A low-angle, upward-looking photograph of a modern skyscraper with a glass facade. The building's structure is composed of a grid of dark metal frames and large glass panels. The sky is visible through the glass, and the building's lines converge towards the top of the frame, creating a sense of height and scale. A semi-transparent dark grey rectangle covers the bottom half of the image, serving as a background for the text.

Основные термины и определения

Приложение к документации ViPNet

1991–2017 ОАО «ИнфоТеКС», Москва, Россия

ФРКЕ.00068-09 90 02

Версия продукта

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 зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

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

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

Сайт компании «ИнфоТеКС»: <https://infotecs.ru/>

Электронный адрес службы поддержки: hotline@infotecs.ru

Содержание


Основные термины и определения ViPNet	8
Active Directory (AD)	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
NTP-сервер	9
OCSP-сервер (сервис проверки статуса сертификатов)	9
PKI (инфраструктура открытых ключей)	9
TCP-туннель	10
TSP-сервер (служба штампов времени)	10
URL-адрес	10
ViPNet Administrator	10
ViPNet CSP	10
ViPNet Policy Manager	10
ViPNet Registration Point	10
ViPNet Удостоверяющий и ключевой центр (УКЦ)	11
ViPNet Центр управления сетью (ЦУС)	11
Авторизация	11
Администратор сети ViPNet	11
Администратор УКЦ	11
Администратор ЦУСа	11
Адрес источника	12
Адрес назначения	12
Адреса видимости	12
Адреса доступа	12
Аккредитованный удостоверяющий центр	12
Аннулирование сертификата	12
Антиспуфинг	12
Асимметричное шифрование	12
Аутентификация	12
Виртуальная защищенная сеть	13
Виртуальный IP-адрес	13

Внешние IP-адреса.....	13
Внешний сетевой интерфейс.....	13
Внешняя сеть.....	13
Внутренние IP-адреса.....	13
Внутренний сетевой интерфейс.....	13
Внутренняя сеть.....	14
Входящее соединение.....	14
Вышестоящий удостоверяющий центр.....	14
Глобальная сеть.....	14
Главной удостоверяющий центр.....	14
Граница локальной сети.....	14
Группа узлов.....	14
Динамический адрес.....	14
Дистрибутив ключей.....	14
Доверенная сеть.....	15
Доверенное лицо (администратор) удостоверяющего центра.....	15
Журнал событий.....	15
Запрос на сертификат.....	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
Идентификатор объекта (OID).....	16
Иерархия удостоверяющих центров.....	16
Инкапсуляция пакетов.....	16
Исходящее соединение.....	16
Квалифицированный сертификат.....	16
Клиент (ViPNet-клиент).....	16
Ключ защиты.....	16
Ключ защиты УКЦ.....	17
Ключ обмена.....	17
Тип межсетевого экрана (ФСТЭК).....	17
Ключ проверки электронной подписи.....	17
Ключ электронной подписи.....	17
Ключи администратора УКЦ.....	17
Ключи пользователя ViPNet.....	18
Ключи узла ViPNet.....	18

Компрометация ключей	18
Контейнер ключей	18
Контейнер сертификатов администраторов	18
Контрольная сумма	18
Координатор (ViPNet-координатор)	18
Корневой сертификат	19
Кросс-сертификат	19
Кросс-сертификация	19
Лицензия на сеть	19
Локальная сеть (LAN)	19
Маршрутизатор	19
Маршрутизация	19
Мастер-ключ	20
Маска подсети	20
Межсетевая информация	20
Метрика адреса доступа	20
Межсетевое взаимодействие	20
Межсетевой мастер-ключ	20
Межсетевой экран	20
Межсетевые связи	21
Обновление справочников и ключей	21
Обработка межсетевой информации	21
Обязательные связи	21
Открытый Интернет (Защищенный интернет-шлюз)	21
Открытый сервер DNS или WINS	21
Открытый трафик	22
Открытый узел	22
Папка ключей пользователя	22
Папка ключей сетевого узла	22
Пароль администратора сетевого узла ViPNet	22
Пароль администратора УКЦ	22
Пароль пользователя	22
Пароль пользователя на основе парольной фразы	22
Парольная фраза	23
Персональный ключ пользователя	23
Подразделение	23
Подсеть	23
Подчиненный удостоверяющий центр	23
Политика безопасности	23

Политика применения сертификата	24
Политика штампов времени	24
Полномочия пользователя	24
Пользователь ViPNet.....	24
Порт источника	24
Порт назначения.....	24
Прикладной конверт.....	24
Приостановление действия сертификата	24
Прокси-сервер	24
Протокол 241	25
Протокол Диффи—Хеллмана	25
Публикация.....	25
Публичный адрес	25
Рабочее место администратора сети ViPNet.....	25
Расширения сертификата ключа проверки электронной подписи.....	25
Реальный IP-адрес.....	25
Резервный набор персональных ключей (РНПК)	25
Результирующая политика безопасности	26
Роль	26
Роль пользователей.....	26
Своя сеть	26
Сегмент сети.....	26
Сервер IP-адресов.....	26
Транспортный сервер	26
Сертификат издателя	27
Сертификат ключа проверки электронной подписи	27
Сетевая атака	27
Сетевой интерфейс.....	27
Сетевой объект.....	27
Сетевой порт.....	27
Сетевой протокол.....	27
Сетевой узел ViPNet	27
Сетевой фильтр	28
Сеть	28
Сеть ViPNet.....	28
Симметричное шифрование	28
Симметричный ключ	28
Служба DHCP	28
Служба DNS.....	28

Служебный конверт	28
Список аннулированных сертификатов (CRL)	29
Справочники	29
Справочники и ключи	29
Статический адрес	29
Терминальный сервер	29
Структура сети ViPNet	29
Таблица маршрутизации	29
Точка распространения данных	30
Транспортная квитанция	30
Трансляция сетевых адресов (NAT)	30
Транспортный конверт	30
Транспортный модуль (MFTP)	30
Туннелирование	30
Туннелируемый узел	30
Туннелирующий координатор	30
Туннель	31
Удаленное обновление ПО ViPNet	31
Удаленный защищенный узел	31
Идентификатор ключа субъекта	31
Удостоверяющий центр	31
Файл лицензии	31
Файл с межсетевой информацией	31
Центр регистрации	31
Модуль DPI	32
Цепочка сертификации	32
Частный адрес	32
Шаблон политики безопасности	32
Фильтрация содержимого трафика	32
Шаблон пользователя	32
Шаблон сертификата	32
Широковещательный пакет	33
Шлюз	33
Шлюзовой координатор	33
Штамп времени	33
Электронная подпись	33



Основные термины и определения ViPNet

Active Directory (AD)

Служба каталогов, разработанная Microsoft для доменных сетей Windows. Эта служба интегрирована в большинство операционных систем Windows Server.

Active Directory является центром администрирования и обеспечения безопасности сети. Она служит для аутентификации и авторизации всех пользователей и компьютеров внутри сети доменного типа Windows. При помощи Active Directory задаются и применяются политики безопасности для всех компьютеров в сети, а также устанавливается или обновляется программное обеспечение на компьютерах сети. Active Directory хранит данные и настройки среды в централизованной базе данных.

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.

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.

IP-пакет

Форматированный блок информации, передаваемый в сети по протоколу IP.

IP-трафик

Поток данных, передаваемых в сети по протоколу IP.

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.

NTP-сервер

Сервер точного времени, который необходим для синхронизации времени компьютеров, рабочих станций, серверов и прочих сетевых устройств. Этот сервер играет роль посредника между эталоном времени и сетью. Он получает время от эталона по специальному каналу (интерфейсу) и выдает его для любого узла сети, обеспечивая тем самым синхронизацию устройств.

OCSP-сервер (сервис проверки статуса сертификатов)

Доверенный субъект PKI, предоставляющий информацию о статусах сертификатов по соответствующим запросам в режиме реального времени.

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 том числе ключам проверки электронной подписи) в распределенных системах через создание сертификатов ключей проверки электронной подписи и поддержание их жизненного цикла.

TCP-туннель

Способ соединения клиентов ViPNet, находящихся во внешних сетях, со своим сервером соединений, а затем и с другими узлами сети ViPNet по протоколу TCP. Используется в том случае, если соединение по протоколу UDP заблокировано провайдерами услуг Интернета.

TCP-туннель настраивается на координаторе, который является для клиента сервером соединений.

TSP-сервер (служба штампов времени)

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

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.

ViPNet CSP

Программа ViPNet CSP представляет собой криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей ЭП.

ViPNet Policy Manager

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

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.

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 аннулированных сертификатов.

ViPNet Центр управления сетью (ЦУС)

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.

Авторизация

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

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.

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.

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.

Адрес источника

Адрес сетевого устройства, отправившего IP-пакет.

Адрес назначения

Адрес сетевого устройства, на которое отправлен IP-пакет.

Адреса видимости

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

Адреса доступа

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

Аккредитованный удостоверяющий центр

Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти. Удостоверяющий центр, прошедший аккредитацию в уполномоченном федеральном органе исполнительной власти - <http://minsvyaz.ru/ru/activity/govservices/2/#section-list-of-accredited-centers> в соответствии с требованиями Федерального закона от 6 апреля 2011г. № 63-ФЗ «Об электронной подписи».

Аннулирование сертификата

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

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).

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.

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).

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).

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.

Внешние IP-адреса

Адреса внешней сети.

Внешний сетевой интерфейс

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

Внешняя сеть

Сеть, отделенная от внутренней сети межсетевым экраном.

Внутренние IP-адреса

Адреса внутренней сети.

Внутренний сетевой интерфейс

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

Внутренняя сеть

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

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.

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.

Граница локальной сети

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

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.

Динамический адрес

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

Дистрибутив ключей

Файл с расширением `.dst`, создаваемый в программе ViPNet Удостоверяющий и ключевой центр 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.

Доверенная сеть

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

Доверенное лицо (администратор) удостоверяющего центра

Лицо, обладающее правом издавать сертификаты от имени удостоверяющего центра.

Журнал событий

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

Запрос на сертификат

Защищенное электронной подписью сообщение, содержащее имя пользователя, ключ проверки электронной подписи 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).

Защищенное межсетевое соединение

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

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.

Защищенный DNS или WINS сервер

Сервер DNS или WINS, размещенный на защищенном узле.

Защищенный IP-трафик

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

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.

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

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.

Ключ защиты

Ключ, на котором шифруется другой ключ.

Ключ защиты УКЦ

Ключ, на котором зашифрована вся информация, хранящаяся в программе ViPNet Удостоверяющий и ключевой центр (список администраторов УКЦ, мастер-ключи, пароли пользователей ViPNet, ключи пользователей, узлов и прочее).

Ключ защиты УКЦ входит в состав ключей администратора УКЦ и зашифрован на ключе защиты данного администратора.

Ключ обмена

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

Тип межсетевого экрана (ФСТЭК)

Совокупность особенностей межсетевых экранов в зависимости от их применения в информационных системах и технического исполнения (программное или программно-аппаратное), выделяемые классификацией ФСТЭК России. Выделены несколько типов межсетевых экранов: тип «А», тип «Б», тип „В“, тип «Г», тип «Д». Подробнее см. на сайте ФСТЭК России <http://www.fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1142-informatsionnoe-soobshchenie-fstek-rossii-ot-28-aprelya-2016-g-n-240-24-1986>.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Ключи администратора УКЦ

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

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

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;
- ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи;
- хэш пароля пользователя.

Содержимое ключей пользователя формируется в зависимости от типа аутентификации пользователя.

Ключи узла ViPNet

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

Компрометация ключей

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

Контейнер ключей

Файл или устройство, в котором хранятся ключ электронной подписи и соответствующий ему сертификат ключа проверки электронной подписи.

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.

Контрольная сумма

Значение, используемое для проверки целостности информации.

Координатор (ViPNet-координатор)

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

Корневой сертификат

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.

Кросс-сертификат

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

Кросс-сертификация

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

Лицензия на сеть

Разрешение на пользование определенным набором функций продуктовой линейки ViPNet. В частности, лицензия на сеть ViPNet 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.

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.

Маршрутизация

Процесс выбора пути для передачи информации в сети.

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.

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.

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, списки аннулированных сертификатов).

Метрика адреса доступа

Определяет задержку (в миллисекундах) отправки тестовых пакетов при выполнении опроса узла для определения доступности адреса. Предназначена для задания приоритета использования каналов связи.

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.

Межсетевой мастер-ключ

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

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).

Межсетевые связи

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

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.

Обработка межсетевой информации

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

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 транспортным сервером.

Открытый Интернет (Защищенный интернет-шлюз)

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.

Начиная с версии ПО ViPNet Administrator ЦУС 4.6.3, технология «Открытый Интернет» называется «Защищенный интернет-шлюз».

Открытый сервер DNS или WINS

Сервер DNS или WINS на открытом узле.

Открытый трафик

Поток незашифрованных IP-пакетов.

Открытый узел

Узел, на котором не установлено программное обеспечение ViPNet с функцией шифрования трафика на сетевом уровне.

Папка ключей пользователя

Папка, в которой находятся ключи пользователя ViPNet.

Папка ключей сетевого узла

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

Пароль администратора сетевого узла ViPNet

Пароль для входа на сетевом узле ViPNet в режим администратора, в рамках которого становятся доступны дополнительные возможности настройки приложений ViPNet. Пароль администратора сетевого узла ViPNet может быть создан администратором сети ViPNet в программе ViPNet Удостоверяющий и ключевой центр (в сетях, которые администрируются при помощи ПО ViPNet Administrator) или ViPNet Network Manager (в сетях, которые администрируются при помощи ПО ViPNet Network Manager).

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.

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».

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 «cke;kfnfhktm». В данном случае, при вводе пароля необходимо набирать по 4 первых буквы каждого слова парольной фразы.

Персональный ключ пользователя

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

Подразделение

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

Подсеть

Логически выделенное подмножество узлов сети.

Подчиненный удостоверяющий центр

Удостоверяющий центр, сертификат администратора которого заверен вышестоящим удостоверяющим центром.

Политика безопасности

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

Политика применения сертификата

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

Политика штампов времени

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

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.

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.

Прокси-сервер

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

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).

Публичный адрес

IP-адрес, который может применяться в Интернете.

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.

Расширения сертификата ключа проверки электронной подписи

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).

Реальный IP-адрес

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

Резервный набор персональных ключей (РНПК)

Набор из нескольких запасных персональных ключей, которые администратор УКЦ 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.

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.

Роль

Некоторая функциональность сетевого узла, предназначенная для решения целевых и служебных задач сети ViPNet. Роль используется в лицензировании сети с помощью файла лицензии 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.

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.

Сегмент сети

Объединение узлов на физическом уровне.

Сервер IP-адресов

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

Транспортный сервер

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

Сертификат издателя

Сертификат удостоверяющего центра, которым заверяются издаваемые сертификаты.

Сертификат ключа проверки электронной подписи

Сертификат ключа проверки — это электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевая атака

Компьютерная атака с использованием протоколов межсетевого взаимодействия.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN.

Сетевой объект

Сетевой узел, пользователь, группа узлов или группа пользователей.

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.

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).

Симметричное шифрование

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

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.

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.

Список аннулированных сертификатов (CRL)

Список сертификатов, которые до истечения срока их действия были аннулированы или приостановлены администратором Удостоверяющего центра и потому недействительны на момент, указанный в данном списке аннулированных сертификатов.

Справочники

Набор файлов, содержащих информацию об объектах сети ViPNet, в том числе об их именах, идентификаторах, адресах, связях. Эти файлы формируются в программе ViPNet Центр управления сетью, предназначенной для создания структуры и конфигурирования сети ViPNet.

Справочники и ключи

Справочники, ключи узла и ключи пользователя.

Статический адрес

Постоянный IP-адрес, присвоенный сетевому интерфейсу вручную.

Терминальный сервер

Выделенный компьютер, предоставляющий вычислительные ресурсы клиентам, которые подключаются к терминальному серверу по сети. Преимущества работы в терминальном режиме включают снижение расходов на программное и аппаратное обеспечение, уменьшение затрат времени на администрирование, повышение уровня защиты от внутренних злоумышленников.

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.

Таблица маршрутизации

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

Точка распространения данных

Источник, доступный по общеизвестным протоколам (например, HTTP или LDAP), используемый для размещения сформированной в удостоверяющем центре информации (сертификатов издателей и списков аннулированных сертификатов).

Транспортная квитанция

Файл, оповещающий отправителя о невозможности доставки конверта.

Трансляция сетевых адресов (NAT)

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

Транспортный конверт

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

Транспортный модуль (MFTP)

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

Туннелирование

Технология, позволяющая защитить соединения между узлами локальных сетей, которые обмениваются информацией через Интернет или другие публичные сети, путем инкапсуляции и шифрования трафика этих узлов не самими узлами, а координаторами, которые установлены на границе их локальных сетей. При этом установка программного обеспечения ViPNet на эти узлы необязательна, то есть туннелируемые узлы могут быть как защищенными, так и открытыми.

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.

Туннелирующий координатор

Координатор, который осуществляет туннелирование.

Туннель

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

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.

Удаленный защищенный узел

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

Идентификатор ключа субъекта

Идентификатор (уникальный номер) ключа электронной подписи владельца сертификата.

Удостоверяющий центр

Организация, осуществляющая выпуск сертификатов ключей проверки электронной подписи, а также сертификатов другого назначения.

Файл лицензии

Специальный файл *.itcslic или infotecs.reg, в котором зафиксированы ограничения для вашей сети ViPNet.

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.

Центр регистрации

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

Модуль DPI

программный модуль ПО ViPNet xFirewall, выполняющий фильтрацию трафика на прикладном уровне модели OSI для определенного набора приложений и протоколов.

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.

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.

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.

Фильтрация содержимого трафика

Функция, которая обеспечивает фильтрацию IP-трафика на прикладном уровне модели OSI с помощью технологии глубокой инспекции пакетов (Deep Packet Inspection, DPI) по типам приложений и прикладных протоколов, а также по пользователям.

Шаблон пользователя

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

Шаблон сертификата

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

Используется при создании запросов на сертификаты и издании сертификатов.

Широковещательный пакет

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

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.

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.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.