Столыпинский вестник

Научная статья

Original article

УДК 004.732.056

РЕАЛИЗАЦИЯ СЕРВЕРА VPN С РОССИЙСКИМИ КРИПТОАЛГОРИТМАМИ В ОТЕЧЕСТВЕННОЙ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ

IMPLEMENTATION OF A VPN SERVER WITH RUSSIAN CRYPTO ALGORITHMS IN A DOMESTIC SECURE OPERATING SYSTEM

Кладов В. Е., кандидат технических наук, доцент, доцент кафедры «Вычислительной техники и защиты информации» Уфимский университет науки и технологий Россия, г. Уфа lisinatanya02@yandex.ru

Лисина Т. Е., студент 4 курс, Институт информатики, математики и робототехники Уфимский университет науки и технологий Россия, г. Уфа lisinatanya02@yandex.ru

Kladov V. E., Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer Engineering and Information Security Ufa University of Science and Technology, Ufa, Russia lisinatanya02@yandex.ru

Lisina T. E., 4th year student, Institute of Computer Science, Mathematics and Robotics Ufa University of Science and Technology, Ufa, Russia, kokievagalia@mail.ru

Аннотация. Статья посвящена задаче перехода на отечественные решения в области защиты информации. При этом предлагается за счет использования защищенных операционных систем обойтись без

специализированных дополнительных средств защиты. В статье решается вопросы реализации виртуальных частных сетей для безопасной связи корпоративных сетей и их отдельных сегментов с использованием российских криптоалгоритмов.

Abstract. The article is devoted to the problem of transition to domestic solutions in the field of information security. At the same time, it is proposed to do without specialized additional security tools by using secure operating systems. The article addresses the issues of implementing virtual private networks for secure communication of corporate networks and their individual segments using Russian crypto-algorithms.

Ключевые слова: виртуальные частные сети, сервер OpenVPN, ассиметричная криптография, инфраструктура открытых ключей, защищенные операционные системы.

Keywords: virtual private networks, OpenVPN, asymmetric cryptography, public key infrastructure, secure operating systems.

Наиболее распространенной и наиболее защищенной операционной системой в нашей стране является Astra Linux Special Edition, которая имеет сертификат по классу А1, соответствует первому уровню доверия и может использоваться при обработке любой информации ограниченного доступа, вплоть до государственной тайны с грифом особой важности.

Для обеспечения защищенной связи между отдельными подразделениями предприятия, отдельными сегментами корпоративной сети необходимо использование виртуальных частных сетей VPN.

Они могут быть реализованы с помощью семейства протоколов IPSec с использованием утилиты strongswan, входящей в состав расширенного репозитория, либо с помощью такого инструмента как OpenVPN, который входит в основной репозиторий ОС.

В данной статье остановимся именно на OpenVPN. Он позволяет реализовать защищенные соединения как хост-шлюз, так и хост-хост, в том

числе и на компьютерах, находящихся за межсетевыми экранами, использующими NAT, при чем без необходимости изменения их настроек.

Настроим VPN соединение (рисунок 1).

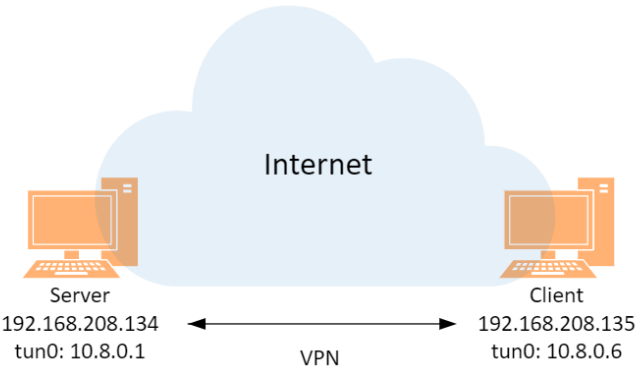

Рисунок 1 – Схема VPN-соединения

В данной статье остановимся на настройке сервера OpenVPN, а вопросы реализации клиента OpenVPN и реализации проверки защищенных каналов в операционной системе Astra Linux Special Edition рассмотрим в отдельной статье.

Пакет OpenVPN входит в дистрибутивы Astra Linux и устанавливается по умолчанию.

OpenVPN использует в свой работе динамически подключаемую библиотеку OpenSSL, которая также устанавливается при установке операционной системы. Это позволяет использовать весь набор криптоалгоритмов библиотеки OpenSSL.

В первую очередь нас интересуют отечественные криптоалгоритмы. Только они могут использоваться в Российской Федерации. Для их использования необходима установка пакета алгоритмов защитного преобразования ГОСТ libgost-astra.

Для быстрой настройки сервера OpenVPN необходимо установить утилиту командной строки astra-openvpn-server или графическую оснастку fly-admin-openvpn-server

apt-get install fly-admin-openvpn-server или

apt-get install astra-openvpn-server

При установке графической оснастки автоматически будет установлена и соответствующая упомянутая утилита командной строки.

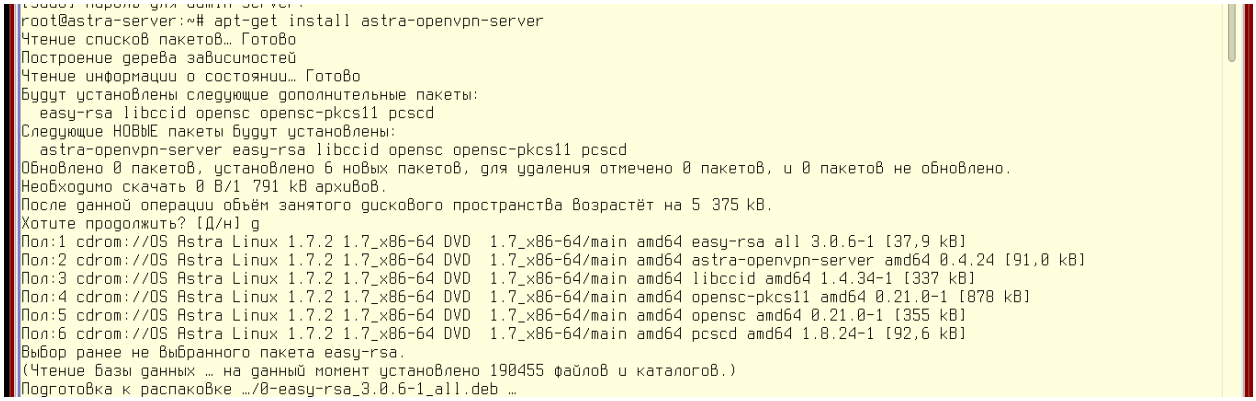

Рисунок 2 – Установка инструмента командной строки astra-openvpn-server

При этом автоматически будет установлен и настроен пакет российских криптоалгоритмов libgost-astra.

Посмотреть полную информацию по работе утилиты можно по команде: astra-openvpn-server -h

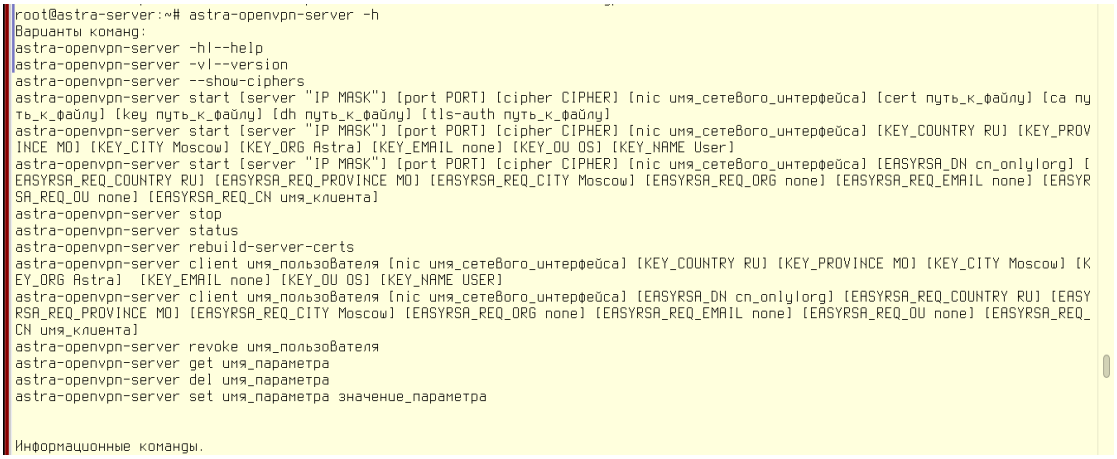

Рисунок 3 – справка astra-openvpn-server

Просмотреть версию сервера OpenVPN и поддерживаемые криптоалгоритмы можно с помощью команд:

astra-openvpn-server -v

astra-openvpn-server --show-ciphers

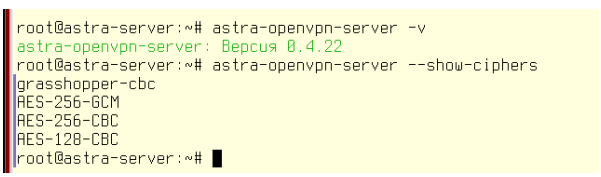

Рисунок 4 – версия и поддерживаемые криптоалгоритмы

Так как пакет libgost-astra установлен, то сервер OpenVPN будет автоматически настроен на работу с отечественным алгоритмом симметричного шифрования "Кузнечик" (grasshopper-cbc), по ГОСТ Р34.12-2015.

Для запуска сервера OpenVPN используем команду

astra-openvpn-server start.

Рисунок 5 – запуск службы astra-openvpn-server

Просмотрев статус службы, можно убедиться, что она работает.

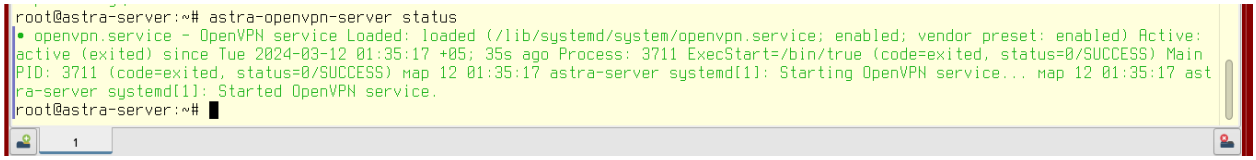

Рисунок 6 – статус службы astra-openvpn-server

При запуске сервера OpenVPN в рабочей папке пакета /etc/openvpn будут созданы:

- файл server.conf конфигурации openvpn;
- подпапка openvpn-certificates с настройками локального удостоверяющего центра (УЦ);
- подпапка keys с ключами;
- сертификат открытого ключа (ОК) УЦ ca.crt;
- сертификат ОК сервера server.crt;
- личный ключ сервера: server.key;

• файл параметров Диффи-Хеллмана для авторизации пользователей dh2048.pem

• файл дополнительной аутентификации TLS ta.key;

• файл списка отзыва сертификатов crl.pem (при выполнении отзыва сертификатов).

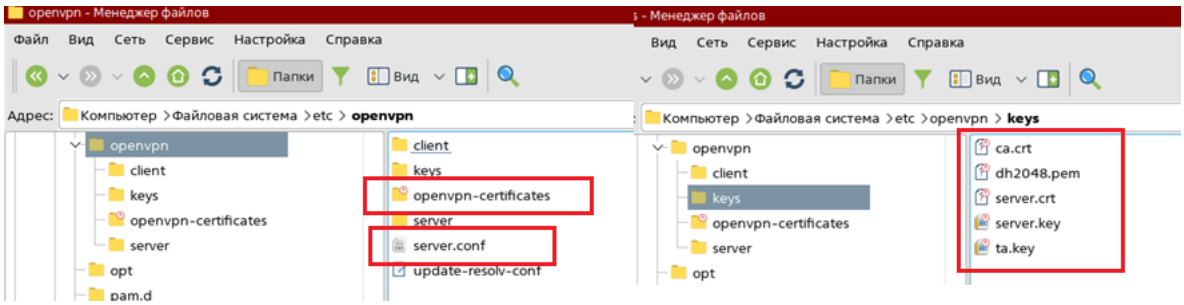

Рисунок 7 – созданные файла и каталоги

Также при первом запуске службы будут выполнены настройки межсетевого экрана и операционной системы для работы OpenVPN как стандартной системной службы с автоматическим запуском при включении компьютера.

Рассмотрим настройки конфигурационного файла сервера:

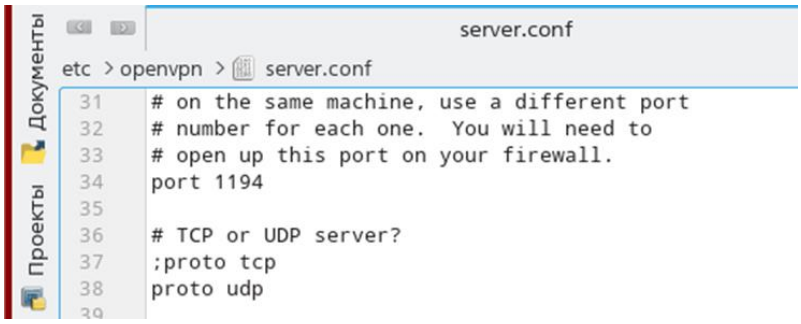

Рисунок 8 – Используемые OpenVPN протокол и порт

Используемый протокол транспортного уровня и используемый порт задаются в строчках 34, 37, 38. UDP рекомендуется использовать при необходимости более быстрой передачи данных, а TCP – когда, требуется более надежное соединение и меньшая вероятность блокировки трафика. Портами по умолчанию будут соответственно 1194 и 443

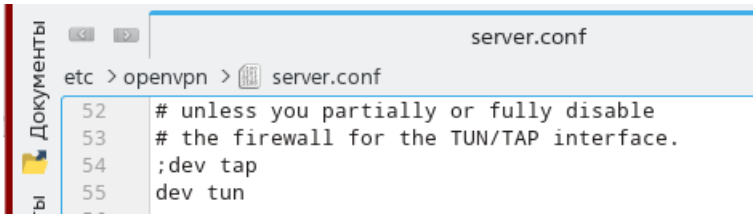

Рисунок 9 – используемые сетевые устройства

В строке 55 указано используемое сетевое устройство tun. TUN и TAP — разные режимы работы сетевых интерфейсов, используемых в VPN приложениях, таких как OpenVPN. TUN работает на сетевом уровне IP, позволяет создавать маршрутизированные VPN и передавать IP-трафик, а TAP работает на канальном уровне, поддерживает передачу всех типов данных, подобно физическому Ethernet-адаптеру, и может создавать мост между удаленными сетями.

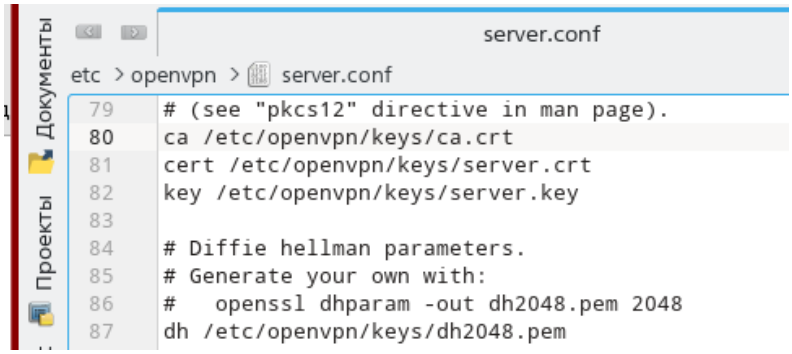

Рисунок 10 – месторасположение ключей

В строках 80–82 прописываем путь до сертификата открытого ключа УЦ и сервера OpenVPN, и также до личного ключа сервера.

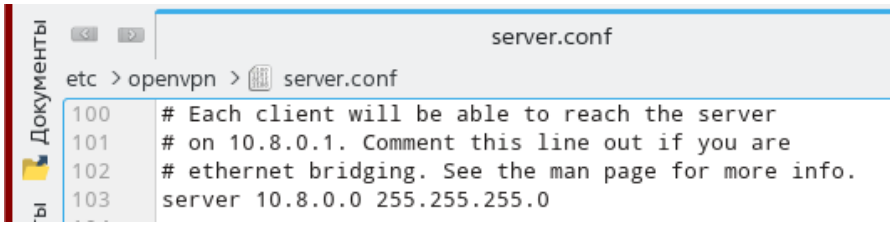

Рисунок 11 – IP-адрес сервера OpenVPN

В строке 103 указываем серверный режим работы и VPN подсеть, из которой OpenVPN будет выделять адреса клиентам, при этом в данном случае серверу OpenVPN будет отведен адрес 10.8.0.1.

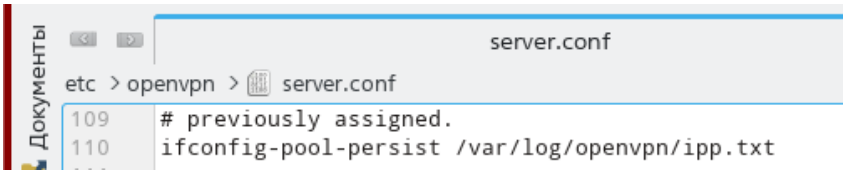

Рисунок 12 – месторасположение файла IP адресов клиентов

В строке 110 прописан путь к файлу с долговременными ассоциации IP-адресов клиентов OpenVPN, что обеспечивает постоянство IP-адресов, назначенных клиентам при каждом их подключении к серверу OpenVPN.

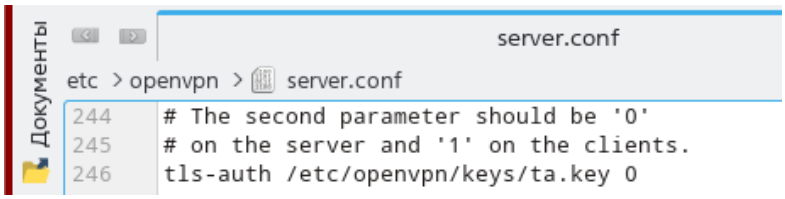

Рисунок 13 – месторасположение файла ta.key

В строке 246 прописан путь к файлу дополнительной аутентификации TLS, который используется для усиления безопасности соединения путем применения дополнительного уровня аутентификации на транспортном уровне модели OSI (TLS).

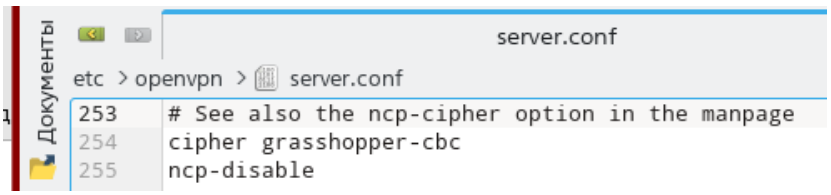

Рисунок 14 -алгоритм шифрования трафика VPN соединения

В строке 254 указываем алгоритм шифрования трафика VPN соединения. В соответствие с законодательством используем современный российский алгоритм симметричного шифрования «Кузнечик» по ГОСТ Р 34.12-2015, обозначаемый как grasshopper-cbc.

ncp-disable в 255 строке указывает на отключение использования Next-Generation Encryption (NGE) или Next-Gen Crypto Proposal (NCP).

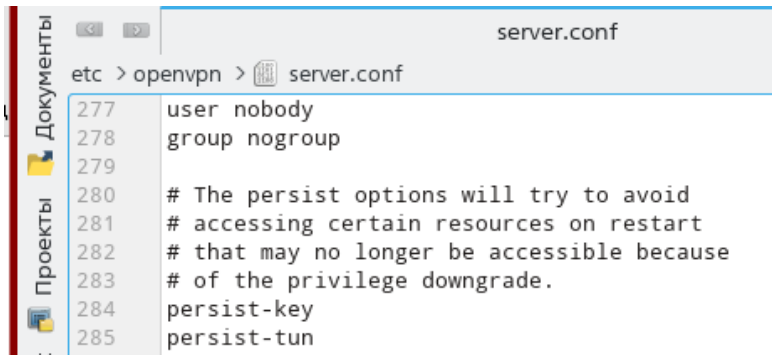

Рисунок 15 – имена, используемые для процесса OpenVPN

Строки 277 и 278 устанавливают пользователя и группу, от имени которых будет выполняться процесс OpenVPN. Рекомендуется использовать пользователя nobody с минимальными привилегиями для запуска сервисов или процессов с минимальными привилегиями доступа к ресурсам системы. и соответствующую ему группу nogroup.

Опции persist key и persist tun в строке 284–285 сохраняет долгосрочные ключи и параметры устройства TUN/TAP даже при перезапуске сервера или клиента.

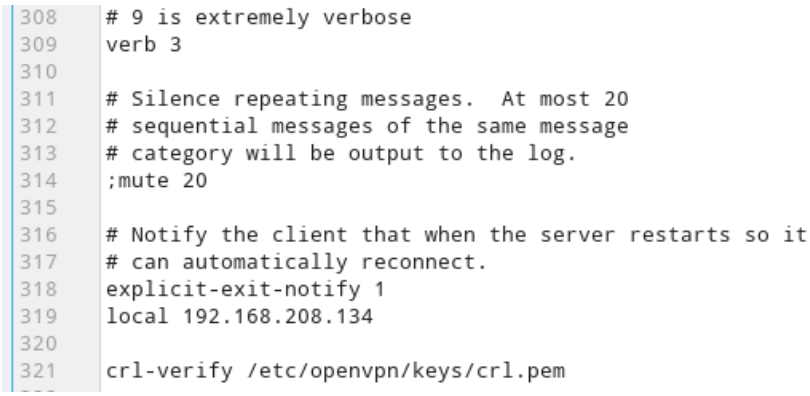

Рисунок 16 – детализация аудита

В строке 309 указан 3 уровень подробности вывода информации в журнале OpenVPN во время работы сервера или клиента. Чем выше число, тем более подробный вывод. Значение 3 обычно предоставляет довольно подробный вывод, что делает его удобным для отладки и просмотра основной информации о соединении в журналах OpenVPN.

Значение «1» для параметра explicit-exit-notify в строке 318 устанавливает режим отправки явных уведомлений об отключении клиента VPN серверу.

Строка 319 указывает на каком локальном IP-адресе ожидать входящие подключения.

Строка 321 указывает путь к файлу отзыва сертификатов.

Для корректной работы OpenVPN необходимо на сервере включить маршрутизацию транзитных IP-пакетов или IP-форвардинг, установив в 1 параметр net.ipv4.ip_forward, в файле /etc/sysctl.conf и сохранив изменения.

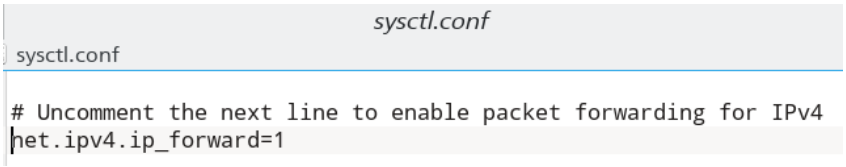

Рисунок 17 – включение маршрутизации транзитных IP-пакетов

Для реализации виртуальной частной сети и обеспечения возможности подключения клиентов к серверу OpenVPN необходимо создать для них ключи.

Создание клиентского набора ключей осуществляется на сервере OpenVPN с помощью опции client утилиты командной строки astra-openvpn-server:

astra-openvpn-server client <имя_клиента>

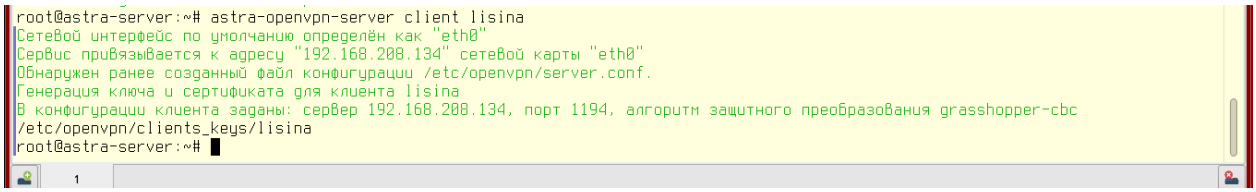

Рисунок 18 – создание клиентского комплекта файлов

При ее выполнении в подпапке клиентских ключей для OpenVPN /etc/openvpn/clients-keys будет создана подпапка с именем указанного клиента, куда будут помещены созданные для клиента файлы личного ключа <имя_клиента>.key и сертификата его ОК <имя_клиента>.crt, подписанного УЦ.

Дополнительно в эту же папку будут скопированы необходимые для клиента файл сертификата УЦ (по умолчанию ca.crt) и дополнительной аутентификации TLS (ta.key).

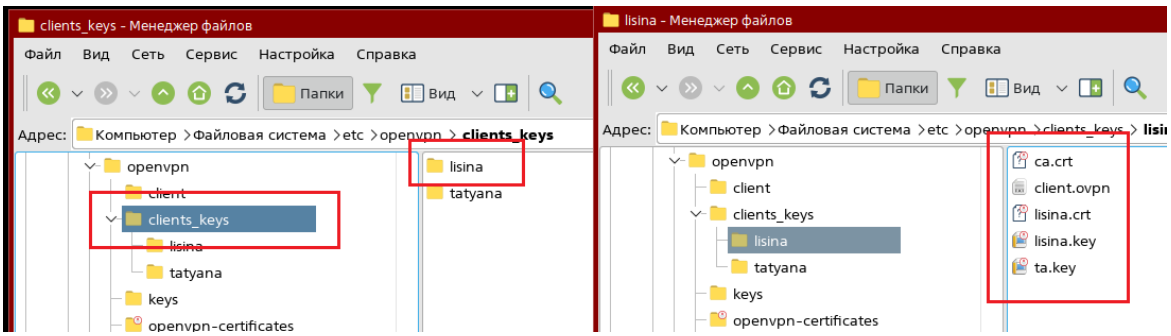

Рисунок 19 – клиентский комплект файлов

Для запрета подключения клиента можно отозвать сертификат его ОК. astra-openvpn-server revoke <имя_клиента>,

При этом:

- сертификат клиента в базе данных УЦ будет помечен как «отозванный»;
- в каталоге etc/openvpn/keys появится список отозванных сертификатов и произойдет перезагрузка сервера OpenVPN

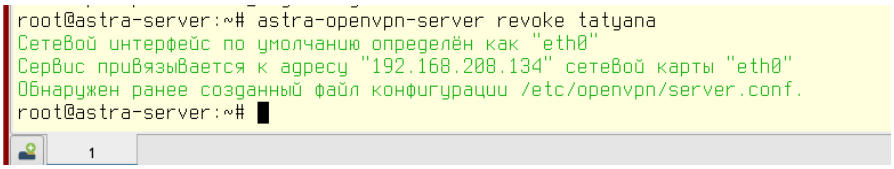

Рисунок 20 – отзыв сертификата для клиента tatyana

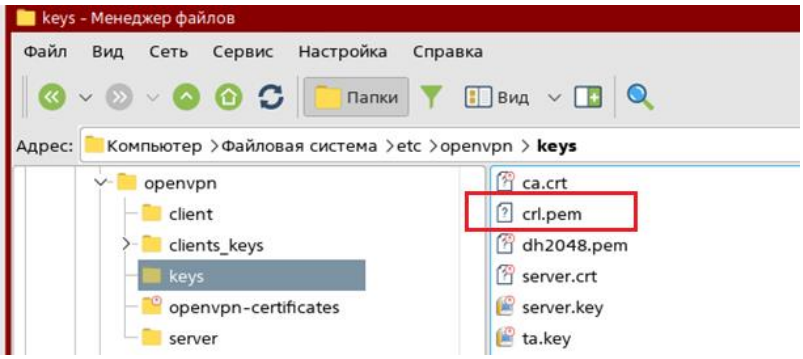

Рисунок 21 – файл списка отозванных сертификатов

Полную замену ключей и сертификатов сервера и УЦ можно произвести с помощью опции rebuild-server-certs команды astra-openvpn-server, которая останавливает службу, удаляет все сертификаты сервера и клиентов, повторно генерирует все сертификаты сервера и запускает его, при этом имена файлов сертификатов сервера берутся из конфигурационного файла сервера.

Таким образом в данной статьи рассмотрены различные аспекты настройки сервера VPN, использующего российские криптоалгоритмы в отечественной защищенной операционной системе Astra Linux Special Edition

Использованные источники:

1. Операционная система специального назначения «ASTRA LINUX SPECIAL EDITION» Руководство администратора. Часть 1.
2. OpenVPN // Справочный центр Astra Linux URL: https://wiki.astralinux.ru/display/doc/OpenVPN (дата обращения: 21.11.2023).

The sources used:

1. Special purpose operating system "ASTRA LINUX SPECIAL EDITION" Administrator's Guide. Part 1.
2. OpenVPN // Astra Linux Help Center URL: https://wiki.astralinux.ru/display/doc/OpenVPN (date of access: 11/21/2023).

Для цитирования: Кладов В. Е., Лисина Т. Е. РЕАЛИЗАЦИЯ СЕРВЕРА VPN С РОССИЙСКИМИ КРИПТОАЛГОРИТМАМИ В ОТЕЧЕСТВЕННОЙ ЗАЩИЩЕННОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ Столыпинский вестник. №5/2024.