок 20. Меню КриптоПро IPsec

При нормальной работе драйвера IPsec отображается сообщение **«IPsec драйвер: работает»**. Если появляется сообщение **«IPsec драйвер: НЕ работает»**, проверьте, хватает ли памяти для максимального числа запущенных ESP-сессий, иначе драйвер не установлен.

Фильтр драйвер обеспечивает фильтрацию всех исходящих IPv4 пакетов, а также возможность исключения из фильтрации пакетов, передаваемых по протоколам UDP 500, UDP 4500, DHCP, SMB, DNS, Kerberos.

Если фильтрация пакетов фильтр драйвером отключена, статус фильтр драйвера будет **«Фильтр драйвер: работает (только проверка)»**. В таком состоянии он проверяет только исходящие ESP-пакеты, обрабатываемые с помощью алгоритма шифрования ГОСТ 28147-89, блокирует их, если проверка не прошла, остальные пакеты фильтр пропускает.

Для защиты конфиденциальной информации необходимо включить фильтрацию пакетов. При этом фильтр будет проверять исходящие ESP-пакеты, обрабатываемые с помощью алгоритма шифрования ГОСТ 28147-89, блокировать их, если проверка не прошла, и блокировать все остальные пакеты (кроме исключений, см. ниже).

Для включения фильтрации пакетов перейдите в меню **Фильтрация пакетов**. Затем нажмите кнопку **Включена**.

Статус работы фильтр драйвера изменится на **«Фильтр драйвер: работает»**.

Выберите в меню необходимые исключения (см. рис. 21). В этом случае передача пакетов, попадающих в исключения, не будет блокироваться фильтром. По умолчанию в исключения внесены порты, использующиеся протоколами согласования ключей (IKE) и базовыми протоколами сети DHCP и DNS.

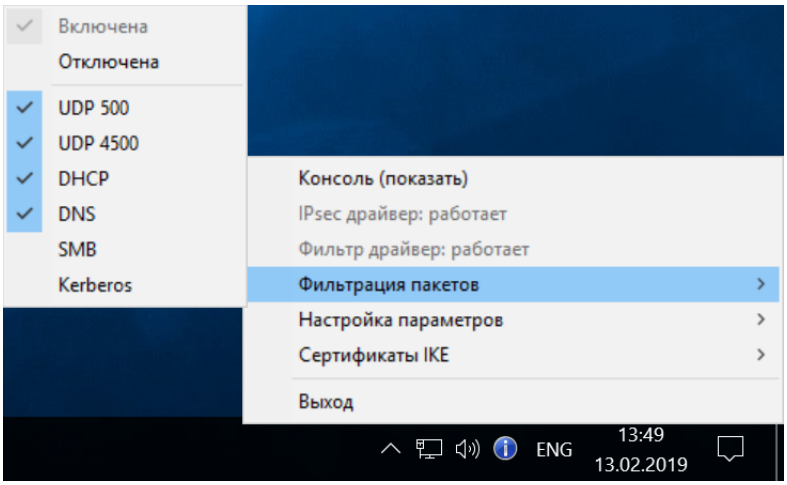

Рисунок 21. Настройка фильтрации пакетов

7.2 Настройка параметров протоколов IKE, ESP

Настройка параметров протоколов IKE и ESP осуществляется при помощи меню **Настройка параметров** (см. рис. 22).

Доступны следующие опции:

- Максимальное число ESP-сессий — необходимое количество ESP-сессий, при этом не должно использоваться более 2 Гб памяти (значение указано в скобках).
- IKE шифрование — набор параметров шифрования протокола IKE.
- IKE хэш — алгоритм хэширования с предустановленным набором параметров.
- IKE группа — группа точек эллиптических кривых.
- IKE PFS-контроль — включение/выключение обязательной отправки PFS ответчику.
- IKE группа (PFS) — значение устанавливается в зависимости от значения параметра IKE PFS-контроль в согласовании с ответчиком.
- ESP Combined Mode — включение/выключение отправки Authentication Algorithm (5) — признак, указывающий на используемое комбинированное преобразование ESP_GOST-4M-IMIT или ESP_GOST-1K-IMIT.
- ESP ESN — включение/выключение использования ESN (64-битный номер пакета).
- ESP узлы замены — набор параметров шифрования протокола ESP.

Все настройки параметров фильтр драйвера сохраняются в реестр Windows. При необходимости администратор может распространить эти настройки, добавив их из реестра Windows в групповую политику.

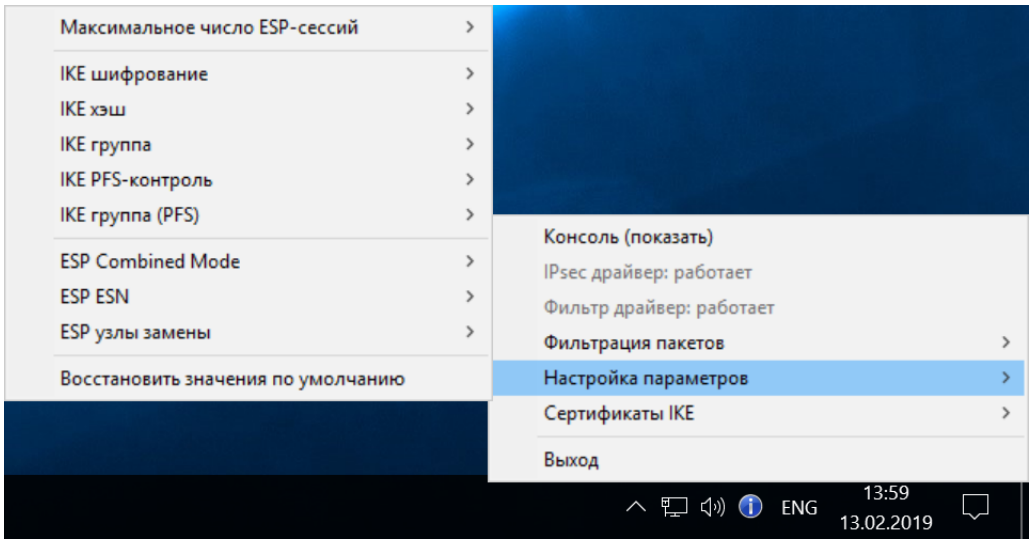

Рисунок 22. Настройка параметров протоколов IKE, ESP

7.3 Особенности настройки свойств протокола IPsec

7.3.1 Режимы защиты конфиденциальности, целостности, аутентификации

При выборе используемых алгоритмов защиты информации в канале связи используется режим защиты конфиденциальности (ESP с шифрованием) и целостности (ESP с контролем целостности) передаваемой информации. Администратор обеспечивает настройку одного из двух комбинированных преобразований: ESP_GOST-4M-IMIT (используется по умолчанию) и ESP_GOST-1K-IMIT (настраивается опционально).

Для настройки преобразований необходимо открыть свойства групповой политики **Политика IP-безопасности**, перейти на вкладку **Правила**, двойным нажатием левой кнопкой мыши открыть необходимое правило, перейти на вкладку **Действие фильтра** и открыть свойства действия фильтра по кнопке Изменить или двойным нажатием левой кнопкой мыши (см. рис. 23).

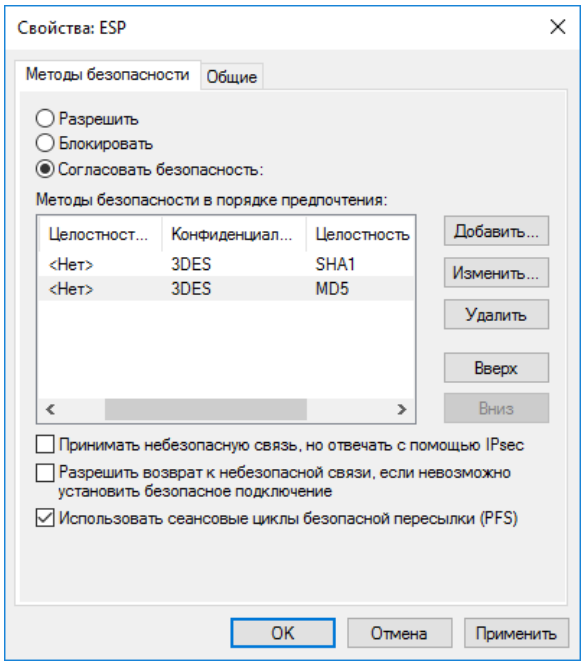

Рисунок 23. Свойства ESP

Для шифрования, контроля целостности и взаимной аутентификации используются алгоритмы ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018).

При выборе в окне **Свойства: ESP** алгоритма целостности SHA1 в действительности используется комбинированное преобразование ESP_GOST-4M-IMIT, при выборе MD5 — преобразование ESP_GOST-1K-IMIT.

Для аутентификации администратором обеспечивается настройка одного из двух алгоритмов: IKE-GOST-SIGNATURE или IKE-GOST-PSK. Для использования алгоритма IKE-GOST-SIGNATURE необходимо выбрать метод проверки подлинности «Центры сертификации», для использования алгоритма IKE-GOST-PSK — «Предварительный ключ» (см. рис. 24).

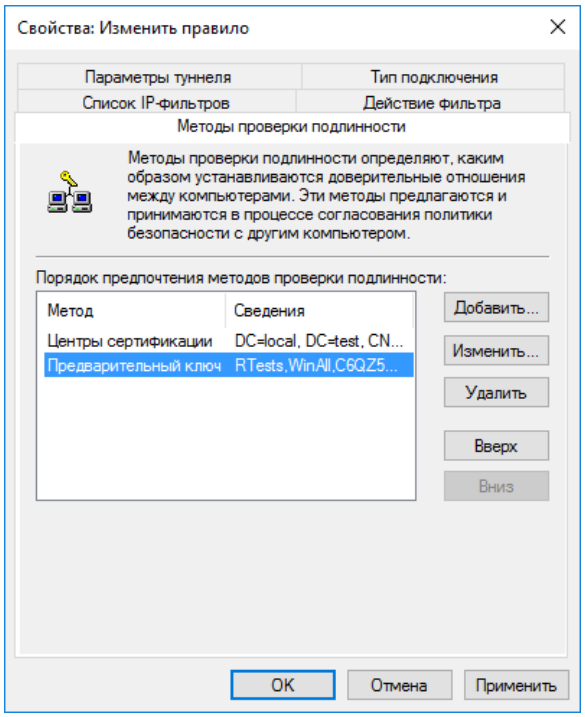

Рисунок 24. Выбор алгоритма аутентификации

7.3.2 Свойства параметров протокола

• Значение максимального размера ESP-вложения не настраивается администратором и равняется значению по умолчанию.

• Администратор может настроить время жизни Ассоциации безопасности (SA), максимальное значение — 8 часов.

• Администратор не имеет возможности настройки максимального значения счетчика неаутентифицированных пакетов, максимальное значение счетчика — 10^5. При исчерпании счетчика неаутентифицированных пакетов прием пакетов в рамках SA блокируется.

• Администратор не имеет возможности непосредственной настройки максимального количества сессий второй фазы. Администратор может только определить политику — либо «без режима PFS», либо «только режим PFS». При выборе политики «Без режима PFS» количество сессий второй фазы не может превышать 10^4.

8 Использование КриптоПро IPsec

В данном разделе рассмотрены базовые варианты использования КриптоПро IPsec в подготовленной сетевой доменной инфраструктуре с организованной ИОК.

Для выпуска сертификатов развернута двухуровневая структура центров сертификации (см. рис. 25).

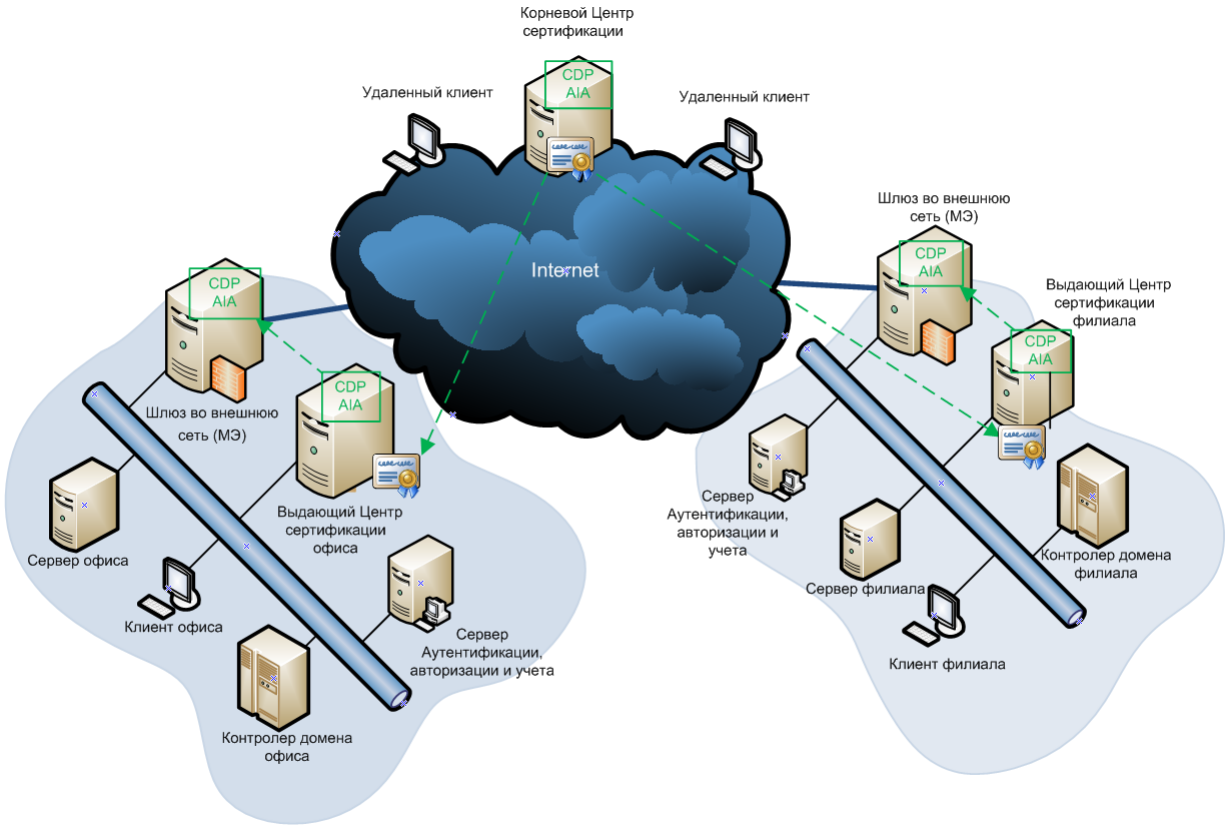

Рисунок 25. Инфраструктура открытых ключей

Изолированный Корневой центр сертификации расположен во внешней сети. Проверка статуса сертификата происходит по спискам отозванных сертификатов (Certificate Revocation List, CRL). Доступ к точкам распространения списков отозванных сертификатов (CRL Distribution Points, CDP) не требует аутентификации (см. рис. 26).

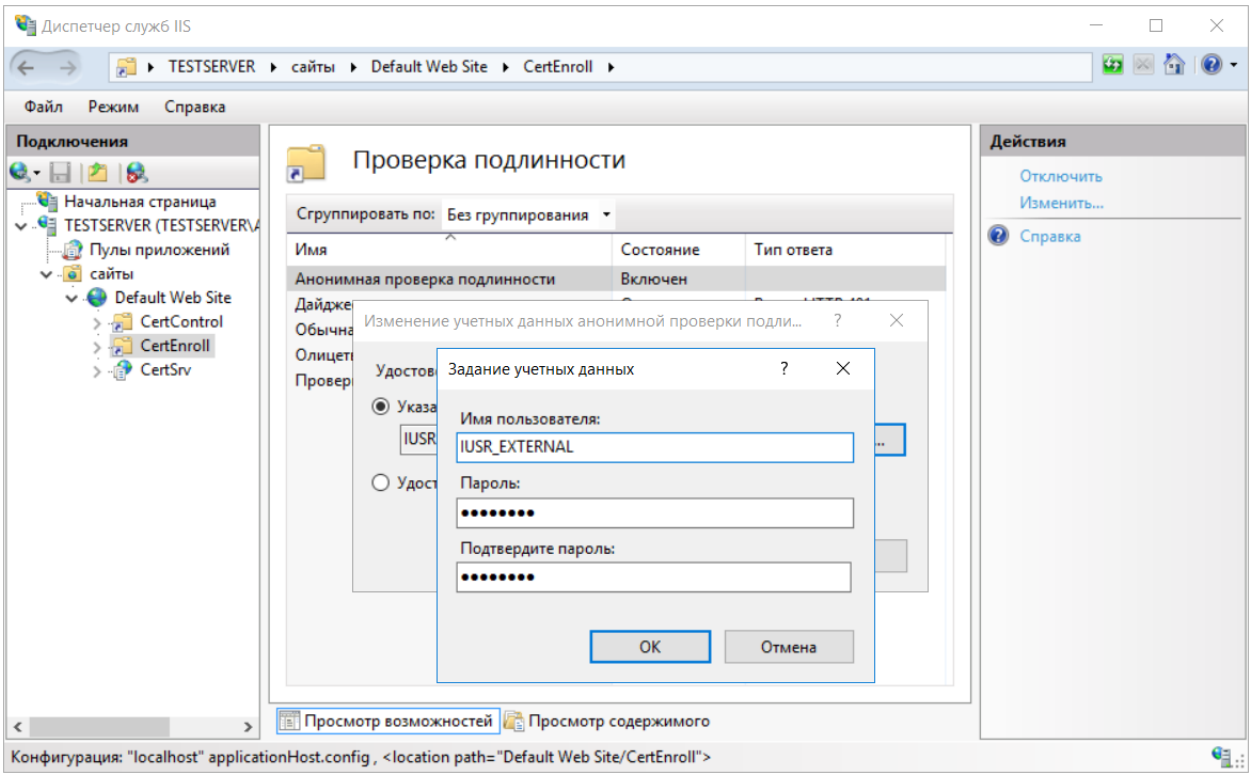

Рисунок 26. Анонимный доступ к CRL в IIS

Подчиненные выпускающие центры сертификации развернуты во внутренних сетях в домене. Проверка статуса сертификата происходит по спискам отзыва, которые доступны без аутентификации. Для удаленных клиентов (сетей) списки отзыва и сертификаты выпускающих центров опубликованы на МЭ (шлюз) во внешнюю сеть.

В домене доверие к корневому сертификату изолированного центра настраивается с помощью групповых политик: **Имя_объекта_политики** ⟶ **Конфигурация компьютера** ⟶ **Конфигурация Windows** ⟶ **Параметры безопасности** ⟶ **Политики открытого ключа** ⟶ **Доверенные корневые центры сертификации.**

Для доменных пользователей и компьютеров выпуск сертификатов производится из оснастки **Microsoft Management Console (MMC)** ⟶ **Сертификаты (пользователя, компьютера)** по шаблонам доменного центра сертификации.

Сертификаты IPsec выпускаются по копии базового шаблона «IPsec», где в качестве поставщика шифрования выбран один из криптопровайдеров КриптоПро CSP (см. рис. 27).

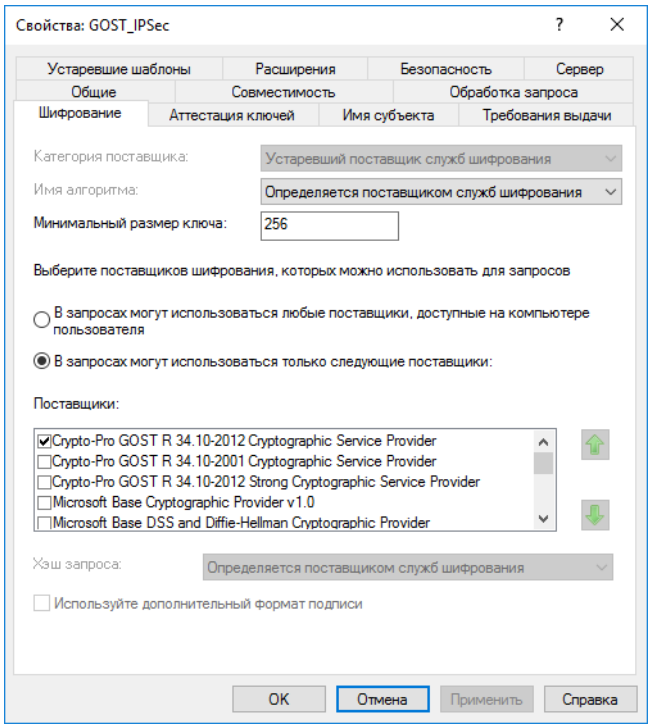

Рисунок 27. Шаблон сертификата для IPsec

В домене выпуск сертификатов клиентской аутентификации происходит по копии шаблона «Пользователь» с криптопровайдером КриптоПро CSP. Выпуск сертификатов аутентификации сервера (VPN-аутентификация) происходит по копии шаблона по умолчанию «RAS и IAS-серверы» с криптопровайдером КриптоПро CSP.

На компьютерах, не являющихся членами домена, невозможно пользоваться описанным выше методом выпуска сертификатов (**MMC** $\longrightarrow$ **Сертификаты** $\longrightarrow$ **Шаблоны AD**). Методы распространения (запрос, выпуск, установка, обновление) сертификатов определяется Администратором. В данных примерах сертификаты для удаленных клиентов создаются с помощью веб-интерфейса пользователя УЦ.

Установка личных сертификатов производится согласно «ЖТЯИ.00101-01 92 01. КриптоПро CSP. Инструкции по использованию», п. 2.5.3. «Установка личного сертификата, хранящегося в файле».

Выпуск сертификатов в КриптоПро УЦ

Для выпуска сертификатов IPsec необходимо произвести настройку КриптоПро ЦР и КриптоПро ЦС (см. «ЖТЯИ.00078-01 90 03. ПАК КриптоПро УЦ 2.0. Руководство по эксплуатации»):

- создать шаблон сертификата с OID «IKE-посредник IP-безопасности» (1.3.6.1.5.5.8.2.2);
- добавить в Политики ЦР разрешение на обработку запроса и отзыв сертификата, содержащего OID «IKE-посредник IP-безопасности» (1.3.6.1.5.5.8.2.2);
- добавить в Модуль политики КриптоПро ЦС Использование ключа «IKE-посредник IP-безопасности» (1.3.6.1.5.5.8.2.2).

Для выпуска сертификатов аутентификации сервера необходимо произвести настройку КриптоПро ЦР:

- создать шаблон сертификата с OID «Проверка подлинности сервера» (1.3.6.1.5.5.7.3.1);
- добавить в Политики ЦР разрешение на обработку и отзыв сертификата.

Для выпуска сертификатов аутентификации клиента необходимо указать UPN пользователя и использовать шаблон, содержащий назначение «Проверка подлинности клиента» (1.3.6.1.5.5.7.3.2).

Организация основных методов (централизованны, распределенный) распространения сертификатов описана в «ЖТЯИ.00078-01 90 03. ПАК КриптоПро УЦ 2.0. Руководство по эксплуатации».

Аутентификация, авторизация и учет

Во время VPN-подключения после выработки IPsec SA (между компьютерами) происходит пользовательская аутентификация, авторизация, и учет информации об этом. Сервера АА и Учета могут быть развернуты как на VPN-сервере, так и на изолированном RADIUS-сервере. RADIUS обеспечивает централизованную ААУ, что может быть удобно в сложной сетевой структуре с несколькими точками удаленного доступа, в том числе, если VPN-сервер не в домене. В качестве RADIUS-серверов в ОС семейства Windows может выступать служба «Сервера политики сети» (Network Policy Server, NPS).

Для использования RADIUS ААУ на VPN-серверах (RRAS, ISA Server, TMG) необходимо проводить дополнительную настройку (RADIUS-клиента, RADIUS-сервера).

Описание реализации EAP-TLS, PEAP методов аутентификации пользователя по сертификатам опубликовано на странице http://www.cryptopro.ru/products/eap-tls/usage.

8.1 Настройка VPN для безопасного подключения клиента к сети офиса

В данном разделе будет рассмотрен сценарий создания защищенного удаленного подключения пользователя (компьютера пользователя) к сети офиса (см. рис. 28).

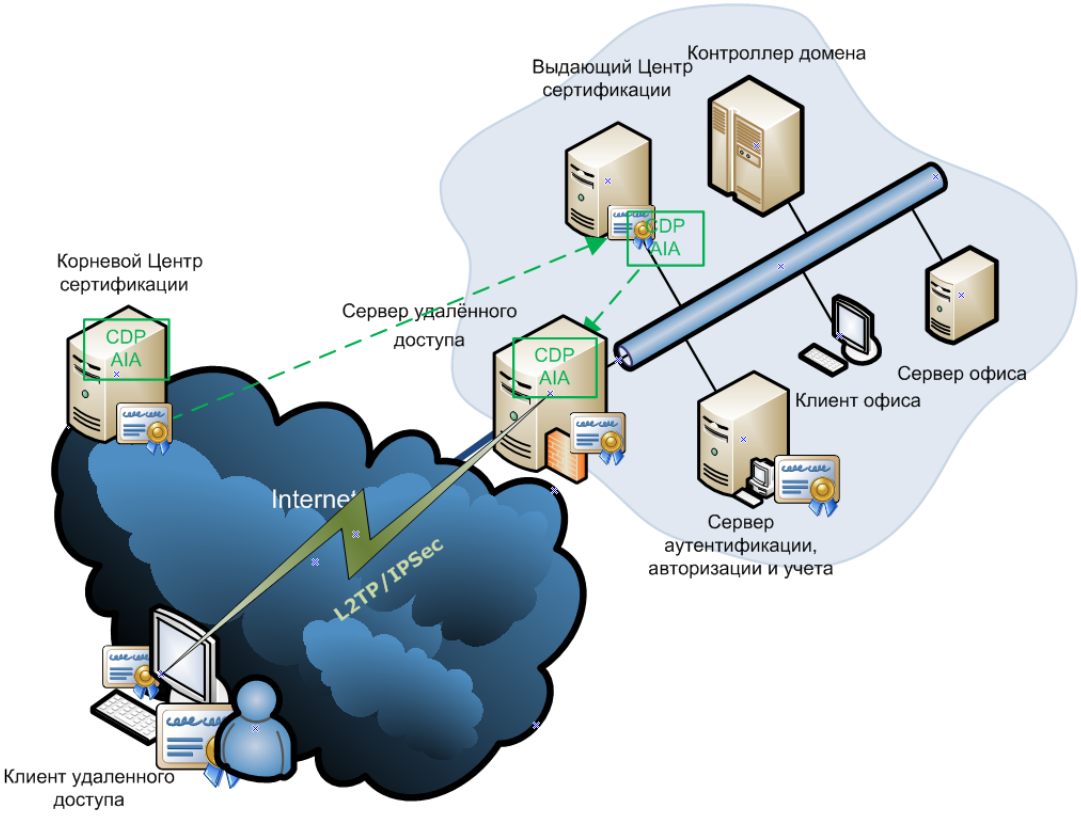

Рисунок 28. Подключение Client-to-Site

Для организации такого решения необходимо выполнить:

- Настройку сервера удаленного доступа(VPN-сервер), состоящую из следующих этапов:
  - выбор протокола удаленного доступа;
  - определение списка IP-адресов, присваиваемых внешним клиентам (DHCP-сервер);
  - настройка правил фильтрации;
  - настройка методов аутентификации, авторизации и учета пользователей;
  - настройка протокола SSTP в качестве резервного;
- Настройку клиента удаленного доступа, включающую:
  - создание VPN-подключения (CMAK или «Мастер новых подключений»).

Допускается доступ к VPN-серверу через Back-to-Back структуру МЭ, например, доступ к внутренней сети через DMZ или «Perimeter network» с двойным NAT.

Сервер удаленного доступа можно настроить с использованием Службы Windows Server RRAS (Routing and Remote Access Server) или развернуть на одном из поддерживаемых МЭ.

Для подключения клиента в удаленную сеть с использованием протокола L2TP/IPsec необходимо в Свойствах Удаленного подключения указать «Тип VPN: Протокол L2TP с IPsec».

При настройке «Тип VPN: Автоматически» запросы на подключение перебираются в следующем порядке: SSTP, L2TP/IPsec, PPTP, пока не будет согласован протокол, поддерживаемый и клиентом и сервером.

На вкладке «Безопасность» VPN-подключения необходимо настроить обязательность шифрования (см. рис. 29).

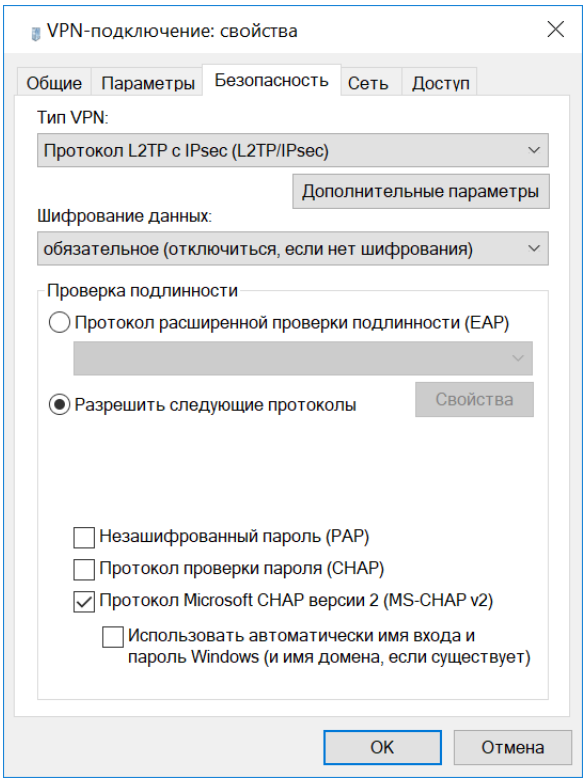

Рисунок 29. Вкладка Безопасность VPN-подключения

PSK используется, если он указан в Свойства, настраиваемого VPN-подключения, в противном случае используется сертификат, удовлетворяющим требованиям IPsec (см. разд. 5.2).

Во время настройки VPN-записи необходимо указать использование протокола L2TP/IPsec (см. рис. 30).

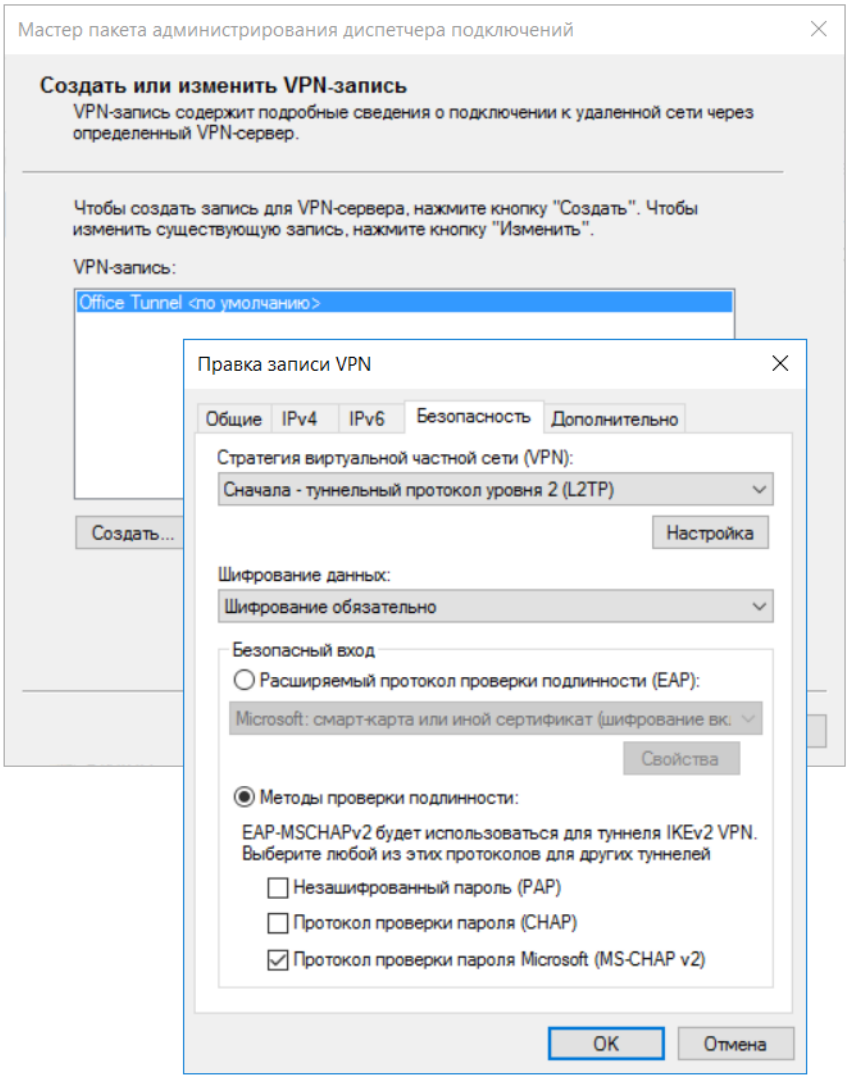

Рисунок 30. Параметры безопасности VPN-записи

Сертификат будет использоваться если не указано «Использовать предварительный ключ для L2TP/IPsec».

Создание профилей подключений пользователей с L2TP/IPsec на PSK требует дополнительных действий. Профиль, созданный с помощью мастера, считается родительским. На его базе создаются профили для конечных пользователей. Для этого необходимо:

- в файле родительского профиля `%ProgramFiles%\Cmak\Profiles\Имя_профиля\Имя_профиля.sed` указать актуальный путь к файлу установщика профилей **cmstp.exe** (файл **cmstp.exe** находится в пакете `%ProgramFiles%\Cmak\Support\cmbins.exe`);
- скопировать файлы `%ProgramFiles%\Crypto Pro\IPsec\cpcmak_builder.exe`, `%ProgramFiles%\Crypto Pro\IPsec\cpcmak_cpacker.exe`, `%ProgramFiles%\Crypto Pro\IPsec\genpsk.exe` в директорию родительского профиля `Program-Files%\Cmak\Profiles\Имя_профиля`;
- создать текстовый файл с конечными пользователями. Первая строка в этом файле должна соответствовать следующим 4 сущностям разделенным пробелами: ИмяОфиса(ИлиДомена) ИмяСети ИмяКонтейнера ПинКонтейнера (эти параметры будут использоваться для генерации PSK (см. разд. 5.1). В остальных строках задаются имена пользователей.

Пример:
TestNet ForClient MainCont 12345678
mDima
Sergei
Ivan
bDima

• запустить **cpcmak_builder.exe** , используя в качестве одного параметра файл (полный путь в кавычках) с пользователями (созданный на предыдущем шаге);

Процесс заканчивается созданием исполняемых и текстовых файлов с паролями для каждого пользователя.

Способы распространение, передачи исполняемого файла профиля определяются администратором.

Создание VPN-подключения происходит после запуска файла профиля. Если использовались PSK, то будет запрошен пароль соответствующего пользователя (созданный во время запуска **cpcmak_builder.exe**).

8.2 Настройка Site-to-Site

В данном разделе будет рассмотрен сценарий создания защищенного соединения сетей, подключенных к сетям общего пользования (см. рис. 31).

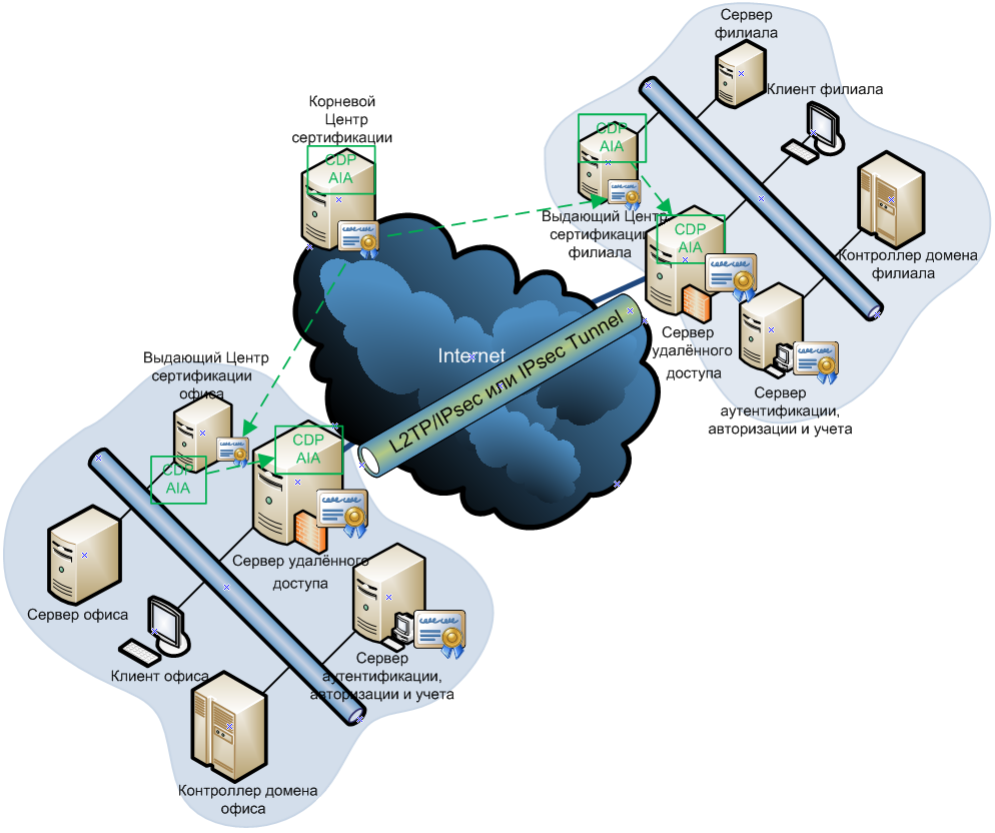

Рисунок 31. Подключение Site-to-Site

Для организации такого решения необходимо выполнить следующие настройки VPN-шлюзов сетей партнеров:

• выбор протокола удаленного доступа;

- настройка правил маршрутизации;
- настройка правил IP-фильтрации;
- настройка методов аутентификации, авторизации и учет site-to-site подключений.

Допускается VPN-соединений сетей по схеме site-to-site с применением двух типов протоколов: IPsec-tunnel и L2TP/IPsec. IPSec в туннельном режиме целесообразно применять только если необходимо создать канал связи site-to-site с VPN-шлюзами сторонних производителей. Существует несколько причин для отказа от использования IPSec в туннельном режиме:

- IPSec в туннельном режиме менее защищен;
- IPSec в туннельном режиме обладает ограничениями по маршрутизации на компьютерах с системой Windows Server 2003;
- IPSec в туннельном режиме может уменьшить эффективную пропускную способность VPN-туннеля.

Допускается развертывание VPN-туннеля между сетями с Back-to-Back структурой МЭ, например, между DMZ или «Perimeter network» сетями филиала и офиса.

8.3 Изоляция домена

В данном разделе будет описан сценарий настройки IPsec с помощью «Политик IP-безопасности». Применение IPsec в сетевых политиках позволяет криптографически изолировать (на 3-ем уровне модели OSI) как весь домен, так и подразделения, сайты, группы компьютеров и серверов. Рассмотрим частный случай изоляции нескольких компьютеров в домене (см. рис. 32).

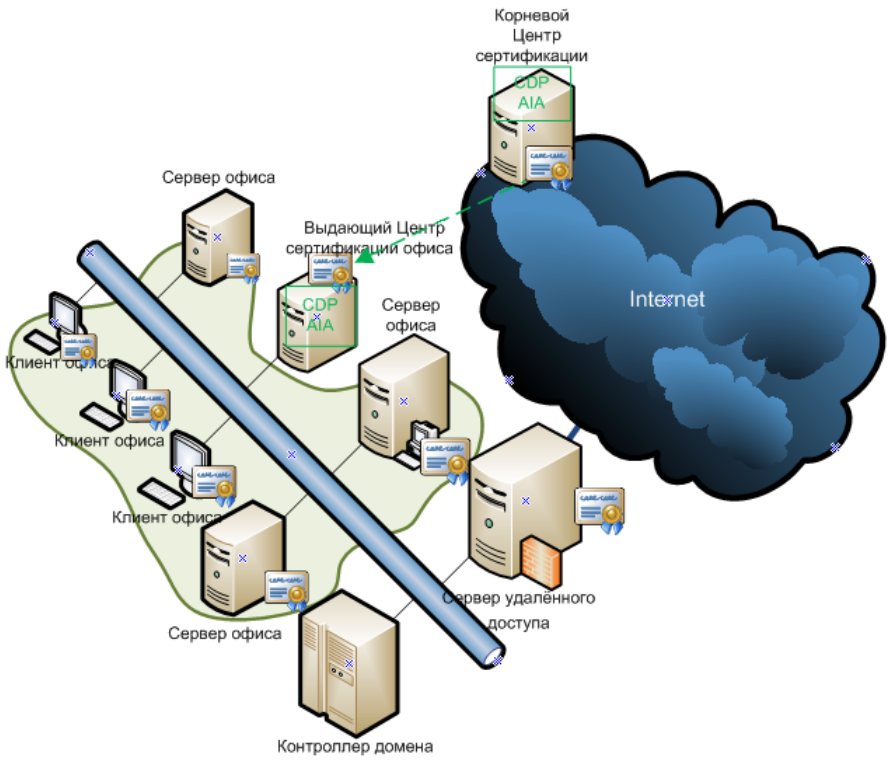

Рисунок 32. Изоляция группы компьютеров в домене

Установка политик безопасности IPsec может выглядеть следующим образом:

- планирование и проектирование. Формирование логических групп безопасности: определение IP-

фильтров, соответствующих компьютерам, подсетям, условиям окружения и необходимые для них действия безопасности;

- создание Политик IPsec, Правил IPsec (фильтры, действия);
- распространение Групповых политик (GPO) IPsec.

При проектировании сложных схем рекомендуется составлять таблицы и диаграммы сетевых подключений. В этом примере будут использованы всего 2 политики, перейдем к их определению без предварительного планирования. Для управления GPO в домене используется «Редактор управления групповыми политиками» (Group Policy Management Console,GPMC). Создаются два объекта групповой политики.

Один GPO назначается компьютерам в группе (в подразделении) исключений: контроллер домена, центр сертификации, DHCP, DNS-сервер. Для них трафик шифроваться не будет. В GPO для исключений создается Политика безопасности, но без Правил безопасности.

Другой GPO привязан ко всему домену. В нем два правила безопасности. Первое Разрешает (действие фильтра) прохождение трафика к группе исключений (фильтр). Второе строго требует шифрование всего трафика (фильтр по умолчанию «All IP Traffic») (см. рис. 33).

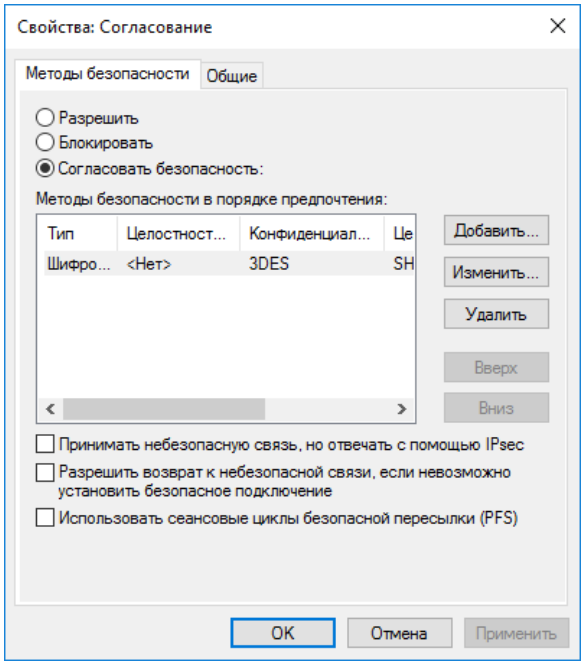

Рисунок 33. Действие фильтра

Применение (замещение) GPO происходит в соответствии с установленными приоритетами групповых политик. Обновляется политика через заданные промежутки времени и при загрузке ОС.

При использование политик для изоляции всего домена (предприятия) без исключений важно помнить:

- о сложности конфигурации и управлении IPSec для защиты соединения между членами домена, контроллерами, DHCP, DNS-серверами, службами распространения ключей;
- IPSec не может согласовывать безопасность для многоадресного и широковещательного трафика;
- о проблемах, которые могут возникать с трафиком связи реального времени и в одноранговых сетях.

Литература

Инструкция Microsoft «Публикация отдельного веб-сайта или системы балансировки нагрузки через HTTP». URL: http://technet.microsoft.com/ru-ru/library/cc441462.aspx

Инструкция Microsoft ««Публикация веб-узла на компьютер под управлением ISA Server 2006 или ISA Server 2004». URL: http://support.microsoft.com/kb/885186

ЖТЯИ.00078-01 90 03. ПАК КриптоПро УЦ 2.0. Руководство по эксплуатации.

Руководство Microsoft «Network Policy Server (NPS) Operations Guide». URL: http://www.microsoft.com/downloads/en/details.aspx?FamilyID=585d2dca-c134-4568-b31c-a535ab0b0b3d&displaylang=en

Документация Microsoft «ISA Server 2004 VPN Deployment Kit». URL: http://technet.microsoft.com/en-us/library/cc302453.aspx

Инструкция Microsoft «Настройка Forefront TMG в качестве клиента RADIUS». URL: http://technet.microsoft.com/ru-ru/library/dd441017.aspx

Инструкция Microsoft «Использование проверки подлинности RADIUS». URL: http://technet.microsoft.com/ru-ru/library/cc778372%28WS.10%29.aspx

Использование КриптоПро EAP-TLS. URL: http://www.cryptopro.ru/products/eap-tls/usage

Инструкция Microsoft «Deploying L2TP/IPSec-based Remote Access». URL: http://technet.microsoft.com/ru-ru/library/cc775490%28WS.10%29.aspx

Инструкция «Роль сервера удаленного доступа или VPN-сервера: настройка сервера удаленного доступа или VPN-сервера». URL: http://technet.microsoft.com/ru-ru/library/cc736357%28WS.10%29.aspx#rrassrvconfig

Инструкция Microsoft «Включение RRAS в качестве VPN-сервера». URL: http://technet.microsoft.com/ru-ru/library/dd458983.aspx

Инструкция Microsoft «Включение базового доступа удаленных клиентов». URL: http://technet.microsoft.com/ru-ru/library/dd897103.aspx

Инструкция Microsoft «Настройка подключения к виртуальной частной сети (VPN) в Windows XP». URL: http://support.microsoft.com/kb/314076

Инструкция Microsoft «Create a VPN connection in Windows Vista and Windows Server 2008». URL: http://technet.microsoft.com/en-us/library/cc726062%28WS.10%29.aspx

Инструкция Microsoft «Создание VPN-подключения». URL: http://technet.microsoft.com/ru-ru/library/cc726062%28WS.10%29.aspx

Инструкция «Мастер пакета администрирования диспетчера подключений». URL: http://technet.microsoft.com/ru-ru/library/cc738870%28WS.10%29.aspx

Инструкция Microsoft «Установка пакета администрирования диспетчера подключений (CMAK)». URL: http://technet.microsoft.com/ru-ru/library/cc771679%28WS.10%29.aspx

Инструкция Microsoft «Этап 2: разработка настраиваемых элементов». URL: http://technet.microsoft.com/ru-ru/library/cc738515%28WS.10%29.aspx

Статья «ISA Server 2006 - IPsec Tunnel Mode Site-to-Site VPN Connections: A Couple of Things That Are Not Supported». URL: http://www.carbonwind.net/ISA/IPsecTunnelModeNotSupportedThings/IPsecTunnelModeNotSupportedThings.htm

Инструкция Microsoft «Creating and Editing GPOs». URL: http://technet.microsoft.com/ru-ru/library/cc782980%28WS.10%29.aspx

Инструкция Microsoft «Создание и изменение объекта групповой политики». URL: http://technet.microsoft.com/ru-ru/library/cc754740%28WS.10%29.aspx

Инструкция Microsoft «Добавление, изменение и удаление политик IPSec». URL: http://technet.microsoft.com/ru-ru/library/cc778422%28WS.10%29.aspx

Статья Microsoft «Обработка и приоритеты групповых политик». URL: http://technet.microsoft.com/ru-ru/library/cc785665%28WS.10%29.aspx