



Основные термины и определения

Приложение к документации ViPNet CUSTOM

1991–2011 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00068-02 90 02

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet является зарегистрированной торговой маркой программного обеспечения, разрабатываемого ОАО «ИнфоТеКС».

Все торговые марки и названия программ являются собственностью их владельцев.

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
Абонентский пункт (АП).....	8
Абонентский пункт с ЦУС (АП ЦУС)	8
Администратор сетевого узла ViPNet	8
Администратор сети ViPNet.....	9
Администратор УКЦ.....	9
Администратор ЦУС.....	9
Адрес источника.....	9
Адрес назначения	9
Адреса видимости	10
Адреса доступа	10
Адресные справочники.....	10
Антиспуфинг.....	10
Асимметричный ключ	10
Аутентификация.....	11
Виртуальная защищенная сеть.....	11
Виртуальный IP-адрес.....	11
Внешние IP-адреса	11
Внешний сетевой интерфейс.....	11
Внешняя сеть	12
Внутренние IP-адреса	12
Внутренний сетевой интерфейс.....	12
Внутренняя сеть	12
Входящее соединение	12
Выпуск (издание) сертификата	12
Вышестоящий удостоверяющий центр.....	13
Глобальная сеть.....	13
Граница локальной сети	13
Группа сетевых узлов	13
Динамическая трансляция сетевых адресов	13
Динамический адрес	14
Дистрибутив ключей.....	14

Доверенная сеть.....	14
Допустимые в Интернете IP-адреса.....	14
Журнал событий.....	14
За координатором (узел, стоящий за координатором).....	15
Защищенное межсетевое соединение.....	15
Защищенное соединение	15
Защищенные прикладные серверы.....	15
Защищенный DNS или WINS сервер	15
Защищенный IP-трафик.....	15
Защищенный узел.....	16
Иерархия удостоверяющих центров.....	16
Инкапсуляция пакетов	16
Исходящее соединение	16
Клиент (ViPNet-клиент).....	16
Ключ защиты УКЦ.....	16
Ключ обмена.....	16
Ключи пользователя ViPNet.....	17
Ключи узла ViPNet.....	17
Коллектив.....	17
Компрометация ключей.....	18
Контейнер ключей.....	18
Контрольная сумма	18
Координатор (ViPNet-координатор).....	18
Корневой сертификат.....	18
Головной удостоверяющий центр	19
Кросс-сертификат.....	19
Кросс-сертификация	19
Лицензия	19
Лицензия на сеть ViPNet CUSTOM.....	20
Локальная сеть (LAN).....	20
Маршрутизатор	20
Маршрутизация	20
Маска подсети	20
Межсетевая информация.....	21
Межсетевое взаимодействие	21
Межсетевой мастер-ключ.....	21
Межсетевой экран (МЭ)	21

Межсетевые связи	22
Необработанная межсетевая информация	22
Обновление ключей узла	22
Обновление справочно-ключевой информации	23
Обработка межсетевой информации	23
Общий коллектив	23
Обязательные связи	24
Отзыв сертификата	24
Отклоненная межсетевая информация	24
Открытый Интернет	25
Открытый ключ	25
Открытый сервер DNS или WINS	25
Открытый трафик	25
Открытый узел	25
Папка (каталог) ключей пользователя	25
Папка справочно-ключевой информации	26
Пароль администратора сетевого узла ViPNet	26
Пароль пользователя	26
Пароль пользователя на основе парольной фразы	26
Парольная фраза	27
Персональный ключ пользователя	27
По умолчанию (настройка или значение)	27
Подсеть	28
Подчиненный удостоверяющий центр	28
Политика информационной безопасности	28
Полномочия пользователя	28
Порт источника	28
Порт назначения	28
Порт сетевой	29
Правило фильтрации	29
Прикладная задача	29
Прикладной конверт	29
Принятая межсетевая информация	29
Приостановление действия сертификата	30
Прокси-сервер	30
Протокол 241	30
Публикация	30

Публичный адрес	30
Рабочее место администратора сети ViPNet.....	30
Реальный IP-адрес	31
Резервный набор персональных ключей (РНПК)	31
Своя сеть (в контексте ViPNet CUSTOM)	31
Сегмент сети	31
Сервер-маршрутизатор (СМ)	31
Сервер IP-адресов.....	32
Сертификат издателя	32
Сертификат открытого ключа подписи пользователя	32
Сетевая атака	32
Сетевая группа.....	32
Сетевое имя компьютера.....	33
Сетевой интерфейс.....	33
Сетевой объект	33
Сетевой протокол	33
Сетевой узел ViPNet (СУ)	33
Сеть.....	34
Сеть ViPNet.....	34
Симметричный ключ	34
Служба DHCP.....	34
Служба DNS.....	34
Служебный конверт	35
Список отозванных сертификатов (СОС).....	35
Справочно-ключевая информация	35
Статическая трансляция сетевых адресов.....	35
Статический адрес.....	35
Структура сети ViPNet.....	36
Таблица маршрутизации.....	36
Точка распространения данных	37
Трансляция сетевых адресов (NAT)	37
Транспортный каталог	37
Транспортный конверт	37
Транспортный модуль (MFTP)	37
Трафик.....	37
Туннелирование.....	38
Туннелируемый узел.....	38

Туннелирующий координатор	38
Туннель.....	38
Удаленная сессия	38
Удаленное обновление ПО ViPNet.....	39
Удаленный защищенный узел.....	39
Удостоверяющий и ключевой центр (УКЦ).....	39
Удостоверяющий центр.....	39
Уполномоченное лицо (администратор) Удостоверяющего центра	39
Файл лицензии.....	40
Файл с межсетевой информацией.....	40
Центр управления сетью (ЦУС).....	40
Частный адрес.....	40
Широковещательный пакет.....	41
Шлюз	41
Шлюзовой координатор.....	41
Электронная подпись.....	41
DHCP (Dynamic Host Configuration Protocol)	42
DMZ (демилитаризованная зона).....	42
FTP (File Transfer Protocol)	42
IP forwarding.....	42
IP-адрес.....	42
IP-пакет.....	42
IP-трафик.....	43
LDAP (Lightweight Directory Access Protocol)	43
Microsoft SQL Server	43
PKI (инфраструктура открытых ключей).....	43
URL-адрес	43
ViPNet Administrator	43



Основные термины и определения ViPNet

Абонентский пункт (АП)

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

См. также: [Координатор \(ViPNet-координатор\)](#), [Маршрутизация](#), [Сетевой узел ViPNet \(СУ\)](#).

Абонентский пункт с ЦУС (АП ЦУС)

Абонентский пункт, назначенный в качестве Центра управления сетью.

См. также: [Абонентский пункт \(АП\)](#), [Центр управления сетью \(ЦУС\)](#).

Администратор сетевого узла ViPNet

Лицо, ответственное за настройку программного обеспечения ViPNet на сетевом узле ViPNet.

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Администратор сети ViPNet

Лицо, отвечающее за конфигурирование сети ViPNet, создание и обновление справочно-ключевой информации для сетевых узлов ViPNet, настройку межсетевое взаимодействия с доверенными сетями и обладающее правом доступа к программе ViPNet Manager или ViPNet ЦУС и (или) ViPNet УКЦ.

См. также: [Доверенная сеть](#), [Межсетевое взаимодействие](#), [Обновление справочно-ключевой информации](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Администратор УКЦ

Лицо, обладающее правом доступа в Удостоверяющий и ключевой центр (УКЦ), отвечающее за создание и обновление справочно-ключевой информации сетевых узлов ViPNet, создание и отзыв сертификатов ViPNet, обеспечение взаимодействия с доверенными сетями ViPNet.

См. также: [Доверенная сеть](#), [Обновление справочно-ключевой информации](#), [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Администратор ЦУС

Лицо, обладающее правом доступа в Центр управления сетью (ЦУС) и отвечающее за конфигурирование сети ViPNet.

См. также: [Сеть ViPNet](#), [Центр управления сетью \(ЦУС\)](#).

Адрес источника

Адрес сетевого устройства, отправившего IP-пакет.

См. также: [IP-пакет](#).

Адрес назначения

Адрес сетевого устройства, на которое отправлен IP-пакет.

См. также: [IP-пакет](#).

Адреса видимости

IP-адреса, виртуальные или реальные, по которым данный узел видит остальные узлы сети ViPNet.

См. также: [Виртуальный IP-адрес](#), [Реальный IP-адрес](#).

Адреса доступа

IP-адреса, по которым можно получить сетевой доступ к определенному узлу.

См. также: [IP-адрес](#).

Адресные справочники

Набор файлов, содержащих информацию об объектах сети ViPNet (узлах, пользователях, коллективах), в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются управляющими приложениями ViPNet, предназначенными для создания структуры и конфигурирования сети ViPNet (ViPNet ЦУС, ViPNet Manager).

См. также: [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Антиспуфинг

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

См. также: [Межсетевой экран \(МЭ\)](#).

Асимметричный ключ

Один из двух ключей (закрытый или открытый), которые используются в инфраструктуре открытых ключей (Public Key Infrastructure (PKI)). При использовании PKI создаются два взаимосвязанных асимметричных ключа: закрытый ключ и открытый ключ. В зависимости от назначения различают асимметричные ключи подписи и асимметричные ключи шифрования.

См. также: [PKI \(инфраструктура открытых ключей\)](#).

Аутентификация

Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности). Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагает субъект.

Виртуальная защищенная сеть

Технология, при которой происходит обмен информацией с удаленной локальной сетью или компьютером во внешней сети через виртуальные каналы связи, создаваемые поверх существующей сети. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменения передаваемых по логической сети сообщений).

См. также: [Аутентификация](#), [Внешняя сеть](#), [PKI \(инфраструктура открытых ключей\)](#).

Виртуальный IP-адрес

Виртуальный IP-адрес назначается непосредственно на данном узле (А) для узла (Б) и привязывается к идентификатору сетевого узла (Б). Использование виртуальных адресов позволяет устранить конфликт, если узлы работают в локальных сетях с пересекающимся адресным пространством, и скрыть реальную топологию сети.

См. также: [Реальный IP-адрес](#), [IP-адрес](#).

Внешние IP-адреса

Адреса внешней сети.

См. также: [Внешняя сеть](#).

Внешний сетевой интерфейс

Сетевой интерфейс, к которому подключена внешняя (глобальная) сеть, как правило, Интернет.

См. также: [Внешняя сеть](#), [Глобальная сеть](#), [Сетевой интерфейс](#).

Внешняя сеть

Сеть, имеющая другое адресное пространство по отношению к внутренней сети. Как правило, этот термин используется для обозначения глобальной сети Интернет.

См. также: [Внутренняя сеть](#).

Внутренние IP-адреса

Адреса внутренней сети.

См. также: [Внутренняя сеть](#).

Внутренний сетевой интерфейс

Сетевой интерфейс, к которому подключена внутренняя сеть.

См. также: [Внутренняя сеть](#), [Сетевой интерфейс](#).

Внутренняя сеть

Локальная сеть, которую требуется защитить.

См. также: [Внешняя сеть](#), [Локальная сеть \(LAN\)](#).

Входящее соединение

Соединение с вашим узлом, инициируемое другим узлом.

Выпуск (издание) сертификата

Заполнение необходимых полей сертификата и заверение его электронной подписью Удостоверяющего центра.

См. также: [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Электронная подпись](#).

Вышестоящий удостоверяющий центр

Если удостоверяющий центр (А) является вышестоящим по отношению к удостоверяющему центру (Б), это значит, что он находится выше УЦ (Б) в иерархической системе доверительных отношений между удостоверяющими центрами. Может быть подчиненным по отношению к удостоверяющему центру (В), если не является головным.

См. также: [Головной удостоверяющий центр](#), [Подчиненный удостоверяющий центр](#), [Удостоверяющий центр](#).

Глобальная сеть

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

Граница локальной сети

Условное понятие, означающее точку выхода из локальной сети в глобальную сеть или другую локальную.

См. также: [Глобальная сеть](#), [Локальная сеть \(LAN\)](#).

Группа сетевых узлов

Именованное множество сетевых узлов ViPNet (см. «[Сетевой узел ViPNet \(СУ\)](#)»). Объединяет сетевые узлы ViPNet для удобства администрирования. Например, позволяет объединять пользователей в один тип коллектива, зарегистрированный более чем на одном СУ, а также для задания одного и того же пароля администратора СУ ViPNet.

См. также: [Пароль администратора сетевого узла ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Динамическая трансляция сетевых адресов

Технология, с помощью которой осуществляется динамическое назначение внешних адресов узлам внутренней сети, когда они пытаются установить соединение с узлами во внешней сети. Узлы внешней сети не могут инициировать соединение с узлами внутренней сети, если их внешние адреса назначаются динамически.

См. также: [Внешние IP-адреса](#), [Внешняя сеть](#), [Внутренние IP-адреса](#), [Внутренняя сеть](#), [Статическая трансляция сетевых адресов](#), [Трансляция сетевых адресов \(NAT\)](#).

Динамический адрес

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

См. также: [Служба DHCP](#).

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр или ViPNet Manager для каждого пользователя сетевого узла ViPNet. В этом файле помещены адресные справочники, ключевая информация 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: [Адресные справочники](#), [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Файл лицензии](#).

Доверенная сеть

Сеть ViPNet, с узлами которой своя сеть ViPNet осуществляет защищенное взаимодействие.

См. также: [Межсетевое взаимодействие](#), [Своя сеть](#) (см. «[Своя сеть \(в контексте ViPNet CUSTOM\)](#)»).

Допустимые в Интернете IP-адреса

Все IP-адреса, кроме зарезервированных для использования в локальных сетях частных IP-адресов.

См. также: [Локальная сеть \(LAN\)](#), [Частный адрес](#).

Журнал событий

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

За координатором (узел, стоящий за координатором)

Сетевой узел ViPNet, использующий координатор в качестве межсетевого экрана. Все защищенные IP-пакеты от этого узла автоматически маршрутизируются на данный координатор, а затем отправляются дальше уже от имени этого координатора.

См. также: [Защищенный IP-трафик](#), [Координатор \(ViPNet-координатор\)](#), [Межсетевой экран \(МЭ\)](#), [Сетевой узел ViPNet \(СУ\)](#).

Защищенное межсетевое соединение

Защищенное с помощью ПО ViPNet соединение между сетевыми узлами своей и доверенной сетей.

См. также: [Доверенная сеть](#), [Своя сеть](#) (см. «[Своя сеть \(в контексте ViPNet CUSTOM\)](#)»).

Защищенное соединение

Соединение между узлами, зашифрованное с помощью ПО ViPNet.

Защищенные прикладные серверы

Прикладные серверы (web-сервер, почтовый сервер, FTP-сервер и т.д.), размещенные на защищенных узлах.

См. также: [Защищенный узел](#).

Защищенный DNS или WINS сервер

Сервер DNS или WINS, размещенный на защищенном узле.

См. также: [Защищенный узел](#).

Защищенный IP-трафик

Поток IP-пакетов, зашифрованных с помощью ПО ViPNet.

См. также: [IP-пакет](#).

Защищенный узел

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

Иерархия удостоверяющих центров

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

См. также: [Вышестоящий удостоверяющий центр](#), [Головной удостоверяющий центр](#), [Подчиненный удостоверяющий центр](#), [Удостоверяющий центр](#).

Инкапсуляция пакетов

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

Исходящее соединение

Соединение, инициированное вашим сетевым узлом.

Клиент (ViPNet-клиент)

Сетевой узел, на котором установлена программа ViPNet Client.

Ключ защиты УКЦ

Ключ, на котором защищены список администраторов Удостоверяющего и ключевого центра, мастер-ключи, пароли пользователей ViPNet, ключи пользователя при хранении их в УКЦ.

См. также: [Администратор УКЦ](#), [Ключи пользователя ViPNet](#), [Пароль пользователя](#).

Ключ обмена

Симметричный ключ, известный отправителю и получателю зашифрованной информации.

См. также: [Симметричный ключ](#).

Ключи пользователя ViPNet

Совокупность файлов, необходимых пользователю для аутентификации в сети ViPNet, к которым имеет доступ только данный пользователь.

Ключи пользователя могут содержать:

- действующий персональный ключ пользователя;
- случайный ключ защиты пользователя;
- контейнер с ключом (ключами) подписи;
- файл хэша пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

См. также: [Аутентификация](#), [Персональный ключ пользователя](#).

Ключи узла ViPNet

Совокупность файлов, необходимых пользователям сетевых узлов ViPNet для защиты информации приложений ViPNet, хранимой локально на компьютере, и (или) трафика, а также для проверки электронной подписи.

См. также: [Сетевой узел ViPNet \(СУ\)](#), [Электронная подпись](#).

Коллектив

Совокупность пользователей одного сетевого узла ViPNet, имеющих одни и те же ключи для шифрования конфиденциальной информации.

См. также: [Сетевой узел ViPNet \(СУ\)](#).

Компрометация ключей

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

После компрометации необходимо создать ключи пользователя и ключи узлов и выслать обновления на сетевые узлы ViPNet. Поскольку изменяются как общие ключи, так и личные, а также ключи обмена, необходимо выслать ключи узлов на все сетевые узлы ViPNet, связанные с данным сетевым узлом.

См. также: [Ключ обмена](#), [Ключи пользователя ViPNet](#), [Ключи узла ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Контейнер ключей

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

При формировании запроса на обновление сертификата имя контейнера, в котором будет храниться новая пара ключей подписи (закрытый и сертификат), задается автоматически и имеет вид `sgn-<случайное число 16-ричного формата>`.

См. также: [Сертификат открытого ключа подписи пользователя](#).

Контрольная сумма

Значение, используемое для проверки целостности файла.

Координатор (ViPNet-координатор)

Сетевой узел с установленным программным обеспечением ViPNet Coordinator, выполняющий в рамках сети ViPNet серверные функции, маршрутизацию трафика и служебной информации.

См. также: [Маршрутизация](#), [Сеть ViPNet](#).

Корневой сертификат

Самоподписанный сертификат администратора сети ViPNet, являющийся последним сертификатом в цепочке доверия, то есть для корневого сертификата нет сертификата, на

котором его можно было бы проверить. С помощью корневого сертификата проверяется достоверность сертификатов пользователей сети ViPNet.

См. также: [Администратор сети ViPNet](#), [Сертификат открытого ключа подписи пользователя](#).

Головной удостоверяющий центр

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

См. также: [Вышестоящий удостоверяющий центр](#), [Иерархия удостоверяющих центров](#), [Подчиненный удостоверяющий центр](#), [Удостоверяющий центр](#).

Кросс-сертификат

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

См. также: [Кросс-сертификация](#), [Уполномоченное лицо \(администратор\) удостоверяющего центра](#).

Кросс-сертификация

Механизм установления доверительных отношений между удостоверяющими центрами.

См. также: [Удостоверяющий центр](#).

Лицензия

Разрешение на пользование определенным набором функций ПО ViPNet. Лицензия на сеть ViPNet определяет: максимальное количество координаторов, клиентов на координатор, незащищенных узлов для туннелирования одним координатором (туннелируемых соединений) и некоторые другие параметры.

См. также: [Клиент \(ViPNet-клиент\)](#), [Координатор \(ViPNet-координатор\)](#), [Сеть ViPNet](#), [Туннелирование](#).

Лицензия на сеть ViPNet CUSTOM

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet CUSTOM. В частности, лицензия на сеть ViPNet CUSTOM определяет: номер сети, максимальное количество координаторов и клиентов, максимальное суммарное количество адресов, туннелируемых координаторами сети, максимальное количество узлов в прикладных задачах, максимальную разрешенную версию ПО ViPNet, срок действия лицензии, номера подчиненных сетей и другие параметры.

См. также: [Клиент \(ViPNet-клиент\)](#), [Координатор \(ViPNet-координатор\)](#), [Прикладная задача](#), [Сеть ViPNet](#), [Туннелирование](#).

Локальная сеть (LAN)

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

Маршрутизатор

Сетевое устройство, используемое в компьютерных сетях передачи данных, которое на основании информации о топологии сети (таблицы маршрутизации), а также сетевого адреса назначения пакета определяет дальнейший маршрут пересылки пакетов их получателю. Обычно применяется для связи нескольких сегментов сети.

См. также: [Сегмент сети](#), [Таблица маршрутизации](#).

Маршрутизация

Процесс выбора пути для передачи информации.

Маска подсети

Битовая маска, определяющая, какая часть IP-адреса сетевого узла относится к адресу самой сети, а какая часть — к адресу узла в этой сети.

См. также: [Подсеть](#), [IP-адрес](#).

Межсетевая информация

Информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия.

См. также: [Доверенная сеть](#), [Межсетевое взаимодействие](#), [Своя сеть](#) (см. «[Своя сеть \(в контексте ViPNet CUSTOM\)](#)»).

Межсетевое взаимодействие

Между своей сетью и другими сетями ViPNet может быть организовано межсетевое взаимодействие. Межсетевое взаимодействие позволяет сетевым узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между сетевыми узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Своя сеть](#) (см. «[Своя сеть \(в контексте ViPNet CUSTOM\)](#)»).

Межсетевой мастер-ключ

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

См. также: [Ключ обмена](#), [Сетевой узел ViPNet \(СУ\)](#), [Сеть ViPNet](#).

Межсетевой экран (МЭ)

Устройство или программа, установленная на узле на границе сети, которая проверяет весь входящий и исходящий IP-трафик и принимает решение о возможности его дальнейшего направления к пункту назначения, т.е. служит для предотвращения несанкционированного доступа из одной сети в другую. МЭ обычно осуществляет преобразование внутренних адресов в адреса, доступные из внешней сети (выполняет NAT). В ViPNet различаются три типа МЭ с NAT:

- ViPNet-координатор — режим, при котором в роли МЭ выступает компьютер с установленным ПО ViPNet Coordinator, обеспечивающий NAT шифрованного трафика.
- Со статической трансляцией адресов — режим, при котором между защищенным узлом и внешней сетью находится МЭ, осуществляющий статическую трансляцию

адресов, то есть, обеспечивающий взаимодействие внешних узлов с определенным внутренним адресом сети по протоколу UDP с заданным портом.

- С динамической трансляцией адресов — режим, при котором между защищенным узлом и внешней сетью находится МЭ, осуществляющий динамическую трансляцию адресов. При этом необходимо наличие в открытой сети координатора для поддержки соединений. МЭ этого типа используется, когда подключение к внешней сети производится, например, через xDSL-модем, используемый как маршрутизатор, через беспроводные устройства, сеть GPRS, других провайдеров, которые предоставляют частные адреса.

См. также: [Внешняя сеть](#), [Внутренняя сеть](#), [Граница локальной сети](#), [Динамическая трансляция сетевых адресов](#), [Защищенный узел](#), [Маршрутизатор](#), [Статическая трансляция сетевых адресов](#), [Трансляция сетевых адресов \(NAT\)](#), [Частный адрес](#).

Межсетевые связи

Связи между сетевыми узлами ViPNet своей сети и доверенной сети, определяющие возможность обмена защищенными IP-пакетами.

См. также: [Доверенная сеть](#), [Своя сеть](#) (см. «[Своя сеть \(в контексте ViPNet CUSTOM\)](#)»).

Необработанная межсетевая информация

Межсетевая информация, полученная ViPNet Manager или ЦУС, но не обработанная администратором сети ViPNet.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Центр управления сетью \(ЦУС\)](#).

Обновление ключей узла

Совокупность файлов, к которым относятся справочники сертификатов администраторов УКЦ, списки отозванных сертификатов (как своей сети, так и доверенных), контрольные суммы паролей администраторов, корневые сертификаты администраторов доверенных сетей и служебная информация о пользователе данного узла (право подписи).

Фактически, обновление ключей узла является урезанным вариантом ключей узла ViPNet.

При внесении каких-либо изменений в структуру сети ViPNet администратором сети ViPNet адресные справочники и ключи узлов, которых коснулись эти изменения, тоже

изменяются. В этом случае администратор должен разослать обновления ключей узлов на эти узлы сети ViPNet.

Обновление ключей узла формируется в УКЦ, рассылается из ЦУСа. После обновления ключей узла изменяется справочно-ключевая информация для сетевых узлов ViPNet.

См. также: [Адресные справочники](#), [Доверенная сеть](#), [Ключи узла ViPNet](#), [Контрольная сумма](#), [Корневой сертификат](#), [Своя сеть](#) (см. «Своя сеть (в контексте ViPNet CUSTOM)»), [Список отозванных сертификатов \(СОС\)](#), [Справочно-ключевая информация](#).

Обновление справочно-ключевой информации

При различных изменениях в сети ViPNet (добавление, удаление сетевого узла ViPNet, добавление пользователя, издание нового сертификата и т.д.), производимых администратором в ЦУС, УКЦ, ViPNet Manager, может изменяться справочно-ключевая информация для сетевых узлов ViPNet. В этом случае администратор сети ViPNet централизованно высылает на СУ сформированные обновления из ЦУС или ViPNet Manager (возможно обновление как одного из совершенных изменений, так и всех одновременно).

См. также: [Администратор сети ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#), [Сеть ViPNet](#), [Справочно-ключевая информация](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Обработка межсетевой информации

Принятие или отклонение межсетевой информации администратором сети ViPNet в ЦУС или ViPNet Manager.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Общий коллектив

Коллектив, который автоматически регистрируется на сетевом узле и включает всех пользователей данного сетевого узла.

Ключи для обмена между общими коллективами сетевых узлов используются в программах:

- ViPNet Монитор для защиты трафика,
- ViPNet Деловая почта при зашифровании писем (если не нужно разграничивать доступ между пользователями сетевого узла ViPNet),
- ViPNet MFTP при обмене служебными конвертами.

См. также: [Коллектив](#).

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, за которым он стоит.

См. также: [За координатором](#) (см. «[За координатором \(узел, стоящий за координатором\)](#)»), [Клиент \(ViPNet-клиент\)](#), [Координатор \(ViPNet-координатор\)](#), [Сетевой узел ViPNet \(СУ\)](#), [Сеть ViPNet](#).

Отзыв сертификата

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

См. также: [Компрометация ключей](#).

Отклоненная межсетевая информация

Межсетевая информация, полученная ЦУС или ViPNet Manager и отклоненная администратором сети ViPNet.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Открытый Интернет

Технология, реализованная в ПО ViPNet, которая позволяет подключить группу компьютеров локальной сети, которым разрешена работа в Интернете, к открытым интернет-ресурсам, обеспечивая их изолированность от возможных атак извне без физического отключения от локальной сети.

См. также: [Локальная сеть \(LAN\)](#), [Сетевая атака](#).

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).

См. также: [Электронная подпись](#).

Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

См. также: [Открытый узел](#).

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел, с которым обмен информацией происходит в незашифрованном виде.

Папка (каталог) ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

См. также: [Ключи пользователя ViPNet](#).

Папка справочно-ключевой информации

Папка, в которую устанавливается дистрибутив ключей. Несколько программ ViPNet могут использовать одну и ту же папку справочно-ключевой информации.

См. также: [Дистрибутив ключей](#).

Пароль администратора сетевого узла ViPNet

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

См. также: [Администратор сети ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [ViPNet Manager](#).

Пароль пользователя

Индивидуальный пароль пользователя для работы в приложениях ViPNet на сетевом узле ViPNet. Первоначально создается администратором сети ViPNet в УКЦ или ViPNet Manager. Этот пароль может быть изменен пользователем на сетевом узле ViPNet.

См. также: [Администратор сети ViPNet](#), [Пользователь ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#), [ViPNet Manager](#).

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 русском, английском и немецком языках. Фразы представляют собой грамматически корректные конструкции, однако слова, составляющие фразу, выбираются случайным образом из большого по объему словаря (русского, немецкого или английского). 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 английской раскладке 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 «rfn.dtenfclj».

См. также: [Пароль пользователя](#), [Парольная фраза](#).

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 «**служащий латает рельс**» соответствует пароль «ske;kfnfhktm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

См. также: [Пароль пользователя на основе парольной фразы](#).

Персональный ключ пользователя

Главный ключ защиты ключей, к которым имеет доступ пользователь. Персональный ключ используется для защиты ключей пользователя. Действующий персональный ключ входит в состав ключей пользователя, поэтому его необходимо хранить в безопасном месте, так как компрометация этого ключа означает компрометацию всех других ключей пользователя и ключей защиты коллективов, в которых пользователь зарегистрирован. При компрометации ключей пользователя в УКЦ изменяется вариант персонального ключа пользователя (его порядковый номер в РНПК), при этом для него устанавливается следующий ключ из резервного набора персональных ключей (РНПК).

См. также: [Ключи пользователя ViPNet](#), [Коллектив](#), [Компрометация ключей](#), [Пользователь ViPNet](#), [Резервный набор персональных ключей \(РНПК\)](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

По умолчанию (настройка или значение)

Настройка или значение, автоматически заданное для программы или устройства без вмешательства пользователя.

Подсеть

Логически видимое подмножество IP-сети.

Подчиненный удостоверяющий центр

Удостоверяющий центр, которому в иерархической системе распространения доверительных отношений доверяет вышестоящий удостоверяющий центр.

См. также: [Вышестоящий удостоверяющий центр](#), [Головной удостоверяющий центр](#), [Иерархия удостоверяющих центров](#), [Удостоверяющий центр](#).

Политика информационной безопасности

Документально зафиксированная совокупность принципов, правил и рекомендаций, регулирующих управление, защиту и распределение информационных ресурсов в организации.

Полномочия пользователя

Права, определяющие допустимость различных действий пользователей на сетевом узле ViPNet по изменению настроек установленного на нем ПО ViPNet.

Администратор ЦУС выставляет полномочия пользователей одного сетевого узла ViPNet в рамках прикладной задачи. Если полномочия пользователя ограничены, ввод пароля администратора сетевого узла ViPNet снимет эти ограничения, предоставив максимальные полномочия в приложениях.

См. также: [Администратор ЦУС](#), [Пароль администратора сетевого узла ViPNet](#), [Прикладная задача](#), [Сетевой узел ViPNet \(СУ\)](#).

Порт источника

TCP- или UDP-порт, используемый в качестве источника при установлении соединения (TCP) или отправке пакета (UDP).

Порт назначения

TCP- или UDP-порт, используемый принимающей стороной при установлении соединения (TCP) или приеме пакета (UDP).

Порт сетевой

Системный ресурс, выделяемый приложению для связи с другими приложениями, выполняемыми на узлах, доступных через сеть (в том числе другим приложением на этом же узле). Позволяет различным программам, выполняемым на одном узле, получать данные независимо друг от друга (предоставлять сетевые сервисы). Каждая программа обрабатывает данные, поступающие на определенный порт.

Правило фильтрации

Совокупность параметров, на основании которых ПО ViPNet принимает решение пропустить IP-пакет или заблокировать его. Фильтры определяют правила фильтрации.

Прикладная задача

Совокупность программных средств, предназначенных для решения целевых и служебных задач сети ViPNet. Прикладная задача выполняет две основные функции: используется в лицензировании сети с помощью файла infotecs.reg и определяет допустимость выполнения какой-либо функциональности ПО ViPNet для заданного сетевого узла.

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

Приложение ViPNet может включать в себя несколько прикладных задач. Каждая прикладная задача имеет свое название.

См. также: [Полномочия пользователя](#), [Сеть ViPNet](#).

Прикладной конверт

Файл, формируемый приложением «Деловая почта» или «Файловый обмен», для передачи другим сетевым узлам.

Принятая межсетевая информация

Межсетевая информация, полученная ЦУС или ViPNet Manager от другой сети, одобренная администратором принимающей сети, что позволяет установить межсетевое взаимодействие.

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Межсетевое взаимодействие](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Приостановление действия сертификата

Однократное временное ограничение действия сертификата в период его действия.

Прокси-сервер

Программа-посредник, транслирующая запросы различных протоколов из частной локальной сети во внешнюю сеть, выступая при этом как сервер между клиентами и реальным сервером.

См. [Внешняя сеть](#), [Локальная сеть \(LAN\)](#).

Протокол 241

IP-протокол с идентификатором 241, специально разработанный для ПО ViPNet.

Публикация

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

См. также: [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Публичный адрес

IP-адрес компьютера, который может применяться во внешних (глобальных) сетях (в том числе и в Интернете).

См. также: [Внешняя сеть](#), [Глобальная сеть](#), [IP-адрес](#).

Рабочее место администратора сети ViPNet

Компьютер, на котором установлено ПО ViPNet Manager или ЦУС/УКЦ.

См. также: [Сеть ViPNet](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Реальный IP-адрес

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

См. также: [Виртуальный IP-адрес](#), [Локальная сеть \(LAN\)](#), [Сетевой интерфейс](#), [IP-адрес](#).

Резервный набор персональных ключей (РНПК)

Администратор УКЦ создает для пользователя несколько запасных персональных ключей (в виде файла AAAA.pk, где AAAA – идентификатор пользователя в рамках своей сети). Резервный набор персональных ключей (РНПК) пользователя предназначен для удаленного обновления ключей пользователя при их компрометации и при смене мастер-ключа персональных ключей. Файл РНПК входит в состав дистрибутива ключей и передается пользователю вместе с ним или отдельно. Пользователи должны хранить РНПК в безопасном месте отдельно от ключей пользователя ViPNet.

См. также: [Администратор УКЦ](#), [Дистрибутив ключей](#), [Ключи пользователя ViPNet](#), [Компрометация ключей](#), [Персональный ключ пользователя](#).

Своя сеть (в контексте ViPNet CUSTOM)

Сеть ViPNet, номер которой указан в вашем файле infotecs.re.

См. также: [Сеть ViPNet](#).

Сегмент сети

Объединение узлов на физическом уровне.

Сервер-маршрутизатор (СМ)

Функциональность ПО ViPNet Coordinator, обеспечивающая маршрутизацию конвертов между узлами сети ViPNet.

См. также: [Координатор \(ViPNet-координатор\)](#), [Маршрутизация](#), [Сеть ViPNet](#).

Сервер IP-адресов

Функциональность ПО ViPNet Coordinator, обеспечивающая регистрацию, рассылку и предоставление информации о состоянии защищенных узлов (включен, выключен, информацию о подключении и т.д.).

См. также: [Защищенный узел](#), [Координатор \(ViPNet-координатор\)](#).

Сертификат издателя

Сертификат, с помощью закрытого ключа которого подписывается другой сертификат.

Сертификат открытого ключа подписи пользователя

Электронный документ заранее 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 сети ViPNet сертификат создается программой УКЦ и заверяется электронной подписью администратора УКЦ.

Электронная подпись Удостоверяющего центра (администратора УКЦ), заверяющая содержимое каждого сертификата, обеспечивает подлинность и целостность указанной в нем информации, включая описание владельца и его открытый ключ. Спецификация содержимого и формат сертификата в сети ViPNet соответствует стандарту X.509 версии 3 и Федеральному закону РФ № 63 «Об электронной подписи» от 6 апреля 2011 года.

См. также: [Администратор УКЦ](#), [Открытый ключ](#), [Электронная подпись](#).

Сетевая атака

Попытка злоумышленника вывести узел из строя (как 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.

Сетевая группа

Именованное множество сетевых узлов ViPNet. Объединяет сетевые узлы ViPNet для удобства администрирования. Например, позволяет объединять пользователей в один тип

коллектива, зарегистрированный более чем на одном сетевом узле ViPNet, а также для задания одного и того же пароля администратора сетевого узла ViPNet.

См. также: [Пароль администратора сетевого узла ViPNet](#), [Пользователь ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Сетевое имя компьютера

Имя компьютера в локальной сети.

См. также: [Локальная сеть \(LAN\)](#).

Сетевой интерфейс

Устройство для подключения компьютера к сети. Посредством сетевого интерфейса компьютером осуществляется прием и передача IP-пакетов. Сетевым интерфейсом может служить сетевая плата, модем и другие подобные устройства.

См. также: [Сеть, IP-адрес](#).

Сетевой объект

Сетевой узел либо группа сетевых узлов.

Сетевой протокол

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

Сетевой узел ViPNet (СУ)

Узел с установленным ПО ViPNet, с помощью которого защищают информацию приложений ViPNet, хранимую локально на компьютере, и (или) трафик посредством шифрования, имитозащиты и электронной подписи.

См. также: [Сеть ViPNet](#), [Электронная подпись](#).

Сеть

Два или более компьютеров, между которыми установлено соединение.

Сеть ViPNet

Логическая сеть, организованная с помощью ПО 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 \(СУ\)](#).

Симметричный ключ

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

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

См. также: [Прикладной конверт](#), [Служебный конверт](#).

Служба DHCP

Предназначена для динамического распределения адресов и некоторых сетевых параметров между подключенными к DHCP-серверу узлами.

См. также: [DHCP \(Dynamic Host Configuration Protocol\)](#).

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 в себе обновление справочно-ключевой информации или обновление ПО. Служебный конверт предназначен для выполнения задачи управления и формируется Центром управления сетью.

См. также: [Обновление ПО ViPNet](#), [Обновление справочно-ключевой информации](#), [Центр управления сетью \(ЦУС\)](#).

Список отозванных сертификатов (СОС)

Список сертификатов, которые были отозваны администратором Удостоверяющего центра и на данный момент недействительны.

См. также: [Уполномоченное лицо \(администратор\) Удостоверяющего центра](#).

Справочно-ключевая информация

Включает в себя адресные справочники, ключи узла и ключи пользователя. Изменяется при обновлении из Центра управления сетью или ViPNet Manager.

См. также: [Адресные справочники](#), [Ключи пользователя ViPNet](#), [Ключи узла ViPNet](#), [Обновление справочно-ключевой информации](#).

Статическая трансляция сетевых адресов

Технология, при которой создается постоянное соответствие между внешним IP-адресом или портом узла внутренней сети и IP-адресом или портом, в который он транслируется. Таким образом, IP-адрес узла внутренней сети всегда транслируется в один и тот же статический внешний адрес. Узлы внешней сети могут инициировать соединение с узлами внутренней сети, для которых задана статическая трансляция (если это разрешено правилами фильтрации).

См. также: [Внешние IP-адреса](#), [Внешняя сеть](#), [Внутренние IP-адреса](#), [Внутренняя сеть](#), [Динамическая трансляция сетевых адресов](#).

Статический адрес

Постоянный IP-адрес, прописанный на компьютере.

См. также: [IP-адрес](#).

Структура сети ViPNet

Для обеспечения безопасности корпоративной сети необходима установка программного обеспечения ViPNet, которое позволяет защитить весь сетевой трафик, а также информацию, хранящуюся на компьютерах. При этом доступ к защищенному компьютеру с открытых или других защищенных компьютеров может быть в той или иной степени ограничен.

Для организации такой защиты необходимо развернуть сеть ViPNet, базовыми компонентами которой являются:

- рабочее место администратора сети ViPNet с установленным ПО ViPNet Administrator и ViPNet Client или ViPNet CryptoService (для сети ViPNet CUSTOM) или ViPNet Manager и ViPNet Client (для сети ViPNet OFFICE) для организации обмена служебной информацией с другими узлами сети ViPNet;
- координаторы — серверы с установленным ПО ViPNet Coordinator, размещенные на границах сетей или сегментов сети;
- компьютеры пользователей с установленным клиентским ПО ViPNet Client (для сетей ViPNet CUSTOM и ViPNet OFFICE) или ViPNet CryptoService (только для сетей ViPNet CUSTOM).

Каждый клиентский узел должен быть зарегистрирован на координаторе. Каналы 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: [«ViPNet Administrator»](#), [«Координатор \(ViPNet-координатор\)»](#), [«Защищенный узел»](#), [«Открытый узел»](#), [«Сеть ViPNet»](#), [«Граница локальной сети»](#), [«Обязательные связи»](#), [«Рабочее место администратора сети ViPNet»](#), [«Сегмент сети»](#).

Таблица маршрутизации

Таблица, согласно которой происходит процесс выбора оптимального пути для передачи информации.

См. также: [Маршрутизация](#).

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: [FTP \(File Transfer Protocol\)](#), [LDAP \(Lightweight Directory Access Protocol\)](#), [Сертификат издателя](#), [Список отозванных сертификатов \(COC\)](#), [Удостоверяющий центр](#).

Трансляция сетевых адресов (NAT)

Технология, позволяющая преобразовывать IP-адреса, используемые в одной сети, в адреса, используемые в другой. При этом одна сеть будет называться внутренней сетью, другая — внешней.

Например, NAT служит для преобразования адресов, зарезервированных для использования в локальных сетях, в адреса Интернета.

См. также: [Внешняя сеть](#), [Внутренняя сеть](#), [Динамическая трансляция сетевых адресов](#), [Статическая трансляция сетевых адресов](#).

Транспортный каталог

См. [Папка справочно-ключевой информации](#).

Транспортный конверт

Информация служб или приложений в защищенном виде, доставляемая узлам ViPNet транспортным модулем ViPNet MFTP.

См. также: [Транспортный модуль \(MFTP\)](#).

Транспортный модуль (MFTP)

Программный модуль, предназначенный для обмена информацией в сети ViPNet.

Трафик

Поток данных, передаваемых по сети.

См. также: [IP-трафик](#).

Туннелирование

Шифрование трафика открытых узлов при передаче через сеть общего пользования.

См. также: [Открытый узел](#).

Туннелируемый узел

Узел, на котором не установлено ПО 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: [За координатором \(узел, стоящий за координатором\)](#), [Клиент \(ViPNet-клиент\)](#), [Координатор \(ViPNet-координатор\)](#), [Туннелирование](#).

Туннелирующий координатор

Одна из функциональных составляющих ПО ViPNet Coordinator, определяемая в ЦУС или ViPNet Manager, при которой обеспечивается туннелирование трафика от заданных компьютеров локальной сети, на которых по каким-либо причинам невозможно установить ПО ViPNet Client или ViPNet Coordinator. При этом трафик остается открытым только на участке от туннелируемого узла до этого координатора, а в дальнейшем весь трафик идет в зашифрованном виде.

См. также: [Координатор \(ViPNet-координатор\)](#), [Открытый трафик](#), [Туннелирование](#), [Туннелируемый узел](#).

Туннель

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

См. также: [Туннелирование](#).

Удаленная сессия

Сессия, инициированная через сеть, стартующая на сервере при подключении терминального клиента к терминальным службам.

Удаленное обновление ПО ViPNet

Централизованный процесс обновления ПО на сетевых узлах ViPNet, которое проводит администратор ЦУС.

См. также: [Администратор ЦУС](#), [Обновление ПО ViPNet](#), [Сетевой узел ViPNet \(СУ\)](#).

Удаленный защищенный узел

Узел с установленным на нем программным обеспечением ViPNet, находящийся вне локальной сети и выходящий на связь через Интернет.

См. также: [Защищенный узел](#), [Локальная сеть \(LAN\)](#).

Удостоверяющий и ключевой центр (УКЦ)

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

См. также: [Администратор УКЦ](#), [Корневой сертификат](#), [Пользователь ViPNet](#), [Список отозванных сертификатов \(СОС\)](#), [ViPNet Administrator](#).

Удостоверяющий центр

Удостоверяющий центр (англ. Certificate authority, CA) — сервис, осуществляющий выпуск сертификатов ключей электронной подписи, а также сертификатов другого назначения. В сетях ViPNet сертификаты выпускает Удостоверяющий и ключевой центр (УКЦ).

См. также: [Сертификат открытого ключа подписи пользователя](#), [Сеть ViPNet](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#).

Уполномоченное лицо (администратор) Удостоверяющего центра

Лицо, обладающее правом заверять сертификаты от имени удостоверяющего центра.

См. также: [Удостоверяющий центр](#).

Файл лицензии

Специальный файл, создаваемый ОАО «Инфотекс» (infotecs.re), без которого невозможен запуск программ семейства ViPNet CUSTOM.

Файл с межсетевой информацией

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

См. также: [Администратор сети ViPNet](#), [Межсетевая информация](#), [Межсетевое взаимодействие](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

Центр управления сетью (ЦУС)

Программа, входящая в ПО ViPNet Administrator. Предназначена для создания и управления конфигурацией сети и позволяет решить следующие основные задачи:

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

См. также: [Адресные справочники](#), [Полномочия пользователя](#), [Сетевой объект](#), [Удостоверяющий и ключевой центр \(УКЦ\)](#), [ViPNet Administrator](#).

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 применяются в Интернете. Если вы имеете адрес из такого диапазона и хотите выйти в Интернет, используйте межсетевой экран с NAT.

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

См. также: [Межсетевой экран \(МЭ\)](#), [Трансляция сетевых адресов \(NAT\)](#).

Широковещательный пакет

Пакет, предназначенный всем компьютерам, относящимся к одной подсети.

См. также: [Подсеть](#).

Шлюз

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

См. также: [Локальная сеть \(LAN\)](#).

Шлюзовой координатор

Координатор, через который осуществляется межсетевое взаимодействие с доверенной сетью.

Шлюзовые координаторы назначаются в ЦУС (ViPNet Manager) каждой сети при организации взаимодействия между двумя различными сетями ViPNet. В настройках транспортного модуля можно изменить маршрутизацию почтовых конвертов в другие сети.

См. также: [Доверенная сеть](#), [Маршрутизация](#), [Межсетевое взаимодействие](#), [Транспортный модуль \(MFTP\)](#), [Центр управления сетью \(ЦУС\)](#), [ViPNet Manager](#).

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 ключа подписи, а также установить отсутствие искажения информации в электронном документе.

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 (демитаризованная 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](#), [Внутренняя сеть](#), [Межсетевой экран \(МЭ\)](#), [Сегмент сети](#).

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 forwarding

Функция в операционной системе, которая отвечает за включение механизма маршрутизации IP-трафика.

См. [Маршрутизация, IP-трафик](#).

IP-адрес

Адрес узла в сети, построенной по протоколу IP.

IP-пакет

Форматированный блок информации, передаваемый по сети по протоколу IP.

IP-трафик

Поток данных, передаваемых в сети по протоколу IP.

См. также: [IP-пакет](#).

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.

Microsoft SQL Server

Система управления реляционными базами данных, разработанная Microsoft.

PKI (инфраструктура открытых ключей)

PKI (инфраструктура открытых ключей) — комплекс аппаратных и программных средств, политик и процедур, обеспечивающих распространение доверительного отношения к открытым ключам в распределённых системах через создание сертификатов открытых ключей и поддержание их жизненного цикла.

См. также: [Открытый ключ](#).

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 ЦУС и УКЦ.

См. также: [Сеть ViPNet, Удостоверяющий и ключевой центр \(УКЦ\), Центр управления сетью \(ЦУС\)](#).