ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.008РЭ-ЛУ

Программно-аппаратный комплекс «ФПСУ-TLS» версии 3.1.20

Руководство по эксплуатации

ПЕРС.26.20.40.140.008РЭ

Листов 253

2025

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем криптографической защиты информации, построенных с применением программно-аппаратных комплексов «ФПСУ-TLS» версии программного обеспечения 3.1.20. В документе содержатся сведения о ФПСУ-TLS, дано описание возможностей изделия, последовательности действий при настройке параметров ФПСУ-TLS в процессе эксплуатации и в аварийных ситуациях.

Одним из наиболее существенных факторов, обеспечивающих нормальную работу сети под защитой ФПСУ-TLS и требуемый уровень безопасности, является отсутствие ошибок при конфигурировании ФПСУ-TLS. Поэтому конфигурирование ФПСУ-TLS должно производиться квалифицированным специалистом, хорошо знакомым с сертификатами X.509, топологией сети, имеющим опыт работы с различным сетевым оборудованием и его программным обеспечением, а также внимательно изучившим принципы, методику и конкретные процедуры конфигурирования, изложенные в соответствующих разделах данного документа.

Если у вас возникнут какие-либо вопросы или предложения, вы можете обратиться непосредственно в ООО «АМИКОН». Вам всегда будут представлены подробные консультации по телефону или электронной почте.

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

Наш адрес: ООО «АМИКОН», Варшавское шоссе, д. 125 (секция 1, цокольный этаж), г. Москва, 117587.

Телефон и факс: +7-(495)797-64-12, +7-(495)797-64-13.

Адрес в Интернет: https://www.amicon.ru/

Электронная почта: info@amicon.ru

Веб-форум ООО «АМИКОН»: https://forum.amicon.ru

Мы работаем с 10:00 до 19:00 по московскому времени, кроме субботы и воскресенья.

© ООО «АМИКОН», 1994-2025. Все права защищены.
Все авторские права на эксплуатационную документацию защищены.
Документ входит в комплект поставки изделия.
Без специального письменного разрешения ООО «АМИКОН» настоящий документ или его часть в печатном или электронном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.
Информация, содержащаяся в настоящем документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны ООО «АМИКОН».

Содержание

1. Список используемых сокращений и определений

АП – аппаратная платформа;

Веб-Сервис – Интернет-Банк, сервис, к которому требуется предоставить защищенный доступ через открытую сеть (например, сеть Интернет);

НСД – несанкционированный доступ к информации;

ОС – операционная система;

ПО – программное обеспечение;

ПЭВМ – персональная электронная вычислительная машина, персональный компьютер;

СКЗИ – средство криптографической защиты информации;

СКЗИ «ФПСУ-TLS» – средство криптографической защиты информации «ФПСУ-TLS», 11485466.26.20.40.140.031;

Сертификат – сертификат открытого ключа стандарта X.509, электронный или печатный документ, подтверждающий принадлежность владельцу открытого ключа;

ТМ (ТМ-идентификатор) - электронный идентификатор «touch-memory», iButton DS1993 – DS1996 или микроэлектронное USB-устройство «TM-Key» производства ООО «АМИКОН» (ПЕРС.466226.004, ПЕРС.466226.005, ПЕРС.466226.008, ПЕРС.466226.009);

УЦ – удостоверяющий центр X.509 сертификатов;

ФПСУ-TLS – комплекс «ФПСУ-TLS» версии программного обеспечения 3.1.20, TLS-шлюз, программная компонента которого является модификацией 3.1.20 средства криптографической защиты информации «ФПСУ-TLS», 11485466.26.20.40.140.031;

ICMP – «Internet Control Message Protocol», протокол для передачи команд и сообщений об ошибках;

IP – «Internet Protocol», базовый протокол межсетевого объединения Интернет;

OCSP – Online Certificate Status Protocol, протокол о статусе онлайн-сертификата, регламентированный стандартом RFC 6960.

PKCS10 – стандарт, описывающий формат сообщения, содержащего запрос

сертификата X.509;

TCP – «Transmission Control Protocol», протокол транспортного уровня, осуществляющий доставку дейтаграмм с установлением соединения и гарантирующий доставку сообщений;

TLS – протокол защиты транспортного уровня (The Transport Layer Security Protocol, RFC 5246, 8446). Криптографический протокол, предназначенный для организации защищённой передачи данных между узлами в сети Internet;

UDP – «User Datagram Protocol», протокол транспортного уровня, не требующий подтверждения доставки дейтаграмм;

X.509 – стандарт, определяющий форматы данных и процедуры распределения общих ключей с помощью сертификатов с цифровыми подписями, которые предоставляются сертификационными органами.

2. Общие сведения

Программно-аппаратный или программный комплекс «ФПСУ-TLS» является средством защиты от несанкционированного доступа к информации, в котором реализован необходимый набор телекоммуникационных функций клиентской и серверной сторон протокола TLS (The Transport Layer Security Protocol, RFC 5246, 8446) в соответствии с рекомендациями по стандартизации Р 1323565.1.020-2020 (TLS 1.2) и Р 1323565.1.030-2020 (TLS 1.3). ФПСУ-TLS выполняет функцию защиты данных, передаваемых в соответствии с протоколом HTTP в глобальных и локальных вычислительных сетях.

ФПСУ-TLS предназначен для применения в вычислительных сетях, использующих среду передачи данных Ethernet, тип кадра Ethernet II, и стек протоколов TCP/IP.

Основным назначением ФПСУ-TLS является обеспечение защиты от несанкционированного доступа (НСД) к информации, передаваемой между HTTP-серверами локальной вычислительной сети и удаленными абонентскими пунктами через сети передачи данных общего пользования.

ФПСУ-TLS является основным компонентом (сервером) распределенной системы защиты передаваемых данных от НСД. В качестве абонентских пунктов системы (клиентов) может выступать программное или программно-аппаратное решение, взаимодействующее с ФПСУ-TLS в роли клиента в соответствии с протоколом TLS (далее TLS-клиент).

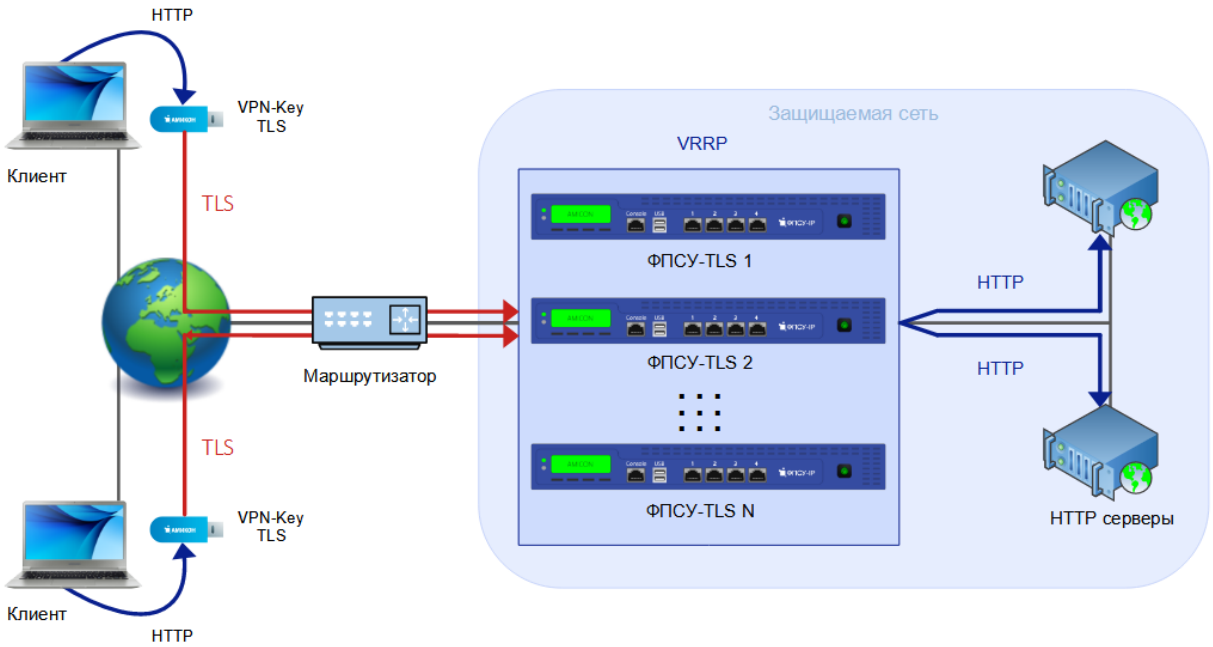


Рисунок 1 - Общая схема применения ФПСУ-TLS

ФПСУ-TLS обеспечивает формирование защищенных межсетевых HTTPS туннелей в соответствии с протоколами TLS 1.2 и TLS 1.3. В межсетевых туннелях осуществляется:

- обязательная двухсторонняя аутентификация взаимодействующих ФПСУ-TLS и TLS-клиента при установлении TLS-соединения;
- шифрование HTTP-трафика, обеспечивающее сокрытие полей данных передаваемых пакетов.

Ключевая система защиты передаваемой информации построена на основе сертификатов X.509.

Аутентификация и идентификация между ФПСУ-TLS и TLS-клиентами осуществляется на базе инфраструктуры открытых ключей (PKI) в соответствии с протоколом TLS.

ФПСУ-TLS в случае программно-аппаратного решения представляет собой специализированное программно-аппаратное устройство, функционирующее под управлением ОС на основе Linux.

ФПСУ-TLS в случае программного решения представляет собой виртуальную машину, функционирующую под управлением гостевой ОС на основе Linux (подробнее про работу программного решения см. пункт «ФПСУ-TLS в виртуальной машине»).

ФПСУ-TLS использует диалоговые средства для управления своей работой (настройки сетевых параметров, установления правил идентификации и аутентификации доступа к ФПСУ-TLS, просмотра регистрационной информации, настройка сертификатов и т.д.), а также для установки некоторых параметров работы самого устройства (даты и времени).

Защитные функции ФПСУ-TLS гарантируют конфиденциальность, целостность и достоверность передаваемой в процессе его эксплуатации информации при соблюдении организационно-технических требований, находящихся в поставляемом с ФПСУ-TLS документе «Правила пользования» на СКЗИ «ФПСУ-TLS».

ФПСУ-TLS следует использовать в соответствии с формуляром и правилами пользования СКЗИ «ФПСУ-TLS», входящими в комплект поставки.

Средство криптографической защиты информации «ФПСУ-TLS» удовлетворяет:

- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для классов КС1, КС2 и КС3;

- «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)» по уровню $КС_Б$;
- «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_Б$.

Ниже приведен список нормативных документов, которым соответствует реализация программного обеспечения ФПСУ-TLS:

Протокол TLS:

- МР 26.2.001-2013 Информационная технология. Криптографическая защита информации. Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS).
- Рекомендации по стандартизации Р 1323565.1.020-2020. Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2).
- Рекомендации по стандартизации Р 1323565.1.030-2020. Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3).

Алгоритмы и режимы криптографических алгоритмов:

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры.

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров.

Р 50.1.113-2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования.

Р 1323565.1.026-2019 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование.

Параметры эллиптических кривых для криптографических алгоритмов:

Р 50.1.114-2016 Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов.

Р 1323565.1.024-2019 Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов.

Поддерживаемые криптонаборы:

TLS_GOSTR341112_256_WITH_28147_CNT_IMIT

TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC

TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L

TLS_GOSTR341112_256_WITH_MAGMA_MGM_L

TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S

TLS_GOSTR341112_256_WITH_MAGMA_MGM_S

RSA:

TLS_AES_128_GCM_SHA256*

TLS_AES_256_GCM_SHA384*

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*

**Примечание: использование указанных алгоритмов для защиты информации конфиденциального характера запрещается в случаях, определенных пунктом 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.*

3. Разграничение доступа и пользователи

Программное обеспечение ФПСУ-TLS функционирует в собственной изолированной и функционально замкнутой операционной среде, ACCESS-TM SHELL. Среда осуществляет разграничение доступа к операционной системе ФПСУ-TLS, защиту программных и информационных модулей на ПЗУ комплекса.

Разграничение доступа допущенных лиц и контроль их полномочий при запуске ФПСУ-TLS и управлении его работой осуществляется по предъявляемым допущенными лицами ТМ-идентификаторам и символьным паролям в соответствии с логическим разделением лиц ФПСУ-TLS на две роли и четыре условных класса, представленных в нижеследующей таблице:

Таблица 1. Роли и классы пользователей ФПСУ-TLS

Роль/Класс	**Разрешенные действия**
Пользователь/ /Оператор	• запуск ФПСУ-TLS при выключенном режиме автостарта; • остановка рабочего режима.
Администратор/ /Инженер	Все права класса «Оператор» и дополнительно: • просмотр конфигураций; • изменение параметров хранимых конфигураций без права активировать конфигурацию; • переинициализация ПДСЧ; • контроль целостности без записи результатов.
Администратор/ /Администратор	Все права класса «Инженер» и дополнительно: • управление конфигурациями; • настройка сетевых параметров; • установка сертификатов УЦ, СОС, установка и управление личными сертификатами; • настройка автозагрузки СОС; • добавление адресов защищаемых http-серверов; • взаимодействие с Syslog, SNMP; • настройка NTP сервера;

Роль/Класс	**Разрешенные действия**
	• установка времени, даты; • настройка параметров защиты; • настройка общих параметров (статистика, watchdog); • настройка параметров масштабирования; • регистрация ТМ-идентификаторов; • просмотр и управление ТМ-идентификаторами; • включение/отключение подсистемы автоматического старта; • резервирование и восстановление конфигурации ФПСУ-TLS; • контроль целостности ПО ФПСУ-TLS по списку или с записью результатов; • регистрация нового администратора; • регистрация и предоставление полномочий на определенные действия удаленным администраторам.
Администратор/ /Главный администратор	Все права класса «Администратор» и дополнительно: • установка дополнений/изменений; • переинсталляция ФПСУ-TLS и перевод в рабочий режим из технологического.
Администратор/УА	В зависимости от назначенных Администратором или Главным Администратором полномочий, УА (удаленному администратору) могут быть разрешены следующие действия: • опрос текущего состояния; • получение данных о работе абонентов; • получение данных о работе локальных администраторов; • получение данных о работе удаленных администраторов; • чтение конфигурации; • изменение конфигурации; • согласование времени.

Примечание: ряд действий с ФПСУ-TLS не требуют авторизации:

- выключение питания ФПСУ-TLS по кнопке Power;
- просмотр текущих настроек состояния сети и ФПСУ-TLS (с использованием утилит);

- просмотр текущего состояния ФПСУ-TLS рабочего режима (текущие сессии, ARP, статистика, автозагрузки, черный список).

4. Характеристики и производительность ФПСУ-TLS

В данном пункте приведены предельные значения производительности ФПСУ-TLS, при соблюдении которых гарантируется стабильная работа ФПСУ-TLS. В основных характеристиках приведены сведения о допустимом количестве одновременно установленных соединениях, сетевых тайм-аутах. Производительность платформы демонстрируется показателями скорости шифрования при приеме/передаче при различных используемых криптонаборах, показателями пропускной способности в зависимости от размера посылаемого пакета.

Основные характеристики

Количество одновременно установленных соединений

ФПСУ-TLS поддерживает одновременно установленных соединений:

- в роли клиента - 15 000;
- в роли сервера - 15 000;
- всего клиентских и серверных соединений - 15 000.

Тайм-ауты

На ФПСУ-TLS реализованы тайм-ауты, приведенные в таблице ниже.

Таблица 2. Тайм-ауты

Тайм-аут	Описание	Время по умолчанию
На соединение с веб-сервером	Время ожидания ответа от веб-сервера. Если ответ за указанное время не получен - считается, что веб-сервер недоступен.	10 с
На ожидание получения подтверждения закрытия сессии	Время ожидания ответа от клиента на подтверждение закрытия сессии. Если ответ за указанное время не получен - сессия все равно закрывается.	0
На ожидание приема/передачи	Время ожидания приема/передачи. Если за указанное время нет данных от	43 200 с (12 часов)

Тайм-аут	Описание	Время по умолчанию
	клиента - сессия закрывается.	
На отклик от партнера (при масштабировании)	Время ожидания ответа от другого ФПСУ-TLS (партнера). Если за это время партнер не ответил - считается, что он недоступен.	3 с, может быть изменен в конфигурации
На удержание соединения (при масштабировании)	При масштабировании главный ФПСУ-TLS распределяет клиентов по другим ФПСУ-TLS (партнерам) по заданному алгоритму масштабирования. Если между сессиями прошло указанное время - главный может передать клиента партнеру.	50 с, может быть изменен в конфигурации

Размер пакета

Максимальный размер Ethernet пакета 9000 байт.

Производительность

Нагрузочное тестирование проводилось на платформах FPSUTLS3-ULT7 со следующими характеристиками:

Процессор: Intel(R) Xeon(R) CPU E5-2680 v4 2.40GHz;

Количество процессоров: 28;

Количество ядер: 14;

Оперативная память, Гб: 16;

Сетевой адаптер: Intel® E810-XXVDA4 Ethernet 25G PCI Express v4.0 x16 Quad-port SFP28 (с 4 портами).

Для измерения использовался указанный на рисунке ниже тестовый стенд, для генерации трафика использовалась программа iperf3, запущенная на Сервере и Клиенте.

Рисунок 2 - Защищенное TLS-соединение

Между Сервером и Клиентом стенда были расположены две платформы ФПСУ-TLS, строящие между собой защищенное TLS-соединение для передачи и приема данных. От Клиента к Серверу и обратно направлялся TCP трафик. В тесте изменялось количество потоков и замерялась скорость шифрования применяемых в ФПСУ-TLS криптонаборов, а также замерялась пропускная способность при изменении размера посылаемого пакета. Пиковые результаты измерений приведены в таблицах ниже.

Суммарная скорость шифрования ФПСУ-TLS при приеме и передаче трафика в зависимости от используемого криптонабора приведена в таблице ниже.

Таблица 3. Скорость шифрования

Криптонабор	**Максимальная скорость**
TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L	8.5 Гбит/с
TLS_GOSTR341112_256_WITH_MAGMA_MGM_L	15.4 Гбит/с

Пропускная способность ФПСУ-TLS при изменении размера посылаемого пакета приведена в таблице ниже.

Таблица 4. Пропускная способность

Размер пакета	**Пропускная способность**	**Пропускная способность пакетов, pps**
88	9.9 Гбит/с	11 700 000
150	12 Гбит/с	8 990 000
250	5.8 Гбит/с	2 737 000
500	3.5 Гбит/с	851 000

Размер пакета	**Пропускная способность**	**Пропускная способность пакетов, pps**
1 000	15.1 Гбит/с	2 284 000
1 500	15.4 Гбит/с	1 567 000

5. Запуск и первоначальная настройка ФПСУ-TLS

Для локального администрирования (изменения параметров, наблюдения за TLS-соединениями, установки или изменения сертификатов, настройки сетевых параметров и т.д.) к соответствующим разъемам программно-аппаратного комплекса ФПСУ-TLS (или рабочей станции гипервизора) должны быть подсоединены мышь, монитор и клавиатура.

ФПСУ-TLS в программном исполнении для виртуальных машин требует предварительной настройки менеджеров виртуальных машин. Подробнее см. пункт «ФПСУ-TLS в виртуальной машине».

После включения питания (включении виртуальной машины) ФПСУ-TLS и проведения диагностических тестов BIOS на экран монитора будет выдан запрос на подтверждение права доступа пользователя к работе с ФПСУ-TLS, сопровождаемый звуковым сигналом, дополняющим экранную выдачу запроса в случае отсутствия монитора. Прижмите к ТМ-считывателю ТМ-идентификатор зарегистрированного на ФПСУ-TLS пользователя или подключите ТМ-идентификатор к USB-порту ФПСУ-TLS

При первом запуске комплекса в ответ на запрос приложите ТМ-идентификатор Главного администратора - он всегда поставляется зарегистрированным на ФПСУ-TLS.

В случае успешной идентификации будет выдан соответствующий звуковой сигнал, стартовый BIOS продолжит работу и ФПСУ-TLS будет загружен.

Если это первый запуск ФПСУ-TLS, то после авторизации будет выдано главное меню ФПСУ-TLS с признаком работы в технологическом режиме. Следует перевести ФПСУ-TLS из технологического режима в рабочий перед дальнейшей эксплуатацией (подробнее см. пункт «Технологический режим ФПСУ-TLS»).

Если ФПСУ-TLS был уже переведен в рабочий режим, и на нём была задействована подсистема автоматического старта (см. пункт «Включение подсистемы автоматического старта»), данная процедура первоначальной идентификации пропускается, и ФПСУ-TLS сразу переходит в рабочий режим приема TLS-соединений от клиентов: при условии что ФПСУ-TLS уже сконфигурирован и параметры его работы установлены, загрузчик через несколько секунд автоматически осуществит переход в рабочий режим защиты HTTP-трафика к обслуживаемым серверам.

Если последовал отказ от запуска (для изменения параметров конфигурации или настройки системы) и его работа не может быть начата без установки параметров, будет осуществлен выход в главное меню ФПСУ-TLS. Выход в главное меню будет осуществлен также и при выходе из рабочего режима по нажатию сочетания клавиш <Alt+X> или <Alt+F1>. Подробнее про главное меню см. пункт «Главное меню ФПСУ-TLS»).

5. 1. ФПСУ-TLS в виртуальной машине

Допускается эксплуатация ФПСУ-TLS по классу КС1 СКЗИ под управлением следующих виртуальных машин:

- VMware Workstation Player: 16.0.0,16.1.0, 16.1.1, 16.1.2, 16.2.0, 16.2.1, 16.2.2, 16.2.3, 16.2.4, 17.0.0, 17.0.1, 17.0.2, 17.5.0, 17.5.1;
- VMware Workstation Pro: 16.0.0, 16.1.0, 16.1.1, 16.1.2, 16.2.0, 16.2.1, 16.2.2, 16.2.3, 16.2.4, 17.0.0, 17.0.1, 17.0.2, 17.5.0, 17.5.1;
- ESXi: 6.7.0, 6.7.0 U1, 6.7.0 U2, 6.7.0 U3, 6.7.0 P04, 7.0.0, 7.0.0b, 7.0.1, 7.0.2, 7.0.3, 8.0.0, 8.0.1;
- Qemu: 6.2.0, 7.0.0, 7.1.0, 8.0.0, 8.1.0, 8.2.0.

Виртуальные машины могут эксплуатироваться под управлением следующих хостовых ОС: Windows 7 x64, Windows 8.1 x64, Windows 10 x64, Windows 11 x64, Windows Server 2019 x64, ubuntu 22.04 LTS x86-64, ubuntu 24.04 LTS x86-64, Debian 12 x86-64, Debian 13 x86-64, Astra Linux SE 1.7.4 x86-64, REDOS 8 x86-64.

5. 1. 1. Настройка виртуальной машины VMware

В данном разделе описывается подготовка виртуальной машины VMware Workstation Pro/VMware Workstation/VMware EsXi для развертывания ФПСУ-TLS.

Виртуальные машины могут эксплуатироваться под управлением следующих хостовых ОС: Windows 7 x64, Windows 8.1 x64, Windows 10 x64, Windows 11 x64, Windows Server 2019 x64, ubuntu 22.04 LTS x86-64, ubuntu 24.04 LTS x86-64, Debian 12 x86-64, Debian 13 x86-64, Astra Linux SE 1.7.4 x86-64, REDOS 8 x86-64.

Поддерживаемые виртуальные машины:

- VMware ESXi версий 6.7.0 (8169922), 6.7.0 U1 (10302608), 6.7.0 U2 (13006603), 6.7.0 U3 (14320388), 6.7.0 P04 (17167734), 7.0.0 (15843807), 7.0.0b (16324942), 7.0.1 (16850804), 7.0.2 (18538813), 7.0.3 (20036589), 8.0.0 (20513097), 8.0.1 (21203435);
- VMware Workstation/Workstation Pro версий 16.0.0 (16894299), 16.1.0 (17198959),

16.1.1 (17801498), 16.1.2 (17966106), 16.2.0 (18760230), 16.2.1 (18811642), 16.2.2 (19200509), 16.2.3 (19376536), 16.2.4 (20089737), 17.0.0 (20800274), 17.0.1 (21139696), 17.0.2 (21581411), 17.5.0 (22583795), 17.5.1 (23185310).

Для создания в интерфейсе VMware виртуальной машины с поддерживаемыми характеристиками выполните следующее:

1. Выберите 64-х разрядную операционную систему семейства Linux.

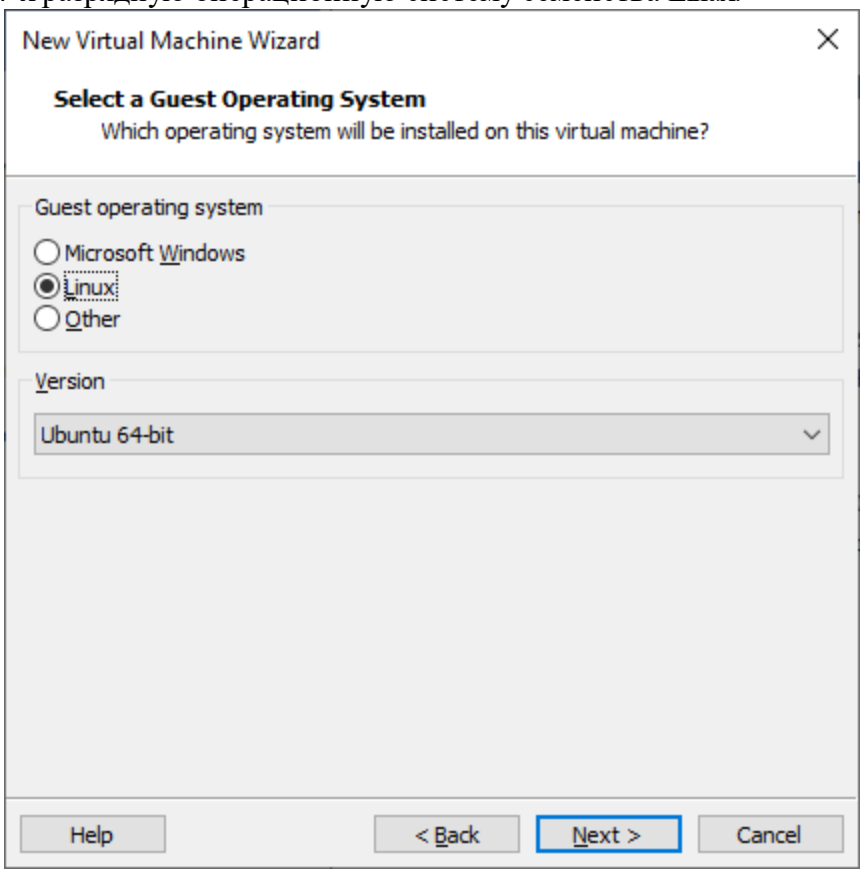


Рисунок 3 - Выбор ОС

2. Количество оперативной памяти, которое выделяется виртуальной машине при создании, должно быть минимум 2°GB. Это же количество памяти будет доступно в гостевой ОС (ОС ФПСУ). Рекомендуется выбирать 4°GB и больше.

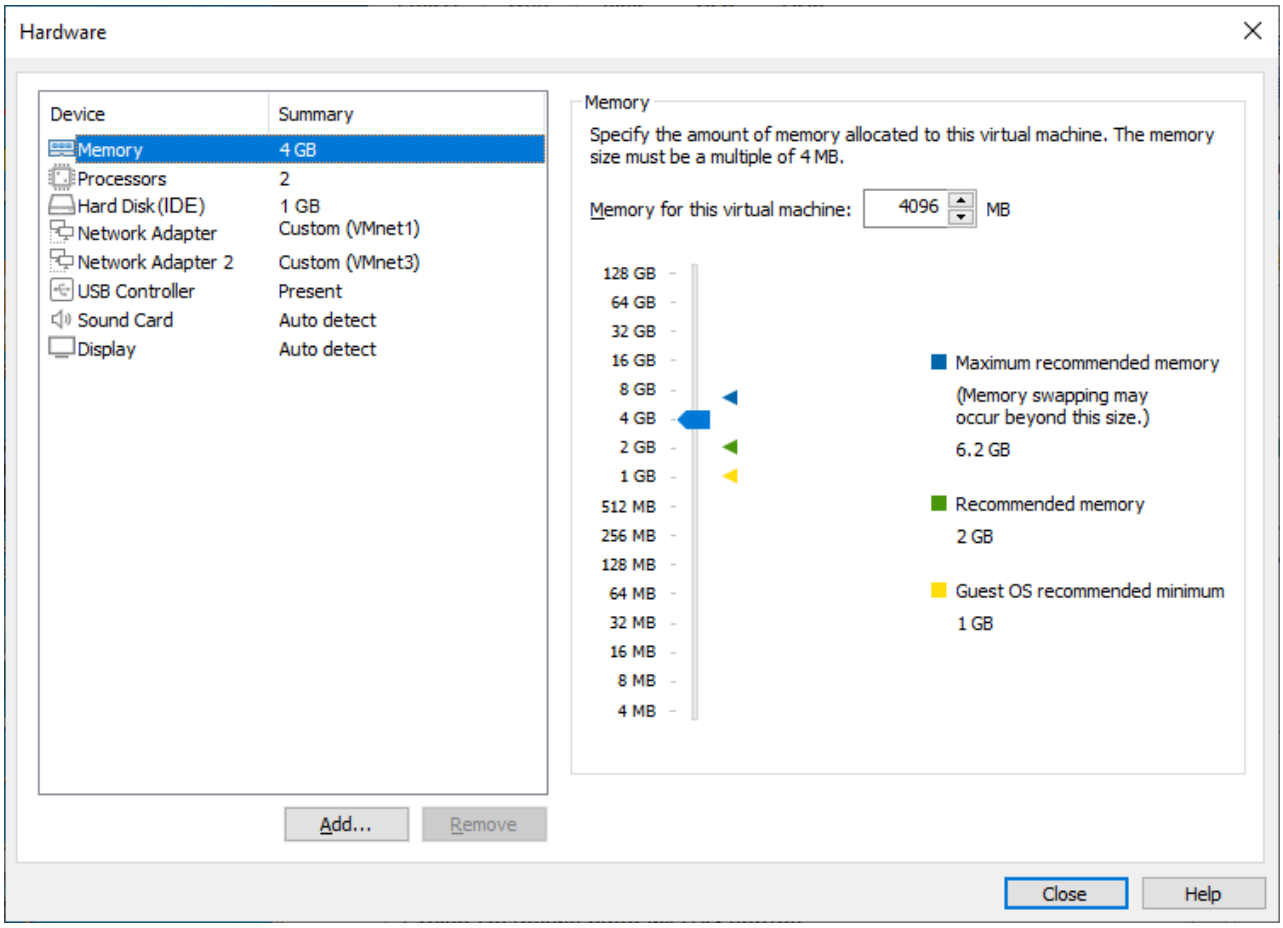


Рисунок 4 - Оперативная память виртуальной машины

3. В настройках процессора количество ядер для виртуальной машины устанавливается исходя из лицензии ФПСУ.
4. Для процессоров включите поддержку виртуализации – флаг «VirtualizeVT-x/EPT or AMD-V/RVI».

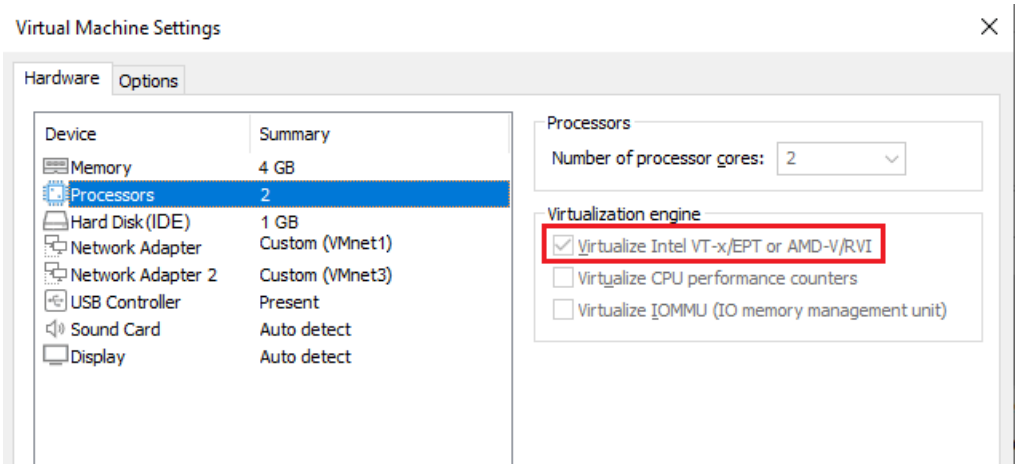


Рисунок 5 - Настройки процессора

5. Добавьте виртуальный жесткий диск объемом 1°GB, выберите контроллер виртуального жесткого диска – «IDE». В ОС ФПСУ поддерживается только данный контроллер.
6. Задайте минимум 2 сетевых адаптера, как показано на рисунке выше. Для корректной работы виртуальной машины рекомендуется заменить драйвера сетевых адаптеров. Для VMware EsXi в настройках сетевых адаптеров выберите драйвер «vmxnet3». Для VMware Workstation Pro/VMware Workstation после завершения процесса создания виртуальной машины внесите изменения в файл с расширением .vmx из каталога виртуальной машины, как указано в пункте 10.
7. Для подключения TM-Key, VPN-Key, USB-носителей добавьте устройство USB-контроллер, если не установлено по умолчанию.
8. Добавьте устройство дисплей, если не установлено по умолчанию.
9. Для VMware EsXi/VMware Workstation Pro выберите на вкладке «Options» пункт «Advanced». Установите тип встроенного ПО - «UEFI».

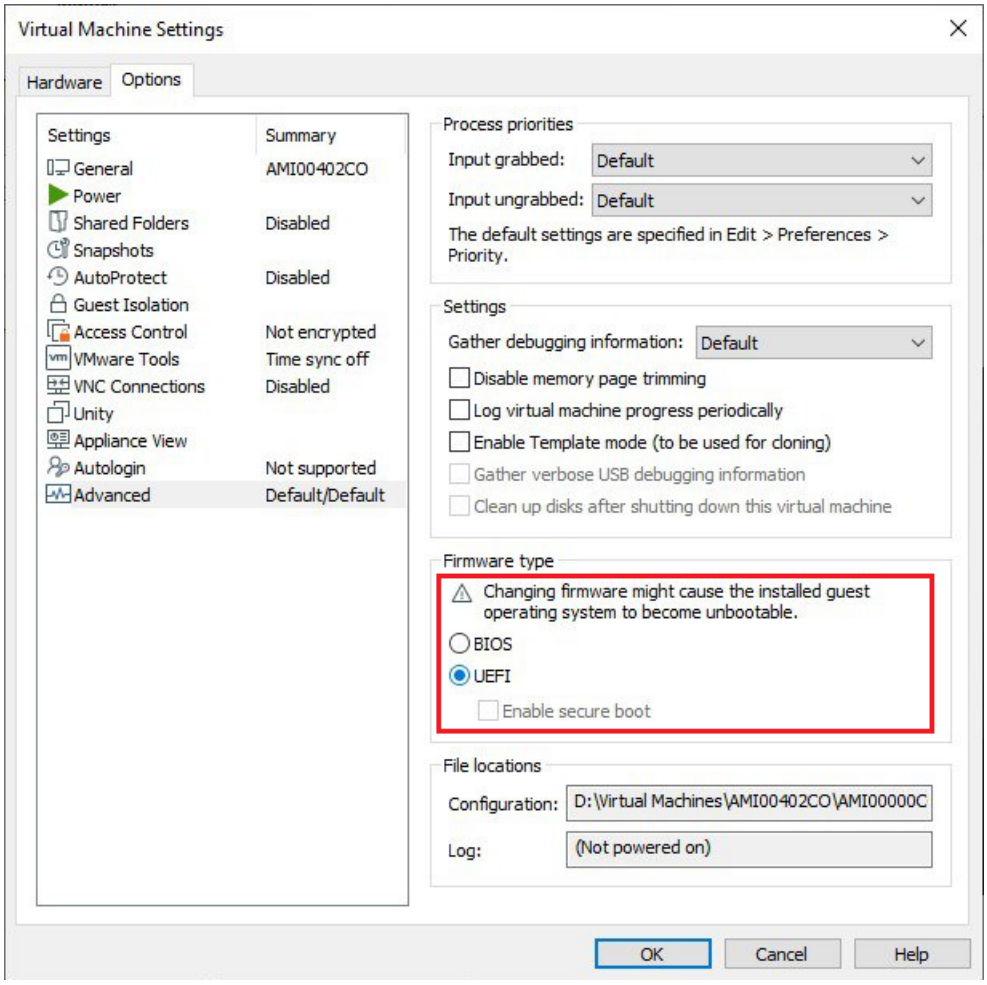


Рисунок 6 - Настройки интерфейса прошивки

Для VMware Workstation после завершения процесса создания виртуальной машины внесите изменения в файл с расширением .vmx из каталога виртуальной машины, как указано в пункте 11.

Закройте окно настроек и завершите создание виртуальной машины.

10. Для VMware Workstation Pro/VMware Workstation измените в конфигурации виртуальной машины драйвер сетевых адаптеров. Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, для каждого адаптера в свойстве «virtualDev» задано значение по умолчанию «e1000», найдите строки с этим значением и замените его на «vmxnet3»:

```
ethernet0.virtualDev = "vmxnet3"
ethernet1.virtualDev = "vmxnet3"
```

Сохраните файл.

11. Для VMware Workstation измените в конфигурации виртуальной машины тип встроенного ПО «UEFI». Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, добавьте в середину файла (например после параметра mem.hotadd) строку:

```
firmware = "efi"
```

Сохраните файл.

Внести изменения в конфигурацию виртуальной машины можно с помощью утилиты VM_Tweaker.exe. Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, на вкладке «EFI BIOS Tweaks» включите флаг «Enable "efi" BIOS boot type» и сохраните изменения, нажав на кнопку «Apply Changes».

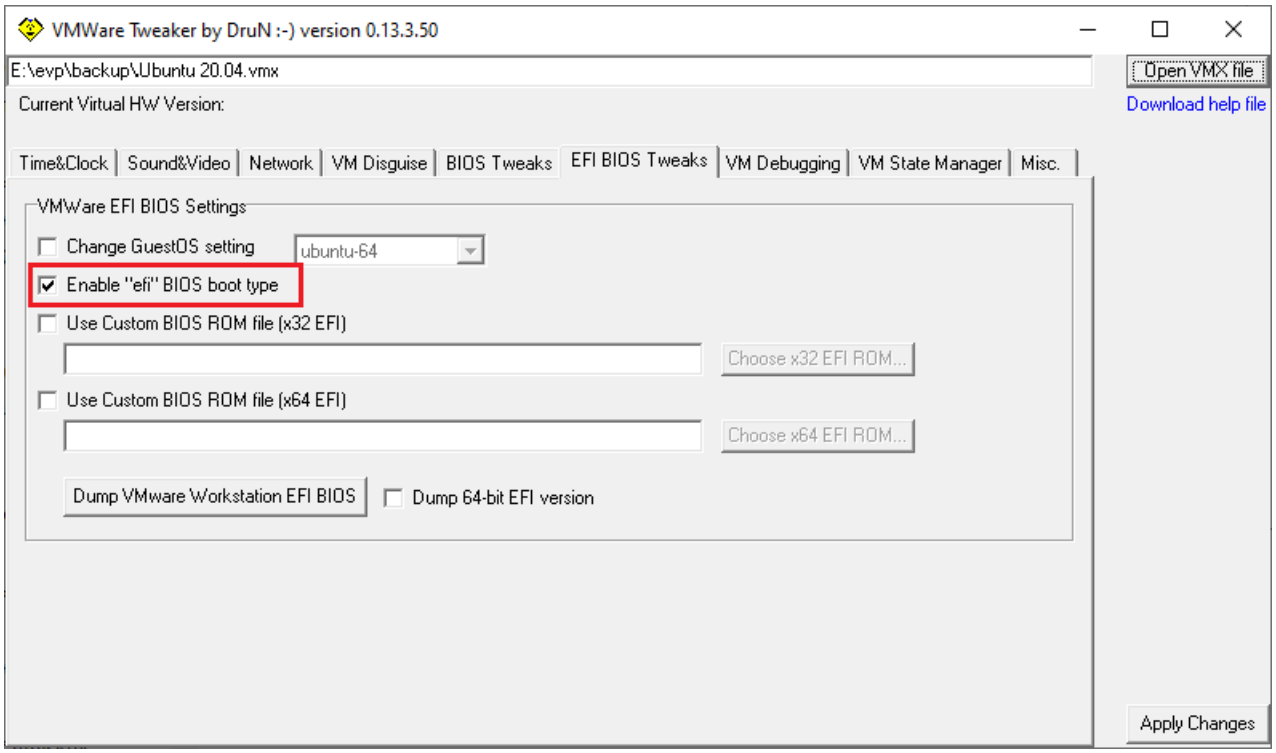


Рисунок 7 - Настройка BIOS

Создание виртуальной машины закончено.

Описание процедуры установки ПО ФПСУ-TLS находится в разделе «Инсталляция ПО ФПСУ-TLS».

5. 1. 2. Настройка виртуальной машины QEMU/KVM

В данном разделе описывается подготовка виртуальной машины QEMU/KVM для развертывания ФПСУ-TLS.

Виртуальные машины могут эксплуатироваться под управлением следующих хостовых ОС: Windows 7 x64, Windows 8.1 x64, Windows 10 x64, Windows 11 x64, Windows Server 2019 x64, ubuntu 22.04 LTS x86-64, ubuntu 24.04 LTS x86-64, Debian 12 x86-64, Debian 13 x86-64, Astra Linux SE 1.7.4 x86-64, REDOS 8 x86-64.

Поддерживаемые версии QEMU: 6.2.0, 7.0.0, 7.1.0, 8.0.0, 8.1.0, 8.2.0.

В операционной системе семейства Linux должна быть установлена программа эмуляции аппаратной платформы QEMU. Для использования аппаратной виртуализации KVM необходимо:

- установить библиотеки и ПО;
- настроить доступ к управлению виртуальной машиной;

- создать виртуальную машину с гостевой операционной системой ФПСУ;
- настроить сетевые интерфейсы и другие устройства.

Далее приводится пример установки ФПСУ в QEMU/KVM 6.2.0 на Ubuntu 22.04.4 LTS.

QEMU/KVM 6.2.0 предварительно установлена.

Предварительно установлены пакеты libvirt-clients версии 8.0.0-1ubuntu7.10 amd64, libvirt-daemon-system версии 8.0.0-1ubuntu7.10 amd64, bridge-utils версии 1.7-1ubuntu3 amd64.

Необходимо проверить, поддерживаются ли рабочей станцией необходимые расширения виртуализации для KVM. Для процессоров Intel должна поддерживаться технология Intel VT, для процессоров AMD – AMD SVM. Введите команду в терминале:

```
kvm-ok
```

Если виртуализация поддерживается и включена в BIOS/UEFI, на экран будет выдано сообщение о возможности использовать KVM.

```
INFO: /dev/kvm exists
KVM acceleration can be used
```

В случае, если в сообщении указано что ускорение KVM не может быть использовано, а процессор поддерживает виртуализацию, проверьте, что аппаратная виртуализация включена в BIOS/UEFI материнской платы компьютера.

Если процессор не поддерживает аппаратную виртуализацию, в выводе команды терминала будет возвращено значение 0.

```
egrep -c '(vmx | svm)' /proc/cpuinfo
```

После установки qemu необходимо настроить доступ к управлению виртуальной машиной. Добавить группу libvirtd и добавить пользователя в эту группу для управления виртуальными машинами. Данный пользователь получит доступ к расширенным сетевым опциям. Введите команды в терминале:

```
sudo groupadd libvirtd
sudo adduser $USER libvirtd
```

Если в качестве пользователя выбран текущий, потребуется выйти из системы и войти снова, чтобы применить новое членство в группе.

Проверить членство в группе можно командой:

```
groups <имя пользователя>
```

Включите поддержку встроенного ПО UEFI для виртуальной машины QEMU/KVM,

установив пакет ovmf:

```
sudo apt install ovmf
sudo cp /usr/share/OVMF/OVMF_CODE.fd /var/lib/libfirt/
```

Версия устанавливаемого пакета ovmf 2022.02-3ubuntu0.22.04.3.

Для автоматизации процесса установки ОС используется утилита virt-install, могут быть использованы preseeds, kickstart и пр. Утилита virt-install является частью пакета virtinst. Данный пакет был установлен ранее. Версия установленного пакета virtinst 4.0.0-1.

Запустите гостевую операционную систему ФПСУ-TLS в виртуальной машине QEMU/KVM, vfpsu, выполнив команду в терминале:

```
sudo virt-install --name vfpsu --memory 2048 --disk vfpsu.qcow2,size=1 --osinfo
detect=off,require=off  --import --boot
loader=$(pwd)/OVMF_CODE.fd,bootmenu.enable=on,bios.useserial=on --network none
```

Примечание. Параметр size=1 следует убрать, если используется готовый образ диска на USB-носителе.

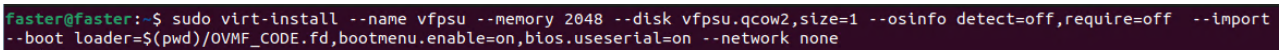


Рисунок 8 - Создание виртуальной машины

Закройте окно виртуальной машины.

В некоторых случаях необходимо отключить безопасную загрузку UEFI. Для этого при загрузке виртуальной машины, нажать *<F2>*, зайти в настройки BIOS, выбрать в меню «Device Manager → Secure Boot Configuration», выбрать опцию «Attempt Secure Boot» и снять флаг, выйти из BIOS с сохранением изменений по *<F10>*.

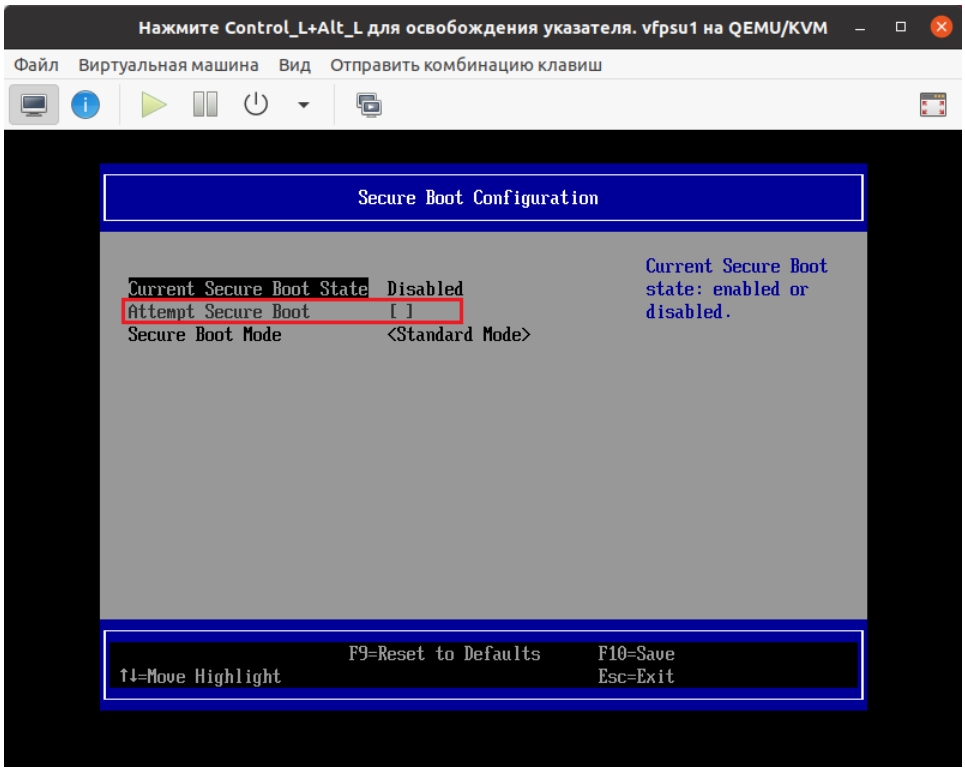


Рисунок 9 - Настройки BIOS виртуальной машины

Перед запуском виртуальной машины необходимо настроить второй сетевой интерфейс, проверить или настроить процессоры, загрузочный диск для ФПСУ-TLS, добавить в список оборудования USB Disk 2.0 и TM-Key, изменить порядок загрузки, задав загрузку с USB-носителя на время установки ФПСУ-TLS.

Настройка QEMU/KVM отличается для двух вариантов установки ФПСУ-TLS - с установочного носителя и с готового образа диска.

Настройка QEMU/KVM для установки ФПСУ-TLS с готового образа диска приведена в пунктах 1 - 9.

Настройка QEMU/KVM для установки ФПСУ-TLS с установочного носителя приведена в пунктах 1 - 7, 10.

1. Запустите графический интерфейс виртуальной машины QEMU/KVM.

Для управления виртуальной машиной могут быть использованы различные утилиты. В примере используется рекомендуемый пакет virt-manager, который содержит утилиту с графическим интерфейсом для управления локальными и удаленными виртуальными машинами. Утилита virt-manager является частью пакета virtinst. Данный пакет был ранее установлен. Версия установленного пакета virtinst 4.0.0-1.

Запустите virt-manager командой:

```
sudo virt-manager
```

(Если менеджер виртуальных машин не установлен, установите пакет virt-manager командой: `sudo apt-get install virt-manager`).

Откроется окно управления виртуальными машинами:

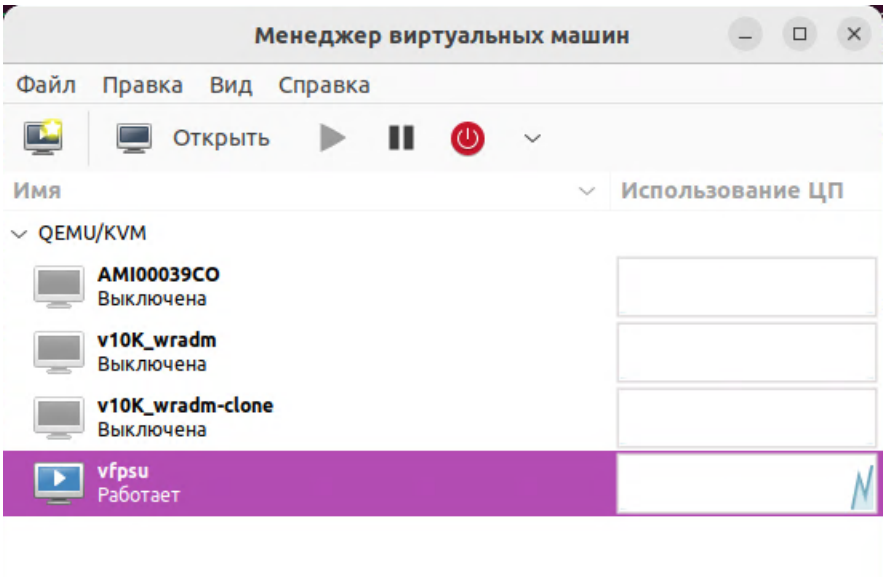


Рисунок 10 - Окно менеджера виртуальных машин

ВНИМАНИЕ! Для изменения настроек виртуальная машина должна быть выключена.

Выключите виртуальную машину vfpsu, выбрав соответствующую команду в контекстном меню.

Откройте виртуальную машину vfpsu, откройте настройки виртуального оборудования, нажав на кнопку  .

2. Виртуальная машина создается с одним сетевым интерфейсом (по умолчанию). Необходимо добавить ещё один сетевой интерфейс:

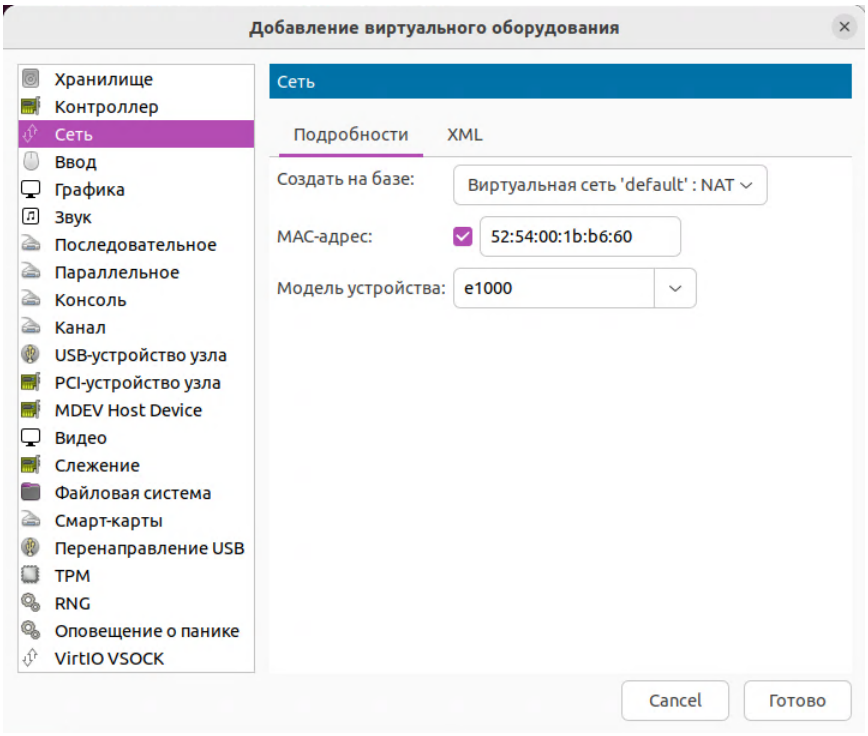


Рисунок 11 - Добавление сетевого интерфейса

Для сетевого интерфейса необходимо выбрать модель устройства «e1000».

3. В настройках процессоров виртуальной машины установите флаг «Копировать конфигурацию ЦП хоста».

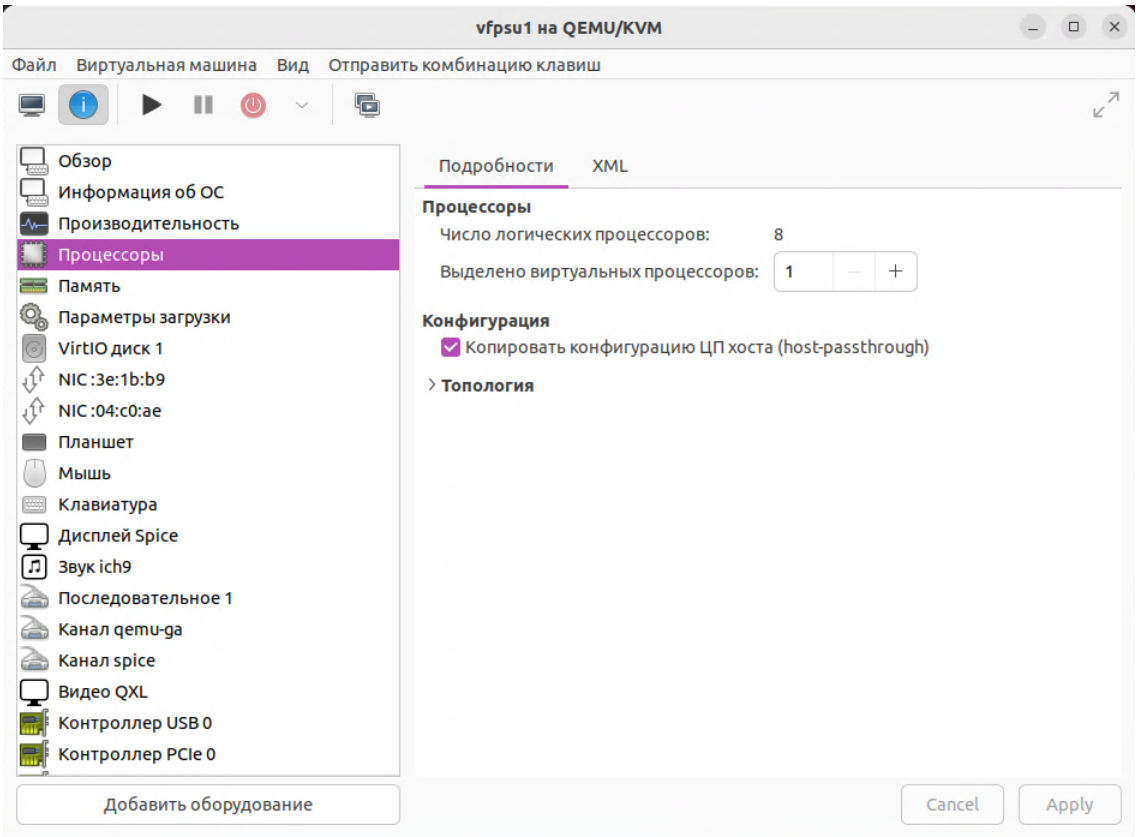


Рисунок 12 - Процессоры

4. Проверьте настройки диска виртуальной машины. Тип шины диска выбирается «IDE», размер диска установите 1 ГБ.

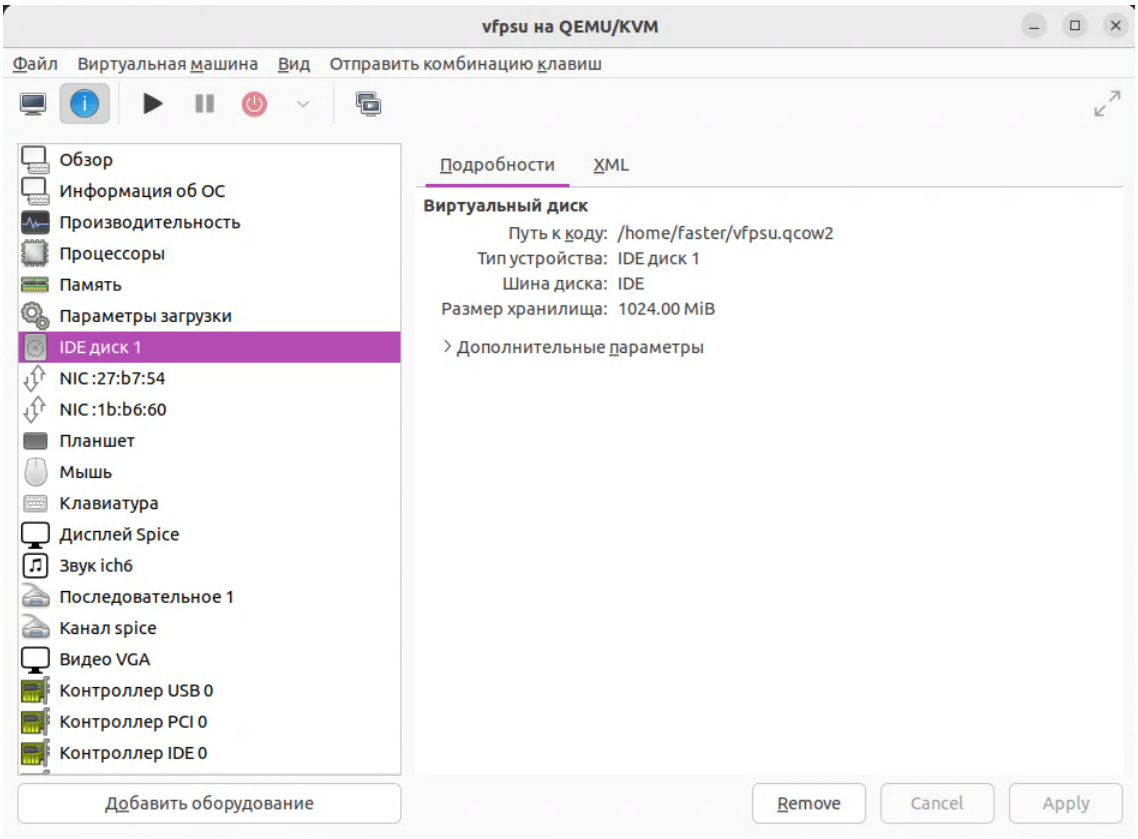


Рисунок 13 - Диск

5. Проверьте настройки видео виртуальной машины. Выберите модель «VGA».

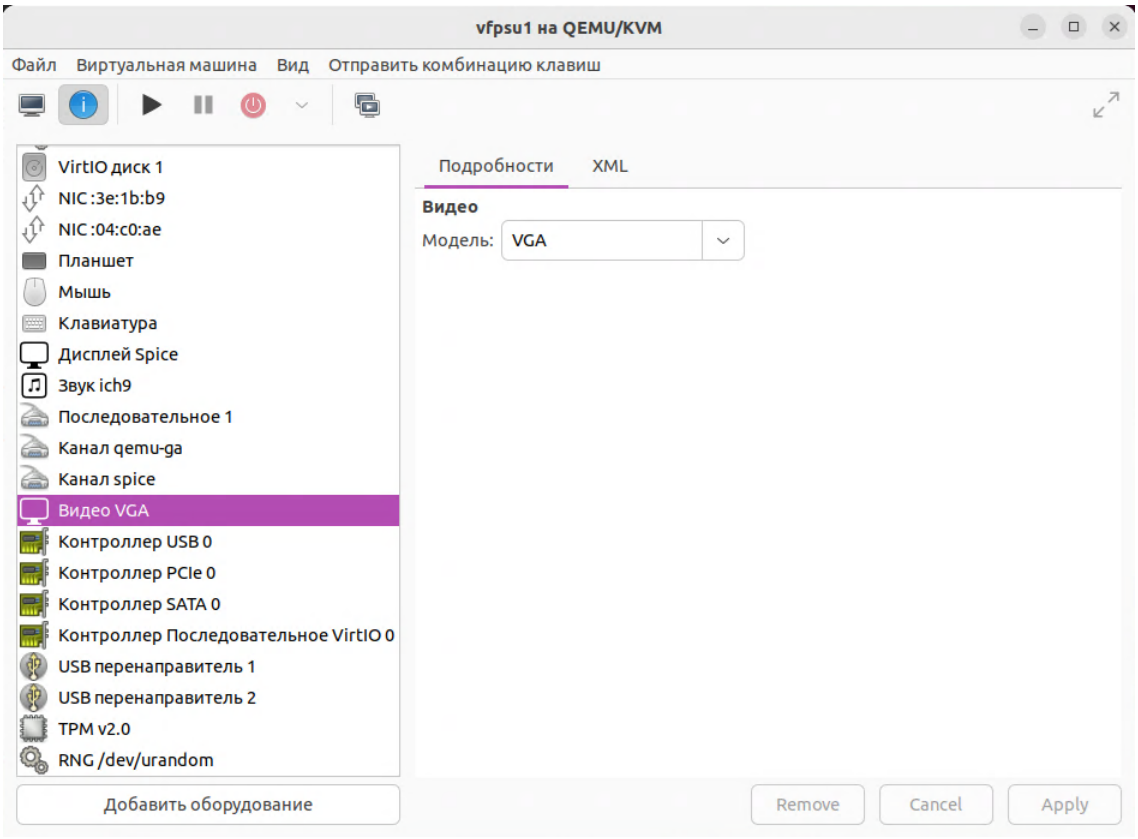


Рисунок 14 - Видео

6. При создании виртуальной машины необходимо добавить в список оборудования USB Disk 2.0 и USB-устройство ТМ (ТМ-считыватель или ТМ-Key):

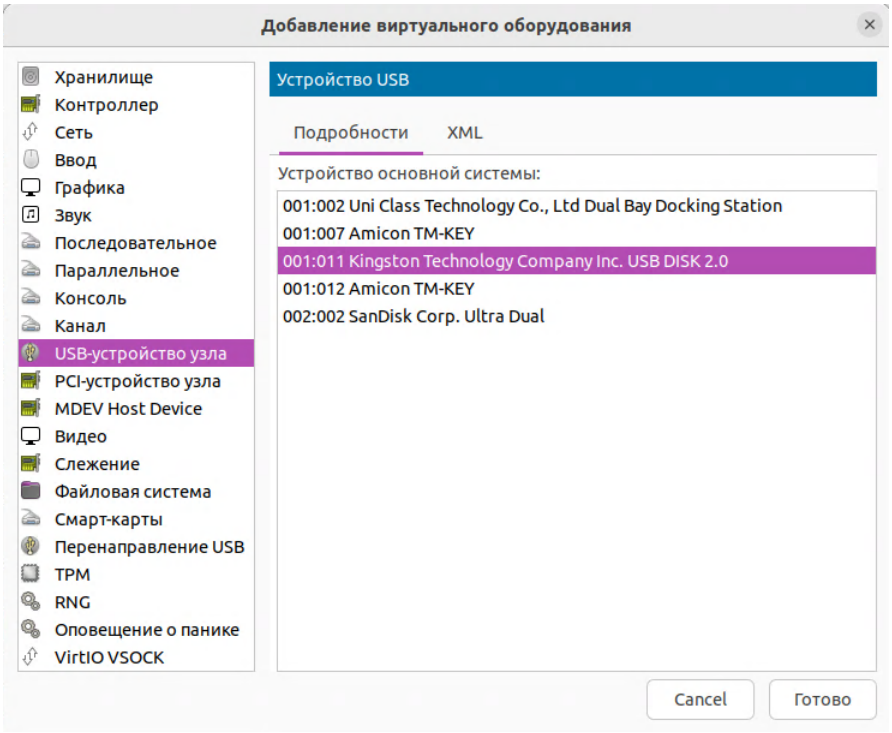


Рисунок 15 - Добавление оборудования

Подключите установочный USB-носитель к рабочей станции, нажмите кнопку «Добавить оборудование», в открывшемся окне выберите «USB-устройства узла», в списке найденного оборудования отметьте «USB Disk 2.0» и подтвердите выбор по кнопке «Готово».

Подключите TM-Key к рабочей станции, нажмите кнопку «Добавить оборудование», в открывшемся окне выберите «USB-устройства узла», в списке найденного оборудования отметьте «Amicon TM-KEY» и подтвердите выбор по кнопке «Готово».

7. В параметрах загрузки виртуальной машины необходимо изменить порядок загрузки дисков, чтобы у USB-носителя с инсталляционным комплектом ФПСУ-TLS приоритет был выше. Как показано на рисунке USB-носитель с инсталляционным комплектом ФПСУ-TLS будет загружаться первым, отмечен флагом.

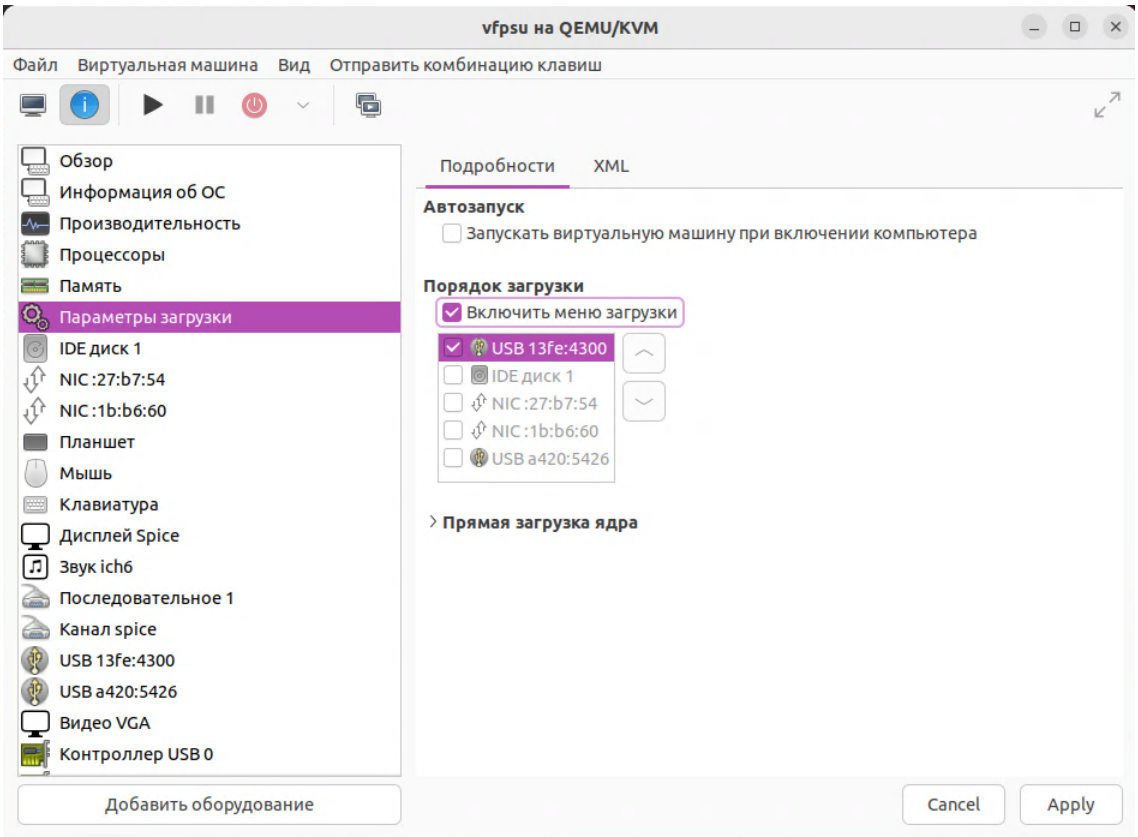


Рисунок 16 - Изменение порядка загрузки дисков

Настройка QEMU/KVM для установки ФПСУ-TLS с готового образа диска

8. Дальнейшие действия по установке ФПСУ-TLS с готового образа диска приводятся в пункте «Установка в QEMU/KVM».

9. В параметрах загрузки виртуальной машины необходимо вернуть первоначальный порядок загрузки дисков (был изменен в пункте 7).

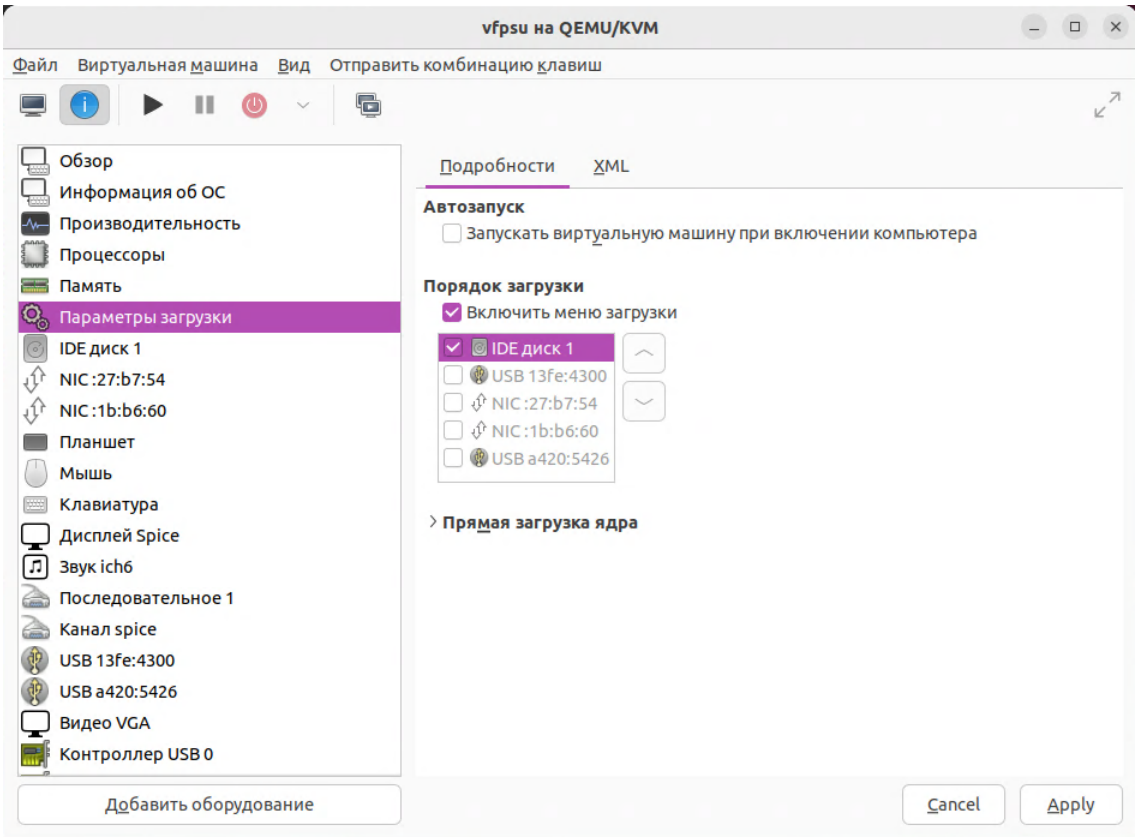


Рисунок 17 - Изменение порядка загрузки дисков

Настройка QEMU/KVM для установки ФПСУ с установочного носителя

10. После добавления в конфигурационный файл виртуальной машины USB-носителя с инсталляционным комплектом ФПСУ-TLS поменяйте порядок загрузки, установив загрузку с USB-носителя (действие аналогичное п. 7), и проведите установку ПО. Описание процедуры установки ПО ФПСУ-TLS находится в разделе «Инсталляция ПО ФПСУ-TLS». После процедуры установки и первоначальной настройки (см. пункт «Технологический режим ФПСУ-TLS») поменяйте обратно порядок загрузки, установив загрузку с диска (действие аналогичное п. 9).

Создание виртуальной машины закончено.

Для запуска ФПСУ-TLS в QEMU/KVM запустите vfpsu по кнопке  или введите команду в терминале:

```
virsh start vfpsu
```

На экране отобразится главное меню ФПСУ-TLS.

5. 2. Технологический режим ФПСУ-TLS

Программно-аппаратный комплекс ФПСУ-TLS поставляется с установленным программным обеспечением, работающим в технологическом режиме. Программный комплекс ФПСУ-TLS, поставленный в виде образа для виртуальной машины, находится в технологическом режиме. Также технологический режим включается после повторной инсталляции программного обеспечения ФПСУ-TLS.

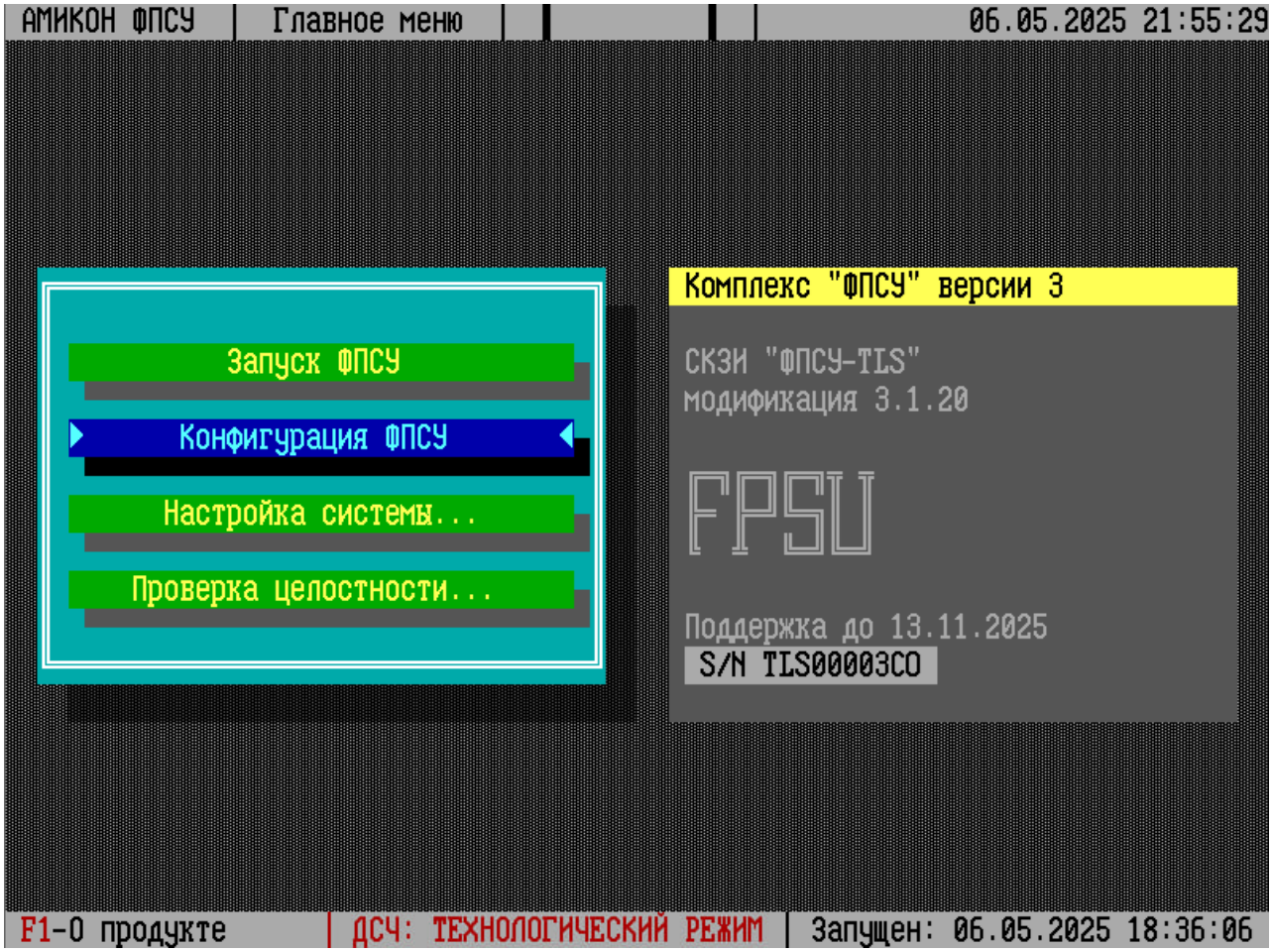


Рисунок 18 - Предупреждение о работе в технологическом режиме

Технологический режим предназначен для первоначальной проверки работоспособности ФПСУ-TLS до ввода в эксплуатацию, и имеет следующие ограничения:

- невозможность работы с подсистемой регистрации электронных идентификаторов touch-memory ФПСУ-TLS (см. пункт «Регистрация ТМ-идентификаторов»);
- Ограничение работы с ключевыми данными (см. пункт «»Установка сертификатов»). Возможна работа только с тестовыми ключами и сертификатами.

Внимание! Тестовые ключи и сертификаты невозможно использовать после перехода в рабочий режим ФПСУ-TLS!

При работе в технологическом режиме каждый раз при запуске ФПСУ-TLS будет выдаваться служебное оповещение.

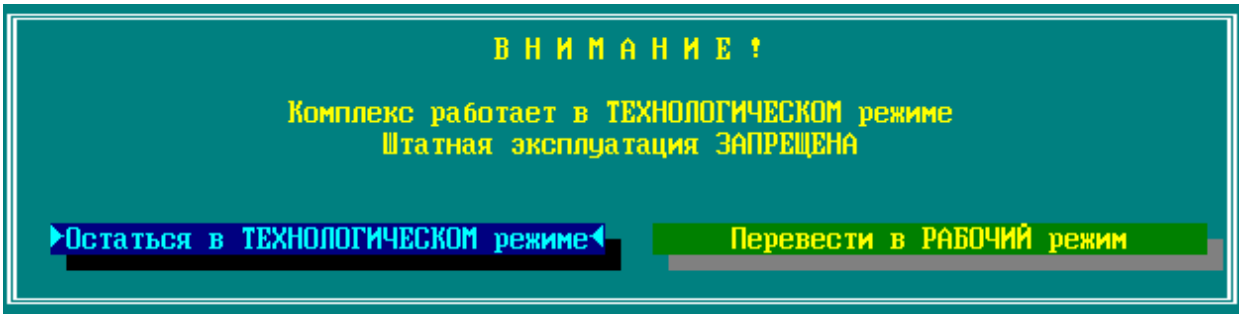


Рисунок 19 - Технологический режим

Для выхода из технологического режима в штатный, рабочий режим, выберите и нажмите кнопку «Перевести в РАБОЧИЙ режим».

Переход в рабочий режим начинается с инициализации программного датчика случайных чисел.

После выполнения команды «Перевести в РАБОЧИЙ режим» откроется окно выбора источника ключа ПДСЧ. Инициализация ПДСЧ может быть проведена средствами БиоДСЧ, путем передвижения мыши в пределах экрана, или с помощью ЦВК, путем загрузки файла с ключом ПДСЧ, выданного ЦВК.

ВНИМАНИЕ! Программным комплексам ФПСУ-TLS, функционирующим под управлением виртуальных машин запрещается проводить инициализацию ПДСЧ средствами БиоДСЧ. Следует в качестве источника ключа ПДСЧ выбрать опцию «ЦВК» и предъявить съемный носитель с выданным ЦВК файлом ключа ПДСЧ.

Рисунок 20 - Инициализация программного датчика случайных чисел

Для продолжения потребуется подтвердить полномочия Главного администратора (права класса *Главный администратор*, см. пункт «Разграничение доступа и пользователи»), подключив USB ТМ-идентификатор к USB-порту ФПСУ-TLS или приложив ТМ-

идентификатор к ТМ-считывателю ФПСУ-TLS.

При использовании БиоДСЧ от администратора требуется передвигать мышь в пределах экрана. Переинициализация ключа ПДСЧ завершится успешно, как только датчик считает достаточное для генерации ключа количество движений указателя мыши.

Рисунок 21 - Биологический датчик случайных чисел

При использовании команды «ЦВК» от администратора требуется загрузить на ФПСУ-TLS файл ключа ПДСЧ, выданный ЦВК.

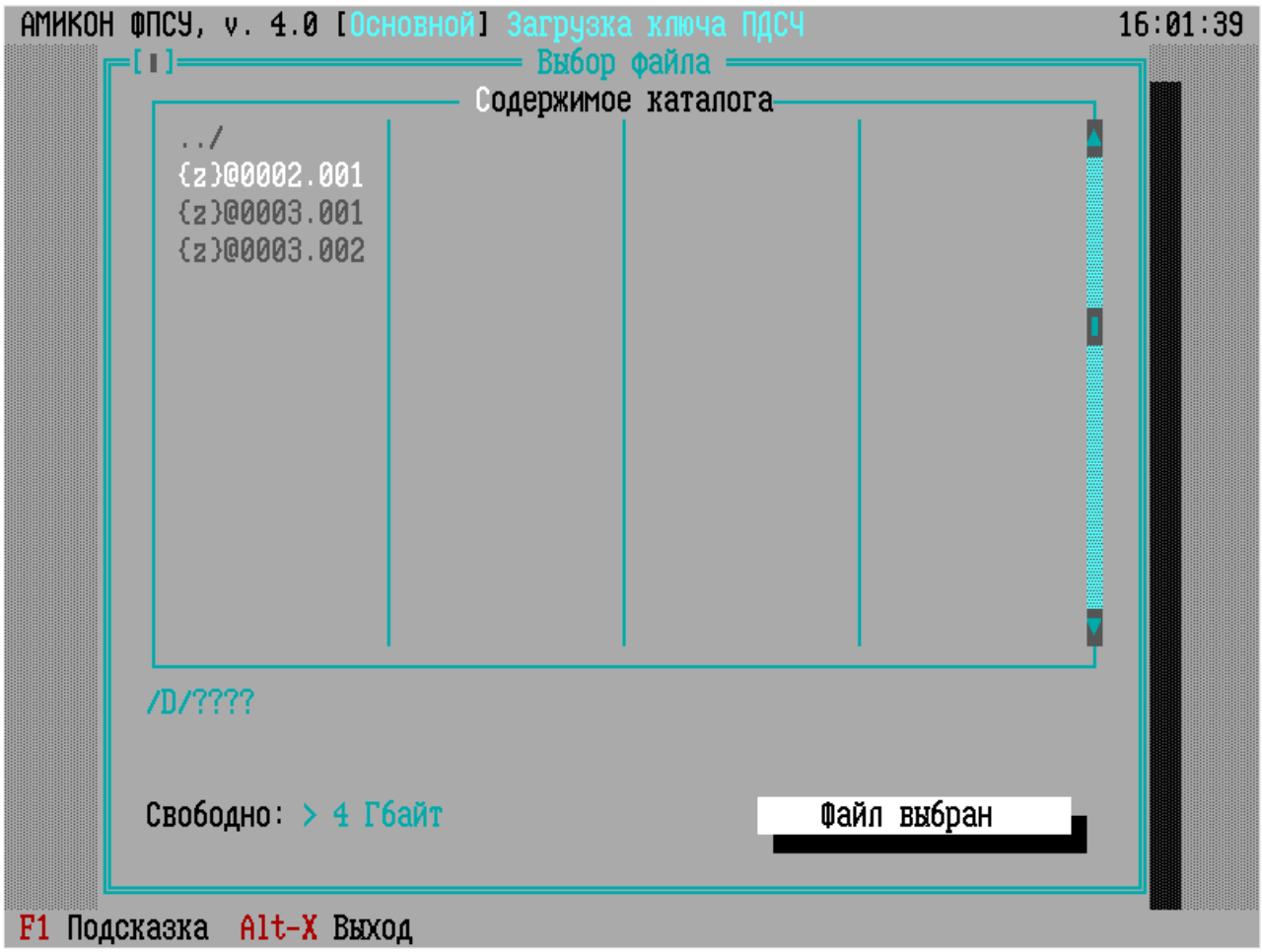


Рисунок 22 - Загрузка ключа ПДСЧ из файла

Переместите курсор на выбранный файл. Переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>. Подтвердите выбор файла, нажав на клавишу <*Enter*>. В открывшемся окне отобразится информация о ЦВК, выдавшем файл с ключом ПДСЧ и предложением загрузить этот файл.

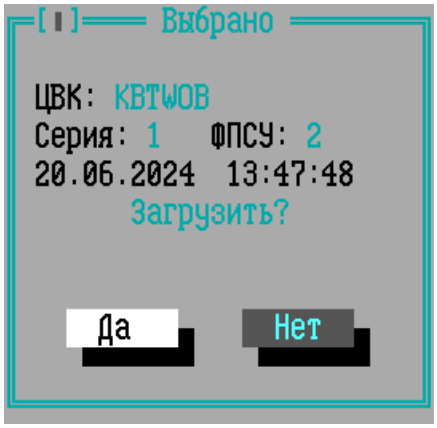


Рисунок 23 - Информация о загружаемом файле

После загрузки файла, ФПСУ-TLS выдаст системное оповещение о завершении процедуры:

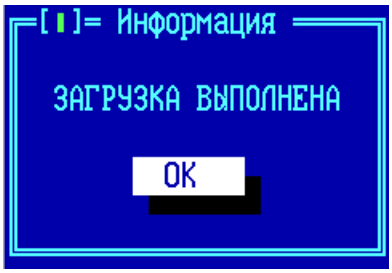


Рисунок 24 - Файл загружен

После инициализации программного датчика случайных чисел для завершения перехода в рабочий режим будет предложено перерегистрировать ТМ-идентификатор Главного администратора и зарегистрировать ещё один ТМ-идентификатор (рекомендуется зарегистрировать ТМ-идентификатор за записью «*Администратор-Запасная ТМ*» таблицы, подробнее о процедуре регистрации ТМ-идентификатора см. пункт «Регистрация запасного ТМ»).

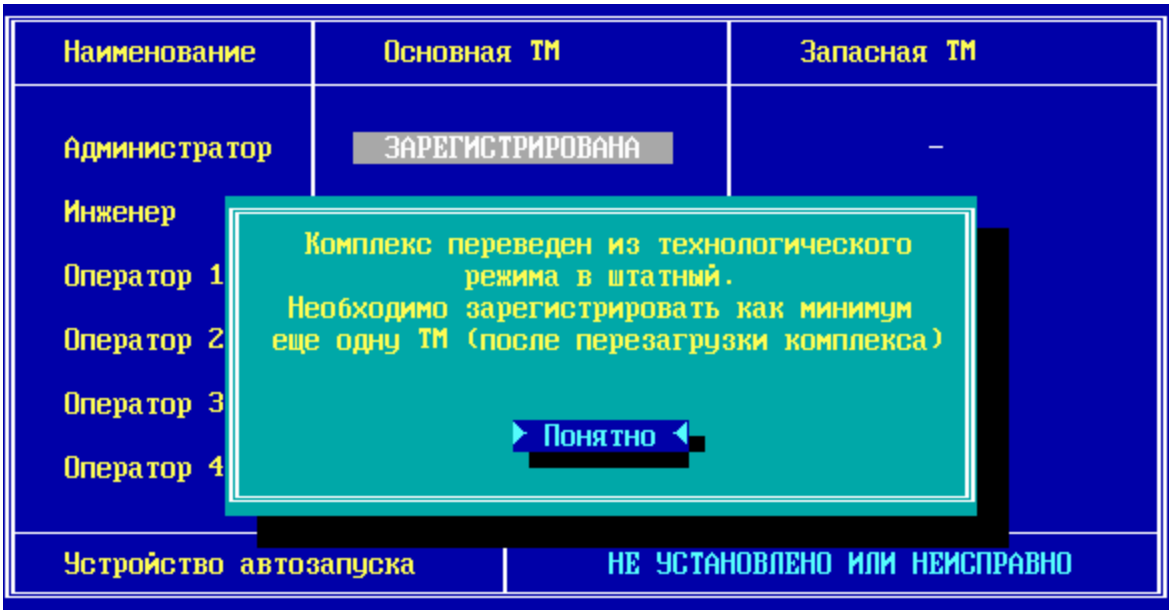


Рисунок 25 - Переход в рабочий режим

5. 3. Главное меню ФПСУ-TLS

В главном меню ФПСУ-TLS отображается версия программного обеспечения (3.1.20 на рисунке) и серийный номер этого ФПСУ-TLS (TLS00003C0 на рисунке).

Главное меню содержит команды для настройки системы, конфигурирования оборудования, установки режимов работы ФПСУ-TLS. Выбор каждой команды повлечет за

собой запрос на идентификацию администратора и проверку его прав доступа (с предъявлением соответствующего электронного ТМ-идентификатора) на запрашиваемые действия.

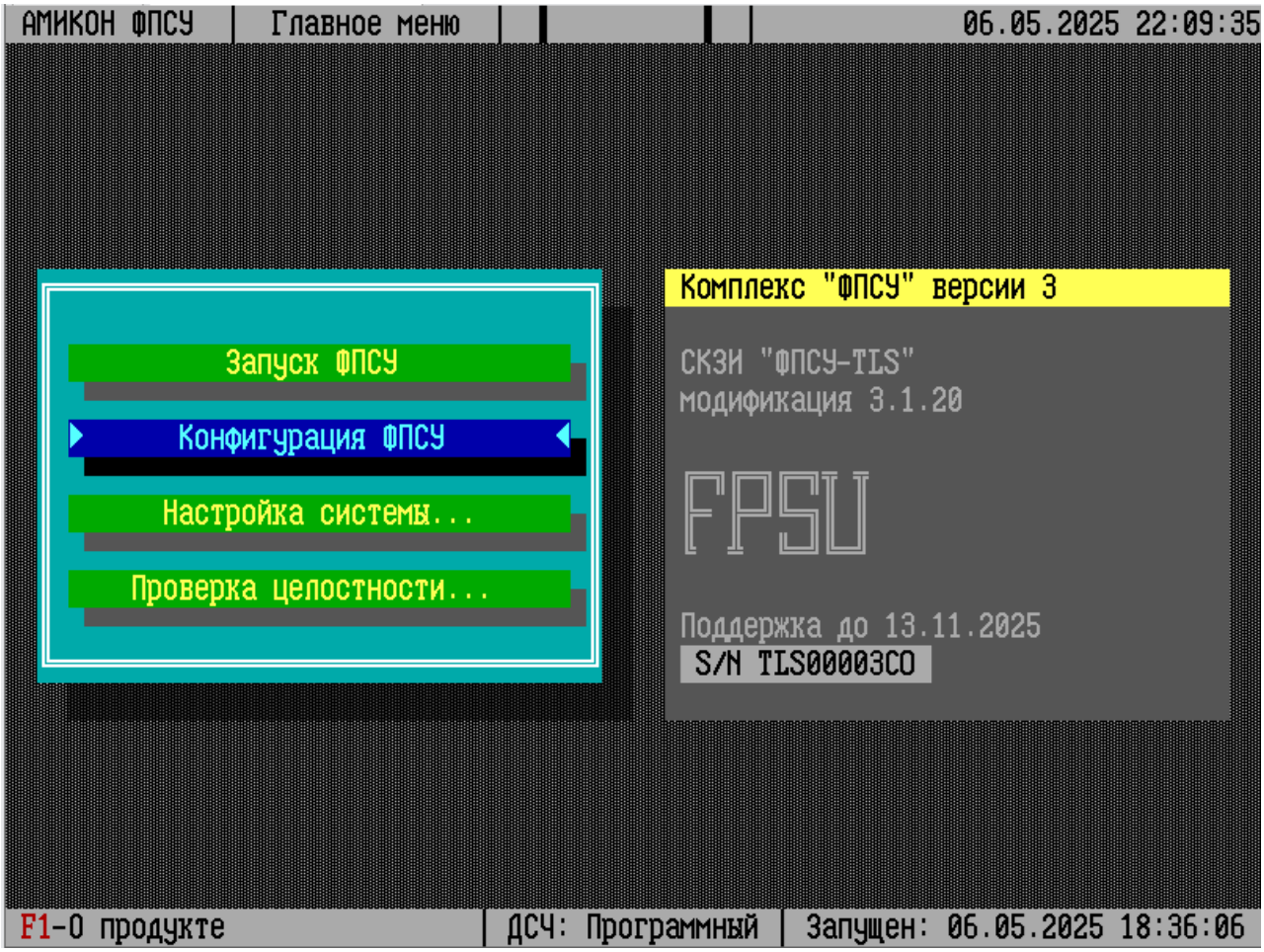


Рисунок 26 - Главное меню ФПСУ-TLS

При истечении срока действия открытого ключа АРМ УА, ФПСУ-TLS каждый раз при попадании в главное меню будет выдавать оповещение:

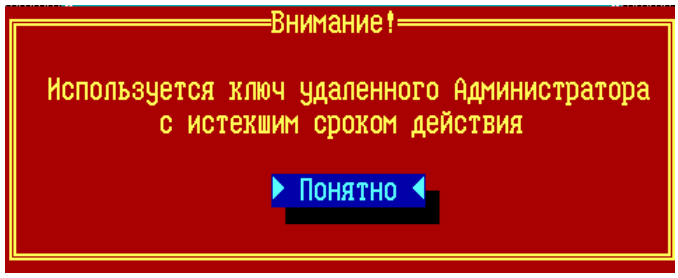


Рисунок 27 - Срок действия открытого ключа АРМ УА истек

Выполнение команды «Запуск ФПСУ» переводит ФПСУ-TLS в рабочий режим

защиты http-трафика.

Операция доступна администраторам класса *Оператор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

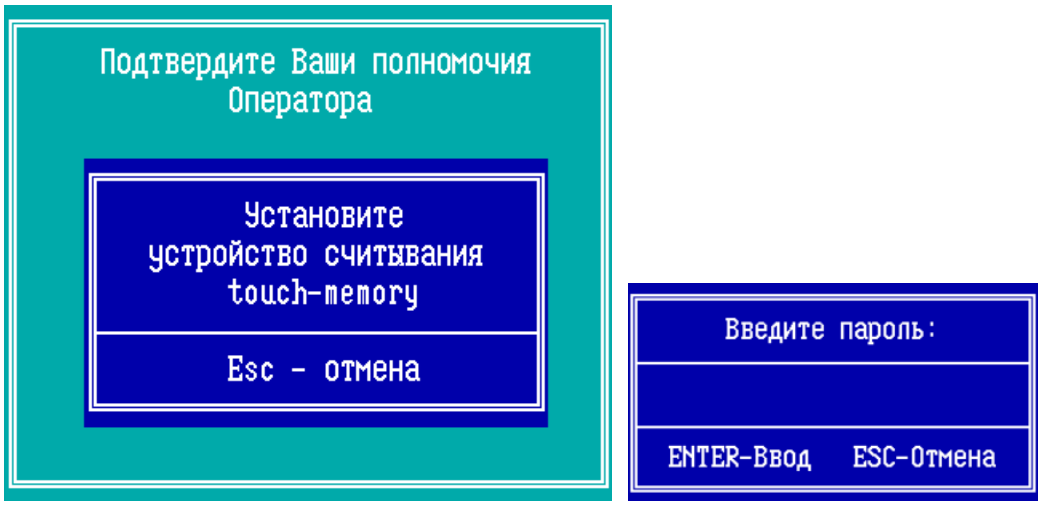


Рисунок 28 - Подтверждение полномочий и ввод пароля ТМ

ФПСУ-TLS выдает оповещение об истечении срока действия ключа запуска на главном экране в момент запуска, а также при открытии меню «Конфигурация ФПСУ»:

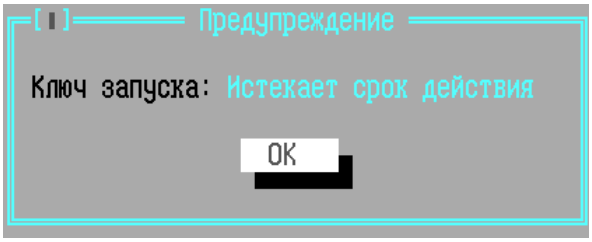


Рисунок 29 - Оповещение об истечении срока действия ключа запуска

В случае если текущая дата превышает срок действия ключа запуска выдается следующее предупреждение:

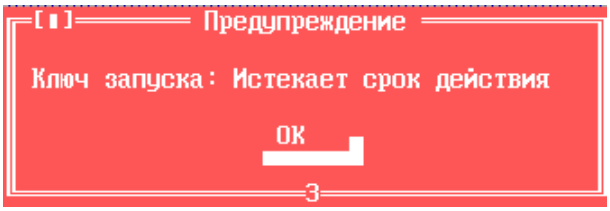


Рисунок 30 - Срок действия ключа запуска истек

ФПСУ-TLS выдает оповещение об истечении срока действия ключа ПДСЧ на главном экране в момент запуска, а также при открытии меню «Конфигурация ФПСУ»:

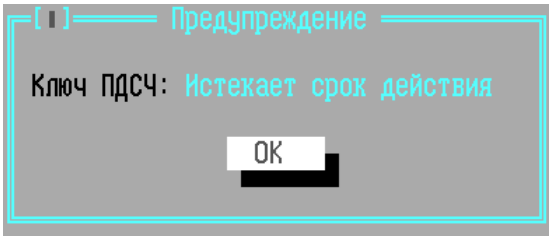


Рисунок 31 - Оповещение об истечении срока действия ключа ПДСЧ

В случае если текущая дата превышает срок действия ключа ПДСЧ выдается следующее предупреждение:

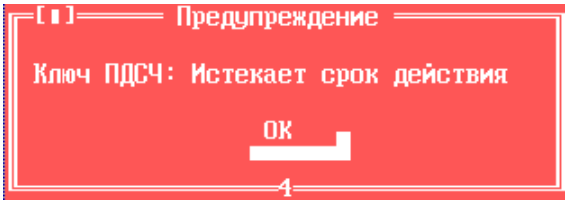


Рисунок 32 - Срок действия ключа ПДСЧ истек

ФПСУ-TLS выдает оповещение об истекшем сроке действия ключа для связи с АРМ УА на главном экране в момент запуска:

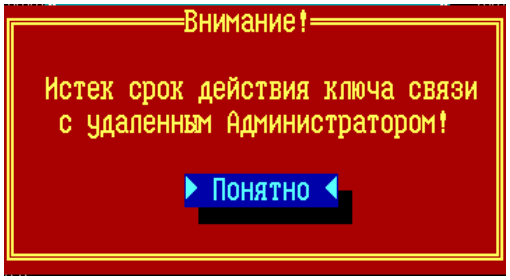


Рисунок 33 - Срок действия ключа для связи с АРМ УА истек

После авторизации выполнения команды «Запуск ФПСУ», ФПСУ-TLS переходит в рабочий режим защиты http-трафика и выводит на экран окно текущего состояния ФПСУ-TLS:

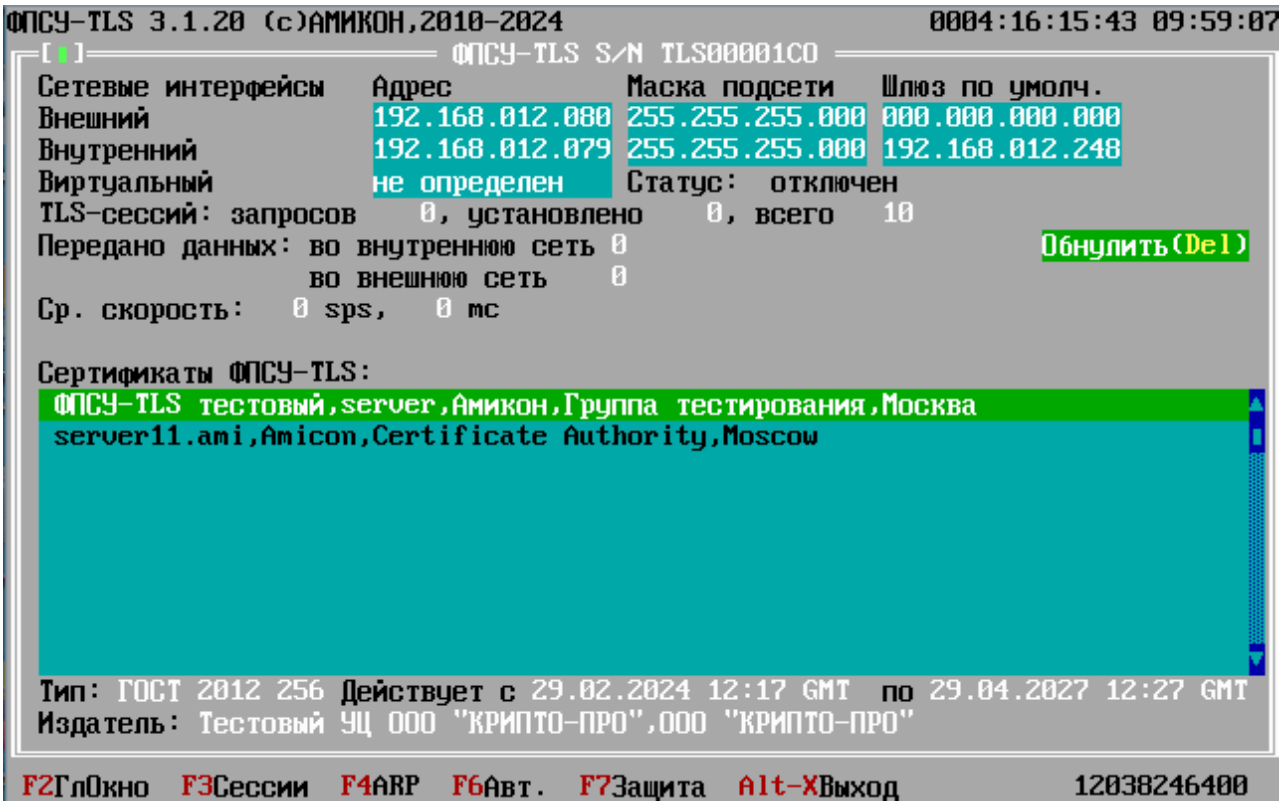


Рисунок 34 - Окно текущего состояния ФПСУ-TLS

Все остальные команды главного меню описаны подробно в соответствующих разделах далее.

В верхней строке экрана отображаются: текущая версия операционной среды ACCESS-TM SHELL, текущие время и дата на ФПСУ-TLS.

В нижней строке экрана содержится информация об аппаратном обеспечении, типе датчика случайных чисел (ДСЧ) и времени последнего запуска программного обеспечения ФПСУ-TLS.

5. 4. Конфигурация ФПСУ-TLS

Конфигурирование ФПСУ-TLS заключается в определении режимов и правил его работы, позволяющих осуществлять контроль передаваемого трафика данных в соответствии с топологией сети и требуемой степенью безопасности.

В конфигурации хранятся параметры сетевых настроек ФПСУ-TLS, установки сертификатов, адресов защищаемых http-серверов, взаимодействия с Syslog, NTP серверами, а также установки прочих особенностей работы. Параметры конфигурации описываются в пунктах далее.

На ФПСУ-TLS могут храниться несколько конфигураций, но активной может быть только одна. Переход в интерфейс управления конфигурациями, окно менеджера конфигураций, выполняется командой главного меню «Конфигурация ФПСУ».

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

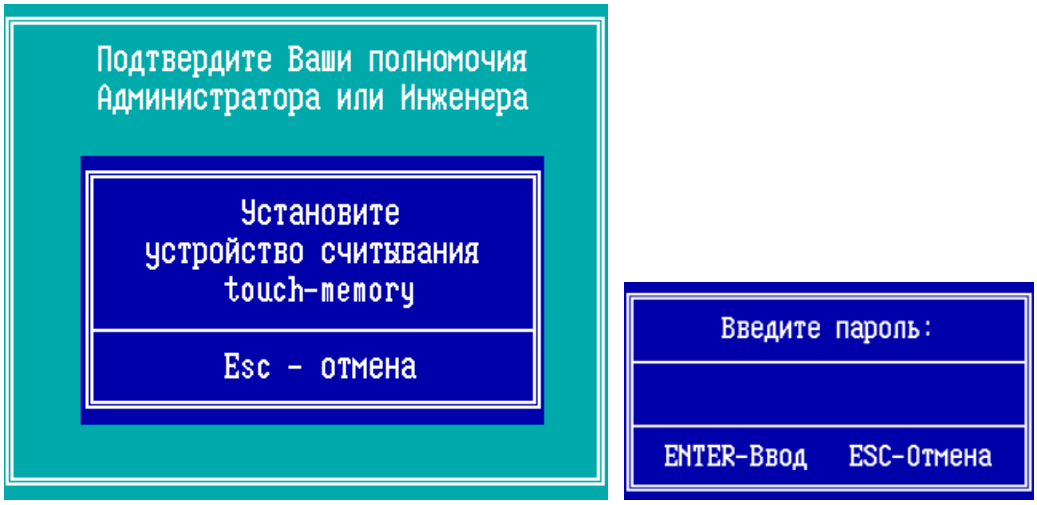


Рисунок 35 - Подтверждение полномочий и ввод пароля ТМ

ФПСУ-TLS выдает оповещение об истечении срока действия ключа запуска на главном экране в момент запуска, а также при открытии меню «Конфигурация ФПСУ»:

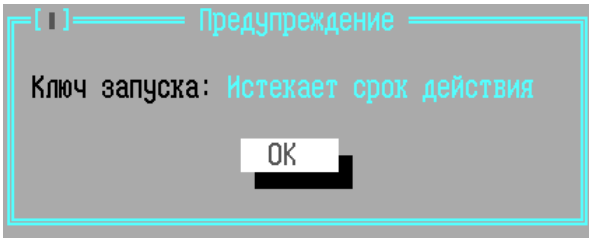


Рисунок 36 - Оповещение об истечении срока действия ключа запуска

В случае если текущая дата превышает срок действия ключа запуска выдается следующее предупреждение:

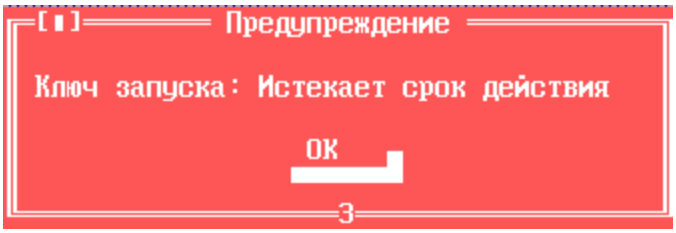


Рисунок 37 - Срок действия ключа запуска истек

ФПСУ-TLS выдает оповещение об истечении срока действия ключа ПДСЧ на главном экране в момент запуска, а также при открытии меню «Конфигурация ФПСУ»:

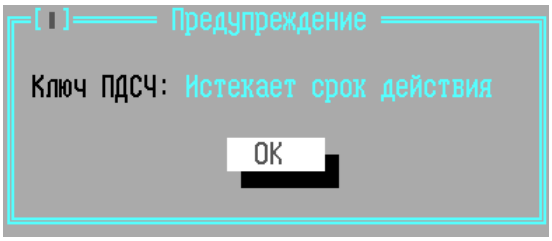


Рисунок 38 - Оповещение об истечении срока действия ключа ПДСЧ

В случае если текущая дата превышает срок действия ключа ПДСЧ выдается следующее предупреждение:

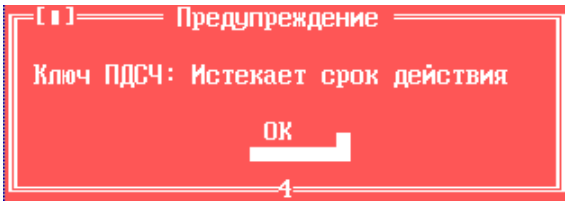


Рисунок 39 - Срок действия ключа ПДСЧ истек

После выполнения команды откроется окно менеджера конфигураций с пустым списком конфигураций. Для продолжения создайте конфигурацию ФПСУ-TLS, нажав клавишу <Ins>.

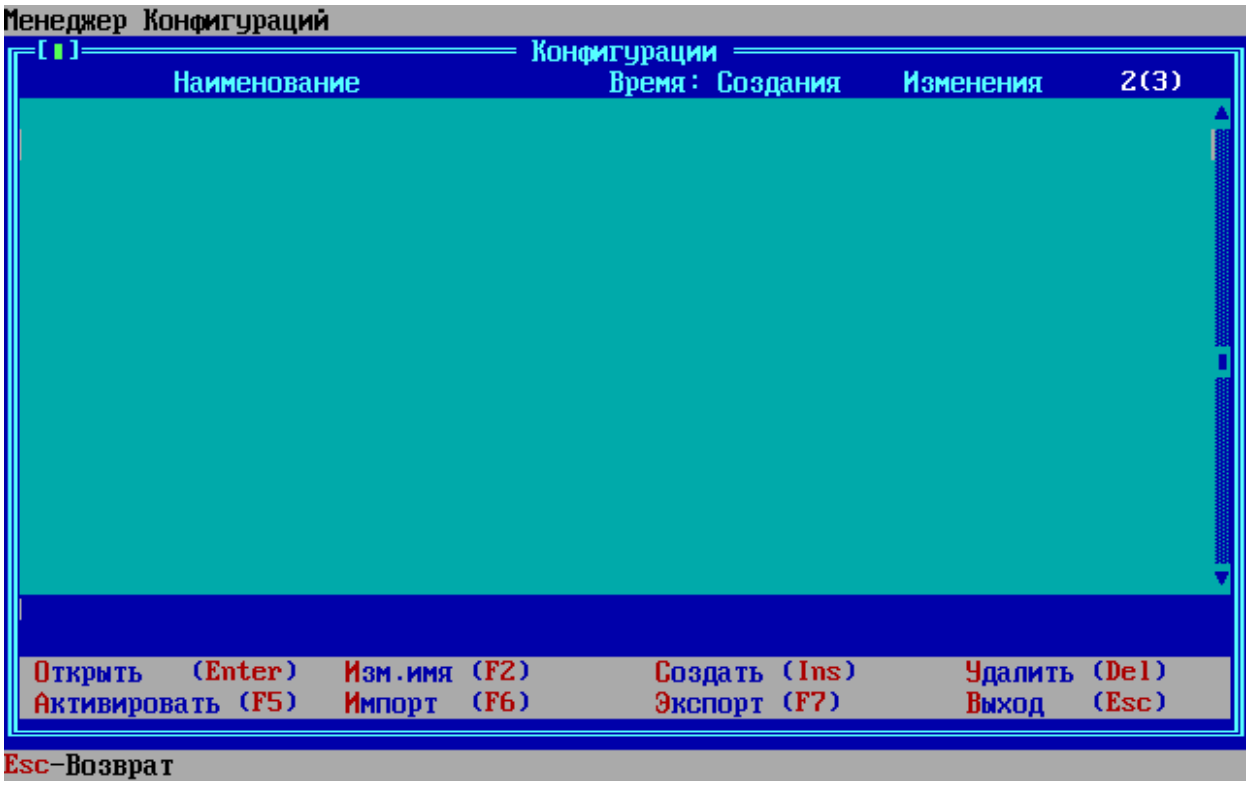


Рисунок 40 - Стартовое пустое окно менеджера конфигураций

Подтвердите создание новой конфигурации:

Рисунок 41 - Создание конфигурации

Конфигурацию режимов и правил работы можно скопировать с уже имеющейся конфигурации. Необходимо выделить конфигурацию, нажать клавишу <Ins> и подтвердить копирование, при этом ключевая информация не копируется.

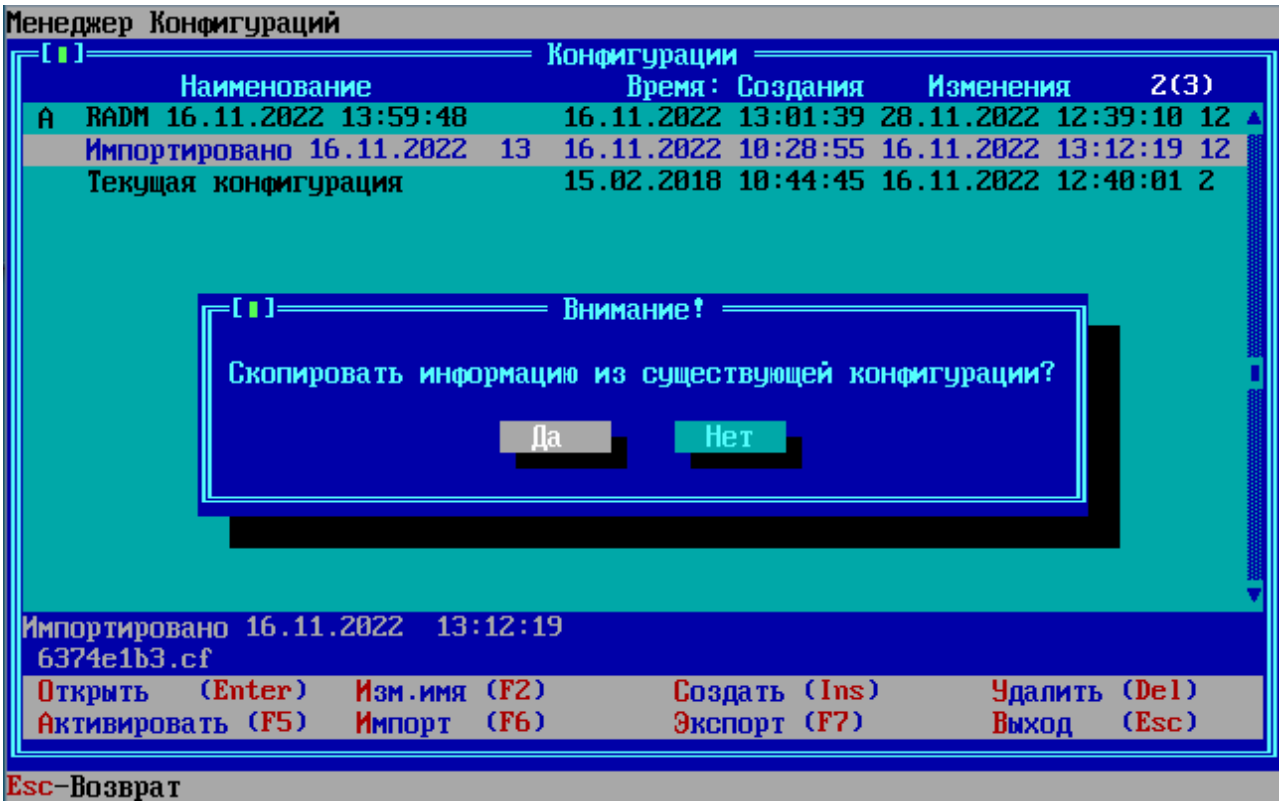


Рисунок 42 - Создание конфигурации копированием выбранной конфигурации

Откроется меню установки параметров ФПСУ-TLS. Для запуска ФПСУ-TLS в рабочий режим требуется выполнить предварительные обязательные настройки – указать сетевые параметры ФПСУ-TLS и защищаемых серверов, установить ключи и сертификаты, выданные Удостоверяющим Центром.

На рисунке приведено меню управления настройками конфигурации для администратора ФПСУ-TLS с правами класса «Инженер».

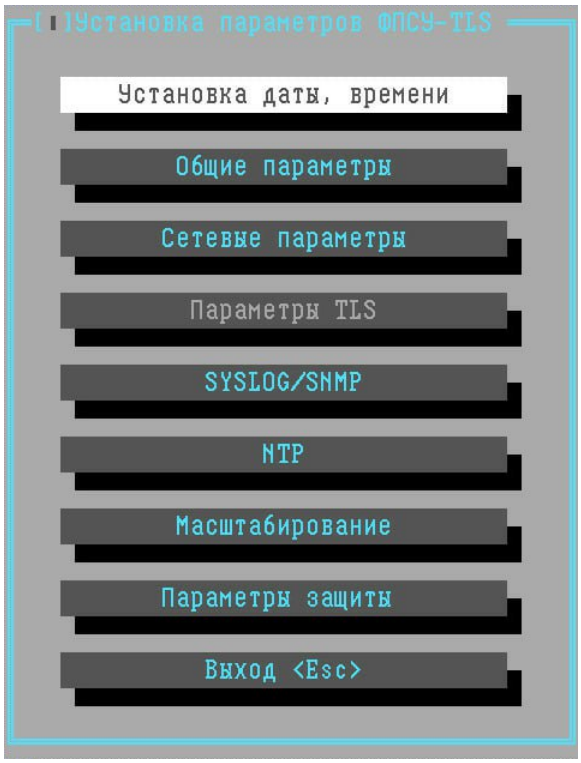


Рисунок 43 - Меню установки параметров ФПСУ-TLS

Настройка обязательных пунктов: сетевых параметров, установка ключей и сертификатов подробно описана в пунктах «Настройка сетевых параметров» и «Установка сертификатов» соответственно, настройка остальных параметров конфигурации ФПСУ-TLS описывается в разделе «Эксплуатация "ФПСУ-TLS"».

5. 5. Настройка сетевых параметров

Пункт «Сетевые параметры» меню установки параметров ФПСУ-TLS предназначен для задания основных сетевых настроек – IP-адресов внешнего и внутреннего сетевого интерфейса, маски сети, шлюза по умолчанию, а также защищаемых http-серверов.

Внешним интерфейсом ФПСУ-TLS называется сетевой адаптер, который подключен к маршрутизатору, взаимодействующему с внешней открытой сетью (Интернет). TLS-клиенты подключаются к ФПСУ-TLS со стороны внешнего интерфейса.

Внутренним интерфейсом ФПСУ-TLS называется сетевой адаптер, который подключен к внутренней локальной сети передачи данных, где установлены защищаемые http-сервера.

Для перехода в окно настроек сетевых параметров ФПСУ-TLS, выполните команду «Сетевые параметры» в меню установки параметров.

Откроется окно настройки внешнего и внутреннего интерфейсов и DNS-серверов.

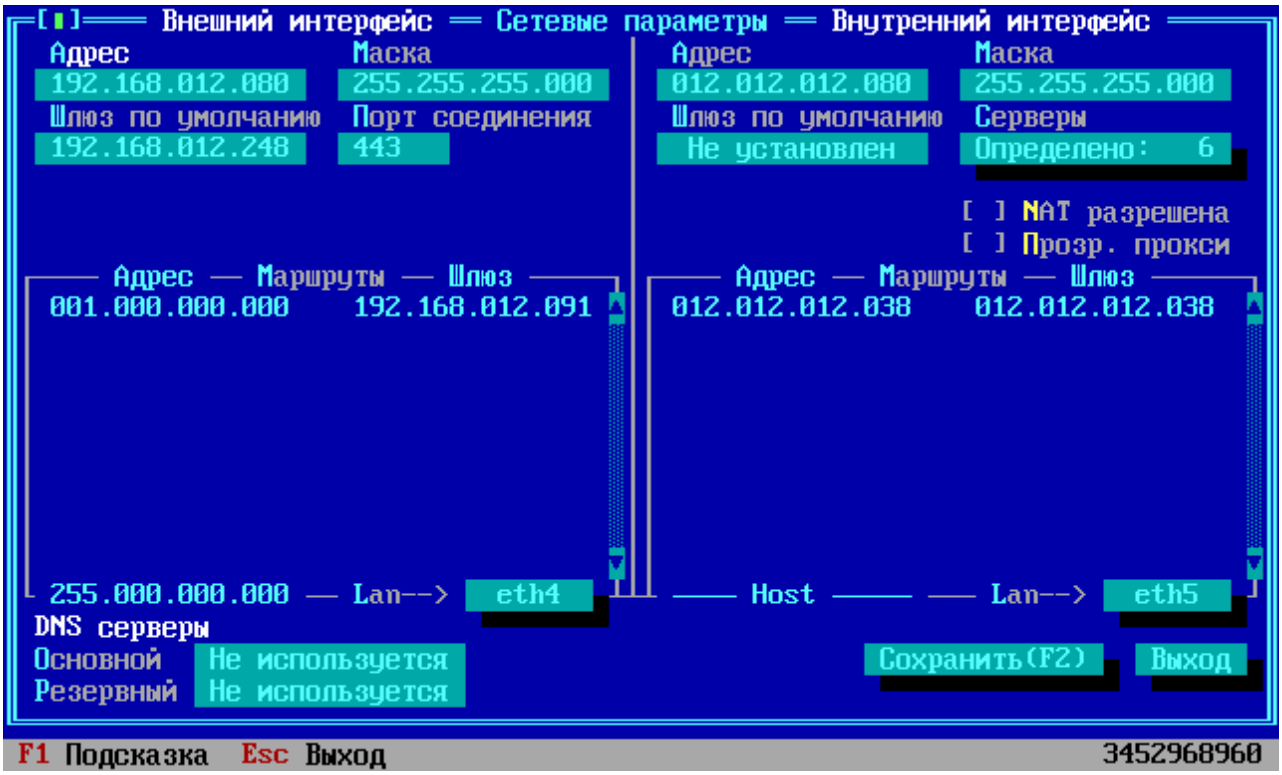


Рисунок 44 - Окно настройки сетевых параметров ФПСУ-TLS

Необходимо указать следующие параметры:

Сетевые параметры, Внешний интерфейс – в левой части окна указываются следующие параметры внешнего интерфейса ФПСУ-TLS:

- ***Адрес*** – логический IP-адрес внешнего интерфейса;
- ***Маска*** – маска IP-сети передачи данных стороны внешнего интерфейса;
- ***Шлюз по умолчанию*** – IP-адрес маршрутизатора, отвечающего за доставку пакетов во внешнюю открытую сеть (опционально);
- ***Порт соединения*** – порт TCP службы, на который ФПСУ-TLS принимает запросы TLS-клиентов на установку TLS-соединения (рекомендуемый порт по умолчанию – 443).

DNS-серверы – в нижней части окна указываются IP-адреса основного и резервного DNS-серверов, отвечающих за процедуру разрешения Интернет-имен, если TLS-клиенты используют для обращения к http-серверам не IP-адреса, а систему доменных имен Интернет (например, server.domain.org).

Сетевые параметры, Внутренний интерфейс – в правой части окна указываются следующие параметры внутреннего интерфейса ФПСУ-TLS:

- ***Адрес*** – логический IP-адрес внутреннего интерфейса;
- ***Маска*** – маска IP-сети передачи данных стороны внутреннего интерфейса;
- ***Шлюз по умолчанию*** – IP-адрес маршрутизатора, отвечающего за доставку пакетов во внешнюю открытую сеть (опционально);
- ***Серверы, Определено*** – кнопка перехода в окно настройки защищаемых http-серверов внутренней сети передачи данных (подробнее см. пункт «Настройка защищаемых http-серверов»).

Под кнопкой «Серверы, Определено» находится блок настроек NAT, преобразования сетевого адреса внутреннего порта ФПСУ-TLS. При включенном флаге ***«NAT разрешена»*** внутреннему порту ФПСУ-TLS добавляется указанное число виртуальных IP-адресов. Этот диапазон виртуальных IP-адресов используется для разделения по IP адресам клиентских TLS-сессий во внутренней сети с целью, например, последующей балансировки нагрузки на сервера Веб-Сервисов (подробнее см. пункт «О работе "ФПСУ-TLS" в режиме NAT»). При включенном флаге диапазон виртуальных IP-адресов распределяется равномерно между подключенными к ФПСУ-TLS TLS-клиентами, причем всем сессиям одного клиента в рамках текущего соединения назначается один и тот же виртуальный IP-адрес.

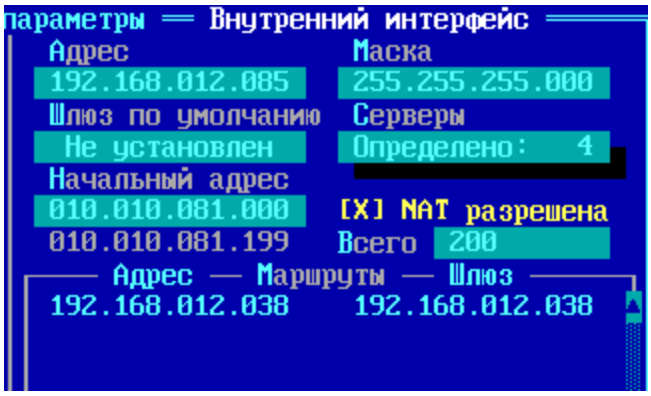


Рисунок 45 - Настройки NAT

NAT разрешена – флаг, активирующий режим преобразования сетевых адресов; если отключен, то все сессии TLS-клиентов передаются во внутреннюю сеть с одним и тем же IP адресом внутреннего порта ФПСУ-TLS.

Начальный адрес – начальный IP адрес выделяемого для режима NAT диапазона IP адресов. IP адрес должен быть из той же подсети. Под полем «Начальный адрес» указывается значение последнего IP-адреса, выделенного для режима NAT диапазона.

Всего – количество IP адресов, начиная с начального адреса, которое будет выдано для режима NAT.

Прозр. Прокси (прозрачный прокси) – установленный флаг означает, что ФПСУ-TLS будет соединяться с защищаемыми http-серверами от адреса клиента.

Режим «прозрачный прокси» и NAT нельзя устанавливать одновременно.

Для исключения ошибок при работе ФПСУ-TLS в режиме «прозрачный прокси», необходимо, чтобы находящееся за ФПСУ-TLS оборудование (серверы, балансировщики нагрузки, маршрутизаторы и т.д.) отрабатывало gratuitous ARP запросы. Это необходимо, т.к. один и тот же клиент может соединиться через разные ФПСУ.

Если не выбраны режимы «прозрачный прокси» и NAT, то соединение с защищаемыми http-серверами устанавливается от внутреннего адреса ФПСУ-TLS.

Для возврата в меню настройки ФПСУ-TLS с внесением выполненных изменений в конфигурацию нажмите кнопку «Сохранить».

По команде «Выход» осуществляется возврат в главное меню без сохранения изменений.

5. 5. 1. Настройка защищаемых http-серверов

На ФПСУ-TLS указывается список разрешенных http-серверов, к которым будет разрешен доступ удаленным пользователям, так называемый белый список.

Для указания защищаемых ФПСУ-TLS http-серверов выполните команду ***«Серверы, Определено»*** окна настройки сетевых параметров ФПСУ-TLS.

В открывшемся окне «Обслуживаемые серверы» требуется указать сетевые параметры защищаемых объектов – http-серверов.

Окно содержит список заранее сконфигурированных обслуживаемых ФПСУ-TLS http-серверов (от 1 до 64 записей).

Http-сервер по умолчанию – Одна из записей списка должна иметь статус «По умолчанию» (статус присваивается первой созданной записи) – на этот http-сервер будут перенаправлены запросы TLS-клиентов, в которых не указан адрес http-сервера, к которому подключается TLS-клиент. Строка сервера по умолчанию отмечена зеленым цветом. Для установки другой записи как сервера по умолчанию, требуется установить курсор на запись и нажать клавишу <Пробел>.

Выход из окна списка обслуживаемых серверов обратно в окно настройки сетевых параметров осуществляется нажатием клавиши <Esc>.

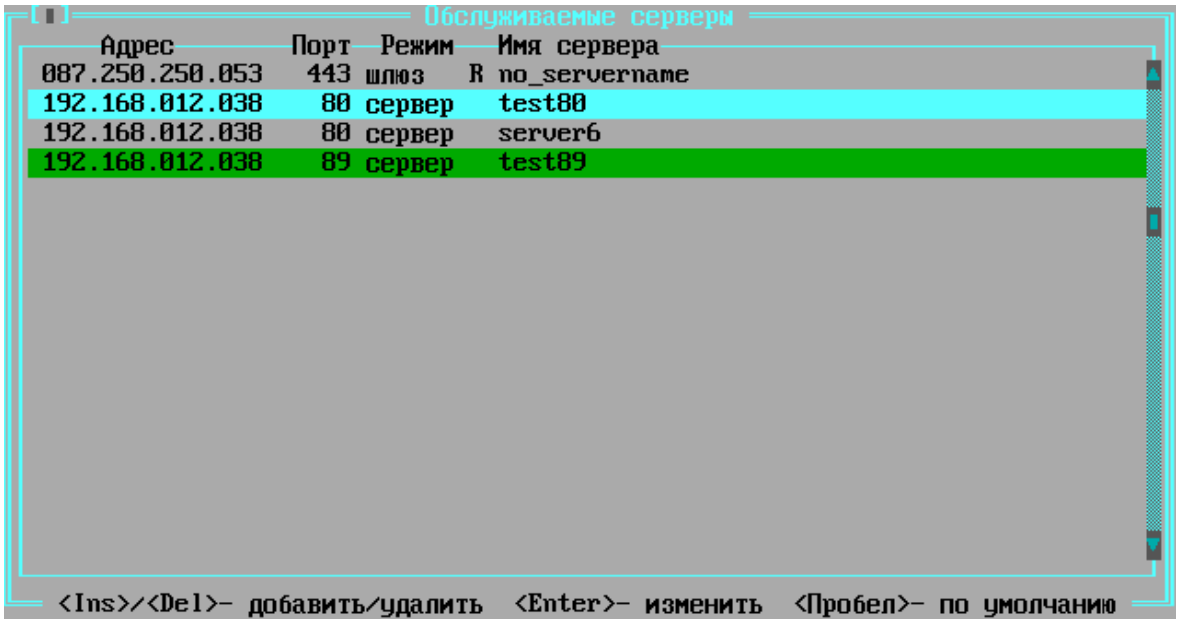


Рисунок 46 - Список обслуживаемых серверов

По умолчанию список обслуживаемых серверов пуст. Для добавления http-сервера нажмите клавишу <Ins>. В открывшемся окне ввода параметров обслуживаемого сервера введите:

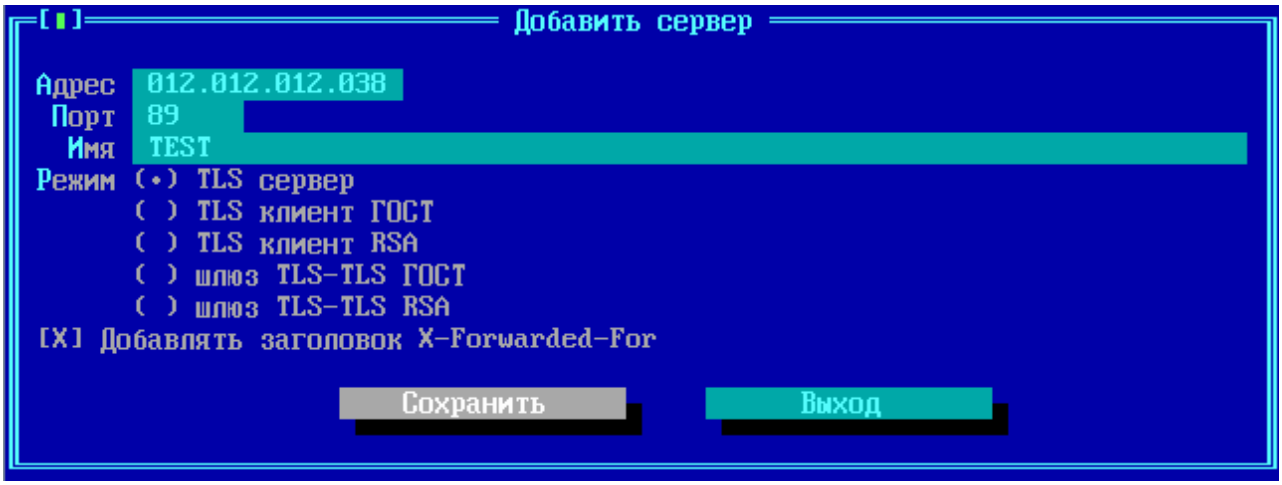


Рисунок 47 - Указание параметров обслуживаемого сервера

Адрес – IP-адрес рабочей станции, на котором запущена служба http-сервера;

Порт – номер TCP/UDP-службы, выделенный приложению http-сервера;

Имя сервера – произвольное символьное имя описываемого http-сервера;

Режим – опция, указывающая модель взаимодействия ФПСУ-TLS и сервера, находящегося по указываемому IP-адресу. Если добавляется адрес и порт защищаемого http-сервера, следует оставить режим по умолчанию, «TLS сервер» (подробнее см. пункт «Режимы взаимодействия ФПСУ-TLS и защищаемой службы»);

Добавлять заголовок X-Forwarded-For - заголовок «X-Forwarded-For» используется для идентификации происхождения IP-адреса клиента, подключающегося к веб-серверу через HTTP-прокси или через балансировщик нагрузки. Когда трафик перехватывается между клиентами и серверами, журналы доступа к серверу содержат только IP-адрес прокси-сервера или балансировки нагрузки. Установленный флаг позволяет использовать заголовок запроса «X-Forwarded-For», чтобы увидеть исходный IP-адрес клиента.

После ввода параметров обслуживаемого http-сервера нажмите кнопку «Сохранить» для внесения изменений в конфигурацию. Нажатием кнопки «Выход» окна «Добавить сервер» осуществляется возврат в окно списка обслуживаемых серверов без внесения изменений.

Обратите внимание, что на одном логическом IP-адресе может быть запущено более одной службы (на различных TCP/UDP-портах). Http-сервер, на котором запущено две www-службы, например, на порту 80 и порту 8080, требует создания двух описаний в списке обслуживаемых ФПСУ-TLS серверов.

5. 5. 2. О работе ФПСУ-TLS в режиме NAT

Настройка работы ФПСУ-TLS в режиме NAT выполняется в меню установки параметров, пункт «Сетевые параметры» (см. пункт «Настройка сетевых параметров»).

Режим NAT предназначен, главным образом, для балансировки нагрузки на защищаемые http-сервера Веб-Сервисов.

При включении режима «NAT», соединения от ФПСУ-TLS к серверам будут осуществляться не от одного IP-адреса (внутреннего адреса ФПСУ-TLS), а адрес будет выбираться из некоторого заданного администратором ФПСУ-TLS интервала IP-адресов.

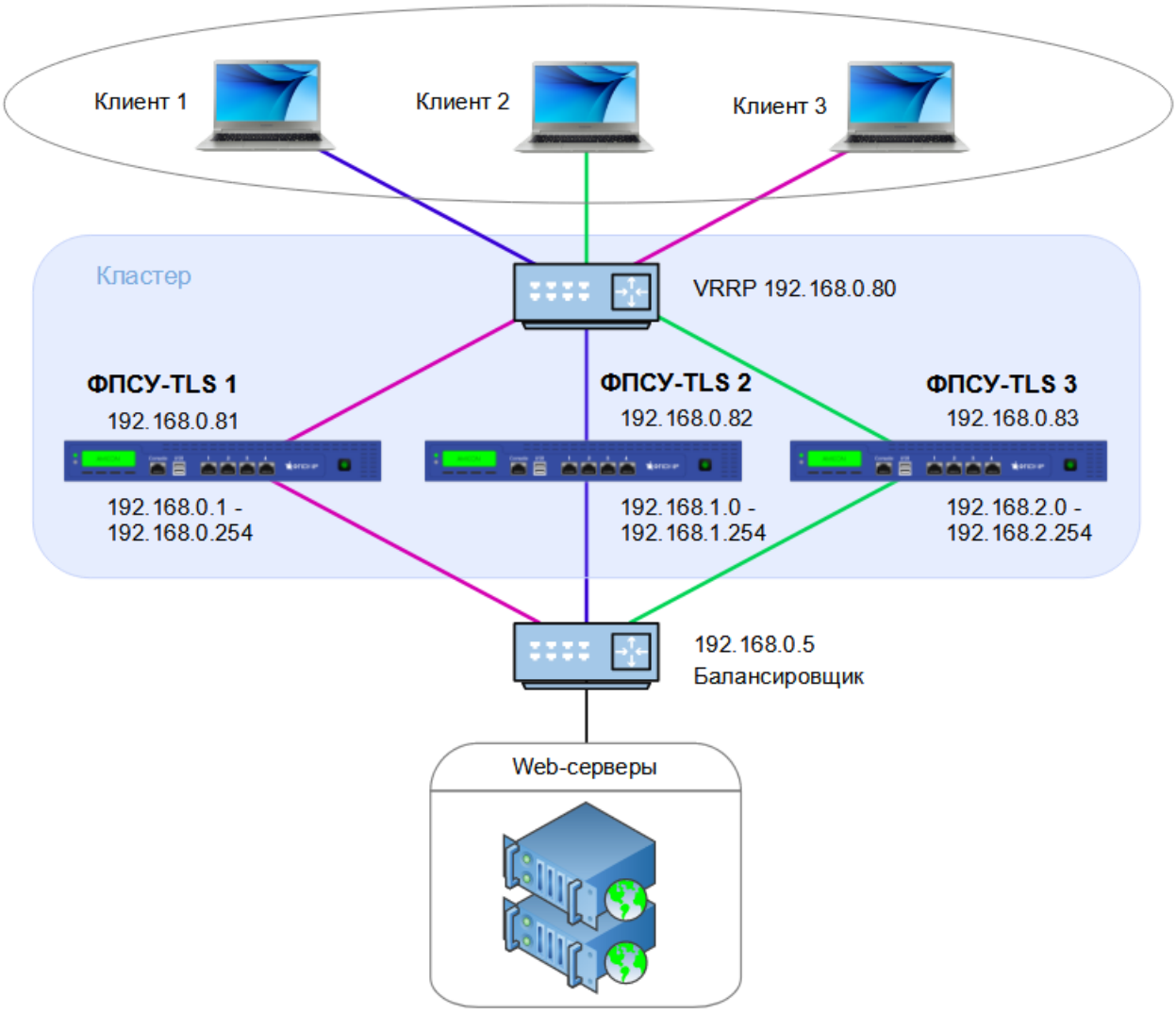


Рисунок 48 - Схема работы ФПСУ-TLS в режиме NAT

Перед кластером обслуживаемых http-серверов устанавливается сторонний балансировщик нагрузки, работающий на основе исходящего IP-адреса источника соединения.

5. 6. Общие настройки

По команде «Параметры TLS → Общие настройки» меню установки параметров ФПСУ-TLS устанавливаются настройки используемых версий протокола TLS, обеспечивающих формирование защищенных межсетевых HTTPS туннелей.

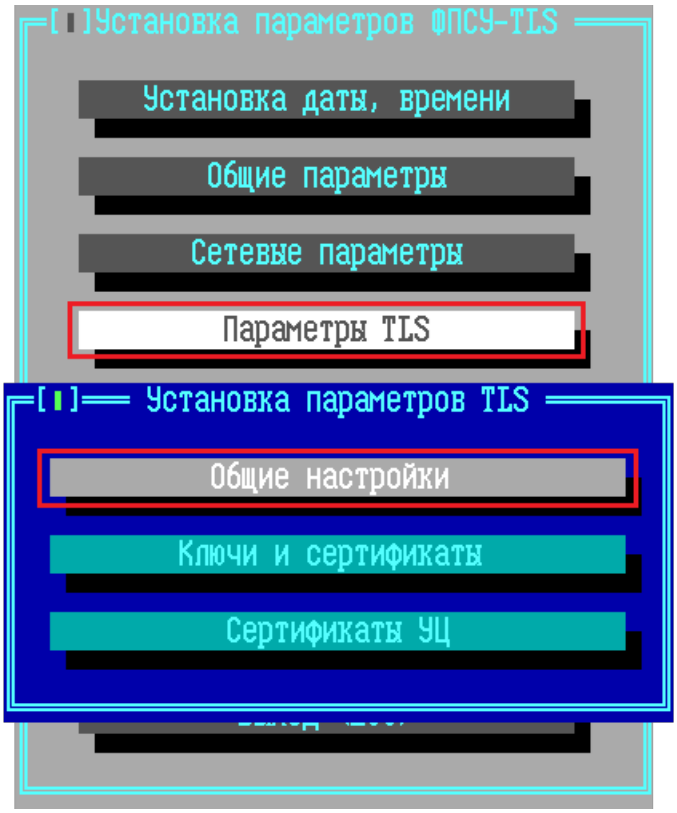


Рисунок 49 - Меню ФПСУ-TLS

Откроется окно настройки общих параметров TLS.

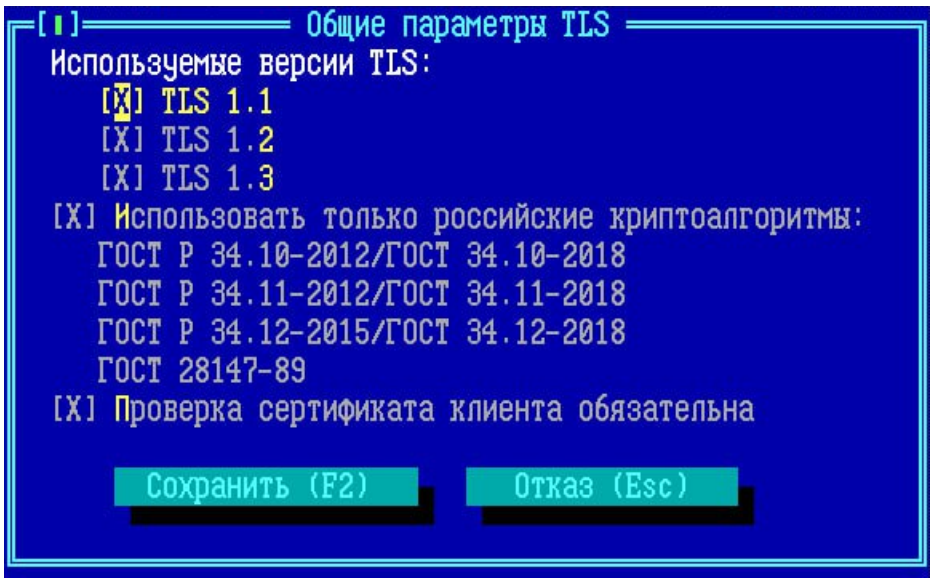


Рисунок 50 -Общие настройки TLS

По умолчание установлены флаги для версий 1.1, 1.2, 1.3 протокола TLS, т.е. ФПСУ-TLS обеспечивает формирование защищенных межсетевых HTTPS туннелей в соответствии

с протоколами TLS 1.2 и TLS 1.3, также поддерживается протокол TLS 1.1.

Использовать только российские криптоалгоритмы – при включении флага ФПСУ-TLS разрешено использовать только перечисленные российские алгоритмы для работы. Для версий протокола TLS 1.1 и 1.2 разрешено использовать криптоалгоритмы: ГОСТ Р 34.10-2012 (256 и 512 бит), ГОСТ Р 34.11-2012 (256 и 512 бит), ГОСТ 28147-89. Для версии протокола TLS 1.3 разрешено использовать криптоалгоритмы: ГОСТ 34.10-2018 (256 и 512 бит), ГОСТ 34.11-2018 (256 и 512 бит), ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (Кузнечик), ГОСТ Р 34.12-2015/ГОСТ 34.12-2018 (Магма). После включения флага «Использовать только российские криптоалгоритмы» ФПСУ-TLS не будет принимать или устанавливать соединения с применением сертификатов на основе алгоритма RSA (криптонаборы TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) .

Проверка сертификата клиента обязательна – установленный флаг включает взаимную аутентификацию по протоколу TLS, при соединении у TLS-клиента проверяется сертификат X.509. При выключенном флаге устанавливается односторонняя аутентификация, сертификат TLS-клиента не проверяется.

5. 7. Установка сертификатов

Вторым обязательным шагом в первоначальной настройке ФПСУ-TLS является установка следующих ключевых данных:

1. Сертификатов Удостоверяющих Центров;
2. Списка отозванных сертификатов;
3. Секретного ключа и личного сертификата сервера ФПСУ-TLS.

Интерфейс управления сертификатами удостоверяющих центров вызывается по команде «Сертификаты УЦ» меню установки параметров ФПСУ-TLS (подробнее см. пункт «Установка сертификатов удостоверяющих центров»).

Список отозванных сертификатов (СОС) – электронный документ с электронной цифровой подписью уполномоченного лица УЦ формата X.509, предназначенный для обеспечения возможности проверки сертификатов взаимодействующих сторон на предмет их актуальности (см. пункт «Установка списка отозванных сертификатов»).

Личный сертификат сервера ФПСУ-TLS используется TLS-клиентом, при установлении соединения, для проверки подлинности ФПСУ-TLS как TLS-сервера (см.

пункт «Установка личных сертификатов ФПСУ-TLS»).

5. 7. 1. Установка сертификатов удостоверяющих центров

Установка корневого сертификата удостоверяющего центра (УЦ) необходима, чтобы доверять сертификатам X.509, которые были подписаны этим удостоверяющим центром.

Установка файла с корневым сертификатом УЦ выполняется с внешнего USB-устройства, подключаемого к ФПСУ-TLS.

Для перехода в окно управления сертификатами удостоверяющего центра, выполните команду «Параметры TLS → Сертификаты УЦ» меню установки параметров ФПСУ-TLS.

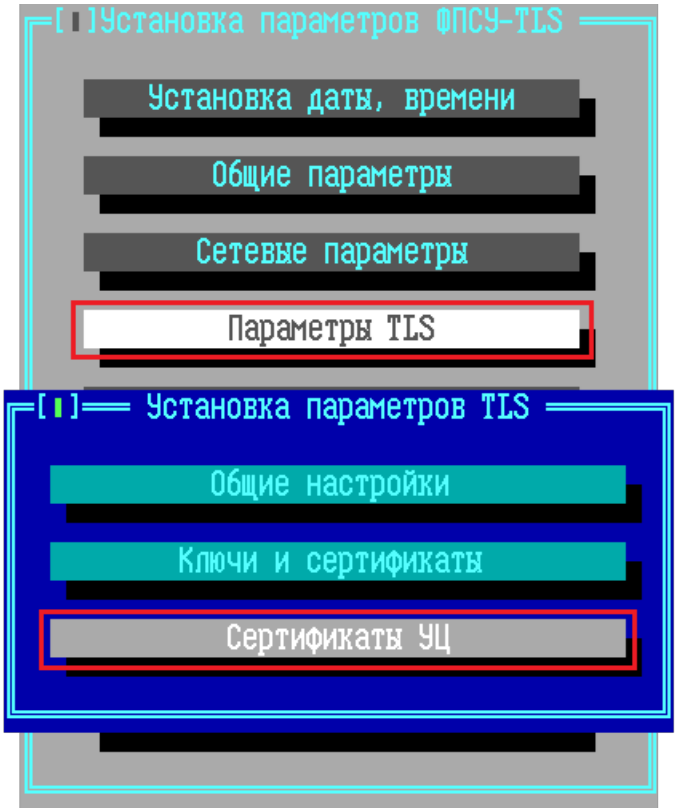


Рисунок 51 - Меню ФПСУ-TLS

В окне «Просмотр сертификатов» находится область «Загрузка сертификатов» – группа следующих команд, предназначенных для управления загрузкой сертификатов на ФПСУ-TLS:

- ***Корневой*** – загрузка на ФПСУ-TLS файла корневого сертификата УЦ;
- ***Некорневой*** – загрузка на ФПСУ-TLS файла сертификата промежуточного УЦ, который подписывает личный сертификат ФПСУ-TLS;

- ***Конверт*** – загрузка на ФПСУ-TLS файла с комплектом сертификатов, хранящихся в формате PKCS#7.

Для начала установки корневого сертификата УЦ в окне «Просмотр сертификатов» выполните команду «Корневой» области «Загрузка сертификатов УЦ».

Интерфейс выдаст приглашение подключить USB-носитель, на котором расположен файл с корневым сертификатом УЦ:

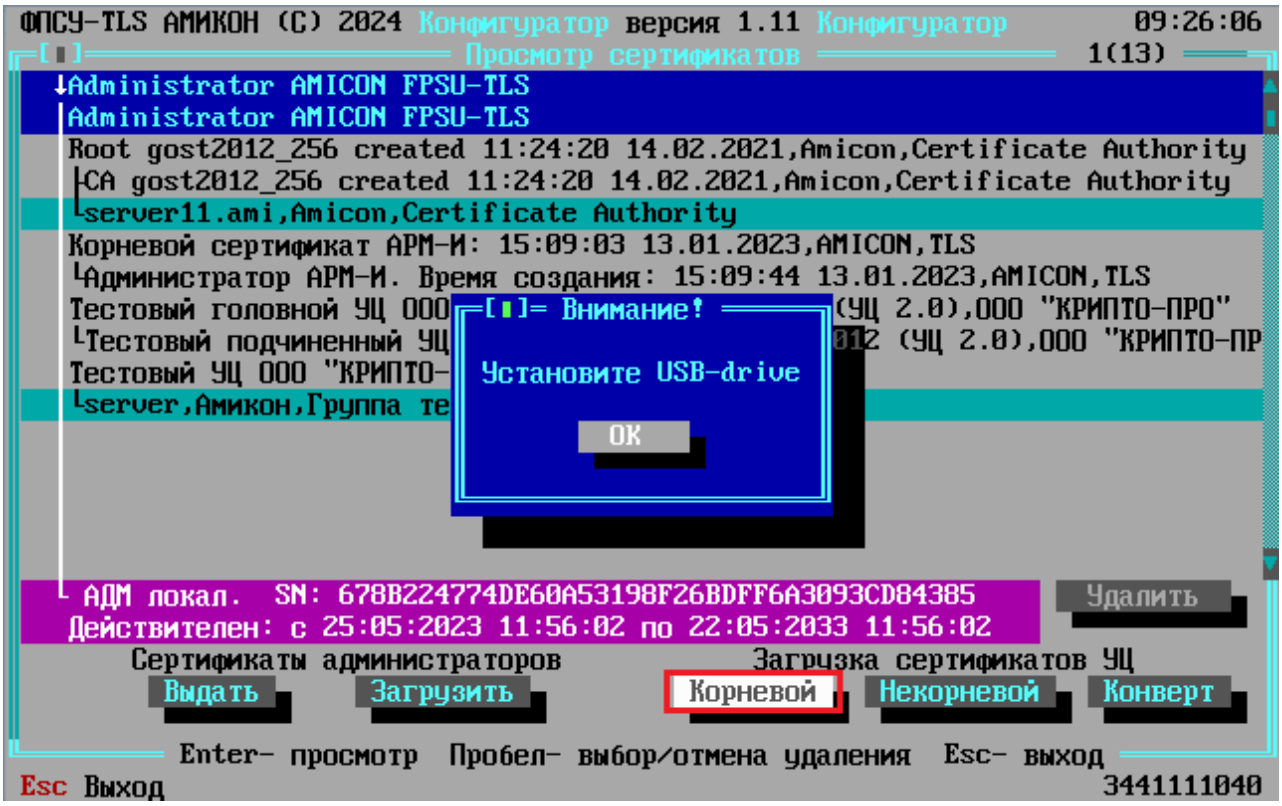


Рисунок 52 - Загрузка корневого сертификата

Подключите USB-носитель, на котором находится корневой сертификат удостоверяющего центра, к ФПСУ-TLS, и нажмите кнопку «ОК».

В открывшемся окне выбора каталога и файла установите курсор на файле, в котором находится корневой сертификат удостоверяющего центра, и нажмите на кнопку «Файл выбран».

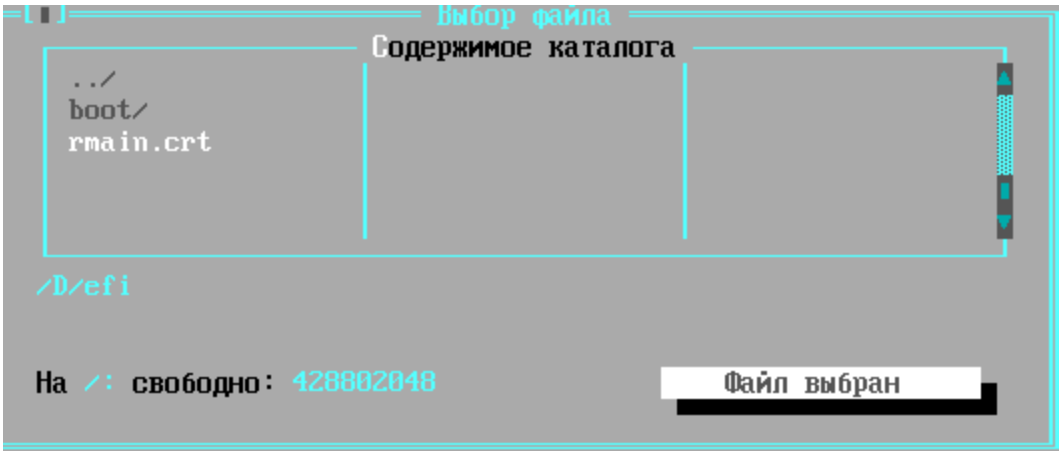


Рисунок 53 - Выбор файла с корневым сертификатом УЦ

Корневой сертификат УЦ будет установлен на ФПСУ-TLS.

После установки корневого сертификата удостоверяющего центра выполните, если требуется, установку сертификатов промежуточных удостоверяющих центров.

Установка сертификатов промежуточных удостоверяющих центров выполняется по команде «Некорневой» поля «Загрузка сертификатов» окна «Просмотр сертификатов». Порядок установки сертификатов промежуточных УЦ такой же, как и при установке корневого сертификата УЦ.

Если сертификаты УЦ хранятся в формате PKCS#7, их можно загрузить одним комплектом, использовав команду «Конверт» поля «Загрузка сертификатов» окна «Просмотр сертификатов». Порядок установки комплекта сертификатов, хранящихся в формате PKCS#7 такой же, как и при установке корневого сертификата УЦ.

Для удаления сертификата, выделите курсором соответствующую строку и нажмите <Пробел>, строка будет отмечена слева знаком «√», затем нажмите кнопку ***«Удалить»***.

Для выхода в меню ФПСУ-TLS нажмите клавишу <Esc>.

5. 7. 2. Управление сертификатами администраторов ФПСУ-TLS

На ФПСУ-TLS может быть загружена конфигурация другого ФПСУ-TLS из кластера. В этом случае необходимо:

на ФПСУ-TLS, с которого скачивается конфигурация

- выдать сертификат администратора для ФПСУ-TLS, на который загружается конфигурация;
- при активации текущей конфигурации включить флаг «Разрешить скачивание

партнерам» (см. пункт «Менеджер конфигураций»);

на ФПСУ-TLS, на который загружается конфигурация

- установить сертификат администратора ФПСУ-TLS, с которого скачивается конфигурация;
- включить автообновление конфигурации – задать IP адрес ФПСУ-TLS, с которого скачивается конфигурация, и установить флаг «Обновление разрешено» (см. пункт «Автозагрузка СОС, сертификатов и конфигураций ФПСУ-TLS»).

Для перехода в окно управления сертификатами администраторов выполните команду «Параметры TLS → Сертификаты УЦ» меню установки параметров ФПСУ-TLS.

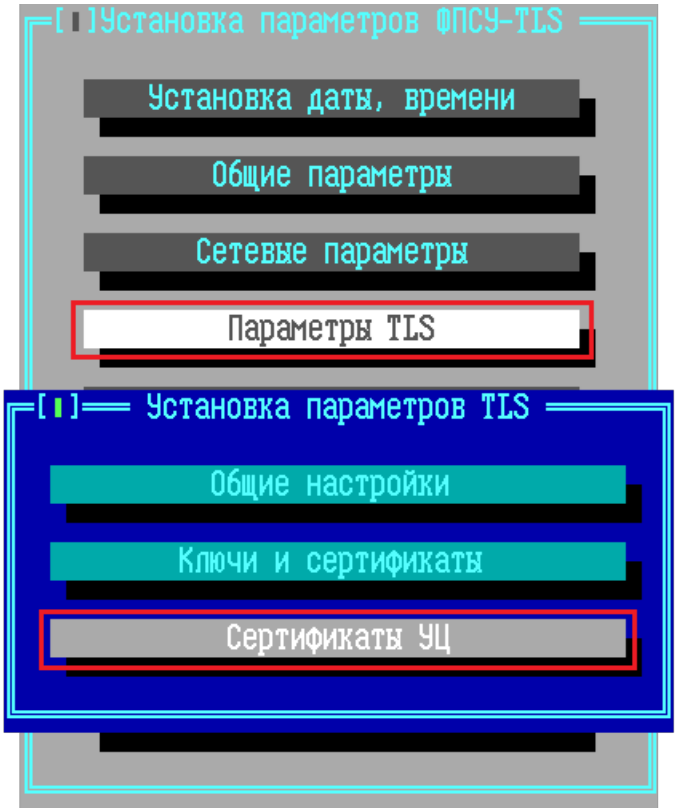


Рисунок 54 - Меню ФПСУ-TLS

На ФПСУ-TLS предустановлен собственный сертификат администратора «Administrator AMICON FPSU-TLS», выделен синим фоном, отображается всегда в первой строке окна «Просмотр сертификатов».

В списке сертификатов собственный сертификат администратора ФПСУ-TLS выделен зеленым фоном.

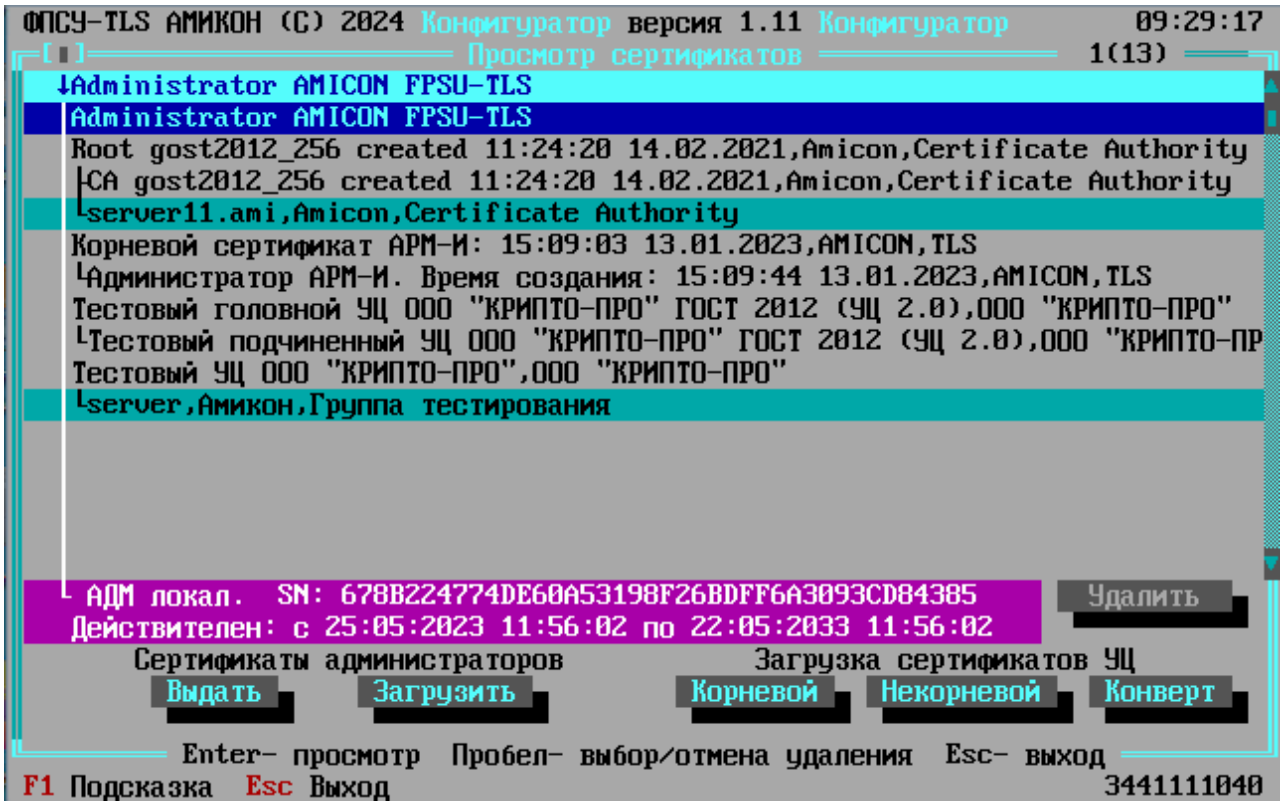


Рисунок 55 - Окно «Просмотр сертификатов»

В области «Сертификаты администраторов» находятся команды, предназначенные для управления сертификатами администраторов ФПСУ-TLS:

Выдать – выдача файла сертификата администратора данного ФПСУ-TLS на внешний носитель. Для выдачи сертификата администратора на внешний носитель требуется подключить USB-носитель и выбрать каталог для сохранения файла сертификата администратора;

Загрузить – загрузка на ФПСУ-TLS файла сертификата администратора другого ФПСУ-TLS из кластера.

Для загрузки сертификата администратора с внешнего носителя требуется подключить USB-носитель. В окне выбора каталога и файла выберите файл сертификата администратора ФПСУ-TLS.

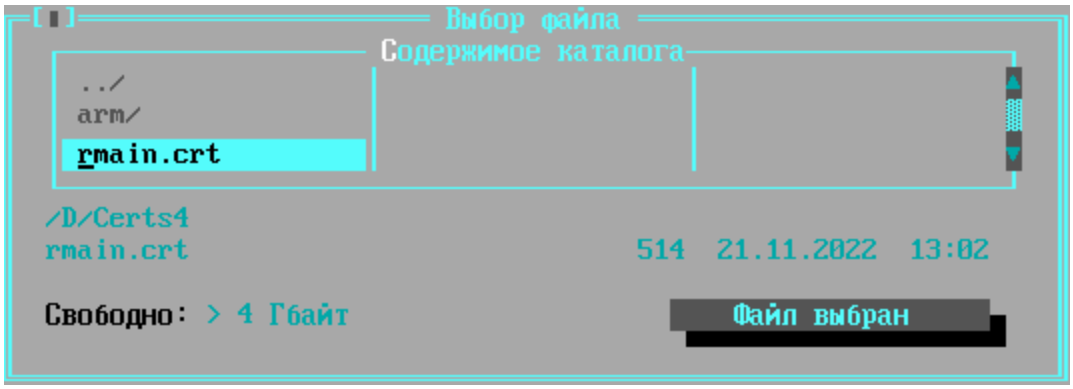


Рисунок 56 - Выбор файла с сертификатом администратора ФПСУ-TLS

Подтвердите загрузку по кнопке «Принять сертификат».

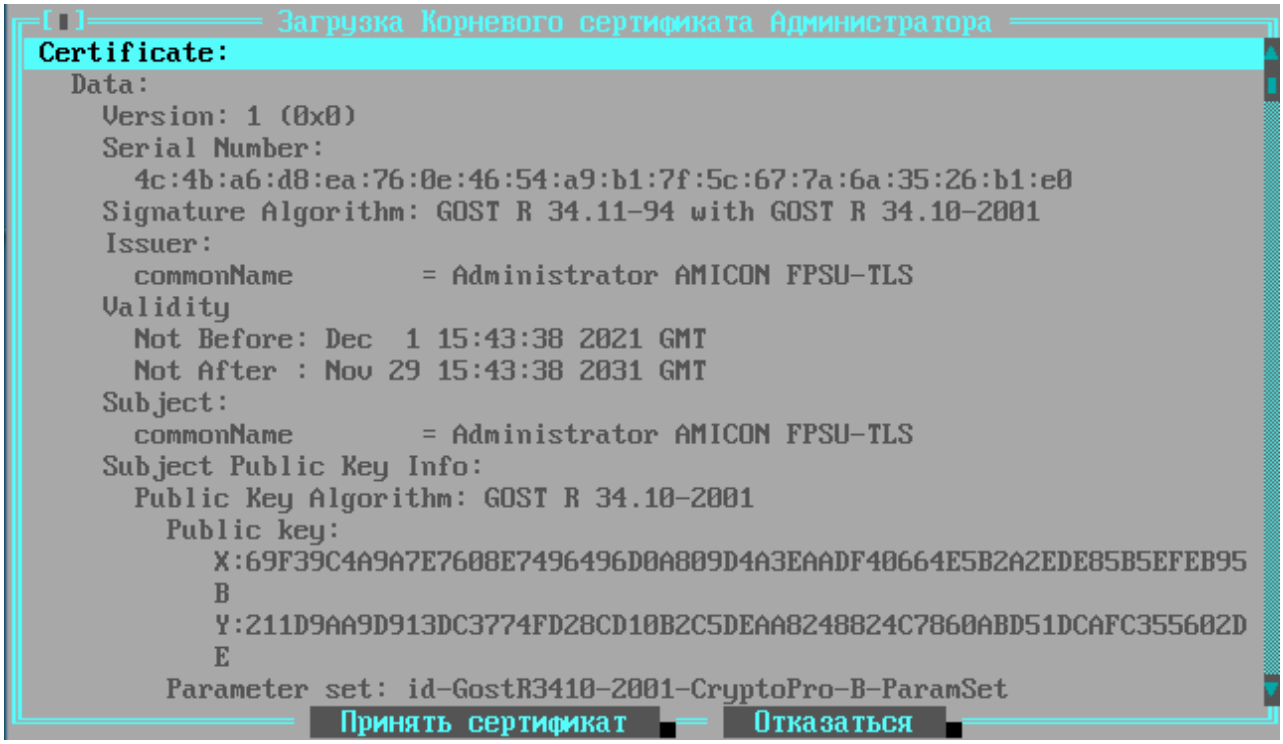


Рисунок 57 - Загрузка сертификата администратора на ФПСУ-TLS

В списке сертификатов отобразится загруженный сертификат администратора. Сертификаты администраторов не отличаются наименованием, идентифицируются серийным номером.

5. 7. 3. Установка списка отозванных сертификатов

Для установки списка отозванных сертификатов (СОС) и настройки параметров работы с ними, выполните команду «Параметры TLS → Ключи и Сертификаты» меню установки параметров ФПСУ-TLS.

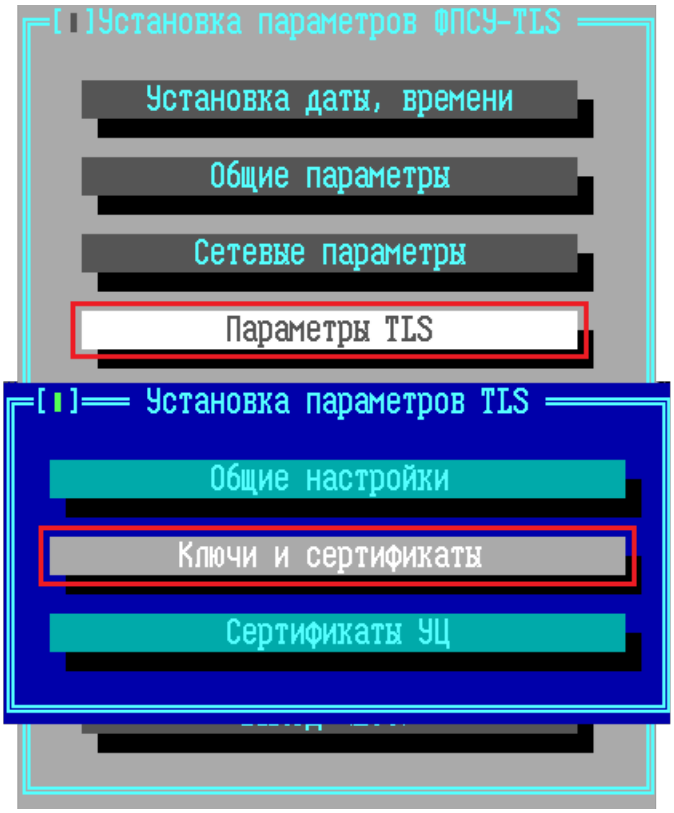


Рисунок 58 - Меню установки параметров ФПСУ-TLS

В открывшемся окне «Параметры аутентификации, ключи, сертификаты» нажмите кнопку ***«СОС»***:

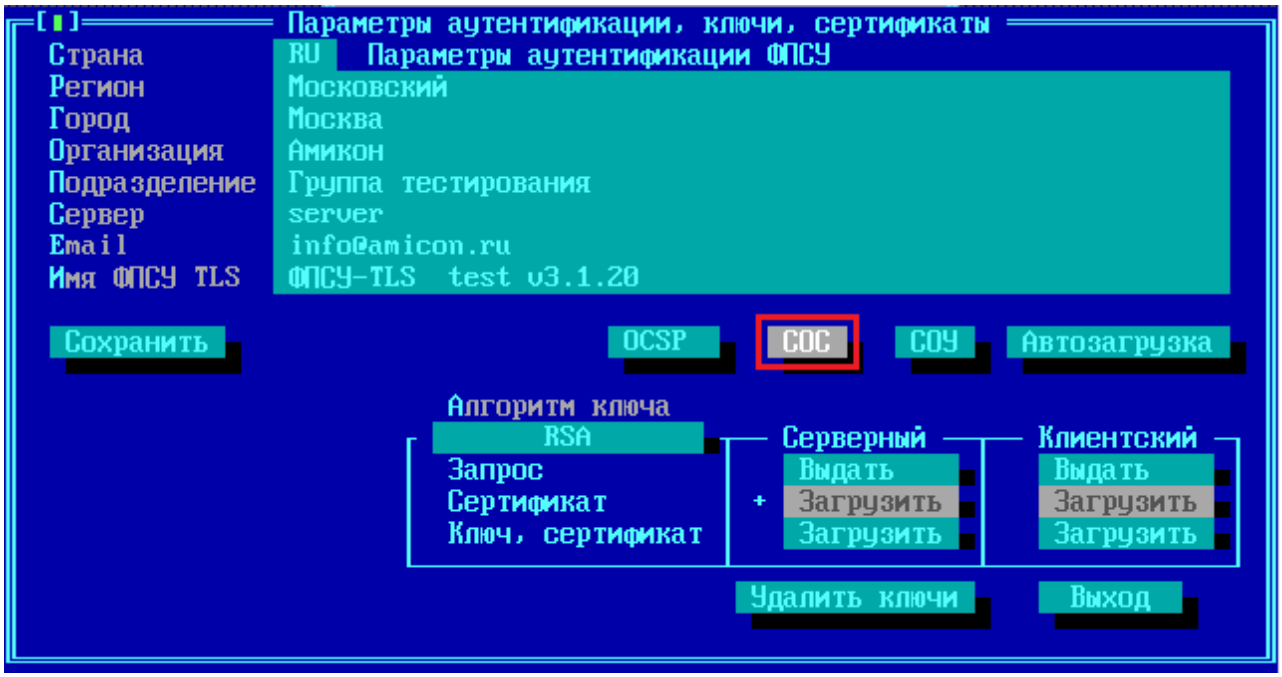


Рисунок 59 - Вызов окна списка отозванных сертификатов

Откроется окно, содержащее список установленных файлов со списками отозванных сертификатов (по умолчанию пустой).

Рисунок 60 - Файлы списков отозванных сертификатов

Для загрузки списка отозванных сертификатов, хранящегося в файле на внешнем носителе, нажмите кнопку ***«Загрузить с USB диска»***. Интерфейс выдаст приглашение подключить USB-носитель, на котором расположен файл со списками отозванных сертификатов. Подключите USB-носитель, на котором находится корневой сертификат удостоверяющего центра, к ФПСУ-TLS, и нажмите кнопку «ОК».

В открывшемся окне выбора каталога и файла, установите курсор на файле, в котором находится один из списков отозванных сертификатов, и нажмите на кнопку «Файл выбран». Если файлов со списком отозванных сертификатов несколько, процедуру загрузки, вызываемой по кнопке «Загрузить с USB диска», потребуется повторить для каждого такого файла отдельно.

Файлы COC могут быть автоматически загружены с доверенного веб-сервера, подробнее см. пункт «Автозагрузка COC, сертификатов и конфигураций ФПСУ-TLS».

После загрузки на ФПСУ-TLS файла COC, в окне списка появится новая запись, содержащая информацию о загруженном списке отозванных сертификатов:

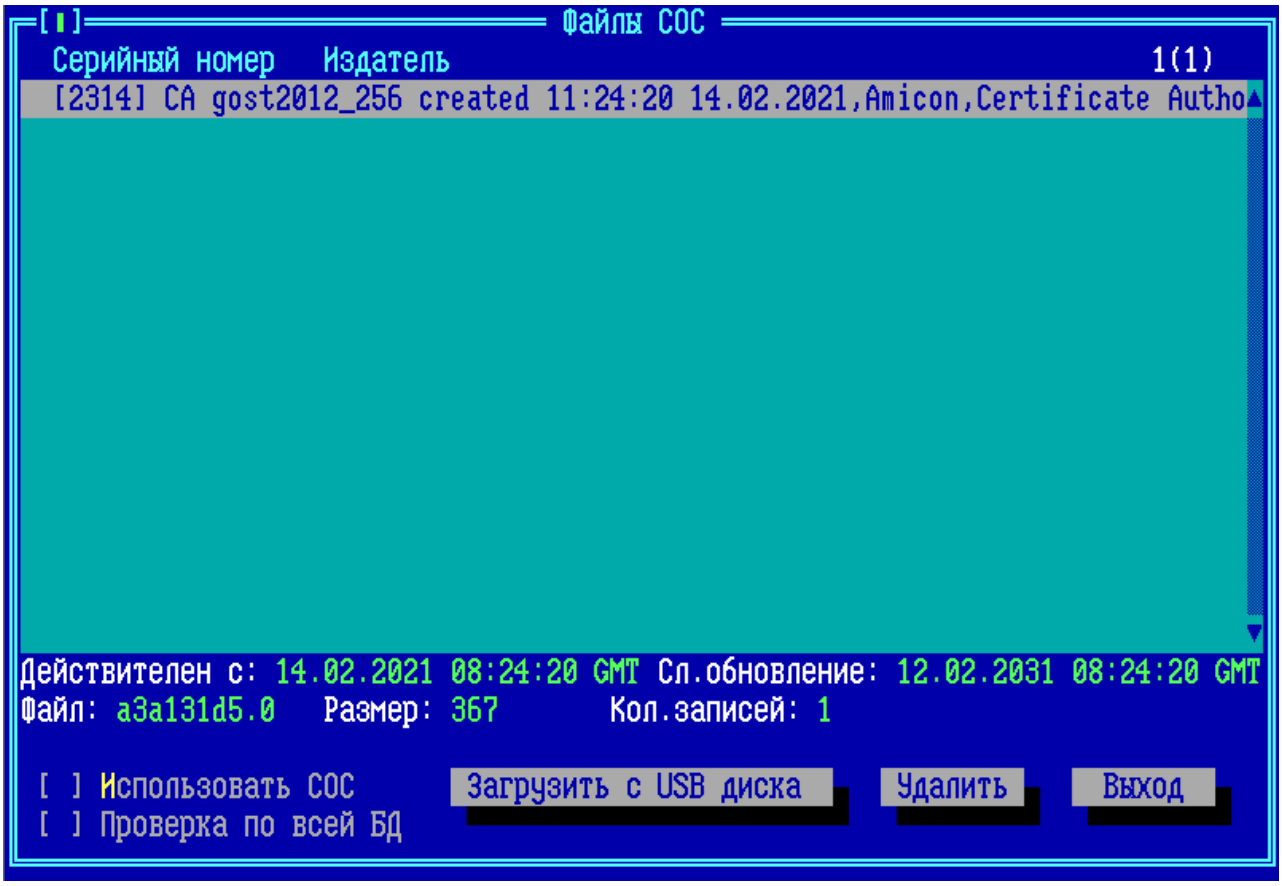


Рисунок 61 - Окно списка отозванных сертификатов

В окне списка содержится информация о серийном номере списка отозванных сертификатов, и его издателе.

Флаг ***«Использовать COC»*** задействует проверку используемых на ФПСУ-TLS сертификатов со списками отозванных сертификатов. Если флаг не установлен, проверка проводиться не будет.

ОБРАТИТЕ ВНИМАНИЕ! ФПСУ-TLS может выполнять проверку только по тем спискам отозванных сертификатов, которые подписаны теми УЦ, корневые сертификаты которых были ранее загружены на ФПСУ-TLS! Надпись в окне файлов COC «Внимание: этот COC не задействован, т.к. нет сертификата издателя» означает, что по выбранному курсором списку проверка проводиться не будет.

Установленный флаг ***«Проверка по всей БД»*** включает проверку сертификата не только по выданному его УЦ файлу COC, но и по спискам, выданным другими УЦ.

Для удаления записи об отозванном сертификате выделите строку и нажмите кнопку ***«Удалить»***.

Для возврата в окно «Параметры аутентификации, ключи, сертификаты» нажмите кнопку ***«Выход»***.

5. 7. 4. Установка списка отозванных устройств

Для установки списка отозванных устройств (СОУ) и настройки параметров работы с ними, выполните команду «Параметры TLS → Ключи и Сертификаты» меню установки параметров ФПСУ-TLS.

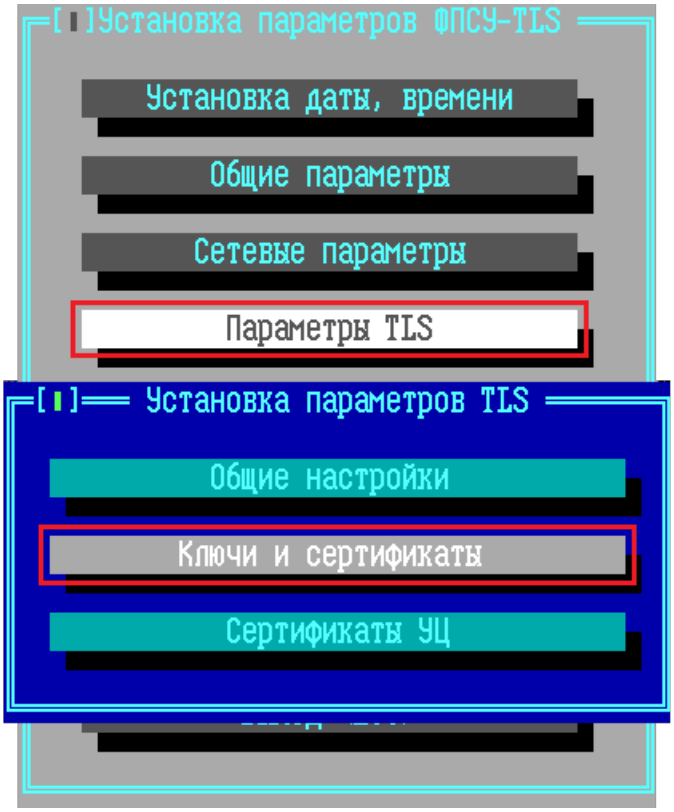


Рисунок 62 - Меню установки параметров ФПСУ-TLS

В открывшемся окне «Параметры аутентификации, ключи, сертификаты» нажмите кнопку ***«СОУ»***:

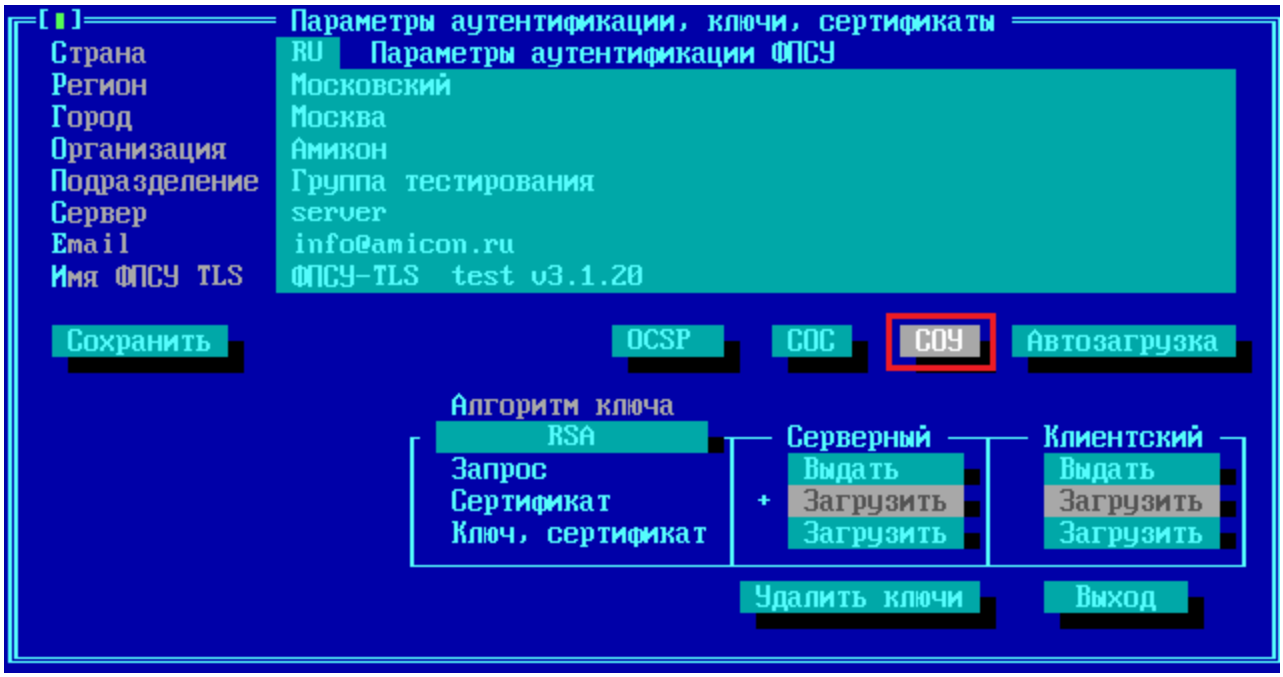


Рисунок 63 - Вызов окна списка отозванных устройств

Откроется окно, содержащее список отозванных устройств (по умолчанию пустой).

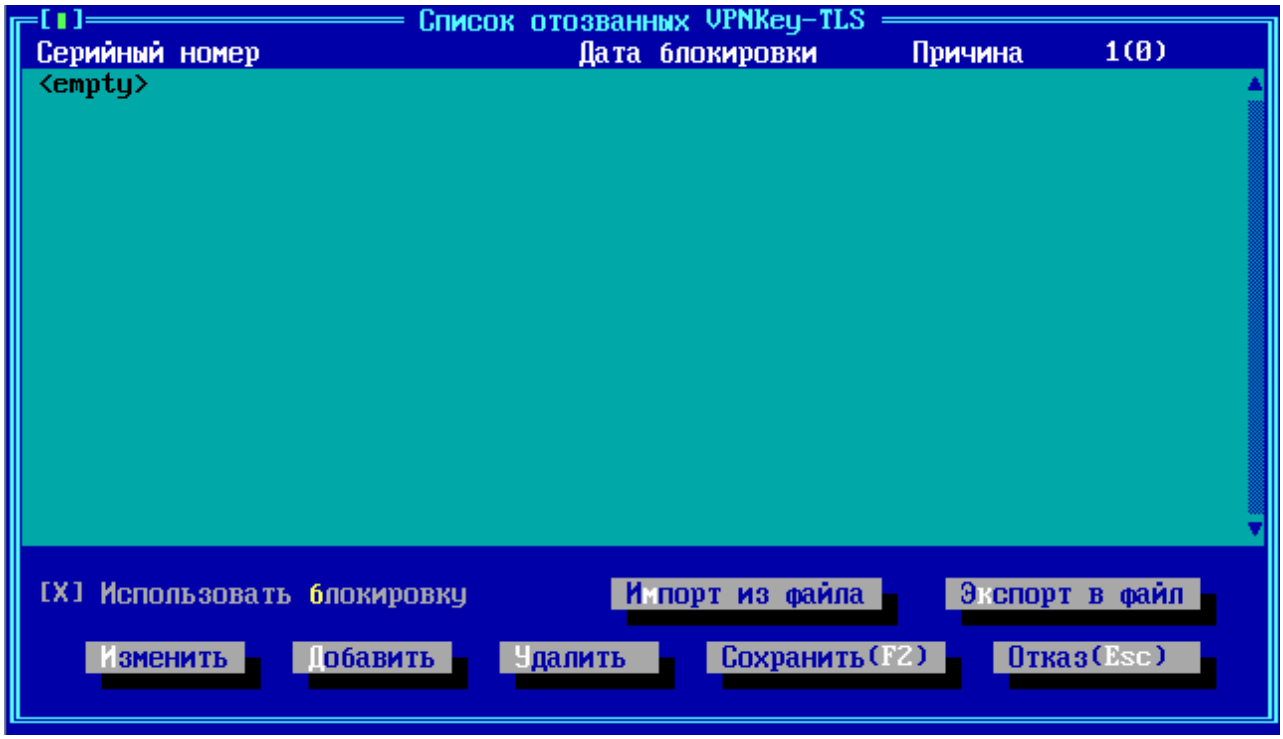


Рисунок 64 - Список отозванных устройств

Для добавления отозванного устройства VPN-Key TLS в список нажмите кнопку ***«Добавить»***. В открывшемся окне необходимо ввести серийный номер устройства VPN-Key

TLS, причину и дату блокировки.

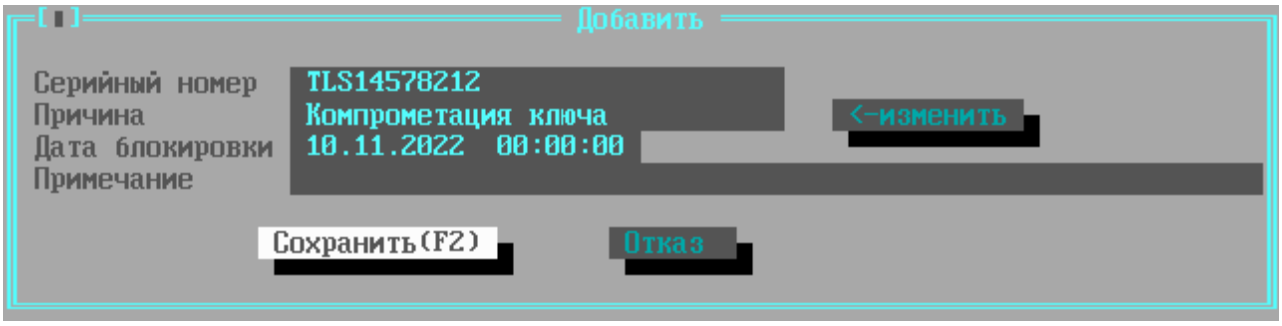


Рисунок 65 - Добавление в список отозванного устройства VPN-Key TLS

Для возврата в окно со списком отозванных устройств с внесением выполненных изменений, выполните команду ***«Сохранить»***.

В окне списка отозванных устройств содержится информация о серийном номере отозванного устройства, дате и причине блокировки.

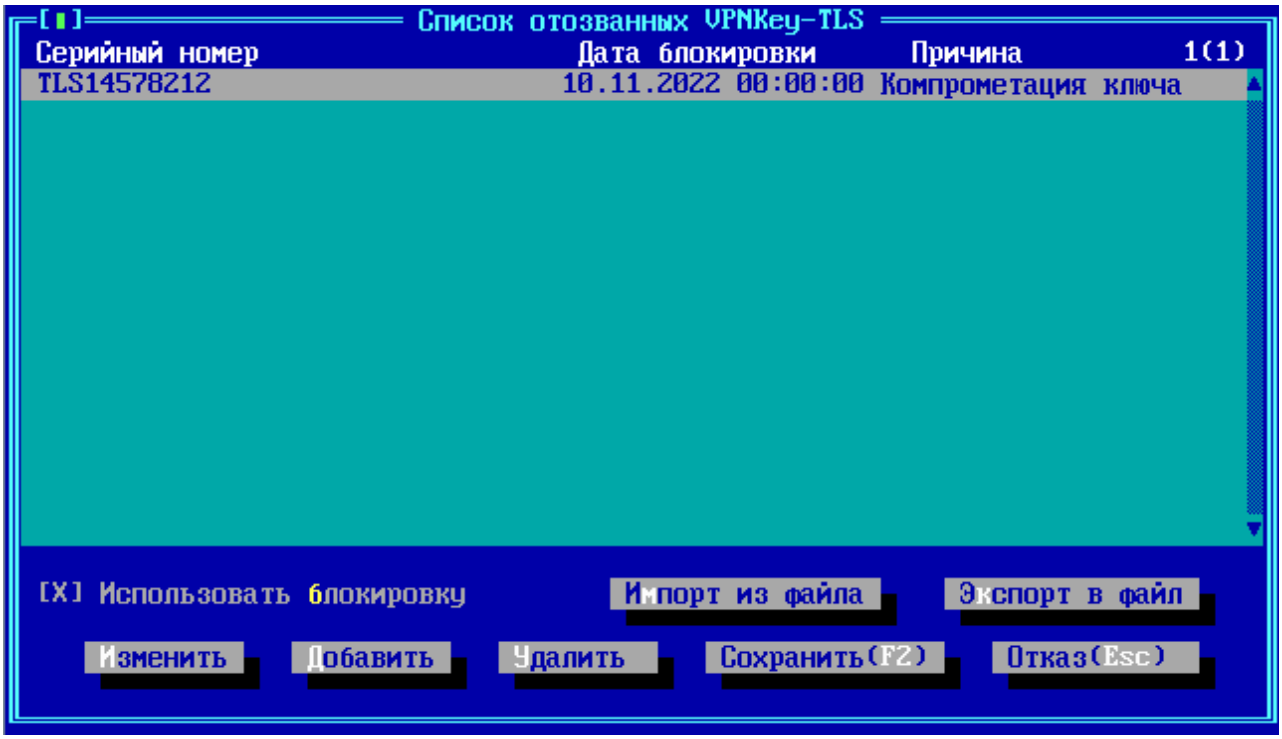


Рисунок 66 - Окно списка отозванных устройств

Внести изменения в запись об отозванном устройстве VPN-Key TLS можно по кнопке ***«Изменить»***.

Для удаления записи об отозванном устройстве выделите строку с серийным номером и нажмите кнопку ***«Удалить»***.

Для загрузки списка отозванных устройств, хранящегося в файле на внешнем носителе, нажмите кнопку ***«Импорт из файла»***. Интерфейс выдаст приглашение подключить USB-носитель, на котором расположен файл со списком отозванных устройств. Подключите USB-носитель, на котором находится файл со списком отозванных устройств, к ФПСУ-TLS, и нажмите кнопку «ОК». В открывшемся окне выбора каталога и файла, установите курсор на файле, в котором находится один из списков отозванных устройств, и нажмите на кнопку «Файл выбран». Если файлов со списком отозванных устройств несколько, процедуру загрузки, вызываемой по кнопке «Импорт из файла», потребуется повторить для каждого такого файла отдельно.

После загрузки на ФПСУ-TLS файла СОУ, в окне списка появится новая запись, содержащая информацию о загруженном списке отозванных устройств.

СОУ может быть экспортирован на внешний носитель. Экспорт осуществляется по нажатию кнопки ***«Экспорт в файл»***. Система предложит подключить к ФПСУ-TLS внешний носитель. В открывшемся окне выберите каталог для сохранения СОУ и нажмите «Каталог выбран». Будет выдано сообщение о выгрузке СОУ в файл.

Флаг ***«Использовать блокировку»*** задействует проверку используемых на ФПСУ-TLS устройств VPN-Key TLS и блокирует отозванные. Если флаг не установлен, проверка проводиться не будет.

Для возврата в окно «Параметры аутентификации, ключи, сертификаты» нажмите кнопку ***«Отказ»*** или клавишу <Esc>.

5. 7. 5. Установка личных сертификатов ФПСУ-TLS

Для перехода в интерфейс управления личными сертификатами ФПСУ-TLS, выполните команду «Параметры TLS → Ключи и Сертификаты» меню установки параметров ФПСУ-TLS.

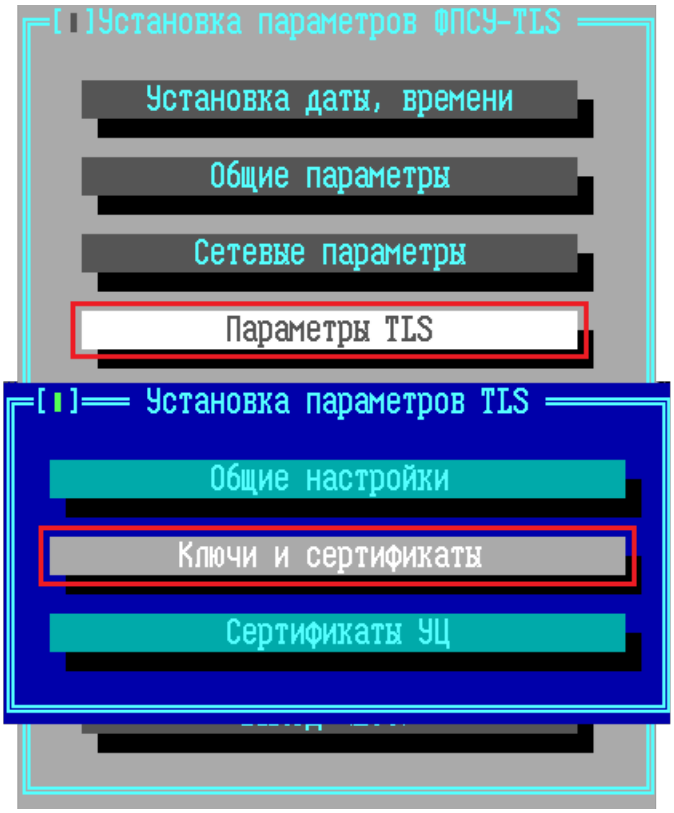


Рисунок 67 - Меню установки параметров ФПСУ-TLS

Окно установки и управления личными сертификатами ФПСУ-TLS и списком отозванных сертификатов, «Параметры аутентификации, ключи, сертификаты», содержит следующие информационные и управляющие поля:

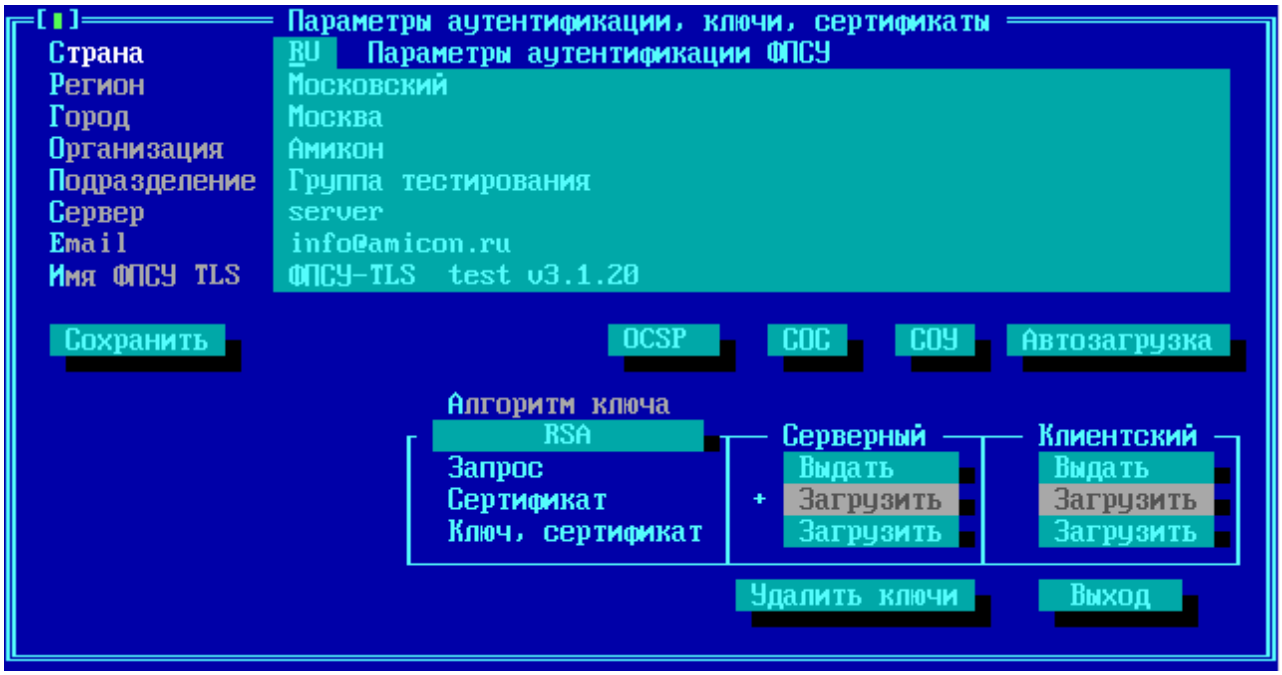


Рисунок 68 - Параметры аутентификации, ключи, сертификаты

Параметры аутентификации ФПСУ – здесь указываются параметры ФПСУ-TLS, которые будут подтверждаться личными сертификатами сервера и клиента, выданными для данного ФПСУ-TLS Удостоверяющим Центром, при установлении TLS-соединений.

Сохранить – сохранение изменений, внесенных в поле «Параметры аутентификации ФПСУ» для последующей генерации запроса к УЦ на выдачу сертификата.

Автозагрузка – переход в окно настроек автоматической установки на ФПСУ-TLS личных сертификатов и списков отозванных сертификатов (подробнее см. пункт «Автозагрузка СОС, сертификатов и конфигураций ФПСУ-TLS»).

Ключи и сертификаты ФПСУ – в этой области находятся команды управления секретными ключами ФПСУ-TLS и соответствующих им сертификатов X.509:

- ***Алгоритм ключа*** – создание секретного ключа ФПСУ-TLS по задаваемому криптографическому алгоритму для личного сертификата ФПСУ-TLS, указанного в поле «Параметры аутентификации ФПСУ». Могут быть выбраны алгоритмы RSA* или ГОСТ.

  ГОСТ – применен алгоритм открытого ключа ГОСТ Р 34.10-2012 для ключей длины 256 бит или 512 бит (подпись сертификата с хешированием ГОСТ 34.11-2012).

  RSA – применен алгоритм открытого ключа RSA* (подпись сертификата с хэшированием SHA256);

**Примечание: использование алгоритмов RSA для защиты информации конфиденциального характера запрещается в случаях, определенных пунктом 3 Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.*

- ***Запрос*** – запрос на сертификат, выдача на внешний USB-носитель запроса к удостоверяющему центру, созданного на основе секретного ключа, для заверения. После заверения удостоверяющим центром запроса на сертификат будет выпущен личный сертификат ФПСУ-TLS, который может быть загружен с USB-носителя с помощью опций «Сертификат» и «Ключ, сертификат»;
- ***Сертификат*** – установка с внешнего USB-носителя заверенного удостоверяющим центром личного сертификата ФПСУ-TLS;
- ***Ключ, сертификат*** – установка с внешнего USB-носителя секретного ключа ФПСУ-TLS и заверенного удостоверяющим центром личного сертификата ФПСУ-TLS.

Серверный комплект сертификатов используется в защищенных соединениях, когда ФПСУ-TLS выступает в роли TLS-сервера (основной режим).

Клиентский комплект сертификатов используется в защищенных соединениях, когда ФПСУ-TLS выступает в роли TLS-клиента (например, в режиме «шлюз TLS-TLS»).

Для использования ФПСУ-TLS в качестве TLS-сервера, необходимо загрузить на него выданный УЦ личный серверный сертификат.

Для загрузки сертификата или комплекта с секретным ключом и сертификатом, выполните соответствующую команду меню загрузки, после чего ФПСУ-TLS выдаст служебное приглашение на подключение USB-носителя к ФПСУ-TLS:

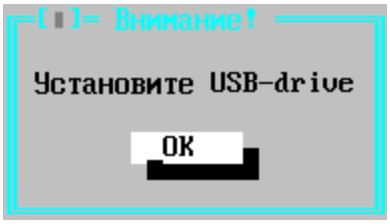


Рисунок 69 - Подключите USB-носитель

Подключите к ФПСУ-TLS внешний носитель с файлом сертификата, и нажмите кнопку «ОК». На экран будет выведено окно диалога выбора каталога и файла, в котором находится сертификат. Отметьте курсором файл с сертификатом, и выполните команду «Файл выбран».

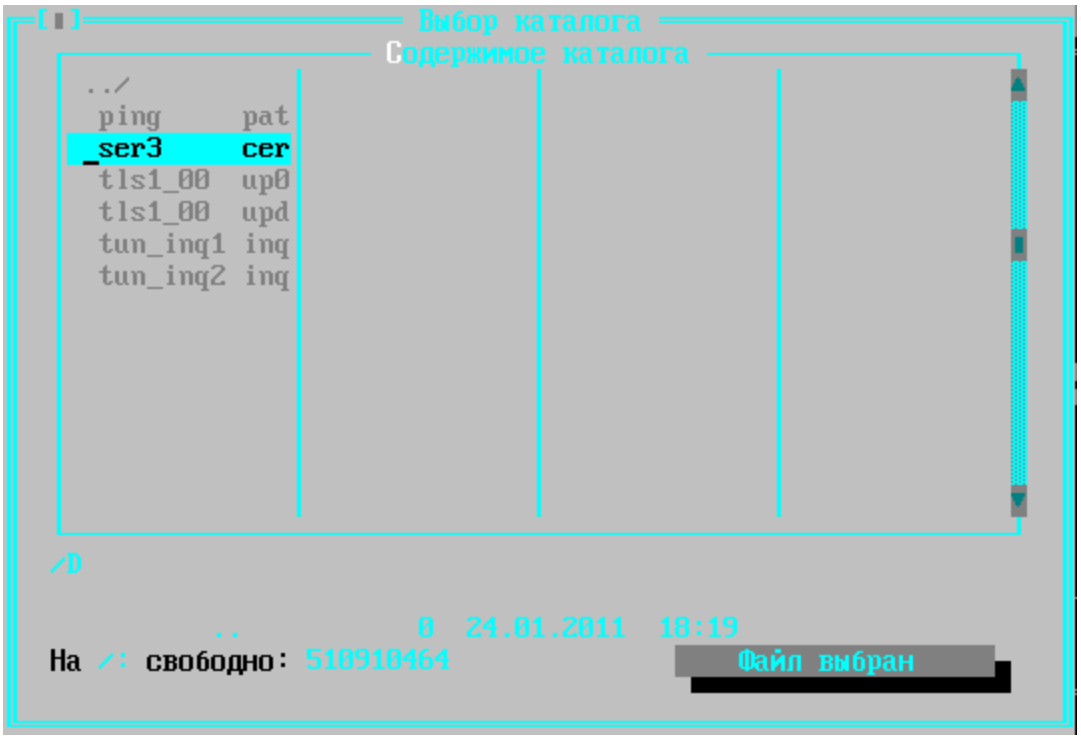


Рисунок 70 - Окно диалога выбора файла

После выполнения команды «Файл выбран», находящийся в нём сертификат (или секретный ключ) будет выведен на экран для ознакомления.

Нажмите кнопку ***«Принять сертификат»*** для его установки в качестве сертификата ФПСУ-TLS, или ***«Отказаться»*** для отмены операции.

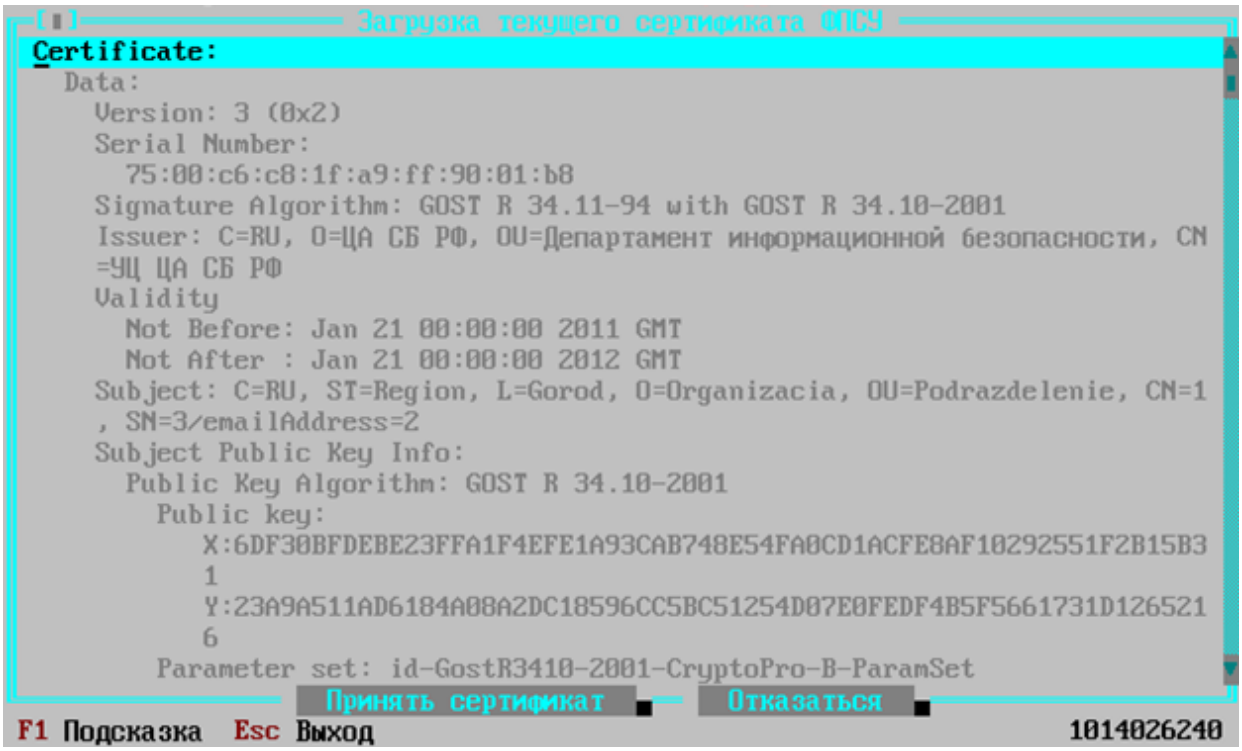


Рисунок 71 - Просмотр устанавливаемого сертификата

Удалить ключи – команда удаления всей ключевой информации с жесткого диска ФПСУ-TLS. Удаляются все секретные ключи и личные сертификаты ФПСУ-TLS.

Выход – возврат в меню настройки ФПСУ-TLS.

5. 7. 6. Автозагрузка СОС, сертификатов и конфигураций ФПСУ-TLS

Используемые на ФПСУ-TLS сертификаты и список отозванных сертификатов могут быть установлены в автоматическом режиме, с указанного администратором ФПСУ-TLS http-сервера.

Для перехода в интерфейс управления автоматическими загрузками, сначала выполните команду «Параметры TLS → Ключи и Сертификаты» меню установки параметров ФПСУ-TLS:

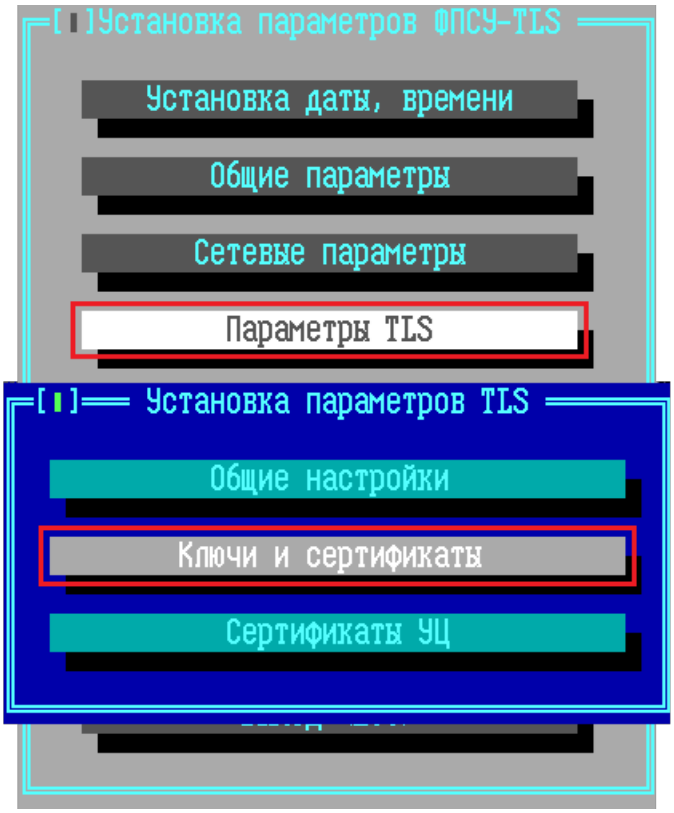


Рисунок 72 - Меню установки параметров ФПСУ-TLS

В открывшемся окне, «Параметры аутентификации, ключи, сертификаты», выполните команду «Автозагрузка»:

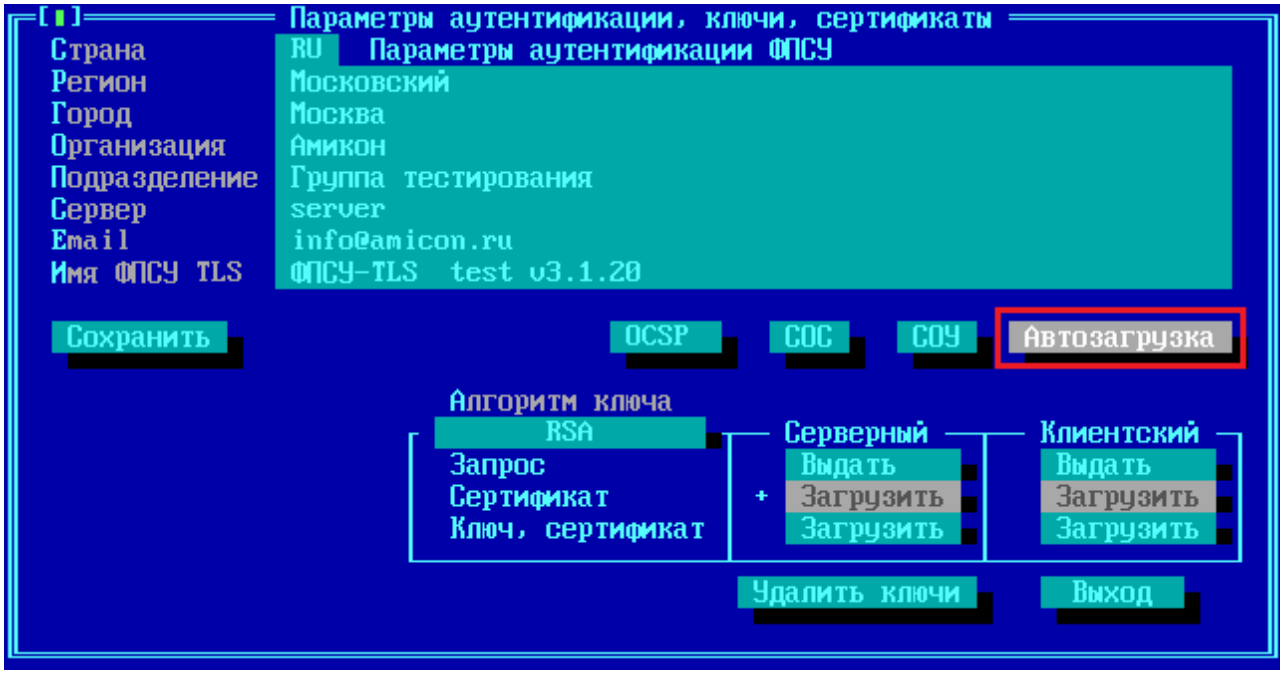


Рисунок 73 - Вызов окна автозагрузки сертификатов

Откроется окно «Автозагрузка СОС, контейнеров сертификатов», в котором можно настроить параметры автозагрузки. Общие параметры автозагрузки:

- ***Время обновления*** – суточное время на ФПСУ-TLS, в которое будет отправлен запрос на указанный сервер;
- ***Интервал обновления*** – временной промежуток, через который будет отправлен повторный запрос.

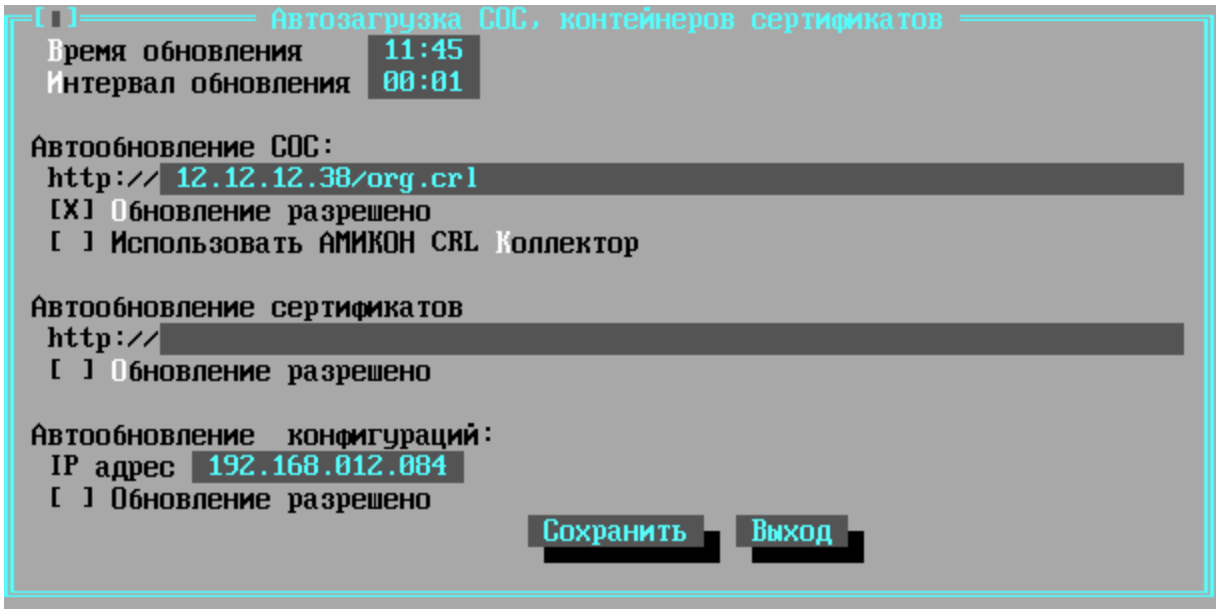


Рисунок 74 - Окно управления автоматической загрузкой

Для включения автоматической загрузки файлов со списками отозванных сертификатов укажите в разделе «Автообновление СОС» следующие параметры:

- ***http://*** – адрес источника СОС, адрес http-сервера и месторасположение файла со списком отозванных сертификатов на указанном сервере или сетевой адрес АМИКОН CRL Коллектора. Если в качестве источника списков отозванных сертификатов используется не веб-сервер, а сетевой АМИКОН CRL Коллектор (для этого требуется установить флаг «Использовать АМИКОН CRL Коллектор»), то в поле адрес требуется указать только адрес коллектора, без указания файла;
- ***Использовать АМИКОН CRL Коллектор*** – установленный флаг означает, что в качестве адреса источника СОС задан сетевой адрес АМИКОН CRL Коллектора;
- ***Обновление разрешено*** – установленный флаг, включает автообновление из указанного источника с заданной интервалом.

В окне «Автозагрузка СОС, контейнеров сертификатов» в разделе «Автообновление сертификатов» выполняется настройка параметров загрузки списка сертификатов

(контейнера сертификатов) с http-сервера. Таким образом могут быть загружены только обычные (некорневые) сертификаты удостоверяющего центра. Корневые сертификаты удостоверяющих центров могут быть установлены только вручную администратором с внешнего носителя (см. пункт «Установка сертификатов удостоверяющих центров»).

Для настройки загрузки контейнера сертификатов с http-сервера требуется указать в разделе «Автообновление сертификатов» следующие параметры:

- Адрес источника, адрес http-сервера и месторасположение файла со списком сертификатов на указанном сервере;
- Установить флаг «Обновление разрешено».

В разделе «Автообновление конфигураций», администратор ФПСУ-TLS может задействовать режим копирования конфигурации ФПСУ-TLS с другого ФПСУ-TLS. Администратор другого ФПСУ-TLS должен предварительно отметить доступные к такой удаленной загрузке конфигурации (подробнее см. пункт «Менеджер конфигураций»).

Для настройки автоматической загрузки конфигурации с другого ФПСУ-TLS, требуется указать следующие параметры:

- IP-адрес, один из сетевых адресов другого ФПСУ-TLS, на который будет отправлять запрос о наличии новой версии конфигурации;
- Установить флаг «Обновление разрешено».

Для выхода из окна «Автозагрузка СОС, контейнеров сертификатов» и возвращению к окну настроек сертификатов, с сохранением внесенных изменений в конфигурацию ФПСУ-TLS, нажмите кнопку ***«Сохранить»***.

По нажатию кнопки ***«Выход»*** осуществляется возврат к окну настроек сертификатов без сохранения выполненных изменений.

5. 7. 7. Протокол состояния сетевого сертификата OCSP

OCSP (Online Certificate Status Protocol) – протокол о статусе онлайн-сертификата, регламентированный стандартом RFC 6960, позволяет ФПСУ-TLS определять состояние (отзыв) сертификата TLS-клиента или сертификата сервера, получая ответ о состоянии сертификата от OCSP ответчика.

ФПСУ-TLS при установлении соединения с TLS-клиентом или сервером отправляет запрос о состоянии (отзыве) сертификата OCSP ответчику. В случае положительного ответа от OCSP ответчика, сертификат исправен или проверен, устанавливается TLS-соединение

между TLS-клиентом и ФПСУ-TLS или HTTPS сервером и ФПСУ-TLS.

Предварительно на ФПСУ-TLS должны быть установлены собственный сертификат и корневой сертификат УЦ, которым подписан собственный сертификат ФПСУ-TLS, на TLS-клиенте должны быть установлены клиентский личный сертификат и корневой сертификат УЦ, которым подписан личный сертификат клиента.

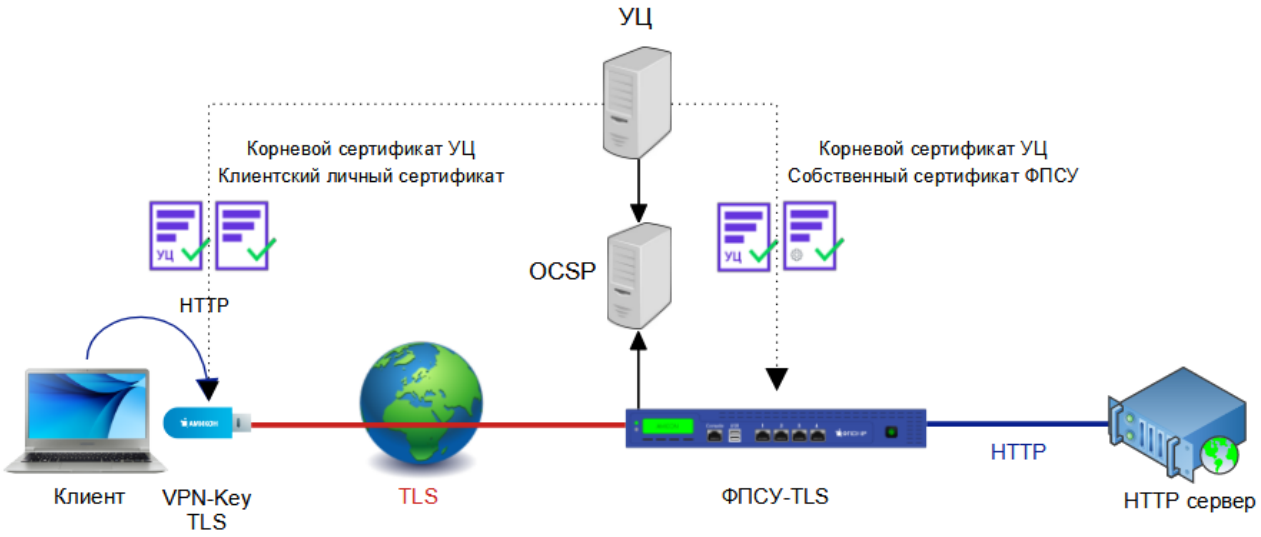


Рисунок 75 - Схема взаимодействия ФПСУ-TLS с OCSP

Для перехода в интерфейс управления OCSP, выполните команду «Параметры TLS → Ключи и Сертификаты» меню установки параметров ФПСУ-TLS.

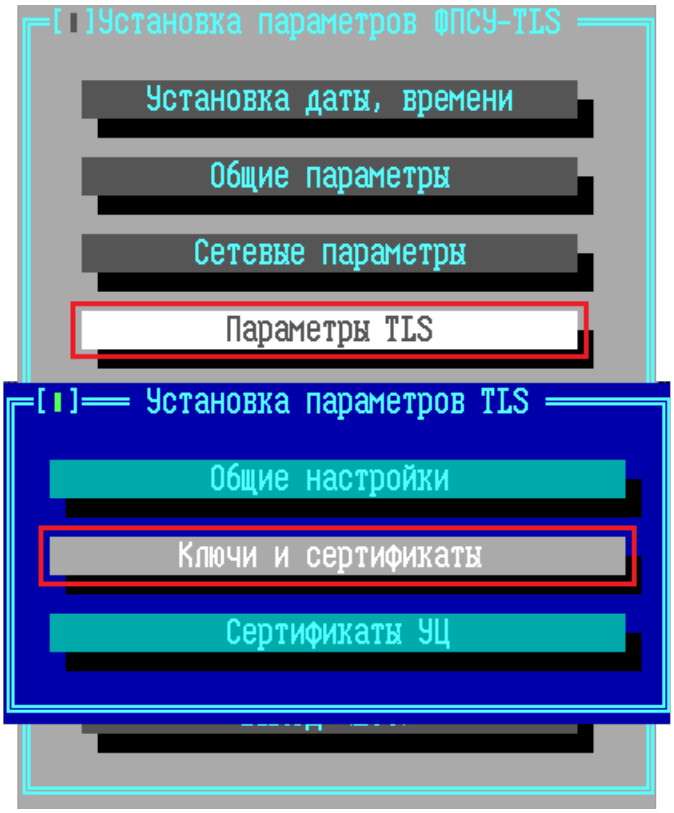


Рисунок 76 - Меню установки параметров ФПСУ-TLS

В открывшемся окне, «Параметры аутентификации, ключи, сертификаты», выполните команду «OCSP»:

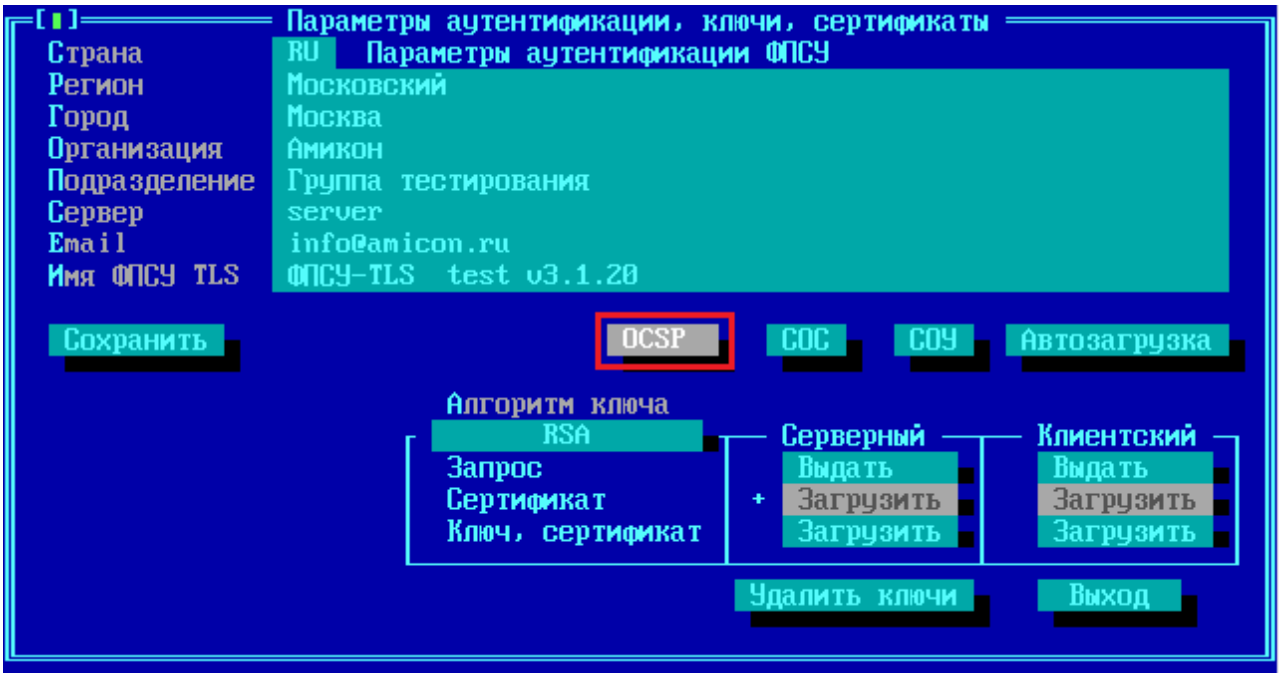


Рисунок 77 - Параметры аутентификации, ключи, сертификаты

Откроется окно «Настройка OCSP», в котором можно настроить следующие параметры:

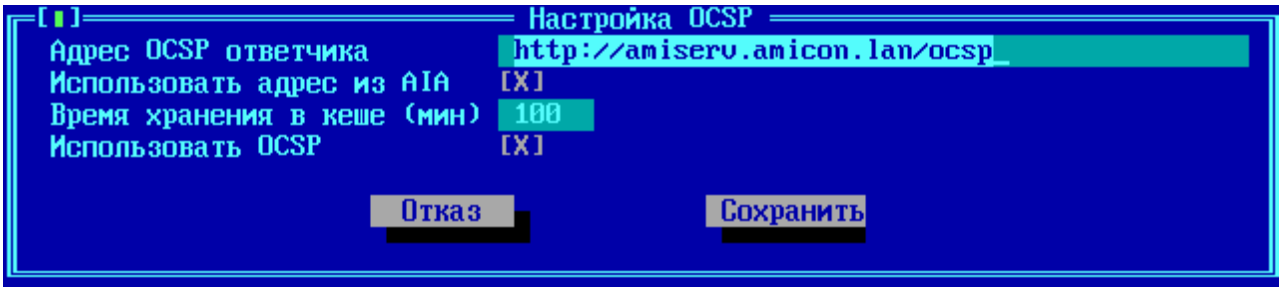


Рисунок 78 - Параметры аутентификации, ключи, сертификаты

Адрес OCSP ответчика – указывается URL-адрес или IP-адрес OCSP ответчика. Если порт ответчика отличен от порта по умолчанию, 80, то указывается дополнительно порт.

Использовать адрес из AIA – AIA (Authority Information Access) расширение сертификата, где указывается адрес ответчика OCSP для проверки этого сертификата. При включении флага проверяется отзыв сертификата по AIA. Если адрес OCSP ответчика задан, сначала отзыв проверяется по указанному адресу, затем в случае, если OCSP ответчик не отвечает, проверяется по AIA.

Время хранения в кеше (мин) – ответ, полученный от OCSP ответчика, ФПСУ-TLS хранит в кеше указанное время.

Использовать OCSP – установленный флаг включает проверку отзыва сертификатов на OCSP ответчике.

5. 8. Запуск ФПСУ-TLS в рабочий режим

После выполнения первоначальных настроек, ФПСУ-TLS можно переводить в рабочий режим обслуживания http-серверов.

Перевод в рабочий режим защиты http-трафика осуществляется выполнением команды «Запуск ФПСУ» главного меню ФПСУ-TLS:

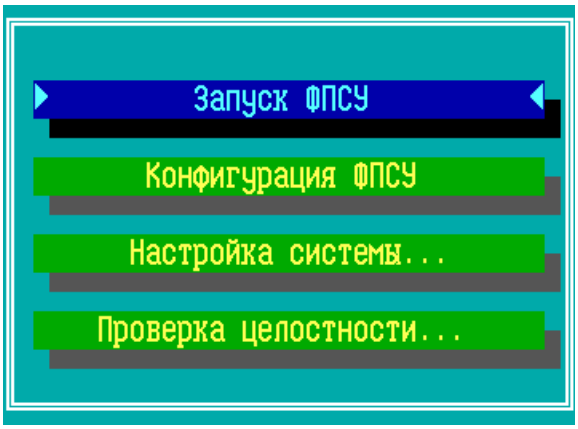


Рисунок 79 - Главное меню ФПСУ-TLS

Помимо обязательных настроек, на ФПСУ-TLS реализован ряд дополнительных возможностей, описание которых находится в пунктах:

- «Экраны состояния рабочего режима»,
- «Менеджер конфигураций»,
- «Режимы взаимодействия ФПСУ-TLS и защищаемой службы»,
- «Масштабирование»,
- «Общие параметры конфигурации ФПСУ-TLS»,
- «SNMP-клиент»,
- «Syslog-клиент»,
- «Дата и время ФПСУ-TLS»,
- «Просмотр установленных сертификатов»,
- «Параметры защиты ФПСУ-TLS».

6. Контроль целостности программного обеспечения

ФПСУ-TLS содержит ряд механизмов, обеспечивающих защиту программных модулей от НСД, в частности, автоматический контроль целостности информации на жестком диске компьютера.

Администратор имеет возможность осуществить контроль целостности программных и информационных частей ФПСУ-TLS с использованием специальной подсистемы контроля целостности, в том числе путем сравнения с эталонными контрольными суммами, указанными в формуляре на СКЗИ, поставляемым вместе с ФПСУ-TLS.

Контрольные значения файлов (хэш-коды) рассчитываются согласно ГОСТ Р 34.11-2012.

Дополнительная проверка целостности программного обеспечения ФПСУ-TLS осуществляется из пункта «Проверка целостности» главного меню:

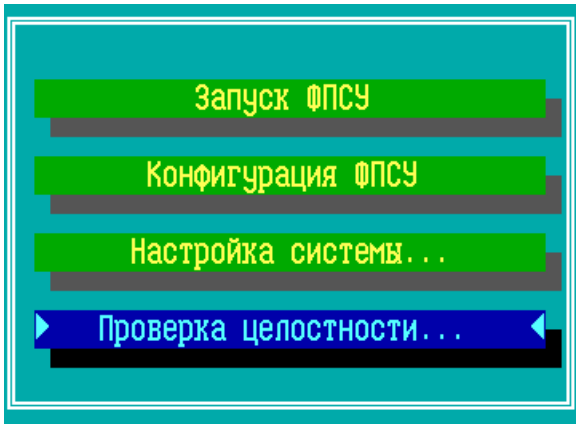


Рисунок 80 - Главное меню ФПСУ-TLS

При выполнении команды открывается дополнительное подменю, где указаны команды трех вариантов проверок.

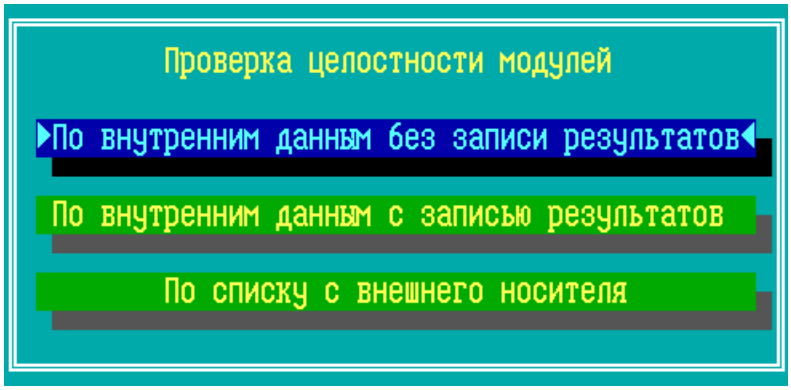


Рисунок 81 - Меню проверки целостности

При выборе пункта «По внутренним данным без записи результатов» проверка ПО ФПСУ-TLS происходит по хранящимся на ФПСУ-TLS контрольным эталонным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран. Операция доступна администраторам класса *Администратор* или *Инженер*, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

При выборе пункта «По внутренним данным с записью результатов» проверка ПО ФПСУ-TLS происходит по хранящимся на ФПСУ-TLS контрольным эталонным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран и в файл с расширением .LST на внешний носитель. Операция доступна администраторам класса *Администратор*, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

После отработки программы результаты проверки будут выданы на экран монитора и в файл FPSUHASH.LST на тот же носитель, который может быть прочитан и обработан на другом компьютере средствами текстового редактора, поддерживающим кодировку OEM/DOS.

Проверка в режиме «По списку с внешнего носителя» не является обязательной. При выборе пункта «По списку с внешнего носителя», проверка ПО ФПСУ-TLS происходит по специальному файлу-заданию с контрольными суммами, считываемого с внешнего носителя, с выводом результата проверки (успешно или обнаружена ошибка) на экран и в файл с расширением .LST на внешний носитель. Файл-задание FPSUHASH.HSH не поставляется вместе с ФПСУ-TLS и может быть получен от поставщика ФПСУ-TLS отдельно. Операция доступна администраторам класса *Администратор*, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Если в результате выполнения проверки появляется сообщение о нарушении целостности контролируемых файлов, дальнейшая эксплуатация ФПСУ-TLS не допускается. Следует проанализировать причину изменения контролируемых файлов, и затем, в случае необходимости, переустановить контролируемые файлы.

7. Эксплуатация ФПСУ-TLS

Минимальные обязательные настройки ФПСУ-TLS, позволяющие выполнять основные функции по защите http-трафика к web-серверам локальной сети, описаны в пункте «Запуск и первоначальная настройка ФПСУ-TLS». Помимо обязательных настроек, на ФПСУ-TLS реализован ряд дополнительных возможностей, описание которых находится ниже.

Переход по экранам осуществляется по нажатию комбинаций клавиш:

<Ctlr+Alt+F1> или <Alt+F1> - на экран главного меню;

<Alt+F2> - экран с утилитами для проверки настроек;

<Alt+F3> - экран текущего состояния ФПСУ-TLS рабочего режима.

7. 1. Экраны состояния рабочего режима

После запуска ФПСУ-TLS в рабочий режим защиты http-трафика (см. пункт «Запуск ФПСУ-TLS в рабочий режим»), на подсоединенном к ФПСУ-TLS мониторе можно отследить динамическую информацию о текущем состоянии сети, а также сформировать и выдать запрос к подсистеме статистики, регистрирующей происходящие на ФПСУ-TLS события.

7. 1. 1. Экран текущего состояния ФПСУ-TLS

По умолчанию, на экран выдается информативное окно текущего состояния ФПСУ-TLS, открывается по нажатию клавиш <Alt+F3>:

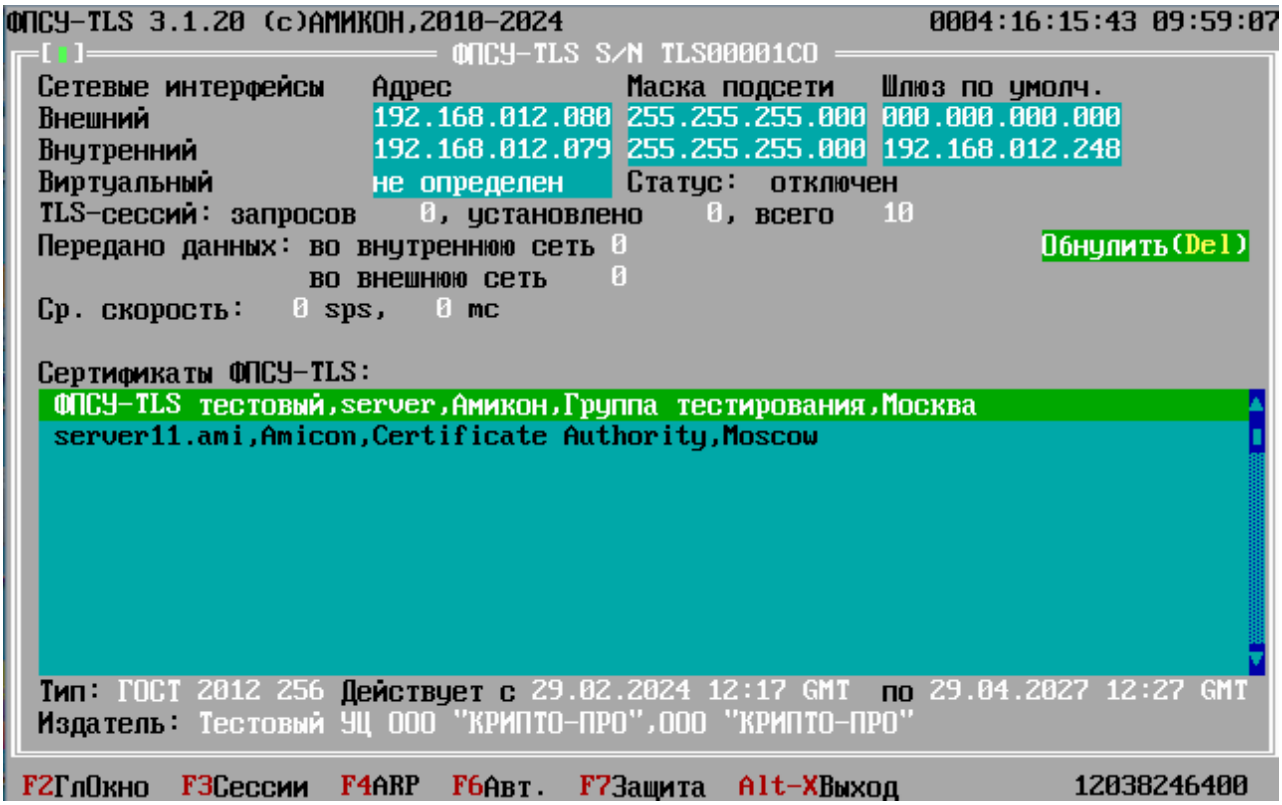


Рисунок 82 - Окно текущего состояния ФПСУ-TLS

В окне текущего состояния отображается следующая информация:

- символьное наименование ФПСУ-TLS;
- параметры аутентификации ФПСУ-TLS, указанные в личном сертификате;
- срок действия личного сертификата ФПСУ-TLS;
- информация об издателе сертификата;
- краткая конфигурация сетевых интерфейсов ФПСУ-TLS;
- число установленных в текущий момент TLS-сессий;
- общий объем принятых и переданных данных;
- кнопка «Обнулить (Del)», скидывающая значения переданных данных в ноль.

Внешний и внутренний интерфейсы настраиваются в меню конфигурации (см. пункт «Настройка сетевых параметров»), виртуальный интерфейс включается при настройке подсистемы масштабирования (см. пункт «Настройка подсистемы масштабирования»).

В ФПСУ-TLS запрещено использование просроченного секретного ключа TLS-соединения. ФПСУ-TLS выдает оповещение об истекшем сроке действия секретного ключа TLS-соединения на экране текущего состояния, при этом в окне текущих сессий отсутствуют

соединения.

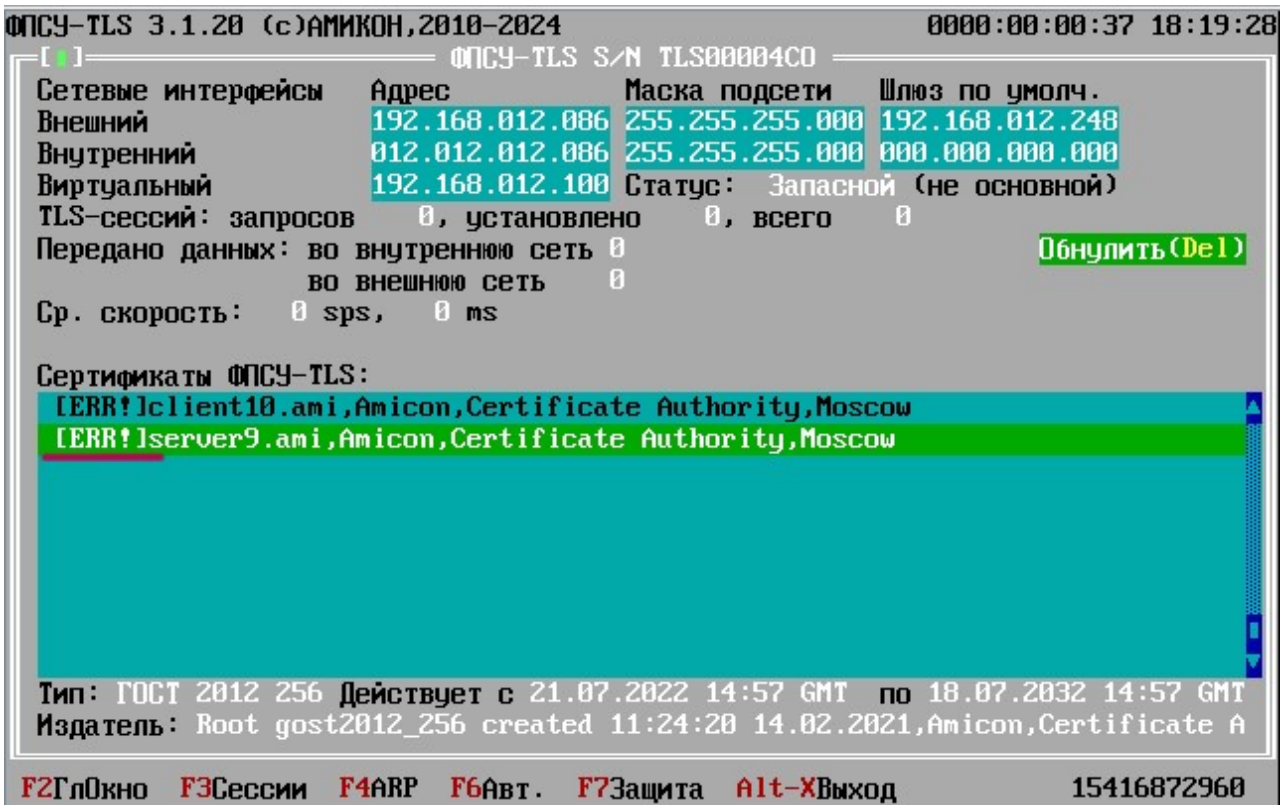


Рисунок 83 - Срок действия секретного ключа TLS-соединения истек

7. 1. 2. Текущие сессии

При нахождении ФПСУ-TLS в рабочем режиме, можно просмотреть список текущих сессий TLS-клиентов данного ФПСУ-TLS по нажатию клавиши <F3>:

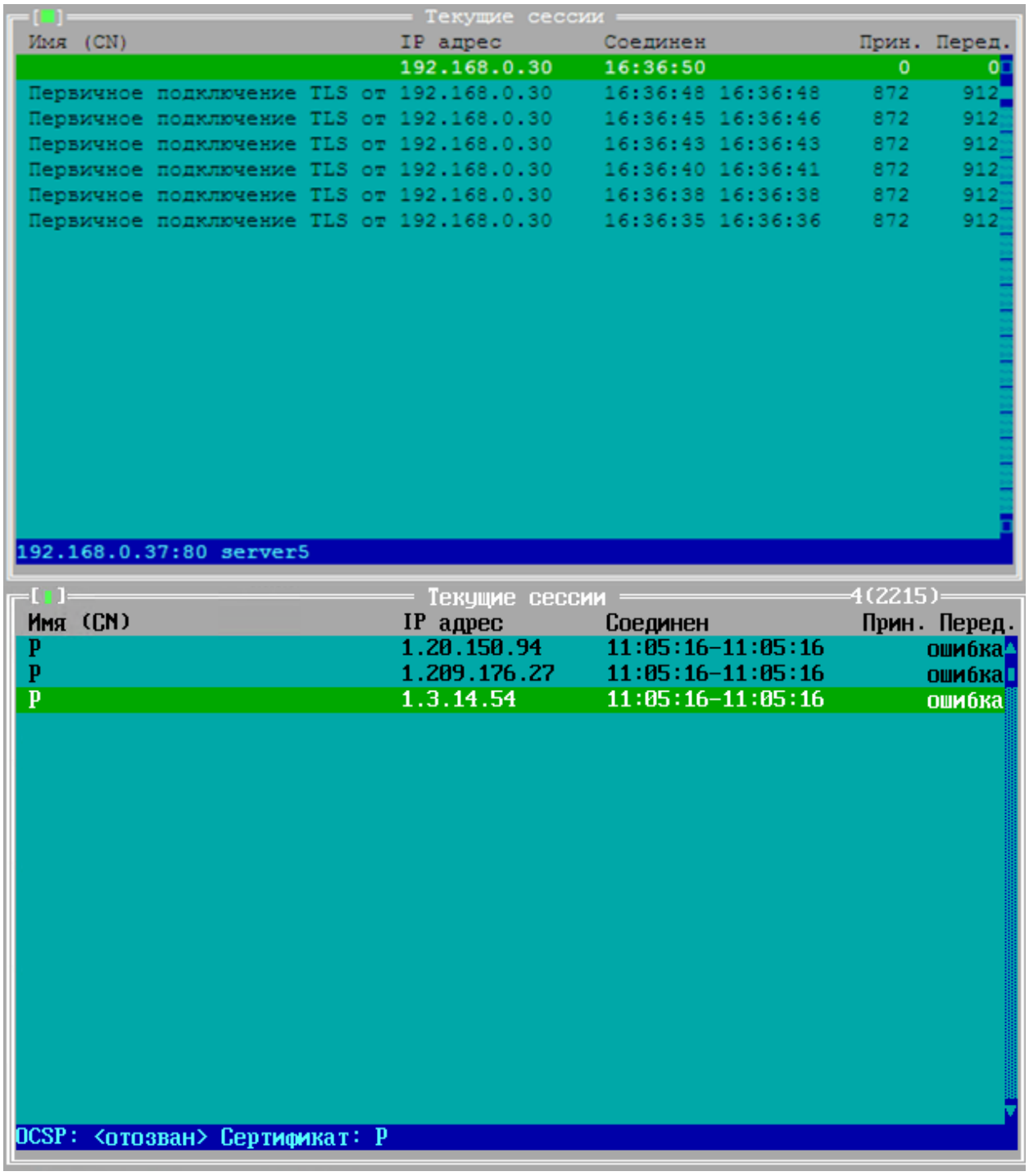


Рисунок 84 - Окно текущих сессий TLS-клиентов

В окне текущих сессий TLS-клиентов отображается следующая информация:

- имя, указанное в сертификате TLS-клиента;
- IP-адрес, с которого подключился TLS-клиент;

- время начала соединения;
- объем принятого и переданного в рамках соединения трафика в байтах;
- ошибка подключения в случае, если сертификат отозван.

При выделении курсором сессии, в строке состояния внизу экрана выдается дополнительная информация по данной сессии:

- IP-адрес Веб-Сервиса, с которым соединился клиент;
- имя данного Веб-Сервиса, как он описан администратором в конфигурации ФПСУ-TLS (см. пункт «Настройка защищаемых http-серверов»), если соединение TLS-клиента Веб-Сервисом выполнено успешно;
- код ошибки и текстовое описание ошибки, если соединение TLS-клиента и Веб-Сервиса не состоялось.

ВНИМАНИЕ! В ФПСУ-TLS запрещено использование просроченного секретного ключа TLS-соединения, информация об использовании такого ключа не выводится на экран, и в окне текущих сессий отсутствуют соединения.

7. 1. 3. ARP таблица

При нахождении ФПСУ-TLS в рабочем режиме, можно просмотреть текущую таблицу ARP по нажатию клавиши <F4>, в которой содержатся результаты работы ARP протокола на всех интерфейсах ФПСУ-TLS.

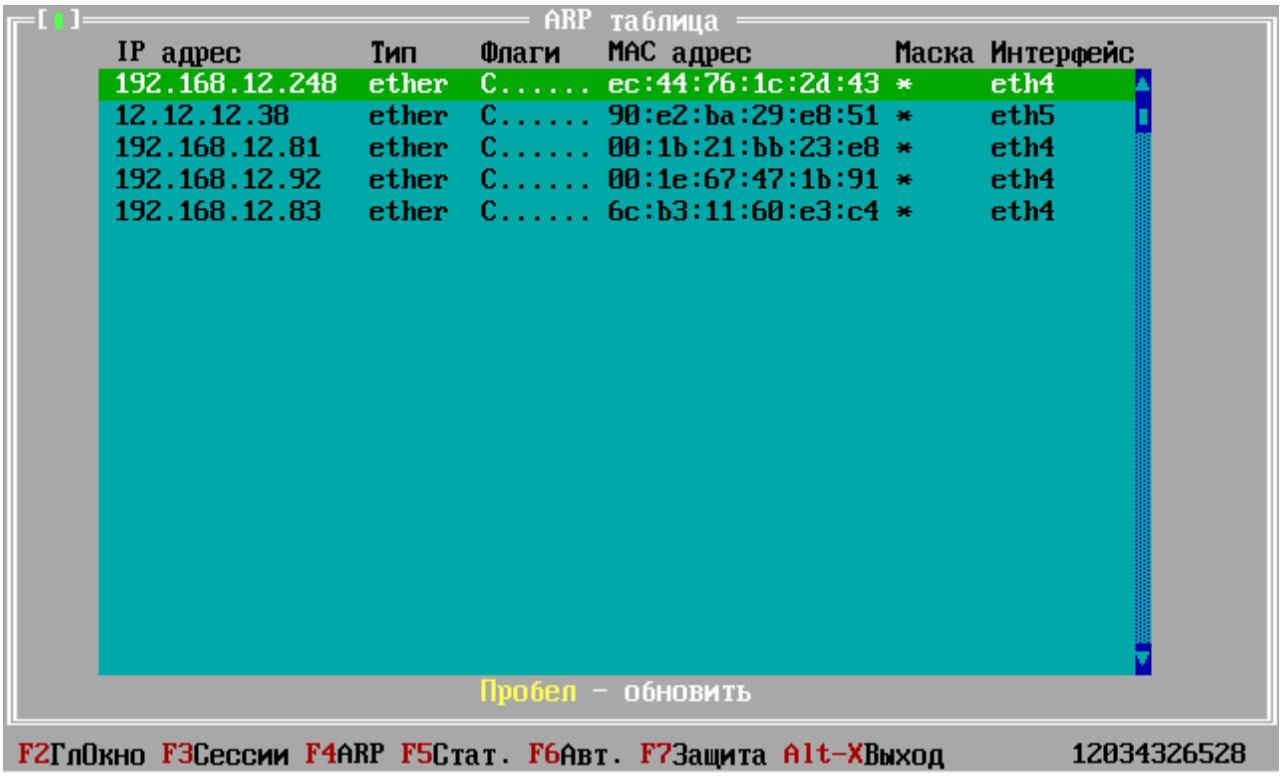


Рисунок 85 - ARP таблица

Каждая запись имеет следующий вид:

IP адрес, для которого ищется MAC-адрес	Тип среды передачи данных	Дополнительные флаги ARP протокола	MAC-адрес (если найден)	Маска подсети IP адреса	Интерфейс, со стороны которого находится хост

7. 1. 4. Просмотр состояния автозагрузок

При нажатии в рабочем режиме клавиши <F6> ФПСУ-TLS на экран выводятся настраиваемые в пункте «Установка сертификатов удостоверяющих центров» параметры автоматической загрузки списка отозванных сертификатов и загрузки пакета сертификатов Удостоверяющих Центров.

Отображается следующая справочная информация:

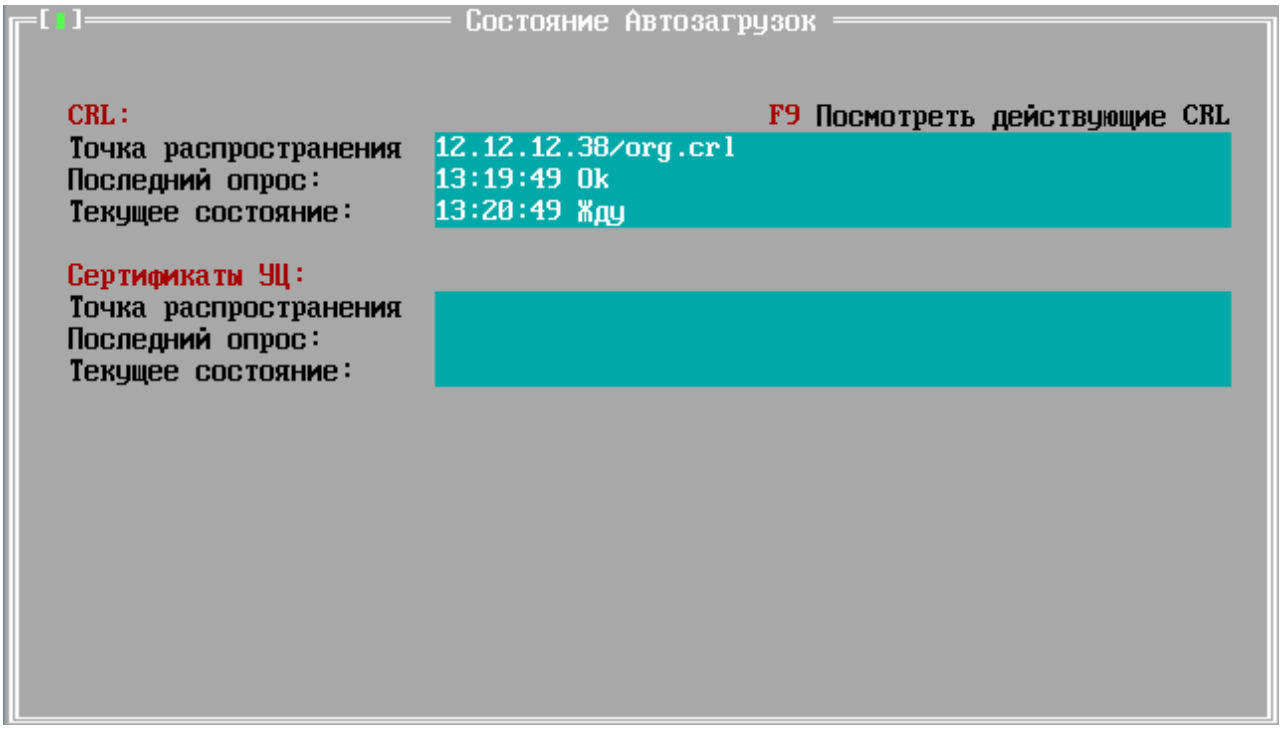


Рисунок 86 - Окно состояния автоматических загрузок сертификатов

В разделе «CRL» выводится информация о загруженном на ФПСУ-TLS списке отозванных сертификатов:

- http-адрес, с которого загружается список отозванных сертификатов («Точка распространения»);
- время последнего опроса точки распространения;
- текущее состояние службы обновления списка отозванных сертификатов.

В разделе «Сертификаты УЦ» выводится информация о загружаемом на ФПСУ-TLS пакете сертификатов (некорневых) Удостоверяющих Центров:

- http-адрес, с которого загружается пакет сертификатов Удостоверяющих Центров («Точка распространения»);
- время последнего опроса точки распространения;
- текущее состояние службы обновления списка отозванных сертификатов.

Информация об издателе, источнике, номере, сроке действия и обновления для отозванного сертификата из списка CRL отображается по нажатию клавиши <F9>.

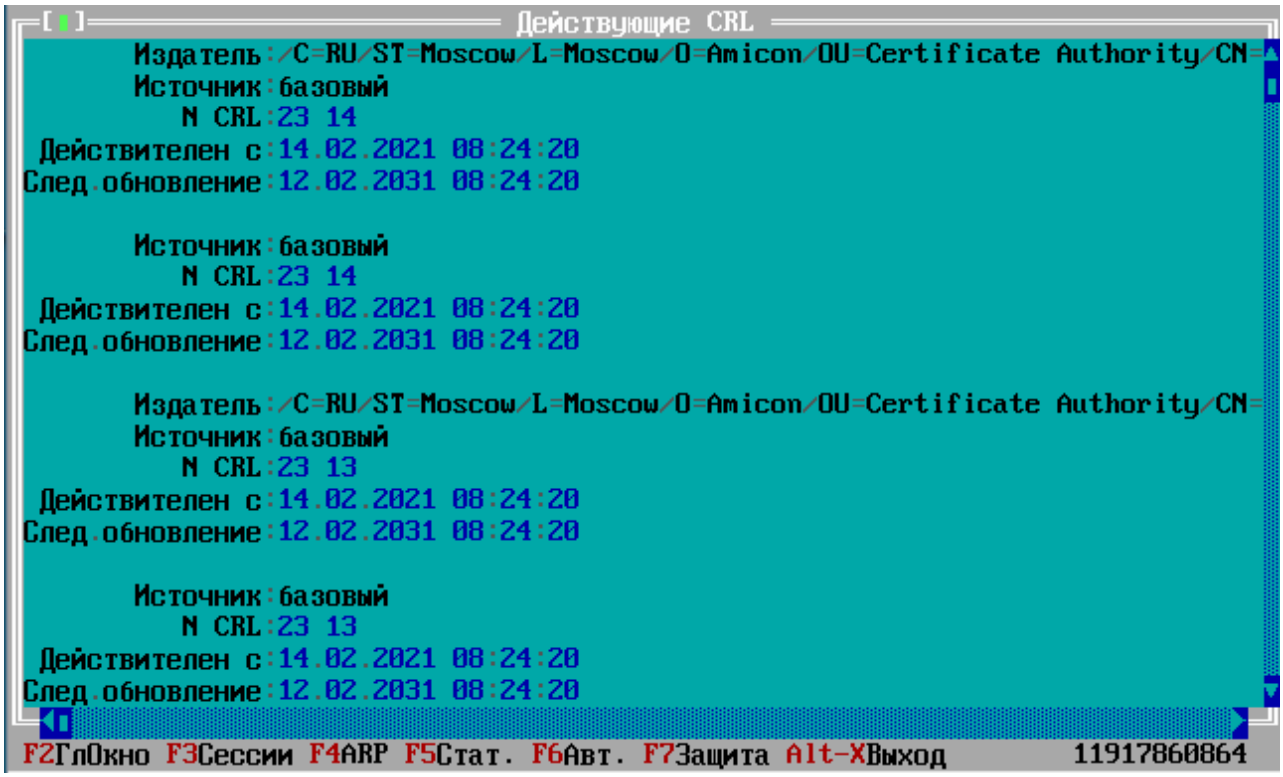


Рисунок 87 - Просмотр действующих CRL

7. 1. 5. Просмотр черного списка IP-адресов

При нажатии в рабочем режиме клавиши <F7> ФПСУ-TLS на экран выводится список IP адресов, соединение которых с ФПСУ-TLS в настоящий момент блокируется.

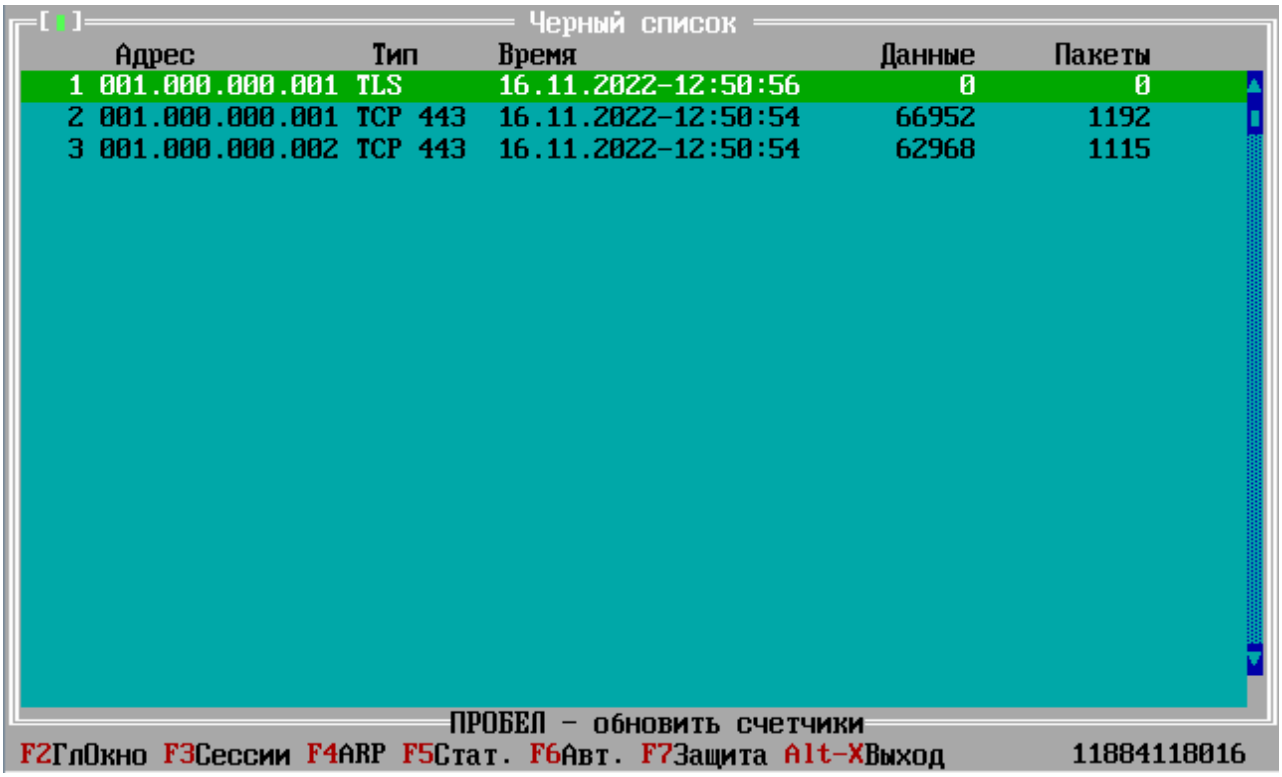


Рисунок 88 - Список IP адресов, соединение которых с ФПСУ-TLS блокируется

7. 1. 6. Выход из рабочего режима ФПСУ-TLS

Выход из окон мониторинга, а также из рабочего режима ФПСУ-TLS осуществляется по нажатию сочетания клавиш <Alt+X> или <F10>.

Появляется окно диалога, позволяющее администратору выбрать режим выхода из окон мониторинга с возвращением к главному меню ФПСУ-TLS:

Выбор команды «Да» в диалоге означает завершение рабочего режима и переход к менеджеру конфигураций. Передача пользовательских данных через ФПСУ-TLS останавливается.

Выбор команды «Нет» в диалоге означает переход к менеджеру конфигураций, сохраняя рабочий режим ФПСУ-TLS активным.

Команда «Отказ» возвращает к предыдущему окну мониторинга.

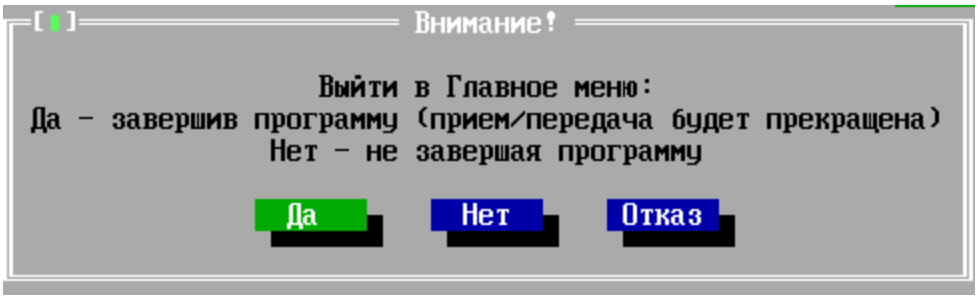


Рисунок 89 - Выбор выхода из рабочего режима

7. 2. Менеджер конфигураций

Менеджер конфигураций ФПСУ-TLS предназначен для создания, хранения, изменения и рассылки хранящихся на этом ФПСУ-TLS конфигураций настроек на другие комплексы ФПСУ-TLS.

На ФПСУ-TLS может храниться множество заранее созданных или загруженных с другого ФПСУ-TLS конфигураций, но только одна из них может быть активной и управлять рабочим режимом ФПСУ-TLS.

Окно менеджера конфигураций вызывается после выхода из окон мониторинга рабочего режима, или выполнения команды «Конфигурация ФПСУ» главного меню ФПСУ-TLS.

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

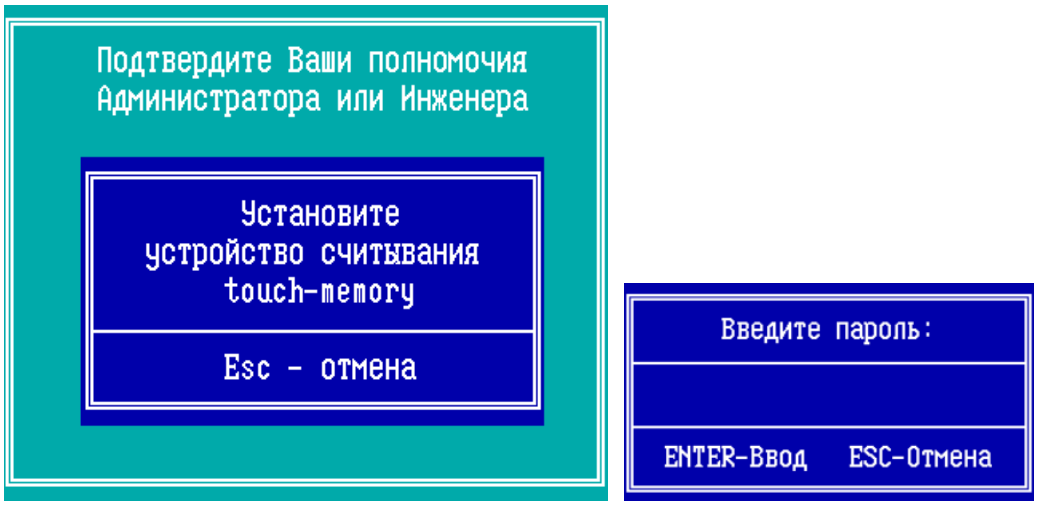


Рисунок 90 - Подтверждение полномочий и ввод пароля ТМ

Окно менеджера конфигураций содержит список созданных конфигураций, с наименованием, временем создания и последнего изменения.

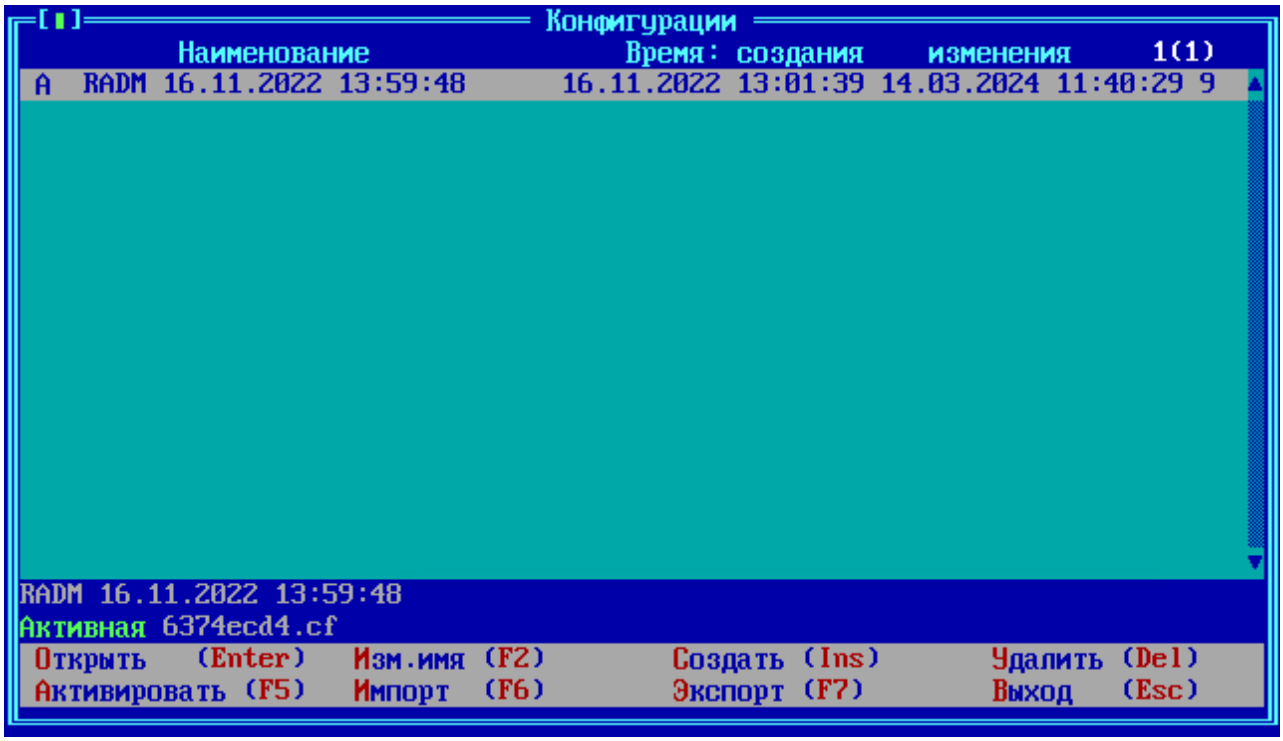


Рисунок 91 - Окно менеджера конфигураций

Статус ***«A»*** в строке записи конфигурации означает, что данная конфигурация является активной, и в соответствии с ней задействован рабочий режим ФПСУ-TLS.

Администратору доступны следующие возможности по управлению конфигурациями:

- открытие выбранной курсором конфигурации на просмотр, редактирование, и последующее сохранение внесенных изменений (<Enter>);
- изменение наименования выбранной курсором конфигурации (<F2>);
- создание новой пустой конфигурации (<Ins>);
- удаление выбранной курсором конфигурации (<Del>);
- активация выбранной курсором конфигурации в качестве рабочей (<F5>);
- выгрузка выбранной курсором конфигурации на внешний носитель (<F6>);
- загрузка конфигурации с внешнего носителя (<F7>).

По нажатию клавиши <Esc> осуществляется возврат из окна менеджера конфигураций в главное меню ФПСУ-TLS.

Активация конфигурации

Активация конфигурации в качестве рабочей осуществляется по нажатию клавиши <F5>, на экран выдается окно:

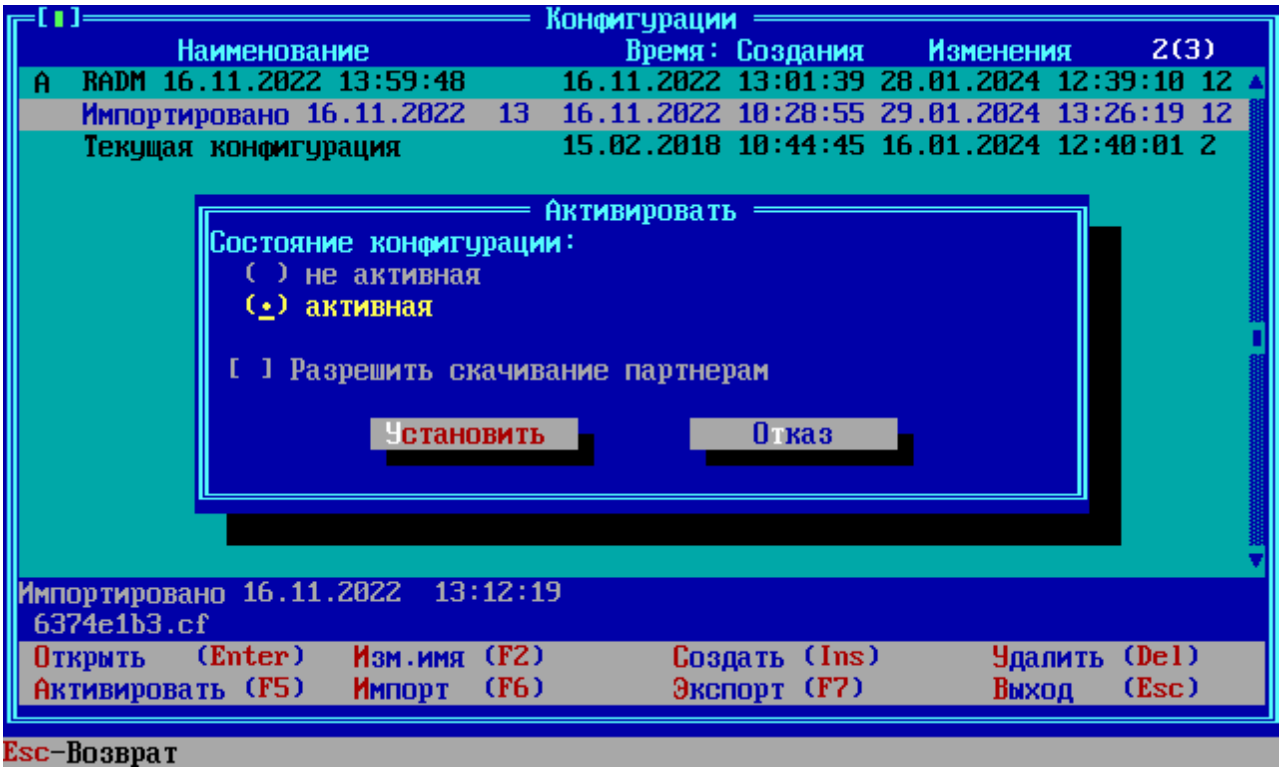


Рисунок 92 - Окно активации конфигурации

В окне «Активировать» необходимо отметить состояние конфигурации «активная» по нажатию клавиши <Пробел> и подтвердить по команде «Установить».

Разрешить скачивание партнерам - в случае изменения конфигурации установленный флаг позволяет ФПСУ-TLS, входящим в кластер, видеть и вносить изменения данной конфигурации. При установлении данного флага. скачивание партнерами будет осуществляться только в том случае, если сертификат администратора данного ФПСУ-TLS установлен на ФПСУ-TLS партнеров. В статус конфигурации добавится символ ***«S»*** - ФПСУ-TLS становится сервером, с которого партнерами скачивается данная конфигурация.

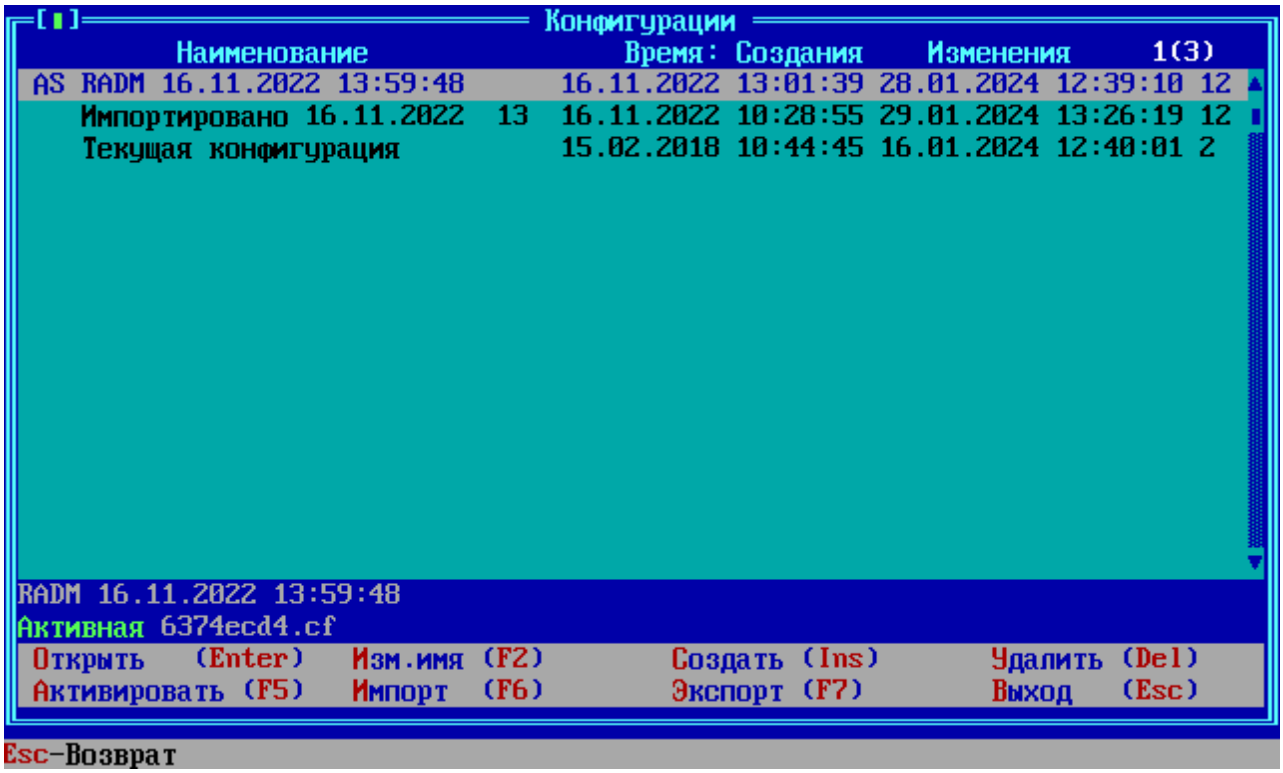


Рисунок 93 - Рабочая конфигурация

Статус ***«a»*** в строке записи конфигурации означает, что были внесены изменения в рабочую конфигурацию, данный статус отображается до следующего сохранения или активации конфигурации по клавише <F5>.

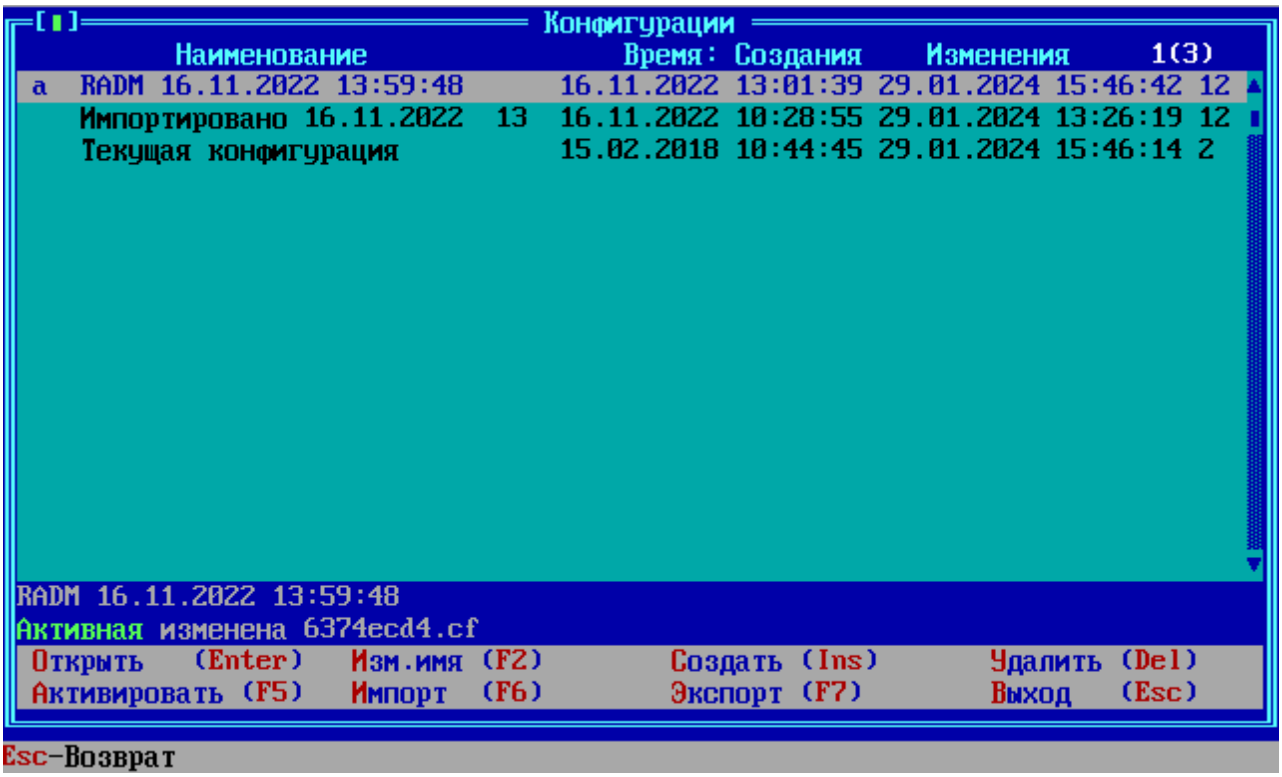


Рисунок 94 - Рабочая конфигурация с внесенными изменениями

Экспорт конфигурации

Данные конфигурации могут быть экспортированы на внешний носитель. Экспорт осуществляется по нажатию клавиши <F7>. Система предложит подключить к ФПСУ-TLS внешний носитель.

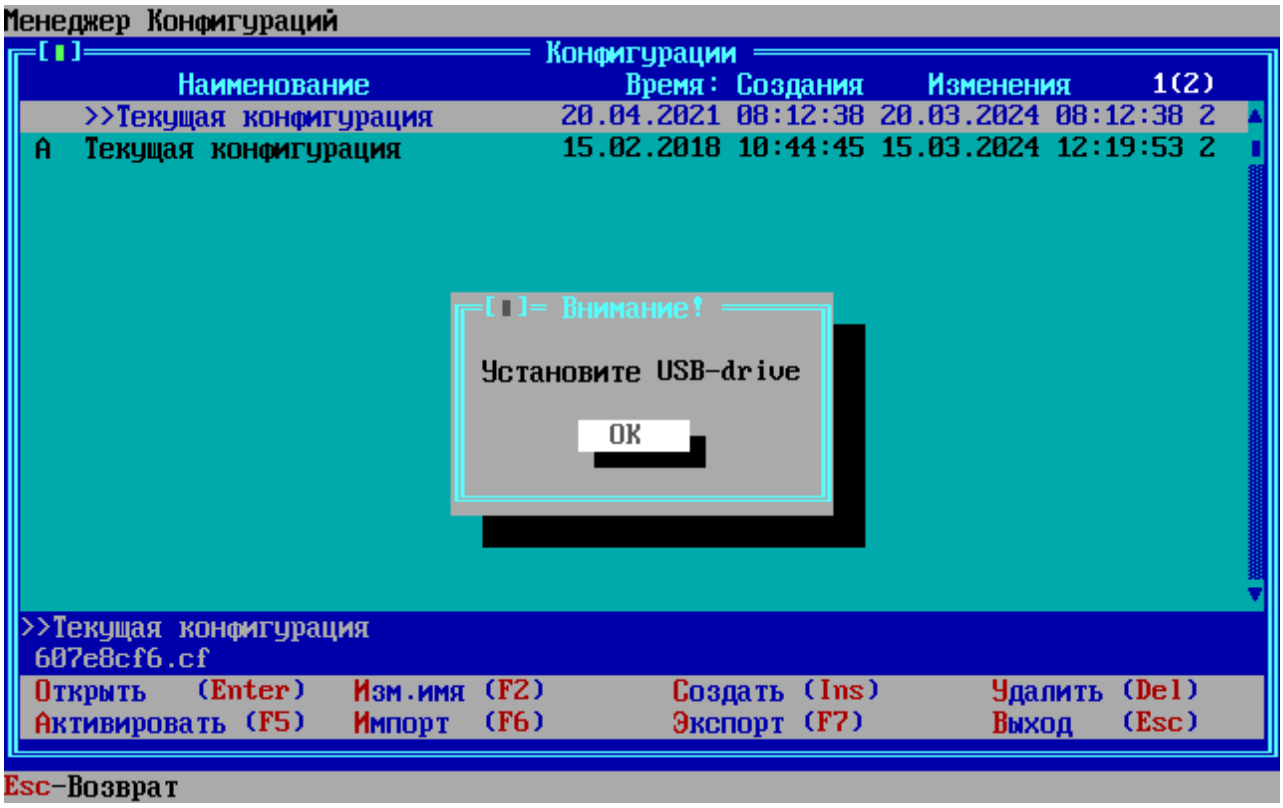


Рисунок 95 - Носитель для экспорта конфигурации

В открывшемся окне выберите каталог для сохранения конфигурации и нажмите «Каталог выбран».

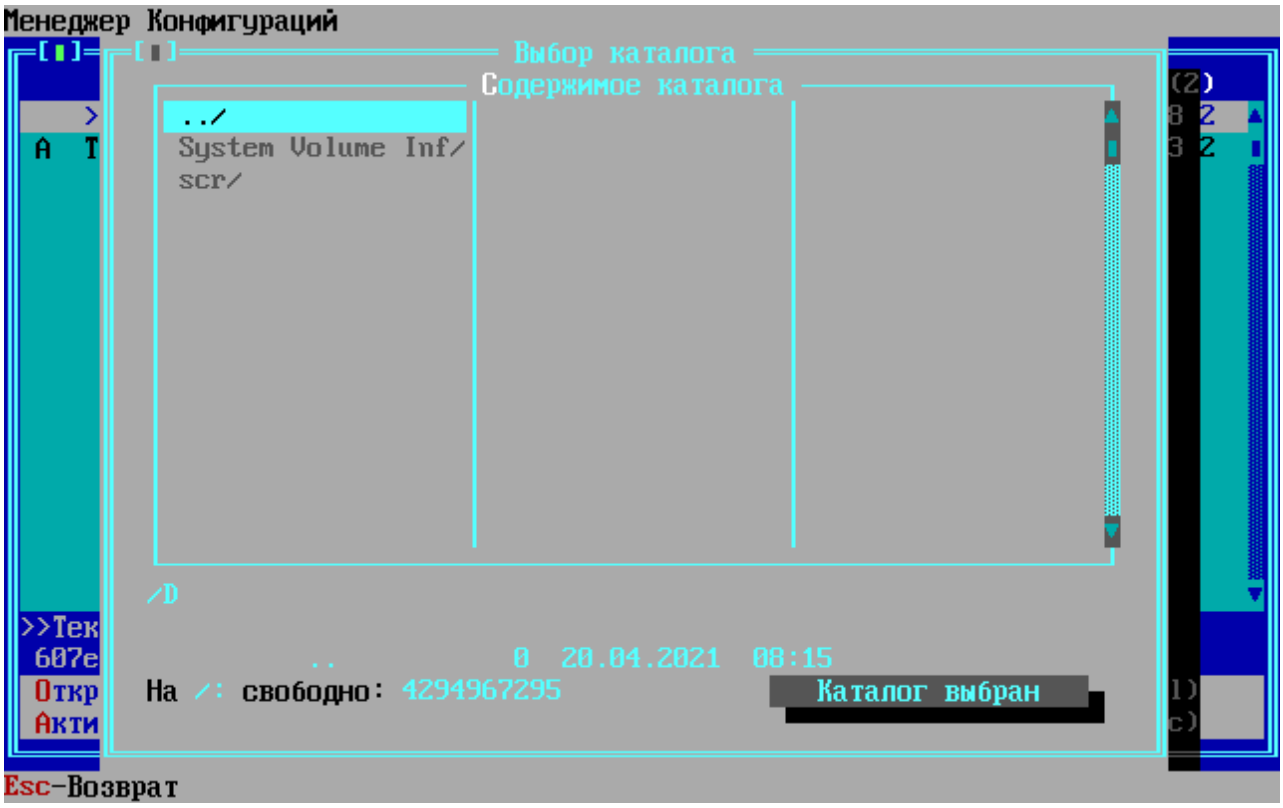


Рисунок 96 - Выбор каталога для экспорта

Далее будет выдано сообщение о выгрузке конфигурации в файл .cf.

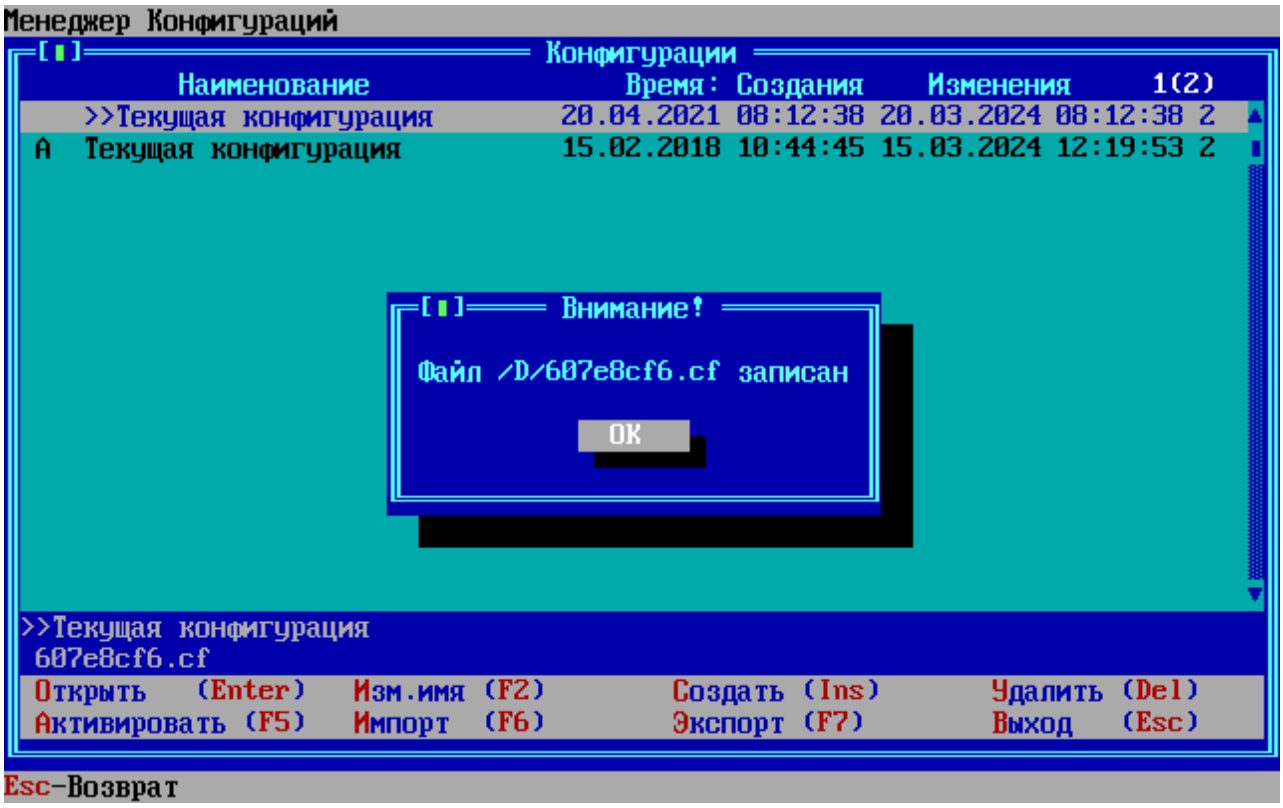


Рисунок 97 - Экспорт конфигурации в файл

Импорт конфигурации

Экспортированная ранее конфигурация может быть импортирована обратно. Импорт осуществляется по нажатию клавиши <F6>. Система предложит подключить к ФПСУ-TLS внешний носитель.

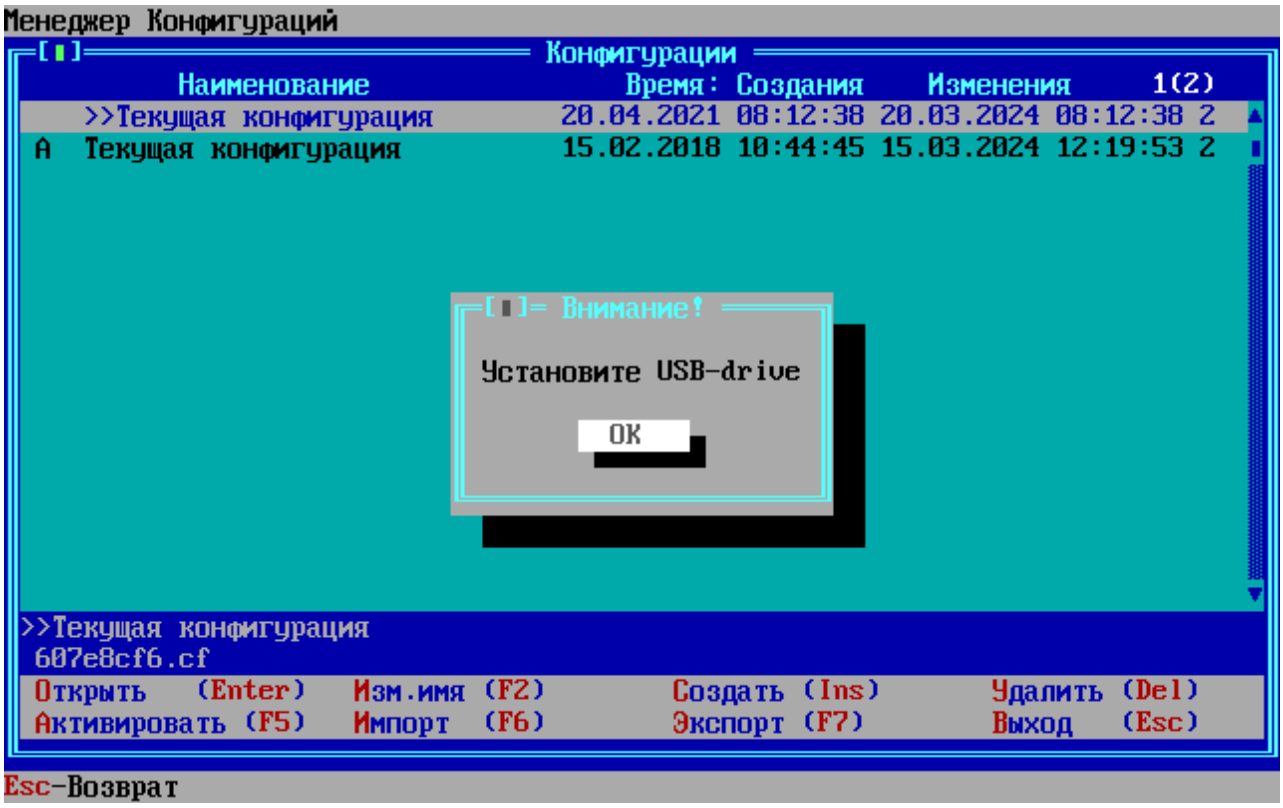


Рисунок 98 Носитель с конфигурацией

В открывшемся окне выберите файл конфигурации для загрузки и нажмите «Файл выбран».

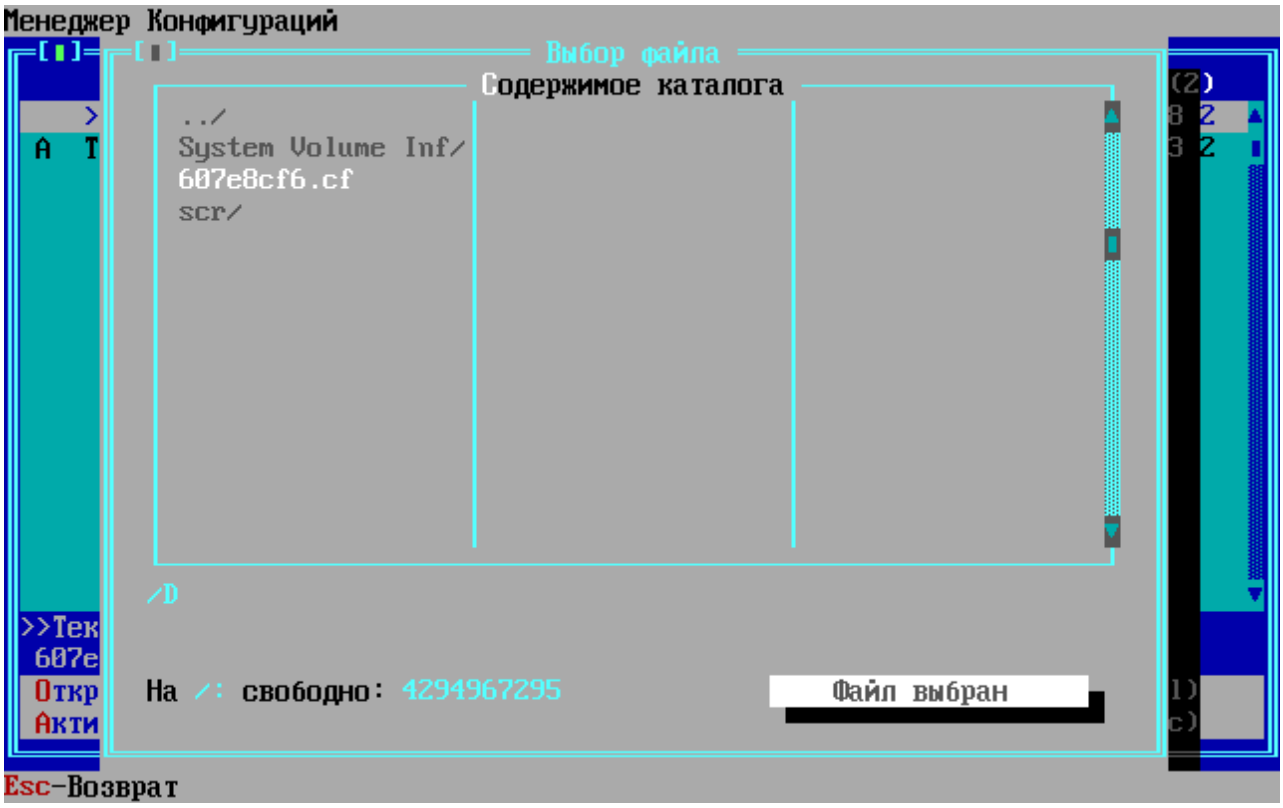


Рисунок 99 - Выбор файла для импорта

Конфигурация получит наименование «Импортировано» с датой изменения.

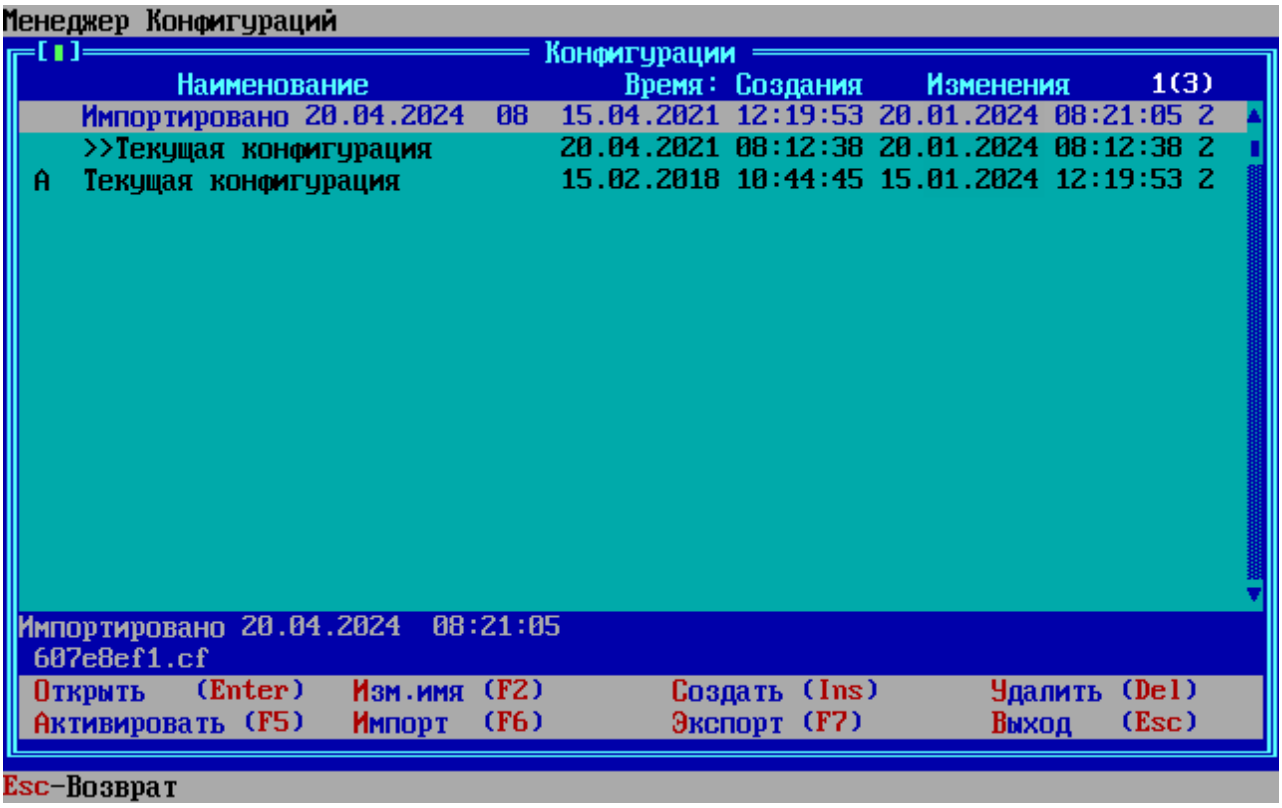


Рисунок 100 - Импортированная конфигурация

При импорте конфигурации проверяется серийный номер ФПСУ-TLS, если совпадает, то восстанавливаются индивидуальные параметры: внешний и внутренний сетевые адреса и их маски; параметры масштабирования; собственные ключи и сертификаты, параметры аутентификации ФПСУ. Если серийный номер не совпадает, то восстанавливаются только общие параметры: сертификаты УЦ, параметры обслуживаемых серверов, маршруты интерфейсов, параметры NAT, идентификатор масштабирования, параметры Syslog и SNMP, параметры загрузки СОС, параметры подсистемы защиты от атак.

7. 3. Режимы взаимодействия ФПСУ-TLS и защищаемой службы

При добавлении в список защищаемых серверов новой записи (см. пункт «Настройка защищаемых http-серверов»), администратор ФПСУ-TLS может уточнить, каким образом будет осуществляться обработка направляемого к добавляемому серверу клиентского трафика: передаваться в открытом виде с применением только HTTP протокола или по защищенному TLS-соединению, при котором ФПСУ-TLS будет выступать инициирующим соединение клиентом, а добавляемый сервер – в роли TLS-сервера.

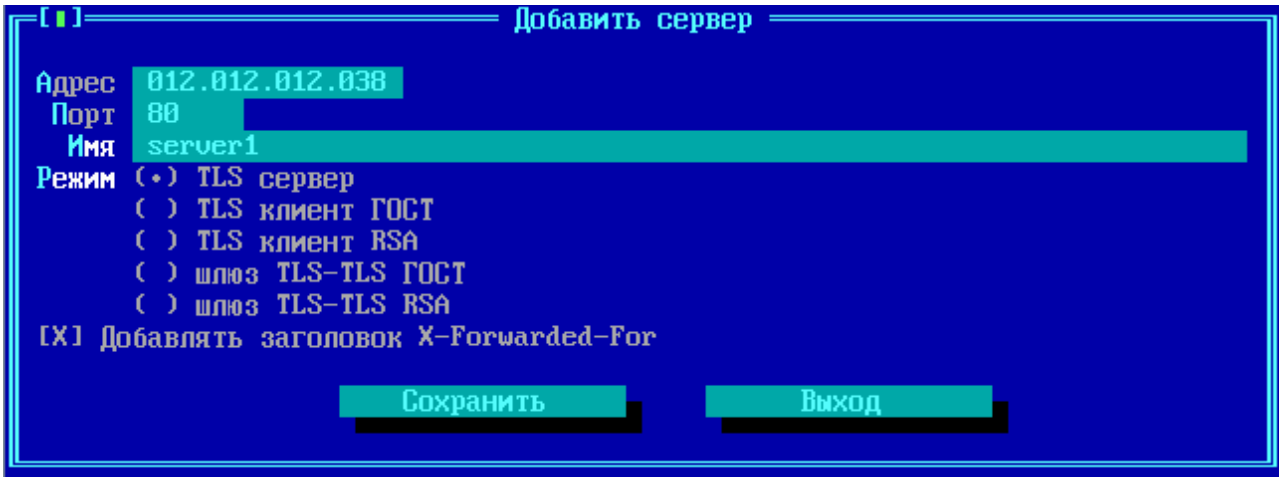


Рисунок 101 - Параметры соединения с защищаемым сервером

Режим «TLS-сервер»

Опция по умолчанию, «TLS-сервер», предполагает защищенное соединение с ФПСУ-TLS от TLS-клиента из внешней сети, и незащищенное http-соединение с защищаемым сервером, транслирующее клиентский трафик Веб-Сервису. Более подробно по применяемым алгоритмам и криптонаборам изложено в пункте «Общие сведения».

В режиме «TLS-сервер» выбор криптографических алгоритмов зависит от криптоалгоритма в сертификате ФПСУ-TLS.

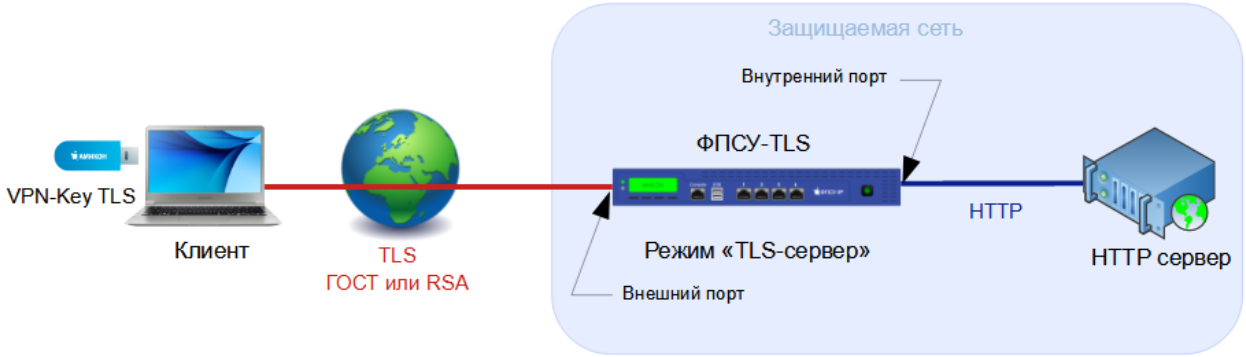


Рисунок 102 - Режим работы по умолчанию, «TLS-сервер»

Такая схема предполагается к использованию, когда защищаемый сервер установлен в доверенной среде внутренней локальной сети организации, а клиент подключается к локальной сети из общедоступной сети (например, Internet).

Для организации соединения ФПСУ-TLS с защищаемым сервером в режиме «TLS-сервер» должны быть установлены:

- на клиенте - личный клиентский сертификат; корневой сертификат УЦ, которым

подписан личный клиентский сертификат; корневой сертификат УЦ, которым подписан серверный сертификат ФПСУ-TLS.

- на ФПСУ-TLS - личный серверный сертификат; корневой сертификат УЦ, которым подписан личный серверный сертификат; корневой сертификат УЦ, которым подписан личный клиентский сертификат.

Режим «TLS-клиент»

Опции «TLS-клиент ГОСТ» и «TLS-клиент RSA» используют одну и ту же схему работы, отличаясь только используемым в TLS-соединении криптонаборами. Более подробно по применяемым алгоритмам и криптонаборам изложено в пункте «Общие сведения».

Режим «TLS-клиент» предусматривает незащищенное HTTP соединение между ФПСУ-TLS и клиентом во внутренней защищаемой сети и защищенное TLS соединение, использующее шифрование между ФПСУ-TLS и сервером во внешней сети.

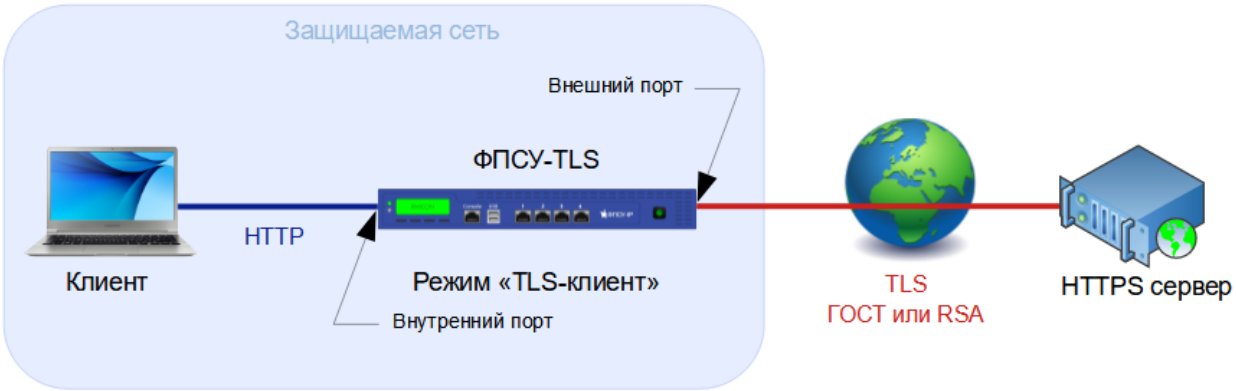


Рисунок 103 - Режимы работы «TLS-клиент»

Такая схема может быть использована, когда клиент не имеет возможности использовать TLS-протокол.

Для организации соединения ФПСУ-TLS с защищаемым сервером в режиме «TLS-клиент» должны быть установлены:

- на ФПСУ-TLS - личный клиентский сертификат; корневой сертификат УЦ, которым подписан личный клиентский сертификат.
- на сервере - личный серверный сертификат; корневой сертификат УЦ, которым подписан личный серверный сертификат; сертификат УЦ, которым подписан клиентский сертификат ФПСУ-TLS.

ФПСУ-TLS может быть применен для защиты взаимодействия Клиента и Веб-сервиса, осуществляемого через недоверенную среду, в случае когда клиент и сервер Веб-сервиса находятся в защищаемых сетях, соединенных общедоступной сетью (например, Internet). ФПСУ-TLS в такой схеме используется в паре для организации криптографически защищенного туннеля от клиента к серверу. Со стороны внутреннего порта ФПСУ-TLS в режиме «TLS-клиента» используется незащищенное HTTP соединение клиента с ФПСУ-TLS, со стороны внешнего порта настроено защищенное TLS соединение, использующее шифрование по российским криптографическим алгоритмам (опция ГОСТ) или по международным криптографическим алгоритмам (опция RSA), с соседним ФПСУ-TLS в режиме «TLS-сервера», за которым находится защищаемый сервер, соединение с сервером незащищенное по протоколу HTTP.

Рисунок 104 - Организация криптографически защищенного туннеля

Защищенное TLS-соединение может быть организовано с помощью ФПСУ-TLS для пересылки почтовых сообщений по протоколам SMTP, POP3, IMAP4.

Рисунок 105 - Защита прикладных протоколов

Защищенное TLS-соединение может быть организовано для протокола распространения, запрашивания, размещения и получения групп новостей при взаимодействии между сервером новостей и клиентом, NNTP, а также для протокола установления прямой связи между узлами, в данном случае между клиентом и сервером, PPP.

Режим «шлюз TLS-TLS»

Опции «шлюз TLS-TLS ГОСТ» и «шлюз TLS-TLS RSA» используют одну и ту же схему работы, отличаясь только используемым в TLS соединении криптографическим протоколом. Более подробно по применяемым алгоритмам и криптонаборам изложено в

пункте «Общие сведения».

Схема взаимодействия, при которой режим «шлюз TLS-TLS» предусматривает защищенное TLS соединение, использующее шифрование по российским криптографическим алгоритмам (опция ГОСТ), между ФПСУ-TLS и клиентом во внешней сети и защищенное TLS соединение, использующее шифрование по российским криптографическим алгоритмам (опция ГОСТ) или по международным криптографическим алгоритмам (опция RSA), между ФПСУ-TLS и защищаемым сервером во внутренней сети.

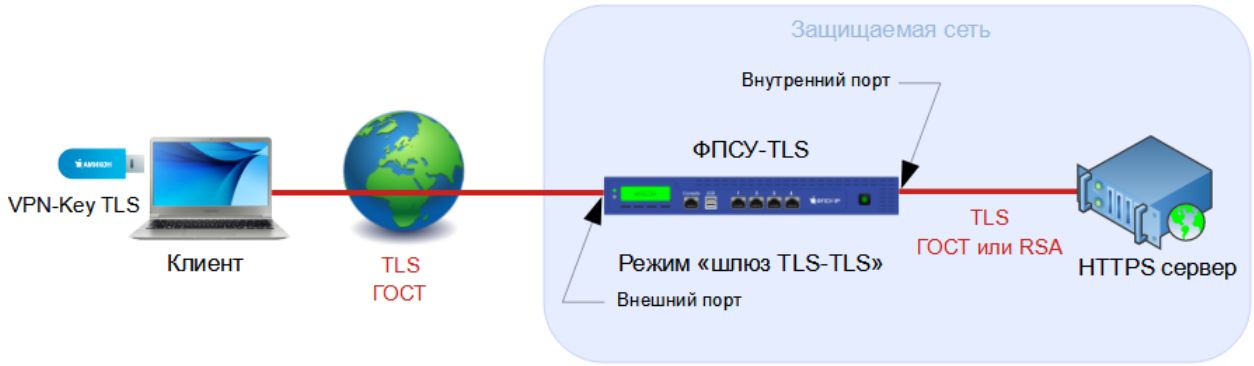


Рисунок 106 - Режимы работы «шлюз TLS-TLS»

Примером применения данной схемы может служить организация защищенного TLS соединения, использующего шифрование по российским криптографическим алгоритмам, между ФПСУ-TLS и клиентом во внешней сети и организация защищенного TLS соединения, использующего шифрование по международным криптографическим алгоритмам, чтобы разгрузить https сервер, так как реализация российских криптографических алгоритмов более требовательна к ресурсам.

Для организации соединения ФПСУ-TLS с защищаемым сервером в режиме «шлюз TLS-TLS» должны быть установлены:

- на клиенте - личный клиентский сертификат; корневой сертификат УЦ, которым подписан личный клиентский сертификат; корневой сертификат УЦ, которым подписан серверный сертификат ФПСУ-TLS.
- на ФПСУ-TLS - личный клиентский сертификат; корневой сертификат УЦ, которым подписан личный клиентский сертификат; личный серверный сертификат; корневой сертификат УЦ, которым подписан личный серверный сертификат.
- на сервере - личный серверный сертификат; корневой сертификат УЦ, которым подписан личный серверный сертификат; сертификат УЦ, которым подписан клиентский сертификат ФПСУ-TLS.

7. 4. Масштабирование

Для повышения доступности и обеспечения бесперебойной работы защищаемых подсетей, ФПСУ-TLS содержит подсистему масштабирования, позволяющую объединить группу ФПСУ-TLS в один виртуальный комплекс в соответствии с протоколом VRRP (Virtual Router Redundancy Protocol, RFC 5798).

7. 4. 1. Описание подсистемы масштабирования

Важнейшей особенностью ФПСУ-TLS является механизм масштабирования, который позволяет объединить в один виртуальный комплекс (кластер) несколько ФПСУ-TLS (узлов). Этот механизм позволяет расширять и наращивать производительность системы за счёт увеличения количества узлов системы и повышает надежность системы. При выходе из строя одного из узлов система автоматически перераспределит нагрузку на работающие узлы.

Масштабирование на ФПСУ-TLS реализовано на базе продуктов:

1) IPVS (http://www.linuxvirtualserver.org/software/ipvs.html), которая является частью проекта http://www.linuxvirtualserver.org. Это встроенный в ядро Linux load-balancer для создания кластеров, балансирующих нагрузку под Linux. Именно этот модуль реализует протокол VRRP.
2) keepalived - демон, управляющий конфигурированием IPVS.

Кластеру ФПСУ-TLS назначается один общий виртуальный IP-адрес, по которому подключаются клиенты и идентификатор (число от 1 до 254). Идентификатор для каждого кластера должен быть уникальным в рамках локальной сети.

Все узлы, входящие в кластер, могут иметь состояние основной или неосновной. Состояние основной имеет только один узел, назначенный при конфигурировании. Если основной узел выключается (или не был включен), через 1 секунду инициализируется процесс голосования, где выбирается новый основной узел.

Основной узел выполняет следующие действия:

- раз в 3 секунды (значение по умолчанию, может быть изменено администратором ФПСУ-TLS) посылает специальный запрос на узлы-партнеры, указанные в конфигурации. Если узел-партнер ответил, он добавляет его в пул работающих узлов (таблица балансировки IPVS);
- отвечает на ARP-запросы и принимает пакеты на IP-адрес ассоциированный с виртуальным IP-адресом;

- пакеты, принятые по виртуальному адресу, перенаправляет на узлы-партнеры по алгоритму масштабирования. Алгоритм по умолчанию - Source Hash Scheduling (может быть изменен администратором ФПСУ-TLS, см. пункт «Настройка подсистемы масштабирования»). Согласно этому алгоритму, все поступающие на внешний виртуальный адрес соединения распределяются в пуле работающих узлов в соответствии с IP адресом отправителя из статической hash-таблицы, где индекс таблицы i вычисляется по формуле i=hash (IP-адрес отправителя).

Например, кластер состоит из 3 узлов. Тогда все множество интернет-адресов будет разбито на 3 подсети (A, B, C). Клиент 1 из подсети A (синяя линия), который устанавливает защищенное соединение с ФПСУ-TLS по виртуальному адресу 192.168.1.80, будет перенаправлен на ФПСУ-TLS №2 и тот установит соединение с интерфейса 192.168.2.82 с защищаемым http-сервером.

Этот алгоритм позволяет добиться того, что все соединения от одного клиента будут поступать на один и тот же ФПСУ-TLS.

При изменении количества узлов, происходит перестройка hash-таблицы, соответственно изменится распределение клиентов в пуле работающих узлов. Но при этом сохраняются ранее созданные распределения: если клиентом было установлено соединение с определенным узлом до перестройки hash-таблицы, все последующие соединения будут выполняться с этим узлом.

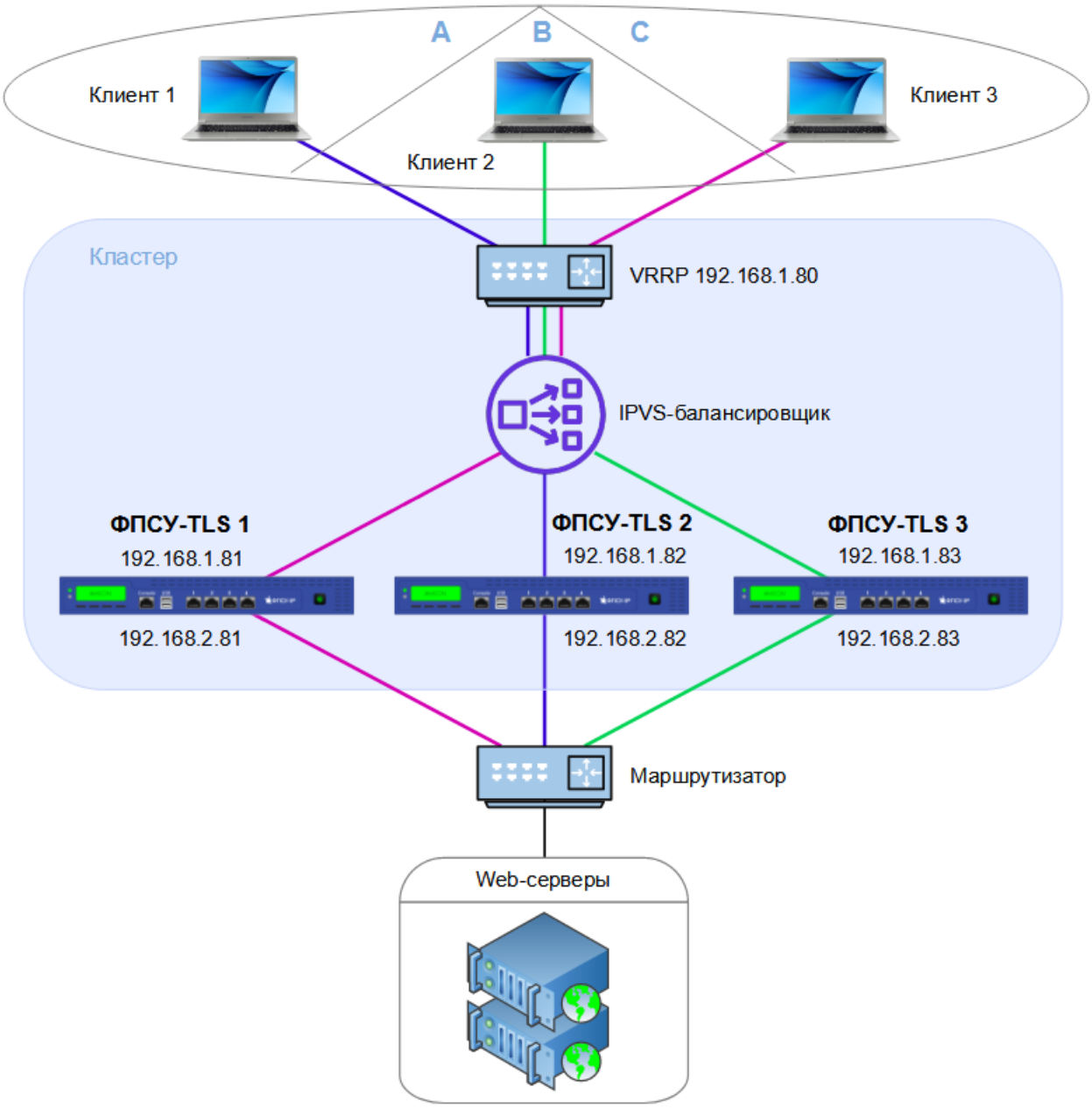


Рисунок 107 - Схема работы кластера ФПСУ-TLS

7. 4. 2. Настройка подсистемы масштабирования

Для настройки подсистемы выполните команду «Масштабирование» в меню установки параметров ФПСУ-TLS.

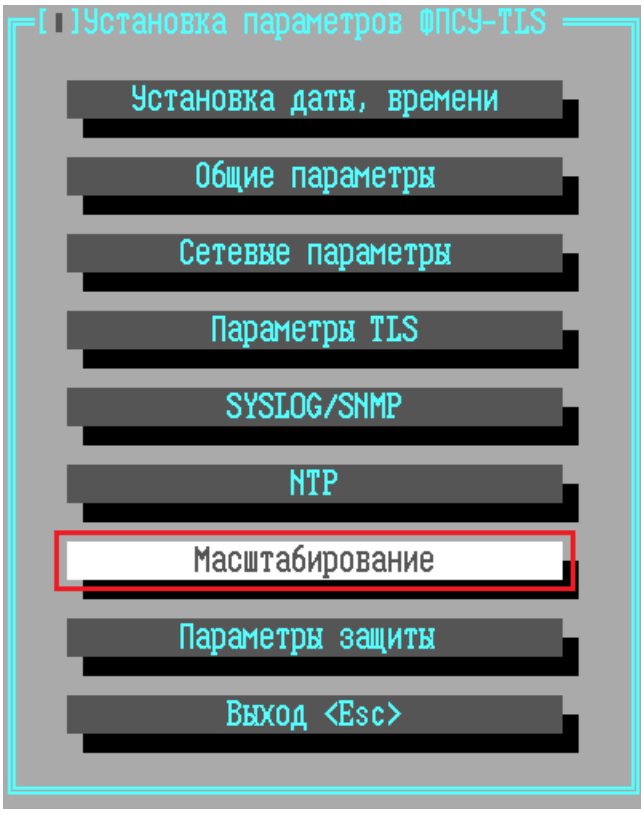


Рисунок 108 - Меню установки параметров ФПСУ-TLS

В открывшемся окне будут указаны следующие параметры работы подсистемы:

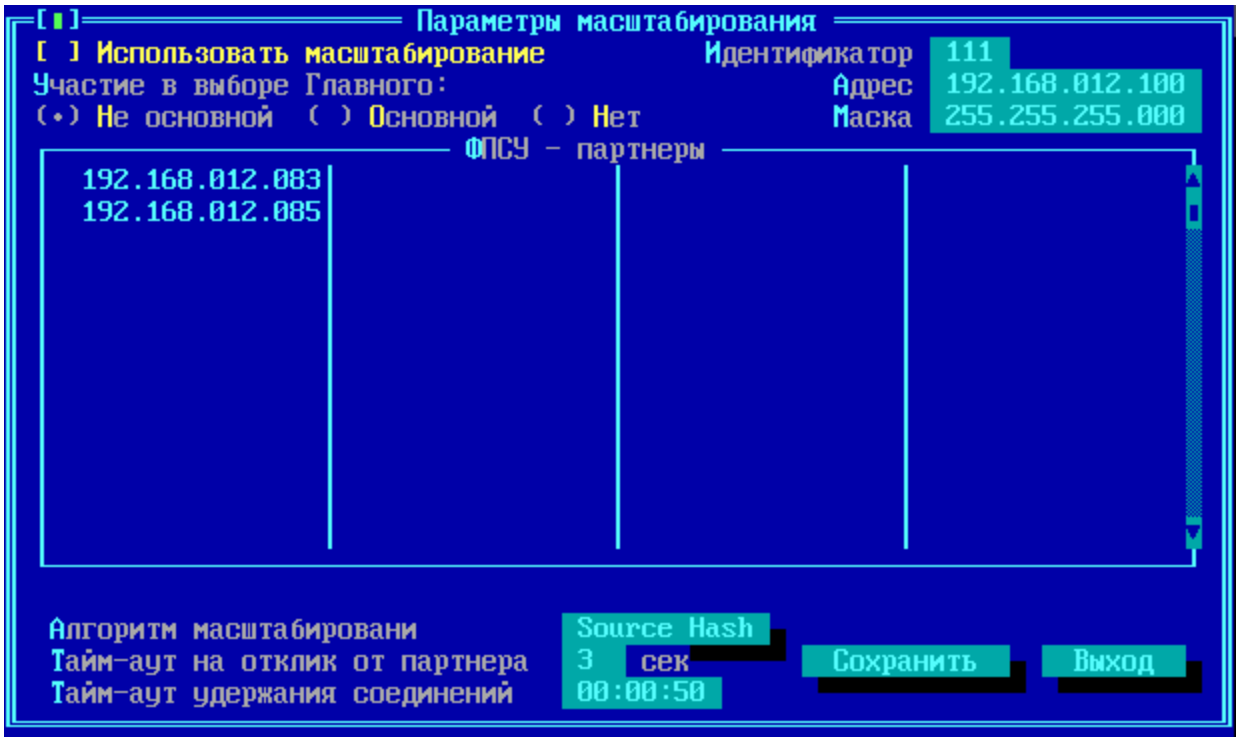


Рисунок 109 - Настройка масштабирования

Участие в выборе Главного – в процессе создания виртуального комплекса из нескольких ФПСУ-TLS, один из ФПСУ-TLS должен быть сконфигурирован как «Основной» в создаваемом виртуальном комплексе, а остальные ФПСУ-TLS, участвующие в распределении нагрузки получают статус «Не основной».

- *«Основной»* ФПСУ-TLS подсистемы масштабирования отвечает за отправку пакетов, отправленных на основной IP-адрес (общий виртуальный IP-адрес), и за ответы на ARP-запросы, отправленные на этот адрес.
- *«Не основной»* ФПСУ-TLS находится в резерве, и может взять на себя роль «основного» ФПСУ-TLS, если текущий становится недоступен.
- Статус *«Нет»* для ФПСУ-TLS означает, что он не будет участвовать в выборе.

Использовать масштабирование – установленный флаг активирует настройки масштабирования, при снятом флаге ФПСУ-TLS не будет участвовать в масштабировании.

Идентификатор – уникальный в рамках локальной сети идентификатор (Virtual Router Identifier, VRID в соответствии с протоколом VRRP) виртуального комплекса ФПСУ-TLS, настраиваемое значение в диапазоне от 1 до 255. Если в локальной сети работает несколько систем, использующих протокол VRRP, совпадение идентификаторов этих систем может приводить к ошибкам. Для корректной работы на всех ФПСУ-TLS, входящих в один кластер, идентификатор должен совпадать.

Адрес – здесь требуется указать основной IP-адрес, который будет использоваться как адрес TLS-сервера для TLS-клиентов по умолчанию. Пакеты, отправленные на этот основной IP-адрес, может принять и обработать любой из ФПСУ-TLS, участвующий в системе распределения нагрузки.

Маска – маска подсети основного IP-адреса.

ФПСУ-партнеры – в этот список следует добавить все ФПСУ-TLS, которые участвуют с данным ФПСУ-TLS в распределении нагрузки.

Для добавления информации о новом ФПСУ-TLS-партнере, нажмите клавишу <Ins> и в открывшемся окне введите IP-адрес внешнего интерфейса партнера. Нажмите клавишу <F2> или <Enter> для сохранения и добавления партнера в список.

IP-адрес находящегося в списке партнеров ФПСУ-TLS можно изменить, выделив описатель курсором и нажав клавишу <Enter>.

Для возврата в меню установки параметров ФПСУ-TLS, с сохранением выполненных изменений, выполните команду ***«Сохранить»***.

Алгоритм масштабирования – опция, указывающая используемый в кластере ФПСУ-TLS алгоритм балансировки запросов клиентов. По указанному алгоритму определяется, которому ФПСУ-TLS из узлов кластера будет направлен новый запрос клиента на соединение. Можно выбрать один из следующих алгоритмов:

- *Source Hash* – алгоритм по умолчанию, алгоритм балансировки нагрузки определяет ФПСУ-TLS, на который следует направить запрос на основе IP-адреса клиента. Для каждого входящего запроса определяется IP-адрес клиента, применяется хеш-функция к IP-адресу для получения числового значения, хеша. Хеш значение используется для выбора ФПСУ-TLS из кластера. Одному и тому же клиенту всегда будет назначен один и тот же узел кластера. Алгоритм позволяет поддерживать сессию между клиентом и сервером, когда необходимо сохранять состояние в течение сеанса.
- *Round Robin* – запросы клиентов отправляются на все узлы кластера ФПСУ-TLS по очереди, по кругу. При использовании этого алгоритма все ФПСУ-TLS в кластере считаются равными, вне зависимости от текущей загрузки и мощности.
- *Least Conn* – алгоритм наименьшего количества соединений. Этот алгоритм учитывает количество текущих соединений, имеющихся у каждого ФПСУ-TLS, выбирает узел кластера с наименьшим количеством активных соединений из числа доступных ФПСУ-TLS в кластере.

Тайм-аут на отклик от партнера – параметр ФПСУ-TLS, имеющего статус основного в масштабировании. Здесь указывается ожидания ответа от партнера по масштабированию, на который основной ФПСУ-TLS пытается перенаправить нового TLS-клиента. Если за указанное время ответа не приходит, партнер считается вне сети.

Тайм-аут удержания соединений – время (по умолчанию 50 секунд), за которое повторно подключившегося TLS-клиента основной ФПСУ-TLS системы масштабирования автоматически направит на тот же ФПСУ-TLS, с которым TLS-клиент соединялся ранее. Механизм балансировки нагрузки соединений в случае быстрого повторного подключения TLS-клиента не будет запущен.

7. 5. Общие параметры конфигурации ФПСУ-TLS

Эта группа установок определяет общие правила работы ФПСУ-TLS. При выполнении команды «Общие параметры» меню конфигурации ФПСУ-TLS откроется окно, содержащее следующие команды и параметры:

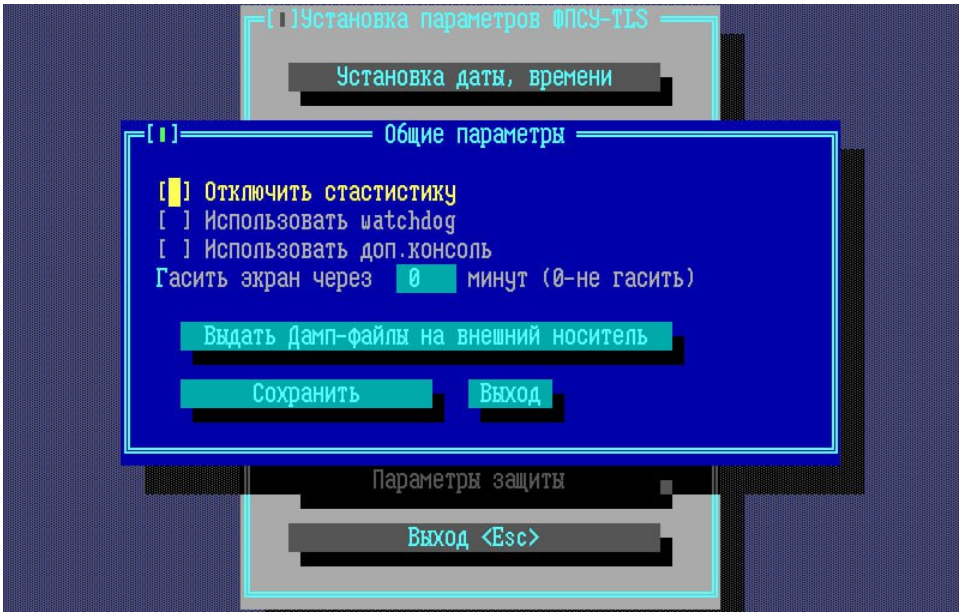


Рисунок 110 - Общие параметры

Отключить статистику – администратор может ввести ограничения на типы статистики, собираемой ФПСУ-TLS. По умолчанию никаких ограничений не выставлено, собирается статистическая информация обо всех происходящих на ФПСУ-TLS событиях и TLS-соединениях. Флаг «Отключить статистику» ограничивает запись статистической информации на ФПСУ-TLS.

Использовать watchdog **–** данный флаг позволяет активировать автоматическую

перезагрузку ФПСУ-TLS при аппаратном или программном сбое комплекса. При включении таймера активизируется аппаратный таймер и его программный аналог, который реализован в операционной системе и не зависит от материнской платы. В случае задействования обоих датчиков, порядок их срабатывания следующий: через 30 секунд после зависания ФПСУ-TLS должен сработать программный датчик, перегрузив ФПСУ-TLS, если программный датчик не сработал в течение 5 минут, сработает аппаратный watchdog.

Использовать доп консоль – при установлении флага происходит переключение на 3 консоль. на некоторых платформах данное переключение не происходит автоматически, требуется включение данного флага.

Гашение экрана – в ряде случаев при работе ФПСУ-TLS возникает необходимость визуально отслеживать происходящие на экране события. Если такой необходимости нет, с точки зрения сбережения ресурсов монитора и повышения быстродействия ФПСУ-TLS целесообразно прибегать к гашению экрана. В поле ввода введите время (от 0 до 240 минут), по истечении которого с момента последнего действия администратора (обращения к клавиатуре или к консоли) экран монитора будет автоматически погашен до следующего обращения. Если оставить поле пустым, гашение экрана производиться не будет.

Выдать Дамп-файлы на внешний носитель – команда выдает на внешний носитель дамп, если сохранен в памяти после внезапных перезагрузок или сбоев.

Для возврата в меню настройки ФПСУ-TLS с внесением выполненных изменений в конфигурацию, выполните команду «Сохранить». Кнопка «Выход» предназначена для возврата в меню настройки ФПСУ-TLS без сохранения выполненных изменений.

7. 6. SNMP-клиент

ФПСУ-TLS поддерживает возможность отправки сообщений о происходящих на ФПСУ-TLS событиях по протоколу SNMP. Для этого реализована подсистема, которая отслеживает происходящие на ФПСУ-TLS события и отправляет их в ответ на запросы SNMP-менеджера.

Для перехода к окну настроек параметров SNMP, выполните команду «SYSLOG/SNMP» меню установки параметров ФПСУ-TLS:

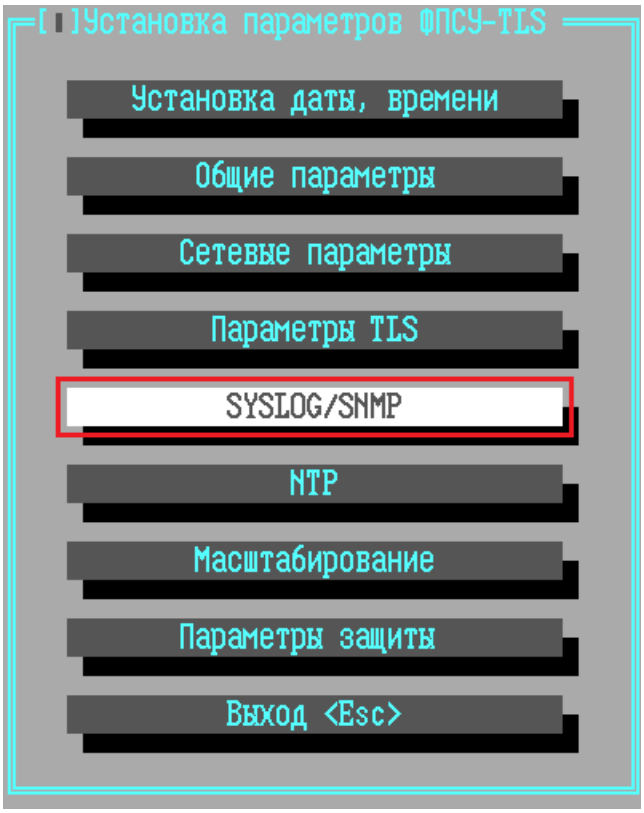


Рисунок 111 - Меню установки параметров ФПСУ-TLS

В правой нижней части окна настройки протокола SysLog и SNMP находится ряд параметров, относящихся к работе протокола SNMP на ФПСУ-TLS. ФПСУ-TLS может работать в качестве SNMP-агента, отвечая на запросы.

Для активации SNMP-агента на ФПСУ-TLS, в области настройки SNMP укажите следующие параметры:

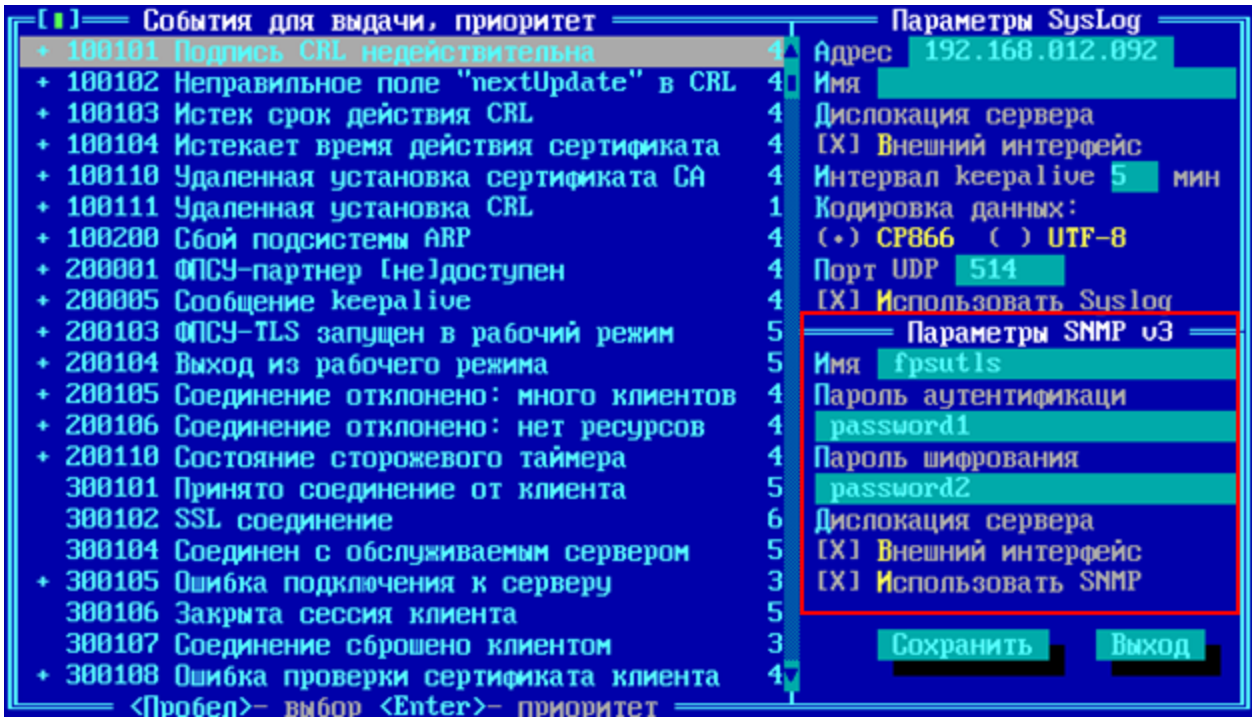


Рисунок 112 - Параметры SNMP

Имя – символьное имя, идентифицирует SNMP агента.

Пароль аутентификации – символьный пароль, указание которого требуется при направлении запроса от SNMP-сервера к работающему на ФПСУ-TLS SNMP-агенту. Поле можно оставить пустым, в таком случае пароль не будет установлен.

Пароль шифрования – символьный пароль, указание которого требуется для шифрования передаваемых данных SNMP-агентом SNMP-серверу.

Дислокация сервера – флаг «Внешний интерфейс» указывает, со стороны какого интерфейса находится SNMP-сервер – внешнего или внутреннего. Если флаг выключен (по умолчанию), то со стороны внутреннего. Если включен – со стороны внешнего сетевого интерфейса.

Использовать SNMP – флаг, включающий/выключающий работу SNMP-ответчика на ФПСУ-TLS. При выключенном флаге взаимодействие ФПСУ-TLS с SNMP-сервером невозможно. Включение или выключение осуществляется клавишей <Пробел>.

Помимо настроек на стороне ФПСУ-TLS, на стороне SNMP-менеджера требуется указать определенные параметры для подключения:

- поддерживаемая версия SNMP-протокола — 3;
- в настройках SNMP-агента используемого SNMP-менеджера следует указать

определенное имя пользователя — «fpsutls». Обратитесь к руководству пользователя используемого SNMP-менеджера для уточнения настраиваемых параметров;

- информация о событиях на ФПСУ-TLS доступна в ветке OID - .1.3.6.1.4.1.37249.

Например, для SNMP-менеджера iReasoning MIB Browser параметры управляемого SNMP-агента выглядят следующим образом:

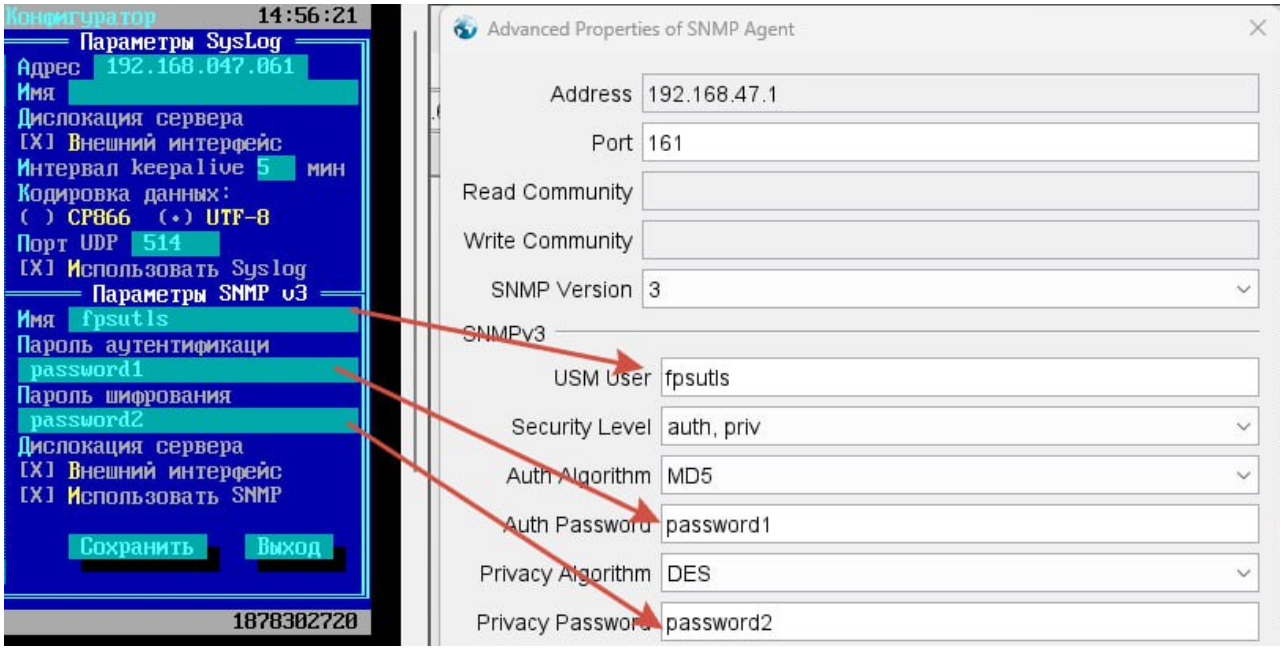


Рисунок 113 - Настройки SNMP-агента ФПСУ-TLS в MIB Browser

Некоторые данные, которые можно получить от ФПСУ-TLS через mib-2 (1.3.6.1.2.1):

1.3.6.1.2.1.2 - Состояние сетевых интерфейсов (скорость, линк, принято/передано ...);

1.3.6.1.2.1.4.2 - TTL по умолчанию;

1.3.6.1.2.1.4.35 - Таблица ARP;

1.3.6.1.2.1.4.21 - Таблица маршрутизации.

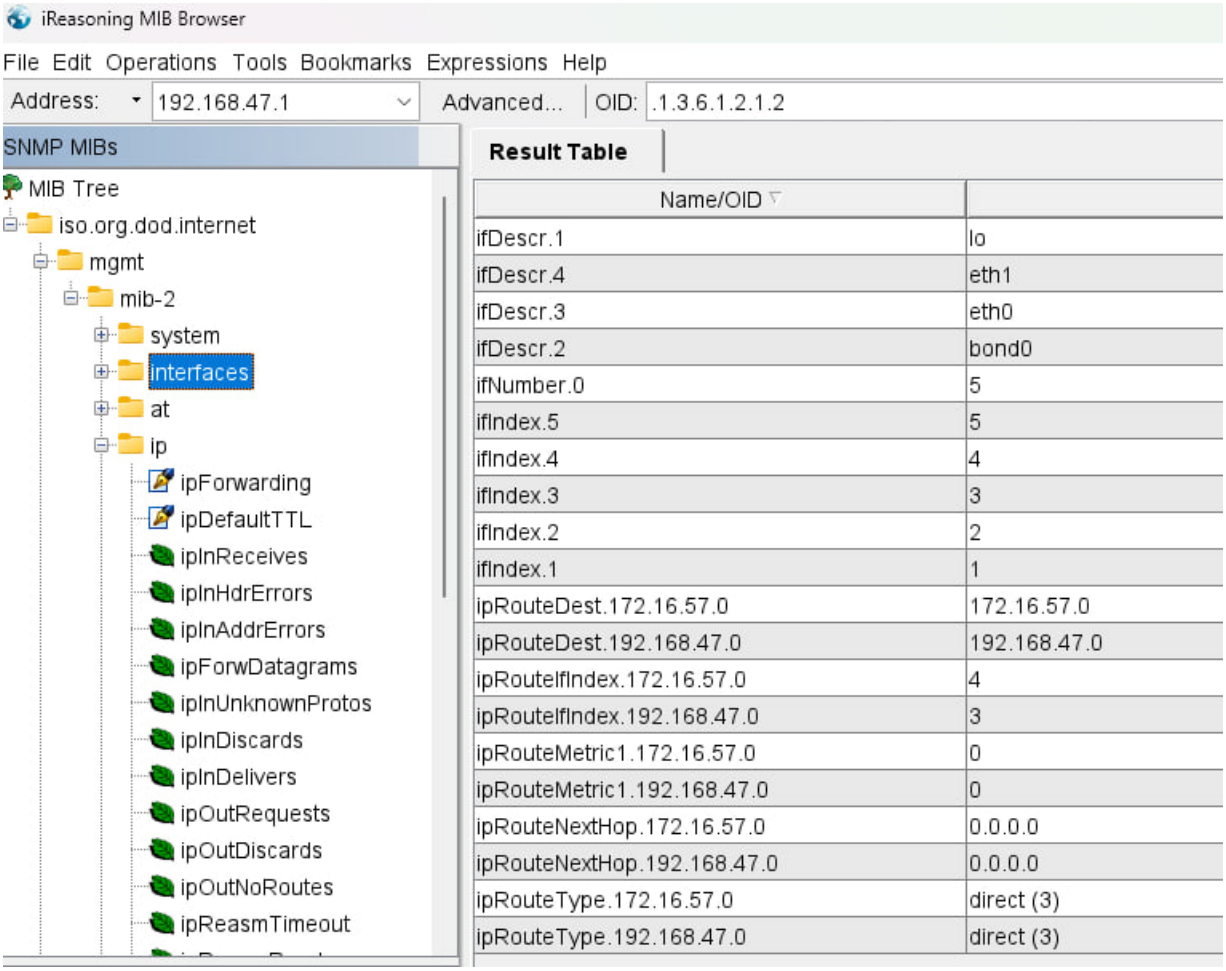


Рисунок 114 - Просмотр элемента MIB-базы в браузере

7. 7. Syslog-клиент

ФПСУ-TLS поддерживает возможность отправки сообщений о происходящих на нём событиях (логов) по протоколу Syslog. Для этого требуется в конфигурации настроить подсистему, которая отслеживает происходящие на ФПСУ-TLS события и отправляет их по протоколу Syslog на указанный сервер.

Для перехода к окну настроек параметров Syslog, выполните команду «SYSLOG/SNMP» меню установки параметров ФПСУ-TLS:

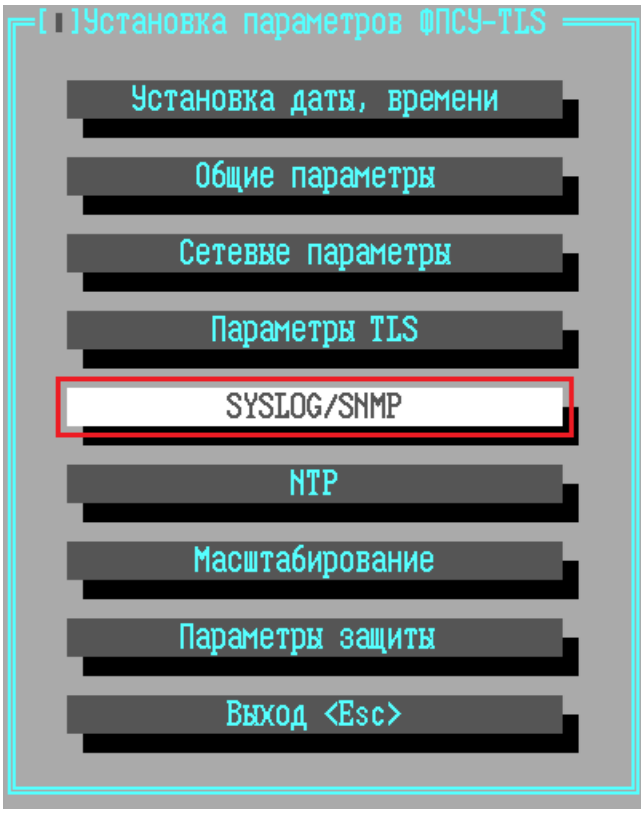


Рисунок 115 - Меню установки параметров ФПСУ-TLS

7. 7. 1. Настройка Syslog событий

В левой части окна расположен список событий, при наступлении которых следует выдать сообщение Syslog серверу.

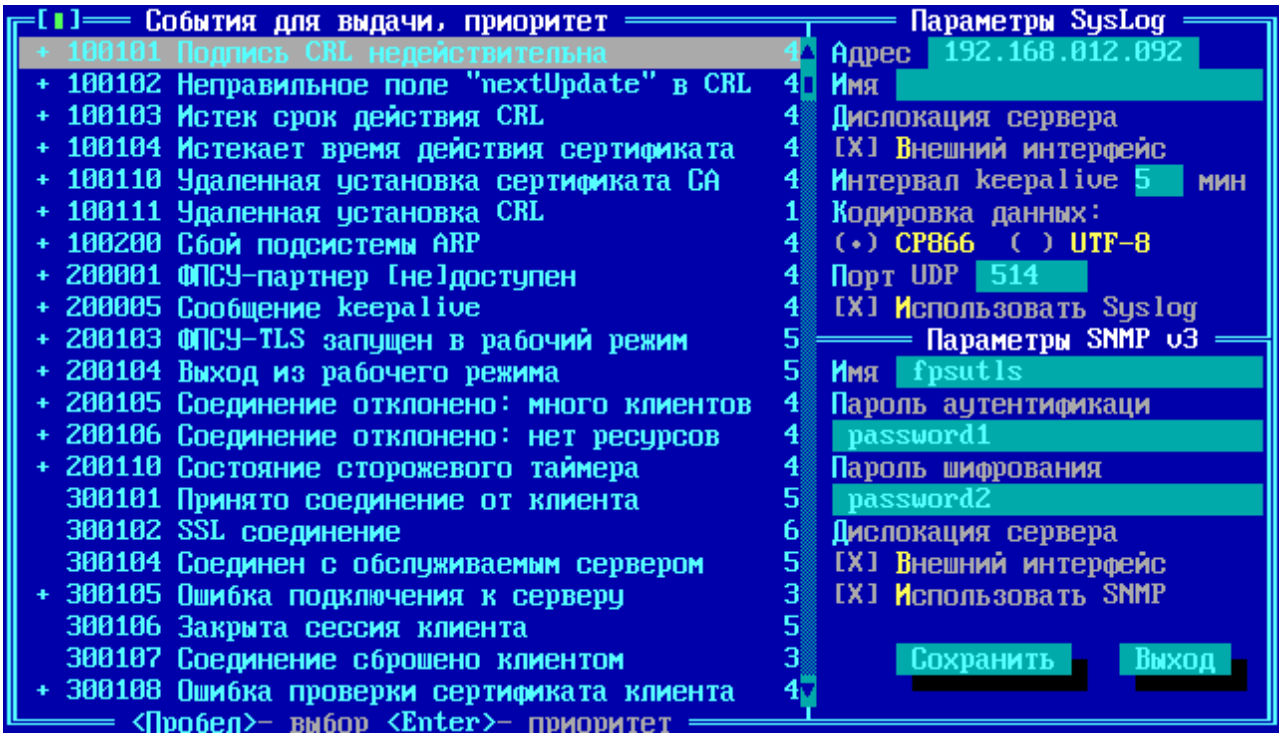


Рисунок 116 - Параметры Syslog и SNMP

Знак «+» около события означает, что оповещение о данном событии будет отправлено серверу Syslog. Включение или выключение отсылки оповещения о событии осуществляется клавишей <Пробел>.

По каждому из отслеживаемых событий ФПСУ-TLS отправляет текстовое Syslog-сообщение, состоящее из нескольких информационных полей.

Формат сообщения имеет вид:

```
fpsu-tls <серийный номер ФПСУ-TLS>: <код события> <причина>
```

Серверу Syslog могут быть отправлены оповещения о событиях, указанных в нижеследующей таблице:

Таблица 5. Оповещения о событиях

Приоритет	**Код события**	**Причина**
4	100101	Подпись CRL недействительна
4	100102	Ошибка CRL: неправильное значение поля nextUpdate

Приоритет	**Код события**	**Причина**
4	100103	Истек срок действия CRL (nextUpdate), необходимо обновить
4	100104	Истекает время действия сертификата. Это сообщение начинает выдаваться за месяц до окончания срока действия сертификата ФПСУ.
4	100110	Удаленная установка сертификата CA. Это сообщение содержит результаты удаленной установки сертификатов. Формат сообщения: 1001100 <серийный номер сертификата>: <результат>. <Результат> может быть одно из: 1) принят, 2) такой сертификат уже есть, 3) ошибка формата, 4) не найден издатель, 5) корневой не разрешен.
4	100111	Удаленная установка CRL
1	100200	Сбой подсистемы ARP
4	100301	Установка даты и времени
4	100302	Изменение параметров конфигурации (сетевые, масштабирования, защиты)
4	100303	Установлен сертификат <серийный номер, имя>
4	100304	Удален сертификат <серийный номер, имя>
4	100305	Создан запрос сертификата
4	100306	Установлен собственный сертификат
5	200001	ФПСУ-партнер недоступен
4	200005	Сообщение keepalive

Приоритет	**Код события**	**Причина**
5	200103	ФПСУ-TLS запущен в рабочий режим
5	200104	Выход из рабочего режима
4	200105	Соединение отклонено: слишком много TLS-клиентов. В этом случае ФПСУ-TLS отвергает новые запросы на соединения.
4	200106	Соединение отклонено: не хватает ресурсов. В этом случае ФПСУ-TLS отвергает новые запросы на соединения.
4	200110	Состояние программного сторожевого таймера. Может быть в состоянии включен и сработал.
6	300101	Принято соединение от клиента. Формат: <система> принято соединение от <IP-адрес>:<порт>
6	300102	SSL соединен: используется предыдущая сессия/ /реализована новая сессия
5	300104	Соединен с обслуживаемым сервером по запросу TLS-клиента. Формат: Соединен <IP-адрес сервера>:<порт>
3	300105	Произошла ошибка при подключении клиента к обслуживаемому серверу. Формат: Ошибка подключения <имя и IP-адрес защищаемого http-сервера> к <IP-адрес TLS-клиента>
5	300106	Сообщение о закрытии сессии клиента. Формат: Соединение сброшено/закрыто: <x> байт передано во внешнюю сеть, <y> байт передано во внутреннюю сеть Клиент: <IP>:<port> Сертификат: [серийный номер] <поле subject из сертификата>
3	300107	Соединение сброшено клиентом.

Приоритет	**Код события**	**Причина**
		Формат: соединение <система> от <IP-адрес> сброшено клиентом
4	300108	Ошибка верификации сертификата клиента Формат: Ошибка верификации: уровень=n, ошибка= <текст ошибки>
4	300109	Сертификат отозван издателем Формат: Сертификат с серийным номером <номер> отозван издателем <имя>
4	300110	Ошибка сокета
4	300111	Ошибка соединения с сервером Формат: Ошибка соединения с сервером <адрес>:<порт> (<имя сервера>)
3	300112	Не определен сервис Формат: не определен сервис: <имя сервиса>
3	300113	IP адрес занесен в «черный список»
3	300114	IP адрес удален из «черного список»

Каждому из событий в соответствии с протоколом Syslog назначается его приоритет, от 0 до 7. Приоритет имеет значение для принимающего сообщение Syslog сервера, и интерпретируется следующим образом:

Таблица 5. Приоритет событий

Приоритет	**Описание**
0	Авария: система неработоспособна (экстренная ситуация или останов системы);
1	Тревога: действия должны быть предприняты немедленно (Срочные ситуации);
2	Критично: критические условия и состояния;

Приоритет	Описание
3	Ошибка: Состояния ошибок (условия ошибки);
4	Предупреждение: условия предупреждений;
5	Извещение: нормальное рабочее состояние, но заслуживающее внимания условие (Необычные состояния);
6	Информация: информационные сообщения;
7	Отладка: сообщения диагностического уровня.

7. 7. 2. Опции работы с Syslog сервером

Кроме списка отправляемых серверу событий, в окне настроек, в правой части, находится ряд опций работы с сервером SysLog, где находятся следующие настраиваемые параметры:

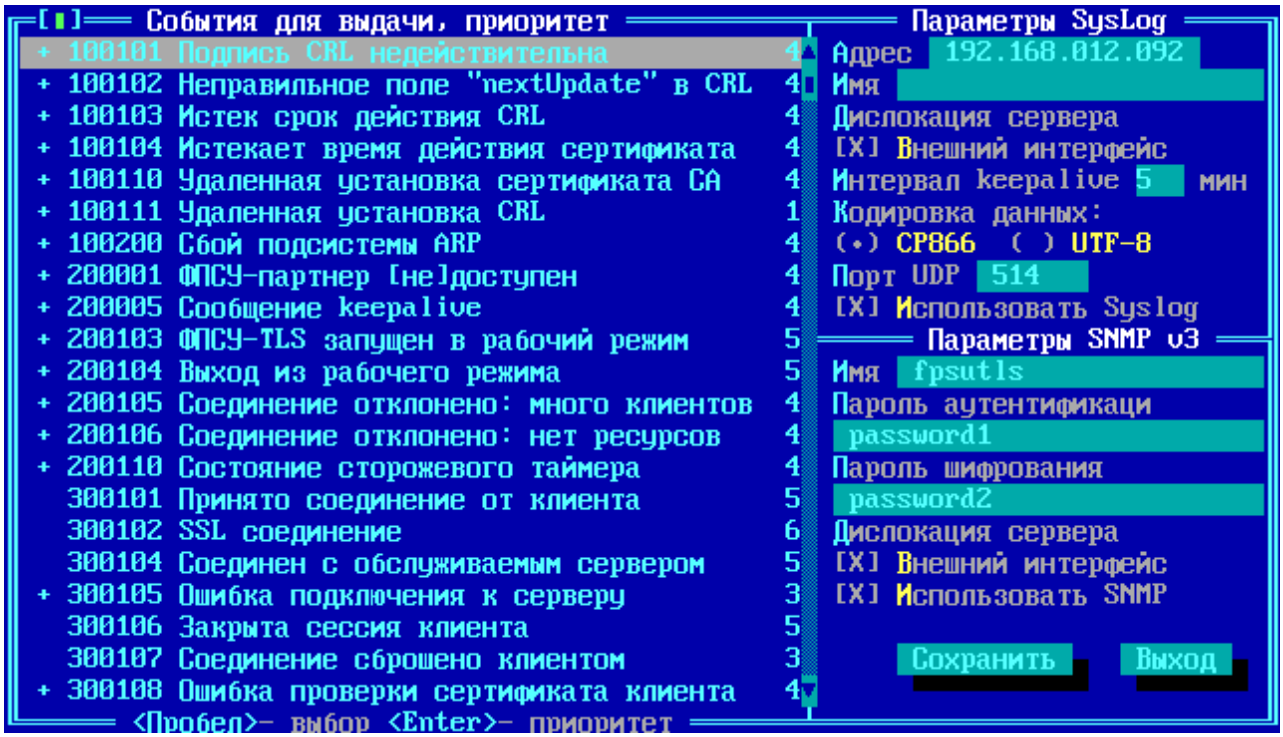


Рисунок 117 - Параметры Syslog и SNMP

Адрес – IP-адрес Syslog сервера, на который следует передавать сообщения о происходящих на ФПСУ-TLS событиях.

Имя – доменное имя Syslog сервера.

Дислокация сервера – флаг «Внешний интерфейс» указывает, со стороны какого интерфейса находится Syslog сервер – внешнего или внутреннего. Если флаг выключен (по умолчанию), то со стороны внутреннего. Если включен – со стороны внешнего сетевого интерфейса.

Интервал keepalive – интервал отправки Syslog серверу специального сообщения keepalive о текущем состоянии ФПСУ-TLS (в минутах).

Сообщение keepalive показывает:

- загрузку процессора, например:

  CPU: 49.8% usr 0.6% sys 0.0% nic 48.9% idle 0.0% io 0.1% irq 0.3% sirq.

  Эти цифры позволяют определить количество процессорного времени, использованного на выполнение различных видов работ:

  - usr – время, затраченное на выполнение процессов в пользовательском режиме;
  - nic – время, затраченное на выполнение процессов в привилегированном пользовательском режиме. Привилегированные процессы выполняются с приоритетом, отличным от приоритета по умолчанию;
  - sys – время, затраченное на выполнение в режиме ядра;
  - idle – время выполнения процесса ожидания;
  - io – время ожидания завершения ввода-вывода;
  - irq – время обработки прерываний;
  - sirq – время обработки прерываний softIRQs;
- количество сессий с момента последнего обнуления счетчика пакетов и данных;
- (в скобках) количество установленных сессий;
- количество переданных данных в открытую сеть;
- количество переданных данных в защищаемую сеть.

Кодировка данных – выбор кодировки, в которой будет отправлено текстовое сообщение от ФПСУ-TLS к Syslog серверу.

Порт UDP – выбор номера UDP-порта Syslog сервера (по умолчанию 514).

Использовать Syslog – флаг, включающий/выключающий работу с указанным в поле «Адрес» Syslog сервером. При выключенном флаге обработка и отправка сообщений Syslog

серверу не происходит. Включение или выключение осуществляется клавишей <Пробел>.

7. 8. Дата и время ФПСУ-TLS

Для корректировки текущих даты и времени на ФПСУ-TLS предусмотрены следующие возможности:

- изменение даты и времени в процессе работы по специальной команде меню установки параметров ФПСУ-TLS вручную администратором;
- автоматическая синхронизация времени на ФПСУ-TLS с NTP-сервером.

7. 8. 1. Коррекция даты и времени по команде администратора

Для изменения текущих даты и времени на ФПСУ-TLS вручную администратором выполните команду меню установки параметров ФПСУ-TLS «Установить дату, время»:

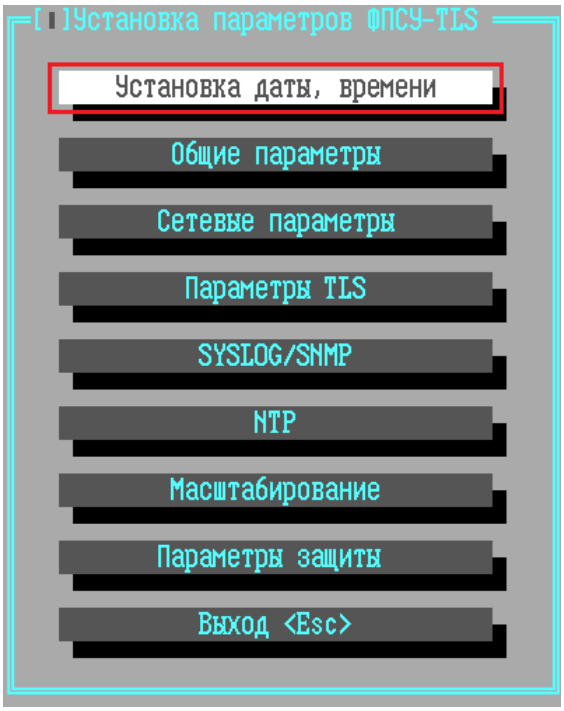


Рисунок 118 - Меню установки параметров ФПСУ-TLS

На экран будет выдано диалоговое окно установки:

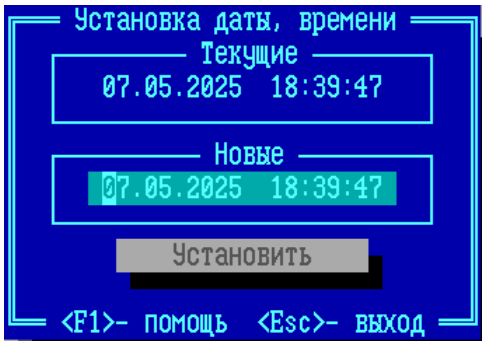


Рисунок 119 - Диалог установки времени на ФПСУ-TLS

Введите в поле «Новые» актуальные значения даты и времени примените выполненные изменения, нажав кнопку «Установить». Для возврата в меню установки параметров ФПСУ-TLS нажмите клавишу <Esc>.

7. 8. 2. Синхронизация даты и времени с NTP-сервером

ФПСУ-TLS позволяет установить режим автоматической коррекции времени ФПСУ-TLS по данным сервера, работающего по протоколу NTP (Network Time Protocol).

В таком режиме, независимо от текущих выполняемых задач, ФПСУ-TLS периодически запускает механизм NTP-ассоциации, посылая указанному NTP-серверу запросы на получение точного времени. Если отклонение составляет более 2 секунд, время на ФПСУ-TLS будет синхронизировано со временем NTP-сервера.

Для установки режима синхронизации времени на ФПСУ-TLS со временем NTP-сервера выполните команду «NTP» меню установки параметров ФПСУ-TLS:

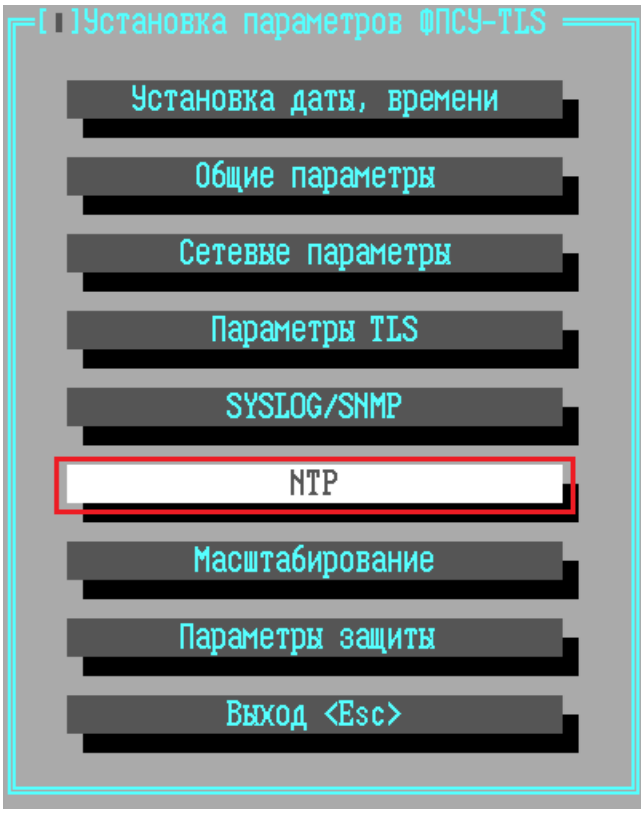


Рисунок 120 - Меню установки параметров ФПСУ-TLS

На экран будет выдано диалоговое окно установки параметров:

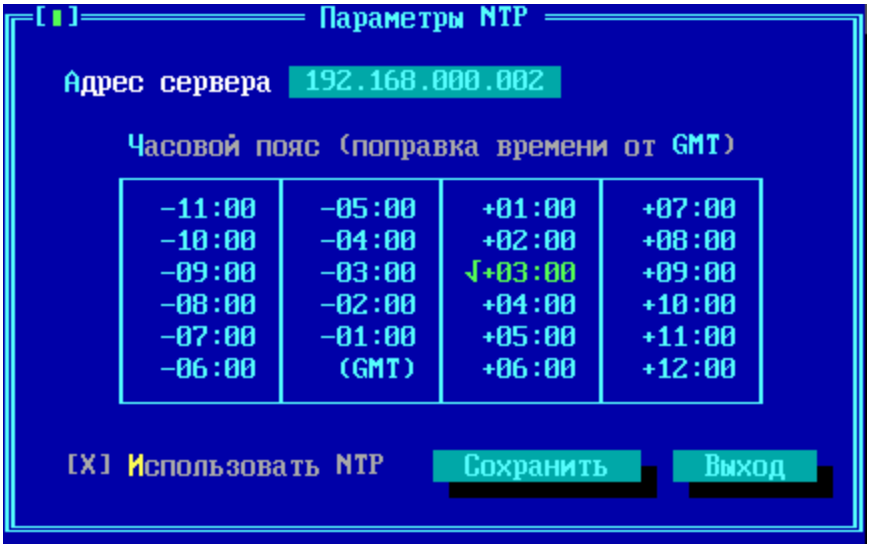


Рисунок 121 - Установка параметров взаимодействия с NTP-сервером

В поле диалогового окна ***«Адрес сервера»*** введите IP-адрес NTP-сервера, с которым будет осуществляться синхронизация времени.

В таблице ***«Часовой пояс (поправка времени от GMT)»*** выберите курсором и установите нажатием клавиши <Пробел> часовой пояс используемого на ФПСУ-TLS времени.

Автоматическая синхронизации времени на ФПСУ-TLS со временем NTP-сервера будет выполняться только в том случае, если флаг ***«Использовать NTP»*** установлен в положение [X]. Включение и выключение флага производится нажатием клавиши <Пробел>.

Для возврата в меню настройки ФПСУ-TLS с внесением выполненных изменений в конфигурацию, выполните команду ***«Сохранить»***.

Кнопка ***«Выход»*** предназначена для возврата в меню настройки ФПСУ-TLS без сохранения выполненных изменений.

7. 9. Просмотр установленных сертификатов

Команда меню установки параметров ФПСУ-TLS «Сертификаты УЦ» открывает окно, в котором выводится список установленных на ФПСУ-TLS сертификатов:

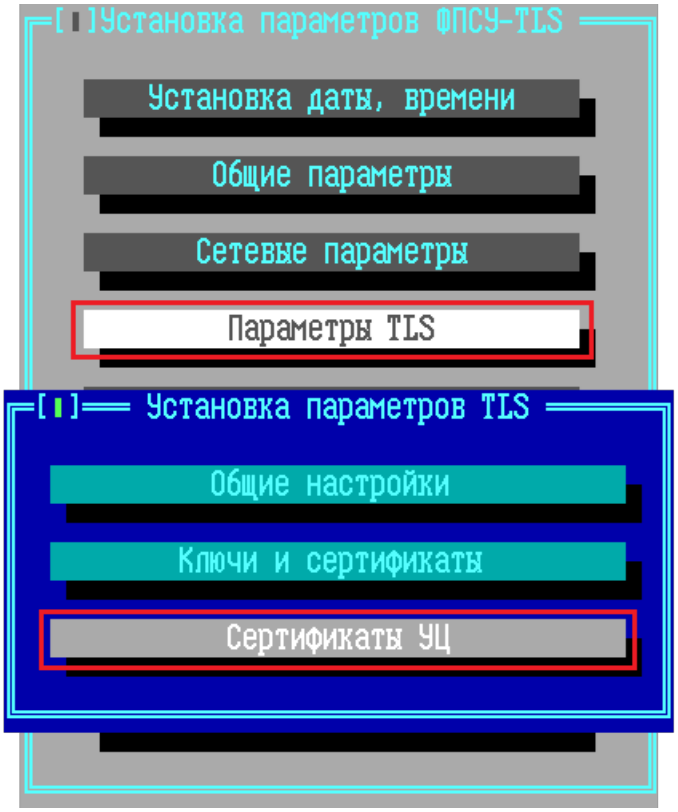


Рисунок 122 - Меню установки параметров ФПСУ-TLS

При выполнении команды на экран будет выведено служебное окно с полным списком установленных на ФПСУ-TLS сертификатов – корневых и некорневых сертификатов Удостоверяющих Центров, текущий и следующий личный сертификаты ФПСУ-TLS:

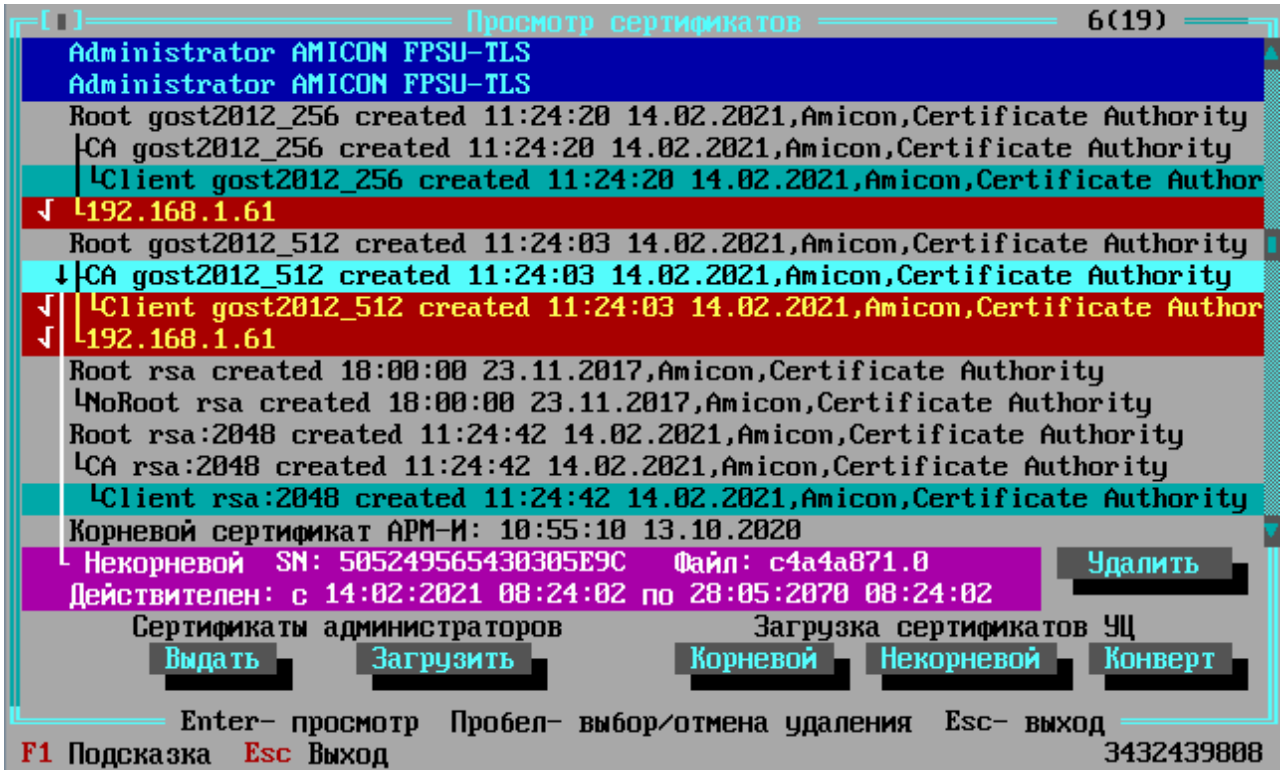


Рисунок 123 - Просмотр списка сертификатов

Для просмотра параметров сертификата выделите его курсором и нажмите клавишу <Enter>. Откроется окно, содержащее информацию о выбранном сертификате в соответствии с типом сертификата.

Для возврата к списку хранящихся на ФПСУ-TLS сертификатов перейдите с помощью клавиши <Tab> на поле «Выход» и активируйте его, нажав клавишу <Enter>.

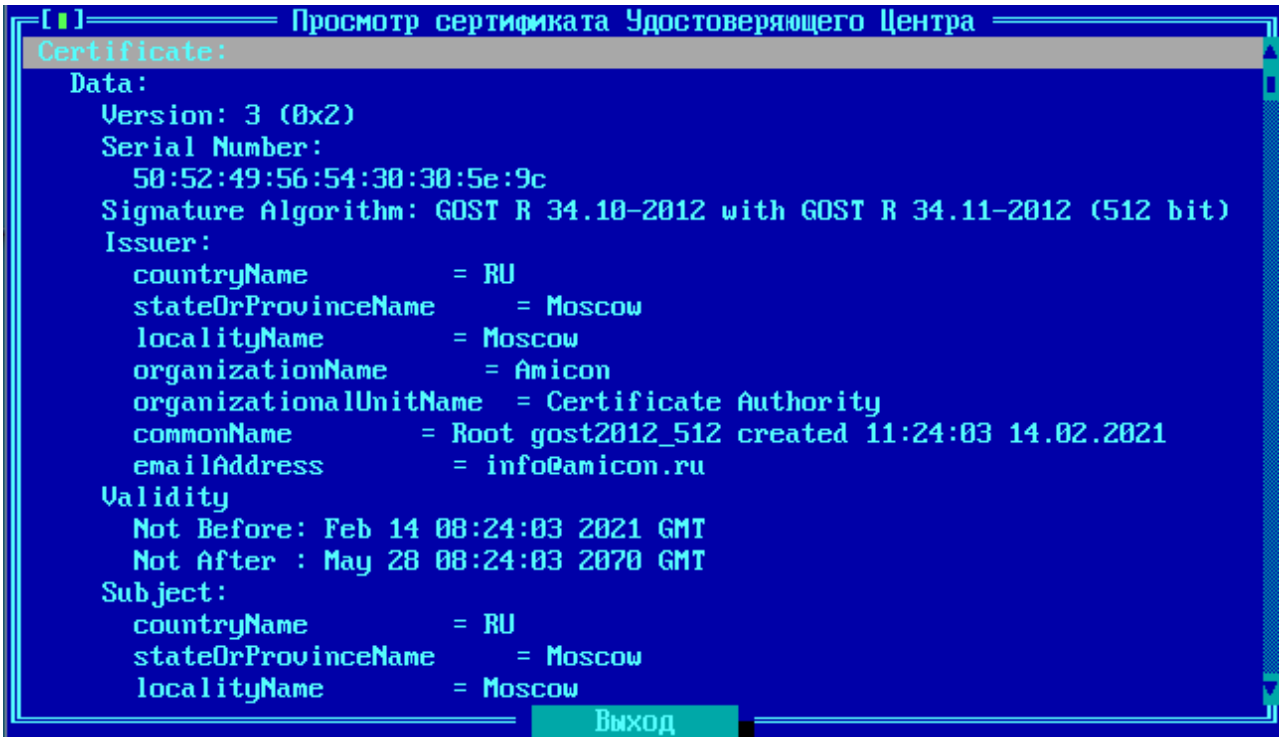


Рисунок 124 - Просмотр сертификата

7. 10. Параметры защиты ФПСУ-TLS

На ФПСУ-TLS могут быть включены механизмы защиты от атак на TLS-службу, принимающую входящие клиентские соединения. Для перехода в окно настройки таких механизмов контроля TLS-сервера, выполните команду «Параметры защиты» меню конфигурации ФПСУ-TLS:

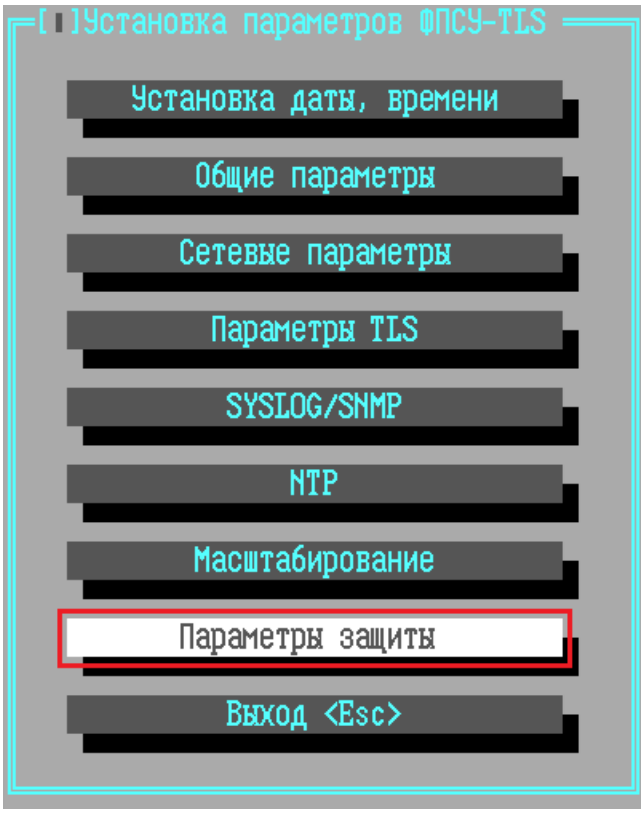


Рисунок 125 - Меню конфигурации ФПСУ-TLS

В открывшемся окне «Параметры защиты» администратор ФПСУ-TLS может выполнить следующие настройки:

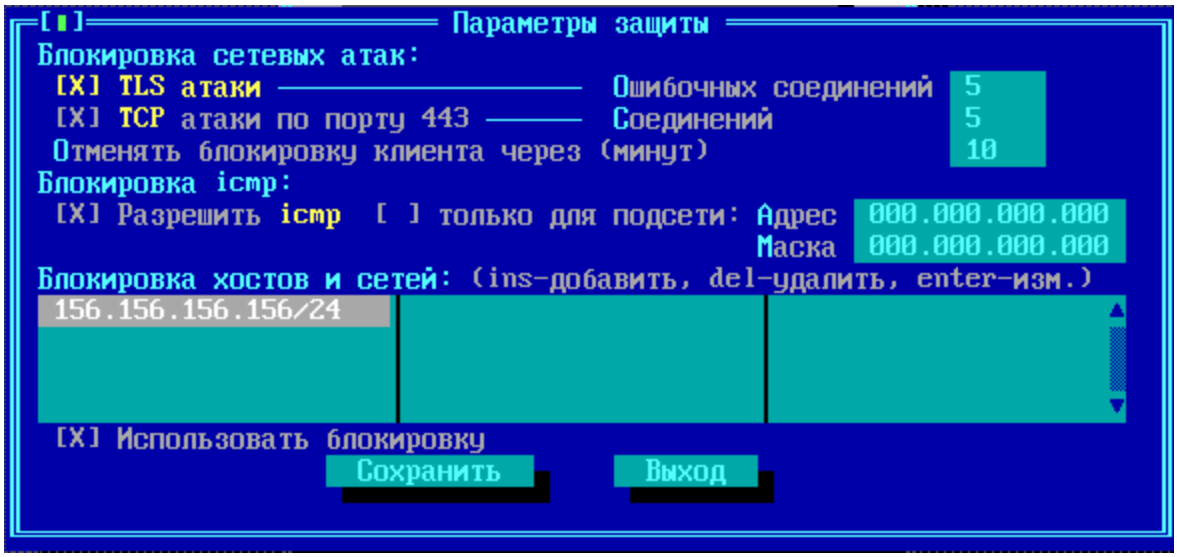


Рисунок 126 - Параметры защиты

TLS атаки – флаг, активирующий механизм контроля сетевых атак, основанных на установлении TLS-соединений с некорректными параметрами (неверно указан протокол,

используемая криптографическая система, неверные ключевые данные, ошибки в TLS-заголовках и т.д.). В поле «Ошибочных соединений» указывается количество таких попыток в секунду, после чего IP-адрес источника соединений будет заблокирован на указанное в поле «Отменять блокировку клиента через» время, в минутах.

TCP атаки по порту 443 – флаг, активирующий механизм контроля сетевых атак, основанных на установлении TCP соединения (TCP-Syn атака). В поле «Соединений» указывается количество таких попыток в секунду, после чего IP-адрес источника соединений будет заблокирован на указанное в поле «Отменять блокировку клиента через» время, в минутах.

Разрешить ICMP – флаг, указывающий ФПСУ-TLS отвечать на ICMP (ECHO) запросы в его собственные IP-адреса. Может быть установлено ограничение ответа на эхо-запросы только из указанной подсети, необходимо установить флаг «Только для подсети» и задать адрес и маску подсети, в таком случае эхо-запросы из других подсетей будут сброшены.

Блокировка хостов и сетей – в этот список следует добавить хосты и подсети, которые не будут иметь доступа к данному ФПСУ-TLS.

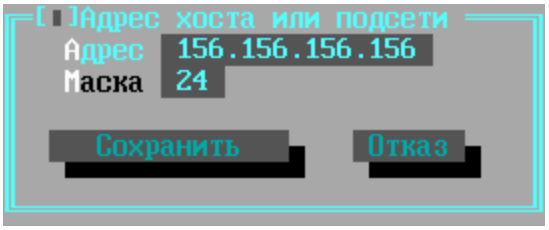


Рисунок 127 - Задание блокировки IP-адреса хоста

Использовать блокировку – установленный флаг активирует настройки блокировки хостов и сетей.

Для возврата в меню настройки ФПСУ-TLS с внесением выполненных изменений в конфигурацию, выполните команду «Сохранить». Кнопка «Выход» предназначена для возврата в меню настройки ФПСУ-TLS без сохранения выполненных изменений.

7. 11. Настройка системы

Опция главного меню ФПСУ-TLS, «Настройка системы», предназначена для установки параметров и режимов работы подсистемы регистрации локальных администраторов (электронных ТМ-идентификаторов) и подсистемы установки дополнений/изменений.

Рисунок 128 - Вызов меню настройки системы

При выборе опции «Настройка системы» откроется подменю:

- «Регистрация ТМ-идентификаторов» (см. пункт «Регистрация ТМ-идентификаторов»);
- «Установка дополнений/изменений» (см. пункт «Обновление программного обеспечения»);
- «Установка пароля администратора» (см. пункт «Установка пароля администратора»);
- «Регистрация Удаленных Администраторов» (см. пункт Регистрация удаленных администраторов»);
- «Просмотр статистики» (см. пункт «Просмотр статистики»);
- «Настройки СКЗИ» (см. пункт «Настройки СКЗИ»).

Рисунок 129 - Меню настройки системы

7. 11. 1. Регистрация ТМ-идентификаторов

Команда «Регистрация ТМ-идентификаторов» меню «Настройка системы» ФПСУ-TLS предназначена для выполнения следующих операций:

- регистрации новых локальных администраторов ФПСУ-TLS (записи их идентификационной информации на ТМ);
- управления паролями для учетных записей локальных администраторов ФПСУ-TLS;
- удаления на потерявших актуальность или скомпрометированных ТМ записанной идентификационной информации;
- проверки корректности хранимой в ТМ идентификационной информации и исправности ТМ-идентификатора;
- разрешения или запрещение использования подсистемы автоматического старта.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для

авторизации в системе.

Рисунок 130 - Подтверждение полномочий и ввод пароля ТМ

При выполнении команды «Регистрация ТМ-идентификаторов» меню «Настройка системы» ФПСУ-TLS на экран будет выведено окно, показывающее наличие зарегистрированных администраторов ФПСУ-TLS (ТМ-идентификаторов), и состояние подсистемы автоматического старта.

Ячейке таблицы «Администратор» - «Основная ТМ» соответствует пользователь класса «*Главный администратор*». Ячейке таблицы «Администратор» - «Запасная ТМ» соответствует пользователь класса «*Администратор*». Ячейкам таблицы строки «Инженер» соответствуют пользователи класса «*Инженер*». Ячейкам таблицы строк «Оператор 1», «Оператор 2», «Оператор 3» и «Оператор 4» соответствуют пользователи класса «*Оператор*».

Рисунок 131 - Меню регистрации администраторов

Для зарегистрированных ТМ-идентификаторов могут быть осуществлены следующие операции:

- основной ТМ администратора может быть проверен на исправность и корректность хранимой идентификационной информации;
- ТМ остальных учетных записей (запасной ТМ-идентификатор администратора, основной и запасной ТМ-идентификатор инженера) могут быть проверены, очищены или перерегистрированы;
- для каждого ТМ-идентификатора может быть задан пароль.

Основной ТМ администратора зарегистрирован быть не может, он перерегистрируется только на этапах инсталляции или перехода из технологического в рабочий режим на ТМ, поставляемый вместе с ФПСУ-TLS.

Новый ТМ-идентификатор может быть только зарегистрирован как запасной для администратора, либо основной/запасной для любой другой учетной записи.

ВНИМАНИЕ! На ФПСУ-TLS должны быть зарегистрированы минимум два ТМ-идентификатора, один из которых ТМ Главного администратора, иначе при закрытии регистратора ТМ-идентификаторов он будет открываться снова, блокируя дальнейшую работу.

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ФПСУ-TLS классов КС2, и опциональным для ФПСУ-TLS

класса КС1.

Пароль основного ТМ-идентификатора выбранного класса администратора задается в окне регистрации ТМ, пароль запасного ТМ-идентификатора выбранного класса администратора задается при перерегистрации ТМ.

Примечание. Не используемый ТМ-идентификатор любого класса пользователей ФПСУ-TLS, кроме ТМ Главного администратора, может быть удален и в дальнейшем зарегистрирован с любым другим классом пользователей. ТМ-идентификатор может быть перерегистрирован с тем же классом пользователей, в этом случае ключевая информация удаляется и записываются новые ключевые данные на ТМ.

Разрешенные для текущей записи действия выполняются при помощи следующих клавиш:

- <Ins> – регистрация или перерегистрация ТМ выбранной учетной записи, установка пароля;
- <Del> – очистка ТМ-идентификатора выбранной учетной записи;
- <Enter> – проверка исправности и корректности находящейся на ТМ информации для выбранной учетной записи.

При выполнении операций по регистрации или очистке система будет требовать подтверждения полномочий администратора (прижатием основного или запасного ТМ-идентификатора учетной записи «Администратор» к считывателю ТМ) с целью предотвращения несанкционированных действий.

Внесенные в настройки изменения сохраняются автоматически.

При выполнении операций по регистрации, проверке или очистке ТМ система будет требовать подтверждения полномочий администратора (посредством подключения ТМ-идентификатора к USB-порту ФПСУ-TLS) с целью предотвращения несанкционированных действий.

При выборе зарегистрированного ТМ-идентификатора и нажатии клавиши <*Enter*>, подключенный ТМ-идентификатор отображается в меню регистрации ТМ-идентификаторов как «Правильный». На рисунке ниже слева выбран основной ТМ-идентификатор администратора, по нажатию клавиши <*Enter*> отображается результат проверки - «Правильный», этот ТМ-идентификатор подключен к ФПСУ-TLS. На рисунке ниже справа выбран запасной ТМ-идентификатор администратора, по нажатию клавиши <*Enter*> отображается результат проверки - «Неправильный», этот ТМ-идентификатор не подключен

к ФПСУ-TLS.

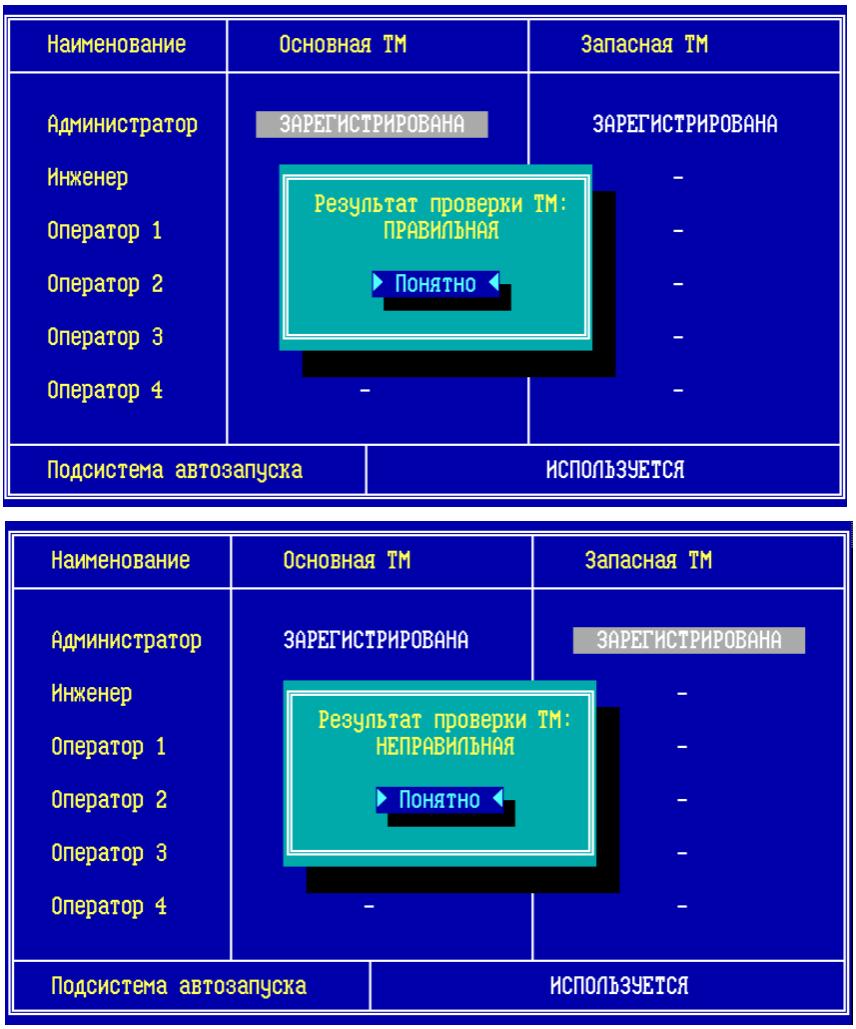


Рисунок 132 - Проверка подключенного ТМ-идентификатора администратора

Выход из окна Регистратора ТМ с возвратом в меню «Настройки системы» ФПСУ-TLS осуществляется по сочетанию клавиш <*ALT*>+<*X*>.

7. 11. 1. 1. Установка пароля Главного администратора

Пароли администраторов ФПСУ-TLS всех классов (см. пункт «Разграничение доступа и пользователи») устанавливаются/изменяются в окне регистрации ТМ. Операция доступна администраторам класса *Администратор* и выше.

Для установки пароля Главного администратора: выделите ячейку *Администратор-Основная ТМ* и нажмите клавишу <*Ins*>, на экране отобразится запрос на задание/изменение пароля основного ТМ. Нажмите «Да» для задания пароля:

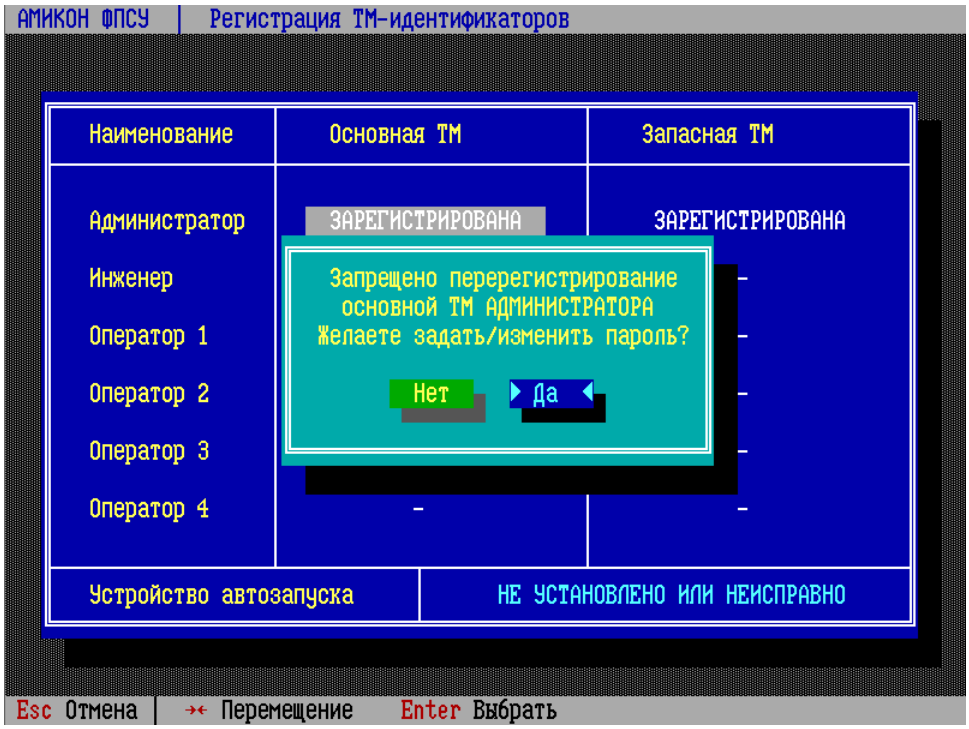


Рисунок 133 - Установка/изменение пароля ТМ

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не будут отображаться на экране, подсистема попросит ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля будет произведена только после повторного введения идентичной комбинации символов.

В операции проверки пароля участвуют ASCII-коды символов, поэтому администратор должен быть внимателен к набору символов в определенных регистре и алфавите.

После установки пароля при попытке изменить конфигурацию ФПСУ-TLS (выборе соответствующей команды) подсистема будет блокировать любые действия администратора до ввода установленного пароля.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <*Enter*>. В открывшемся окне повторно ввести пароль и нажать клавишу <*Enter*>.

Рисунок 134 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы), и нажать <*Enter*>.

Пароль для основного ТМ выбранного класса администратора установлен.

7. 11. 1. 2. Регистрация запасного ТМ

Повторная регистрация запасного ТМ-идентификатора проводится в случае замены ключевой информации ТМ-идентификатора или при компрометации ТМ-идентификатора.

Для выполнения необходимо предъявить ТМ-идентификатор класса Администратор а также регистрируемый запасной ТМ-идентификатор выбранного класса.

Уточнение: при регистрации запасного ТМ-идентификатора администратора требуется ТМ Главного администратора для подтверждения права регистрации и запасной ТМ для регистрации.

Для регистрации запасного ТМ-идентификатора выбранного класса выделите ячейку с запасным ТМ и нажмите клавишу <*Ins*>, на экране отобразится запрос на перерегистрацию ТМ.

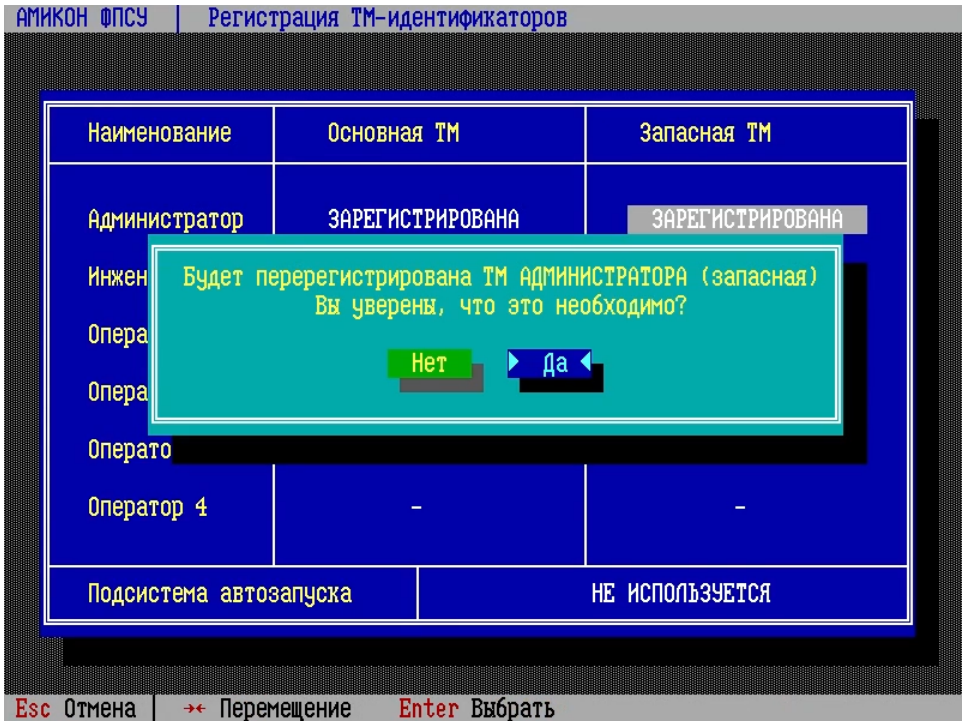


Рисунок 135 - Перерегистрация ТМ

По нажатию кнопки «Да» ТМ будет зарегистрирован заново.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 136 - Подтверждение полномочий и ввод пароля ТМ

Затем необходимо убрать ТМ-идентификатор администратора и предъявить запасной ТМ-идентификатор для его регистрации.

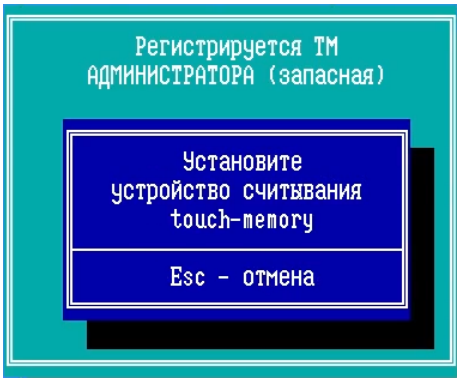


Рисунок 137 - Предъявление запасного ТМ для регистрации

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ФПСУ-TLS классов КС2, и опциональным для ФПСУ-TLS класса КС1.

Рекомендуется установить пароль зарегистрированного ТМ-идентификатора, на экране отобразится запрос на установление пароля ТМ.

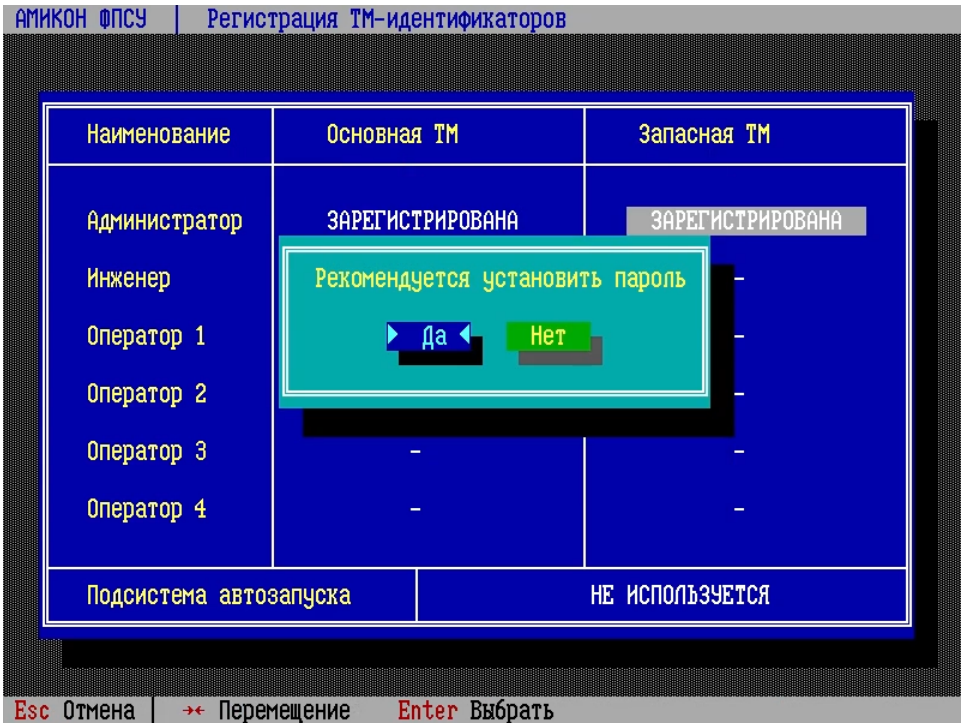


Рисунок 138 - ТМ перерегистрирован

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не будут отображаться на экране, подсистема попросит ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля будет произведена только после повторного введения идентичной комбинации символов.

В операции проверки пароля участвуют ASCII-коды символов, поэтому администратор должен быть внимателен к набору символов в определенных регистре и алфавите.

После установки пароля при попытке изменить конфигурацию ФПСУ-TLS (выборе соответствующей команды) подсистема будет блокировать любые действия администратора до ввода установленного пароля.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <*Enter*>. В открывшемся окне повторно ввести пароль и нажать клавишу <*Enter*>.

Рисунок 139 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы), и нажать <*Enter*>.

В случае если запасной ТМ-идентификатор в процессе ввода пароля был отключен, необходимо повторно предъявить его для добавления пароля.

Рисунок 140 - Предъявление запасного ТМ

После подключения запасной ТМ-идентификатор зарегистрирован с установлением пароля.

7. 11. 1. 3. Удаление ТМ

При удалении записанной на потерявшем актуальность или скомпрометированном ТМ-идентификаторе ключевой информации требуется предъявить ТМ администратора и ТМ-идентификатор, который очищается, чтобы провести удаление ключевых данных. При выполнении операции по очистке ключевых данных ТМ-идентификатора система будет требовать подтверждения полномочий администратора с целью предотвращения несанкционированных действий.

Отказаться от операции удаления ТМ можно, нажав клавишу <Esc>.

Для удаления перейдите в соответствующее ТМ-идентификатору поле таблицы, например ТМ инженера, и нажмите клавишу <*Delete*>. На экране отобразится запрос:

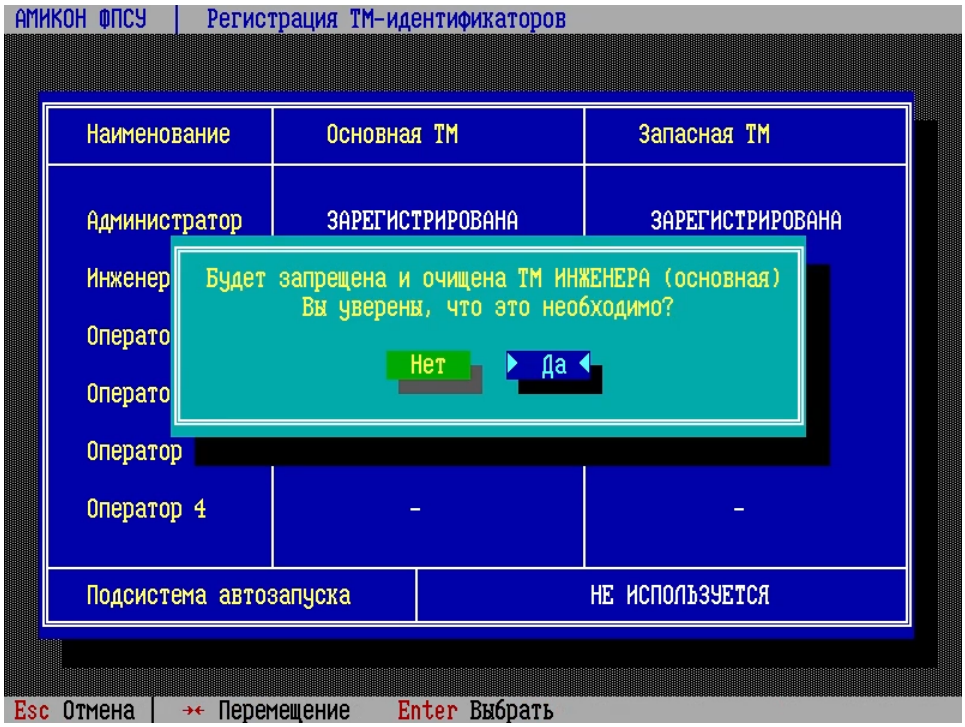


Рисунок 141 - Удаление ТМ

По нажатию кнопки «Да» будет запущен процесс удаления ТМ.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 142 - Подтверждение полномочий и ввод пароля ТМ

Затем необходимо убрать ТМ-идентификатор администратора и предъявить ТМ-идентификатор инженера для его удаления. При этом соответствующий ТМ-идентификатору ключ запуска будет удален с ФПСУ-TLS.

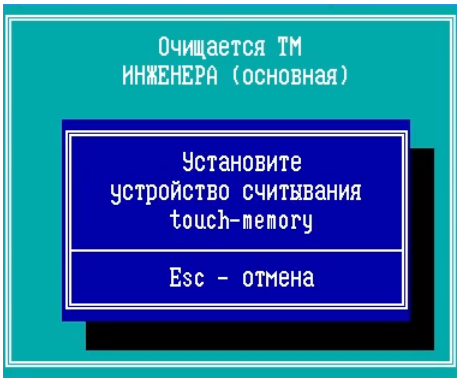


Рисунок 143 - Предъявление ТМ инженера для удаления

ТМ-идентификатор инженера удален.

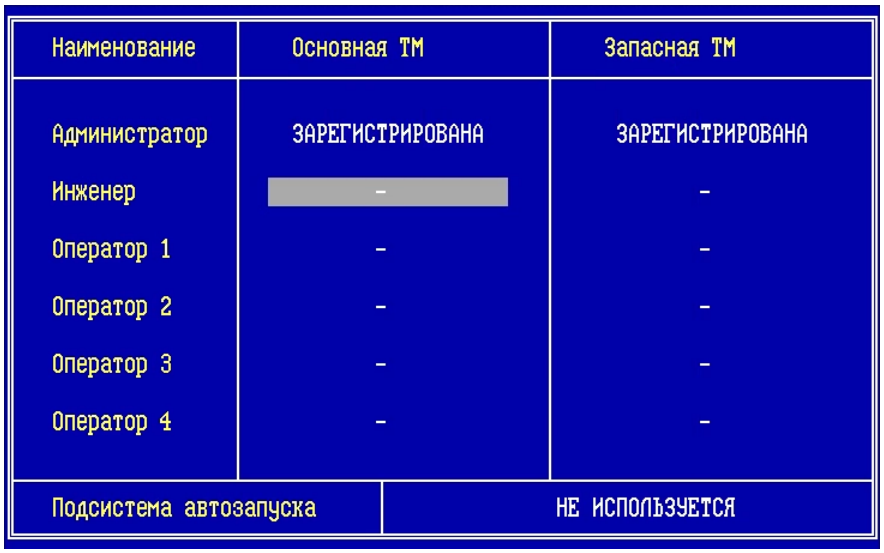


Рисунок 144 - Окно регистратора ТМ

7. 11. 2. Включение подсистемы автоматического старта

Для включения подсистемы автоматического старта:

Перейдите в поле «Подсистема автозапуска» и нажмите клавишу <*Ins*>. Подтвердите в появившемся окне включение режима автоматического старта, выбрав ответ «Да»;

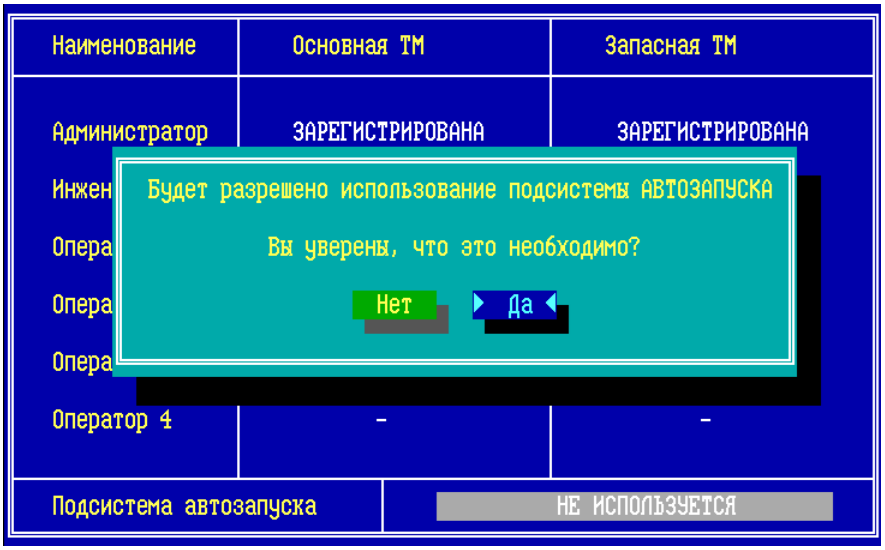


Рисунок 145 - Включение подсистемы автозапуска ФПСУ-TLS

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-

считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 146 - Подтверждение полномочий и ввод пароля ТМ

Режим работы подсистемы автозапуска изменится на «Используется». Подсистема автозапуска включена.

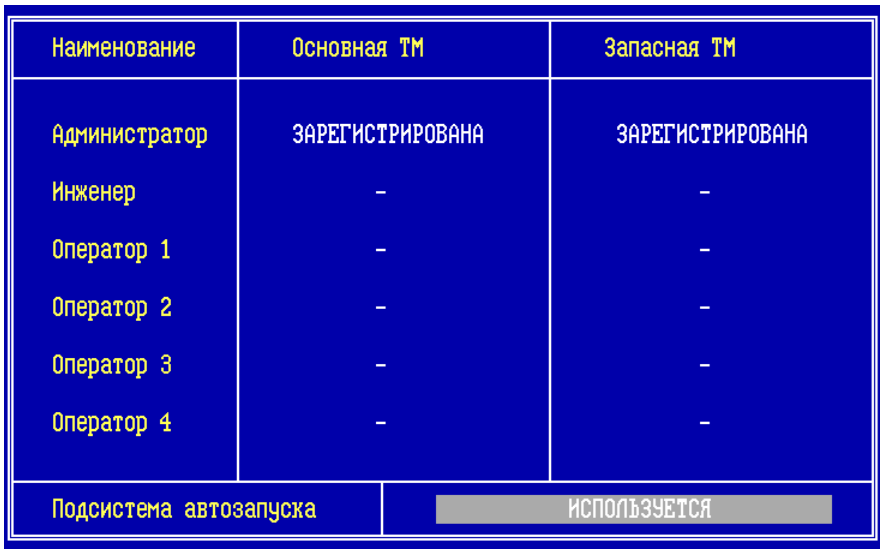


Рисунок 147 - Подсистема автозапуска ФПСУ-TLS включена

При включении электропитания, ФПСУ-TLS с активированной подсистемой автозапуска будет выполнять запуск системы в рабочий режим.

Для выключения подсистемы автоматического старта перейдите в поле «Подсистема автозапуска» и нажмите клавишу <Del>. Подтвердите в открывшемся окне выключение режима автоматического старта, нажав кнопку «Да».

После подтверждения выполнения команды, подсистема автозапуска будет отключена.

7. 11. 3. Обновление программного обеспечения

Опция подменю «Настройка системы → Установка дополнений/изменений» предназначена для установки новых программных модулей или обновлений существующих модулей ФПСУ-TLS.

Рисунок 148 - Переход в меню установки дополнений/изменений

Все изменения или дополнения должны быть получены от организации-поставщика ФПСУ-TLS.

Файлы с изменениями должны сопровождаться контрольными суммами, которые следует проверить перед установкой обновлений или дополнений. Проверка производится

вычислением программой контроля целостности FPSUHASH хэш-функции от файла с обновлениями и сравнением полученного результата с контрольными данными. Программа FPSUHASH и файл с контрольными данными UPDATE.HSH поставляется вместе с файлами обновления. Проверку целостности файлов обновления следует выполнять в соответствии с документом РОФ.ПЕРС.000104-01 34 01, «Программа контроля целостности файлов. Руководство оператора», который размещен на сайте https://wiki.amicon.ru/FPSUHash/2.0/, может также поставляться вместе с файлами обновления.

Для установки обновления программного обеспечения ФПСУ-TLS выполните следующие действия:

Скопируйте полученные от организации-поставщика ФПСУ-TLS файлы, содержащие обновления программного обеспечения на внешний носитель (USB-flash), и подключите носитель к ФПСУ-TLS (USB-порту).

Для начала установки обновления выполните команду главного меню ФПСУ-TLS, «Настройка системы → Установка дополнений/изменений».

Операция доступна администратору класса *Главный администратор* (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

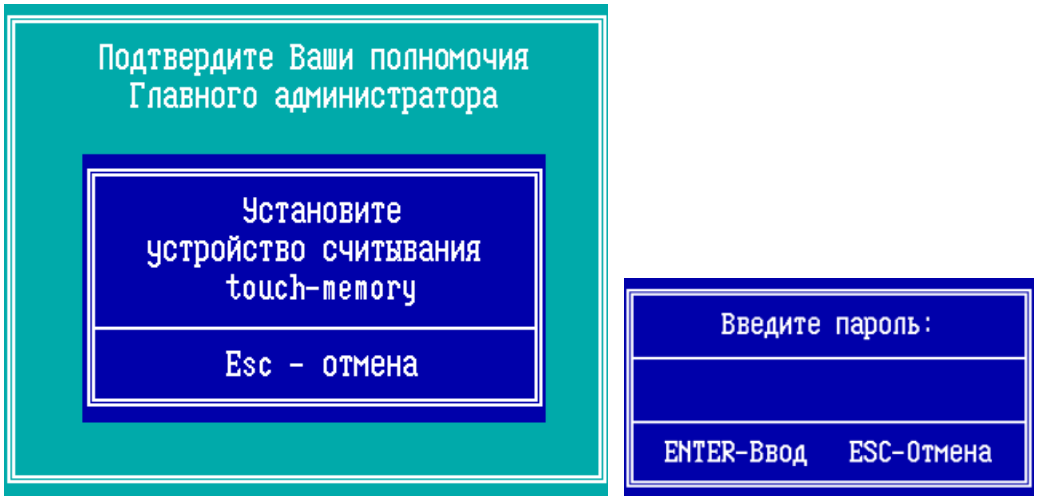


Рисунок 149 - Подтверждение полномочий и ввод пароля ТМ

Подключите USB-носитель к АП ФПСУ-IP или к виртуальной машине.

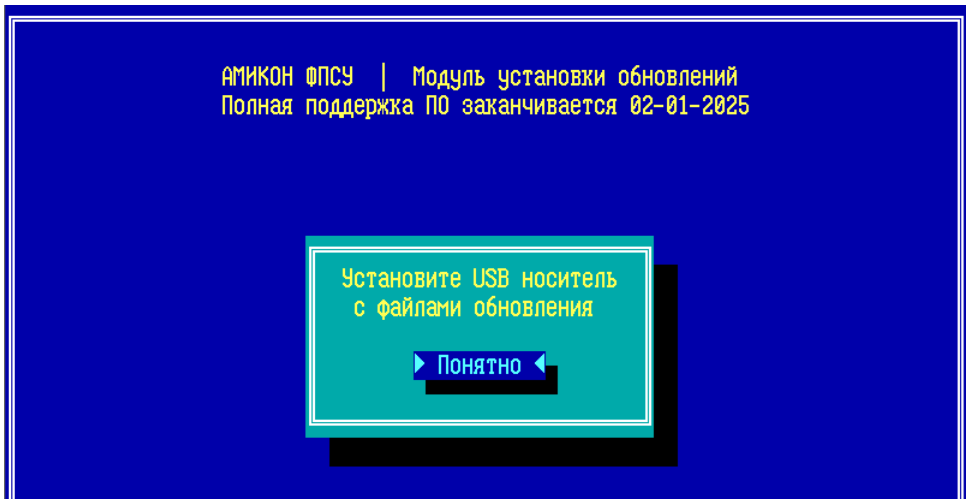


Рисунок 150 - Подсистема обновления, запрос на подключение USB

В появившемся служебном окне нажмите клавишу <*Enter*> для продолжения, проверив корректность подключения внешнего носителя к USB-порту ФПСУ-TLS.

Выберите файл обновления и нажмите клавишу <*Enter*>.

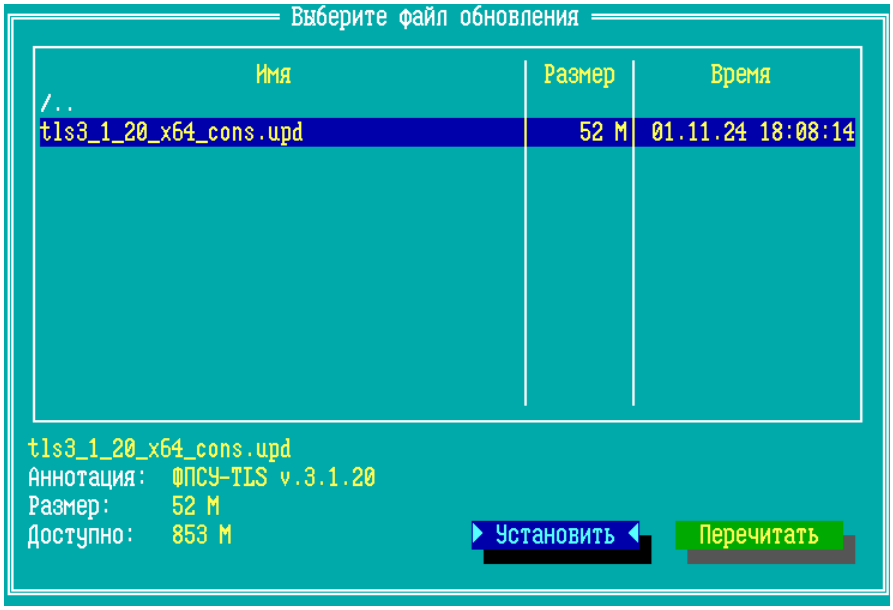


Рисунок 151 - Выбор файла обновления

Требуется подтвердить запуск процесса обновления, выбрав команду «Используем его» и нажав клавишу <Enter>, либо вернуться к выбору другого файла обновления.

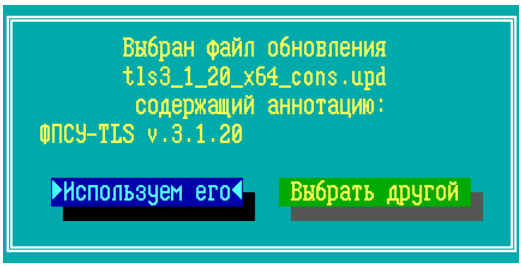


Рисунок 152 - Найден файл обновления

Подсистема установки обновлений начнет копировать файлы обновления на ФПСУ-TLS. В случае успешного копирования будет выдано окно о подтверждении замены программного обеспечения ФПСУ-TLS скопированными файлами. Нажмите кнопку «Понятно» для обновления программного обеспечения ФПСУ-TLS.

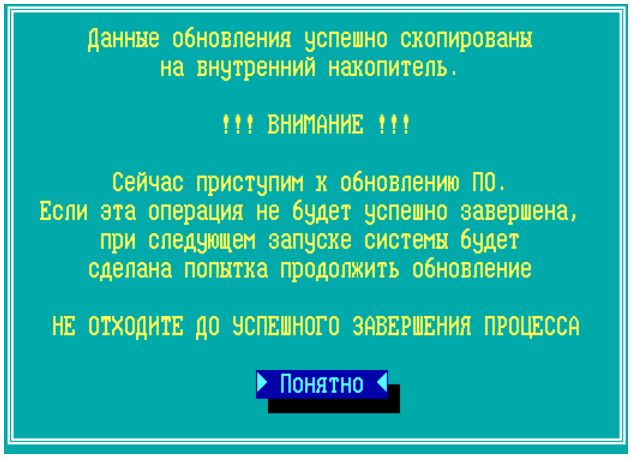


Рисунок 153 - Файлы скопированы, можно запускать обновление

После окончания установки обновления программного обеспечения, ФПСУ-TLS будет перезагружен автоматически.

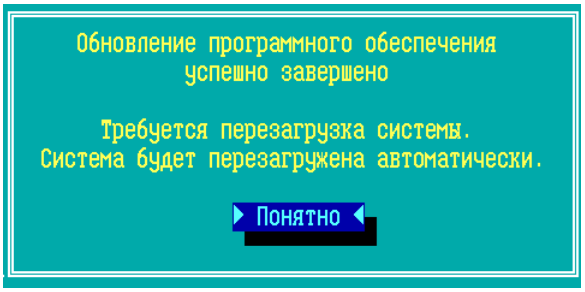


Рисунок 154 - Установка завершена, требуется перезагрузка

Нажмите кнопку «Понятно» для завершения обновления и перезагрузки ФПСУ-TLS. После перезагрузки на экран будет выдано главное меню ФПСУ-TLS.

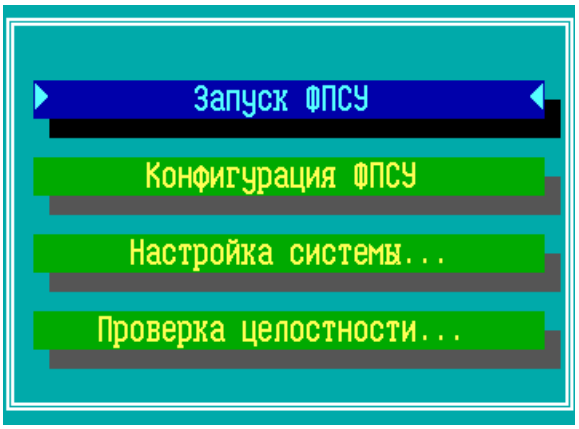


Рисунок 155 - Главное меню ФПСУ-TLS

Установка обновления завершена, ФПСУ-TLS можно запускать в рабочий режим и использовать в штатном порядке.

7. 11. 4. Установка пароля администратора

Команда меню «Настройка системы → Установка пароля администратора» предназначена для задействования, изменения или отмены пароля на вход в подсистемы конфигурирования ФПСУ-TLS. Операции доступны администраторам класса «Администратор» и выше.

ВНИМАНИЕ! Установка пароля условно-постоянного действия на администрирование не рекомендуется для версий ФПСУ-TLS 3.1.20 и выше. Данный пункт меню оставлен для обратной совместимости с предыдущими версиями ФПСУ-TLS. Для дополнительной авторизации пользователей по паролю используйте пароли ТМ-идентификаторов (см. пункт «Регистрация ТМ-идентификаторов»).

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 156 - Подтверждение полномочий и ввод пароля ТМ

Затем откроется окно, в поле редактирования которого следует ввести пароль - комбинацию из 6 - 15 символов.

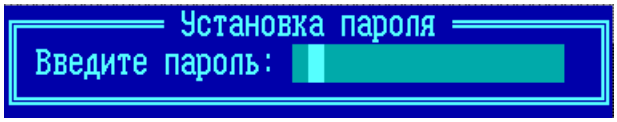


Рисунок 157 - Установка пароля администратора

Поскольку вводимые символы не будут отображаться на экране, подсистема попросит ввести пароль еще раз с целью исключения возможной ошибки. Установка будет произведена только после повторного введения идентичной комбинации символов.

В операции проверки пароля участвуют ASCII-коды символов, поэтому администратор должен быть внимателен к набору символов в определенных регистре и алфавите.

После установки пароля при попытке изменить конфигурацию ФПСУ-TLS (выборе соответствующей команды) подсистема будет блокировать любые действия администратора до ввода установленного пароля.

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду *«Установка пароля администратора»*, оставить поле пустым (не вводить символы), и нажать <*Enter*>. Отмену пароля он сможет осуществить только после введения текущего пароля, который запросит подсистема.

Пароль также может быть изменен администратором, для чего команде «*Установка пароля администратора»* он должен по запросу подсистемы подтвердить текущий пароль, а затем дважды ввести новый пароль.

ВНИМАНИЕ! Если администратор забыл пароль, то для возможности внесения любых изменений в конфигурацию или режим работы ФПСУ-TLS потребуется повторная установка ФПСУ-TLS с дистрибутива.

7. 11. 5. Регистрация удаленных администраторов

Команда меню «Настройка системы → Регистрация Удаленных Администраторов» предназначена для:

- регистрации учетных записей удаленных администраторов ФПСУ-TLS;
- предоставления или отмены им прав на доступ к подсистемам ФПСУ-TLS;
- удаления ранее зарегистрированных удаленных администраторов;
- выдачи открытого ключа ФПСУ-TLS для удаленного администратора;
- повторной генерации пары открытый/секретный ключ ФПСУ-TLS, используемых в подсистеме удаленного управления.

Рисунок 158 - Команда «Регистрация Удаленных Администраторов»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 159 - Подтверждение полномочий и ввод пароля ТМ

Взаимная регистрация ФПСУ-TLS и удаленного администратора производится следующим образом:

1. Локальным администратором ФПСУ-TLS выдается на внешний USB-flash носитель файл с открытым ключом ФПСУ-TLS;
2. Файл с открытым ключом ФПСУ-TLS передается удаленному администратору доверенным способом (передача по незащищенной сети передачи данных запрещается);
3. Получив файл с открытым ключом ФПСУ-TLS, администратор регистрирует у себя данный ФПСУ-TLS в программе «Удаленный администратор ФПСУ-IP»;
4. Удаленный администратор с помощью программы «Удаленный администратор ФПСУ-IP» выдает на внешний носитель файл с открытым ключом удаленного администратора;
5. Файл с открытым ключом удаленного администратора отправляется локальному администратору ФПСУ-TLS доверенным способом (передача файла по незащищенной сети передачи данных запрещается);
6. Локальный администратор ФПСУ-TLS на основании полученного открытого ключа регистрирует удаленного администратора и предоставляет ему права на доступ к подсистемам ФПСУ-TLS.

При выполнении команды меню «Настройки системы → Регистрация удаленных администраторов», на экране появится окно, которое содержит те параметры ФПСУ-TLS (серийный номер, комментарий к нему и дату создания открытого и секретного ключей ФПСУ-TLS), с которыми его зарегистрирует удаленный администратор, а также список уже зарегистрированных удаленных администраторов ФПСУ-TLS (по умолчанию, пустой, с

текстом «Администраторы отсутствуют»).

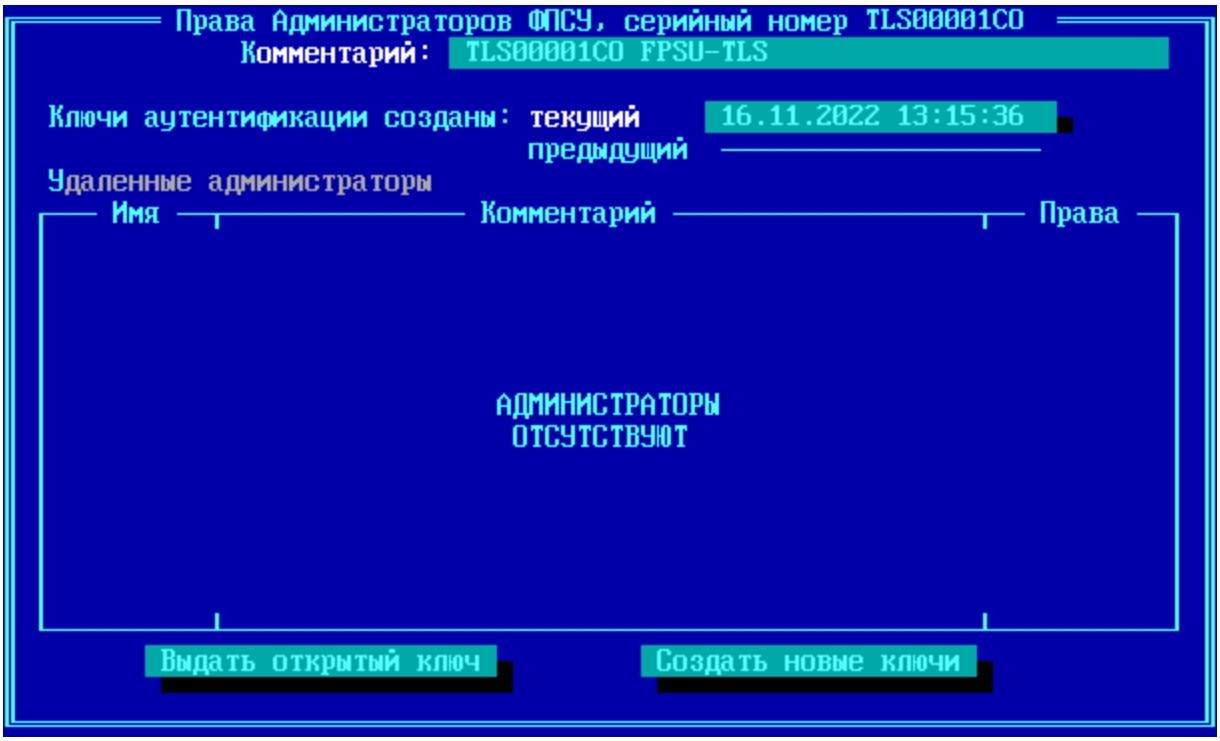


Рисунок 160 - Список удаленных администраторов

Количество удаленных администраторов, зарегистрированных на ФПСУ-TLS, не может превышать тридцати двух.

Выход из подсистемы регистрации удаленных администраторов осуществляется клавишами <Alt+X> или <Esc>.

ФПСУ-TLS выдает оповещение об истечении срока действия ключа для связи с АРМ УА при входе в меню «Настройка системы → Регистрация Удаленных Администраторов»:

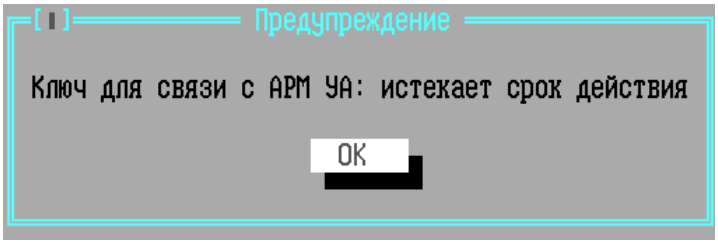


Рисунок 161 - Оповещение об истечении срока действия ключа для связи с АРМ УА

В случае если текущая дата превышает срок действия ключа для связи с АРМ УА выдается следующее предупреждение:

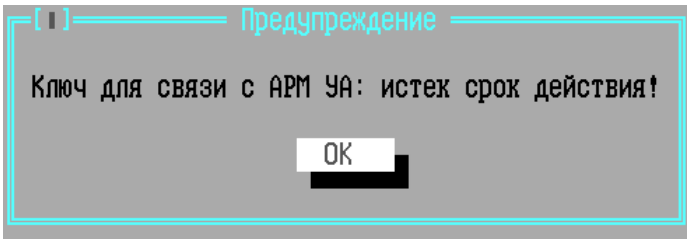


Рисунок 162 - Срок действия ключа для связи с АРМ УА истек

7. 11. 5. 1. Удаленное управление ФПСУ-TLS

Дистанционное управление комплексом ФПСУ-TLS осуществляется с помощью программного обеспечения «Удаленный администратор «ФПСУ-IP» с использованием криптографически защищенного канала связи (VPN-туннеля), в котором производятся взаимная идентификация и строгая двусторонняя аутентификация ФПСУ-TLS и УА ФПСУ-IP.

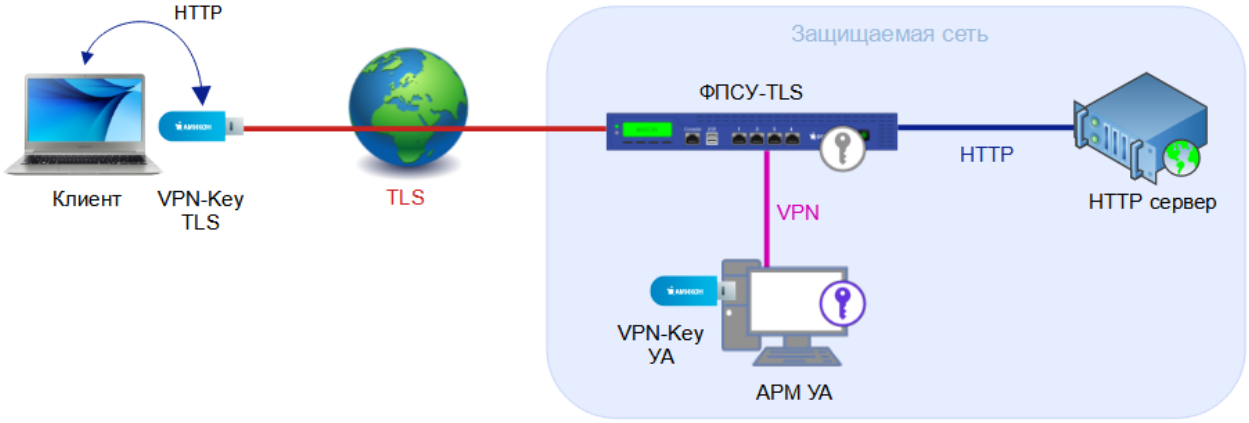


Рисунок 163 - Удаленное управление ФПСУ-TLS

Взаимная регистрация ФПСУ-TLS и УА ФПСУ-IP является обязательным условием для реализации удаленного управления: все операции по дистанционному контролю и управлению осуществляются УА ФПСУ-IP только по отношению к зарегистрированным ФПСУ-TLS, а ФПСУ-TLS могут обмениваться данными только с зарегистрированным ими администраторами УА ФПСУ-IP. Взаимная регистрация осуществляется посредством обмена файлами с открытыми ключами. Процедура взаимной регистрации описывается в пункте «Регистрация удаленных администраторов».

Внимание! Выдать открытые ключи (см. пункт «Открытые ключи ФПСУ-TLS для удаленного управления»), установить собственные сертификаты и ключи (см. пункт «Установка личных сертификатов ФПСУ-TLS»), установить CRL с внешнего носителя администратор может только локально.

7. 11. 5. 2. Регистрация удаленного администратора на ФПСУ-TLS

Для регистрации первой учетной записи удаленного администратора на ФПСУ-TLS нажмите клавишу <Ins>, установив курсор на текст «Администраторы отсутствуют». Подсистема запросит установить носитель с открытым ключом удаленного администратора, который должен быть предварительно получен от удаленного администратора. Подключите USB-носитель с открытым ключом удаленного администратора и нажмите кнопку «ОК» или клавишу <Enter>.

Рисунок 164 - Выбор USB-носителя с открытыми ключами

Когда подсистема опознает и считает находящиеся на USB-носителе открытые ключи удаленных администраторов, она выдаст окно, содержащее их список . В окне «Обнаружены данные» необходимо сначала отметить регистрируемые учетные записи администраторов клавишей <Пробел> (рядом с регистрируемой учетной записью проставляется знак «√»), а потом выполнить команду «Добавить отмеченные».

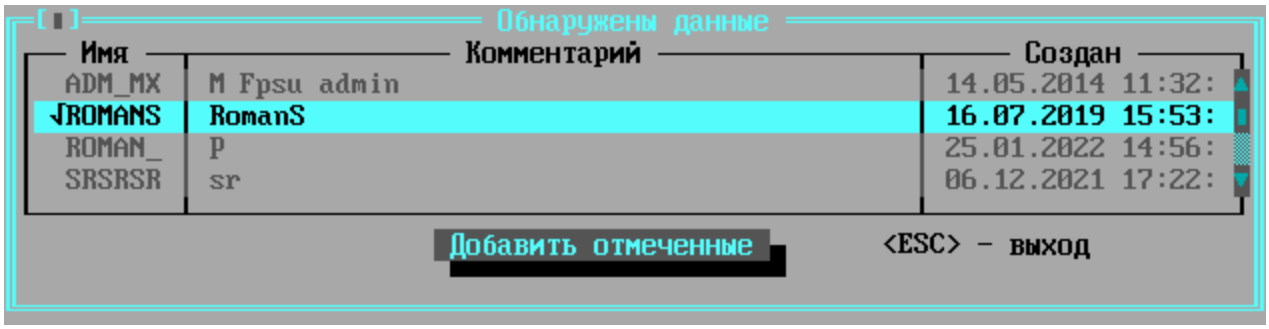


Рисунок 165 - Найденные открытые ключи удаленного администратора

ФПСУ-TLS выдает оповещение об истекшем сроке действия открытого ключа АРМ УА на главном экране при его установке на ФПСУ-TLS:

Рисунок 166 - Срок действия открытого ключа АРМ УА истек

После выполнения команды зарегистрированные удаленные администраторы появятся в списке окна «Права администраторов ФПСУ».

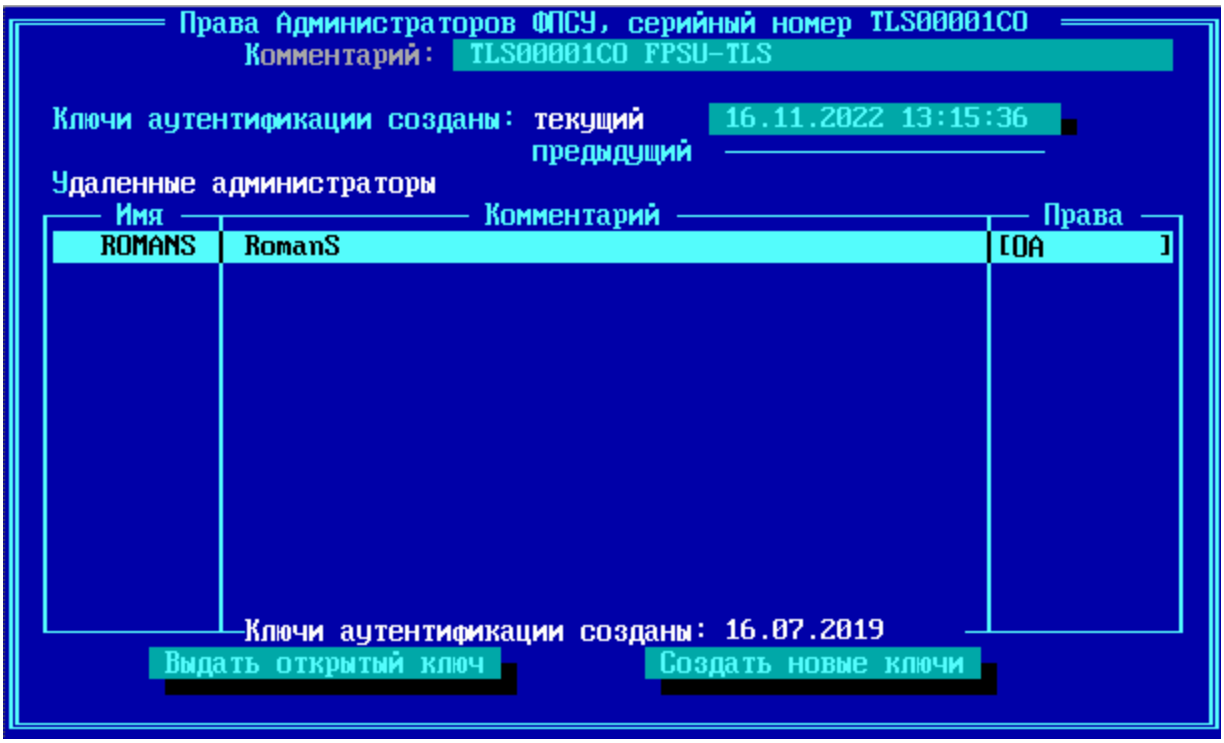


Рисунок 167 - Зарегистрирован удаленный администратор

Для каждого зарегистрированного удаленного администратора будет отображаться имя, комментарий к имени, права на доступ к подсистемам ФПСУ-TLS и дата создания открытого ключа (ключей аутентификации) удаленного администратора.

Новый удаленный администратор регистрируется на ФПСУ-TLS не только с минимальными правами, но и в состоянии «Временно запрещен».

В статусной строке окна динамически (в зависимости от производимой операции) отображаются варианты возможных действий с учетными записями удаленных администраторов: установить или изменить права (<Enter>), зарегистрировать новые (<Ins>), удалить имеющиеся из списка (<Del>) или выйти из подсистемы регистрации (<Alt+X> или <Esc>).

Для присвоения удаленному администратору прав на доступ к подсистемам ФПСУ-TLS или изменения существующих, отметьте его в списке и нажмите <Enter>. В появившемся окне можно установить или изменить права (права на опрос текущего состояния и получения протокола работы абонентов всегда включены) и разрешить/временно запретить работу удаленного администратора.

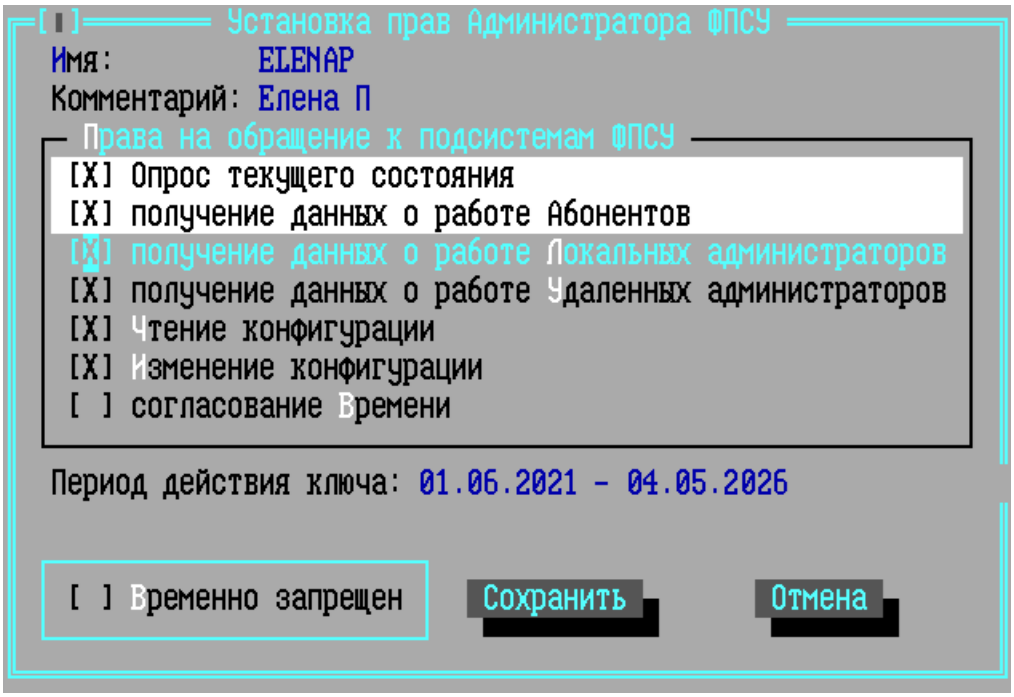


Рисунок 168 - Назначение прав удаленному администратору

Права на обращение к подсистемам ФПСУ-TLS:

Опрос текущего состояния – удаленному администратору доступна информация об изменениях конфигурации ФПСУ-TLS: изменения, внесенные локальным администратором, удаленным администратором; количество запусков ФПСУ-TLS; события согласования времени вручную и автоматически. Удаленному администратору также доступна информация о состояние аппаратной части – скорости вращения вентиляторов, температуре и напряжении.

Получение данных о работе абонентов – удаленному администратору доступно получение информации о состоянии работы абонентов ФПСУ-TLS – статистическая информация о передаче данных в открытом виде и через туннель, об ошибках при передаче, отказе доступа, отсутствии связи, о передаче данных за сутки.

Получение данных о работе локальных администраторов – удаленному администратору доступно получение статистики ФПСУ-TLS о работе локальных администраторов – запуске ФПСУ-TLS, начале и окончании работы ФПСУ-TLS, регистрации ТМ-идентификаторов и их удалении, изменении параметров конфигурации ФПСУ-TLS, регистрации администраторов УА ФПСУ-TLS и т.д.

Получение данных о работе удаленных администраторов – удаленному администратору доступно получение статистики ФПСУ-TLS о работе удаленных

администраторов – получении статистических данных ФПСУ-TLS, изменении текущего времени ФПСУ-TLS и т.д.

Чтение конфигурации – удаленному администратору доступно получать конфигурацию с ФПСУ-TLS.

Изменение конфигурации – удаленному администратору доступно устанавливать конфигурацию на ФПСУ-TLS.

Согласование времени – удаленному администратору доступно устанавливать время на ФПСУ-TLS, устанавливать автокоррекцию времени на ФПСУ-TLS, что позволит автоматически синхронизировать текущее время на ФПСУ-TLS с текущим временем УА ФПСУ-TLS. Право на согласование времени разрешает ФПСУ-TLS синхронизировать время со временем рабочей станции выбранного удаленного администратора. Право на согласование времени может быть выдано только одному удаленному администратору.

Отметив соответствующие выдаваемым правам флаги клавишей <Пробел>, сохраните установки при помощи команды «Сохранить», при этом подсистема вернется в окно списка зарегистрированных удаленных администраторов.

В меню управления Удаленными Администраторами удаленный администратор с истекшим сроком действия открытого ключа АРМ УА отображается красным цветом.

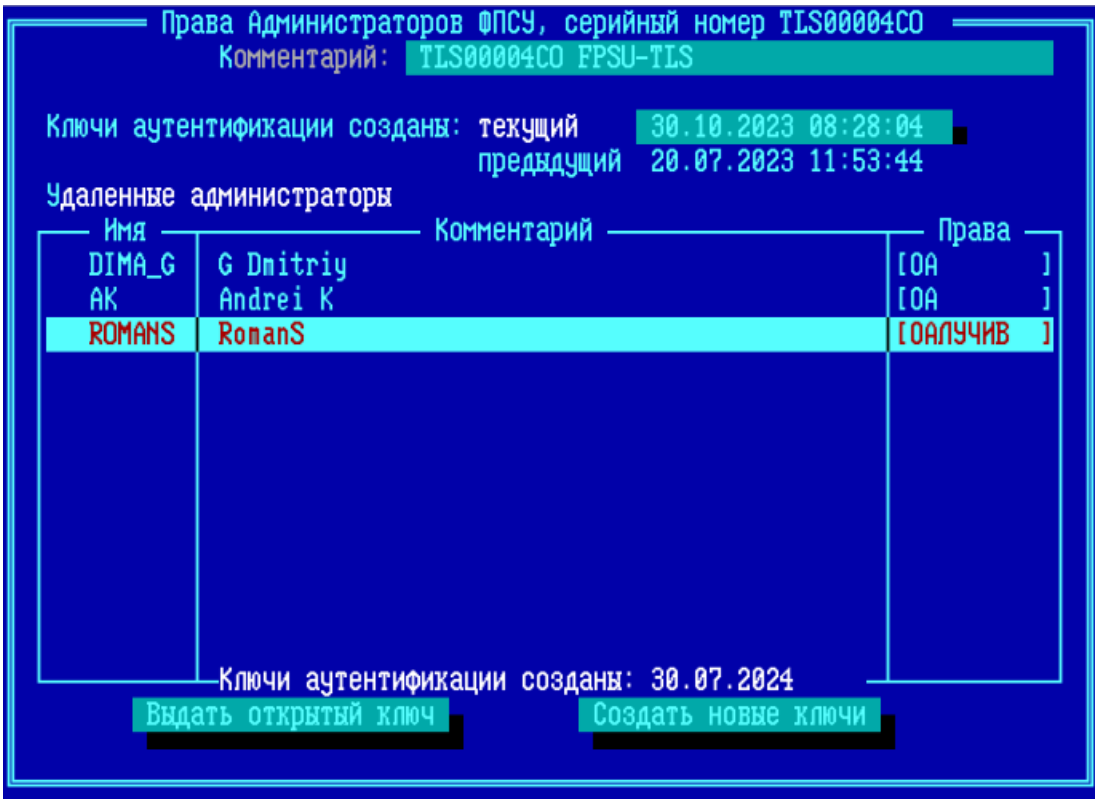


Рисунок 169 - Администратор с истекшим сроком действия открытого ключа АРМ УА

В правах доступа такого администратора период действия ключа отображается с сообщением «Просрочен»:

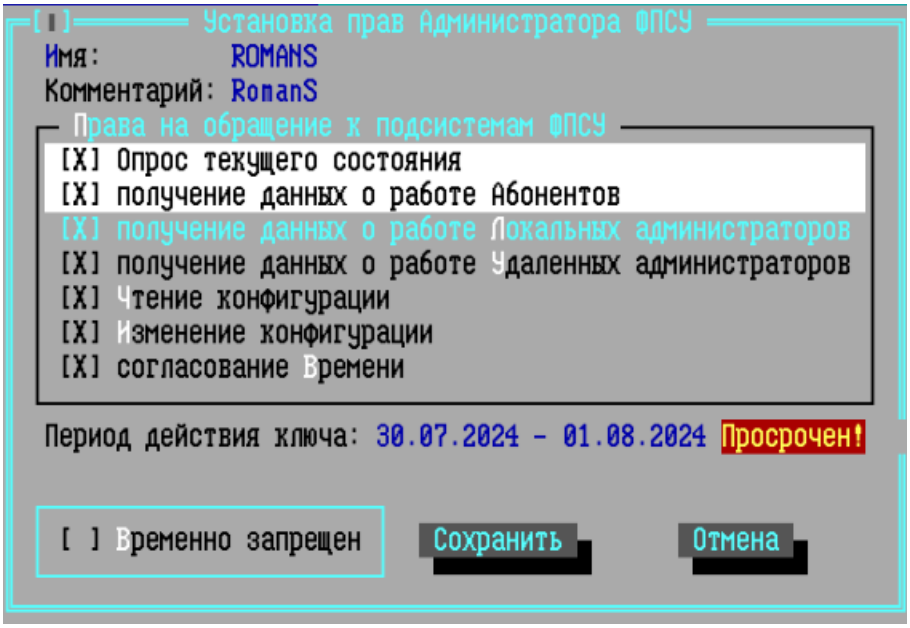


Рисунок 170 - Права администратор с истекшим сроком действия открытого ключа АРМ УА

7. 11. 5. 3. Открытые ключи ФПСУ-TLS для удаленного управления

Открытые ключи ФПСУ-TLS требуются для регистрации ФПСУ-TLS удаленным администратором в программе «Удаленный администратор ФПСУ-IP».

Ключи для аутентификации удаленного администратора ФПСУ-TLS (пара открытый/секретный ключ) ФПСУ-TLS могут иметь статус «текущие» и «предыдущие». И «текущие» и «предыдущие» пары ключей являются действительными для установления соединения с удаленным администратором. При создании на ФПСУ-TLS новой пары ключей , «текущие» ключи становятся «предыдущими», а «предыдущие» становятся недействительными.

Секретный ключ ФПСУ-TLS не может быть выдан и хранится только на внутреннем накопителе ФПСУ-TLS.

Для записи текущего открытого ключа ФПСУ-TLS на внешний носитель, нажмите, находясь в окне списка зарегистрированных удаленных администраторов, кнопку «Выдать открытый ключ». Выдать предыдущий открытый ключ ФПСУ-TLS нельзя.

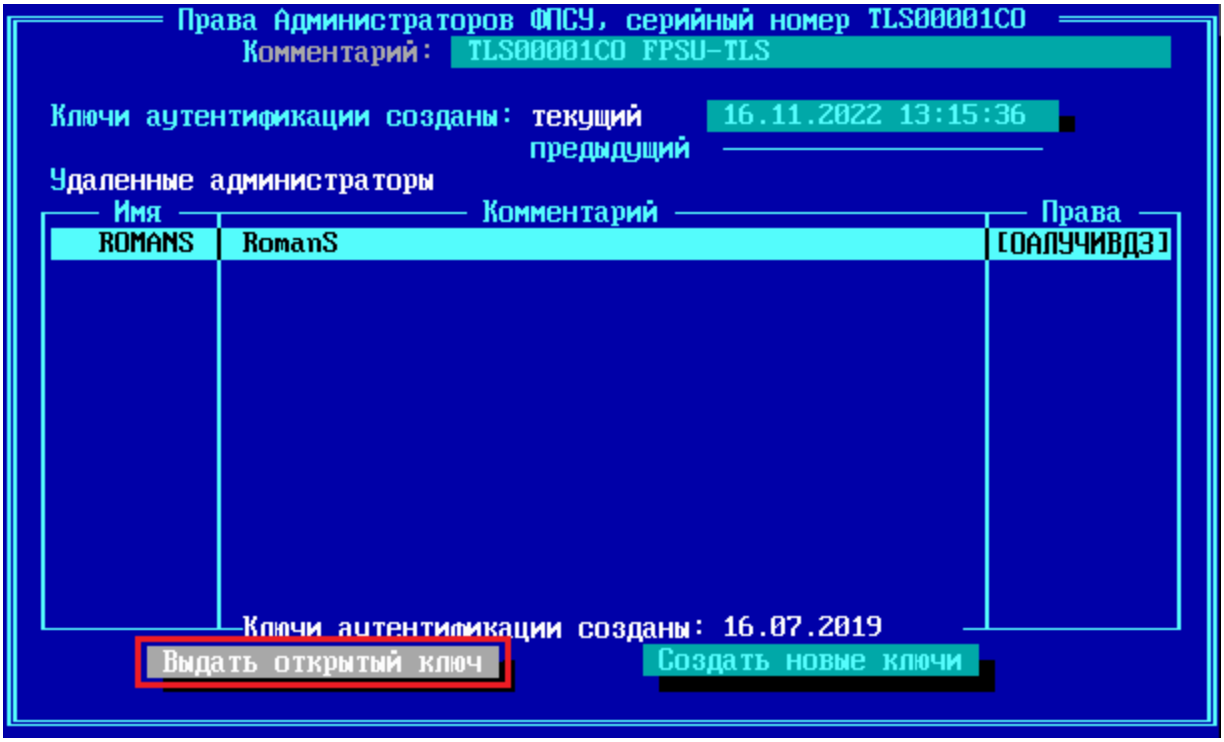


Рисунок 171 - Команда выдачи открытого ключа ФПСУ-TLS

Для выработки новой пары открытый/секретный ключ ФПСУ-TLS, выполните команду «Создать новые ключи». В случае компрометации «текущих» ключей этой командой придется воспользоваться два раза (сначала сделать «текущие» ключи «предыдущими», а

затем недействительными).

После генерации новой пары ключей ФПСУ-TLS, доступ всех удаленных администраторов к ФПСУ-TLS будет заблокирован. Удаленным администраторам потребуется получить от администратора ФПСУ-TLS новые открытые ключи и выполнить на их основе повторную регистрацию ФПСУ-TLS в программе удаленного управления.

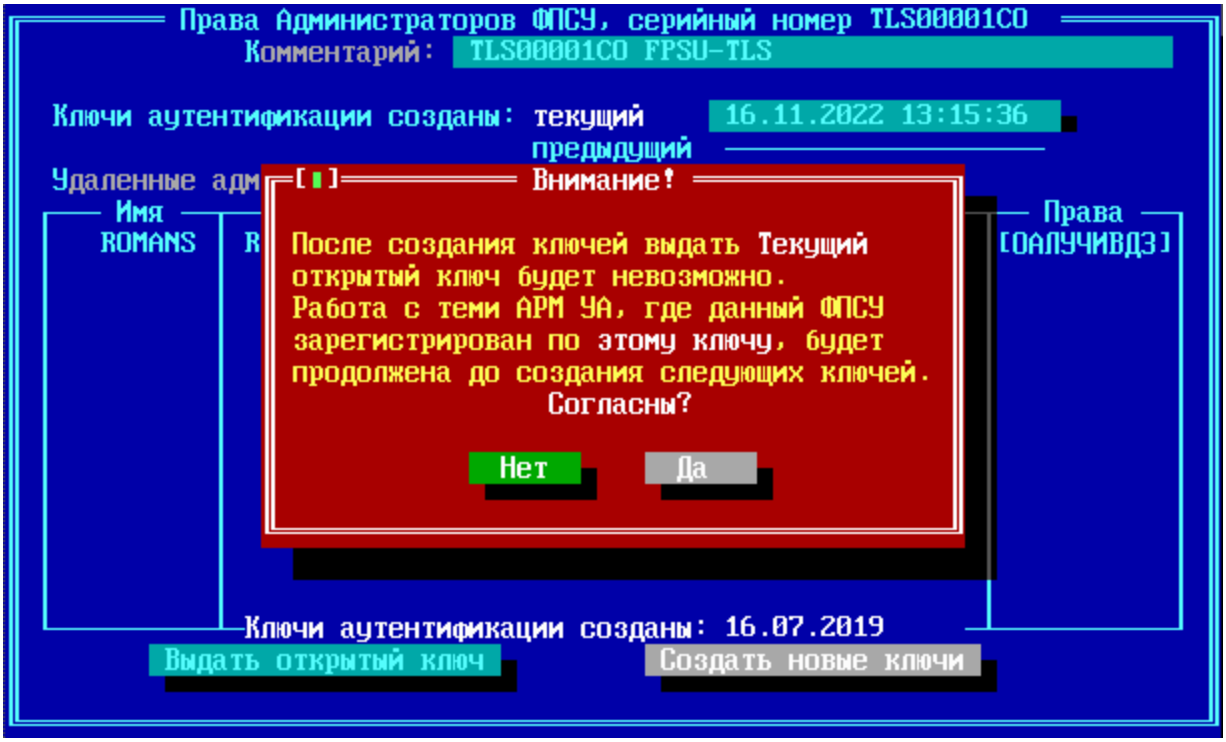


Рисунок 172 - Предупреждение при создании новой пары ключей ФПСУ-TLS

7. 11. 6. Просмотр статистики

Команда меню «Настройка системы → Просмотр статистики» предназначена для перехода в окно установки условий поиска накопленной регистрационной информации.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 173 - Подтверждение полномочий и ввод пароля ТМ

Для получения необходимых данных сначала отметьте нужный тип, выделив курсором соответствующую строку, и нажмите <Пробел>. При этом строка будет отмечена слева знаком «√», а в окне подтипов отобразится относящийся к данному типу список. Переход к подтипам осуществляется по нажатию клавиши <Tab> или <→>. Подтипы отмечаются так же, как и типы.

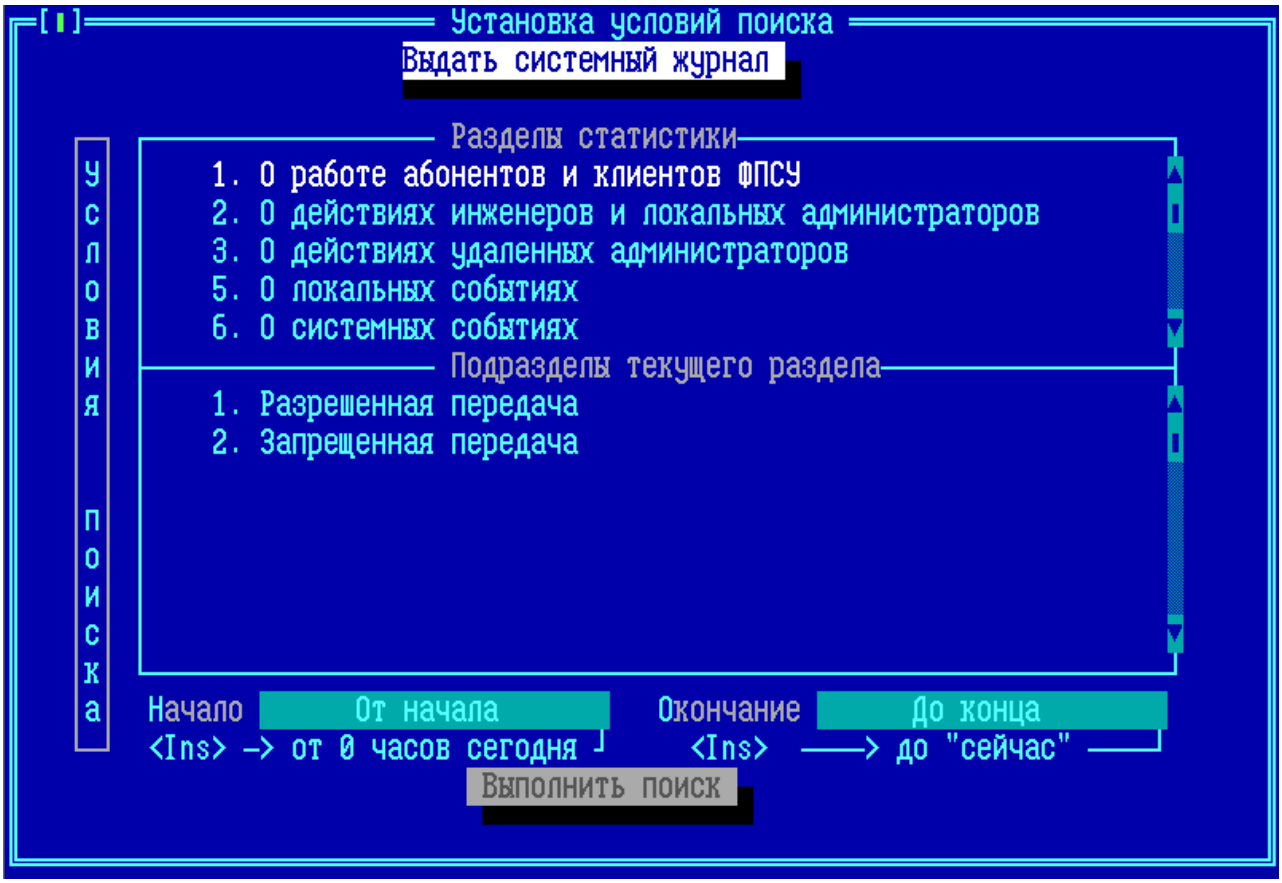


Рисунок 174 - Окно поиска статистики

Далее укажите интервал времени, за который будет выбираться статистика. При входе в окно поля ввода времени будут содержать строки «Начало» и «Окончание». Если необходимо задать другой интервал времени, можно вручную ввести необходимые значения в формате ДД.ММ.ГГГГ, где ДД - число, ММ - номер месяца, ГГГГ - год, и нажать клавишу <Enter>. Если формат введенных данных верен, установится новое значение, если нет – сохранится старая запись.

Переход между всеми полями осуществляется по нажатию <Tab>.

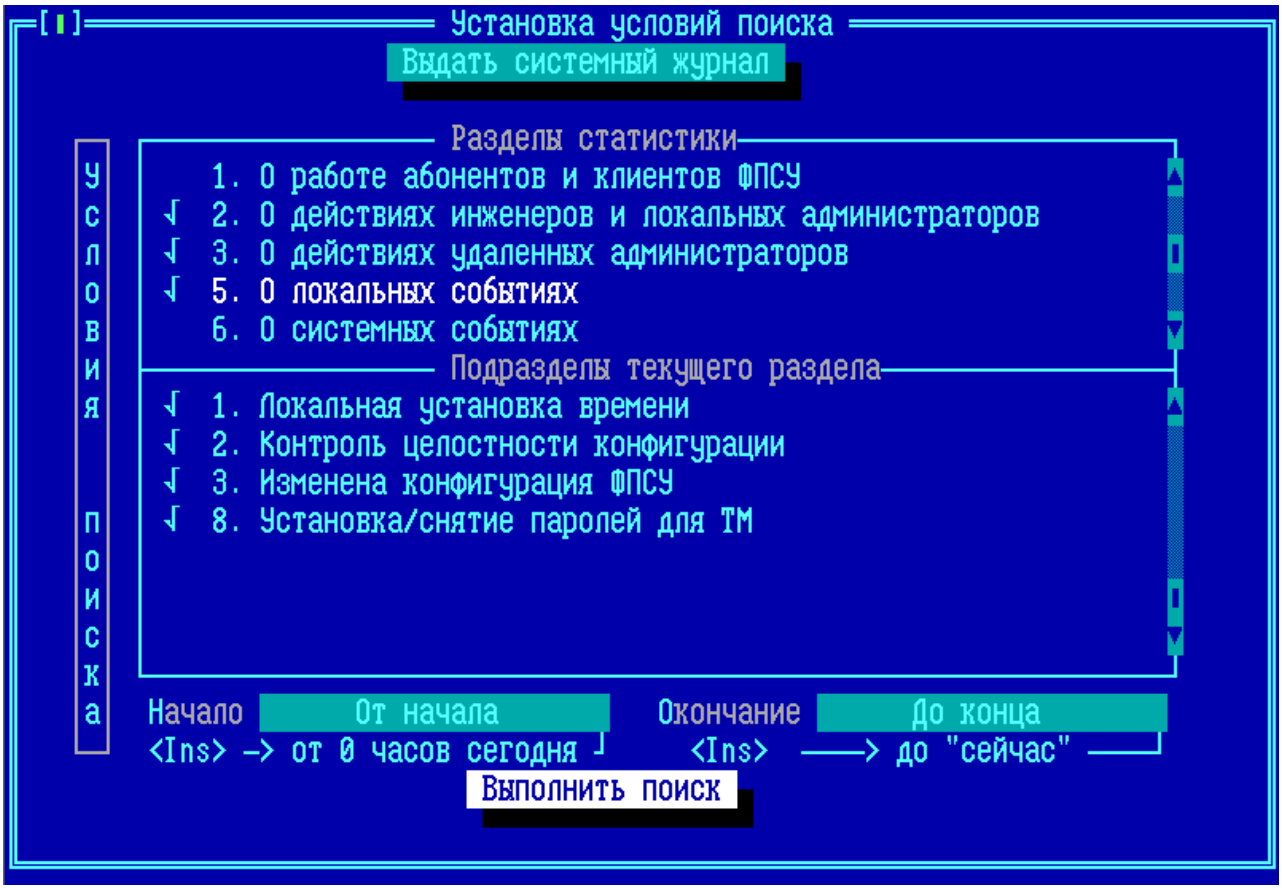


Рисунок 175 - Выбор выводимых данных статистики

После задания всех требуемых установок для поиска следует при помощи клавиши <Tab> отметить команду «Выполнить поиск» и нажать клавишу <Enter>. Подсистема регистрации осуществит поиск и выдаст результат на экран.

Обратите внимание, что поиск будет выполняться лишь в том случае, если отмечен хотя бы один тип запрашиваемых данных.

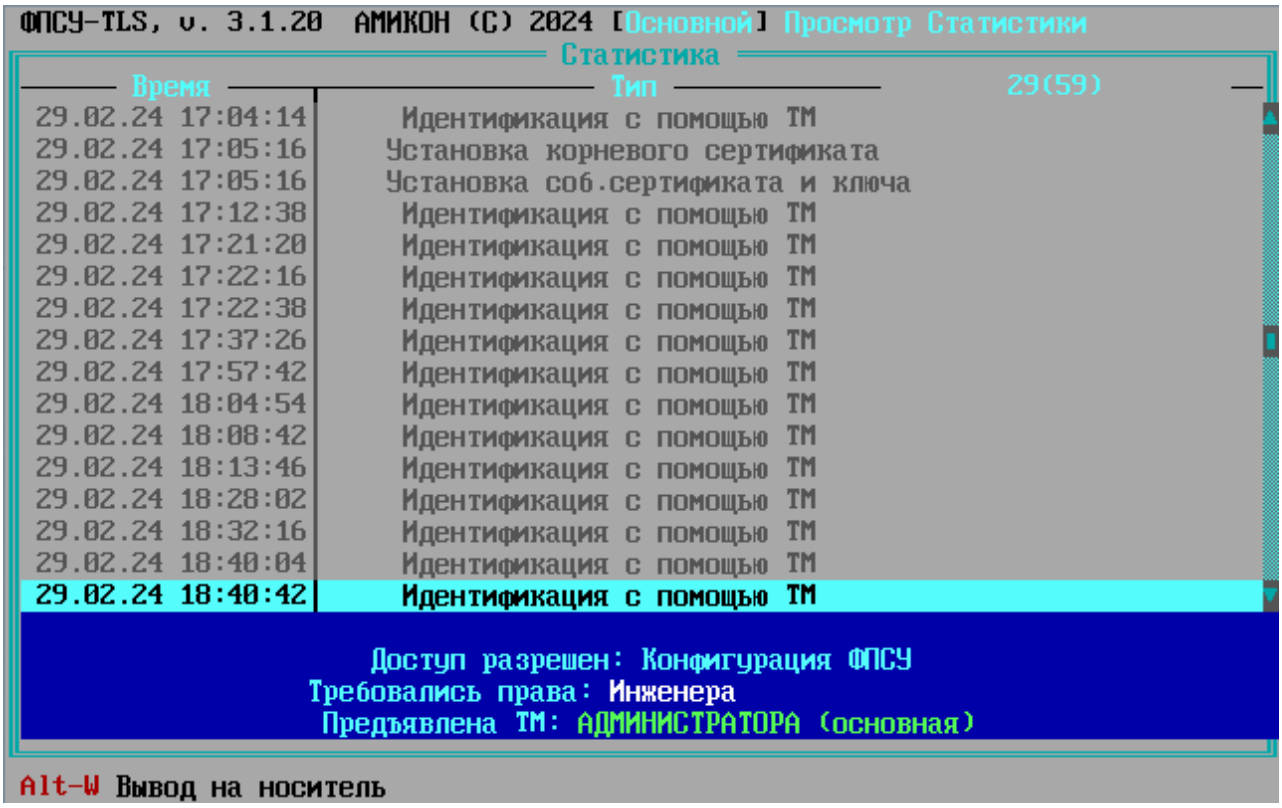


Рисунок 176 - Вывод данных статистики

При выборе раздела «О действиях удаленных администраторов» можно увидеть в статистике, например, события регистрации и удалении открытого ключа удаленного администратора (подробнее см. пункт «Регистрация удаленного администратора на ФПСУ-TLS»):

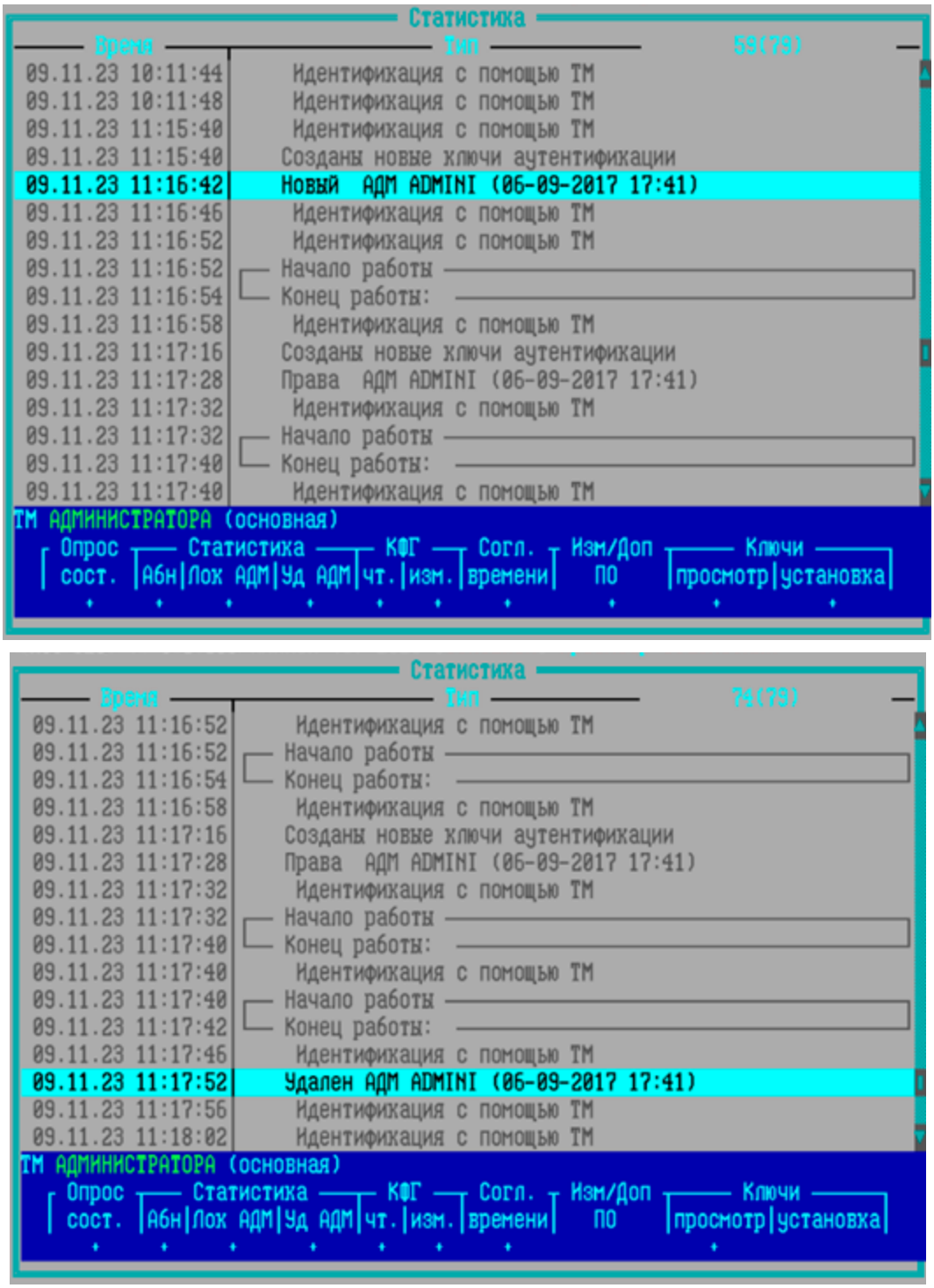


Рисунок 177 - Вывод данных о регистрации и удалении открытого ключа удаленного администратора

При выборе раздела «О действиях инженеров и локальных администраторов» можно увидеть в статистике, например, события создания ключевой пары для связи с АРМ УА

(подробнее см. пункт «Открытые ключи ФПСУ-TLS для удаленного управления», кнопка «Создать новые ключи»):

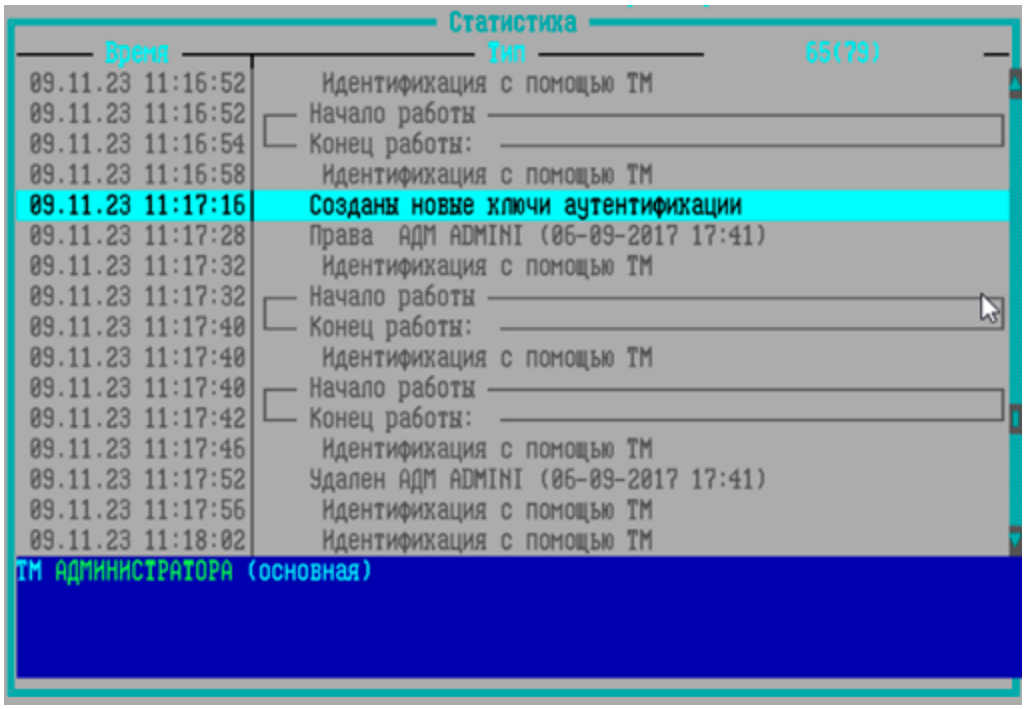


Рисунок 178 - Вывод данных о создании ключевой пары для связи с АРМ УА

При выборе раздела «О действиях инженеров и локальных администраторов» в статистике отображаются события о попытках доступа к не разрешенным данному пользователю функциям (подробнее см. пункт «Разграничение доступа и пользователи»):

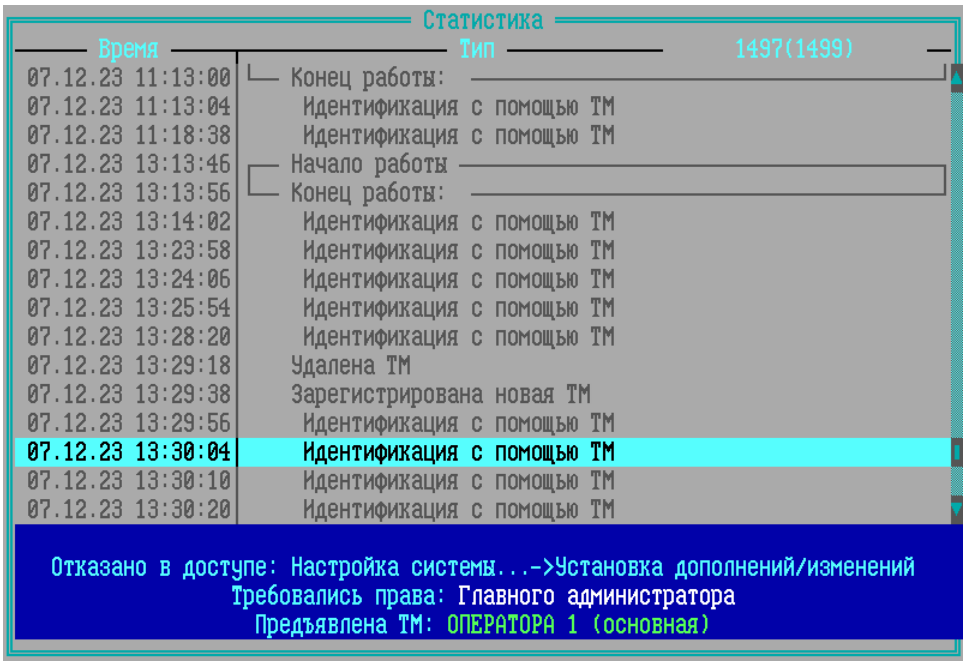


Рисунок 179 - Вывод данных о попытках доступа к не разрешенным функциям

При выборе раздела «О локальных событиях» в статистике отображаются результаты контроля целостности ФПСУ-TLS (подробнее см. пункт «Контроль целостности программного обеспечения»):

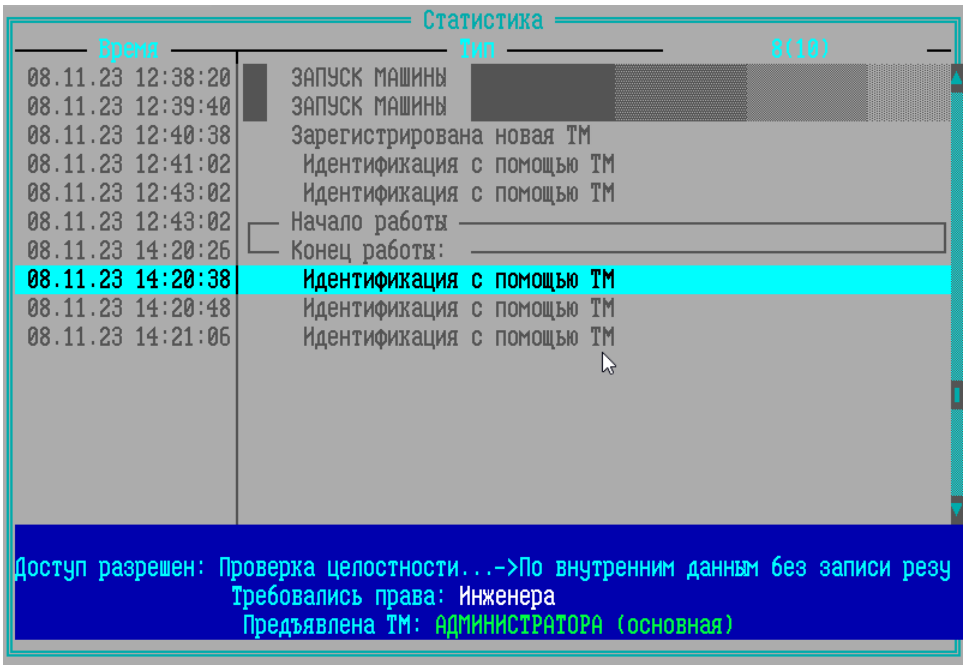


Рисунок 180 - Вывод данных о результатах контроля целостности ФПСУ-TLS

При выборе раздела «О системных событиях» в статистике отображаются записи об установке и удалении собственного сертификата и секретного ключа ФПСУ-TLS (подробнее

см. раздел Установка сертификатов):

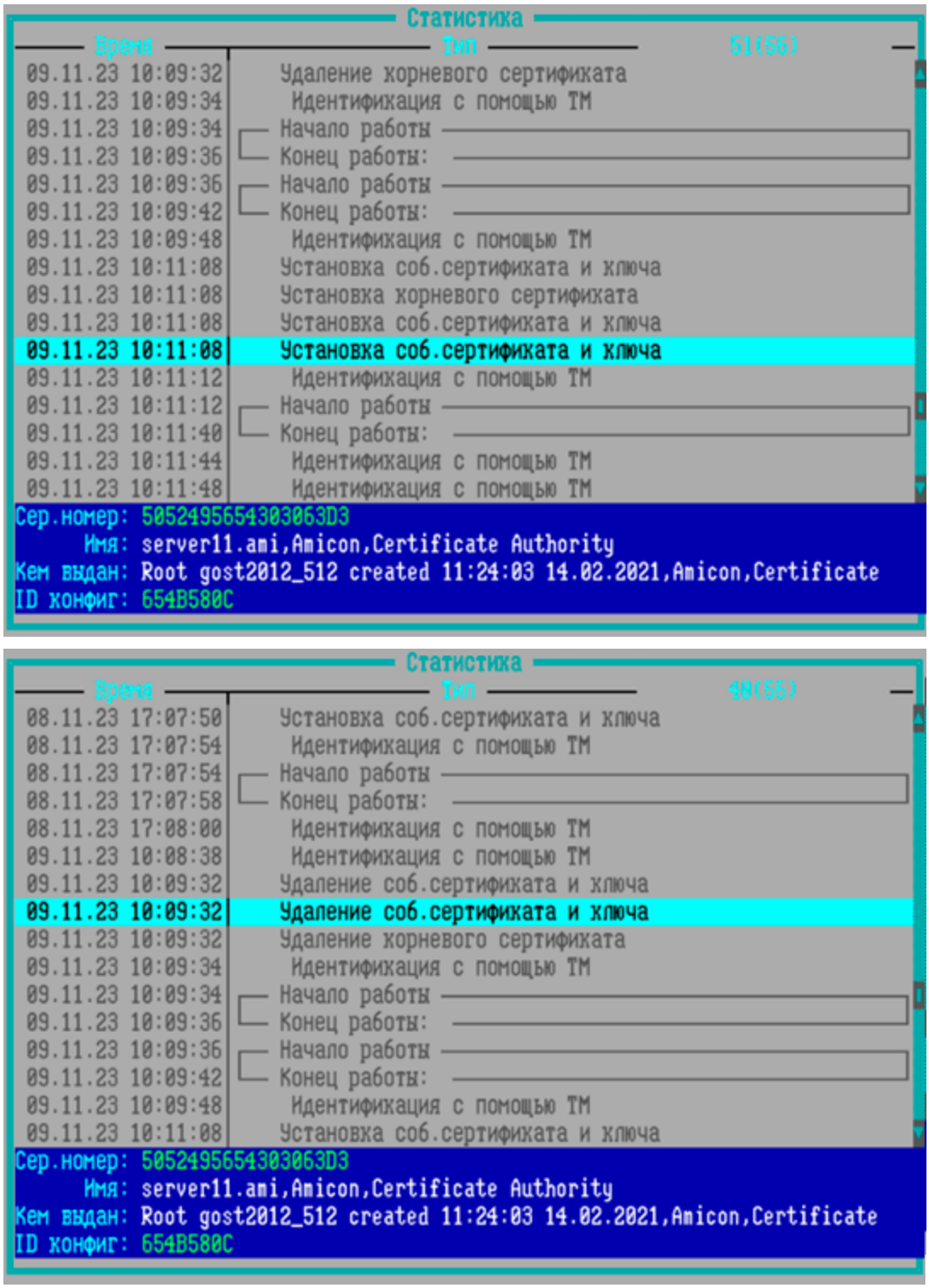


Рисунок 181 - Вывод данных об установке и удалении собственного сертификата и секретного ключа

При выборе раздела «О системных событиях» в статистике отображаются записи об установке и удалении корневого сертификата ФПСУ-TLS (подробнее см. раздел «Установка сертификатов»):

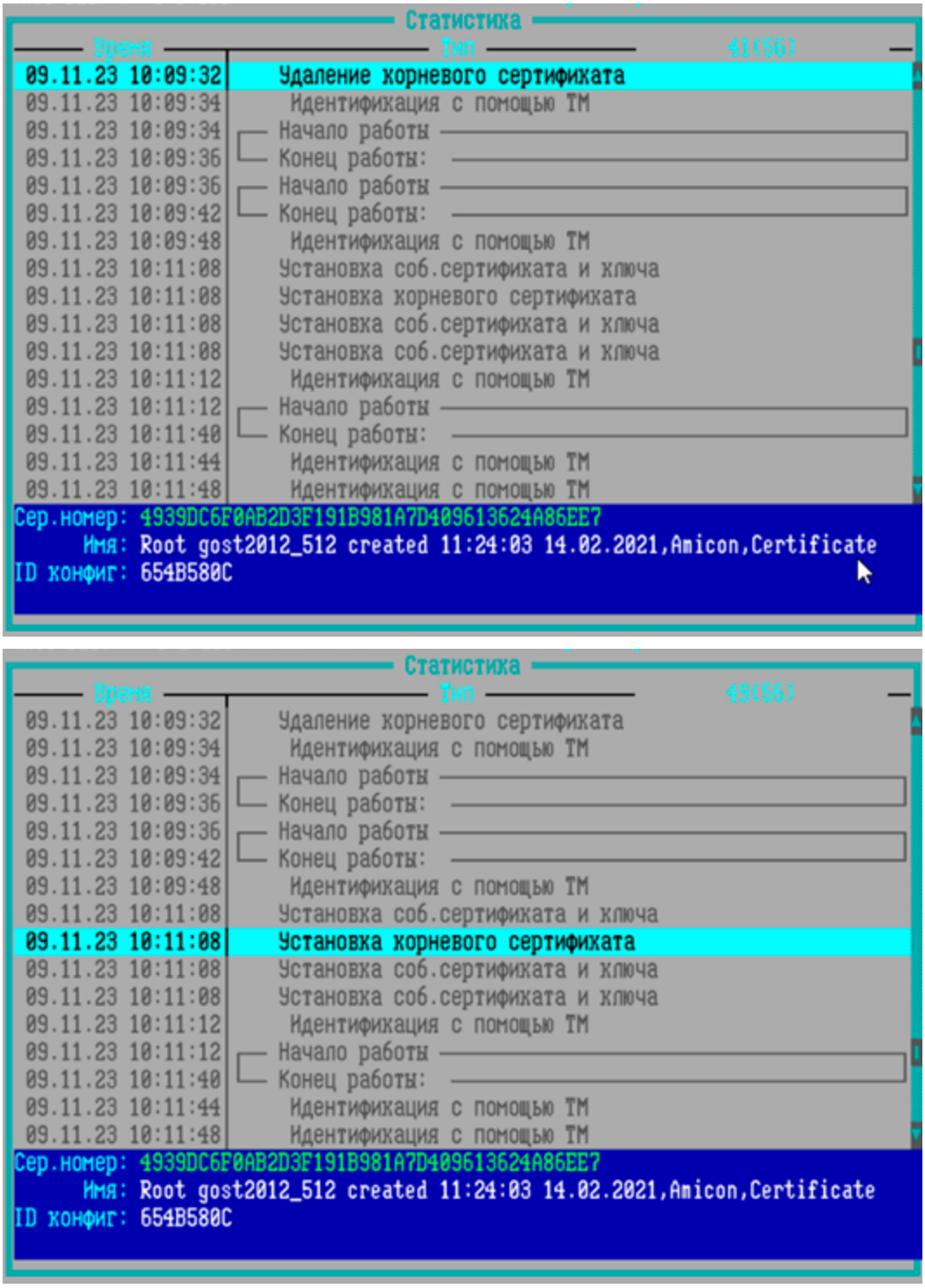


Рисунок 182 - Вывод данных об удалении и установке корневого сертификата

При выборе раздела «О системных событиях» в статистике отображаются записи об установке дополнений/изменений (см. пункт «Обновление программного обеспечения»):

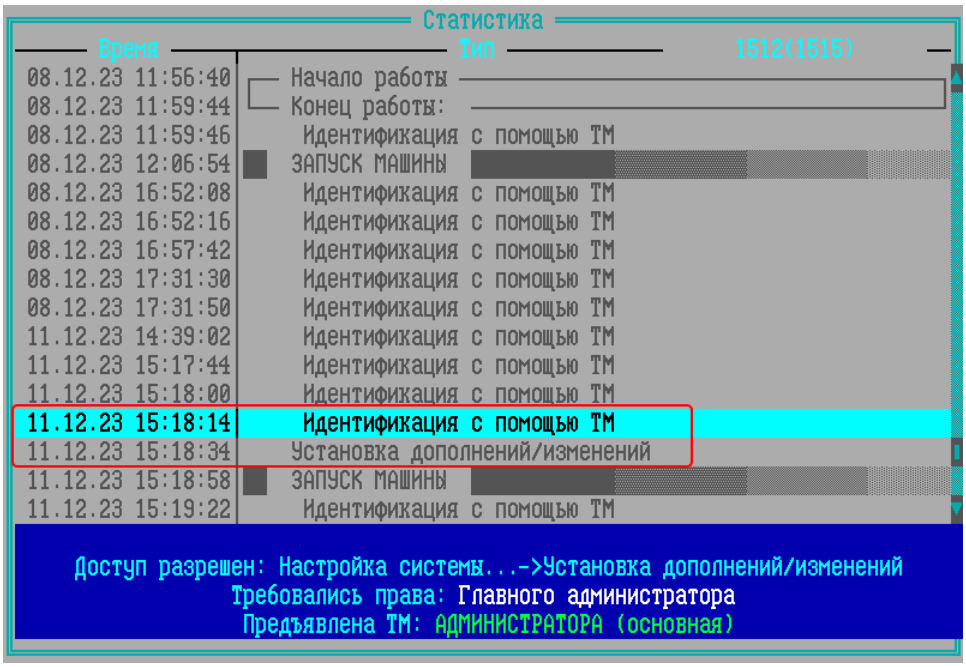


Рисунок 183 - Вывод данных об установке дополнений/изменений

7. 11. 7. Системный журнал

На ФПСУ-TLS предусмотрена возможность выдачи системного журнала на внешний носитель.

В системный журнал записывается информация о:

1) создании (пересоздании) журнала;

2) создании и удалении ключей запуска (допуск и отстранение пользователей);

3) установки и удалении открытых ключей администраторов АРМ УА (регистрация удаленных администраторов);

4) создания и удаления секретных ключей для связи с АРМ УА;

5) дате и времени запуска ФПСУ-TLS;

6) попытках доступа к не разрешенным данному пользователю функциям ФПСУ-TLS;

7) результатах контроля целостности ФПСУ-TLS;

8) установка и удаление собственного сертификата и ключа ФПСУ-TLS;

9) удаление и установка корневого сертификата ФПСУ-TLS;

10) установка дополнений/изменений.

Записи хранятся в файле, содержимое которого удаляется только при выдаче на внешний носитель, при этом первой записью в очищенном файле становится запись о событии выдачи журнала. Помимо этого, в отдельный, циклически перезаписываемый, файл сохраняются данные о событиях, произошедших при функционировании ФПСУ-TLS и необходимых для анализа работы ФПСУ-TLS.

При переходе в окно установки условий поиска накопленной регистрационной информации по команде меню «Настройка системы → Просмотр статистики» можно выдать системный журнал на внешний носитель, нажав кнопку «Выдать системный журнал».

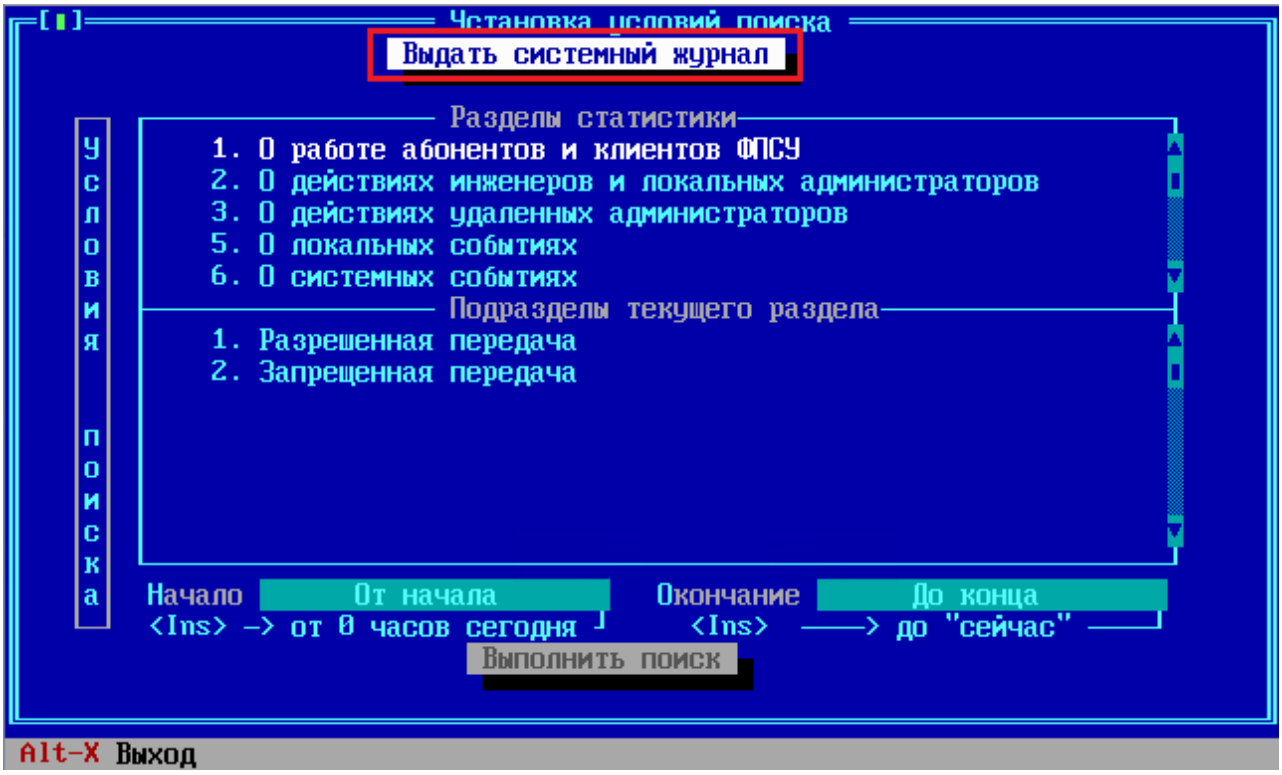


Рисунок 184 - Окно поиска статистики

Файл системного журнала содержит запись о создании журнала, а также о дате и времени выдачи:

```
Системный журнал ФПСУ  TLS00004CO
Создан  29.10.2023  12:59:44


Выдан   29.10.2023  12:59:55
```

При регистрации нового пользователя (см. пункт «Регистрация ТМ-идентификаторов») выводится следующая запись в файле журнала:

```
29.10.2023  12:57:38
 Зарегистрирована новая ТМ
  ИНЖЕНЕРА (основная)
29.10.2023  12:58:48
 Удалена ТМ
  ИНЖЕНЕРА (основная)
```

При регистрации и удалении открытого ключа удаленного администратора (см. пункт «Регистрация удаленного администратора на ФПСУ-TLS») выводится следующая запись в файле журнала:

```
09.11.2023  11:16:58
 Попытка входа с использованием ТМ
  Пункт меню       Доступ разрешен: Настройка системы...->Регистрация Удаленных Администраторов
  Требуемая ТМ     Установщика (запасная)
  Предъявлена ТМ   АДМИНИСТРАТОРА (основная)

09.11.2023  11:16:42
 Зарегистрирован новый Администратор
  ТМ  АДМИНИСТРАТОРА (основная)
  ADMINI (06-09-2017 17:41)
  ┌ Опрос ┬─ Статистика ──┬─ КФГ ─┬ Согл. ┬ Изм/Доп ┬──── Ключи ────┐
  │ сост. │Абн│Лок АДМ│Уд АДМ│чт.│изм.│времени│   ПО    │просмотр│установка│
    +     +     +       +      +     +     +        +         +          +

09.11.2023  11:17:52
 Удален Администратор
  ТМ  АДМИНИСТРАТОРА (основная)
  ADMINI (06-09-2017 17:41)
  ┌ Опрос ┬─ Статистика ──┬─ КФГ ─┬ Согл. ┬ Изм/Доп ┬──── Ключи ────┐
  │ сост. │Абн│Лок АДМ│Уд АДМ│чт.│изм.│времени│   ПО    │просмотр│установка│
    +     +     +       +      +     +     +                  +
```

При создании ключевой пары для связи с АРМ УА (подробнее см. пункт «Открытые ключи ФПСУ-TLS для удаленного управления») выводится следующая запись в файле журнала:

```
09.11.2023  11:17:16
 Созданы новые ключи аутентификации
  ТМ  АДМИНИСТРАТОРА (основная)
```

При запуске (подробнее см. пункт «Главное меню ФПСУ-TLS») выводится следующая запись в файле журнала:

```
09.11.2023  11:17:32
 Попытка входа с использованием ТМ
  Пункт меню       Доступ разрешен: Запуск ФПСУ
  Требуемая ТМ     ОПЕРАТОРА 1 (основная)
  Предъявлена ТМ   АДМИНИСТРАТОРА (основная)
```

В данном случае для прохождения процедуры контроля целостности ключа запуска требовалось предъявление минимальных прав ТМ оператора.

При попытке доступа к не разрешенным данному пользователю функциям (см. пункт «Разграничение доступа и пользователи») выводится следующая запись в файле журнала:

```
07.12.2023  13:30:04
 Попытка входа с использованием ТМ
  Пункт меню       Отказано в доступе: Настройка системы...->Установка дополнений/изменений
  Требуемая ТМ     Установщика (основная)
  Предъявлена ТМ   ОПЕРАТОРА 1 (основная)
```

Под термином «Установщик» в журнале понимается главный администратор ФПСУ-TLS, имеющий право на установку ПО.

Результаты контроля целостности ФПСУ-TLS выводятся следующей записью в файле журнала:

```
08.11.2023  14:20:38
 Попытка входа с использованием ТМ
  Пункт меню       Доступ разрешен: Проверка целостности...->По внутренним данным без записи резу
  Требуемая ТМ     АДМИНИСТРАТОРА (основная)
  Предъявлена ТМ   АДМИНИСТРАТОРА (основная)
```

Установка и удаление собственного сертификата и секретного ключа ФПСУ-TLS (см. раздел «Установка сертификатов») отображаются в файле журнала следующей записью:

```
09.11.2023  10:11:08
 Установка соб.сертификата и ключа
  Сер.номер: 5052495654303063D3
  Имя:server11.ami,Amicon,Certificate Authority
  Кем выдан:Root gost2012_512 created 11:24:03 14.02.2021,Amicon,Certificate Authority

09.11.2023  10:09:32
 Удаление соб.сертификата и ключа
  Сер.номер: 5052495654303063D3
  Имя:server11.ami,Amicon,Certificate Authority
  Кем выдан:Root gost2012_512 created 11:24:03 14.02.2021,Amicon,Certificate Authority
```

Удаление и установка корневого сертификата ФПСУ-TLS (см. раздел «Установка сертификатов») отображаются в файле журнала следующей записью:

```
09.11.2023  10:09:32
 Удаление корневого сертификата
  Сер.номер: 4939DC6F0AB2D3F191B981A7D409613624A86EE7
  Имя:Root gost2012_512 created 11:24:03 14.02.2021,Amicon,Certificate Authority

09.11.2023  10:11:08
 Установка корневого сертификата
  Сер.номер: 4939DC6F0AB2D3F191B981A7D409613624A86EE7
  Имя:Root gost2012_512 created 11:24:03 14.02.2021,Amicon,Certificate Authority
```

Установка дополнений/изменений (см. пункт «Обновление программного обеспечения») отображаются в файле журнала следующей записью:

```
11.12.2023  15:18:14
 Попытка входа с использованием ТМ
  Пункт меню       Доступ разрешен: Настройка системы...->Установка дополнений/изменений
  Требуемая ТМ     Установщика (основная)
  Предъявлена ТМ   АДМИНИСТРАТОРА (основная)
11.12.2023  15:18:34
 Установка дополнений/изменений
  Аннотация: ФПСУ-TLS v.3.1.16b
```

7. 11. 8. Настройки СКЗИ

Команда «Настройки СКЗИ» меню «Настройка системы» предназначена для перехода в интерфейс отключения подсистемы автозапуска, повторной инициализации программно-клавиатурного датчика случайных чисел, управления сроками действия ключевых данных ФПСУ-TLS.

Рисунок 185 - Меню настройки системы ФПСУ-TLS

При выполнении команды «Настройки СКЗИ» происходит переход в меню «Настройки СКЗИ», содержащее следующие пункты:

Рисунок 186 - Меню настройки СКЗИ ФПСУ-TLS

- «Отключение автозапуска» – переход в окно регистрации ТМ-идентификаторов для отключения подсистемы автозапуска ФПСУ-TLS (см. пункт «Отключение автозапуска»);
- «Переинициализация ПДСЧ» – команда запуска процедуры повторной инициализации программного датчика случайных чисел (см. пункт «Переинициализация ПДСЧ»);
- «Загрузка ключа ПДСЧ из файла» – команда, позволяющая загрузить ключ ПДСЧ из файла, выданного ЦВК. Команда предназначена для программных комплексов ФПСУ-TLS, функционирующих под управлением виртуальных машин и программно-аппаратных комплексов ФПСУ-TLS, где не используется БиоДСЧ (см. пункт «Загрузка ключа ПДСЧ из файла»);
- «Установка срока действия ключей» – переход в окно управления сроками действия ключевых данных ФПСУ-TLS (см. пункт «Установка срока действия ключей»);
- «Удаление СКЗИ» – команда, запускающая процедуру удаления программного обеспечения ФПСУ-TLS с аппаратной платформы или виртуальной машины (см. пункт «Удаление программного обеспечения ФПСУ-TLS»).

Возвращение в меню «Настройка системы» осуществляется по клавише <*Esc*>.

7. 11. 8. 1. Отключение автозапуска

Команда «Отключение Автозапуска» предназначена для отключения подсистемы автозапуска, если она была ранее задействована локальным администратором. Команда «Отключение Автозапуска» выполняется из пункта «Настройки СКЗИ». Выполнение команды при включенной подсистеме автозапуска не требует авторизации и может быть выполнена любым пользователем.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 187 - Подтверждение полномочий и ввод пароля ТМ

При выполнении команды осуществляется переход в окно регистрации ТМ-идентификаторов, где система предлагает пользователю подтвердить или отклонить отключение подсистемы автозапуска:

Рисунок 188 - Подтверждение отключения подсистемы автозапуска

Отключение системы автозапуска (выбор опции «Да») сопровождается перезагрузкой ФПСУ-TLS, во время которой удаляется ключ автозапуска.

Для отмены отключения системы автозапуска, выберите опцию «Нет».

7. 11. 8. 2. Переинициализация ПДСЧ

Команда «Переинициализация ПДСЧ» подменю «Настройки СКЗИ» предназначена для повторной инициализации программного датчика случайных чисел (ПДСЧ) ФПСУ-TLS средствами биологического датчика случайных чисел (БиоДСЧ). Частота повторной инициализации программного датчика случайных чисел ФПСУ-IP регулируется правилами пользования СКЗИ.

ВНИМАНИЕ! Программным комплексам ФПСУ-TLS, функционирующим под управлением виртуальных машин, запрещается проводить повторную инициализацию ПДСЧ средствами БиоДСЧ.

Рисунок 189 - Команда повторной инициализации ПДСЧ

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

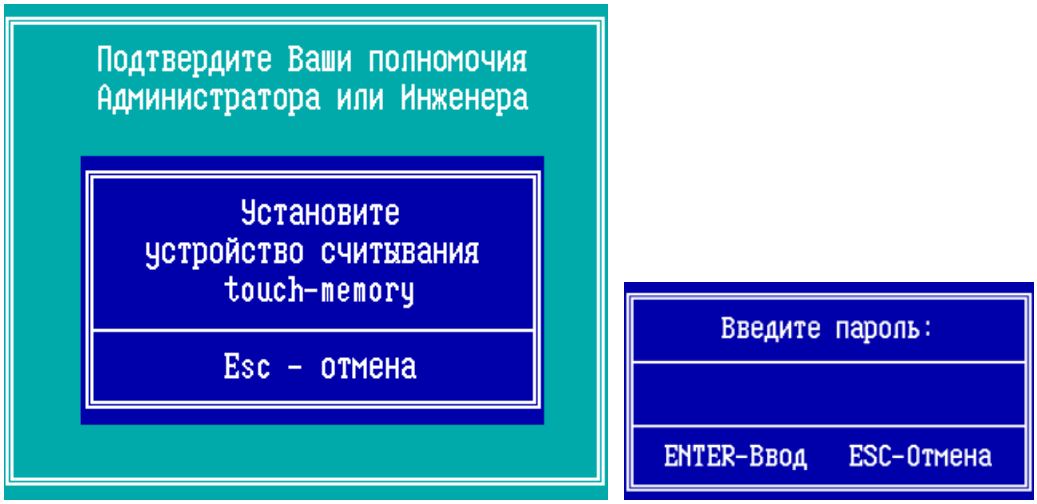


Рисунок 190 - Подтверждение полномочий и ввод пароля ТМ

При выборе команды «Переинициализация ПДСЧ» будет запущен интерфейс биологического датчика случайных чисел. От администратора требуется двигать мышью в пределах экрана:

Рисунок 191 - Биологический датчик случайных чисел

Переинициализация ПДСЧ завершится успешно, как только датчик обработает достаточное количество движений мыши. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <*Esc*> обратно в подменю «Настройки СКЗИ».

7. 11. 8. 3. Загрузка ключа ПДСЧ из файла

Загрузка ключа ПДСЧ из файла, выданного ЦВК, производится для программных комплексов ФПСУ-TLS, функционирующих под управлением виртуальных машин и программно-аппаратных комплексов ФПСУ-TLS, где не используется БиоДСЧ. Частота загрузки ключа ПДСЧ из файла на ФПСУ-TLS регулируется правилами пользования СКЗИ.

Подключите к ФПСУ-TLS USB-носитель с файлом ключа ПДСЧ и выберите команду меню «Загрузка ключа ПДСЧ из файла» подменю «Настройки СКЗИ»:

Рисунок 192 - Команда «Загрузка ПДСЧ из файла»

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

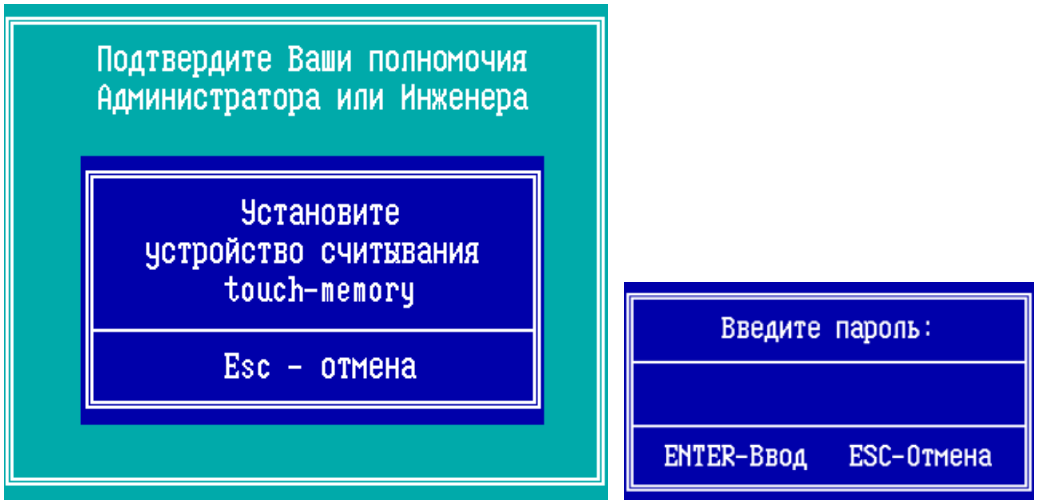
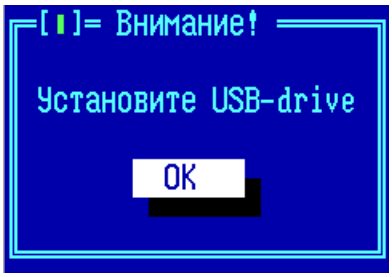


Рисунок 193 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения полномочий и ввода пароля ТМ, если USB-носитель предварительно не подключен, то система предложит подключить к ФПСУ-TLS USB-носитель с файлом ключа ПДСЧ. Подключите носитель к ФПСУ-TLS и подтвердите выполнение команды, нажав клавишу Enter.



Если USB-носитель будет обнаружен ФПСУ-TLS, то откроется окно диалога, в котором следует выбрать файл на носителе.

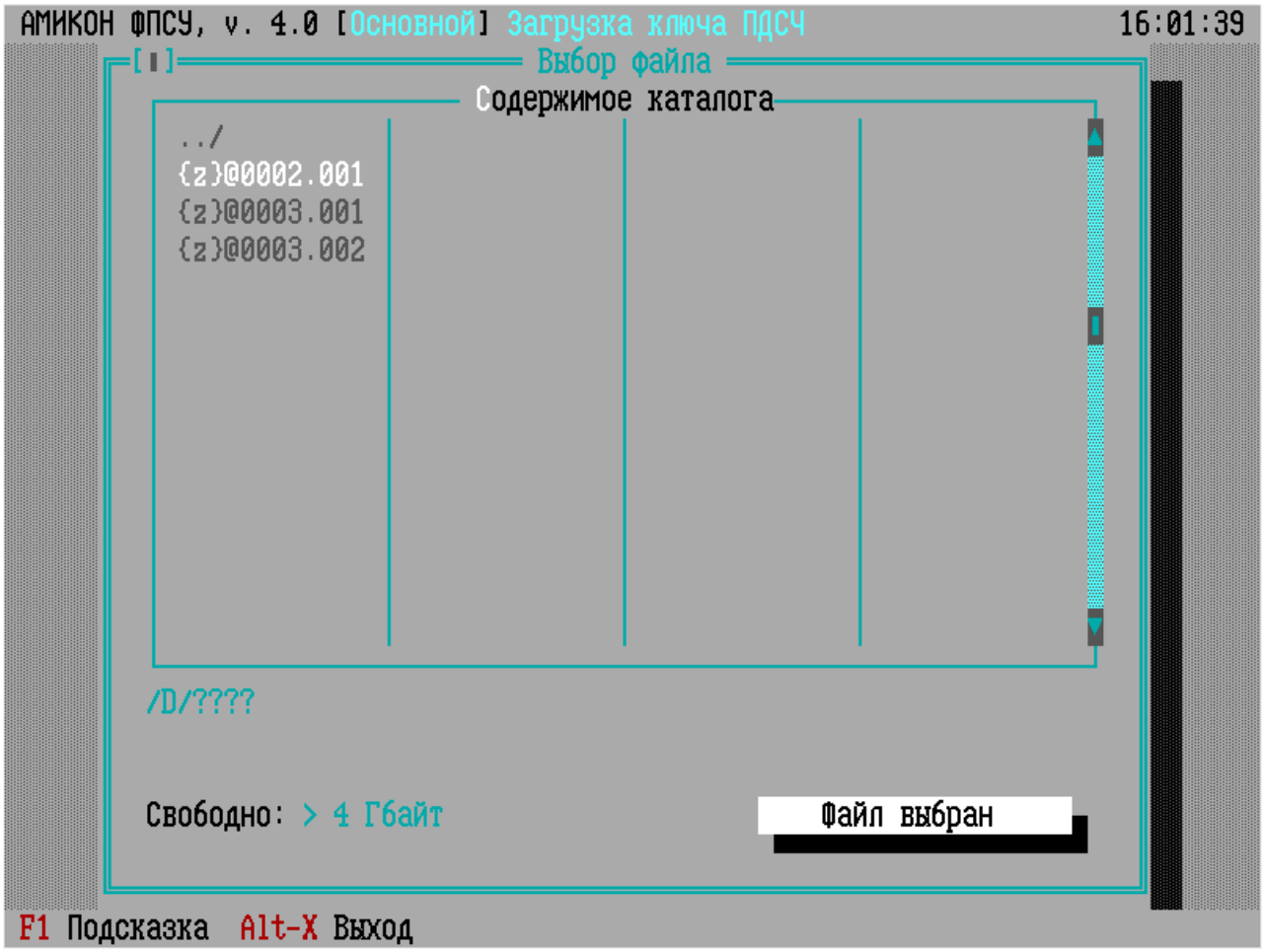


Рисунок 194 - Выбор файла для загрузки

Переместите курсор на выбранный файл. Переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>. Подтвердите выбор файла, нажав на клавишу <*Enter*>. В открывшемся окне отобразится информация о ЦВК, выдавшем файл с ключом ПДСЧ и предложением загрузить этот файл.

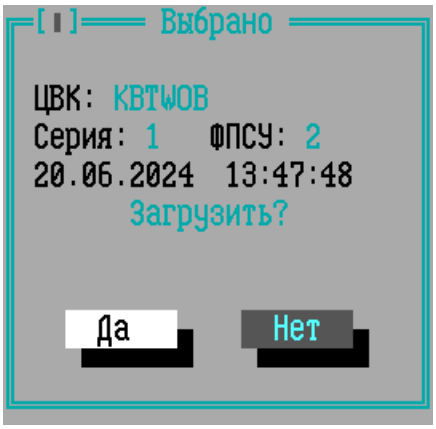


Рисунок 195 - Информация о загружаемом файле

После загрузки файла, ФПСУ-TLS выдаст системное оповещение о завершении процедуры:

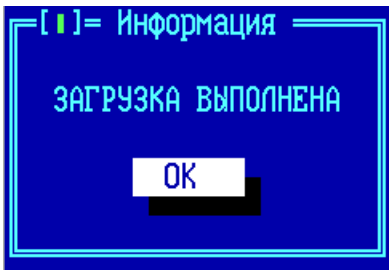


Рисунок 196 - Файл загружен

7. 11. 8. 4. Установка срока действия ключей

Команда «Установка времени действия ключей» меню «Настройки СКЗИ» предназначена для доступа в интерфейс настройки времени действия ключа ПДСЧ ФПСУ-TLS и ключа запуска ФПСУ-TLS.

Рисунок 197 - Команда «Установка времени действия ключей»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 198 - Подтверждение полномочий и ввод пароля ТМ

При выполнении команды будет предложен выбор типа ключа, для которого будут выполнены настройки сроков действия. Настройки для каждого типа ключа выполняются и сохраняются отдельно:

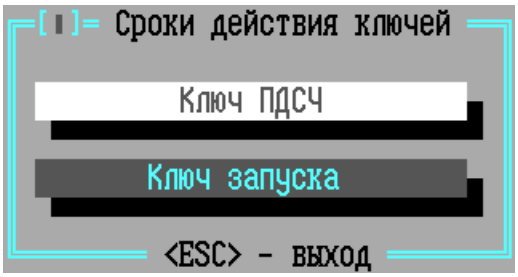


Рисунок 199 - Выбор типа ключа

При выборе пункта меню «Ключ ПДСЧ» или «Ключ запуска» открывается окно настроек сроков действия выбранного ключа, в котором указывается дата создания ключа и текущие настройки.

Рисунок 200 - Настройка сроков действия выбранного ключа

Параметры, доступные администратору для изменения:

Срок действия – число, обозначающее количество дней с даты создания, в течение которого ключ будет считаться рабочим;

Начать оповещение за – число, обозначающее количество дней до срока прекращения действия ключа, с которого на экран при запуске ФПСУ-TLS будет выводиться сообщение о приближающемся окончании срока действия ключа;

Интервал оповещения – число от 1 до 14, обозначающее количество дней, через которое оповещение о приближающемся сроке прекращение действия ключа будет повторяться.

8. Утилиты

Утилиты позволяют смотреть текущие настройки состояния сети и ФПСУ-TLS.

Примечание. ФПСУ-TLS использует стандартные утилиты Linux для просмотра текущего состояния сети: ping, traceroute, ifconfig, netstat, route, arp, dmesg, top, df.

Операция доступна администраторам класса *Оператор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

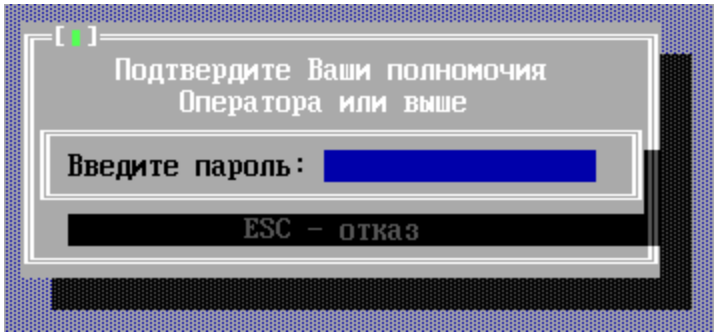


Рисунок 201 - Подтверждение полномочий и ввод пароля ТМ

На экран выдается окно «Утилиты» по нажатию сочетания клавиш <Alt+F2>:

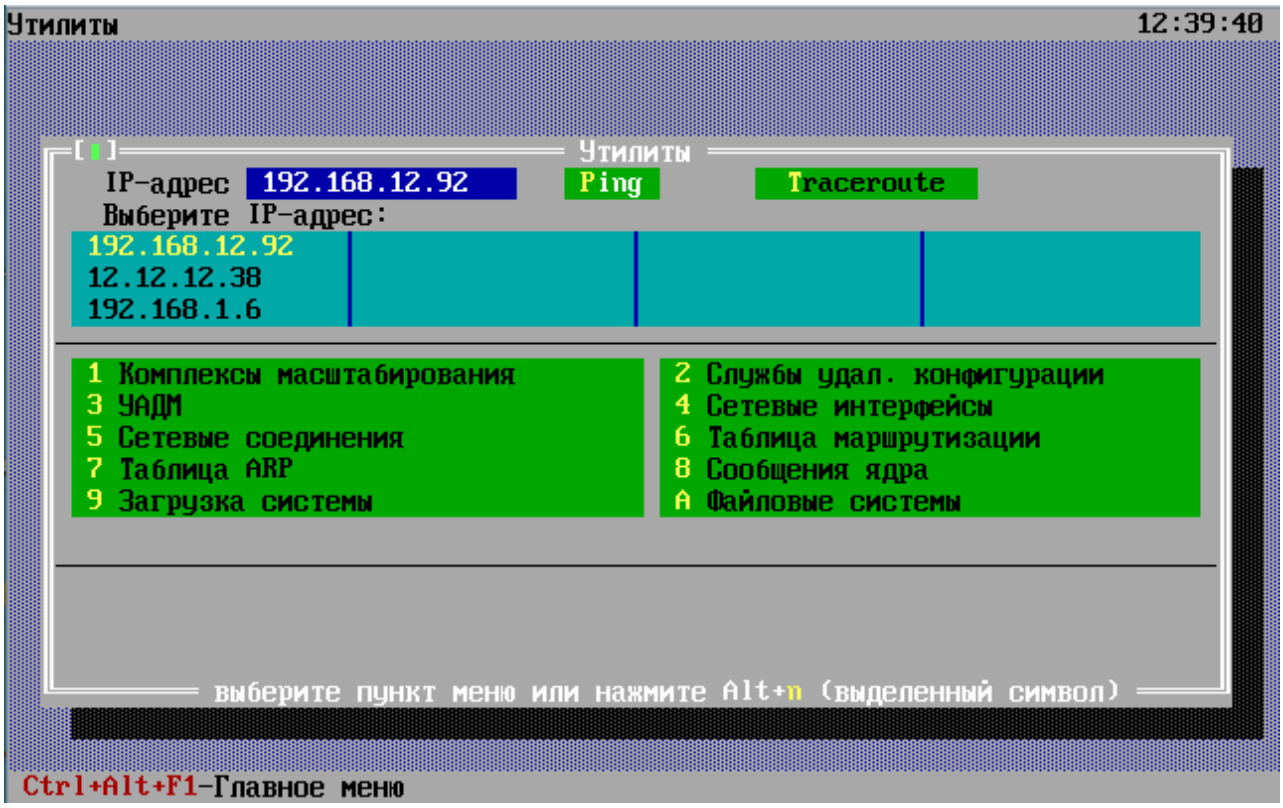


Рисунок 202 - Окно с утилитами ФПСУ-TLS

В окне отображается список обслуживаемых ФПСУ-TLS серверов. Для выбора IP-адреса нажмите клавишу <Enter>. Для выбранного IP-адреса доступны команды:

`Ping` - команда для проверки работоспособности удаленного хоста.

`Traceroute`- команда показывает весь путь следования пакета от источника до узла назначения.

Утилита в меню выбирается по нажатию клавиш <Alt> и номера утилиты или по нажатию клавиши с номером утилиты. После запуска выбранной утилиты, возврат из интерфейса утилиты в окно меню осуществляется комбинацией клавиш <Ctrl+C>.

1. Комплексы масштабирования

Опция «Комплексы масштабирования» вызывается по нажатию клавиш <Alt+1> или <1>. На экран выдается информация о виртуальном адресе, о ФПСУ-TLS входящих в кластер, для каждого из которых отображается IP-адрес и статус устройства. Описание и настройка механизма масштабирования приведены в пунктах «Описание подсистемы масштабирования» и «Настройка подсистемы масштабирования».

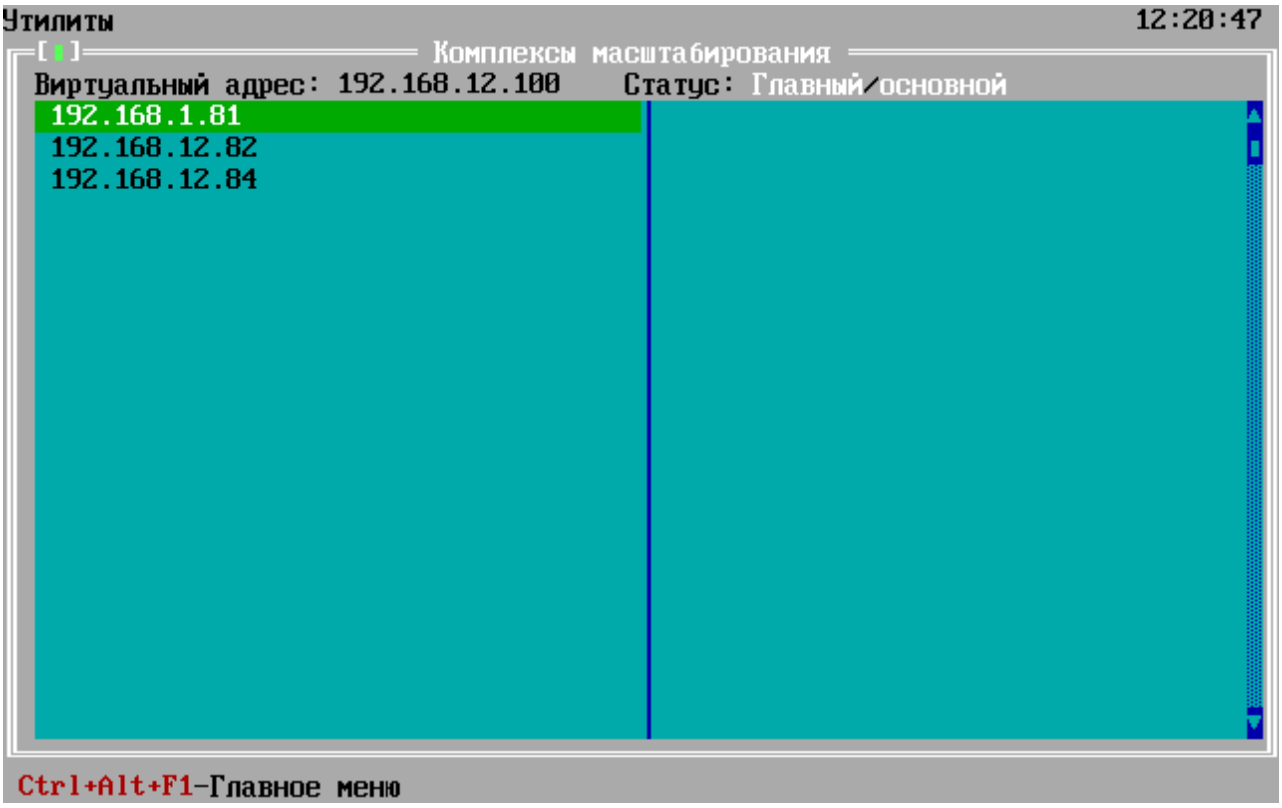


Рисунок 203 - Окно «Комплексы масштабирования»

2. Службы удаленной конфигурации

Опция «службы удал. конфигурации» вызывается по нажатию клавиш <Alt+2> или <2>. На экран выдаются сведения о скачиваемой конфигурации, датах создания и последнего изменения, а также сроке активации. В таблице выводятся IP-адреса партнеров ФПСУ-TLS, скачавших конфигурацию, сведения о переданном трафике и времени соединения.

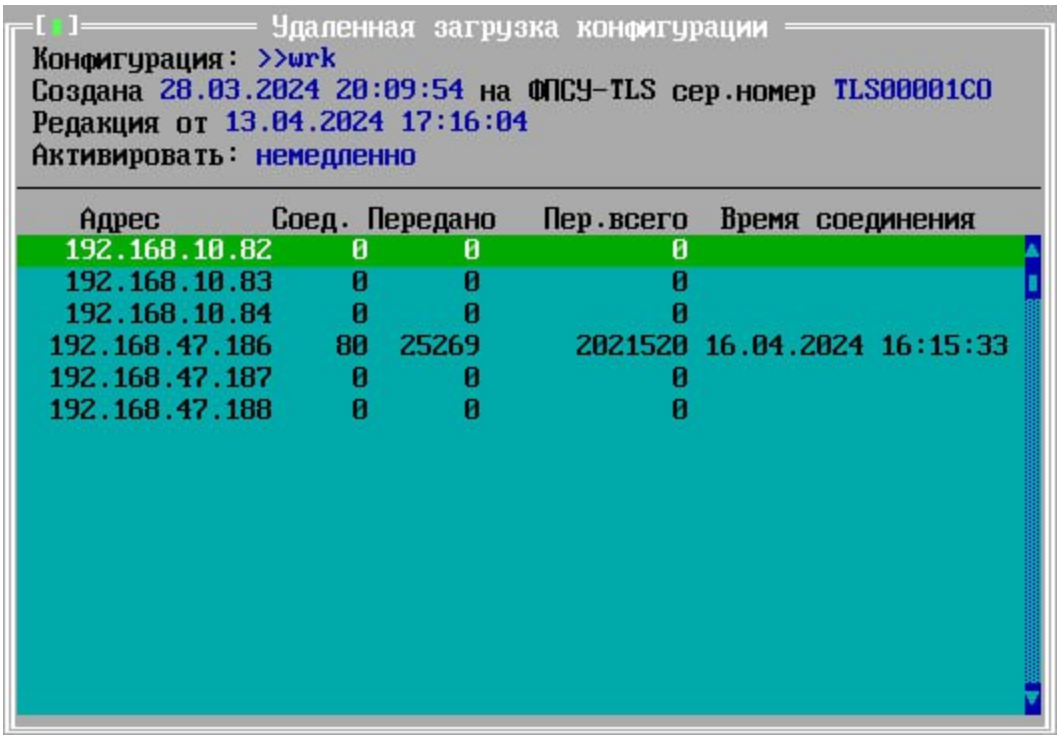


Рисунок 204 - Окно «Удаленная загрузка конфигурации»

3. Состояние УАДМ

Опция «УАДМ» вызывается по нажатию клавиш <Alt+3> или <3>. На экран выдаются сведения обо всех зарегистрированных на ФПСУ-TLS удаленных администраторах, для каждого администратора указываются:

- имя администратора, комментарий к имени;
- IP-адрес и порт АРМ удаленного администратора;
- текущее состояние соединения ФПСУ-TLS с удаленным администратором (готов, не готов, устанавливается);
- алгоритм, по которому строится туннель между ФПСУ-TLS и удаленным администратором;
- количество переданных данных за время существования соединения ФПСУ-TLS с АРМ удаленного администратора, в байтах и пакетах;
- количество ошибок соединения за время существования соединения ФПСУ-TLS с АРМ удаленного администратора;
- время и тип последнего запроса с АРМ удаленного администратора к ФПСУ-TLS;
- время последнего опроса текущего состояния ФПСУ-TLS удаленным администратором.

Рисунок 205 - Окно «Состояние удаленных администраторов»

4. Сетевые интерфейсы

Опция «Сетевые интерфейсы» вызывается по нажатию клавиш <Alt+4> или <4>, выполняет команду `ifconfig` для просмотра текущих параметров сети и состояния сетевых интерфейсов. На экране выводится информация о назначении сетевого адреса, настройках параметров сетевого адаптера и IP протокола.

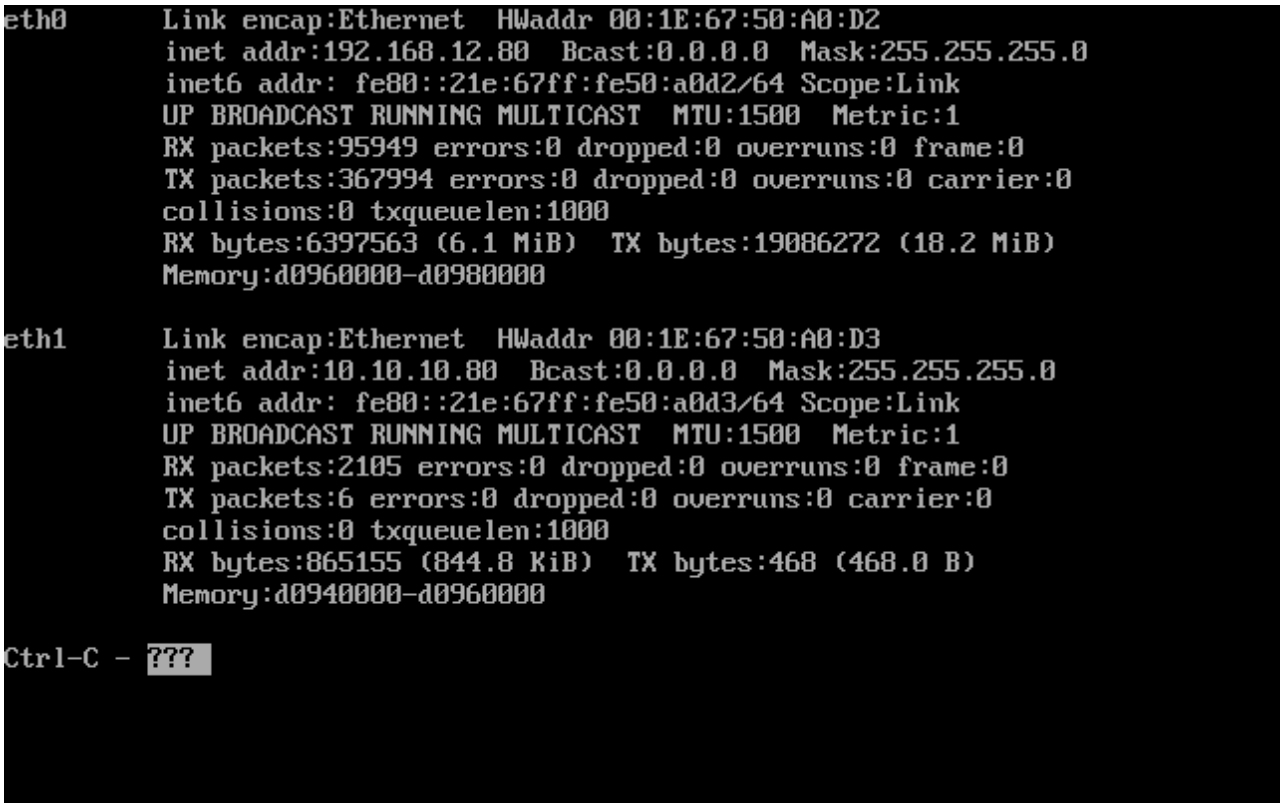


Рисунок 206 - Окно «Сетевые интерфейсы»

5. Сетевые соединения

Опция «Сетевые соединения» вызывается по нажатию клавиш <Alt+5> или <5>, выполняет команду `netstat` для поиска сетевых проблем и определения производительности сети. На экране выводится список активных соединений.

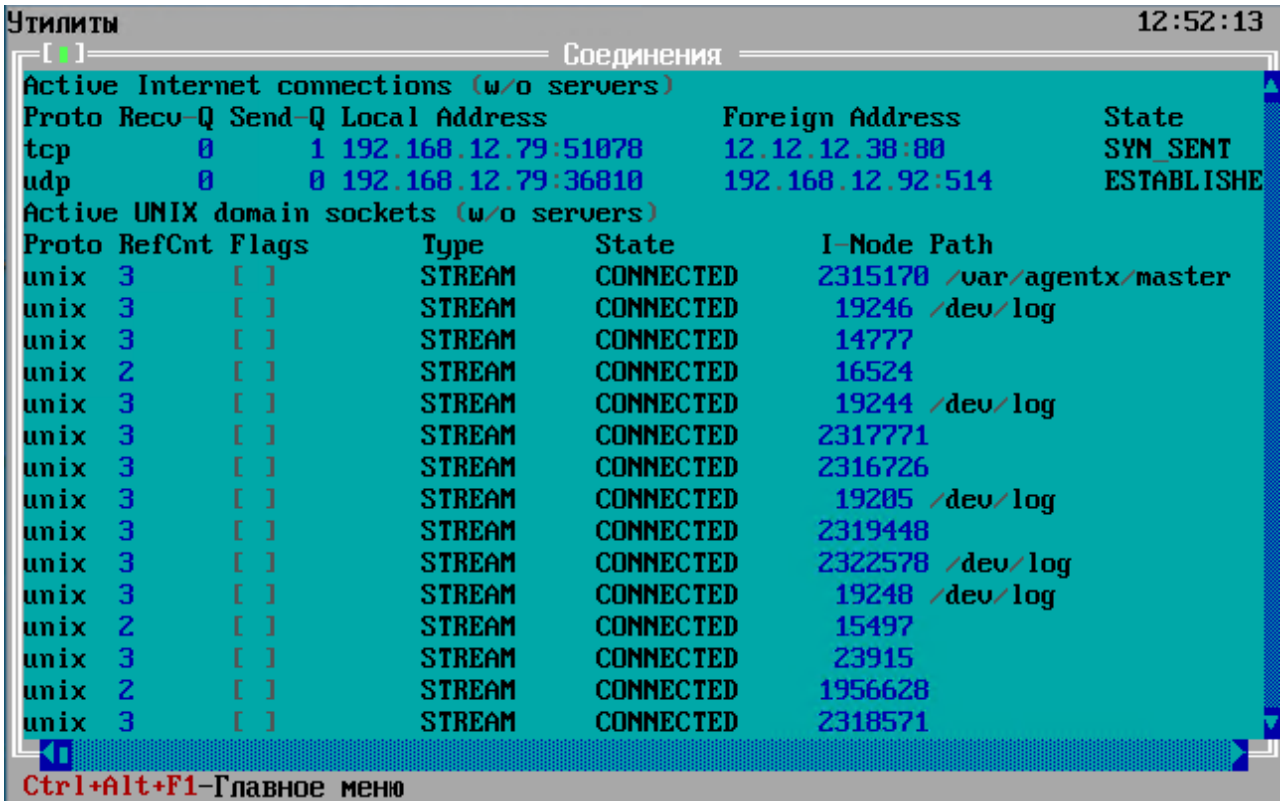


Рисунок 207 - Окно «Сетевые соединения»

6. Таблица маршрутизации

Опция «Сетевые соединения» вызывается по нажатию клавиш <Alt+6> или <6>, выполняет команду `route` для просмотра таблицы маршрутизации.

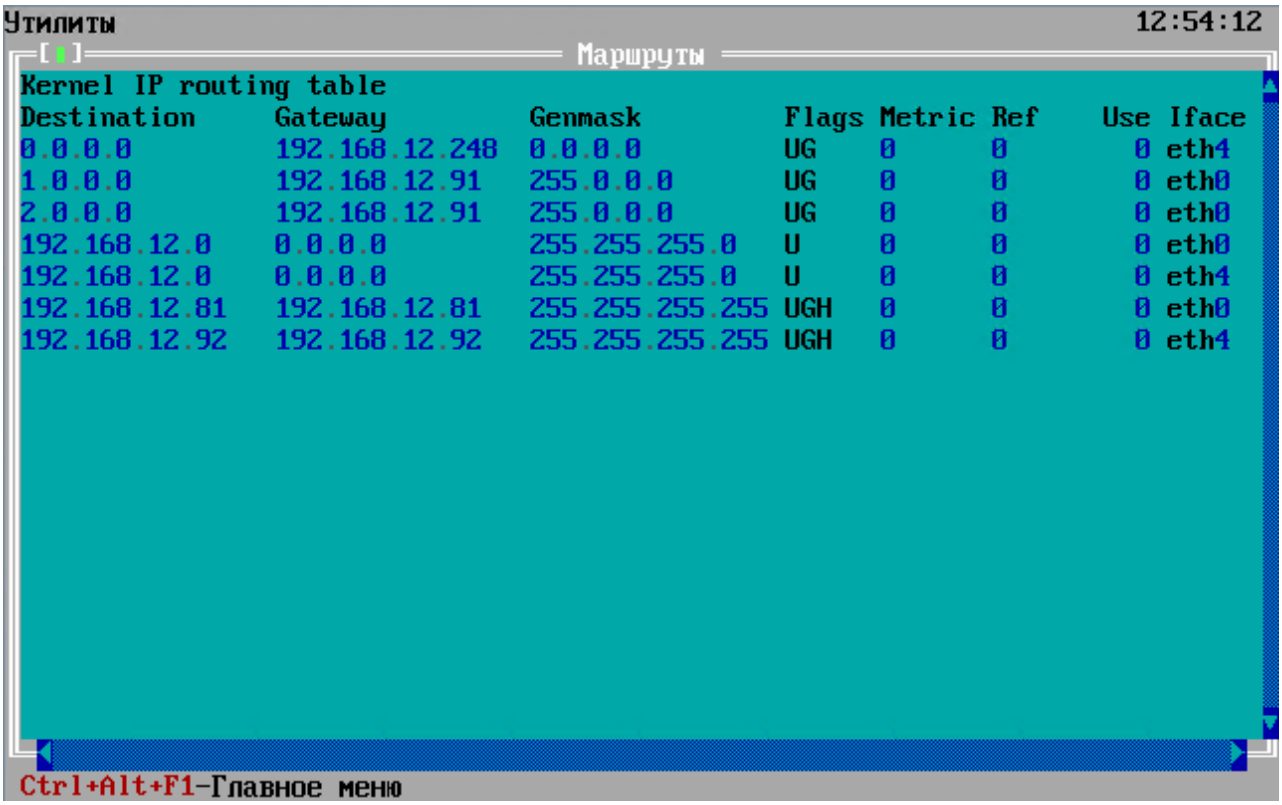


Рисунок 208 - Окно «Таблица маршрутизации»

7. Таблица ARP

Опция «Таблица ARP» вызывается по нажатию клавиш <Alt+7> или <7>, выполняет команду `arp` для вывода записей ARP-таблицы. Запись ARP-таблицы включает IP-адрес, соответствующий ему MAC-адрес с указанием интерфейса.

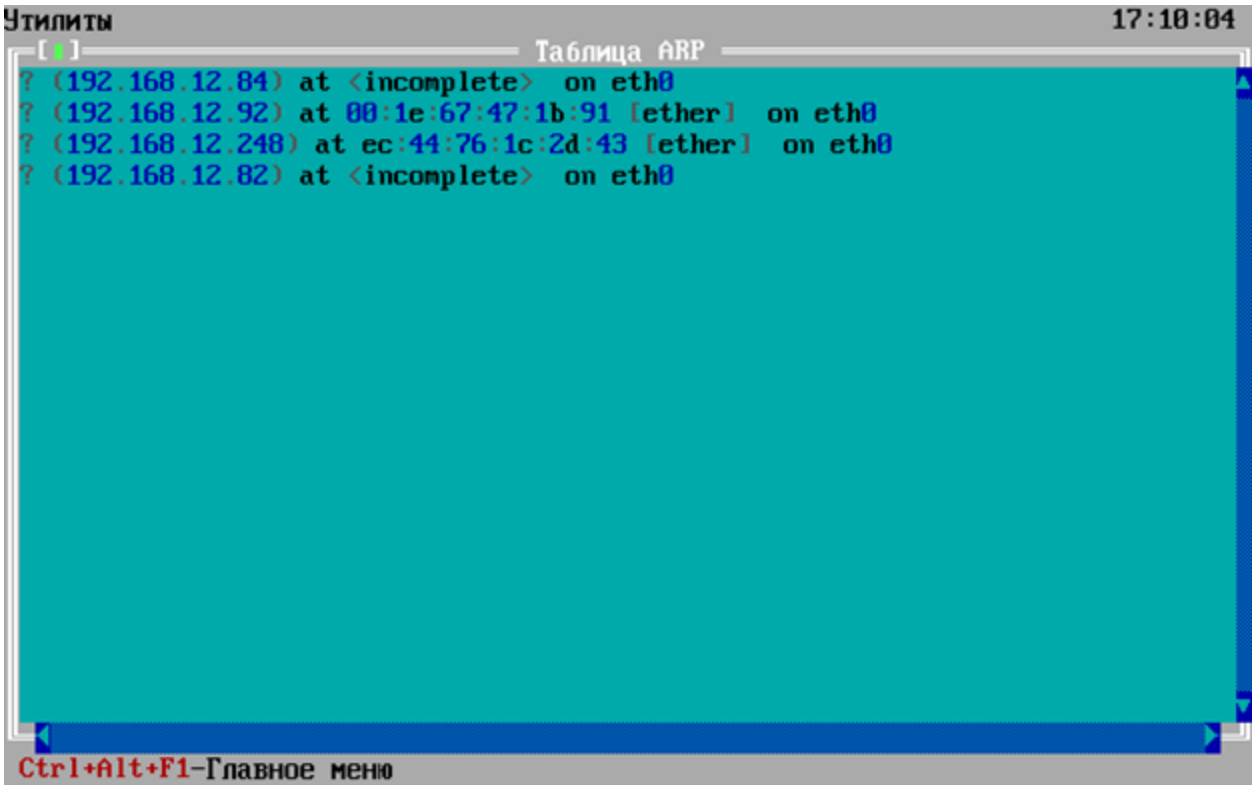


Рисунок 209 - Окно «Таблица ARP»

8. Сообщения ядра

Опция «Сообщения ядра» вызывается по нажатию клавиш <Alt+8> или <8>, выполняет команду `dmesg` для вывода информации о процессе загрузки ядра, включая информацию обо всех устройствах, которые были идентифицированы в процессе загрузки системы. На экран выводится версия ядра, версия компилятора gcc, карта физической памяти.

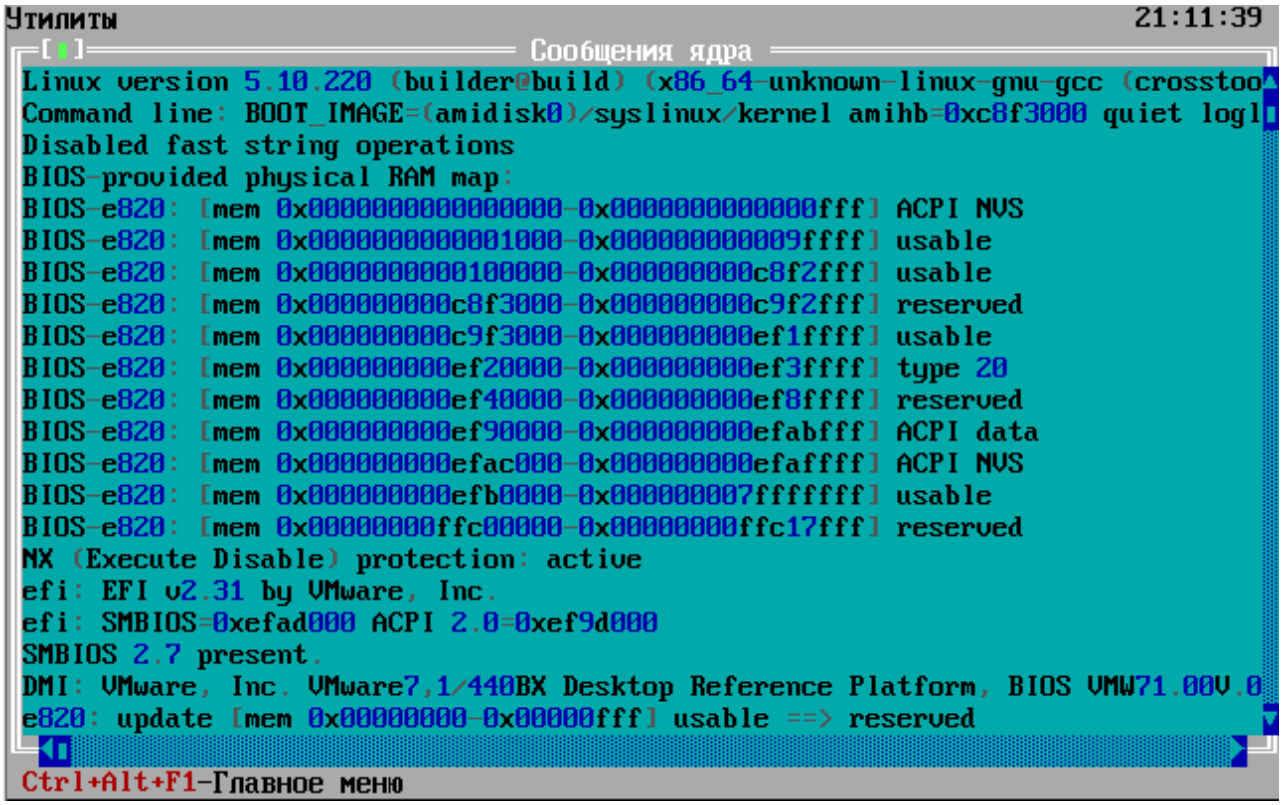


Рисунок 210 - Окно «Сообщения ядра»

9. Загрузка системы

Опция «Загрузка системы» вызывается по нажатию клавиш <Alt+9> или <9>, выполняет команду `top`, выводит список работающих в операционной системе процессов и информацию о них.

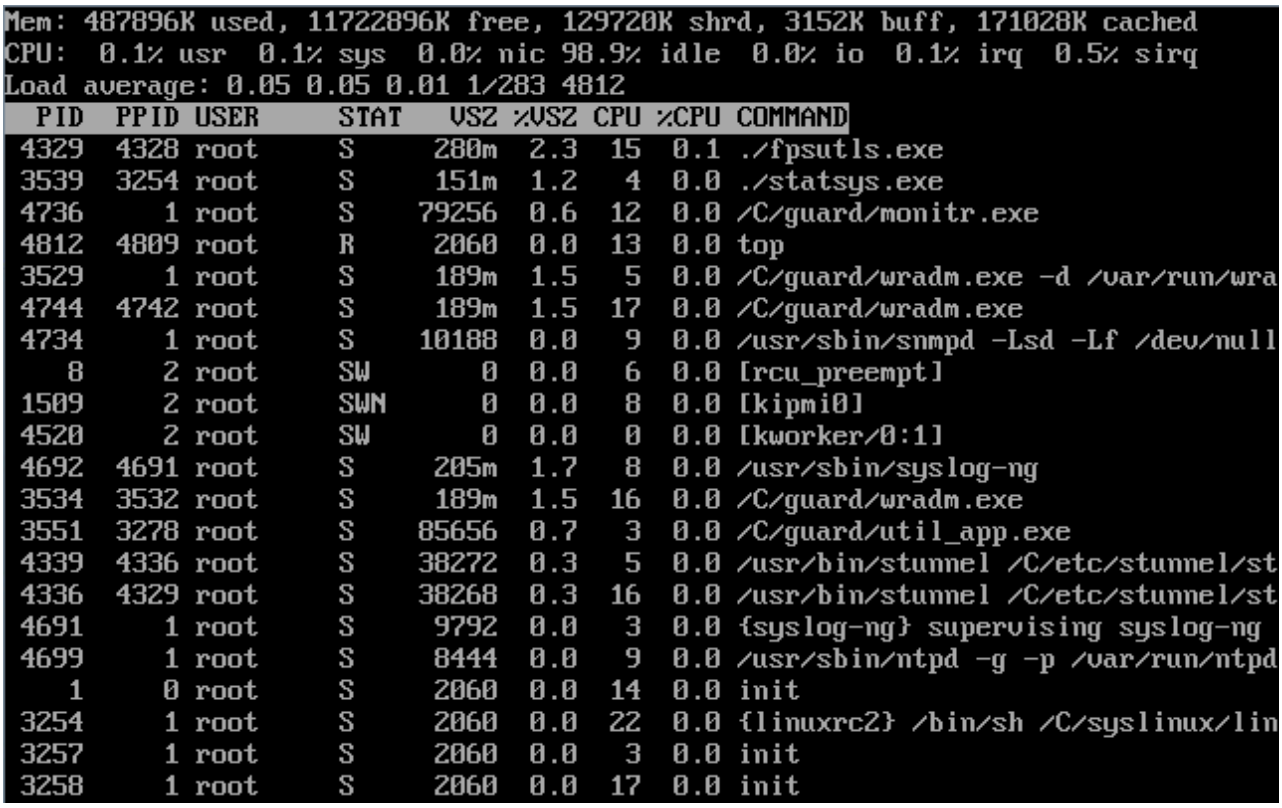


Рисунок 211 - Окно «Загрузка системы»

A. Файловые системы

Опция «Файловые системы» вызывается по нажатию клавиш <Alt+A> или <A>, выполняет команду `df`, выдаёт отчёт о доступном и использованном дисковом пространстве на файловых системах.

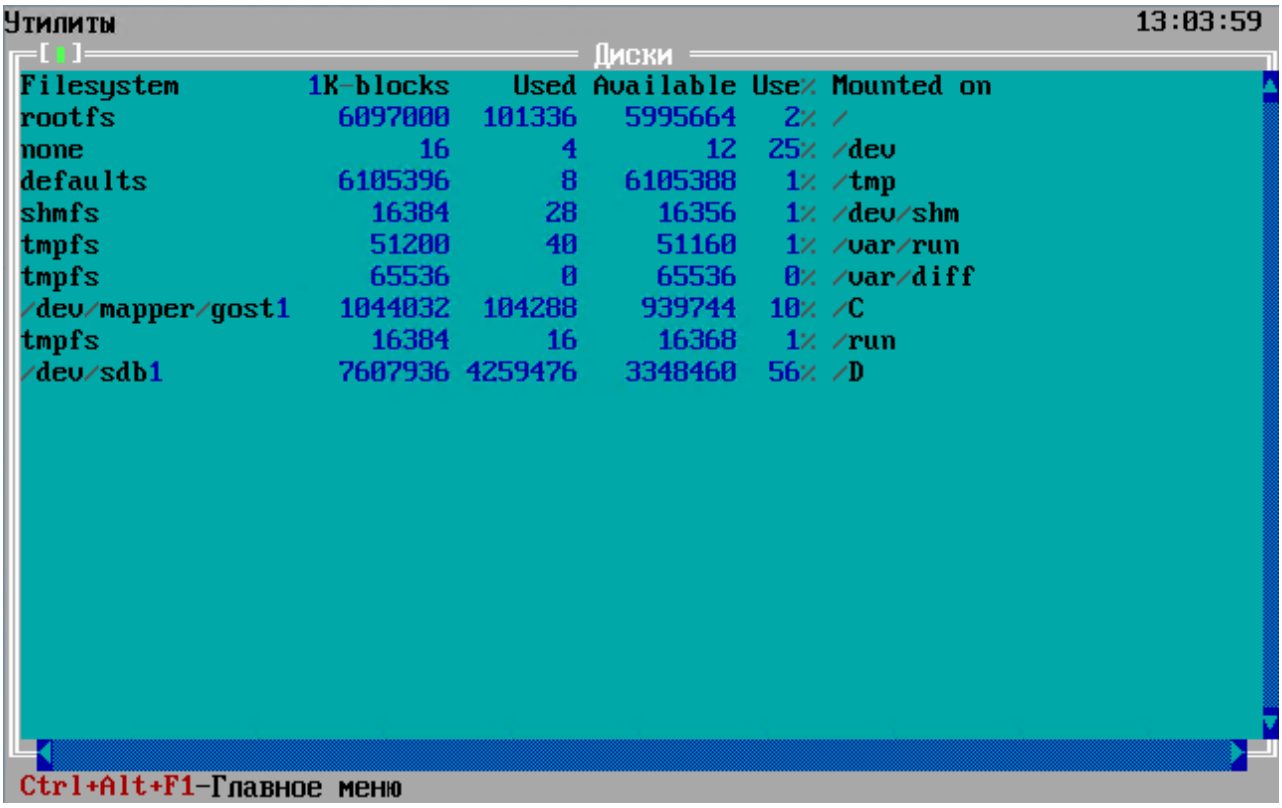


Рисунок 212 - Окно «Файловые системы»

9. Восстановление работы ФПСУ-TLS после сбоев

Сбои оборудования не влияют на защитные функции ФПСУ-TLS, однако некоторые аппаратные неполадки могут нарушить его работоспособность, что приведет к недоступности защищаемых им http-серверов.

При авариях такого оборудования аппаратной части ФПСУ-TLS, как ЦПУ, материнская плата, блок питания и др., неисправные устройства могут быть заменены на аналогичные, после чего ФПСУ-TLS может быть запущен заново для продолжения своей работы. Аварии жесткого диска ФПСУ-TLS, влекущие за собой необходимость его замены и повторной установки ПО и сертификатов ФПСУ-TLS на новый жесткий диск, наиболее критичны в смысле времени восстановления работоспособности ФПСУ-TLS и защищаемых им Веб-Сервисов, поскольку все рабочие установки ФПСУ-TLS и записанные на жесткий диск данные будут потеряны.

Для быстрого восстановления работы следует хранить текущую конфигурацию ФПСУ-TLS на внешнем носителе. В таком случае при смене жесткого диска и повторной инсталляции ПО ФПСУ-TLS (или замене всей аппаратной платформы ФПСУ-TLS) администратор может восстановить конфигурацию ФПСУ-TLS с носителя. Для осуществления восстановления необходимы права класса «Администратор» или «Главный администратор».

Для восстановления текущей конфигурации ФПСУ-TLS:

- запустить ФПСУ-TLS;
- в главном меню выбрать команду «Конфигурация ФПСУ»;
- подтвердить права администратора;
- вставить внешний носитель с текущей конфигурацией ФПСУ-TLS;
- выбрать конфигурацию ФПСУ-TLS;
- загрузить конфигурацию ФПСУ-TLS.

Для возобновления работы ФПСУ-TLS после сбоев электропитания без участия оператора ФПСУ-TLS комплектуется **подсистемой автоматического старта**.

Во избежание нарушений межсетевого взаимодействия защищенных серверов локальной сети, рекомендуется использовать как минимум два ФПСУ-TLS, работающих в режиме распределения нагрузки (масштабирования). Подробнее см. пункт «Масштабирование».

10. Способы разрешения возможных проблем при работе ФПСУ-TLS

Несмотря на то, что подключение ФПСУ-TLS в существующую сеть передачи данных не требует переконфигурирования сетевого оборудования, при первом его запуске после подключения к сети возможны ситуации, когда для нормализации работы сети необходимо предпринять специальные действия.

Это обусловлено тем, что ARP-таблицы сетевого оборудования после установки ФПСУ-TLS будут содержать устаревшие сведения (ARP-записи) об адресах сетевых адаптеров хостов или другого сетевого оборудования, которые могут обновиться только после истечения «времени жизни» записи. Это время задается в конфигурации сетевого оборудования и может оказаться достаточно большим (например, в некоторых моделях маршрутизаторов фирмы Cisco это время может быть равно 4 часам). Понятно, что в течение периода «жизни» устаревших записей необходимо предпринять специальные меры, чтобы восстановить прежнее состояние работы сети и доступ к некоторым хостам защищаемой области.

Для нормализации работы сети в данной ситуации рекомендуется принять следующие меры:

В случае, если ФПСУ-TLS устанавливается между защищаемой областью и ее пограничными маршрутизаторами - очистить ARP-таблицы пограничных маршрутизаторов или перезапустить маршрутизаторы;

Если между защищаемой областью и ФПСУ-TLS пограничные маршрутизаторы отсутствуют — очистить ARP-таблицы «пассивных» хостов или сетевого оборудования, либо перезапустить их, либо осуществить с них попытку обмена пакетами с другими хостами или сетевым оборудованием.

В случае отсутствия пакетов на одном их портов или появления большого числа ошибочных пакетов ФПСУ-TLS на экранах служебных утилит (см. описание окна «Сетевые интерфейсы» пункта «Утилиты») следует проверить работоспособность и тип применяемого сетевого кабеля и убедиться в его соответствии подключенному оборудованию (коммутатору, концентратору, маршрутизатору).

В случае появления на экранах ФПСУ-TLS не указанных документации сообщений следует обратиться в техническую поддержку производителя.

11. Инсталляция ПО ФПСУ-TLS

Программно-аппаратный комплекс ФПСУ-TLS в общем случае поставляется с предустановленным программным обеспечением. Повторная установка программного обеспечения возможна в случае необходимости или при раздельной проставке комплекса ФПСУ-TLS в виде дистрибутива и аппаратной платформы без предустановленного программного обеспечения.

Программный комплекс ФПСУ-TLS для виртуальных машин в общем случае поставляется в виде образа с предустановленным программным обеспечением для определенного при заказе типа виртуальной машины (VMware, QEMU/KVM). Повторная установка программного обеспечения возможна в случае необходимости или при проставке комплекса ФПСУ-TLS в виде дистрибутива. Виртуальная машина должна быть предварительно настроена на работу с комплексом ФПСУ-TLS, рекомендуется предварительно ознакомиться с процедурами настройки (см. раздел «ФПСУ-TLS в виртуальной машине»).

Процедуры установки программного обеспечения приведены в подразделах далее.

11. 1. Установка на аппаратную платформу

Программно-аппаратный ФПСУ-TLS поставляется с предустановленным программным обеспечением, которое в случае необходимости можно повторно установить на аппаратную платформу ФПСУ-TLS. Для повторной установки программного обеспечения потребуются:

- аппаратная платформа ФПСУ-TLS;
- инсталляционный комплект программного обеспечения ФПСУ-TLS, состоящий из USB-носителя с дистрибутивами и ТМ-идентификатором Главного администратора для серийного номера устанавливаемого ФПСУ-TLS. Каждый инсталляционный комплект имеет свой уникальный серийный номер программного обеспечения, устанавливаемый ООО «АМИКОН».

Порядок действий при повторной инсталляции программного обеспечения на АП комплекса следующий:

1. Подключите USB-носитель с дистрибутивом программного обеспечения к ФПСУ-TLS.

2. При включении ФПСУ-TLS следует отменить загрузку подсистемы ACCESS-TM SHELL, запрещающей загружать операционную систему иначе как с защищенной внутренней памяти, и выбрать загрузку с USB. Это можно сделать при выборе Boot Options (обычно при нажатии F10) после включения ФПСУ-TLS, или напрямую зайдя в BIOS и установив в Boot Options первой загрузку USB2.0.

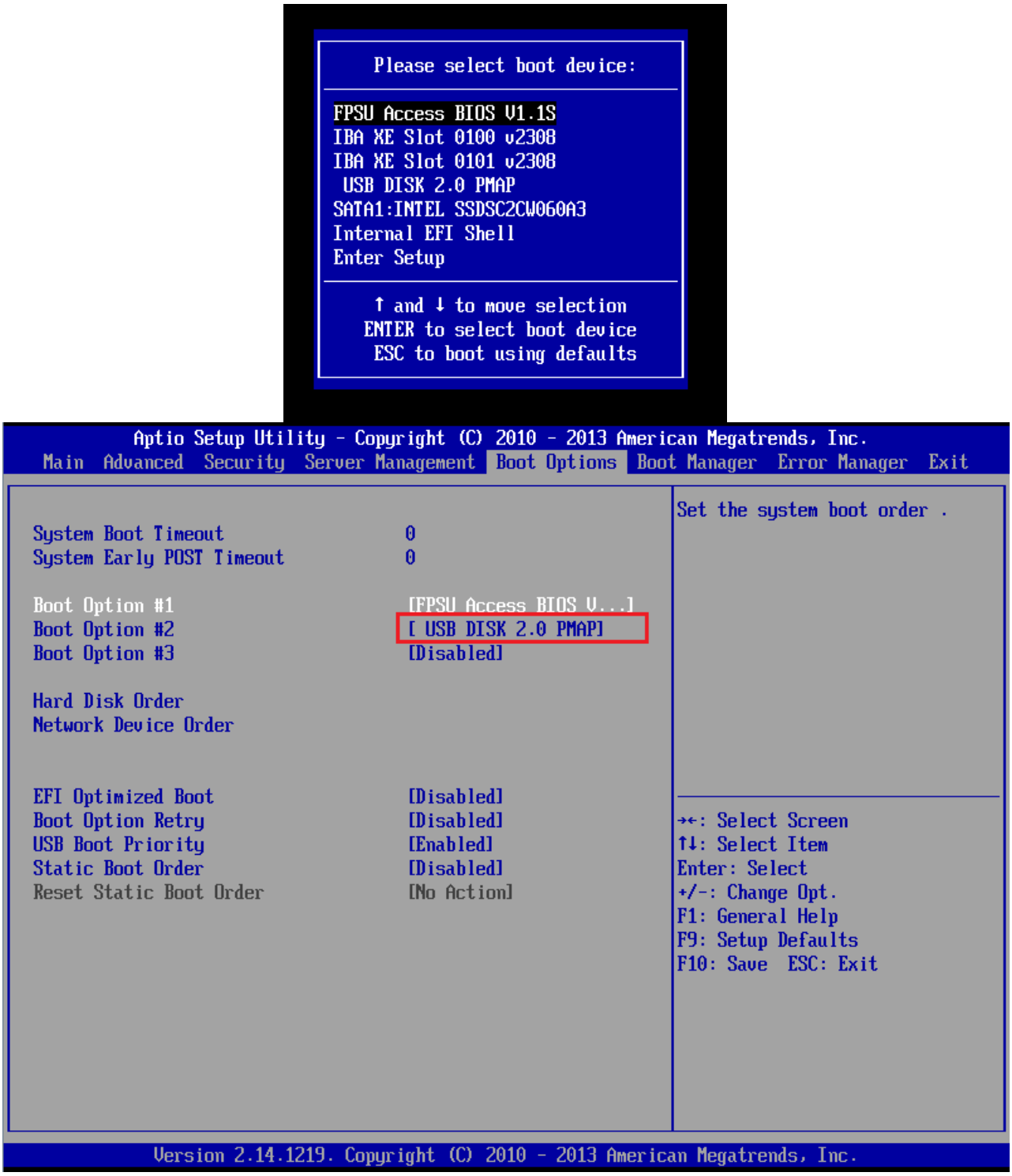


Рисунок 213 - Выбор загрузки с USB

3. Загруженная с инсталляционного USB-носителя программа начнет первый этап установки с проверки ранее установленного программного обеспечения ФПСУ-TLS. Если система была ранее установлена на ФПСУ-TLS, будет выдано

следующее сообщение:

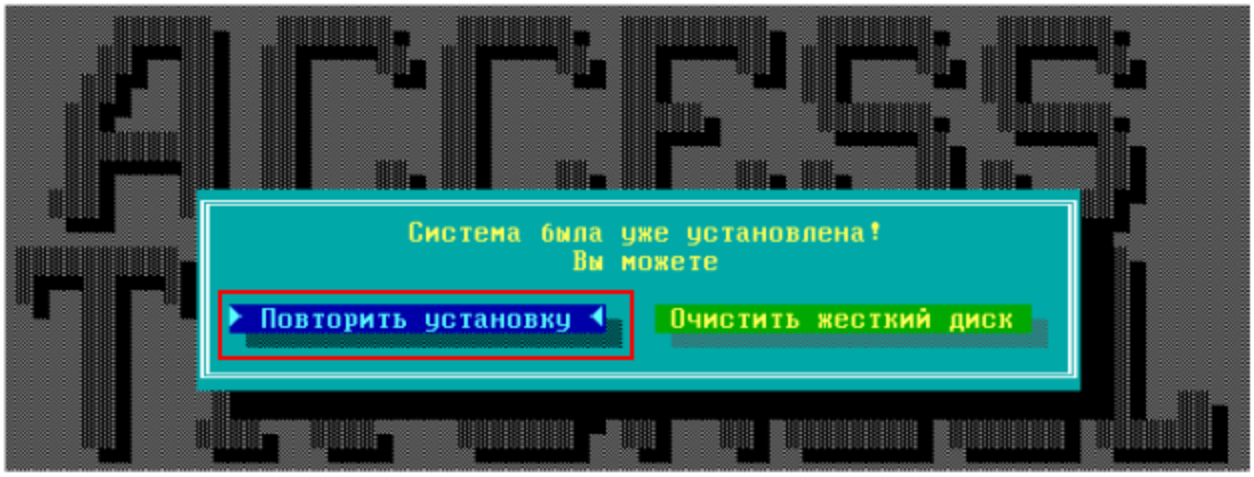


Рисунок 214 - Сообщение при повторной установке

Примечание. Здесь и далее выбор в окнах предлагаемых решений производится нажатием клавиши <Enter>. Месторасположение курсора отмечено синим цветом.

При выборе команды «Очистить жесткий диск» стираются все данных с внутреннего диска и происходит выход из инсталлятора без продолжения процедуры установки.

Выберите команду «Повторить установку» и нажмите <Enter>.

4. Для продолжения необходимо провести форматирование ПЗУ ФПСУ-TLS, на экране отобразится окно с сообщением для подтверждения процесса форматирования.

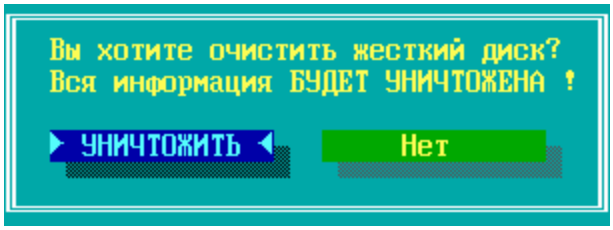


Рисунок 215 - Очистка ПЗУ ФПСУ-TLS

Команда «Нет» отменяет форматирование.

Выберите команду «УНИЧТОЖИТЬ» и нажмите <Enter>.

5. Далее рекомендуется провести тест-проверку работоспособности внутреннего накопителя информации. Для проведение данной проверки следует выбрать команду «Да» и подтвердить выбор нажатием клавиши <Enter>. Если проверка не закончится успешно, следует заменить накопитель.

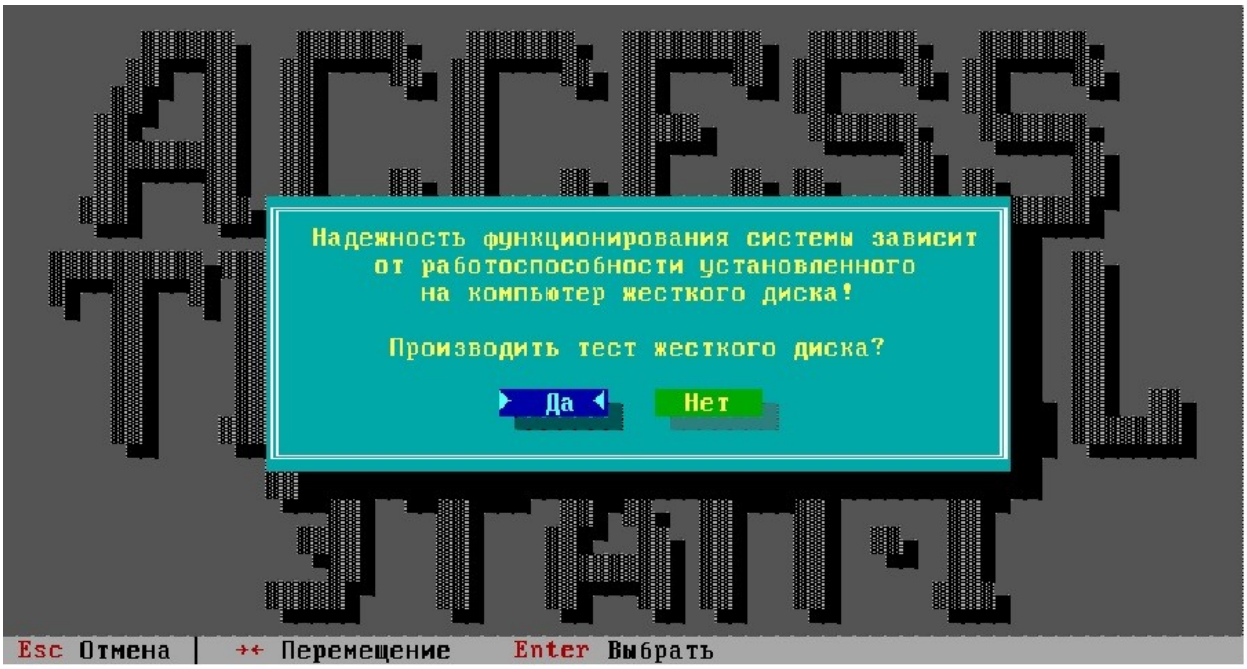


Рисунок 216 - Тест ПЗУ ФПСУ-TLS

Необходимо дождаться завершения теста.

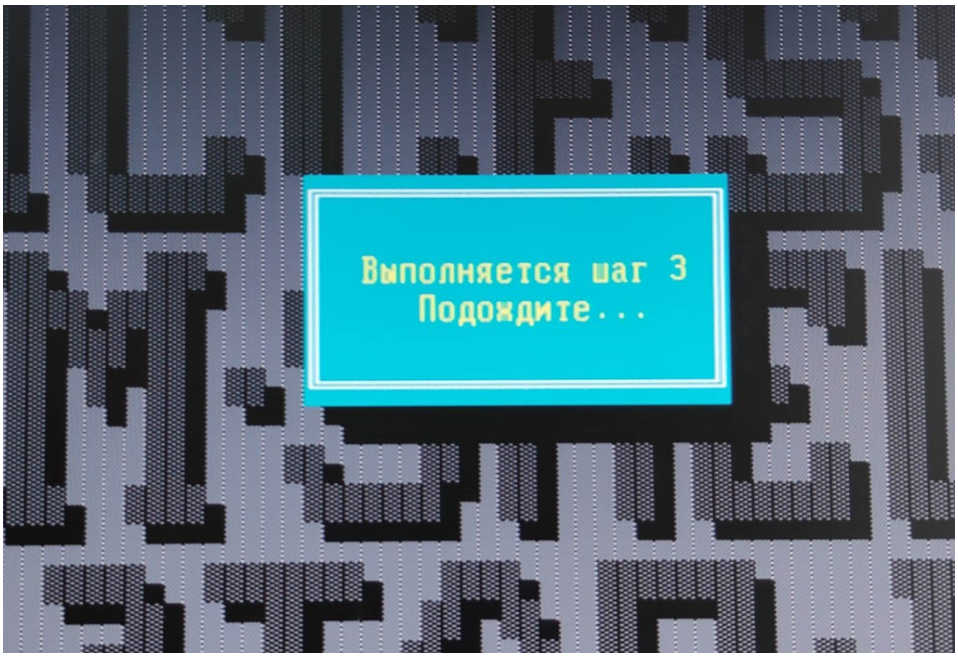


Рисунок 217 - Тест ПЗУ ФПСУ-TLS

6. После успешного теста внутреннего накопителя информации ФПСУ-TLS выполняется следующий шаг установки.

Рисунок 218 - Очистка ПЗУ ФПСУ-TLS

Для продолжения инсталляции выберите команду «Да» и нажмите <Enter>. В случае, если ПЗУ не было форматировано ранее, очистка будет произведена на данном шаге.

Команда «Нет» отменяет процесс установки.

7. После успешного завершения форматирования ПЗУ ФПСУ-TLS будет выдано служебное оповещение о завершении первого этапа установки программного обеспечения.

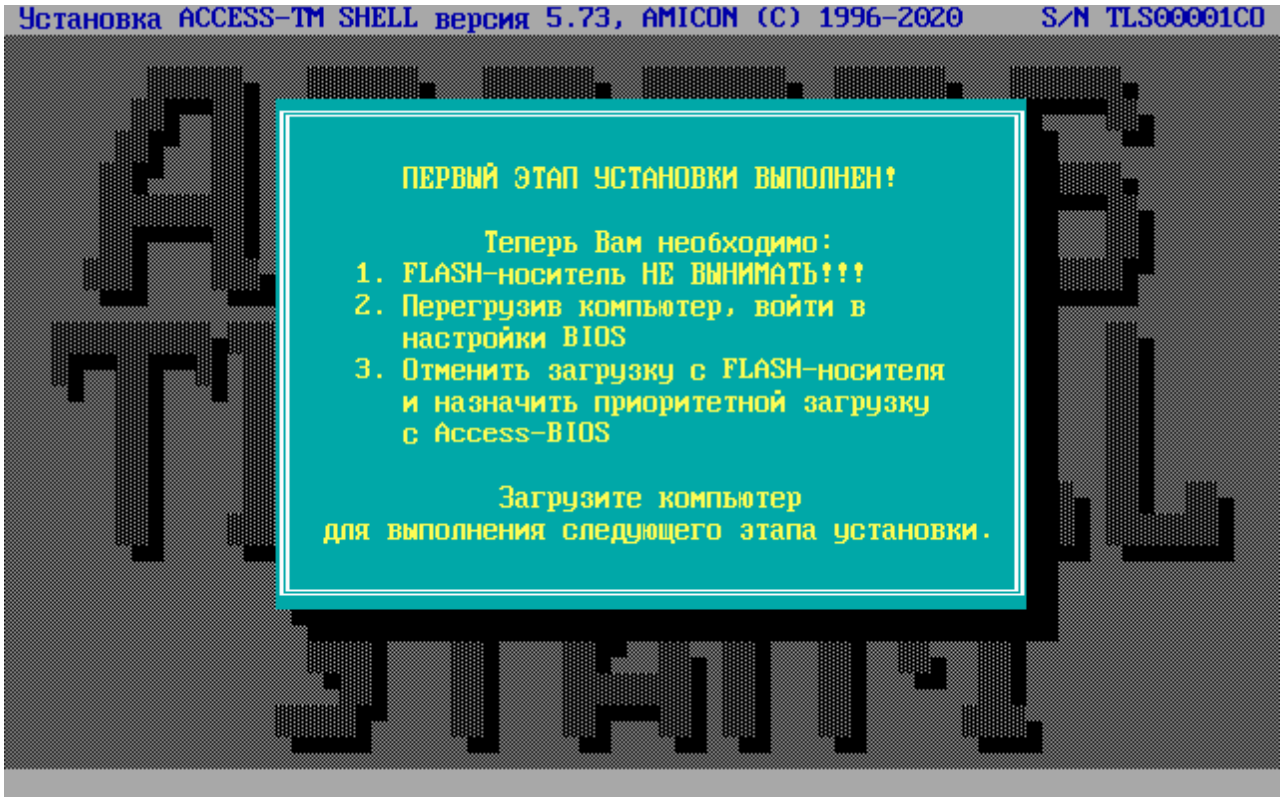


Рисунок 219 - Завершение первого этапа установки

8. Далее необходимо выполнить перезагрузку ФПСУ-TLS, и загрузить комплекс ФПСУ-TLS в штатном порядке загрузки, вернув в BIOS первоначальную первичную загрузку в BIOS Boot Options с устройства (было отменено в пункте 2 процедуры установки).

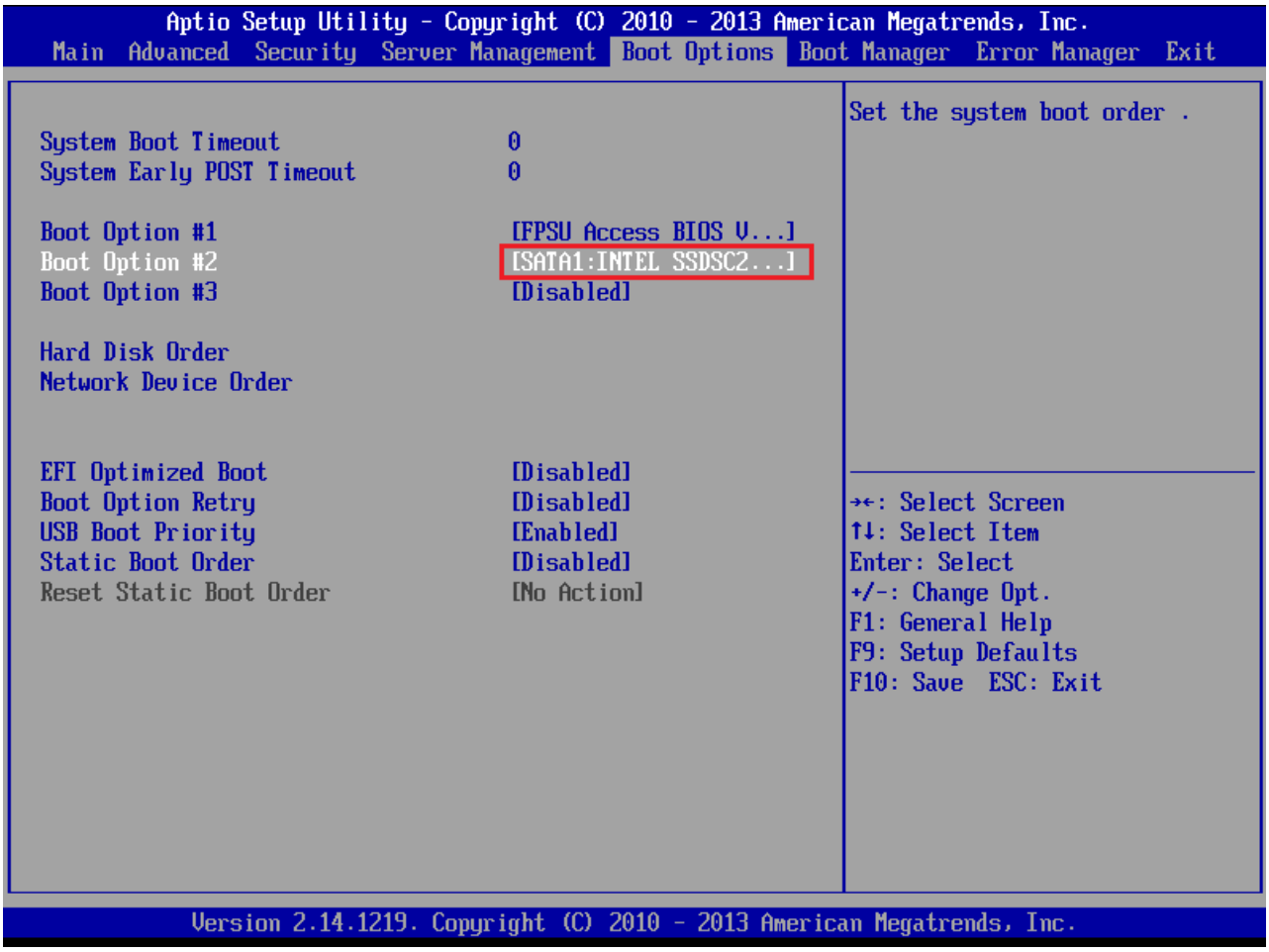


Рисунок 220 - Выбор загрузки с Access BIOS/PnP

9. После перезагрузки и запуска подсистемы ACCESS-TM SHELL начнется второй этап установки программного обеспечения ФПСУ-TLS. Для продолжения потребуется подтвердить права допущенного лица класса Главный администратор, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS:

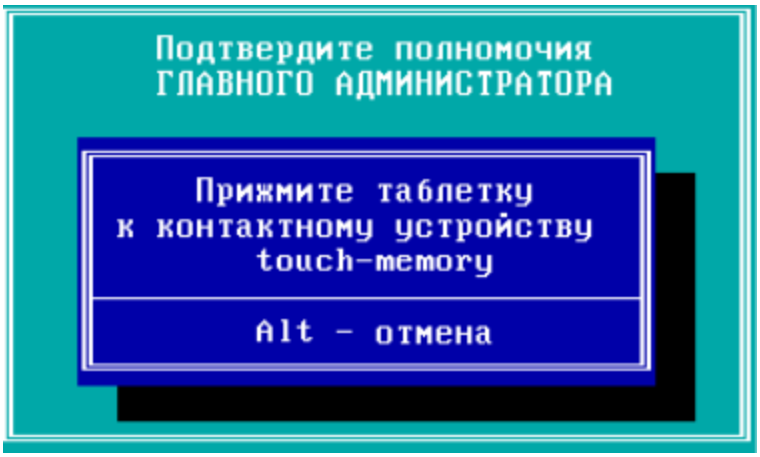


Рисунок 221 - Проверка полномочий Главного администратора

10. После проверки полномочий Главного администратора программа установки предложит указать режим функционирования данного ФПСУ-TLS. Выберите режим «Основной/Единственный» и нажмите клавишу <Enter>.

Примечание. Работа ФПСУ-TLS в режиме «Горячий резерв» не предусмотрена.

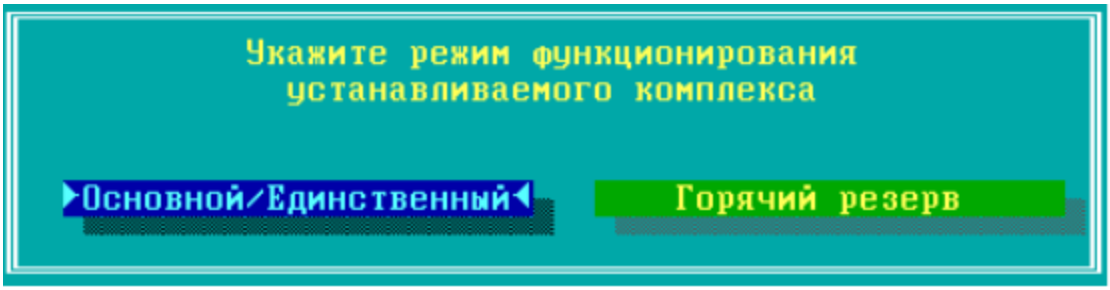


Рисунок 222 - Выбор режима функционирования ФПСУ-TLS

11. Необходимо подтвердить права допущенного лица класса Главный администратор, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS:

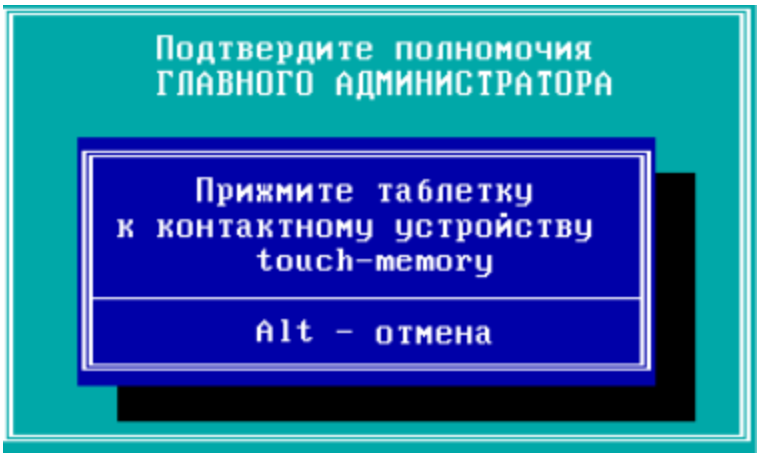


Рисунок 223 - Проверка полномочий Главного администратора

12. После выбора режима функционирования ФПСУ-TLS начнется копирование файлов ФПСУ-TLS на ПЗУ комплекса.

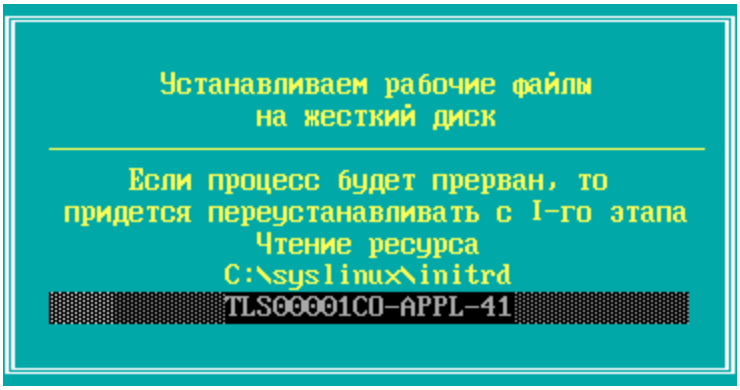


Рисунок 224 - Копирование файлов ФПСУ-TLS на ПЗУ

13. После завершения копирования системных файлов на ПЗУ комплекса, установка программного обеспечения комплекса завершается. ФПСУ-TLS будет перезагружен, и после перезагрузки начнет работать в технологическом режиме (см. пункт. Технологический режим ФПСУ-TLS).

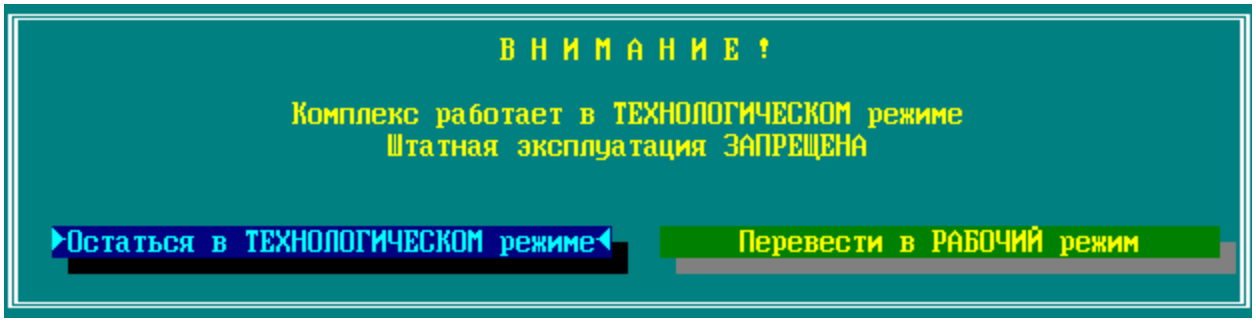


Рисунок 225 - Выбор режима функционирования ФПСУ-TLS

Для перехода в рабочий режим выберите команду «Перевести в РАБОЧИЙ режим».

14. Для перевода ФПСУ-TLS в рабочий режим требуется инициализировать программный датчик случайных чисел. Откроется окно выбора источника ключа ПДСЧ. Инициализация ПДСЧ может быть проведена средствами БДСЧ, путем передвижения мыши в пределах экрана, или с помощью ЦВК, путем загрузки файла с ключом ПДСЧ, выданного ЦВК.

ВНИМАНИЕ! Программным комплексам ФПСУ-TLS, функционирующим под управлением виртуальных машин запрещается проводить инициализацию ПДСЧ средствами БДСЧ.

Рисунок 226 - Инициализация программного датчика случайных чисел

При использовании БиоДСЧ от администратора требуется передвигать мышь в пределах экрана. Дальнейшая работа будет возможна, как только датчик обработает достаточно движений для генерации случайного числа.

Рисунок 227 - Биологический датчик случайных чисел

При использовании опции «ЦВК» от администратора требуется загрузить на ФПСУ-TLS файл ключа ПДСЧ, полученный с ЦВК (ЦВК - программно-аппаратный комплекс «Центр выработки ключей» производства ООО «АМИКОН»):

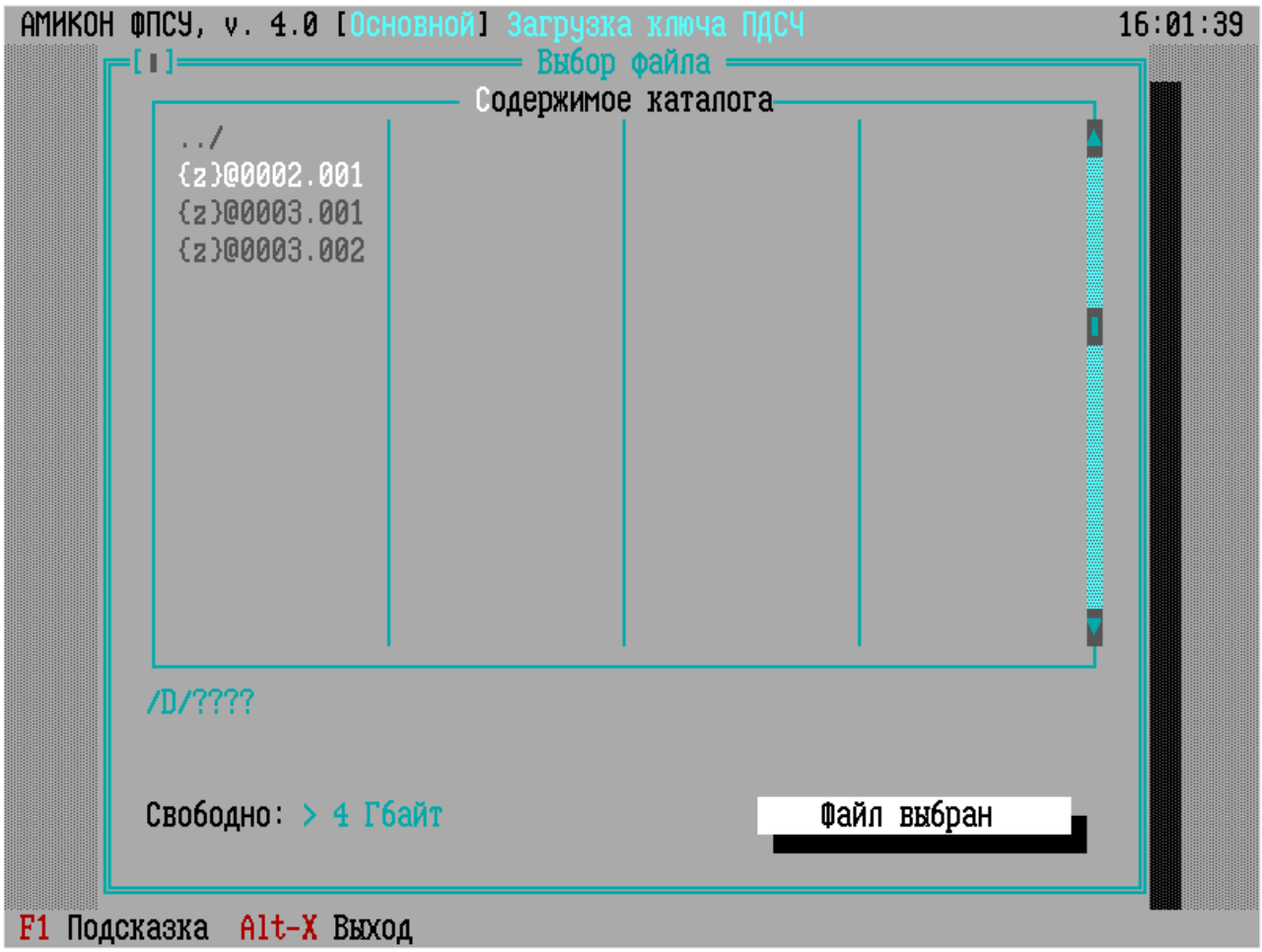


Рисунок 228 - Загрузка ключа ПДСЧ из файла

Переместите курсор на выбранный файл. Переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>. Подтвердите выбор файла, нажав на клавишу <*Enter*>. В открывшемся окне отобразится информация о ЦВК, выдавшем файл с ключом ПДСЧ и предложением загрузить этот файл.

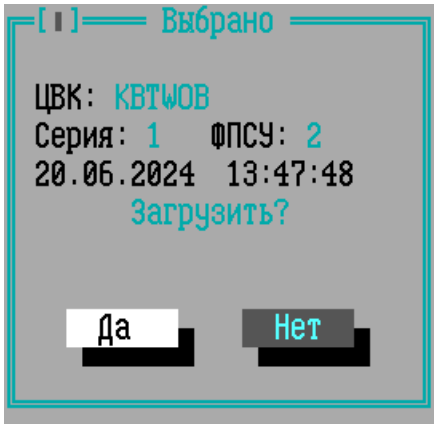


Рисунок 229 - Информация о загружаемом файле

После загрузки файла, ФПСУ-TLS выдаст системное оповещение о завершении процедуры:

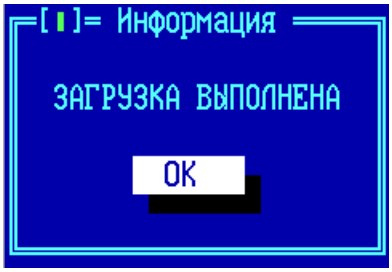


Рисунок 230 - Файл загружен

15. Для завершения перевода комплекса в штатный рабочий режим необходимо перерегистрировать ТМ-идентификатор Главного администратора. Для подтверждения действия нажмите «Понятно».

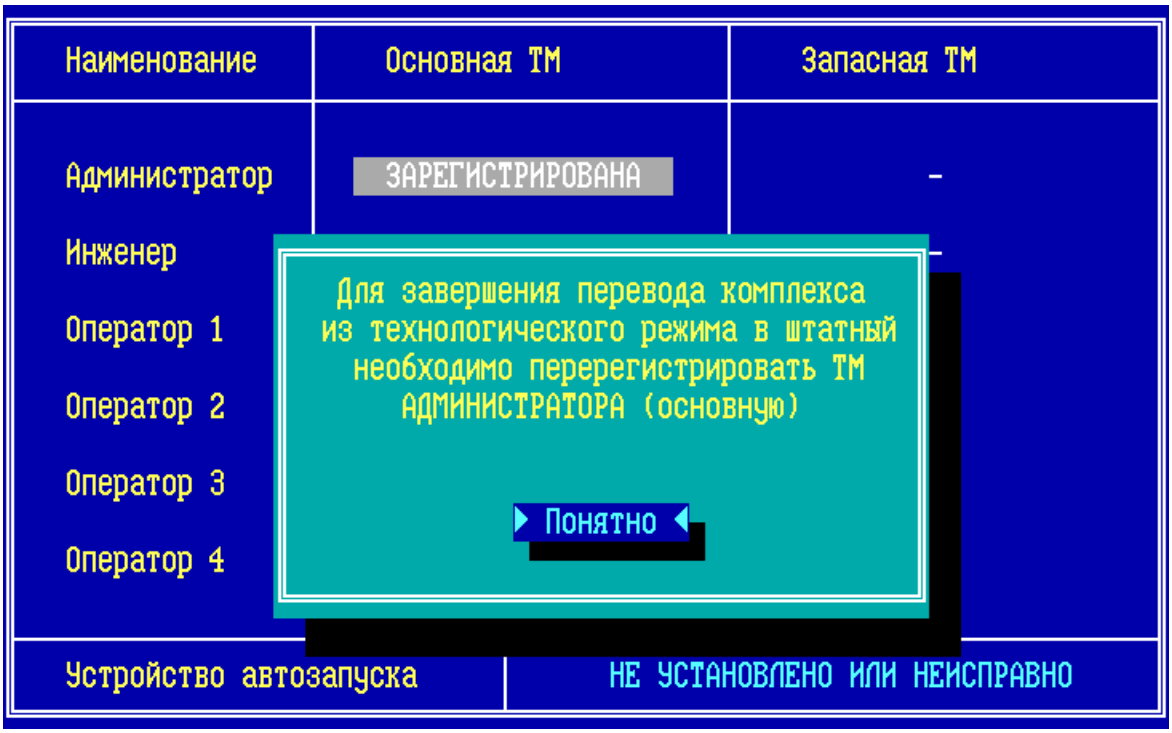


Рисунок 231 - Служебное оповещение о переходе в рабочий режим

16. Приложите ТМ-идентификатор, на который будет записана новая ключевая информация - перерегистрирован ТМ-идентификатор Главного администратора, к ТМ-считывателю ФПСУ-TLS.

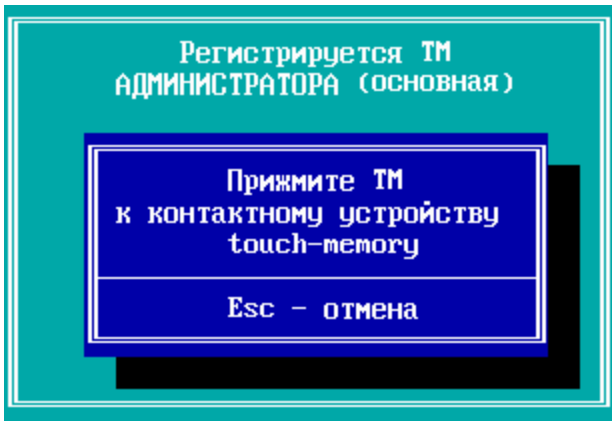


Рисунок 232 - Перерегистрация Главного администратора

После перерегистрации ТМ-идентификатора Главного администратора система предложит установить дополнительную проверку авторизации для этого ТМ-идентификатора: установить пароль. После установки пароля, для авторизации любого действия администратора потребуется не только подключать ТМ-идентификатор к ЦВК, но и вводить символьный пароль. На экране отобразится запрос на установление пароля Главного администратора.

ВНИМАНИЕ! Установка пароля для каждого ТМ-идентификатора обязательна для ЦВК классов КС2, и опциональна для ЦВК класса КС1.

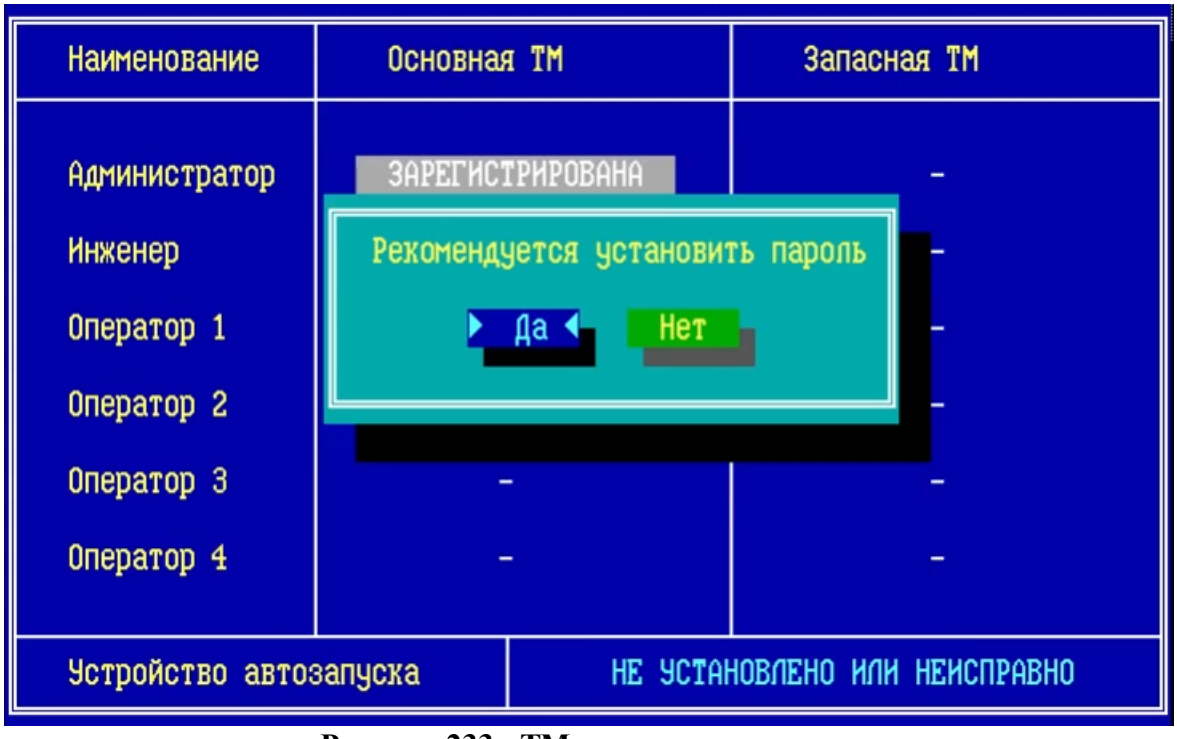


Рисунок 233 - ТМ перерегистрирован

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не будут отображаться на экране, подсистема попросит ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля будет произведена только после повторного введения идентичной комбинации символов.

В операции проверки пароля участвуют ASCII-коды символов, поэтому администратор должен быть внимателен к набору символов в определенных регистре и алфавите.

После установки пароля при попытке изменить конфигурацию ФПСУ-TLS (выборе соответствующей команды) подсистема будет блокировать любые действия администратора до ввода установленного пароля.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <*Enter*>. В открывшемся окне повторно ввести пароль и нажать клавишу <*Enter*>.

Рисунок 234 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы), и нажать <*Enter*>.

В случае если ТМ-идентификатор Главного администратора в процессе ввода пароля был отключен, необходимо повторно предъявить его для добавления пароля.

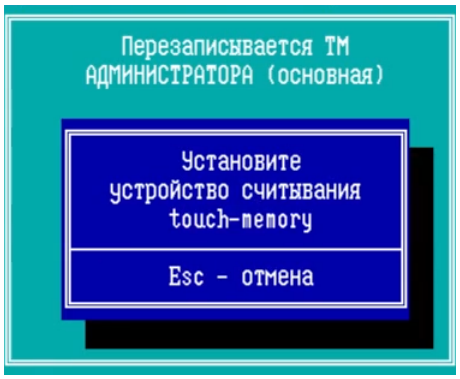


Рисунок 235 - Предъявление ТМ Главного администратора для установления пароля

ТМ-идентификатор Главного администратора перерегистрирован с установлением пароля.

17. При успешной перерегистрации ТМ-идентификатора Главного администратора комплекс переведен в штатный режим и будет принудительно перезагружен.

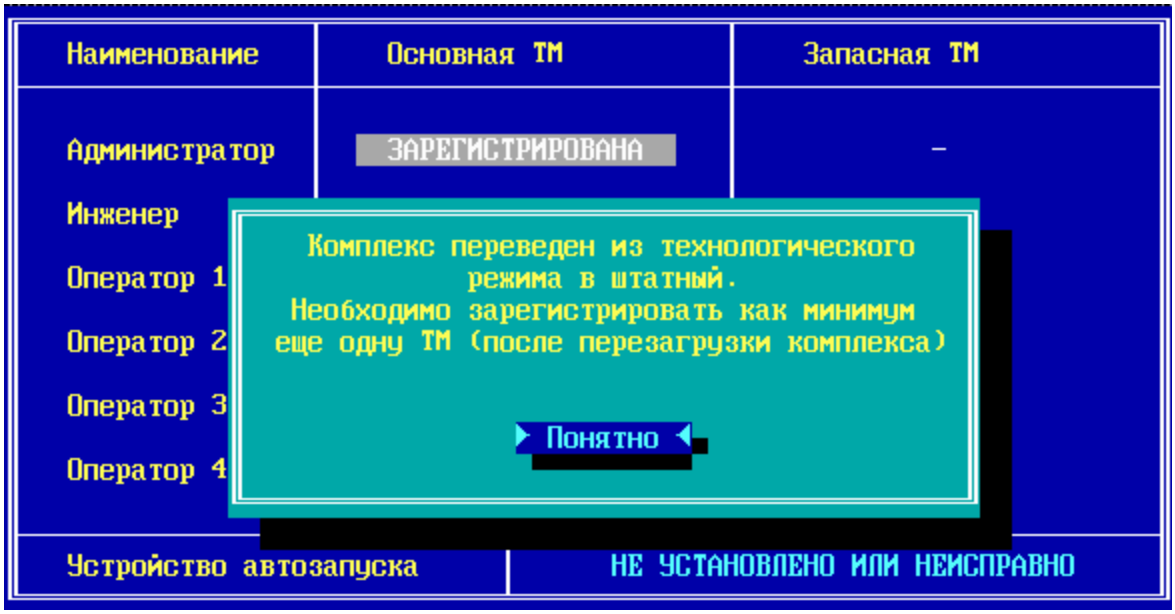


Рисунок 236 - Перезагрузка комплекса

18. Во время перезагрузки необходимо подтвердить права допущенного лица класса Главный администратор, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS:

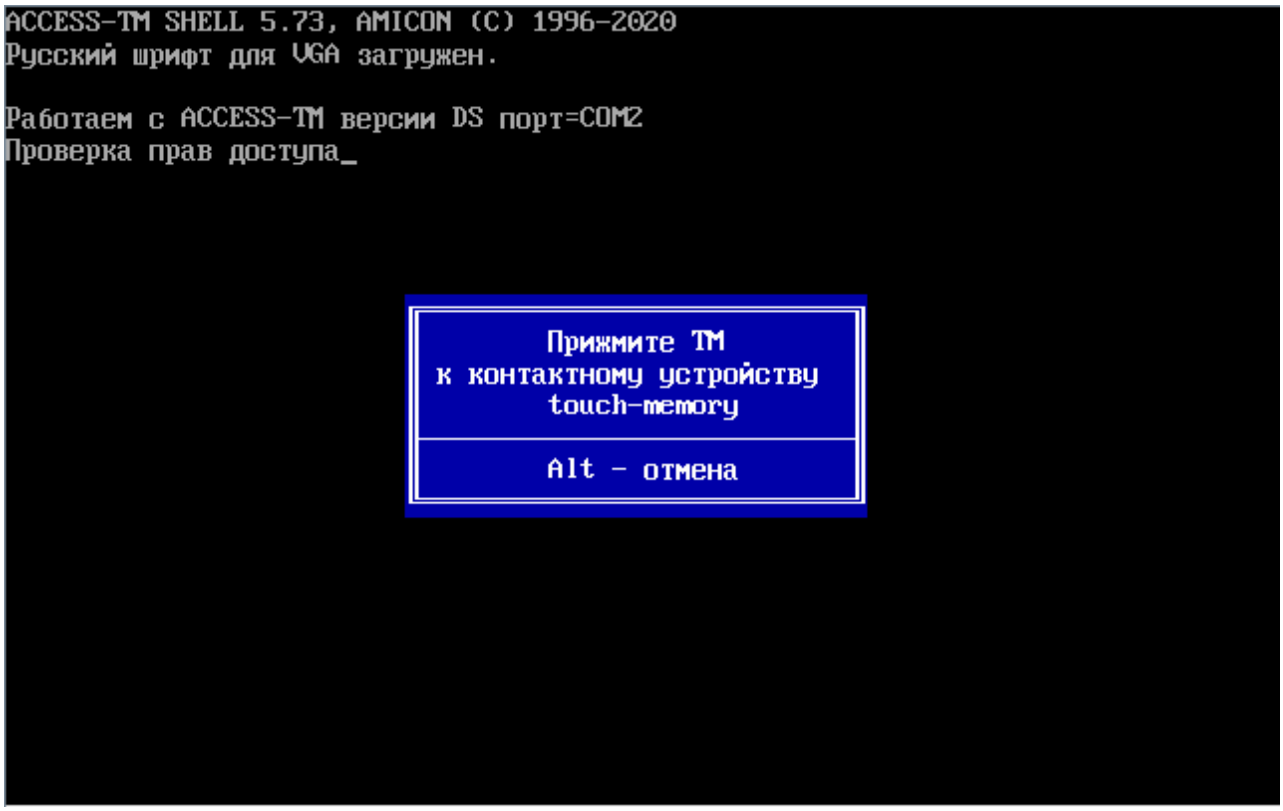


Рисунок 237 - Перезагрузка ФПСУ-TLS

По завершению регистрации ТМ-идентификатор Главного администратора отображается в таблице ТМ-идентификаторов в строке «Администратор» в столбце «Основной ТМ».

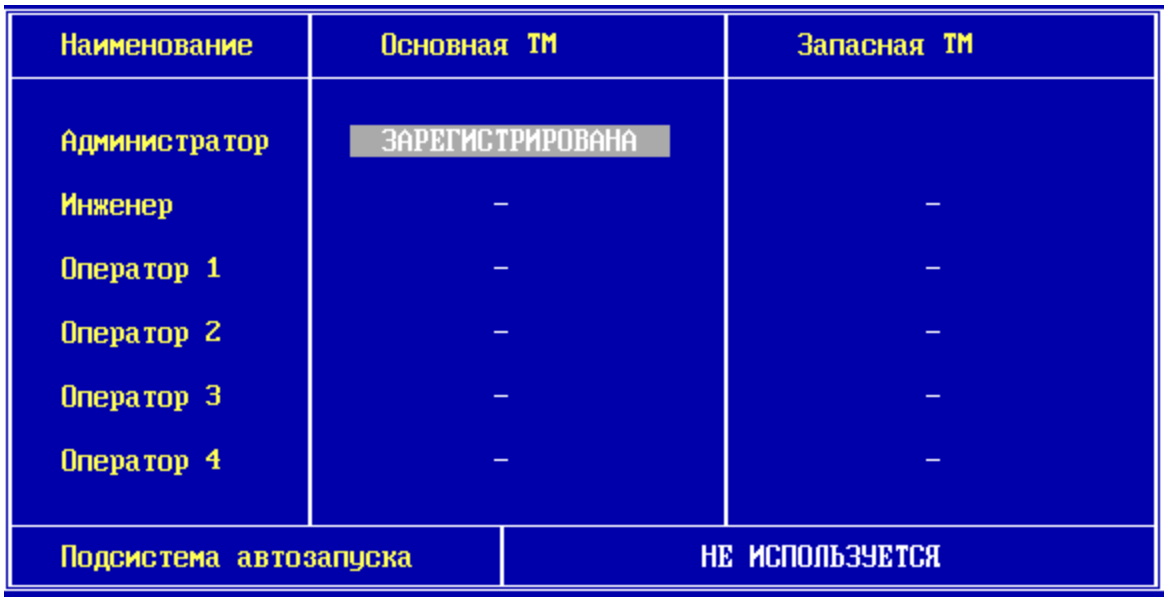


Рисунок 238 - ТМ-идентификатор Главного администратора зарегистрирован

ВНИМАНИЕ! На ФПСУ-TLS должны быть зарегистрированы минимум два ТМ-идентификатора, один из которых ТМ Главного администратора.

Обязательным условием для продолжения работы является регистрация второго ТМ-идентификатора, запасного ТМ администратора или ТМ-идентификатора любого другого класса, иначе при закрытии регистратора ТМ-идентификаторов он будет открываться снова, блокируя дальнейшую работу.

При регистрации второго ТМ-идентификатора требуется ТМ администратора для подтверждения права регистрации и другой ТМ для регистрации выбранного класса пользователя ФПСУ-TLS.

Уточнение: при регистрации запасного ТМ-идентификатора требуется ТМ Главного администратора для подтверждения права регистрации и запасной ТМ для регистрации.

19. Далее зарегистрируйте второй ТМ-идентификатор, например, запасной ТМ-идентификатор администратора. В строке «Администратор» перейдите в столбец «Запасной ТМ» и нажмите <Ins>.

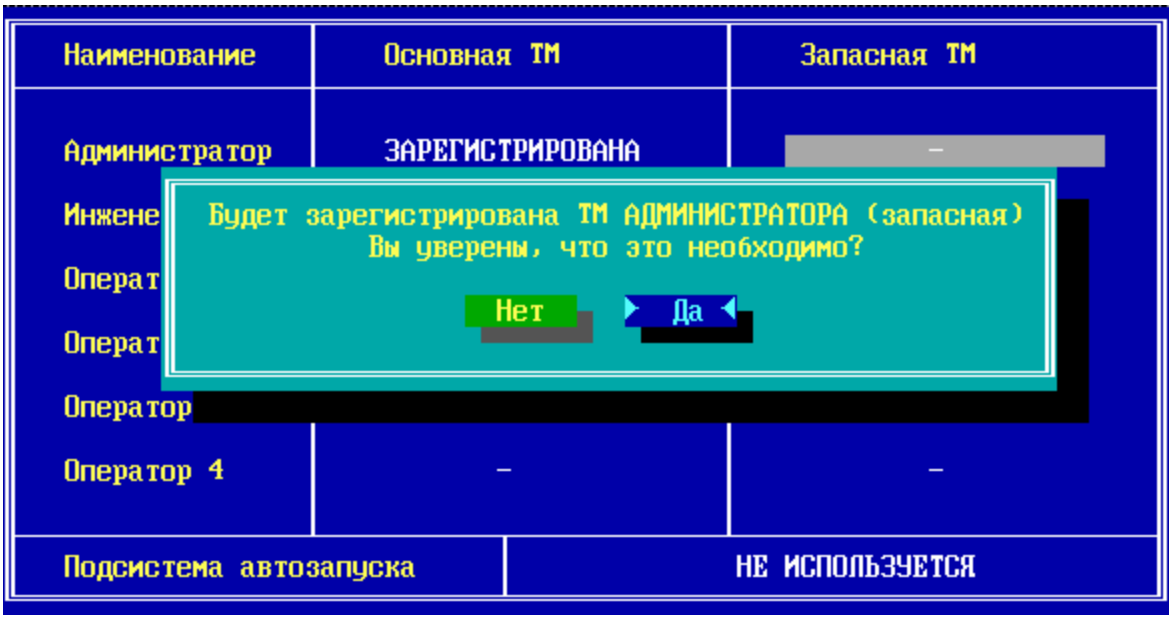


Рисунок 239 - Регистрация запасного ТМ-идентификатора администратора ФПСУ-TLS

Для продолжения выберите команду «Да» и нажмите <Enter>.

20. Подтвердите права допущенного лица класса Главный администратор, приложив основной ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS для продолжения операции:

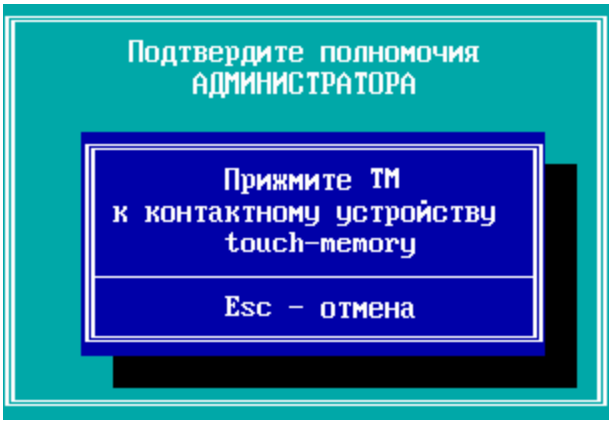


Рисунок 240 - Проверка полномочий Главного администратора

Также запрашивается пароль подключенного ТМ-идентификатора Главного администратора для авторизации в системе, в случае если пароль установлен.

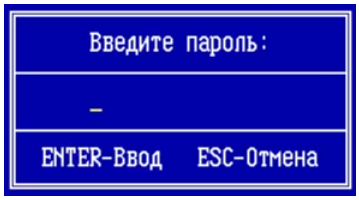


Рисунок 241 - Ввод пароля ТМ Главного администратора

Далее необходимо убрать ТМ-идентификатор Главного администратора, в случае если ТМ остается подключен, на экран будет выдано сообщение:

Рисунок 242 - Сообщение об отключении ТМ

21. Приложите ТМ-идентификатор, на который будет записана ключевая информация запасного ТМ-идентификатора администратора, к ТМ-считывателю ФПСУ-TLS.

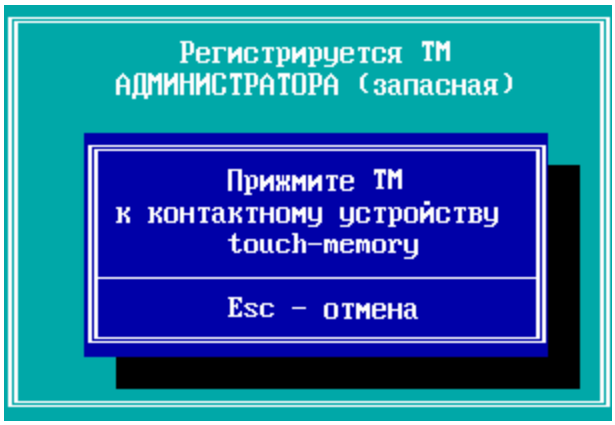


Рисунок 243 - Регистрация запасного ТМ-идентификатора администратора

Рекомендуется установить пароль зарегистрированного ТМ-идентификатора, на экране отобразится запрос на установление пароля ТМ.

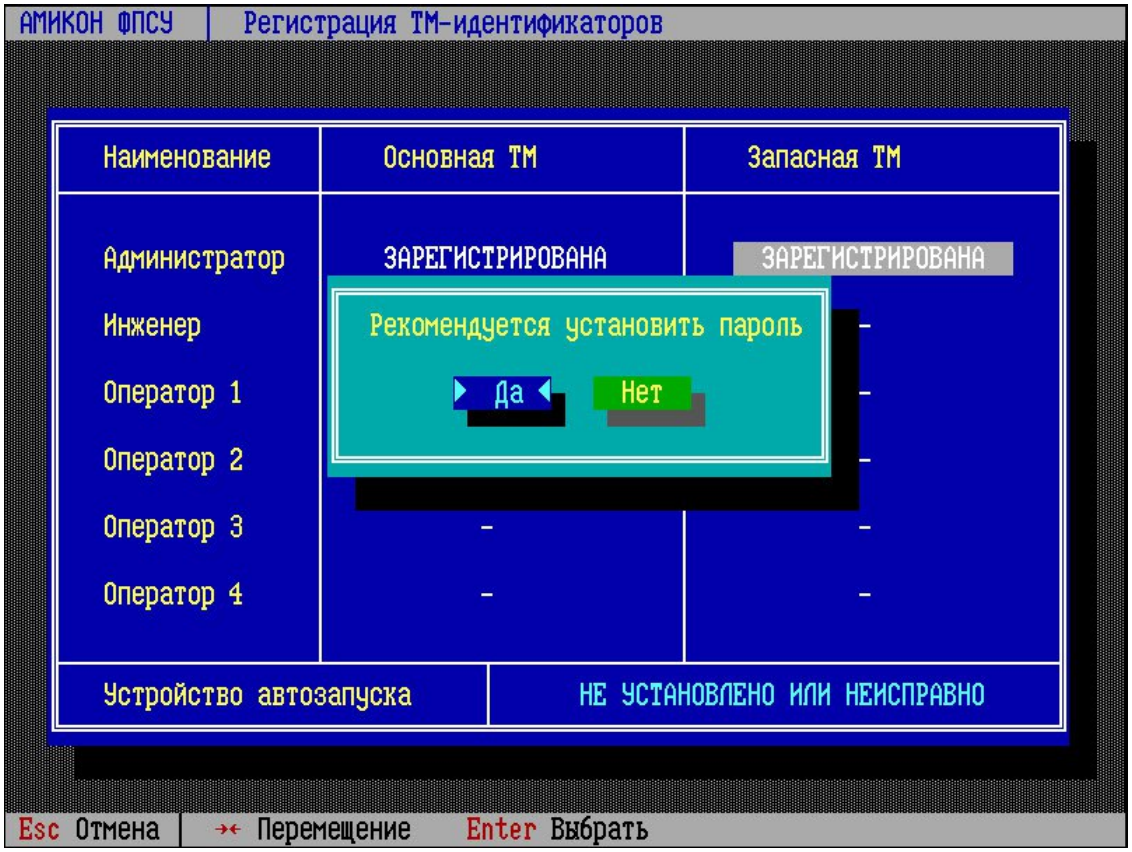


Рисунок 244 - Запасной ТМ зарегистрирован

При подтверждении запроса откроется окно ввода пароля. Все требования к паролю изложены выше (см. установка пароля ТМ Главного администратора).

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <*Enter*>. В

открывшемся окне повторно ввести пароль и нажать клавишу <*Enter*>.

Рисунок 245 - Ввод пароля ТМ

В случае если запасной ТМ-идентификатор в процессе ввода пароля был отключен, необходимо повторно предъявить его для добавления пароля.

Рисунок 246 - Предъявление запасного ТМ

Запасной ТМ-идентификатор администратора зарегистрирован с установлением пароля.

При успешном завершении регистрации запасной ТМ-идентификатор администратора отобразится в таблице ТМ-идентификаторов.

Рисунок 247 - Запасной ТМ-идентификатор администратора зарегистрирован

22. В окне регистратора ТМ-идентификаторов рекомендуется настроить подсистему автозапуска ФПСУ-TLS. Для включения подсистемы перейдите в поле

«Подсистема автозапуска» и нажмите клавишу <Ins>.

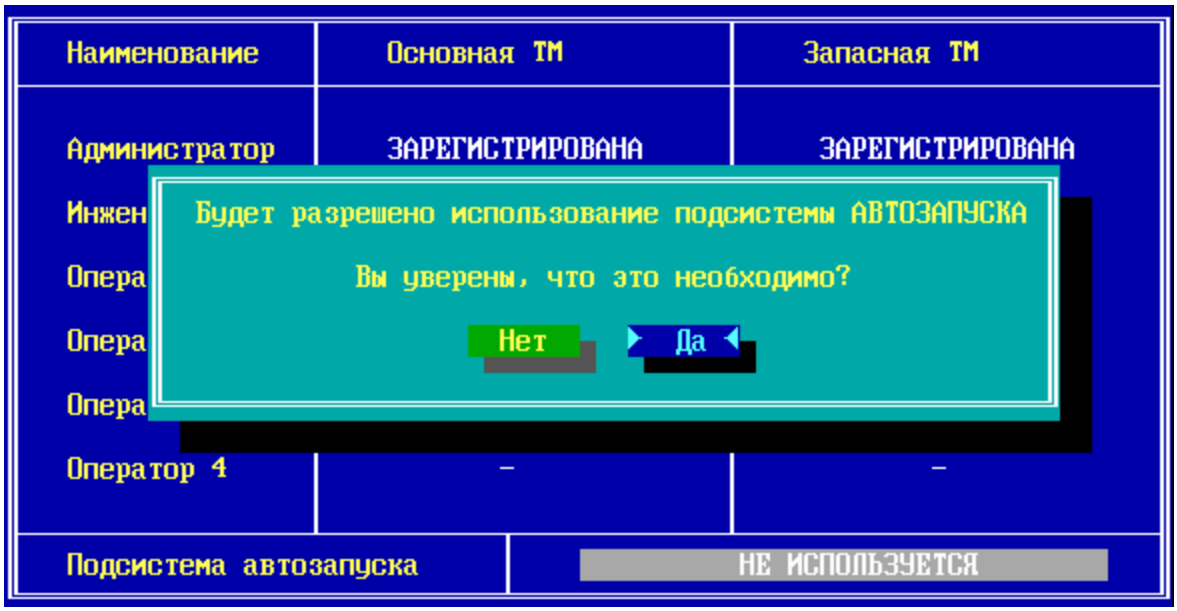


Рисунок 248 - Настройка подсистемы автозапуска

23. Для подтверждения включения подсистемы автозапуска выберите команду «Да» и нажмите <Enter>.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 249 - Подтверждение полномочий и ввод пароля ТМ

Режим работы подсистемы автозапуска изменится на «Используется». Подсистема автозапуска включена.

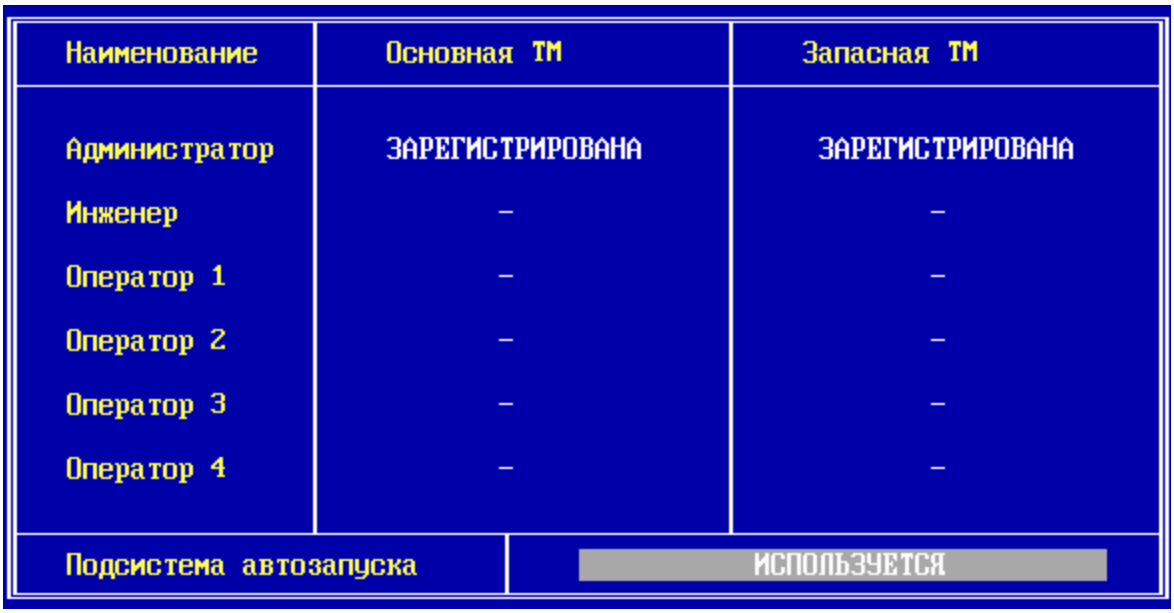


Рисунок 250 - Подсистема автозапуска включена

Выход в главное меню осуществляется по нажатию сочетания клавиш <Alt+X>. Откроется главное меню комплекса:

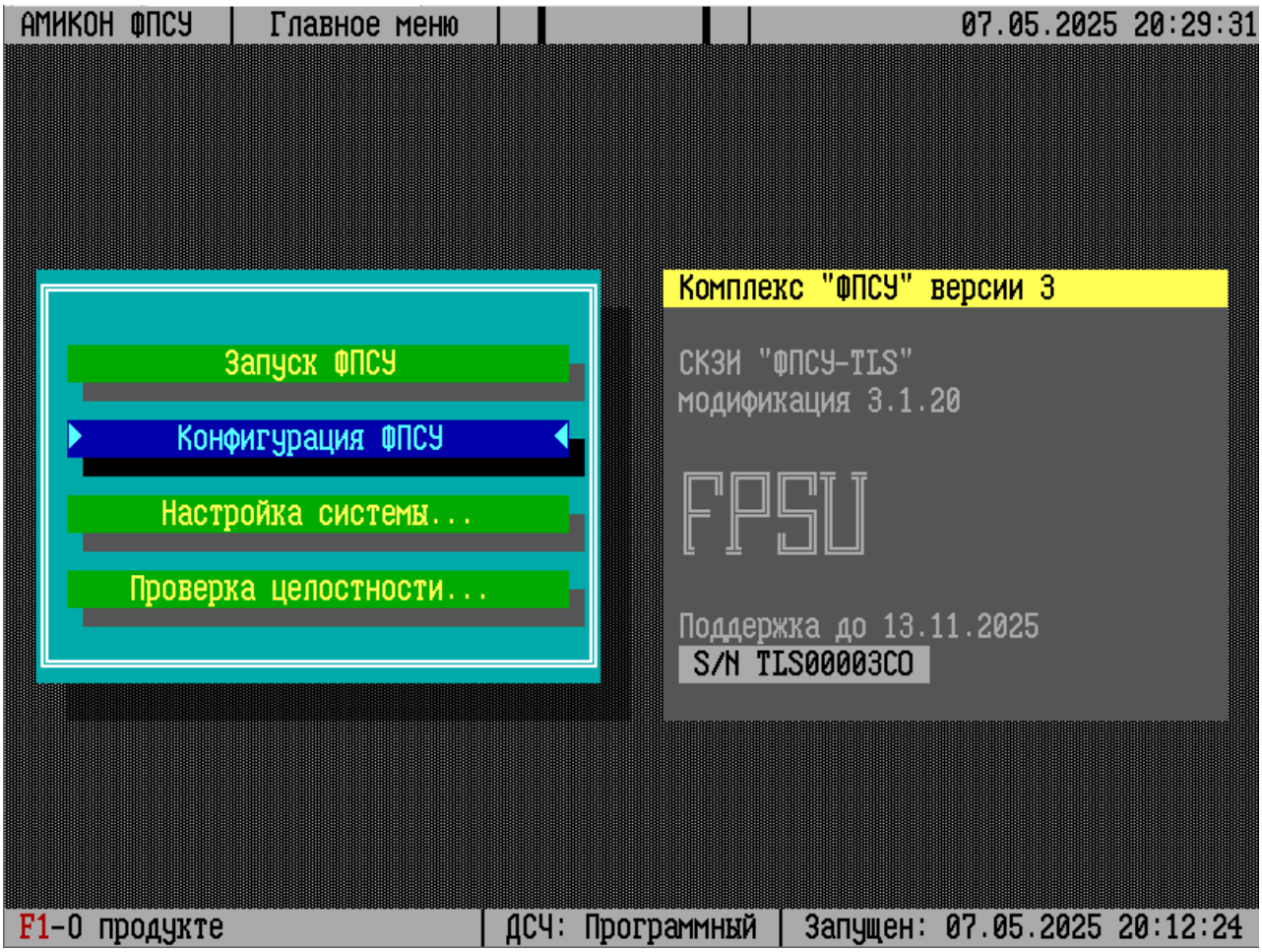


Рисунок 251 - Главное меню ФПСУ-TLS

Переустановка ПО ФПСУ-TLS завершена, перевод из технологического режима завершен, ФПСУ-TLS готов к работе в штатном режиме эксплуатации.

11. 2. Установка в QEMU/KVM

В разделе описываются шаги по установке программного обеспечения ФПСУ-TLS с готового образа диска на USB-носителе в виртуальную среду под управлением QEMU/KVM.

Установка ПО ФПСУ-TLS с готового образа диска на USB-носителе в виртуальную среду заключается в подключении USB-носителя к виртуальной машине QEMU/KVM, последующего запуска виртуальной машины QEMU/KVM, и дальнейшего следования предложениям мастера установки.

Запустите виртуальную машину, нажав на черную стрелку (на рисунке QEMU/KVM 6.2.0 на Ubuntu 22.04.4 LTS).

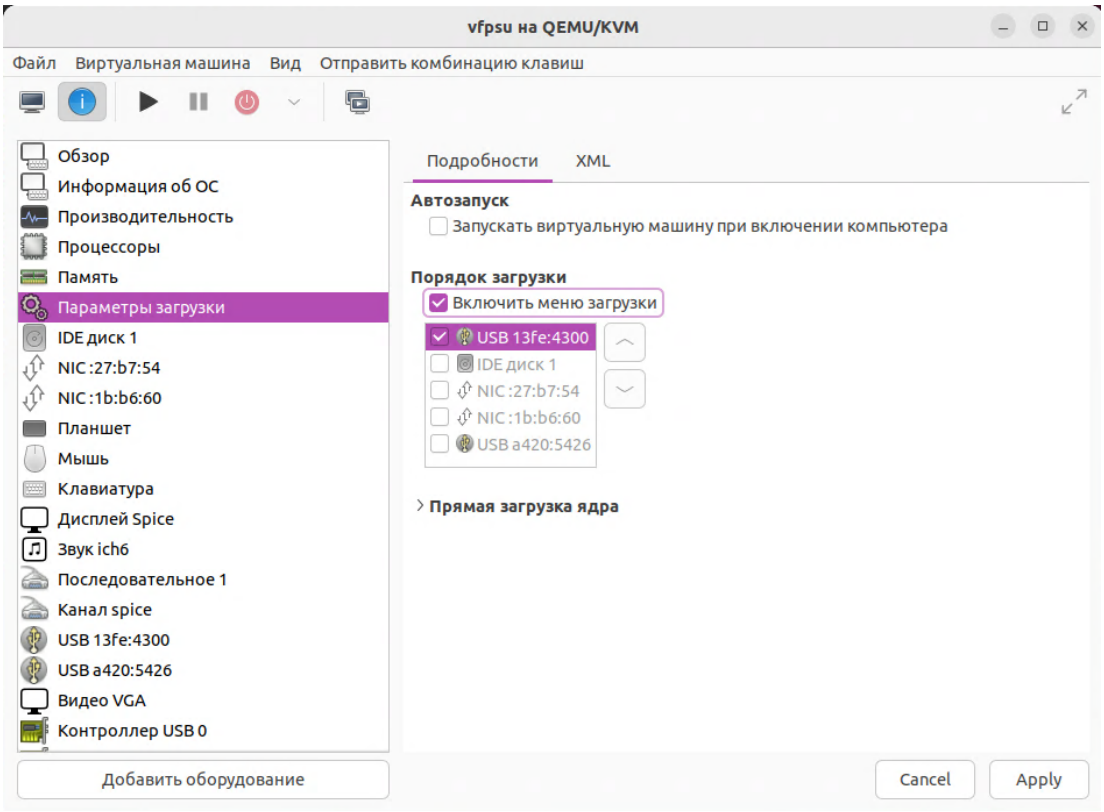


Рисунок 252 - Запуск виртуальной машины

После проверки полномочий Главного администратора программа установки предложит указать режим функционирования данного ФПСУ-TLS. Выберите режим — «Основной/Единственный» и нажмите клавишу <Enter>.

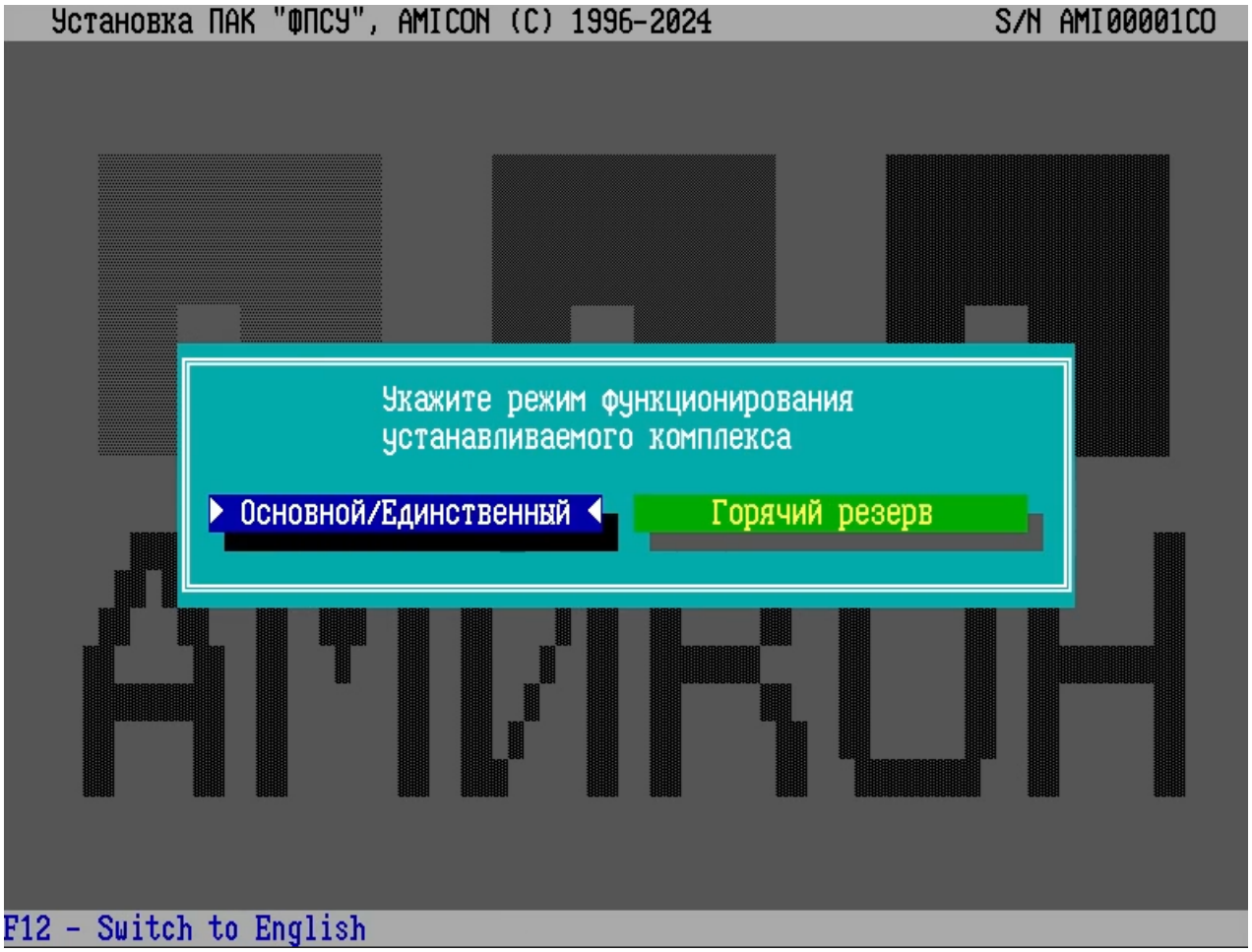


Рисунок 253 - Выбор режима функционирования ФПСУ-TLS

После выбора режима функционирования ФПСУ-TLS будет запрашиваться ТМ Главного администратора для регистрации (при записи ТМ на него записывается ключ запуска).

Рисунок 254 - Регистрация ТМ Главного администратора

Затем начнется формирование разделов на диске:

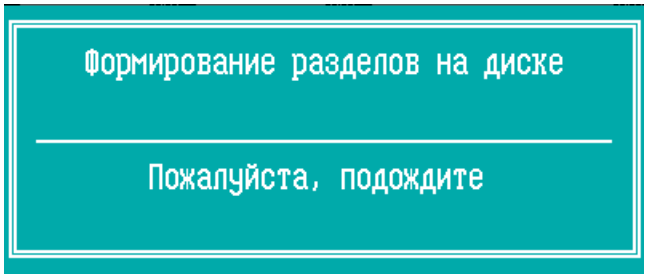


Рисунок 255 - Формирование разделов

Установка программного обеспечения комплекса завершена. ФПСУ-TLS будет перезагружен, и после перезагрузки начнет работать в технологическом режиме.

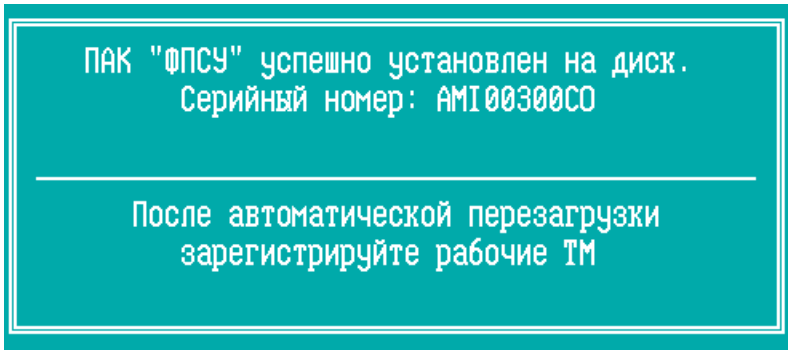


Рисунок 256 - ФПСУ-TLS установлен на диск

Отключите USB-носитель с инсталляционным комплектом ФПСУ-TLS.

После перезагрузки ФПСУ-TLS на экран выдается служебное оповещение о том, что

ФПСУ-TLS работает в технологическом режиме:

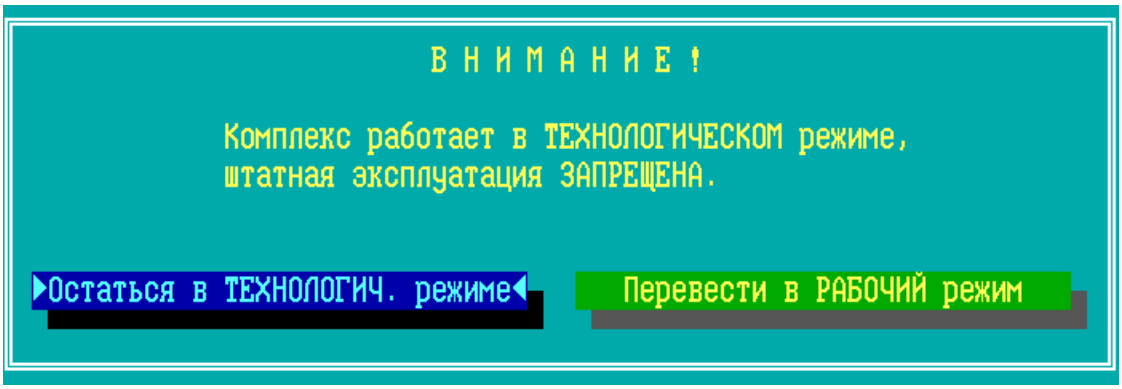


Рисунок 257 - Оповещение о работе в технологическом режиме

Установка ФПСУ-TLS в виртуальную машину QEMU/KVM с USB-носителя с инсталляционным комплектом ФПСУ-TLS закончена.

Для дальнейшей работы:

- переведите ФПСУ-TLS из технологического режима в рабочий, см. пункт «Технологический режим ФПСУ-TLS»;
- зарегистрируйте ТМ-идентификаторы пользователей ФПСУ-TLS (см. пункт «Регистрация ТМ-идентификаторов»).

12. Удаление СКЗИ

Удаление СКЗИ «ФПСУ-TLS» заключается в удалении установленных программных модулей СКЗИ с аппаратной платформы или виртуальной машины, и установочных программных модулей СКЗИ с дистрибутивного USB-носителя.

12. 1. Удаление программного обеспечения ФПСУ-TLS

Локальному администратору ФПСУ-TLS классов *Администратор* или *Главный администратор* доступна возможность форматирования внутреннего накопителя ФПСУ-TLS с удалением операционной системы ФПСУ-TLS и хранящихся файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI.

Для запуска процедуры форматирования внутреннего накопителя:

Выполните команду «Настройка системы» главного меню:

Рисунок 258 - Главное меню ФПСУ-TLS

Выполните команду «Настройки СКЗИ» меню настройки системы:

Рисунок 259 - Меню настройки системы ФПСУ-TLS

Выполните команду «Удаление СКЗИ» меню настройки СКЗИ.

ВНИМАНИЕ! Если при выполнении команды «Удаление СКЗИ» к ФПСУ-TLS подключен USB ТМ-идентификатор ТМ-Key с правами *Администратор* или *Главный администратор,* то последующего окна с подтверждением полномочий не будет выведено на экран. Процедура удаления СКЗИ начнется сразу после выполнения команды «Удаление СКЗИ»!

Рисунок 260 - Запуск процедуры удаления СКЗИ

Если USB ТМ-идентификатор ТМ-Key не был подключен к ФПСУ-TLS, появится окно с предложением подтвердить полномочия администратора или Главного

администратора.

ВНИМАНИЕ! Сразу после приложения к ТМ-считывателю ФПСУ-TLS ТМ-идентификатора, подтверждающего права классов *Администратор* или *Главный администратор*, будет запущен необратимый процесс форматирования внутреннего накопителя!

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи»). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ-TLS или прижатия ТМ-идентификатора к ТМ-считывателю ФПСУ-TLS, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Рисунок 261 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения прав администратора, ФПСУ-TLS начнет форматирование внутреннего накопителя, после чего перезагрузит операционную систему. Удаление операционной системы ФПСУ-TLS и хранящихся на внутреннем накопителе файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI, завершено.

12. 2. Удаление СКЗИ с USB-носителя

В разделе приводятся сведения о процедурах удаления СКЗИ с дистрибутивных USB-носителей в операционных системах семейств Windows и Linux.

12. 2. 1. Удаление СКЗИ с USB-носителя в ОС Windows

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется форматированием носителя штатными средствами операционной системы.

Далее приведен пример удаления разделов и форматирования дистрибутивного USB-носителя средствами операционной системы Windows 10.

При подключении к компьютеру с операционной системой Windows 10, дистрибутивный USB-носитель отображается как три отдельных диска. Буквы дискам присваиваются операционной системой динамически при подключении USB-носителя.

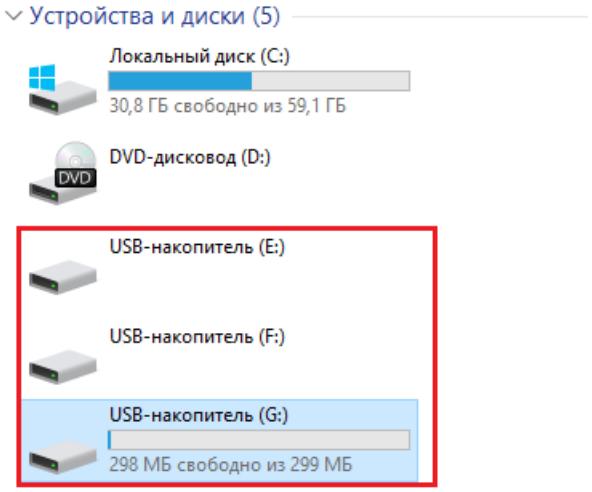


Рисунок 262 - Отображение дистрибутивного USB-носителя

После подключения дистрибутивного USB-носителя операционная система выводи запрос на форматирование каждого из этих дисков:

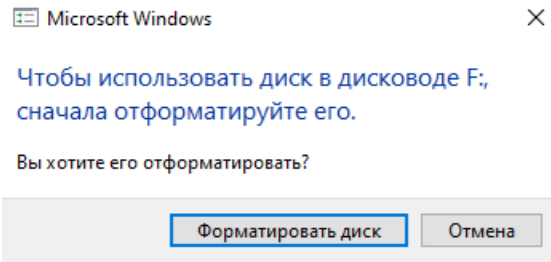


Рисунок 263 - Запрос на форматирование USB-носителя

Закройте сообщение для каждого диска.

Необходимо убедиться, что съемный диск является дистрибутивным USB-носителем, информация с которого подлежит удалению. На не пустом съемном диске найдите и откройте текстовый файл install.txt. Проверьте инсталляционную информацию, в частности

серийный номер находящегося на дистрибутивном USB-носителе программного обеспечения.

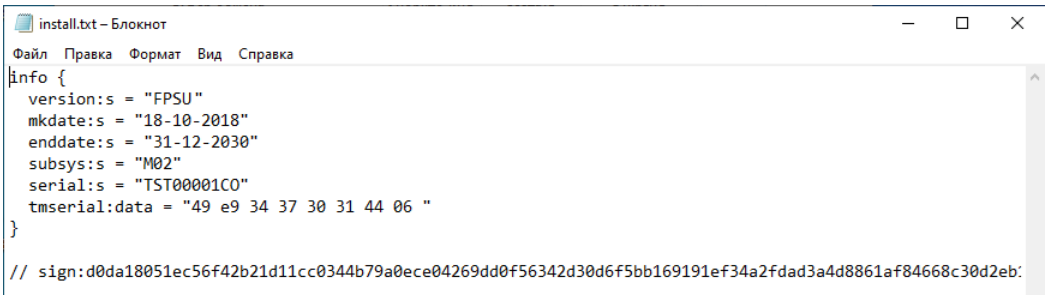


Рисунок 264 - Информация о программного обеспечении на USB-носителе

Откройте окно Windows «Управление компьютером → Управление дисками».

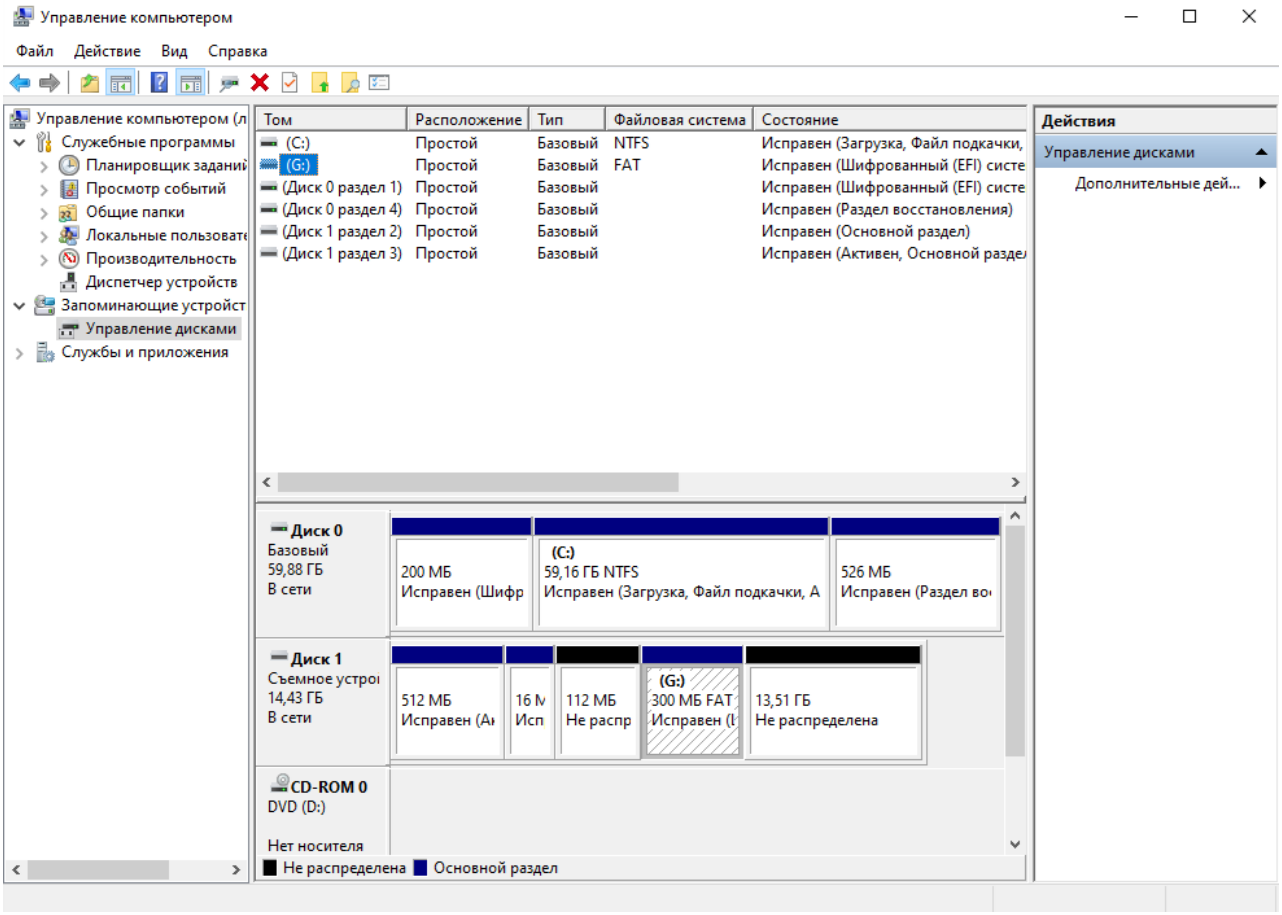


Рисунок 265 - Подключенный USB-носитель

У подключенного съемного USB-носителя необходимо удалить все разделы.

Выделите раздел (диск 1 раздел 3 - Основной раздел съемного устройства) и нажмите команду «Удалить» (красный крест на панели команд). В отобразившемся сообщении

необходимо подтвердить действие.

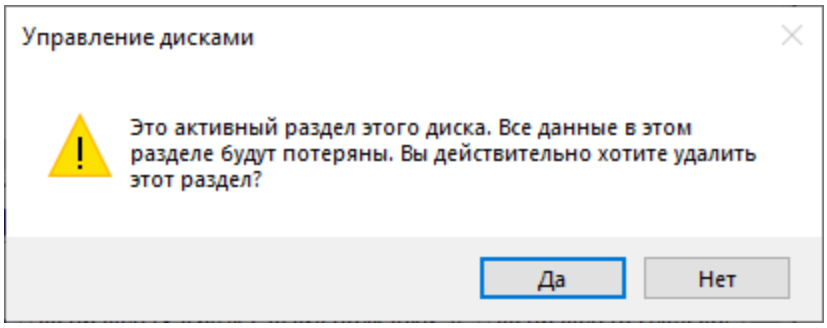


Рисунок 266 - Удаление раздела на дистрибутивном USB-носителе

Для следующего раздела необходимо также подтвердить удаление.

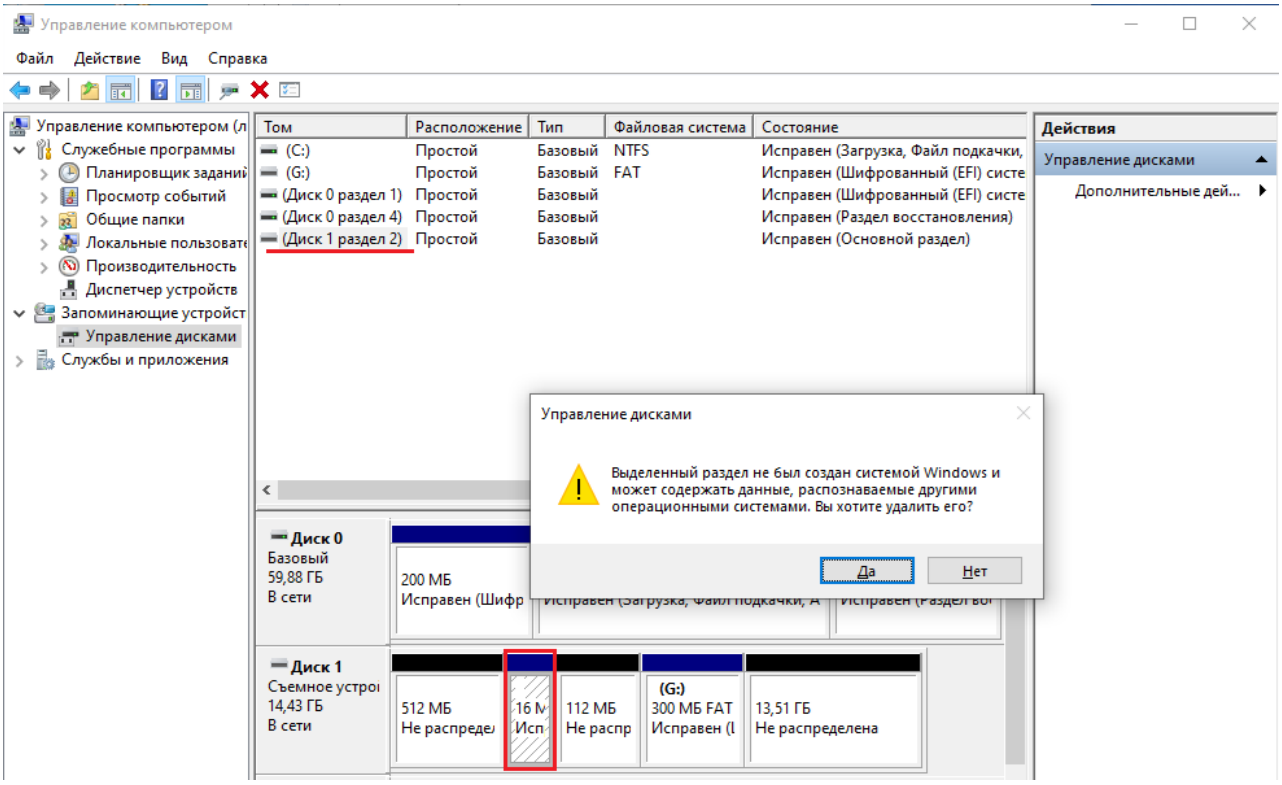


Рисунок 267 - Удаление раздела на дистрибутивном USB-носителе

Для раздела отмеченного буквой необходимо также подтвердить удаление.

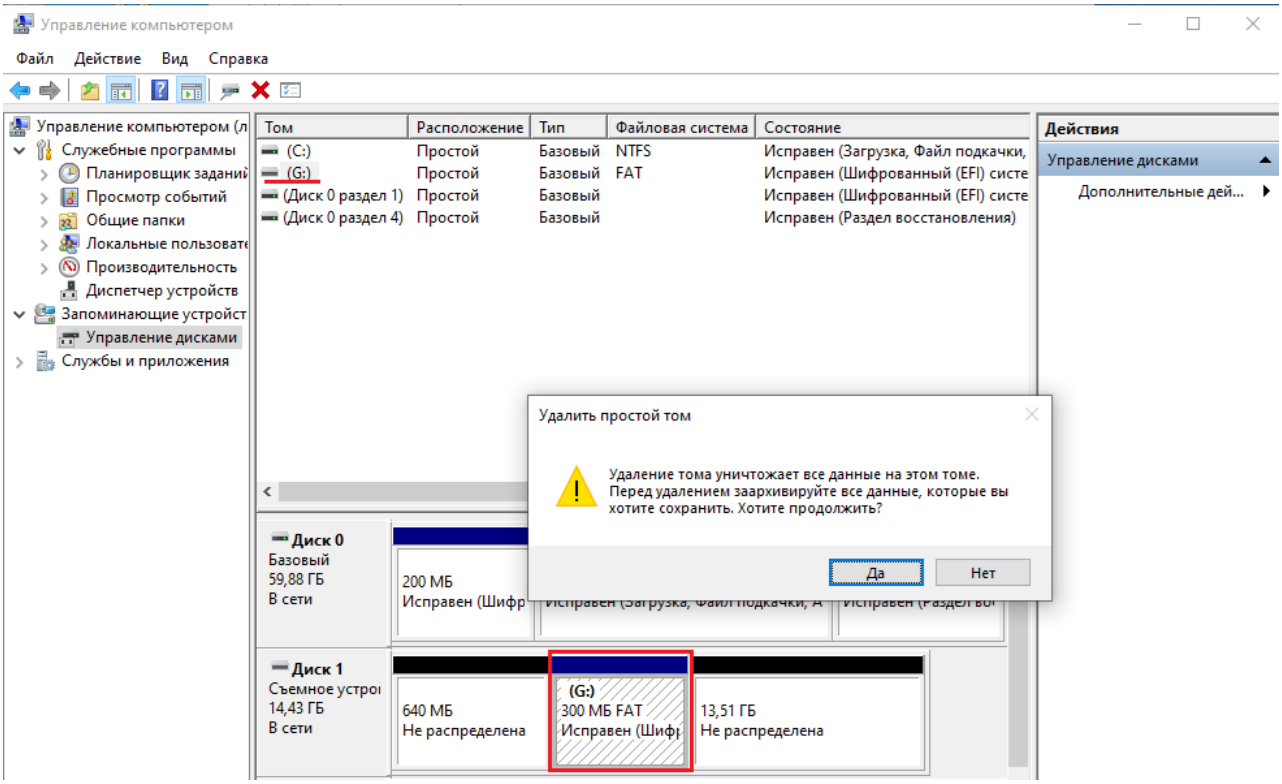


Рисунок 268 - Удаление раздела на дистрибутивном USB-носителе

USB-носитель примет вид неразмеченного диска, он не будет отображаться в списке томов. Создайте простой том на этом диске, выбрав команду в контекстном меню.

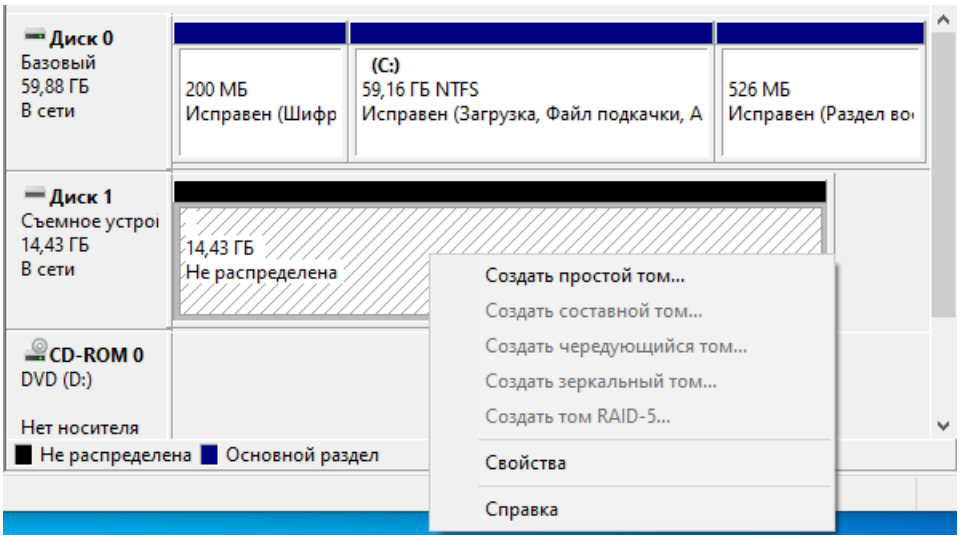


Рисунок 269 - USB-носитель без разделов

Откроется окно мастера создания простого тома.

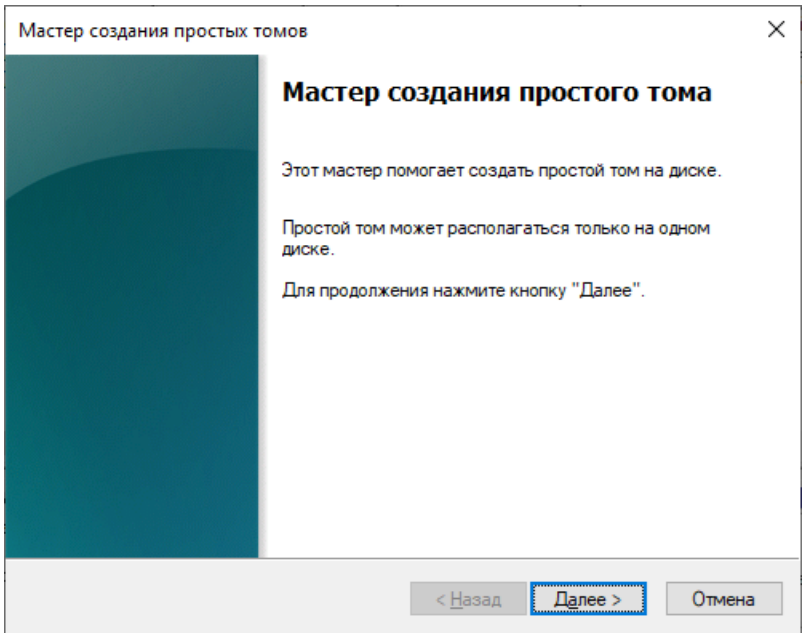


Рисунок 270 - Создание простого тома на дистрибутивном USB-носителе

Укажите размер тома или оставьте параметры по умолчанию.

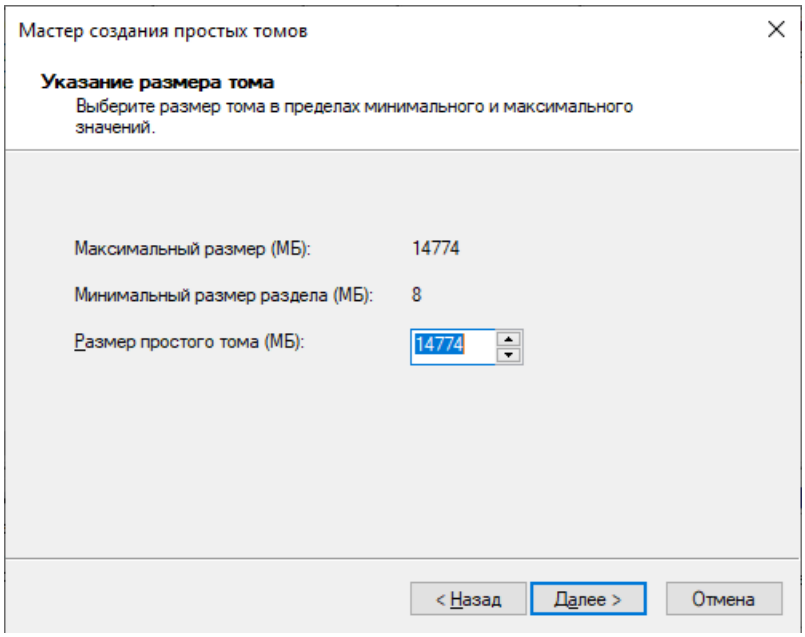


Рисунок 271 - Размер создаваемого тома на дистрибутивном USB-носителе

Назначьте букву диску или оставьте по умолчанию, есть возможность указать путь к диску.

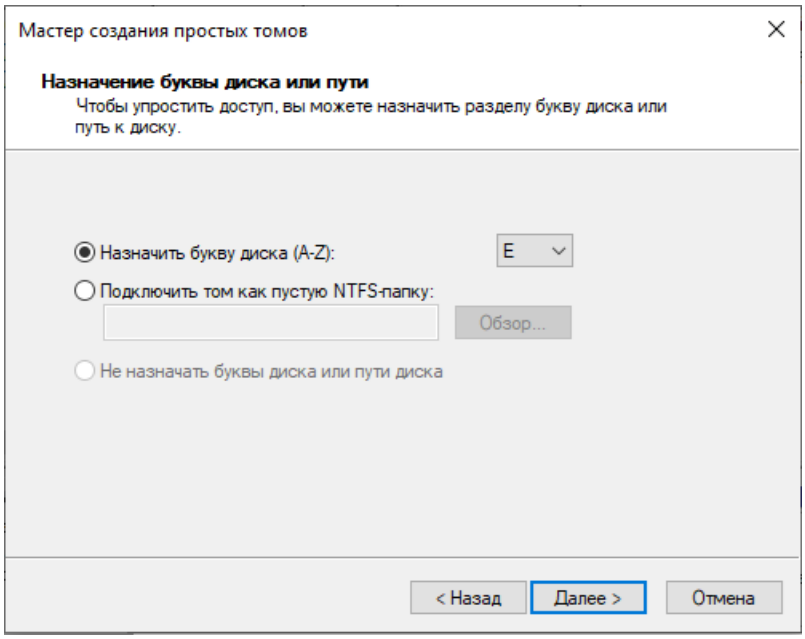


Рисунок 272 - Назначение буквы диска

Отметьте параметры форматирования файловой системы. Рекомендуется снять опцию «Быстрое форматирование».

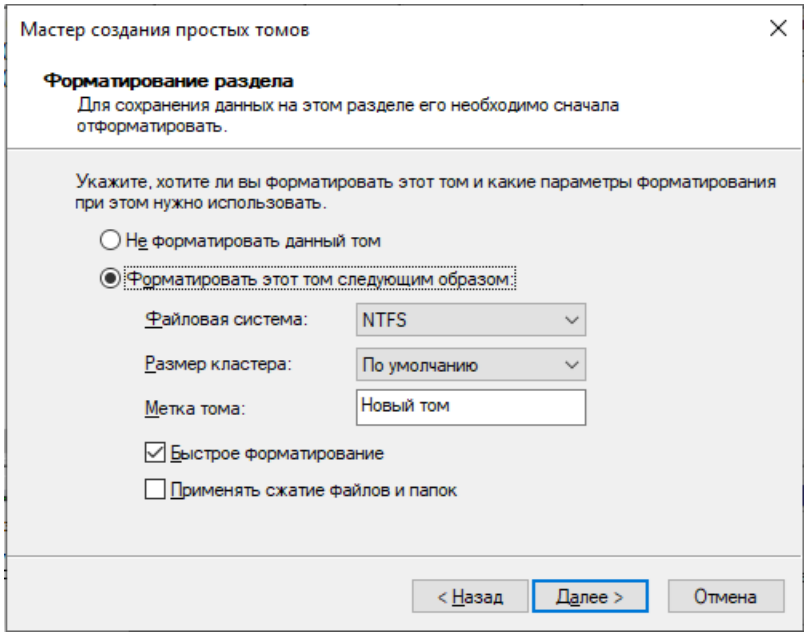


Рисунок 273 - Выбор форматирования

На экран будет выдано окно завершения работы мастера.

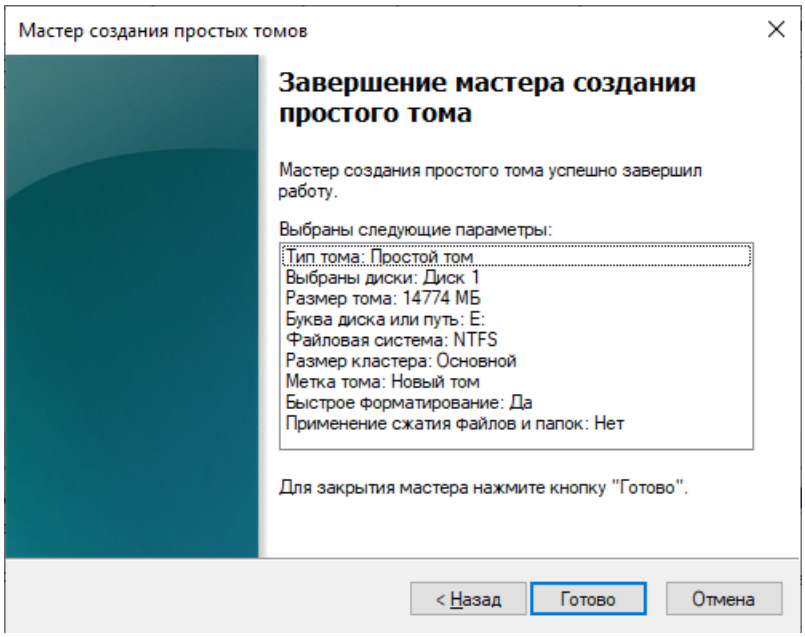


Рисунок 274 - Завершение работы мастера

По завершению работы мастера создания простого тома USB-носитель будет отображаться в списке размеченных томов.

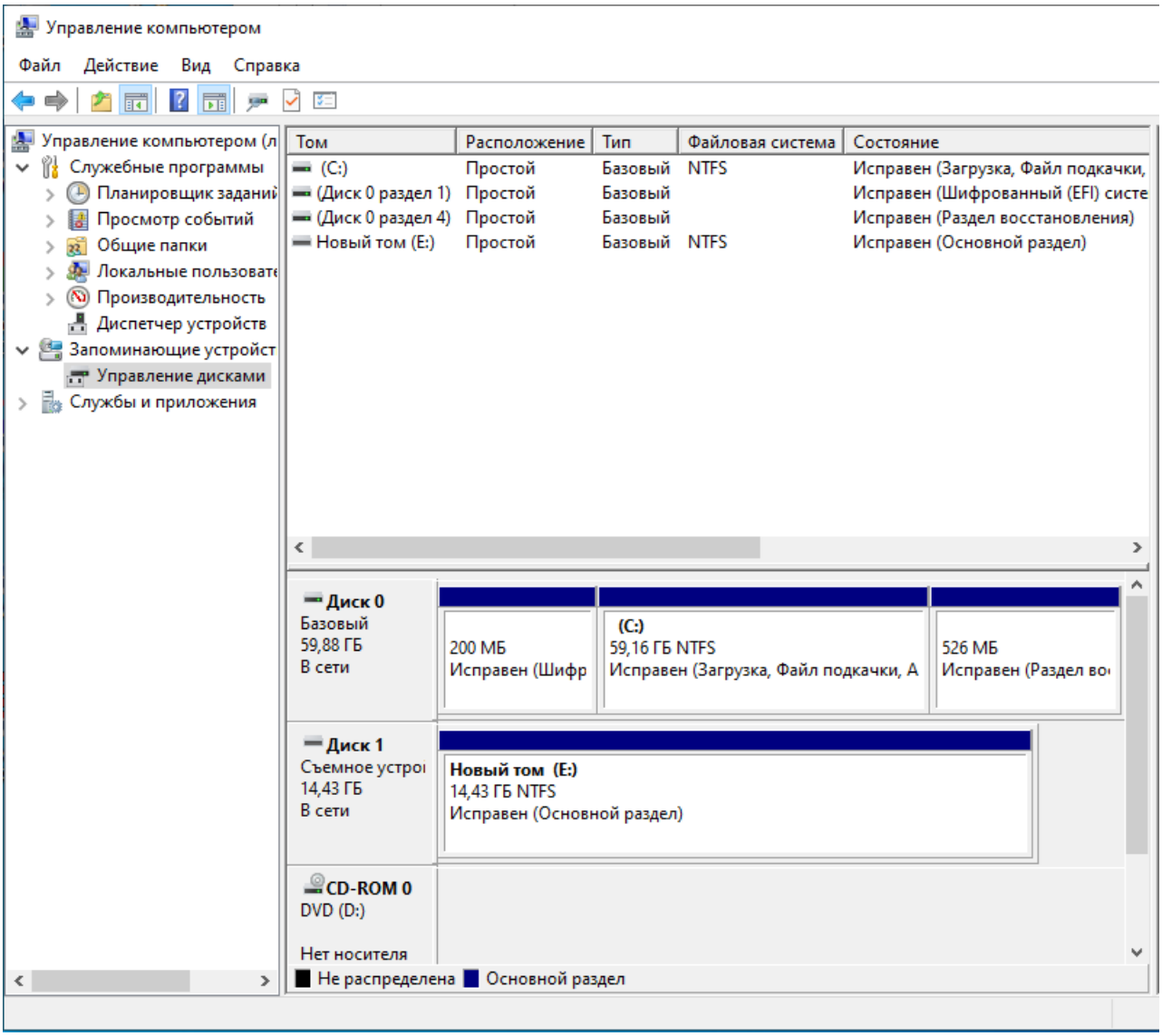


Рисунок 275 - USB-носитель размечен как Основной раздел

После выполнения указанных выше операций, вся информация об экземпляре СКЗИ будет удалена с USB-носителя.

12. 2. 2. Удаление СКЗИ с USB-носителя в ОС Ubuntu

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется форматированием носителя штатными средствами операционной системы.

Далее приведен пример удаления разделов и форматирования дистрибутивного USB-носителя средствами операционной системы 22.04.5 LTS.

Для уничтожения программных модулей СКЗИ с дистрибутивного USB-носителя

необходимо подключить его к компьютеру. Убедитесь, что к компьютеру подключено только это съемное устройство.

Далее следует открыть раздел «Диски», например из меню Dash, задав в строке поиска «disk».

В открывшемся окне отобразится найденный операционной системой USB-носитель с размеченными разделами.

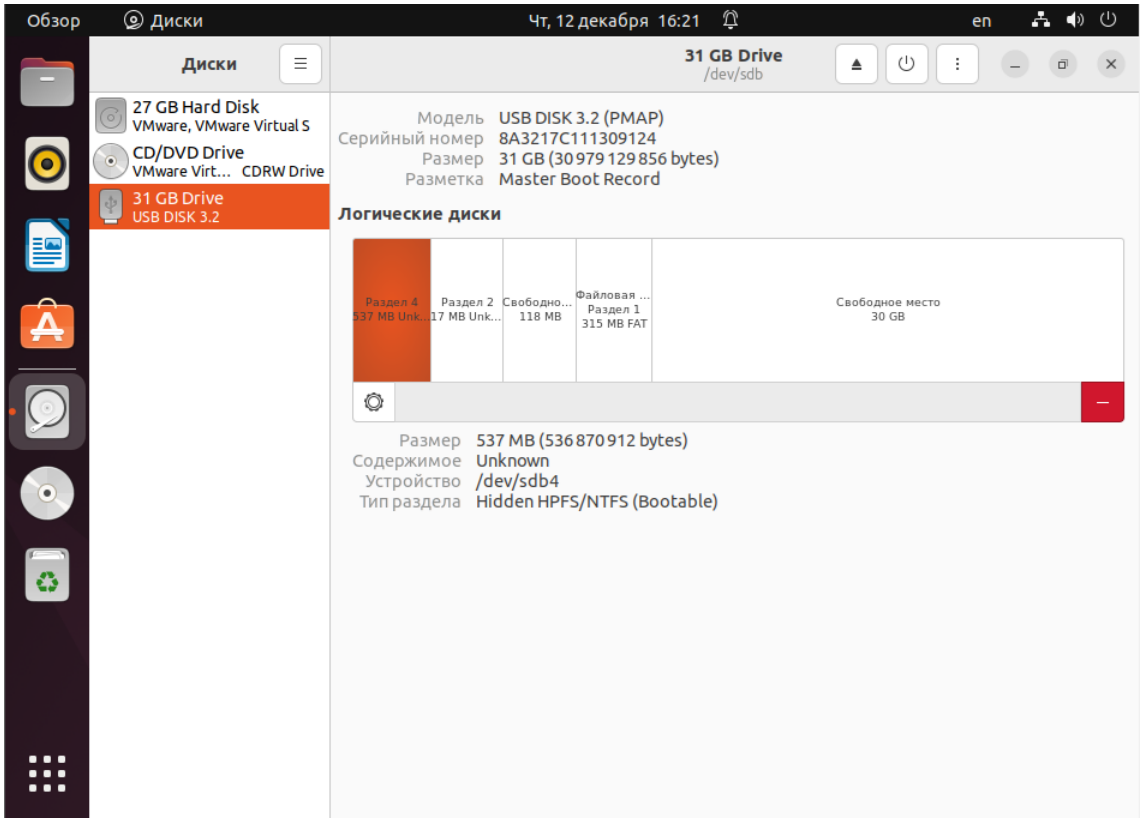


Рисунок 276 - Подключенный дистрибутивный USB-носитель

Требуется удалить все разделы USB-носителя.

Выделите раздел (раздел 4 в примере) и нажмите команду «Удалить выбранный раздел» (красная кнопка в правом углу разметки диска). В отобразившемся сообщении необходимо подтвердить действие.

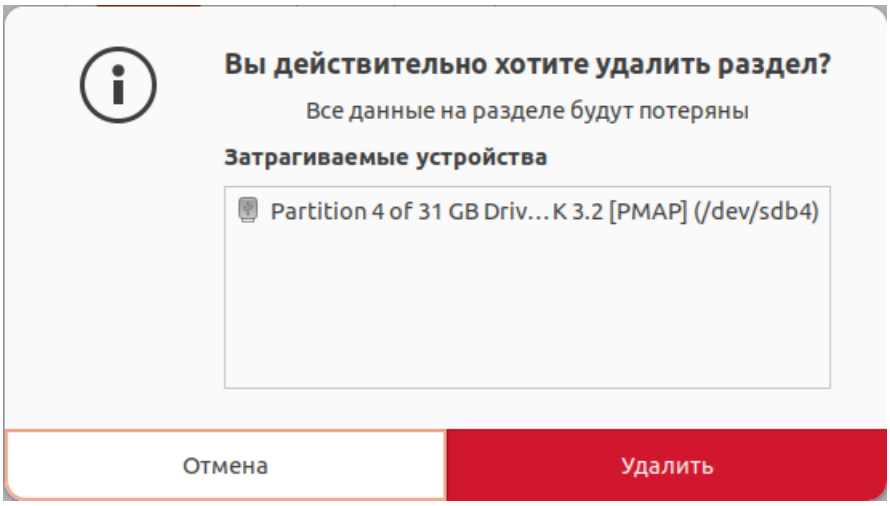


Рисунок 277 - Удаление 4 раздела дистрибутивного USB-носителя

Для следующего раздела необходимо также подтвердить удаление.

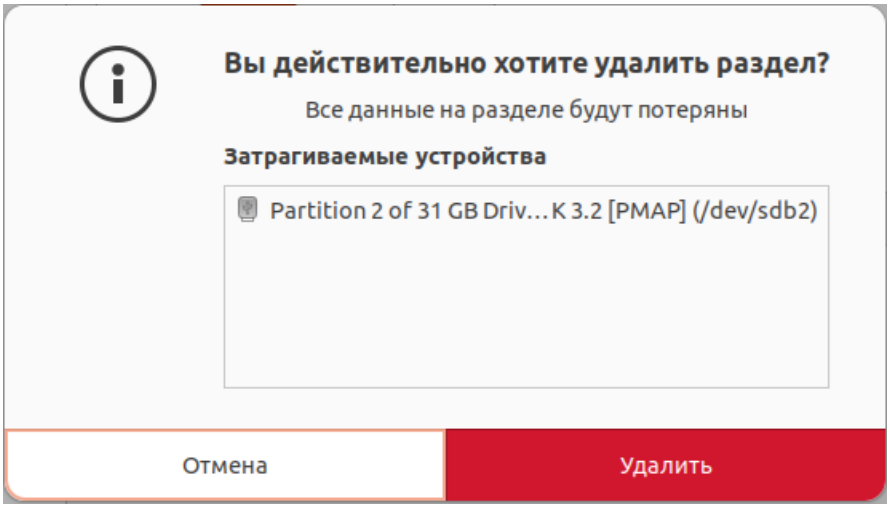


Рисунок 278 - Удаление 2 раздела дистрибутивного USB-носителя

Для последнего, третьего раздела необходимо также подтвердить удаление.

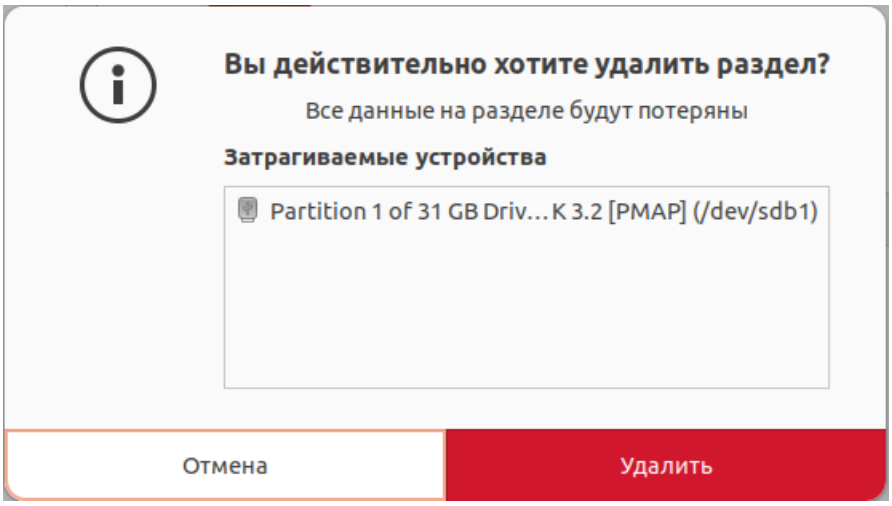


Рисунок 279 - Удаление 1 раздела дистрибутивного USB-носителя

После этого в менеджере дисков операционной системы USB-носитель примет вид неразмеченного диска:

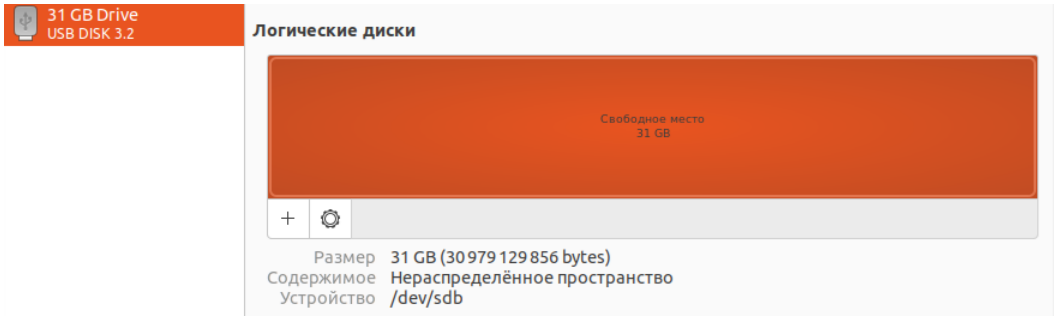


Рисунок 280 - USB-носитель

Далее необходимо создать раздел на неразмеченном диске и форматировать его.

Создайте раздел на этом диске по кнопке «+» в левом углу разметки диска. Откроется окно по созданию раздела, нажмите «Далее» для продолжения.

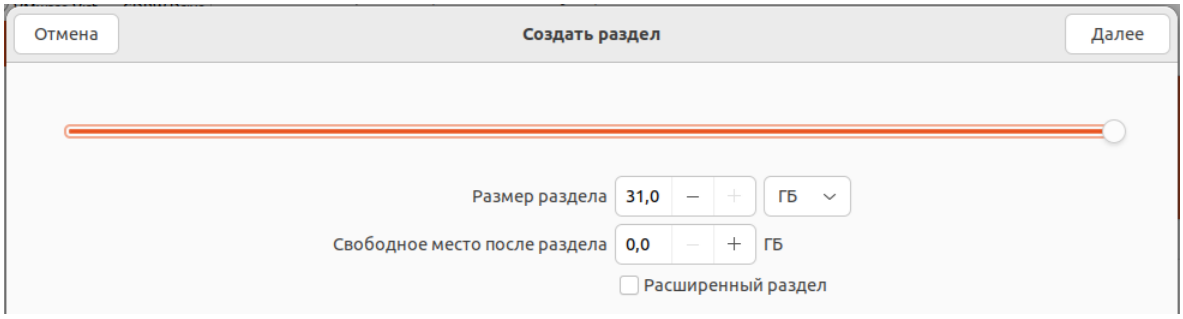


Рисунок 281 - Создание раздела

Отметьте параметры форматирования файловой системы или оставьте настройки по умолчанию. Создайте раздел, нажав на кнопку «Создать».

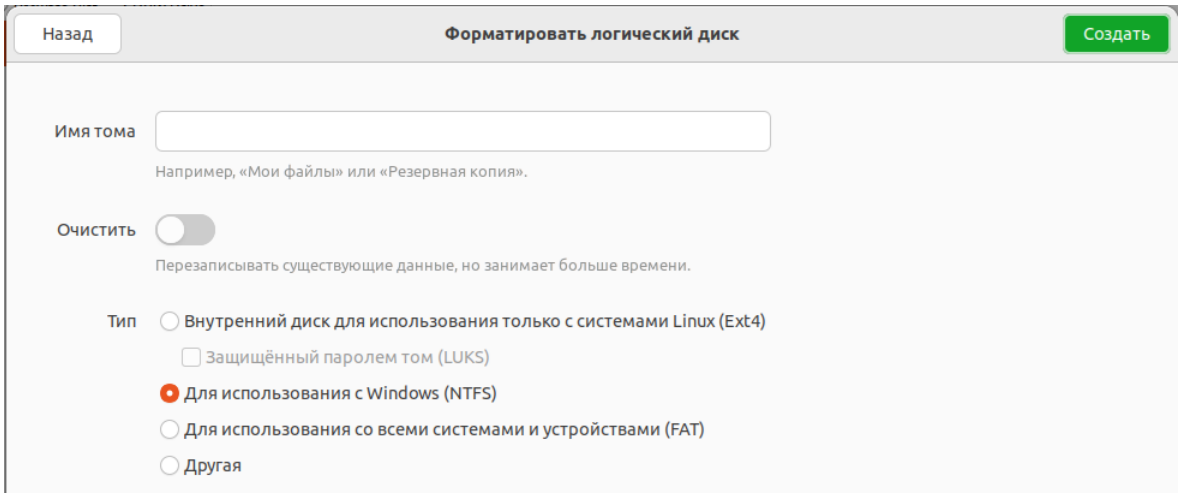


Рисунок 282 - Настройки форматирования

USB-носитель размечен одним разделом.

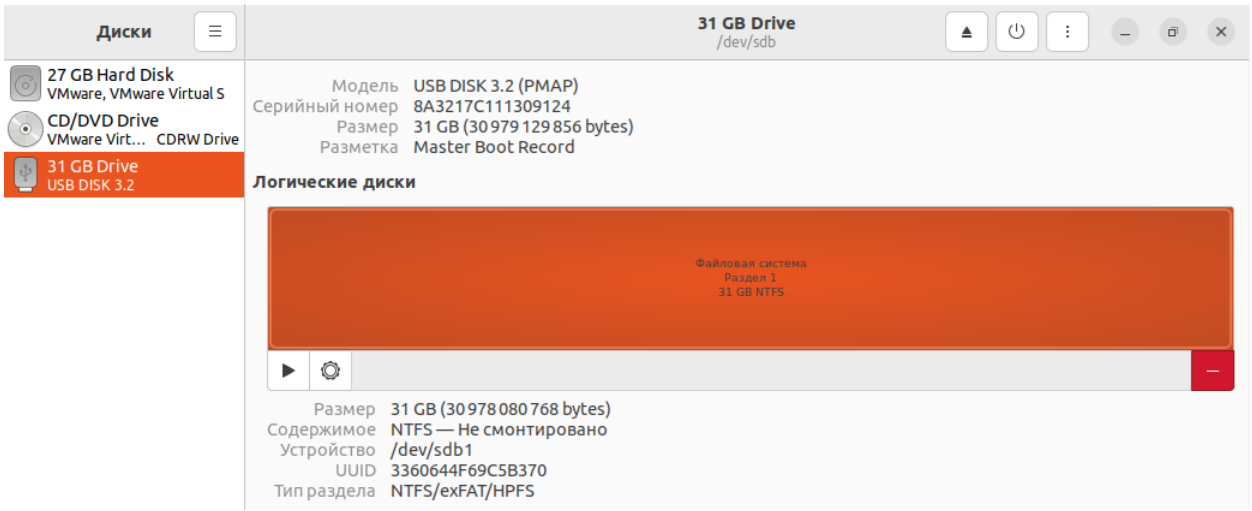


Рисунок 283 - USB-носитель размечен одним разделом

После выполнения указанных выше операций, вся информация об экземпляре СКЗИ будет удалена с USB-носителя.

13. О работе браузера в режиме TLS-клиента

ФПСУ-TLS может применяться для защита информации от НСД, передаваемой между HTTP-сервером и браузером через сети передачи данных общего пользования.

Рассмотрим следующий пример – доступ пользователей браузера к http-серверу wiki.amicon.ru защищается ФПСУ-TLS. Для работы необходимы следующие настройки:

На ФПСУ-TLS:

Необходимо на внутреннем интерфейсе ФПСУ-TLS определить http-сервер wiki.amicon.ru. Каждому http-серверу соответствует внутренний IP-адрес реального сервера, обозначим 012.012.012.012. Браузер в данном случае будет выступать в роли TLS-клиента.

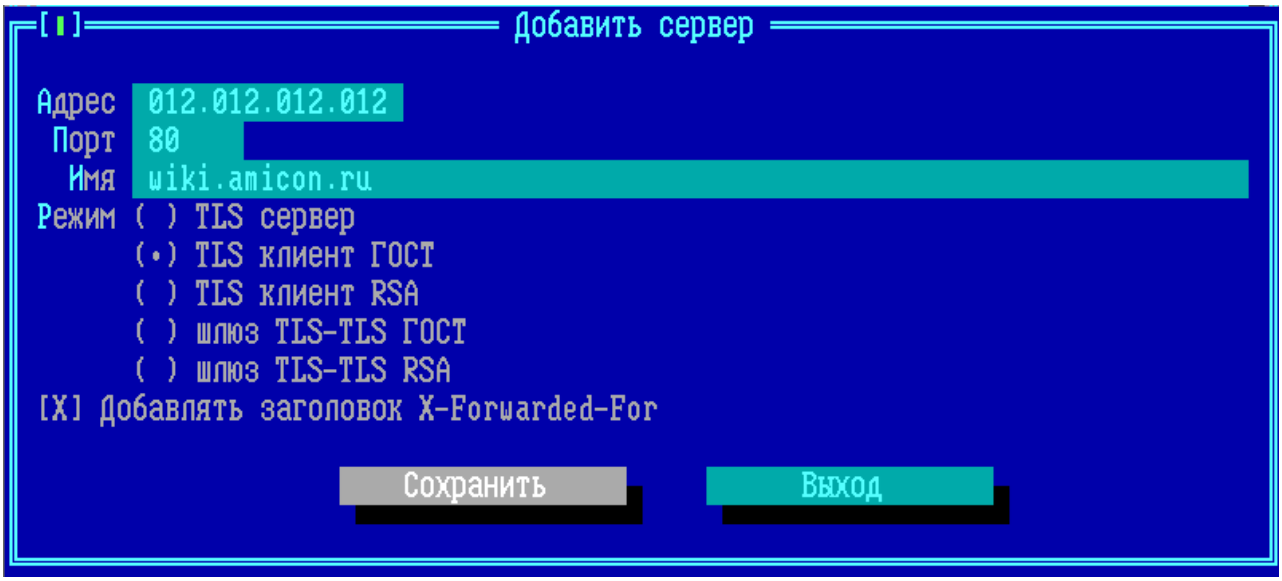


Рисунок 284 - Добавление http-сервера wiki.amicon.ru

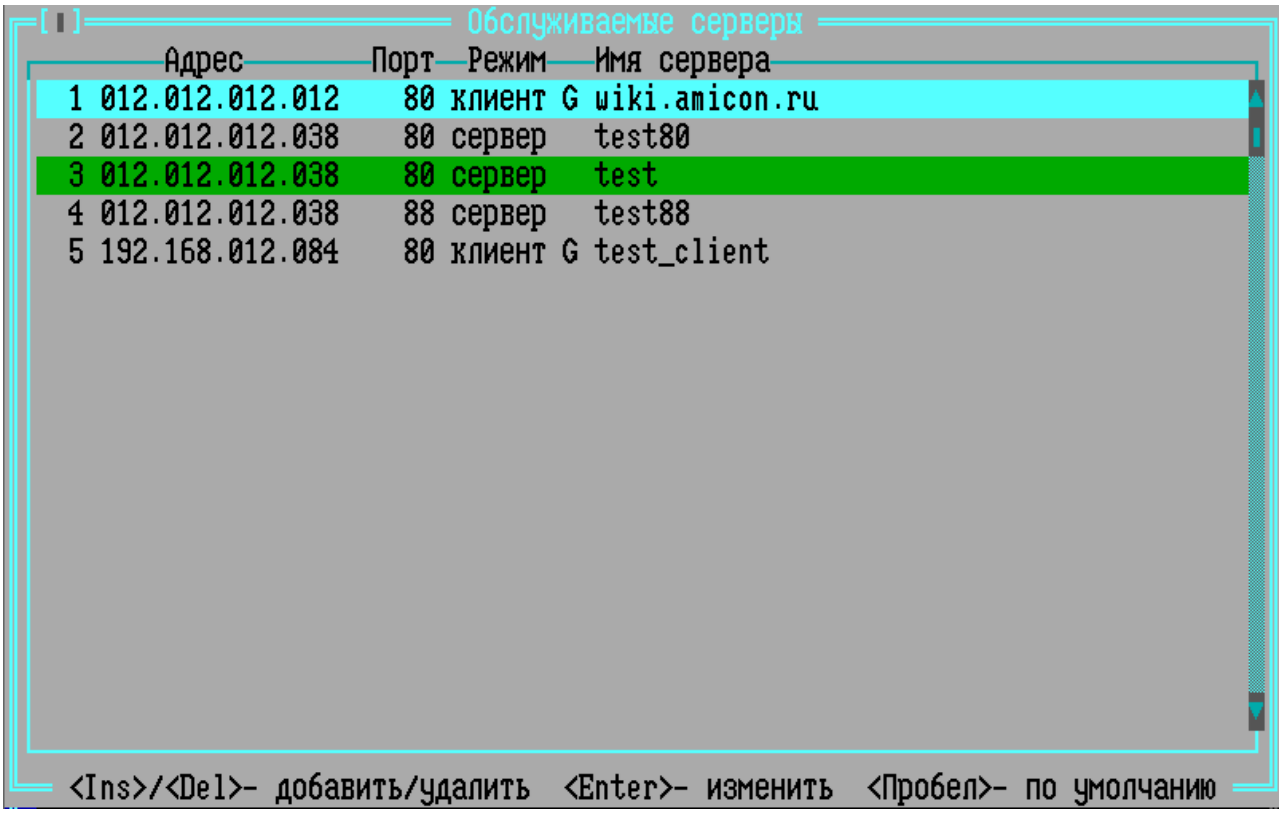


Рисунок 285 - wiki.amicon.ru добавлен в список http-серверов

На DNS сервере:

В глобальном DNS записи «wiki.amicon.ru» должен соответствовать IP-адрес ФПСУ-TLS, обозначим 192.168.001.008. В данном случае IP-адресом ФПСУ-TLS может являться как IP-адрес внешнего интерфейса ФПСУ-TLS, так и виртуальный IP-адрес (см. подробнее пункт «Описание подсистемы масштабирования»).

Пример записи:

192.168.001.008 wiki.amicon.ru

Примечание. Если не используется DNS сервер, запись «wiki.amicon.ru» с IP-адресом ФПСУ-TLS может быть прописана в файле hosts на машине пользователя.

В браузере:

В браузере имя сертификата должно совпадать с именем сервера, в случае несовпадения выдается ошибка.

В адресной строке браузера необходимо указать http-сервер – «https://wiki.amicon.ru».

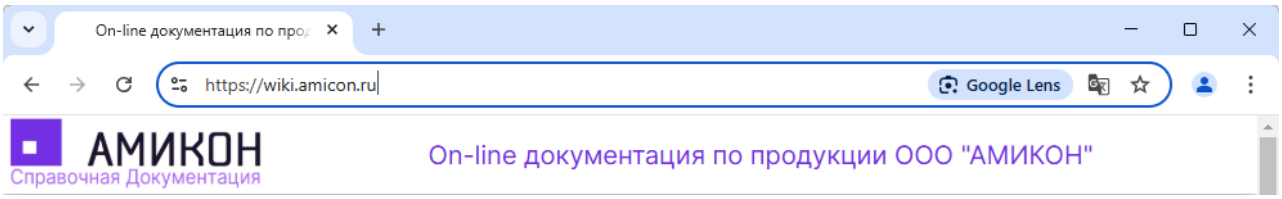


Рисунок 286 - Подключение к http-серверу

После установки данных настроек и обращения к http-серверу из адресной строки браузера будет запущен процесс разыменования имени в адрес ФПСУ 192.168.001.008, установки TLS-соединения и перенаправления уже открытого трафика на адрес 012.012.012.012, указанного для http-сервера wiki.amicon.ru.