Основные термины и определения

Приложение к документации ViPNet CUSTOM

ViPNet Virtual Private Network

infotecs

ФРКЕ.00068-05 90 02

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

Сайт компании «ИнфоТеКС»: http://www.infotecs.ru

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание

Приложение А. Основные термины и определения ViPNet 8
DHCP (Dynamic Host Configuration Protocol) 8
DMZ (демилитаризованная зона) 8
FTP (File Transfer Protocol) 9
IP-адрес 9
IP-пакет 9
IP-трафик 9
LDAP (Lightweight Directory Access Protocol) 9
PKI (инфраструктура открытых ключей) 9
TSP-сервер (служба штампов времени) 10
URL-адрес 10
ViPNet Administrator 10
ViPNet Network Manager 10
ViPNet Policy Manager 10
ViPNet Registration Point 11
ViPNet Удостоверяющий и ключевой центр (УКЦ) 11
ViPNet Центр управления сетью (ЦУС) 11
Авторизация 12
Администратор сети ViPNet 12
Администратор УКЦ 12
Администратор ЦУСа 12
Адрес источника 13
Адрес назначения 13
Адреса видимости 13
Адреса доступа 13
Аккредитованный удостоверяющий центр 13
Антиспуфинг 14
Асимметричное шифрование 14
Аутентификация 14
Виртуальная защищенная сеть 14
Виртуальный IP-адрес 14
Внешние IP-адреса 15

Внешний сетевой интерфейс ... 15
Внешняя сеть ... 15
Внутренние IP-адреса ... 15
Внутренний сетевой интерфейс ... 16
Внутренняя сеть ... 16
Входящее соединение ... 16
Вышестоящий удостоверяющий центр ... 16
Глобальная сеть ... 16
Головной удостоверяющий центр ... 16
Граница локальной сети ... 17
Группа узлов ... 17
Динамический адрес ... 17
Дистрибутив ключей ... 17
Доверенная сеть ... 18
Доверенное лицо (администратор) удостоверяющего центра ... 18
Журнал событий ... 18
Закрытый ключ ... 18
Запрос на сертификат ... 18
Защищенное межсетевое соединение ... 19
Защищенное соединение ... 19
Защищенные прикладные серверы ... 19
Защищенный DNS или WINS сервер ... 19
Защищенный IP-трафик ... 19
Защищенный узел ... 19
Идентификатор объекта (OID) ... 20
Иерархия удостоверяющих центров ... 20
Инкапсуляция пакетов ... 20
Исходящее соединение ... 20
Квалифицированный сертификат ... 20
Клиент (ViPNet-клиент) ... 21
Ключ защиты ... 21
Ключ защиты УКЦ ... 21
Ключ обмена ... 21
Ключи администратора УКЦ ... 21
Ключи пользователя ViPNet ... 22
Ключи узла ViPNet ... 22
Компрометация ключей ... 22

Контейнер ключей ... 23
Контейнер сертификатов администраторов ... 23
Контрольная сумма ... 23
Координатор (ViPNet-координатор) ... 23
Корневой сертификат ... 23
Кросс-сертификат ... 24
Кросс-сертификация ... 24
Лицензия на сеть ViPNet CUSTOM ... 24
Локальная сеть (LAN) ... 24
Маршрутизатор ... 25
Маршрутизация ... 25
Мастер-ключ ... 25
Межсетевая информация ... 25
Межсетевое взаимодействие ... 26
Межсетевой мастер-ключ ... 26
Межсетевой экран ... 26
Межсетевые связи ... 26
Обновление ключей узла ... 27
Обновление справочников и ключей ... 27
Обработка межсетевой информации ... 27
Обязательные связи ... 27
Отзыв сертификата ... 28
Открытый Интернет ... 28
Открытый ключ ... 28
Открытый сервер DNS или WINS ... 28
Открытый трафик ... 29
Открытый узел ... 29
Папка ключей пользователя ... 29
Папка ключей сетевого узла ... 29
Папки обмена ... 29
Пароль администратора сетевого узла ViPNet ... 29
Пароль администратора УКЦ ... 30
Пароль пользователя ... 30
Пароль пользователя на основе парольной фразы ... 30
Парольная фраза ... 30
Персональный ключ пользователя ... 31
Подразделение ... 31

Подсеть ... 31
Подчиненный удостоверяющий центр ... 31
Политика безопасности ... 32
Политика применения сертификата ... 32
Политика штампов времени ... 32
Полномочия пользователя ... 32
Пользователь ViPNet ... 32
Порт источника ... 33
Порт назначения ... 33
Прикладной конверт ... 33
Приостановление действия сертификата ... 33
Прокси-сервер ... 33
Протокол 241 ... 33
Протокол Диффи — Хеллмана ... 33
Публикация ... 34
Публичный адрес ... 34
Рабочее место администратора сети ViPNet ... 34
Расширения сертификата открытого ключа подписи пользователя ... 34
Реальный IP-адрес ... 35
Резервный набор персональных ключей (РНПК) ... 35
Результирующая политика безопасности ... 35
Роль ... 35
Роль пользователей ... 36
Своя сеть ... 36
Сегмент сети ... 36
Сервер IP-адресов ... 36
Сервер управления ... 36
Сервер-маршрутизатор ... 37
Сертификат издателя ... 37
Сертификат открытого ключа подписи пользователя ... 37
Сетевая атака ... 37
Сетевой интерфейс ... 38
Сетевой объект ... 38
Сетевой порт ... 38
Сетевой протокол ... 38
Сетевой узел ViPNet ... 38
Сетевой фильтр ... 38

Сеть ... 39
Сеть ViPNet ... 39
Симметричное шифрование ... 39
Симметричный ключ ... 39
Служба DHCP ... 39
Служба DNS ... 40
Служебный конверт ... 40
Список отозванных сертификатов (СОС) ... 40
Справочники ... 40
Справочники и ключи ... 40
Статический адрес ... 41
Структура сети ViPNet ... 41
Таблица маршрутизации ... 41
Точка распространения данных ... 41
Трансляция сетевых адресов (NAT) ... 42
Транспортный конверт ... 42
Транспортный модуль (MFTP) ... 42
Туннелирование ... 42
Туннелируемый узел ... 42
Туннелирующий координатор ... 43
Туннель ... 43
Удаленное обновление ПО ViPNet ... 43
Удаленный защищенный узел ... 43
Удостоверяющий центр ... 43
Файл лицензии ... 44
Файл с межсетевой информацией ... 44
Центр регистрации ... 44
Цепочка сертификации ... 44
Частный адрес ... 45
Шаблон политики безопасности ... 45
Шаблон пользователя ... 45
Шаблон сертификата ... 45
Широковещательный пакет ... 46
Шлюз ... 46
Шлюзовой координатор ... 46
Штамп времени ... 46
Электронная подпись ... 47

Основные термины и определения ViPNet

DHCP (Dynamic Host Configuration Protocol)

Сетевой протокол прикладного уровня, позволяющий компьютерам автоматически получать IP-адреса и другие параметры, необходимые для работы в сети TCP/IP. К таким параметрам относятся маска подсети, IP-адрес шлюза, IP-адреса серверов DNS, IP-адреса серверов WINS.

DMZ (демилитаризованная зона)

Физическая или логическая подсеть, предоставляющая доступ к внешним корпоративным службам из большей сети, с которой нет отношений доверия, как правило, из Интернета. При этом серверы, отвечающие на запросы из внешней сети или направляющие туда запросы, находятся в этой подсети и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана. Прямых соединений между внутренней сетью и внешней нет: любые соединения возможны только с серверами в DMZ, которые обрабатывают запросы и формируют свои, возвращая ответ получателю уже от своего имени.

См. также: Внешняя сеть (на стр. 15), Внутренняя сеть (на стр. 16), Межсетевой экран (на стр. 26), Сегмент сети (на стр. 36).

FTP (File Transfer Protocol)

Стандартный протокол прикладного уровня для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер.

IP-адрес

Адрес узла в сети, построенной на основе протокола IP.

См. также: Сетевой протокол (на стр. 38).

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-трафик

Поток данных, передаваемых в сети по протоколу IP.

См. также: IP-пакет (на стр. 9).

LDAP (Lightweight Directory Access Protocol)

Упрощённая версия протокола доступа к каталогу стандарта X.500. LDAP является основным протоколом, используемым для доступа к Active Directory и ADAM.

PKI (инфраструктура открытых ключей)

От англ. Public Key Infrastructure — инфраструктура открытых ключей. Комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределенных системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: Открытый ключ (на стр. 28).

TSP-сервер (служба штампов времени)

Доверенный субъект инфраструктуры открытых ключей, обладающий точным и надёжным источником времени и оказывающий услуги по созданию штампов времени.

См. также: PKI (Инфраструктура открытых ключей) (на стр. 9), Штамп времени (на стр. 46).

URL-адрес

Унифицированный указатель информационного ресурса (стандартизованная строка символов, указывающая местонахождение ресурса в Интернете).

ViPNet Administrator

Набор программного обеспечения для администрирования сети ViPNet, включающий в себя серверное и клиентское приложения ViPNet Центр управления сетью, а также программу ViPNet Удостоверяющий и ключевой центр.

См. также: Сеть ViPNet (на стр. 39), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Центр управления сетью (ЦУС) (на стр. 11).

ViPNet Network Manager

Программа, которая входит в состав программного комплекса ViPNet VPN. Предназначена для создания, конфигурирования и управления малыми и средними сетями ViPNet.

ViPNet Policy Manager

Программа, которая входит в состав программного комплекса ViPNet CUSTOM. Предназначена для централизованного управления политиками безопасности узлов защищенной сети ViPNet.

См. также Политика безопасности (на стр. 32), Рабочее место администратора сети ViPNet (на стр. 34), Сеть ViPNet (на стр. 39).

ViPNet Registration Point

Программное обеспечение, предназначенное для регистрации пользователей ViPNet и хранения их регистрационных данных, а также для выдачи сертификатов подписи и дистрибутивов ключей, создаваемых в программе ViPNet Удостоверяющий и ключевой центр по соответствующим запросам.

См. также: Дистрибутив ключей (на стр. 17), Пользователь ViPNet (на стр. 32), Сертификат открытого ключа подписи пользователя (на стр. 37), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

ViPNet Удостоверяющий и ключевой центр (УКЦ)

Программа, входящая в состав программного обеспечения ViPNet Administrator. Администратор УКЦ формирует и обновляет ключи для сетевых узлов ViPNet, а также управляет сертификатами и списками отозванных сертификатов.

См. также: Администратор УКЦ (на стр. 12), Пользователь ViPNet (на стр. 32), Список отозванных сертификатов (СОС) (на стр. 40), ViPNet Administrator (на стр. 10).

ViPNet Центр управления сетью (ЦУС)

В сети ViPNet CUSTOM ViPNet Центр управления сетью — это программа, входящая в состав программного обеспечения ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

- построение виртуальной сети (сетевые объекты и связи между ними, включая межсетевые);
- изменение конфигурации сети;
- формирование и рассылка справочников;
- рассылка ключей узлов и ключей пользователей;
- формирование информации о связях пользователей для УКЦ;
- задание полномочий пользователей сетевых узлов ViPNet.

В сети ViPNet VPN Центр управления сетью — это рабочее место администратора сети ViPNet. В ЦУСе создается структура сети ViPNet, формируются и отправляются на сетевые узлы обновления наборов ключей и программного обеспечения ViPNet.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Ключи пользователя ViPNet (на стр. 22), Ключи узла ViPNet (на стр. 22), Полномочия пользователя (на стр. 32), Рабочее место администратора сети ViPNet (на стр. 34), Сетевой объект (на стр. 38), Справочники (на стр. 40), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Administrator (на стр. 10), ViPNet Network Manager (на стр. 10).

Авторизация

Процесс предоставления доступа в систему или отказа в доступе пользователю по итогам аутентификации.

См. также: Аутентификация (на стр. 14).

Администратор сети ViPNet

Лицо, отвечающее за управление сетью ViPNet, создание и обновление справочников и ключей для сетевых узлов ViPNet, настройку межсетевого взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Центр управления сетью и (или) ViPNet Удостоверяющий и ключевой центр.

См. также: Доверенная сеть (на стр. 18), Межсетевое взаимодействие (на стр. 26), Обновление справочников и ключей (на стр. 27), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Центр управления сетью (ЦУС) (на стр. 11).

Администратор УКЦ

Лицо, обладающее правом доступа к программе ViPNet Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание ключей для сетевых узлов ViPNet, создание и обслуживание сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: Доверенная сеть (на стр. 18), Сетевой узел ViPNet (на стр. 38), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Администратор ЦУСа

Лицо, обладающее правом доступа к программе ViPNet Центр управления сетью (ЦУС) и отвечающее за создание и настройку сети ViPNet, создание и рассылку адресных справочников, обновление ключей, обновление программного обеспечения ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: Сеть ViPNet (на стр. 39), ViPNet Центр управления сетью (ЦУС) (на стр. 11).

Адрес источника

Адрес сетевого устройства, отправившего IP-пакет.

См. также: IP-пакет (на стр. 9), Адрес назначения (на стр. 13).

Адрес назначения

Адрес сетевого устройства, на которое отправлен IP-пакет.

См. также: IP-пакет (на стр. 9), Адрес источника (на стр. 13).

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet и по которым приложения отправляют свой трафик.

См. также: IP-адрес (на стр. 9), Виртуальный IP-адрес (на стр. 14), Реальный IP-адрес (на стр. 35).

Адреса доступа

IP-адреса, по которым узел доступен в сети (например, адреса межсетевого экрана, за которым он находится).

См. также: Межсетевой экран (на стр. 26), IP-адрес (на стр. 9).

Аккредитованный удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти в соответствии с требованиями Федерального закона от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

См. также: Удостоверяющий центр (на стр. 43).

Антиспуфинг

Защита от спуфинг-атак, при которых злоумышленник подделывает адрес источника для обхода межсетевых экранов и организации DoS-атак (от англ. Denial of Service, отказ в обслуживании).

См. также: Межсетевой экран (на стр. 26).

Асимметричное шифрование

Система шифрования, при которой алгоритмы используют два математически связанных ключа. Открытый ключ используется для зашифрования и передается по незащищенному каналу. Закрытый ключ служит для расшифрования.

См. также: Закрытый ключ (на стр. 18), Открытый ключ (на стр. 28), Симметричное шифрование (на стр. 39).

Аутентификация

Процесс идентификации пользователя, как правило, на основании его учетной записи. Аутентификация служит для подтверждения того, что входящий в систему пользователь является тем, за кого себя выдает, но процесс аутентификации не затрагивает права доступа пользователя (в отличие от авторизации).

См. также: Авторизация (на стр. 12).

Виртуальная защищенная сеть

Технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

См. также: Аутентификация (на стр. 14), Внешняя сеть (на стр. 15), PKI (инфраструктура открытых ключей) (на стр. 9).

Виртуальный IP-адрес

IP-адрес, который приложения на сетевом узле ViPNet (А) используют для обращения к ресурсам сетевого узла ViPNet (Б) или туннелируемых им узлов вместо реального IP-

адреса узла. Виртуальные IP-адреса узлу ViPNet Б назначаются непосредственно на узле А. На других узлах узлу ViPNet Б могут быть назначены другие виртуальные адреса. Узлу ViPNet (Б) назначается столько виртуальных адресов, сколько реальных адресов имеет данный узел. При изменении реальных адресов у узла Б выделенные ему виртуальные адреса не изменяются. Виртуальные адреса туннелируемых узлов привязываются к реальным адресам этих узлов и существуют, пока существует данный реальный адрес. Использование виртуальных адресов позволяет избежать конфликта реальных IP-адресов в случае, если узлы работают в локальных сетях с пересекающимся адресным пространством, а также использовать эти адреса для аутентификации удаленных узлов в приложениях ViPNet.

См. также: Реальный IP-адрес (на стр. 35), IP-адрес (на стр. 9).

Внешние IP-адреса

Адреса внешней сети.

См. также: Внешняя сеть (на стр. 15).

Внешний сетевой интерфейс

Сетевой интерфейс на координаторе, который используется для подключения узла к внешней (глобальной) сети, как правило, Интернету.

См. также: Внешняя сеть (на стр. 15), Глобальная сеть (на стр. 16), Координатор (ViPNet-координатор) (на стр. 23), Сетевой интерфейс (на стр. 38).

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

См. также: Внутренняя сеть (на стр. 16), Межсетевой экран (на стр. 26).

Внутренние IP-адреса

Адреса внутренней сети.

См. также: Внутренняя сеть (на стр. 16).

Внутренний сетевой интерфейс

Сетевой интерфейс координатора, который используется для подключения узла к внутренней сети.

См. также: Внутренняя сеть (на стр. 16), Координатор (ViPNet-координатор) (на стр. 23), Сетевой интерфейс (на стр. 38).

Внутренняя сеть

Локальная сеть, где находятся рассматриваемые узлы, которая отделена от внешней сети межсетевым экраном.

См. также: Внешняя сеть (на стр. 15), Локальная сеть (LAN) (на стр. 24), Межсетевой экран (на стр. 26).

Входящее соединение

Соединение между двумя узлами А и Б, инициированное узлом Б, является входящим по отношению к узлу А.

Вышестоящий удостоверяющий центр

Удостоверяющий центр, который является вышестоящим по отношению к другому удостоверяющему центру в иерархической системе доверительных отношений между удостоверяющими центрами. При этом может быть подчиненным по отношению к третьему удостоверяющему центру, если не является головным.

См. также: Головной удостоверяющий центр (на стр. 16), Подчиненный удостоверяющий центр (на стр. 31), Удостоверяющий центр (на стр. 43).

Глобальная сеть

Сеть, объединяющая компьютеры, географически удаленные на большие расстояния друг от друга.

Головной удостоверяющий центр

Удостоверяющий центр, который находится на вершине иерархической системы доверительных отношений между удостоверяющими центрами.

См. также: Вышестоящий удостоверяющий центр (на стр. 16), Иерархия удостоверяющих центров (на стр. 20), Подчиненный удостоверяющий центр (на стр. 31), Удостоверяющий центр (на стр. 43).

Граница локальной сети

Условное понятие, означающее точку выхода из локальной сети во внешнюю сеть.

См. также: Внешняя сеть (на стр. 15), Локальная сеть (LAN) (на стр. 24).

Группа узлов

Множество сетевых узлов ViPNet, объединенное под общим именем для удобства администрирования. Например, позволяет задать единый пароль администратора для всех сетевых узлов ViPNet, входящих в данную группу.

См. также: Пароль администратора сетевого узла ViPNet (на стр. 29), Пользователь ViPNet (на стр. 32), Сетевой узел ViPNet (на стр. 38).

Динамический адрес

IP-адрес, выделяемый пользователю службой DHCP на сеанс его работы.

См. также: Служба DHCP (на стр. 39).

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

См. также: Сетевой узел ViPNet (на стр. 38), Справочники (на стр. 40), Файл лицензии (на стр. 44), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Доверенная сеть

Сеть ViPNet, с узлами которой узлы своей сети ViPNet осуществляют защищенное взаимодействие.

См. также: Межсетевое взаимодействие (на стр. 26), Своя сеть (на стр. 36).

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

См. также: Удостоверяющий центр (на стр. 43).

Журнал событий

Файл или группа файлов, предназначенных для хранения сведений о событиях программы.

Закрытый ключ

Закрытая (секретная) часть пары асимметричных ключей. Служит для создания электронных подписей, которые можно проверять с помощью парного ему открытого ключа, или для расшифрования сообщений, которые были зашифрованы парным ему открытым ключом.

Ключ электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является закрытым ключом.

См. также: Асимметричное шифрование (на стр. 14), Открытый ключ (на стр. 28), Электронная подпись (на стр. 47).

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, открытый ключ и его параметры, желаемый срок действия сертификата, предполагаемые назначения сертификата и другие параметры (полный набор параметров зависит от формата запроса и программного обеспечения, в котором он был сформирован).

См. также: Закрытый ключ (на стр. 18), Открытый ключ (на стр. 28), Сертификат открытого ключа подписи пользователя (на стр. 37), Электронная подпись (на стр. 47).

Защищенное межсетевое соединение

Соединение между сетевыми узлами своей и доверенной сетей, защищенное с помощью программного обеспечения ViPNet.

См. также: Доверенная сеть (на стр. 18), Своя сеть (на стр. 36).

Защищенное соединение

Соединение между узлами, зашифрованное с помощью программного обеспечения ViPNet.

Защищенные прикладные серверы

Прикладные серверы (веб-сервер, почтовый сервер, FTP-сервер и так далее), размещенные на защищенных узлах.

См. также: Защищенный узел (на стр. 19).

Защищенный DNS или WINS сервер

Сервер DNS или WINS, размещенный на защищенном узле.

См. также: Защищенный узел (на стр. 19).

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью программного обеспечения ViPNet.

См. также: IP-пакет (на стр. 9).

Защищенный узел

Сетевой узел, на котором установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Идентификатор объекта (OID)

От англ. “object identifier”. Уникальная числовая последовательность, позволяющая однозначно идентифицировать класс или атрибут объекта.

Частным случаем использования OID является обозначение видов атрибутов и классов объектов в стандартах серии X.500.

Иерархия удостоверяющих центров

Система доверительных отношений между удостоверяющими центрами, в которой вышестоящие удостоверяющие центры выпускают сертификаты для подчиненных удостоверяющих центров.

См. также: Вышестоящий удостоверяющий центр (на стр. 16), Головной удостоверяющий центр (на стр. 16), Подчиненный удостоверяющий центр (на стр. 31), Удостоверяющий центр (на стр. 43).

Инкапсуляция пакетов

Принцип передачи данных, при котором данные в формате одного протокола упаковываются в формат другого протокола.

Исходящее соединение

Соединение, инициированное данным сетевым узлом.

Квалифицированный сертификат

Сертификат открытого ключа подписи пользователя, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.

См. также: Аккредитованный удостоверяющий центр (на стр. 13), Сертификат открытого ключа подписи пользователя (на стр. 37), Электронная подпись (на стр. 47).

Клиент (ViPNet-клиент)

Сетевой узел ViPNet, который является начальной или конечной точкой передачи данных. В отличие от координатора клиент не выполняет функции маршрутизации трафика и служебной информации.

См. также: Координатор (ViPNet-координатор) (на стр. 23), Маршрутизация (на стр. 25), Сетевой узел ViPNet (на стр. 38).

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ защиты УКЦ

Ключ, на котором зашифрованы список администраторов программы ViPNet Удостоверяющий и ключевой центр, мастер-ключи, пароли пользователей ViPNet, ключи пользователей при хранении их в УКЦ.

У каждого администратора УКЦ имеется свой ключ защиты, зашифрованный на пароле этого администратора.

См. также: Администратор УКЦ (на стр. 12), Ключи пользователя ViPNet (на стр. 22), Мастер-ключ (на стр. 25), Пароль пользователя (на стр. 30), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации, которой обмениваются узлы ViPNet. Используется для зашифрования и расшифрования передаваемых данных.

См. также: Симметричный ключ (на стр. 39).

Ключи администратора УКЦ

Формируются при создании учетной записи администратора УКЦ и включают в себя:

- ключ защиты УКЦ, зашифрованный на пароле администратора;
- контейнеры с ключами подписи.

См. также: Ключ защиты УКЦ (на стр. 21), Контейнер ключей (на стр. 23).

Ключи пользователя ViPNet

Совокупность ключей, которые необходимы пользователю для аутентификации в сети ViPNet и шифрования других ключей, и к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- случайный ключ защиты пользователя;
- закрытый ключ и соответствующий ему сертификат открытого ключа подписи пользователя;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

См. также: Аутентификация (на стр. 14), Контейнер ключей (на стр. 23), Персональный ключ пользователя (на стр. 31).

Ключи узла ViPNet

Совокупность ключей, с использованием которых производится шифрование трафика, служебной информации и писем программы ViPNet Деловая почта.

См. также: Обновление ключей узла (на стр. 27), Сетевой узел ViPNet (на стр. 38), Электронная подпись (на стр. 47), IP-трафик (на стр. 9).

Компрометация ключей

Утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Контейнер ключей

Файл, в котором хранятся закрытый ключ и соответствующий ему сертификат открытого ключа.

См. также: Закрытый ключ (на стр. 18), Сертификат открытого ключа подписи пользователя (на стр. 37).

Контейнер сертификатов администраторов

Файл формата PKCS #7, который может содержать списки сертификатов издателей (администраторов удостоверяющего центра) и соответствующие им списки отозванных сертификатов. В программе ViPNet Удостоверяющий и ключевой центр используется для установки межсетевого взаимодействия.

См. также: Межсетевое взаимодействие (на стр. 26), Сертификат издателя (на стр. 37), Список отозванных сертификатов (СОС) (на стр. 40), Удостоверяющий центр (на стр. 43), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Контрольная сумма

Значение, используемое для проверки целостности информации.

Координатор (ViPNet-координатор)

Сетевой узел, представляющий собой компьютер с установленным программным обеспечением координатора (ViPNet Coordinator или ViPNet Coordinator Linux) или специальный программно-аппаратный комплекс. В рамках сети ViPNet координатор выполняет серверные функции, а также маршрутизацию трафика и служебной информации.

См. также: Маршрутизация (на стр. 25), Сеть ViPNet (на стр. 39).

Корневой сертификат

Самоподписанный сертификат администратора удостоверяющего центра, являющийся последним сертификатом в цепочке доверия. Другими словами, для корневого сертификата нет сертификата, с помощью которого можно было бы проверить его достоверность. С помощью корневого сертификата проверяется достоверность сертификатов (пользователей и издателей), заверенных этим сертификатом.

См. также: Сертификат издателя (на стр. 37), Сертификат открытого ключа подписи пользователя (на стр. 37), Удостоверяющий центр (на стр. 43).

Кросс-сертификат

Сертификат уполномоченного лица одного удостоверяющего центра, изданный уполномоченным лицом другого удостоверяющего центра.

См. также: Доверенное лицо (администратор) удостоверяющего центра (на стр. 18), Кросс-сертификация (на стр. 24).

Кросс-сертификация

Механизм установления доверительных отношений между удостоверяющими центрами, осуществляемый через выпуск кросс-сертификатов одним УЦ для другого УЦ.

См. также: Кросс-сертификат (на стр. 24), Удостоверяющий центр (на стр. 43).

Лицензия на сеть ViPNet CUSTOM

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet CUSTOM. В частности, лицензия на сеть ViPNet CUSTOM определяет следующее: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов, на которые можно добавить ту или иную роль, максимальную разрешенную версию программного обеспечения ViPNet, срок действия лицензии и другие параметры.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Координатор (ViPNet-координатор) (на стр. 23), Роль (на стр. 35), Сеть ViPNet (на стр. 39), Туннелирование (на стр. 42).

Локальная сеть (LAN)

Группа компьютеров и других устройств, размещенных на относительно небольшом пространстве и соединенных линиями связи, которые позволяют любому устройству взаимодействовать с любым другим устройством в этой сети.

Маршрутизатор

Сетевое устройство, которое на основании информации о топологии сети (таблицы маршрутизации), а также адреса получателя пакета определяет дальнейший маршрут пересылки пакетов их получателю. Обычно применяется для связи нескольких сегментов сети.

См. также: Адрес назначения (на стр. 13), Сегмент сети (на стр. 36), Таблица маршрутизации (на стр. 41).

Маршрутизация

Процесс выбора пути для передачи информации.

Мастер-ключ

Ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. В сети ViPNet формируется три вида мастер-ключей:

- мастер-ключ ключей обмена;
- мастер-ключ ключей защиты ключей обмена;
- мастер-ключ персональных ключей пользователей.

Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

См. также: Администратор сети ViPNet (на стр. 12), Ключ обмена (на стр. 21), Компрометация ключей (на стр. 22), Межсетевой мастер-ключ (на стр. 26), Персональный ключ пользователя (на стр. 31), Сетевой узел ViPNet (на стр. 38), Сеть ViPNet (на стр. 39), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Межсетевая информация

Информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами, параметры сетевых узлов ViPNet и служебная информация (сертификаты издателей, СОС).

См. также: Доверенная сеть (на стр. 18), Межсетевое взаимодействие (на стр. 26), Своя сеть (на стр. 36), Сетевой объект (на стр. 38), Файл с межсетевой информацией (на стр. 44).

Межсетевое взаимодействие

Информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

См. также: Администратор сети ViPNet (на стр. 12), Межсетевая информация (на стр. 25), Межсетевые связи (на стр. 26), Сеть ViPNet (на стр. 39).

Межсетевой мастер-ключ

Ключ, служащий для формирования ключей обмена между сетевыми узлами разных сетей ViPNet.

См. также: Ключ обмена (на стр. 21), Сетевой узел ViPNet (на стр. 38), Сеть ViPNet (на стр. 39).

Межсетевой экран

Устройство на границе локальной сети, служащее для предотвращения несанкционированного доступа из одной сети в другую. Межсетевой экран проверяет весь входящий и исходящий IP-трафик, после чего принимается решение о возможности дальнейшего направления трафика к пункту назначения. Межсетевой экран обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT).

См. также: Граница локальной сети (на стр. 17), Трансляция сетевых адресов (NAT) (на стр. 42).

Межсетевые связи

Связи между узлами ViPNet своей сети и доверенной сети, определяющие возможность защищенного обмена данными.

См. также: Доверенная сеть (на стр. 18), Межсетевое взаимодействие (на стр. 26), Своя сеть (на стр. 36).

Обновление ключей узла

Совокупность файлов, к которым относятся справочники сертификатов администраторов УКЦ (файл `*.trl`), списки отозванных сертификатов своей и доверенных сетей (файлы `*.crl`, `*.p7s`), контрольные суммы паролей администраторов, корневые сертификаты администраторов доверенных сетей и служебная информация о пользователе узла, на котором обновляются ключи (право подписи). Фактически, обновление ключей узла является неполным вариантом ключей узла ViPNet.

См. также: Доверенная сеть (на стр. 18), Ключи узла ViPNet (на стр. 22), Контрольная сумма (на стр. 23), Корневой сертификат (на стр. 23), Своя сеть (на стр. 36), Список отозванных сертификатов (СОС) (на стр. 40), Справочники и ключи (на стр. 40).

Обновление справочников и ключей

Файлы, формируемые администратором сети ViPNet в управляющем приложении (ViPNet Центр управления сетью, ViPNet Удостоверяющий и ключевой центр, ViPNet Network Manager) при изменении справочников и ключей для сетевых узлов ViPNet, то есть, в случае добавления, удаления сетевого узла ViPNet, добавления пользователя, издания нового сертификата и так далее. Администратор сети ViPNet централизованно высылает на сетевой узел сформированные новые ключи и справочники из ЦУСа или ViPNet Network Manager.

См. также: Администратор сети ViPNet (на стр. 12), Сетевой узел ViPNet (на стр. 38), Сеть ViPNet (на стр. 39), Справочники и ключи (на стр. 40), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Обработка межсетевой информации

Принятие или отклонение межсетевой информации администратором сети ViPNet в программе ViPNet Центр управления сетью или ViPNet Network Manager.

См. также: Администратор сети ViPNet (на стр. 12), Межсетевая информация (на стр. 25), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Обязательные связи

Связи между сетевыми узлами ViPNet, наличие которых является обязательным для функционирования сети ViPNet. Эти связи не могут быть удалены.

Примером обязательных связей является связь клиента с координатором, который является его сервером-маршрутизатором.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Координатор (ViPNet-координатор) (на стр. 23), Сервер-маршрутизатор (на стр. 37), Сетевой узел ViPNet (на стр. 38), Сеть ViPNet (на стр. 39).

Отзыв сертификата

Признание сертификата недействительным до истечения его срока действия (например, в случае компрометации соответствующего закрытого ключа).

См. также: Компрометация ключей (на стр. 22).

Открытый Интернет

Технология, реализованная в программном обеспечении ViPNet. При подключении к Интернету узлы локальной сети изолируются от сети ViPNet, а при работе в сети ViPNet — от Интернета, что обеспечивает защиту от возможных сетевых атак извне без физического отключения компьютеров от локальной сети.

См. также: Локальная сеть (LAN) (на стр. 24), Сетевая атака (на стр. 37), Сеть ViPNet (на стр. 39).

Открытый ключ

Последовательность символов, связанная с закрытым ключом определенным математическим соотношением. Открытый ключ доступен любым пользователям информационной системы и предназначен для подтверждения подлинности электронной подписи (или шифрования).

Ключ проверки электронной подписи (см. Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи») является открытым ключом.

См. также: Асимметричное шифрование (на стр. 14), Закрытый ключ (на стр. 18), Электронная подпись (на стр. 47).

Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

См. также: Открытый узел (на стр. 29).

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

См. также: Туннелируемый узел (на стр. 42).

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

См. также: Ключи пользователя ViPNet (на стр. 22).

Папка ключей сетевого узла

Папка, в которой находятся ключи сетевого узла ViPNet и справочники.

См. также: Ключи узла ViPNet (на стр. 22), Справочники (на стр. 40).

Папки обмена

Папки, которые используют компоненты программного обеспечения ViPNet Administrator — ViPNet Центр управления сетью и ViPNet Удостоверяющий и ключевой центр — для обмена данными.

См. также: ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Administrator (на стр. 10).

Пароль администратора сетевого узла ViPNet

Пароль для включения на сетевом узле ViPNet режима администратора, в рамках которого появляются дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан в УКЦ или ViPNet Network Manager администратором сети ViPNet.

См. также: Сетевой узел ViPNet (на стр. 38), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11), ViPNet Network Manager (на стр. 10).

Пароль администратора УКЦ

Пароль для входа в программу ViPNet Удостоверяющий и ключевой центр.

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Network Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

См. также: Администратор сети ViPNet (на стр. 12), Пользователь ViPNet (на стр. 32), Сетевой узел ViPNet (на стр. 38), ViPNet Network Manager (на стр. 10).

Пароль пользователя на основе парольной фразы

Пароль пользователя необходим для входа в любую программу ViPNet. Случайный пароль создается на основе парольной фразы, которую можно использовать для запоминания пароля. Парольные фразы могут быть созданы на нескольких языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря. Парольная фраза может содержать 3 или 4 слова, при желании пароль может быть создан из двух парольных фраз.

Чтобы получить пароль из парольной фразы, достаточно набрать без пробелов в раскладке латиницей первые X букв из каждого слова парольной фразы, содержащей Y слов. Пользователь сам задает параметры X и Y, а также язык парольной фразы.

Например, при использовании трех первых букв из каждого слова парольной фразы «Затейливый ювелир утащил сдобу» получим пароль «pfn.dtenfclj».

См. также: Пароль пользователя (на стр. 30), Парольная фраза (на стр. 30).

Парольная фраза

Набор грамматически согласованных между собой слов, выбираемых случайным образом из специальных словарей. Парольная фраза формируется при создании паролей и служит для их запоминания. Пароль из парольной фразы получается по следующему правилу: в

латинской раскладке клавиатуры набираются по N первых букв от каждого из M слов парольной фразы без пробелов, где N определяется длиной пароля.

Например, парольной фразе «**служ**ащий **лата**ет **рельс**» соответствует пароль «cke;kfnfhtkm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

См. также: Пароль пользователя на основе парольной фразы (на стр. 30).

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Действующий персональный ключ необходимо хранить в безопасном месте.

См. также: Ключи пользователя ViPNet (на стр. 22), Компрометация ключей (на стр. 22), Пользователь ViPNet (на стр. 32), Резервный набор персональных ключей (РНПК) (на стр. 35), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Подразделение

Множество узлов из числа всех управляемых сетевых узлов, объединенных для коллективного назначения шаблонов политики безопасности. Одно подразделение может входить в другое, образуя иерархию.

См. также: Шаблон политики безопасности (на стр. 45).

Подсеть

Логически выделенное подмножество узлов сети.

Подчиненный удостоверяющий центр

Удостоверяющий центр, сертификат администратора которого заверен вышестоящим удостоверяющим центром.

См. также: Вышестоящий удостоверяющий центр (на стр. 16), Головной удостоверяющий центр (на стр. 16), Иерархия удостоверяющих центров (на стр. 20), Удостоверяющий центр (на стр. 43).

Политика безопасности

Набор параметров, регулирующих безопасность сетевого узла. В технологии ViPNet безопасность сетевых узлов обеспечивается с помощью сетевых фильтров и правил трансляции IP-адресов.

См. также: Результирующая политика безопасности (на стр. 35), Сетевой узел ViPNet (на стр. 38).

Политика применения сертификата

Совокупность правил применения сертификата открытого ключа подписи, определяющих, в каких случаях допустимо или следует использовать данный сертификат в соответствии с требованиями безопасности.

См. также: Расширения сертификата открытого ключа подписи пользователя (на стр. 34), Сертификат открытого ключа подписи пользователя (на стр. 37).

Политика штампов времени

Разновидность политики применения сертификата. Устанавливает набор правил, по которым выдаются штампы времени, а также области применения штампов времени.

См. также: Политика применения сертификата (на стр. 32), Штамп времени (на стр. 46).

Полномочия пользователя

Разрешения на определенные действия пользователей на сетевом узле ViPNet по изменению настроек некоторых программ ViPNet.

Администратор ЦУСа задает полномочия для всех пользователей сетевого узла ViPNet в свойствах ролей.

См. также: Администратор ЦУСа (на стр. 12), Пароль администратора сетевого узла ViPNet (на стр. 29), Роль (на стр. 35), Сетевой узел ViPNet (на стр. 38).

Пользователь ViPNet

Лицо, которое использует программное обеспечение ViPNet и имеет ключи для работы с ним.

Порт источника

TCP- или UDP-порт, используемый отправителем пакета при его отправке.

Порт назначения

TCP- или UDP-порт, на который посылается пакет.

Прикладной конверт

Файл, формируемый приложениями ViPNet (например, «Деловая почта», «Файловый обмен») для передачи другим сетевым узлам.

Приостановление действия сертификата

Временное ограничение действия сертификата до истечения его срока действия.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 37).

Прокси-сервер

Программа, транслирующая соединения по некоторым протоколам из внутренней сети во внешнюю и выступающая при этом как посредник между клиентами и сервером.

См. Внешняя сеть (на стр. 15), Внутренняя сеть (на стр. 16).

Протокол 241

IP-протокол с идентификатором 241, специально разработанный для использования в программном обеспечении ViPNet.

Протокол Диффи — Хеллмана

Протокол открытого распределения ключей, позволяющий двум пользователям вырабатывать общий секретный ключ путем динамического взаимодействия на основе обмена открытыми сообщениями без какой-либо общей секретной информации, распределяемой заранее.

Публикация

Размещение сформированной в удостоверяющем центре информации на источниках данных, доступных по общеизвестным протоколам (например, FTP, LDAP).

См. также: Удостоверяющий центр (на стр. 43).

Публичный адрес

IP-адрес, который может применяться в Интернете.

См. также: Частный адрес (на стр. 45).

Рабочее место администратора сети ViPNet

Компьютер, на котором установлено программное обеспечение ViPNet Network Manager или одна (несколько) из следующих программ:

- ViPNet Центр управления сетью;
- ViPNet Удостоверяющий и ключевой центр;
- ViPNet Policy Manager.

См. также: Сеть ViPNet (на стр. 39), ViPNet Administrator (на стр. 10), ViPNet Network Manager (на стр. 10), ViPNet Policy Manager (на стр. 10).

Расширения сертификата открытого ключа подписи пользователя

Дополнительные атрибуты сертификата, такие как использование ключа, политики сертификата, базовые ограничения, ограничения имени и другие. Расширение может быть критичным или некритичным. Система, использующая сертификаты, должна отвергать сертификат, если она встретила критичное расширение, которое не в состоянии распознать; однако некритичные расширения могут игнорироваться, если они не распознаются. Каждое расширение сертификата должно иметь соответствующий идентификатор объекта (OID).

См. также: Идентификатор объекта (OID) (на стр. 20), Сертификат открытого ключа подписи пользователя (на стр. 37).

Реальный IP-адрес

IP-адрес, назначенный сетевому интерфейсу компьютера в локальной сети или Интернете.

См. также: Виртуальный IP-адрес (на стр. 14), Локальная сеть (LAN) (на стр. 24), Сетевой интерфейс (на стр. 38), IP-адрес (на стр. 9).

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ или ViPNet Network Manager создает для пользователя. Имя этого файла имеет маску `AAAA.pk`, где `AAAA` — идентификатор пользователя ViPNet в рамках своей сети. Используется для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей.

См. также: Администратор УКЦ (на стр. 12), Администратор ViPNet Network Manager, Дистрибутив ключей (на стр. 17), Ключи пользователя ViPNet (на стр. 22), Компрометация ключей (на стр. 22), Мастер-ключ (на стр. 25), Персональный ключ пользователя (на стр. 31).

Результирующая политика безопасности

Политика безопасности для отдельного узла, полученная в результате объединения (с учетом приоритета) шаблонов, назначенных узлу и подразделениям, в которые входит данный узел.

См. также: Подразделение (на стр. 31), Шаблон политики безопасности (на стр. 45).

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла `infotecs.reg` и определяет возможности сетевого узла и программное обеспечение ViPNet, которое может быть установлено на этом узле.

Роли могут иметь атрибуты в виде количественных характеристик и полномочий, которые также влияют на функциональность.

Набор ролей для каждого сетевого узла задается администратором сети ViPNet в программе ViPNet Центр управления сетью.

См. также: Полномочия пользователя (на стр. 32), Сеть ViPNet (на стр. 39).

Роль пользователей

Набор полномочий, предназначенный для обеспечения определенных действий пользователей в программе ViPNet Policy Manager.

Своя сеть

Для сети CUSTOM, сеть ViPNet, номер которой указан в вашем файле `infotecs.re`.

Для сети OFFICE, сеть ViPNet, номер которой совпадает с текущим номером сети в ViPNet Network Manager.

См. также: Сеть ViPNet (на стр. 39), ViPNet Network Manager (на стр. 10).

Сегмент сети

Объединение узлов на физическом уровне.

Сервер IP-адресов

Функциональность координатора, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов.

См. также: Защищенный узел (на стр. 19), Координатор (ViPNet-координатор) (на стр. 23).

Сервер управления

Сетевой узел ViPNet (ViPNet-клиент), на котором установлено программное обеспечение ViPNet Policy Manager. Сервер управления выполняет все основные функции по управлению политиками безопасности.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Политика безопасности (на стр. 32).

Сервер-маршрутизатор

Функциональность координатора, обеспечивающая маршрутизацию транспортных конвертов между узлами сети ViPNet.

См. также: Координатор (ViPNet-координатор) (на стр. 23), Маршрутизация (на стр. 25), Сеть ViPNet (на стр. 39), Транспортный конверт (на стр. 42).

Сертификат издателя

Сертификат уполномоченного лица удостоверяющего центра, которым заверяются издаваемые сертификаты.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 37).

Сертификат открытого ключа подписи пользователя

Электронный документ определенного формата, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Сертификат содержит информацию о владельце ключа, открытый ключ, сведения о его назначении и области применения, информацию о выпустившем сертификат удостоверяющем центре, период действия сертификата, а также некоторые дополнительные параметры. В программе ViPNet Удостоверяющий и ключевой центр сертификат создается в соответствии со стандартом X.509 v3 и заверяется электронной подписью администратора УКЦ.

В терминологии Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи» сертификат открытого ключа подписи пользователя называют «сертификатом ключа проверки электронной подписи».

См. также: Администратор УКЦ (на стр. 12), Открытый ключ (на стр. 28), Удостоверяющий центр (на стр. 43), Электронная подпись (на стр. 47), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Сетевая атака

Попытка злоумышленника вывести узел из строя, например, в случае DoS-атаки (от англ. Denial of Service, отказ в обслуживании), или получить несанкционированный доступ в сеть с целью изменить, удалить данные или добавить нежелательные данные. Успех атаки зависит от степени уязвимости системы защиты и предпринимаемых контрмер.

Сетевой интерфейс

Устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. Сетевым интерфейсом может служить сетевая плата, модем и другие подобные устройства.

См. также: Сеть (на стр. 39), IP-адрес (на стр. 9).

Сетевой объект

Сетевой узел, пользователь, группа узлов или группа пользователей.

См. также: Сетевой узел ViPNet (на стр. 38).

Сетевой порт

Системный ресурс, выделяемый приложению для соединения и обмена данными с другими приложениями, выполняемыми на этом же или других узлах, доступных через сеть. Позволяет различным программам, выполняемым на одном узле, получать данные независимо друг от друга (предоставлять сетевые сервисы). Каждая программа обрабатывает данные, поступающие на определенный сетевой порт.

Сетевой протокол

Набор правил, позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами.

Сетевой узел ViPNet

Узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью или ViPNet Network Manager.

См. также: ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Сетевой фильтр

Совокупность параметров, на основании которых сетевой экран программного обеспечения ViPNet пропускает или блокирует IP-пакет.

Сеть

Два или более компьютеров, между которыми установлено соединение.

Сеть ViPNet

Логическая сеть, организованная с помощью программного обеспечения ViPNet и представляющая собой совокупность сетевых узлов ViPNet.

Сеть ViPNet имеет свою адресацию, позволяющую наладить обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор).

См. также: Сетевой узел ViPNet (на стр. 38).

Симметричное шифрование

Способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами.

См. также: Асимметричное шифрование (на стр. 14), Симметричный ключ (на стр. 39).

Симметричный ключ

Последовательность битов заданной длины (для алгоритма ГОСТ 28147-89 — 256 битов), используемая как для зашифрования, так и для расшифрования информации.

В программном обеспечении ViPNet симметричные ключи используются для зашифрования и расшифрования IP-трафика, информации приложений (в том числе почтовой), служебных и прикладных конвертов.

См. также: Ключи узла ViPNet (на стр. 22), Прикладной конверт (на стр. 33), Симметричное шифрование (на стр. 39), Служебный конверт (на стр. 40).

Служба DHCP

Предназначена для динамического назначения адресов и некоторых сетевых параметров узлам, подключенным к DHCP-серверу.

Служба DNS

Распределенная интернет-служба, используемая для сопоставления логических (доменных) имен и IP-адресов. DNS используется для обеспечения возможности работы с понятными и легко запоминающимися именами вместо IP-адресов в числовом формате.

Служебный конверт

Файл, который может содержать обновление справочников и ключей или обновление программного обеспечения ViPNet. Служебный конверт предназначен для задач администрирования и формируется в программе ViPNet Центр управления сетью или ViPNet Network Manager.

См. также: Удаленное обновление ПО ViPNet (на стр. 43), Обновление справочников и ключей (на стр. 27), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны или приостановлены администратором удостоверяющего центра и недействительны на момент, указанный в данном списке отозванных сертификатов.

См. также: Доверенное лицо (администратор) удостоверяющего центра (на стр. 18), Отзыв сертификата (на стр. 28), Приостановление действия сертификата (на стр. 33).

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в управляющих приложениях ViPNet, предназначенных для создания структуры и конфигурирования сети ViPNet (ViPNet Центр управления сетью, ViPNet Network Manager).

См. также: Сетевой объект (на стр. 38), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

См. также: Ключи пользователя ViPNet (на стр. 22), Ключи узла ViPNet (на стр. 22), Обновление справочников и ключей (на стр. 27), Папка ключей пользователя (на стр. 29), Справочники (на стр. 40).

Статический адрес

Постоянный IP-адрес, присвоенный сетевому интерфейсу вручную.

См. также: IP-адрес (на стр. 9).

Структура сети ViPNet

Упорядоченная совокупность связей между компонентами сети ViPNet, такими как:

- рабочее место администратора сети ViPNet;
- координаторы;
- клиенты.

Каждый клиент должен быть зарегистрирован на координаторе. Связи между координаторами и рабочим местом администратора, а также между координатором и его клиентами обязательны. Остальные связи создаются в соответствии с корпоративной политикой безопасности.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Координатор (ViPNet-координатор) (на стр. 23), Обязательные связи (на стр. 27), Рабочее место администратора сети ViPNet (на стр. 34), Сеть ViPNet (на стр. 39).

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора пути для передачи данных.

См. также: Маршрутизация (на стр. 25).

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, FTP или LDAP), используемый для размещения сформированной в Удостоверяющем центре информации (сертификатов издателей и списков отозванных сертификатов).

См. также: Сертификат издателя (на стр. 37), Список отозванных сертификатов (СОС) (на стр. 40), Удостоверяющий центр (на стр. 43), FTP (File Transfer Protocol) (на стр. 9), LDAP (Lightweight Directory Access Protocol) (на стр. 9).

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса и порты, использующиеся в одной сети, в адреса и порты, использующиеся в другой.

Транспортный конверт

Зашифрованная информация служб или приложений, доставляемая на сетевые узлы ViPNet транспортным модулем ViPNet MFTP.

См. также: Транспортный модуль (MFTP) (на стр. 42).

Транспортный модуль (MFTP)

Компонент программного обеспечения ViPNet, предназначенный для обмена информацией в сети ViPNet.

Туннелирование

Технология, позволяющая защитить соединение с участием открытых узлов при передаче данных через Интернет и другие публичные сети. Туннелирование заключается в шифровании трафика открытых узлов координаторами.

См. также: Открытый узел (на стр. 29), Туннелируемый узел (на стр. 42), Туннелирующий координатор (на стр. 43).

Туннелируемый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне, но его трафик на потенциально опасном участке сети зашифровывается и расшифровывается на координаторе, за которым он стоит.

См. также: Клиент (ViPNet-клиент) (на стр. 21), Координатор (ViPNet-координатор) (на стр. 23), Туннелирование (на стр. 42), Туннелирующий координатор (на стр. 43).

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

См. также: Координатор (ViPNet-координатор) (на стр. 23), Туннелирование (на стр. 42), Туннелируемый узел (на стр. 42).

Туннель

Канал связи между конечными точками сети или взаимодействующих сетей, созданный с помощью технологии туннелирования.

См. также: Туннелирование (на стр. 42).

Удаленное обновление ПО ViPNet

Централизованный процесс обновления программного обеспечения ViPNet на сетевых узлах ViPNet. Осуществляется из программы ViPNet Центр управления сетью или ViPNet Network Manager.

См. также: Обновление ПО ViPNet, Сетевой узел ViPNet (на стр. 38), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Удаленный защищенный узел

Узел с установленным на нем программным обеспечением ViPNet, находящийся вне локальной сети и устанавливающий соединение с ней через Интернет.

См. также: Защищенный узел (на стр. 19), Локальная сеть (LAN) (на стр. 24).

Удостоверяющий центр

В широком смысле, удостоверяющий центр — организация, осуществляющая выпуск сертификатов открытых ключей подписи пользователя, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускаются в программе ViPNet Удостоверяющий и ключевой центр (УКЦ).

В контексте сети ViPNet, термином «Удостоверяющий центр» также обозначается сетевой узел с установленной программой ViPNet Удостоверяющий и ключевой центр.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 37), Сеть ViPNet (на стр. 39), ViPNet Удостоверяющий и ключевой центр (УКЦ) (на стр. 11).

Файл лицензии

Специальный файл `infotecs.reg`, без которого невозможен запуск программ семейства ViPNet CUSTOM.

Файл с межсетевой информацией

Файл с расширением .lzh, содержащий межсетевую информацию. Этот файл создается в ЦУСе или ViPNet Network Manager и используется администраторами сетей ViPNet для установления межсетевого взаимодействия.

См. также: Администратор сети ViPNet (на стр. 12), Межсетевая информация (на стр. 25), Межсетевое взаимодействие (на стр. 26), ViPNet Центр управления сетью (ЦУС) (на стр. 11), ViPNet Network Manager (на стр. 10).

Центр регистрации

Компонент удостоверяющего центра. Центру регистрации делегируется часть функций удостоверяющего центра: регистрация пользователей, предоставление пользователям сертификатов открытого ключа подписи, изданных в удостоверяющем центре, и выполнение других операций.

См. также: Сертификат открытого ключа подписи пользователя (на стр. 37), Удостоверяющий центр (на стр. 43).

Цепочка сертификации

Упорядоченная последовательность сертификатов, соответствующая иерархии издателей этих сертификатов. Сертификат считается действительным, если цепочка сертификации полна (то есть завершается корневым сертификатом) и все входящие в нее сертификаты также действительны.

См. также: Корневой сертификат (на стр. 23), Сертификат открытого ключа подписи пользователя (на стр. 37).

Частный адрес

Для сетей на базе протокола IP, не требующих непосредственного подключения к Интернету, выделено три диапазона IP-адресов: 10.0.0.0–10.255.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255, которые никогда не используются в Интернете. Чтобы выйти в Интернет с адресом из такого диапазона, необходимо использовать межсетевой экран с функцией NAT или технологию прокси.

Любая организация может использовать любые наборы адресов из этих диапазонов для узлов своей локальной сети.

См. также: Межсетевой экран (на стр. 26), Прокси-сервер (на стр. 33), Публичный адрес (на стр. 34), Трансляция сетевых адресов (NAT) (на стр. 42).

Шаблон политики безопасности

Набор настроек, предназначенный для установки на сетевых узлах определенной политики безопасности. В шаблоне задаются необходимые сетевые фильтры и правила трансляции IP-адресов. Шаблон может быть назначен сетевым узлам и подразделениям.

См. также: Подразделение (на стр. 31), Сетевой узел ViPNet (на стр. 38).

Шаблон пользователя

Структура данных, содержащая набор соответствующих атрибутов. Используется для заполнения сведений о пользователе при регистрации в программе ViPNet Registration Point.

См. также: ViPNet Registration Point (на стр. 11).

Шаблон сертификата

Частично заполненная структура, содержащая набор расширений, которые определяют назначение сертификата.

Используется при создании запросов на сертификаты и издании сертификатов.

См. также: Запрос на сертификат (на стр. 18), Расширения сертификата открытого ключа подписи пользователя (на стр. 34), Сертификат открытого ключа подписи пользователя (на стр. 37).

Широковещательный пакет

Пакет, предназначенный всем компьютерам, относящимся к одной подсети, определенной соответствующей маской.

См. также: Подсеть (на стр. 31).

Шлюз

Устройство, предназначенное для соединения двух сетей с разными канальными протоколами. Перед передачей данных из одной сети в другую шлюз их преобразует, обеспечивая совместимость протоколов.

Шлюзовой координатор

Координатор, через который осуществляется обмен транспортными конвертами между сетями ViPNet, установившими межсетевое взаимодействие.

Шлюзовые координаторы назначаются в ЦУСе каждой сети при организации взаимодействия между двумя различными сетями ViPNet.

См. также: Координатор (ViPNet-координатор) (на стр. 23), Межсетевое взаимодействие (на стр. 26), Сеть ViPNet (на стр. 39), Транспортный конверт (на стр. 42), ViPNet Центр управления сетью (ЦУС) (на стр. 11).

Штамп времени

Реквизит электронного документа, которым Служба штампов времени удостоверяет, что в указанный момент времени ей было предоставлено значение хэш-функции данного документа. Штамп времени подтверждает точное время создания документа. Также может подтверждать время получения или отправления документа.

В штампе времени указывается следующее: значение хэш-функции документа, на который выдан штамп; идентификатор политики (OID), в соответствии с которой был выдан штамп; время выдачи штампа; точность времени и другие параметры.

См. также: Идентификатор объекта (OID) (на стр. 20), Электронная подпись (на стр. 47), TSP-сервер (Служба штампов времени) (на стр. 10).

Электронная подпись

Реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата открытого ключа подписи пользователя, а также установить отсутствие искажения информации в электронном документе.

См. также: Закрытый ключ (на стр. 18), Сертификат открытого ключа подписи пользователя (на стр. 37).