ООО «АМИКОН»

УТВЕРЖДЕН

36567521.26.20.40.140.002
РЭ0101-ЛУ

Программно-аппаратный комплекс «ФПСУ-TLS»

Руководство по эксплуатации

Версия документа 1.1

36567521.26.20.40.140.002 РЭ01

Листов 126

2023

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем криптографической защиты информации, построенных с применением программно-аппаратных комплексов «ФПСУ-TLS». В документе содержатся общие сведения о ФПСУ-TLS, приведен перечень необходимых организационно-технических мер и дано описание последовательности действий при настройке параметров функционирования 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.

Содержание

1. Список используемых сокращений и определений

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

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

ОС – операционная система;

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;

УЦ – удостоверяющий центр X.509 сертификатов;

PKCS10 – стандарт, описывающий формат сообщения, содержащего запрос сертификата X.509;

TLS – криптографический протокол, предназначенный для организации защищённой передачи данных между узлами в сети Internet;

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

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

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

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

НСД – несанкционированный доступ к информации;

ПО – программное обеспечение;

ТМ (ТМ-идентификатор) - электронный идентификатор «touch-memory», iButton DS1993 – DS1996;

ФПСУ-TLS – программно-аппаратный комплекс «ФПСУ-TLS» версии 2.5.17, TLS-шлюз, являющийся средством криптографической защиты информации «ФПСУ-TLS».

2. Общие сведения

Программно-аппаратный комплекс «ФПСУ-TLS» является программно-техническим средством защиты от несанкционированного доступа к информации, в котором реализован необходимый набор телекоммуникационных функций сервера в соответствии с требованиями протокола TLS v.1.2 (The Transport Layer Security Protocol, RFC 5246). ФПСУ-TLS выполняет функцию защиты данных, передаваемых в соответствии с протоколом HTTP в глобальных и локальных вычислительных сетях.

ФПСУ-TLS является средством криптографической защиты информации, позволяющим осуществлять шифрование передаваемой информации в соответствии с ГОСТ 28147-89. Алгоритм выработки значения хэш-функции реализован в соответствии с требованиями ГОСТ Р 34.11 94, ГОСТ Р 34.11-2012. Алгоритмы формирования и проверки электронной цифровой подписи (ЭЦП) реализованы в соответствии с требованиями ГОСТ Р 34.10 2001, ГОСТ Р 34.10 2012.

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).

ФПСУ-TLS обеспечивает формирование защищенных межсетевых HTTPS туннелей в соответствии с протоколом TLS v.1.2. 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.

ФПСУ-TLS представляет собой специализированное программно-аппаратное устройство, функционирующее на аппаратной платформе совместимой с IBM PC/AT под управлением ОС Linux.

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.

Программное обеспечение ФПСУ-TLS функционирует в собственной изолированной и функционально замкнутой операционной среде, создаваемой подсистемой ACCESS-TM SHELL. Подсистема осуществляет разграничение доступа к обслуживаемому компьютеру, защиту программных и информационных модулей на жестком диске компьютера, а также реализует диалоговую среду для управления работой ФПСУ-TLS. ФПСУ-TLS содержит удобные диалоговые средства для управления своей работой (настройки сетевых параметров, установления правил идентификации и аутентификации доступа к ФПСУ-TLS, просмотра регистрационной информации, настройка сертификатов), а также для установки некоторых параметров работы самого компьютера (даты и времени).

Разграничение доступа администраторов и контроль их полномочий при запуске ФПСУ-TLS и управлении его работой осуществляется подсистемой ACCESS-TM SHELL по предъявляемым администраторами электронным идентификаторам «touch-memory».

ФПСУ-TLS следует использовать в соответствии с нормативными документами на СКЗИ «ФПСУ-TLS», входящими в комплект поставки.

Программно-аппаратный комплекс «ФПСУ-TLS» разработан ООО «АМИКОН» (лицензии ФСБ РФ № 8264 П от 13 января 2010 г., ФСТЭК России № 0307 от 21 ноября 2006г.).

3. Организационные требования при эксплуатации ФПСУ-TLS

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».

Организационные меры:

При эксплуатации ФПСУ-TLS следует:

- предоставлять право доступа к рабочему месту только ознакомленным с правилами пользования СКЗИ «ФПСУ-TLS» и изучившим эксплуатационную документацию на программно-аппаратный комплекс ФПСУ-TLS лицам;
- запретить осуществление несанкционированного администратором безопасности копирования и использования ключевых носителей.

Организационно-технические меры:

В процессе эксплуатации ФПСУ-TLS необходимо соблюдать ряд организационно-технических требований:

- в BIOS ПЭВМ следует определить установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске;
- в BIOS ПЭВМ следует определить установки, исключающие возможность загрузки операционной системы с гибкого диска, привода CD-ROM, локальной сети и прочих неразрешенных явно в нормативных документах, входящих в состав СКЗИ «ФПСУ-TLS», видов загрузки ОС.

Учет ключевой информации:

В организации, использующей ФПСУ-TLS, должен вестись «Журнал учета СКЗИ» (возможно ведение одного журнала для нескольких ФПСУ-TLS), в соответствии с приложением 2 к приказу ФАПСИ от 13 июня 2001 г. N 152, «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

4. Роли и классы пользователей ФПСУ-TLS

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. ФПСУ-TLS предлагает диалоговые средства для управления своей работой (настройки драйверов сетевого оборудования, задания правил фильтрации, установления правил идентификации и аутентификации доступа к операционной системе ФПСУ-TLS, просмотра регистрационной информации и т.д.), а также для установки параметров работы.

Разграничение доступа допущенных лиц и контроль их полномочий при запуске ФПСУ-TLS и управлении его работой осуществляется подсистемой ACCESS-TM SHELL по предъявляемым допущенными лицами электронным идентификаторам «touch-memory» (в качестве которых могут выступать устройства iButton DS1993 – DS1996) в соответствии с логическим разделением лиц ФПСУ-TLS на две роли и пять условных классов, представленных в нижеследующей таблице:

Таблица 1. Роли и классы пользователей ФПСУ-TLS

Роль/Класс	***Разрешенные действия***
Пользователь/ Без идентификации пользователя	• переинициализация ПСДЧ; • выключение питания ФПСУ-TLS по кнопке Power; • остановка рабочего режима; • 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)
Пользователь/ /Оператор	Все права класса *Без идентификации пользователя* и дополнительно: • запуск ФПСУ-TLS при выключенном режиме автостарта
Администратор/ Инженер	Все права роли *Пользователь* и дополнительно: • просмотр конфигураций; • 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, • 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 ФПСУ-TLS; • контроль целостности ПО ФПСУ-TLS по списку или с записью результатов
Администратор /Главный администратор	Все права класса *Администратор* и дополнительно: • регистрация нового администратора; • установка дополнений/изменений; • переинсталляция ФПСУ-TLS и перевод в рабочий режим из технологического

5. Первоначальная настройка и запуск ФПСУ-TLS

5. 1. Технологический режим ФПСУ-TLS

ФПСУ-TLS поставляется с установленным программным обеспечением, работающим в технологическом режиме. Также технологический режим включается после повторной инсталляции программного обеспечения ФПСУ-TLS.

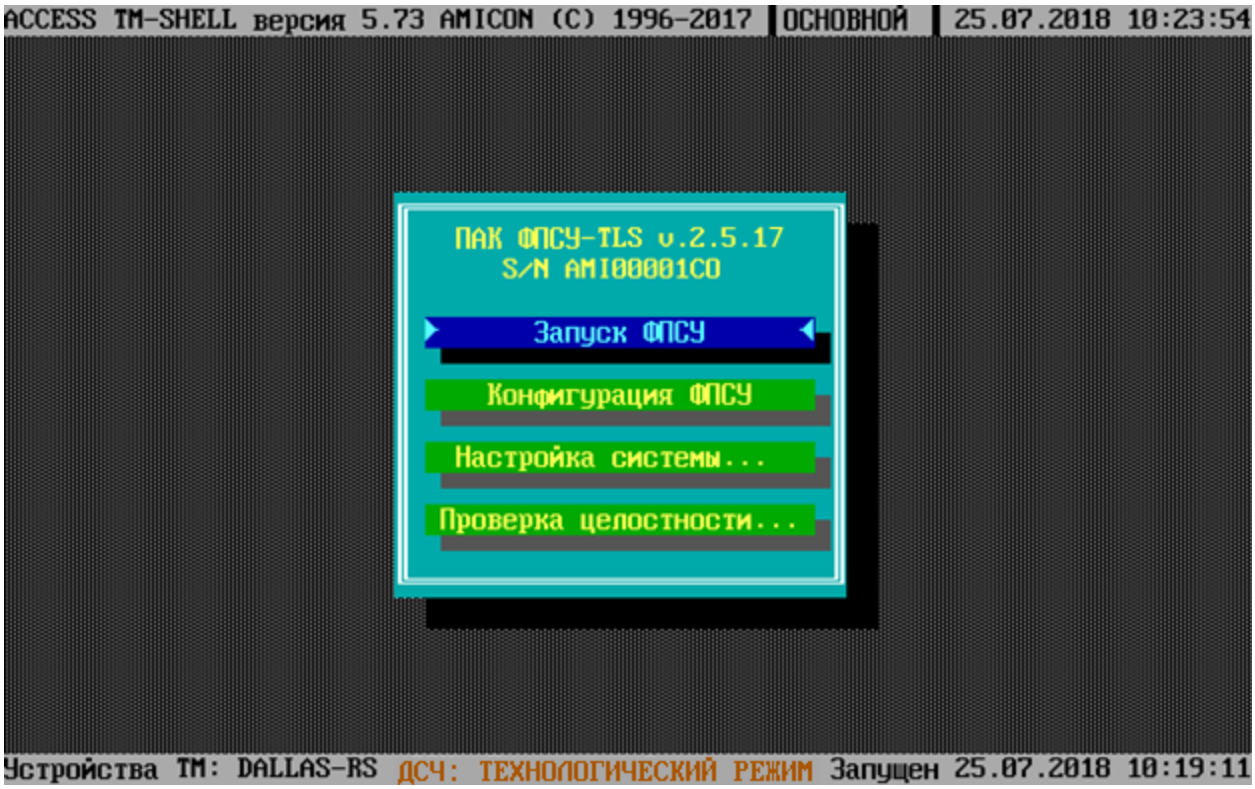

Рисунок 1 - Предупреждение о работе в технологическом режиме

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

- невозможность работы с подсистемой регистрации электронных идентификаторов touch-memory ФПСУ-TLS (см. пункт Регистрация TM-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.

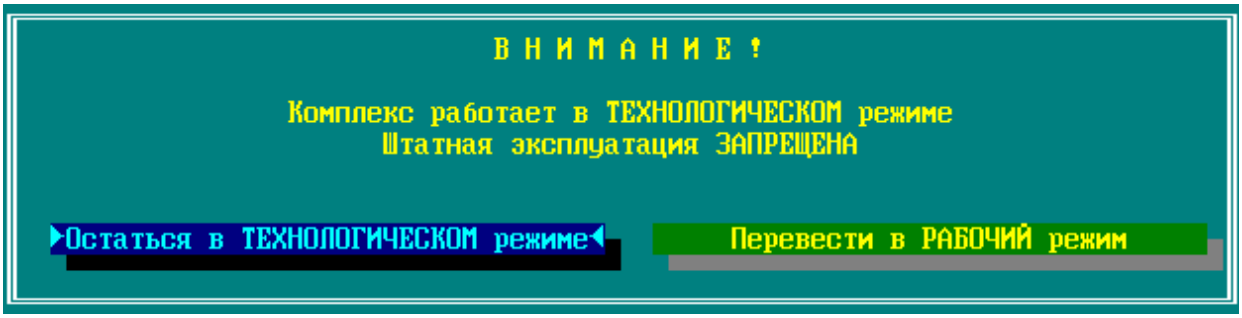

Рисунок <%B%> - Технологический режим

Для выхода из технологического режима в штатный, рабочий режим, выберите и нажмите кнопку «Перевести в РАБОЧИЙ режим». Для перевода ФПСУ-TLS в рабочий режим требуется инициализировать программно-клавиатурный датчик случайных чисел.

От администратора требуется вводить указываемые программой цифры в зависимости от запрашиваемого символа. Дальнейшая работа будет возможна, как только будет осуществлён корректный ввод достаточного количества цифр.

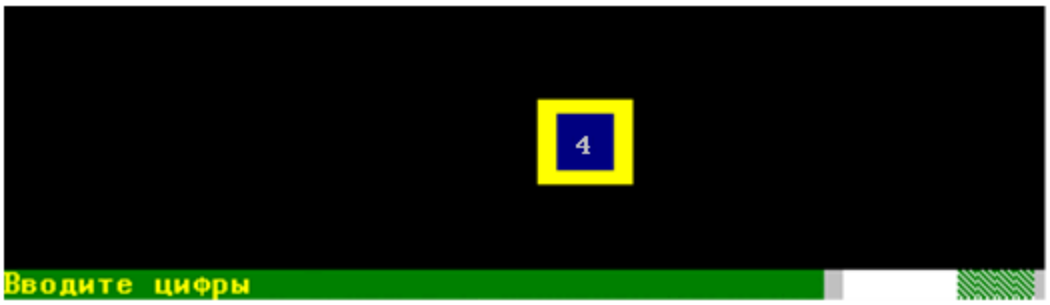

Рисунок 2 - Программно-клавиатурный датчик случайных чисел

После инициализации программного датчика случайных чисел для завершения перехода в рабочий режим будет предложено перерегистрировать основной ТМ Главного администратора и зарегистрировать ещё один ТМ-идентификатор (рекомендуется выбрать запасной ТМ администратора, подробнее о процедуре регистрации ТМ-идентификатора см. пункт Регистрация нового администратора).

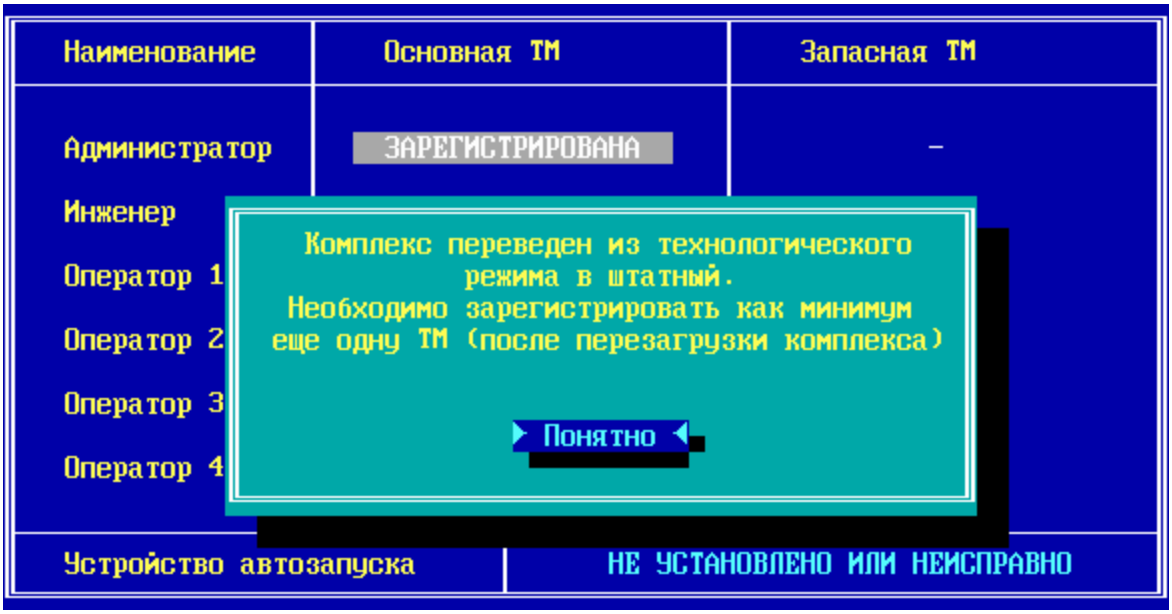

Рисунок <%B%> - Переход в рабочий режим

5. 2. Запуск и главное меню ФПСУ-TLS

После включения питания 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, замещающим экранную выдачу запроса в случае отсутствия монитора. Прижмите к ТМ-считывателю ТМ-идентификатор зарегистрированного на ФПСУ-TLS пользователя. В случае успешной идентификации будет выдан соответствующий звуковой сигнал, стартовый BIOS продолжит работу и ПО ФПСУ-TLS будет загружено. В случае задействованной подсистемы автоматического старта (см. пункт Включение подсистемы автоматического старта) данная процедура первоначальной идентификации пропускается, и ФПСУ-TLS сразу переходит в рабочий режим.

Если 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.

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

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 основное меню ФПСУ-TLS. Выход в основное меню будет осуществлен также и при выходе из рабочего режима по нажатию сочетания клавиш <Alt+X> или <Alt+F1>.

В основном меню ФПСУ-TLS отображается версия программного обеспечения (v.2.5.17 на рисунке) и серийный номер этого ФПСУ-TLS (AMI00001C0 на рисунке).

Основное меню содержит команды для настройки системы, конфигурирования оборудования, установки режимов работы ФПСУ-TLS. Выбор каждой команды (кроме команды «Запуск ФПСУ») повлечет за собой запрос на идентификацию администратора и проверку его прав доступа (с предъявлением соответствующего электронного ТМ-идентификатора) на запрашиваемые действия.

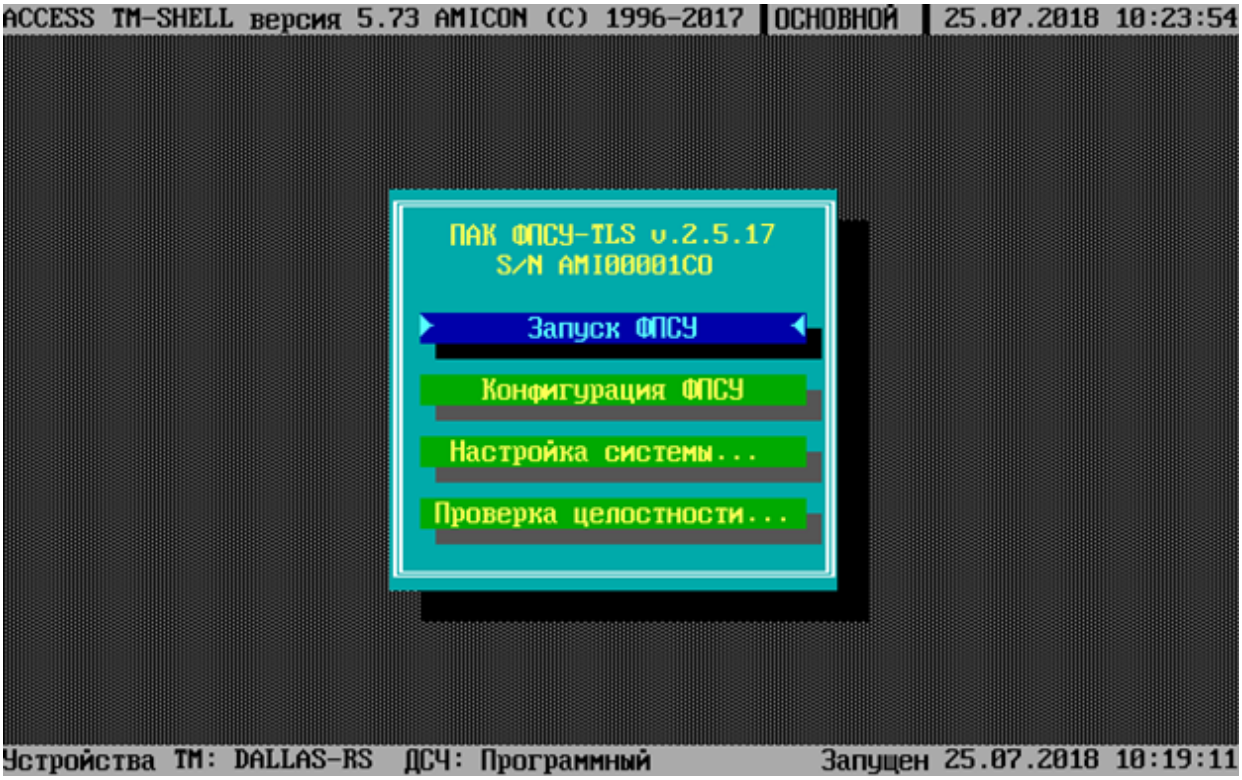

Рисунок 3 - Основное меню ФПСУ-TLS

Выполнение команды «Запуск ФПСУ» переводит ФПСУ-TLS в рабочий режим защиты http-трафика.

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. 3. 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».

Для выполнения команды потребуются права класса «Администратор» или «Инженер» ФПСУ-TLS (см. раздел Роли и классы пользователей ФПСУ-TLS).

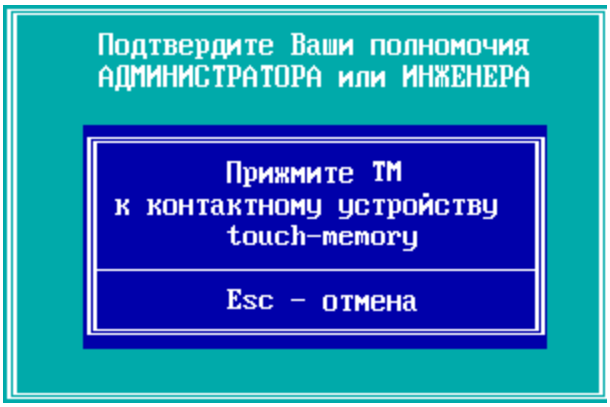

Рисунок 4 - Выполнение команды «Конфигурация ФПСУ»

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

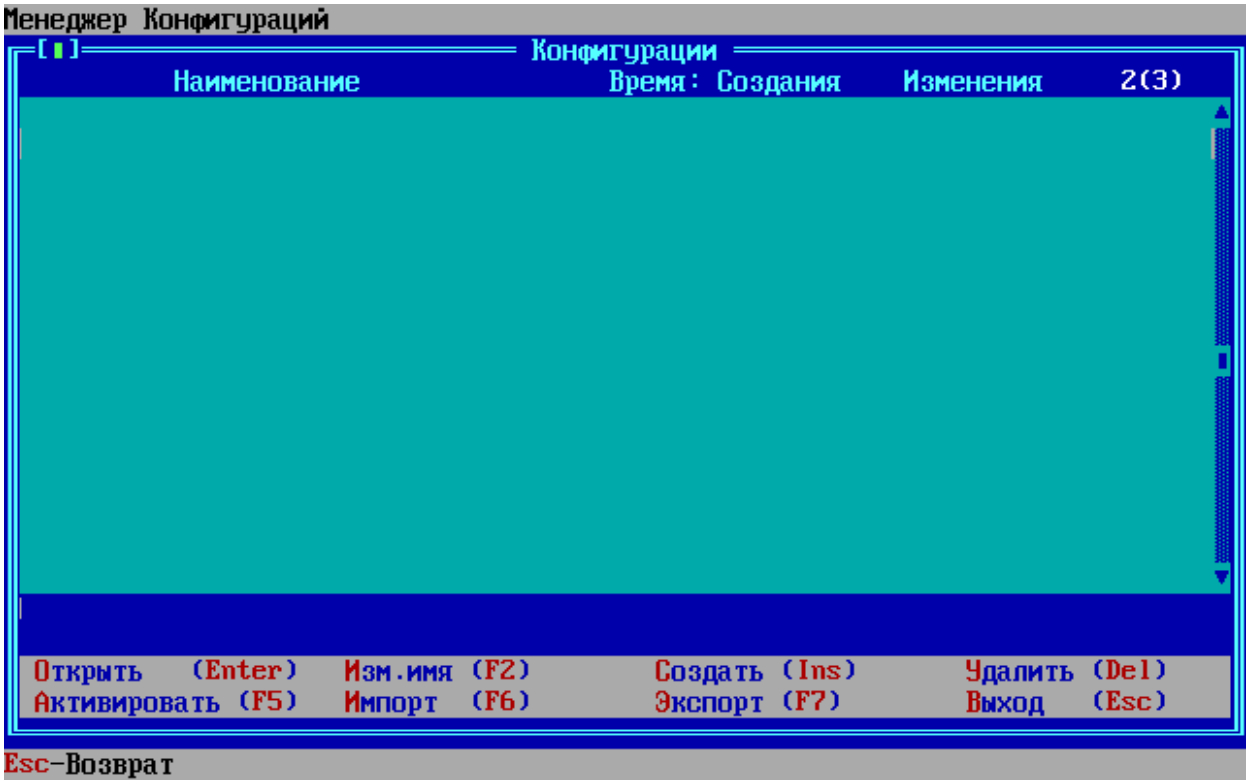

Рисунок 5 - Стартовое пустое окно менеджера конфигураций

Подтвердите создание новой конфигурации:

Рисунок 6

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.

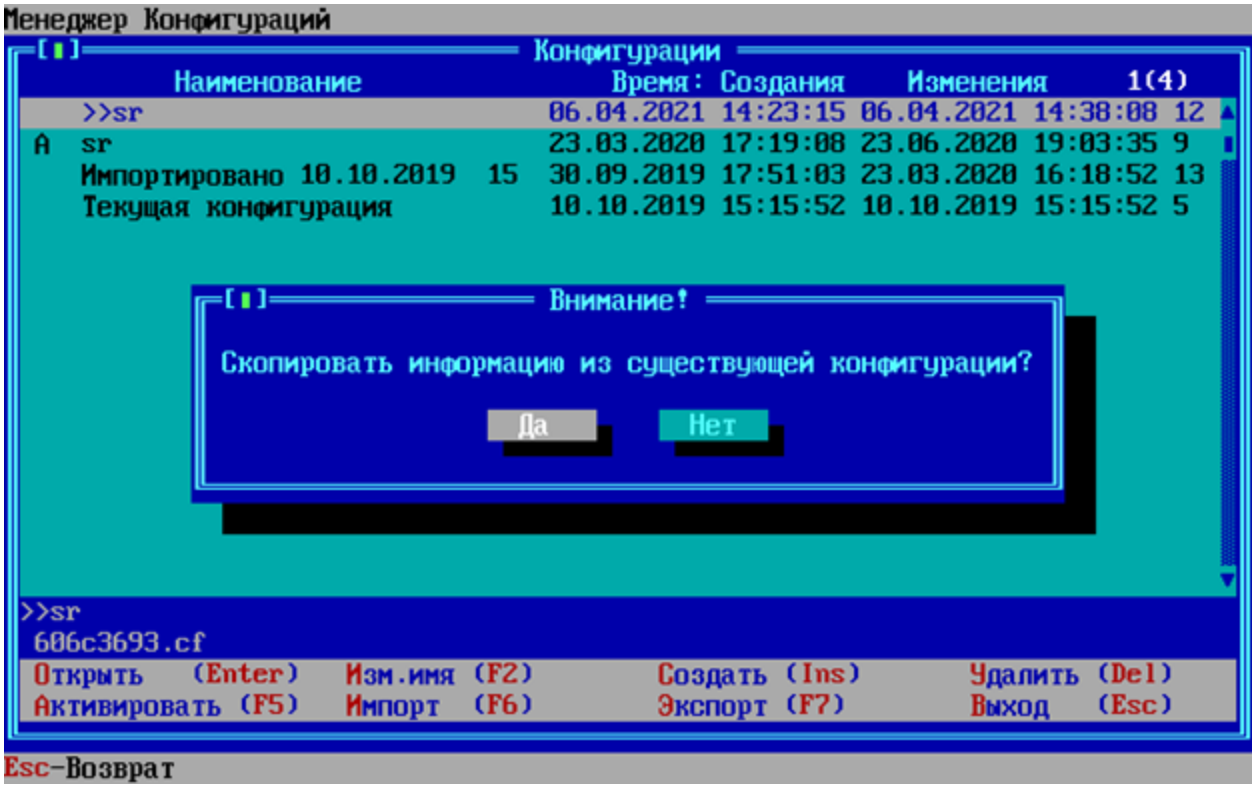

Рисунок 7

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».

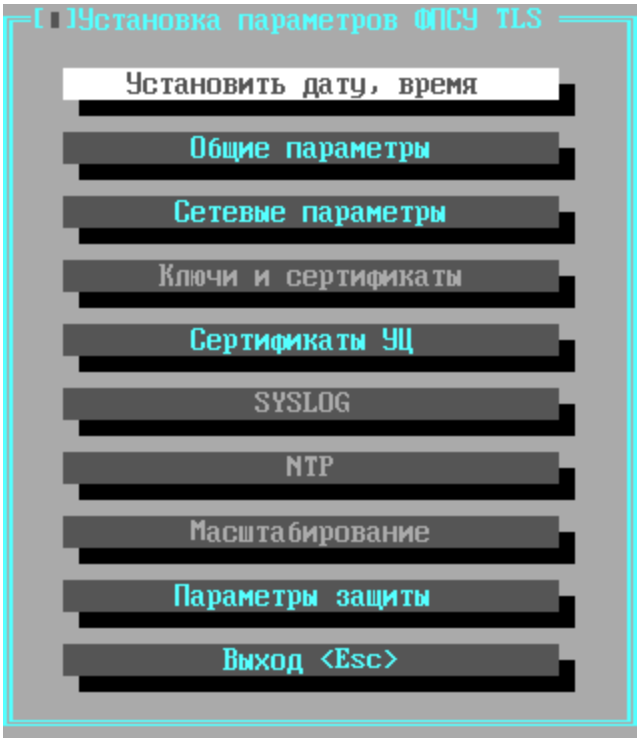

Рисунок 8 - Меню установки параметров ФПСУ-TLS

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. 4. 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.

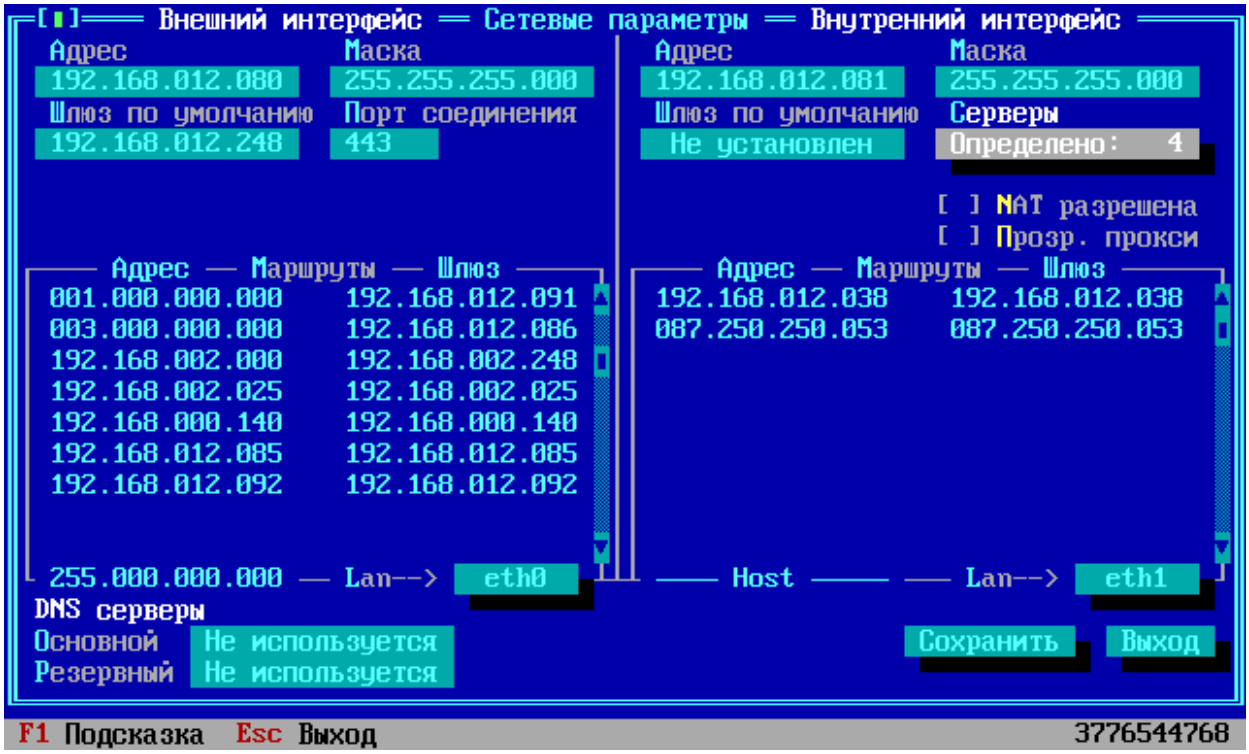

Рисунок 9 - Окно настройки сетевых параметров ФПСУ-TLS

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 которой 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.

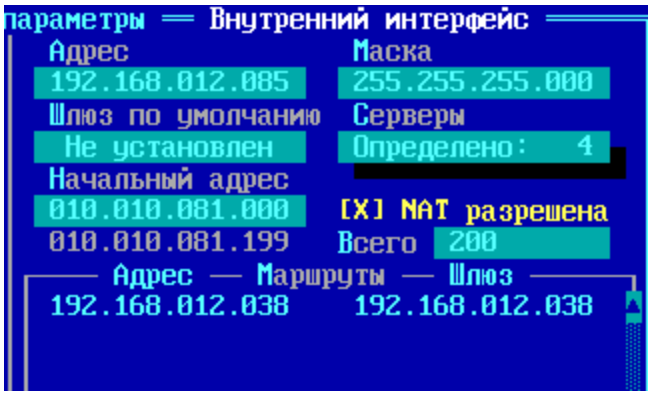

Рисунок 10 - Настройки NAT

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. 4. 1. Настройка защищаемых http-серверов

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>.

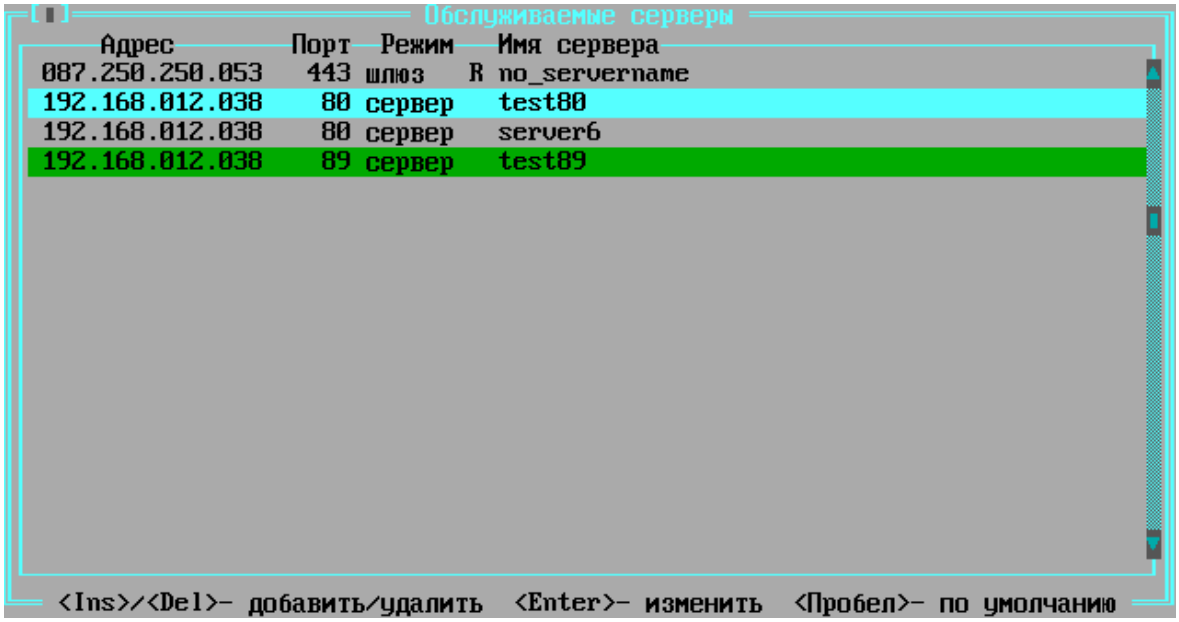

Рисунок 11 - Список обслуживаемых серверов

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

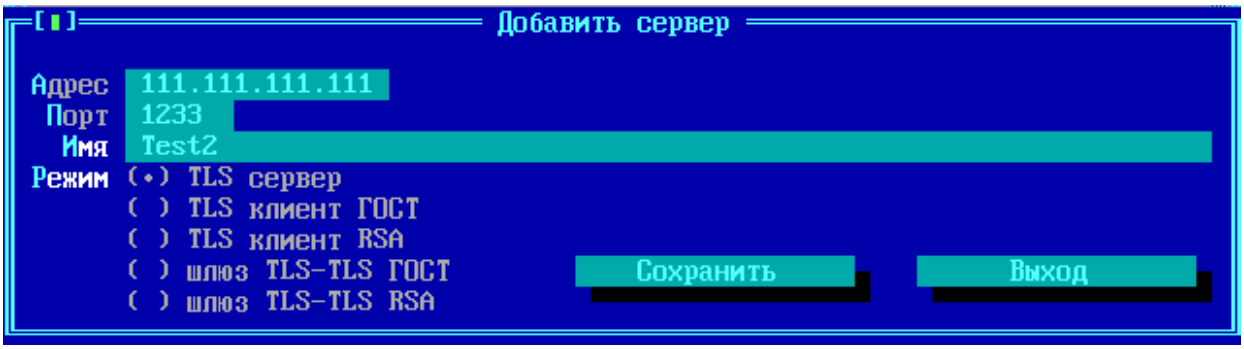

Рисунок 12 - Указание параметров обслуживаемого сервера

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).

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

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

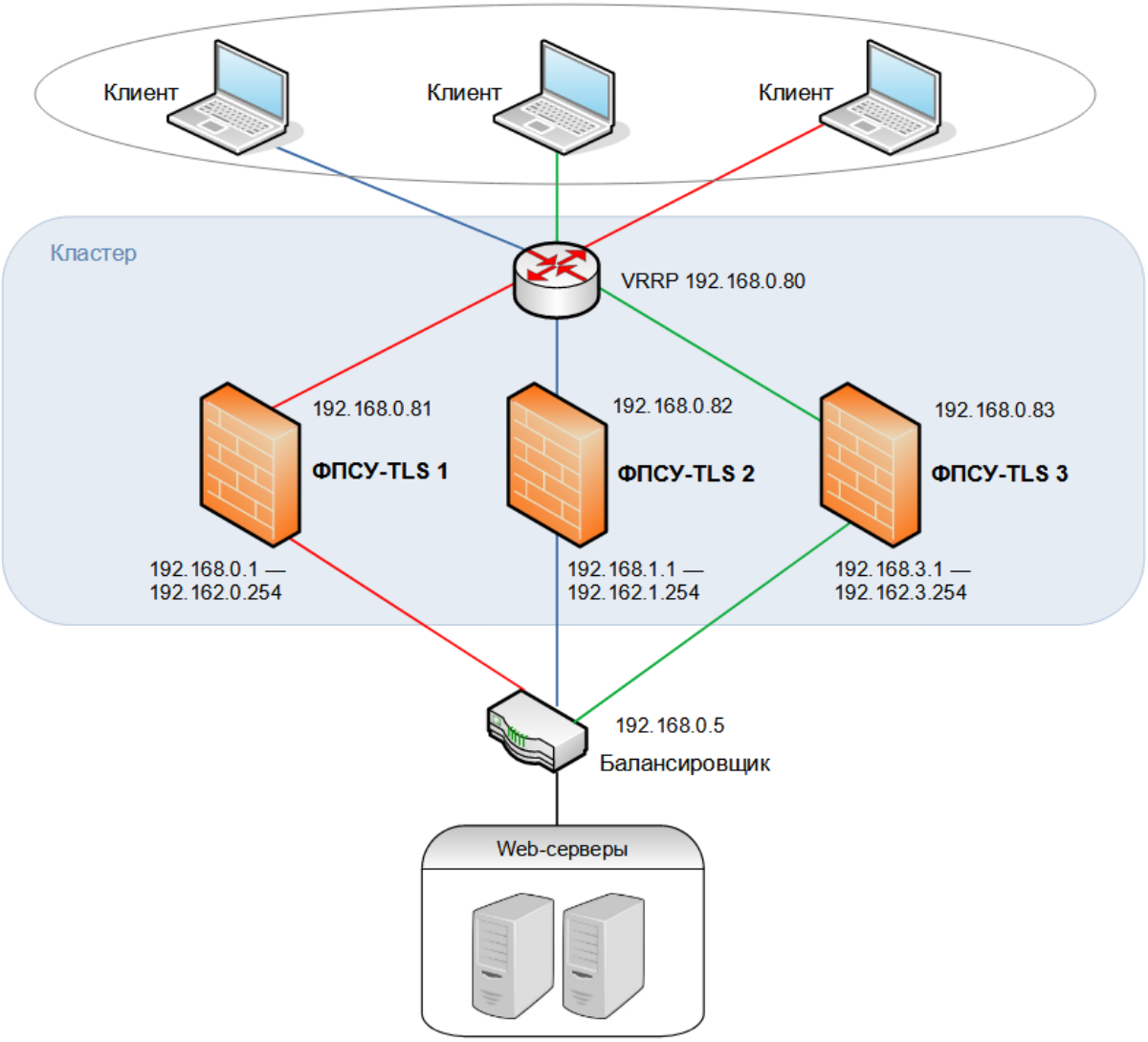

Рисунок 13 - Схема работы ФПСУ-TLS в режиме NAT

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

5. 5. 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. 5. 1. Установка сертификатов удостоверяющих центров

Установка корневого сертификата удостоверяющего центра 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 «Сертификаты УЦ» меню установки параметров ФПСУ-TLS.

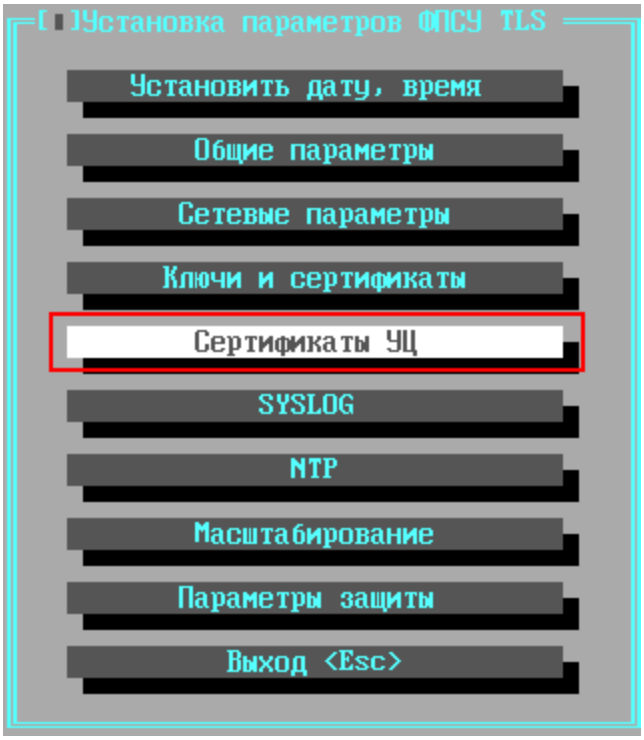

Рисунок 14 - Меню ФПСУ-TLS

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:

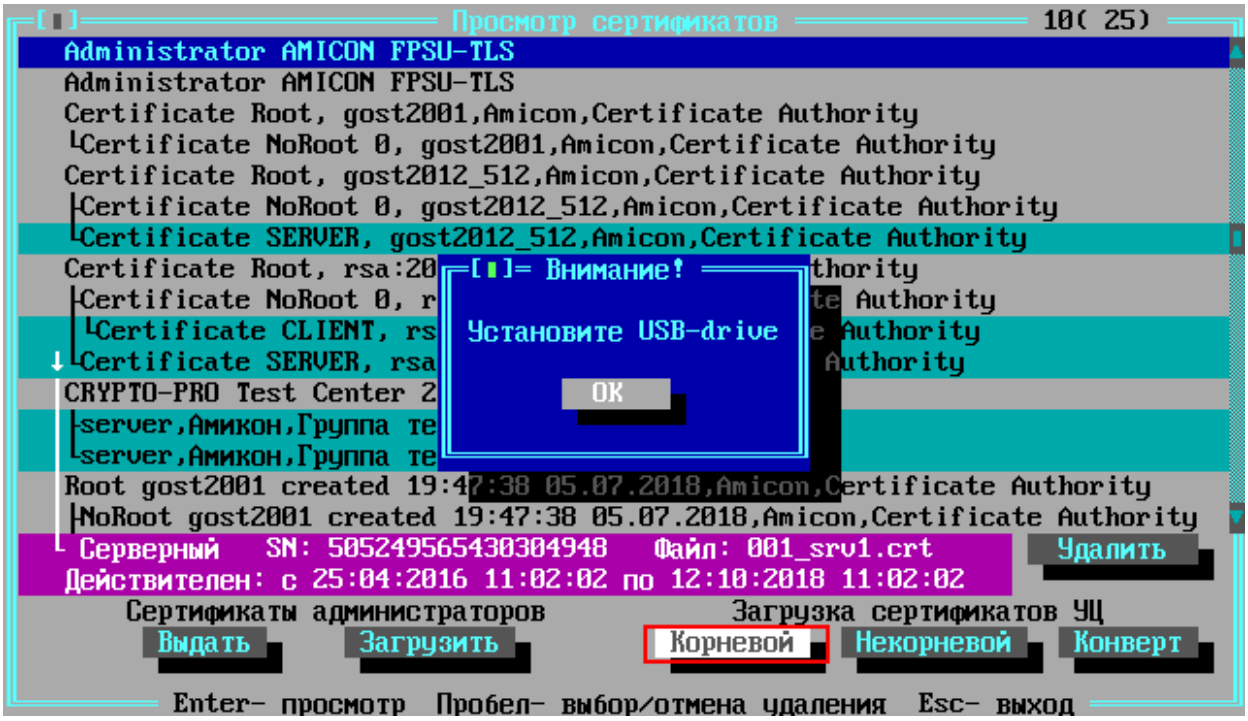

Рисунок 15 - Загрузка корневого сертификата

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».

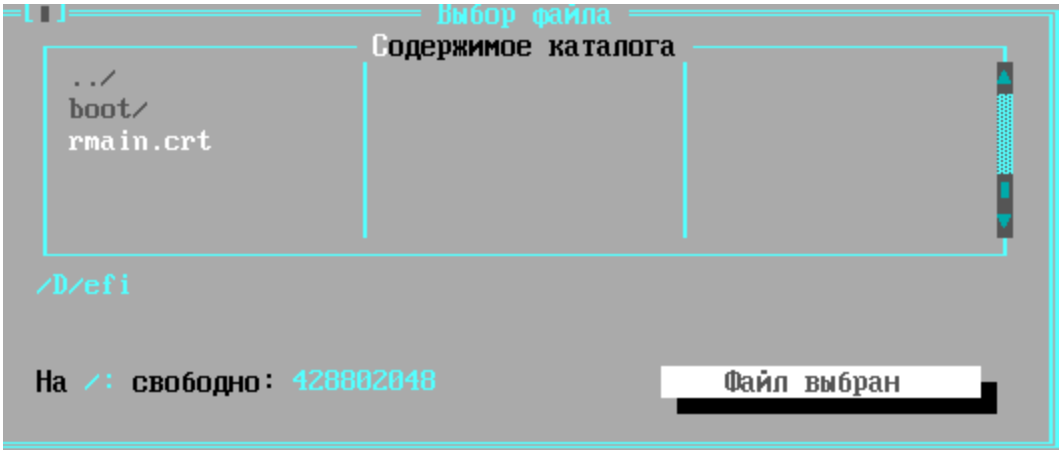

Рисунок 16 - Выбор файла с корневым сертификатом УЦ

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 «v», затем нажмите кнопку ***«Удалить»***.

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

5. 5. 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 «Сертификаты УЦ» меню установки параметров ФПСУ-TLS.

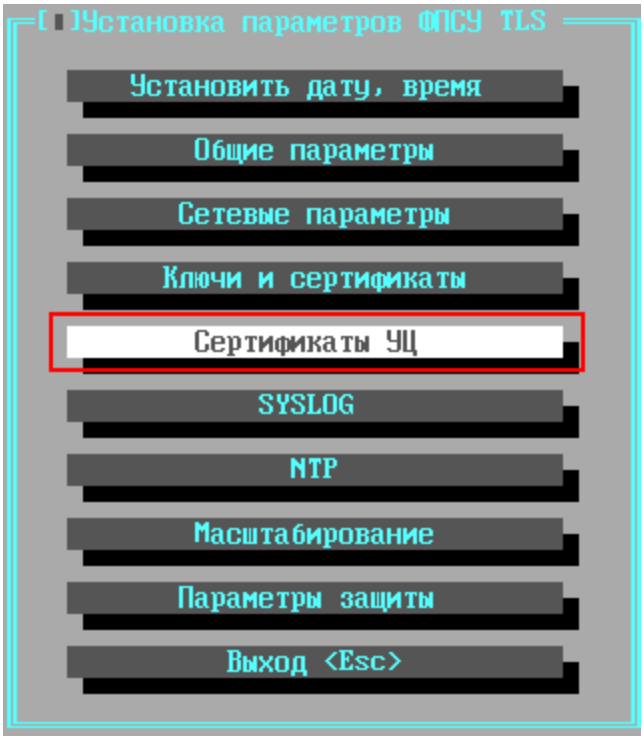

Рисунок 17 - Меню ФПСУ-TLS

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

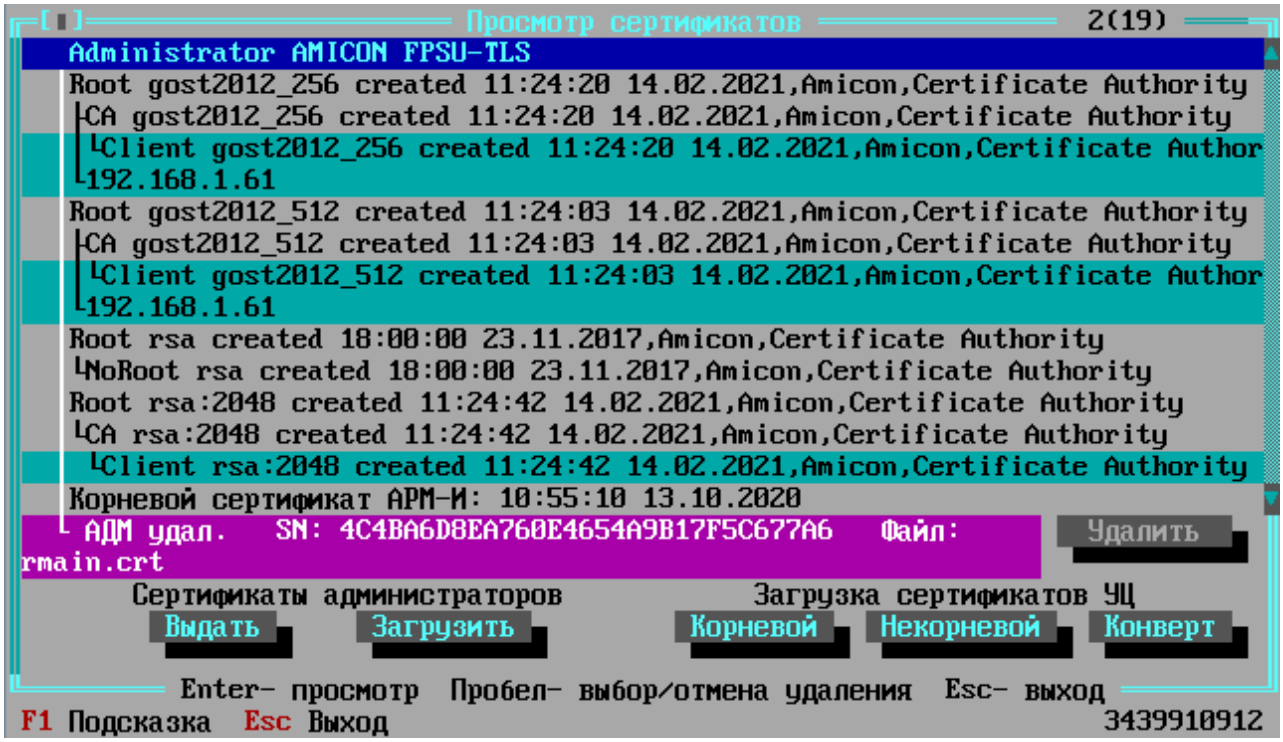

Рисунок 18 - Окно «Просмотр сертификатов»

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.

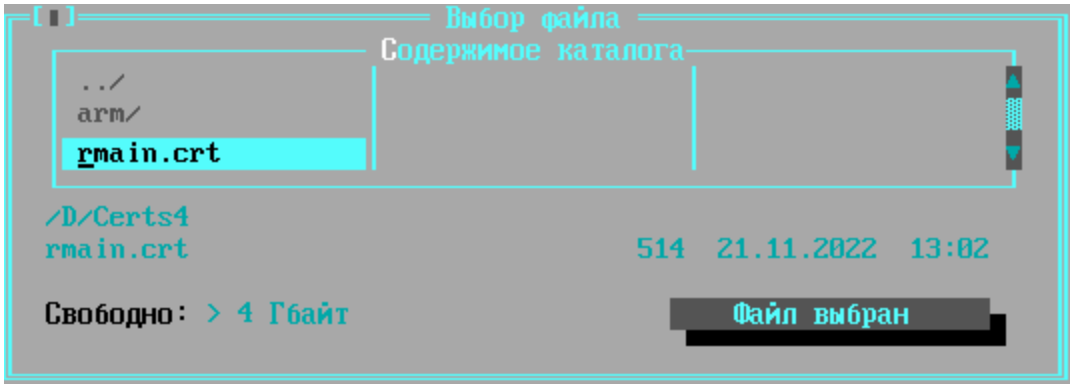

Рисунок 19 - Выбор файла с сертификатом администратора ФПСУ-TLS

Подтвердите загрузку по кнопке «Принять сертификат».

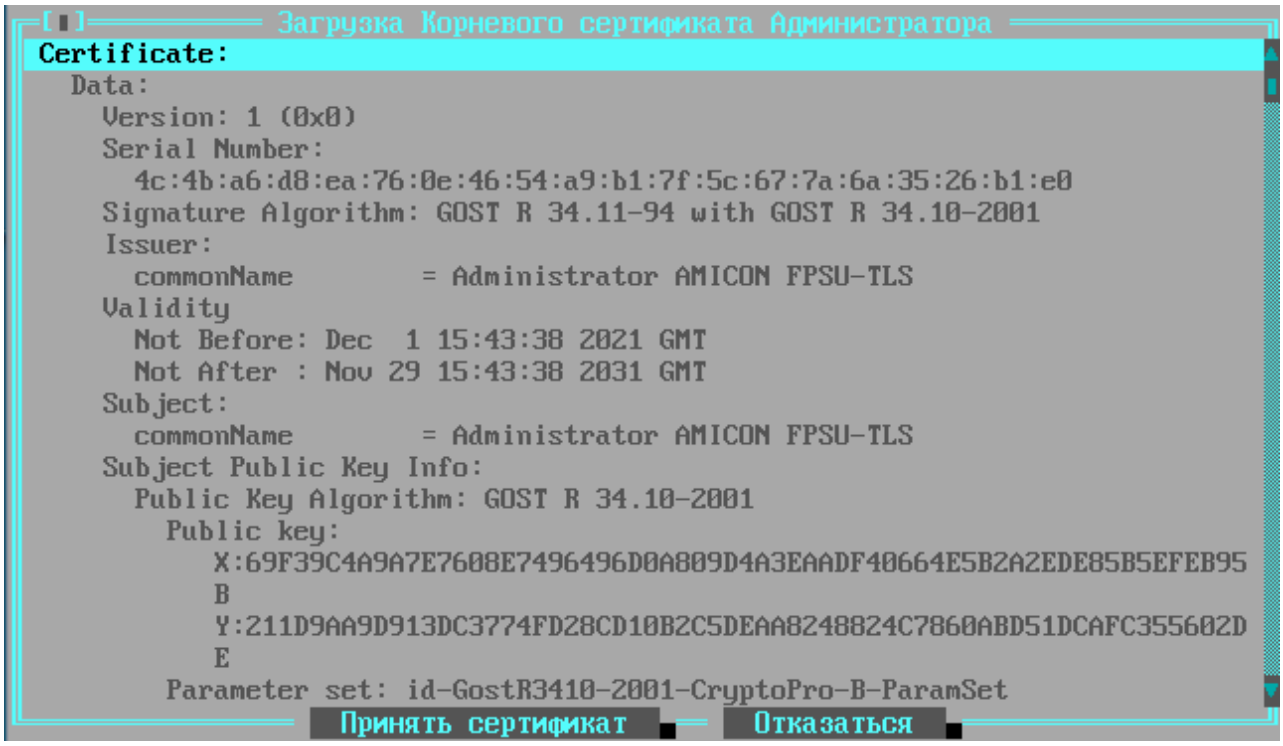

Рисунок 20 - Загрузка сертификата администратора на ФПСУ-TLS

5. 5. 3. Установка списка отозванных сертификатов

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

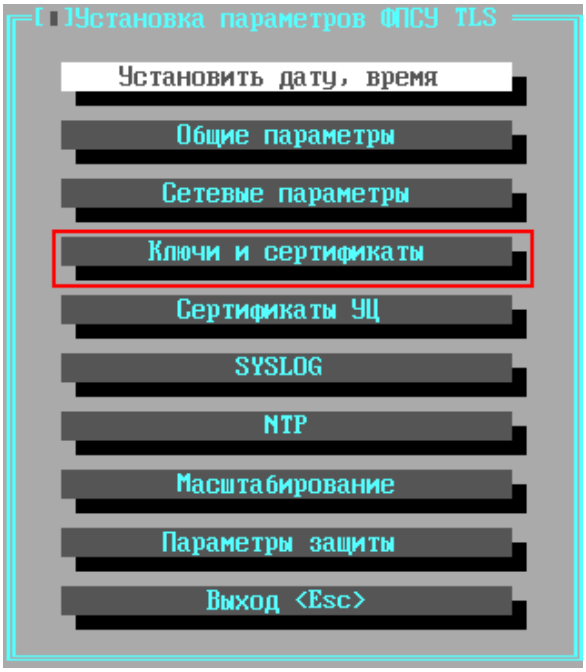

Рисунок 21 - Меню установки параметров ФПСУ-TLS

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

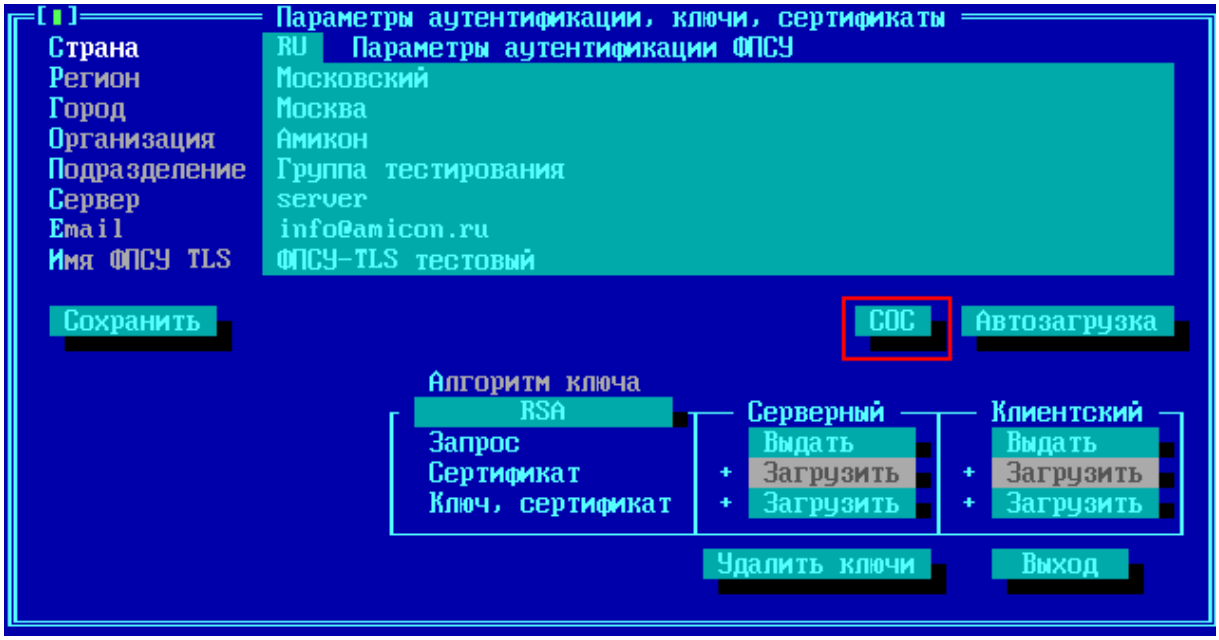

Рисунок 22 - Вызов окна списка отозванных сертификатов

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

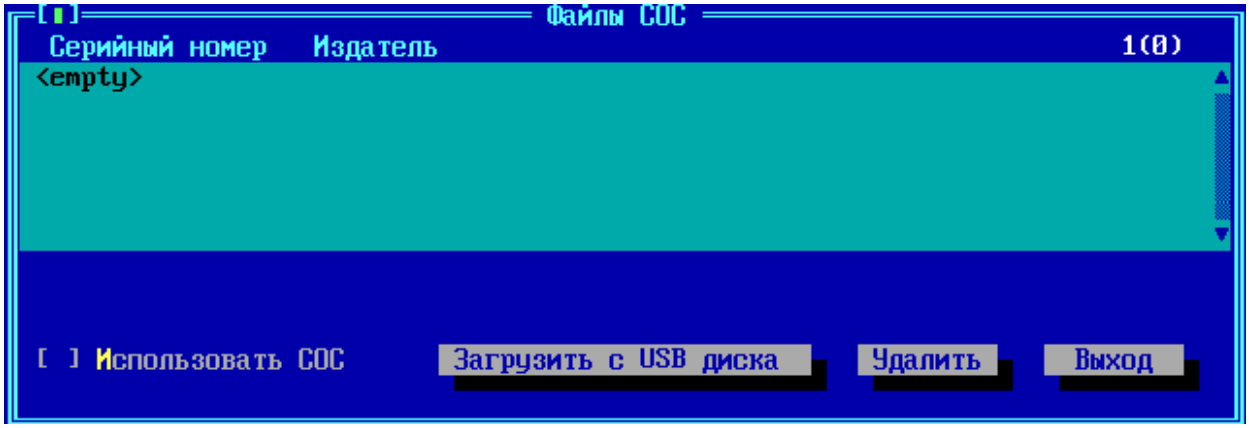

Рисунок 23 - Файлы списков отозванных сертификатов

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:

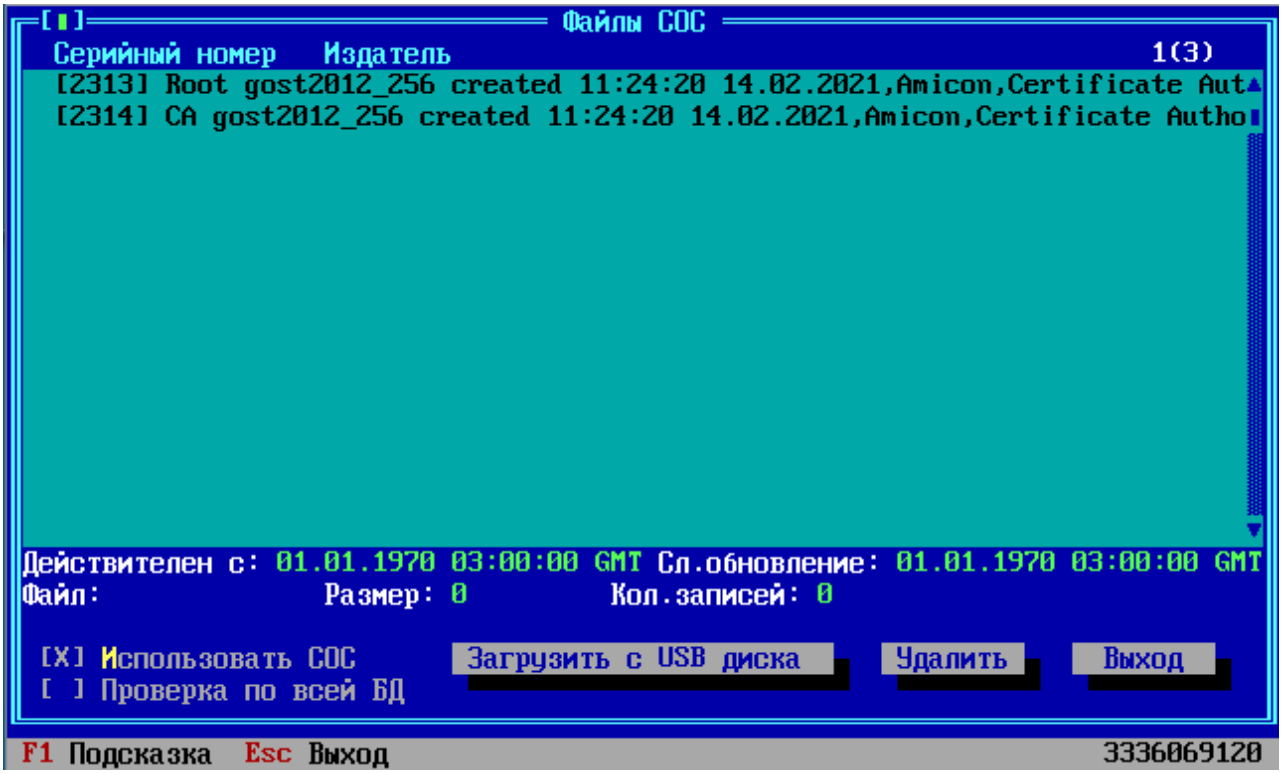

Рисунок 24 - Окно списка отозванных сертификатов

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 возврата к меню ФПСУ-TLS, нажмите кнопку ***«Выход»***.

5. 5. 4. Установка личных сертификатов ФПСУ-TLS

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

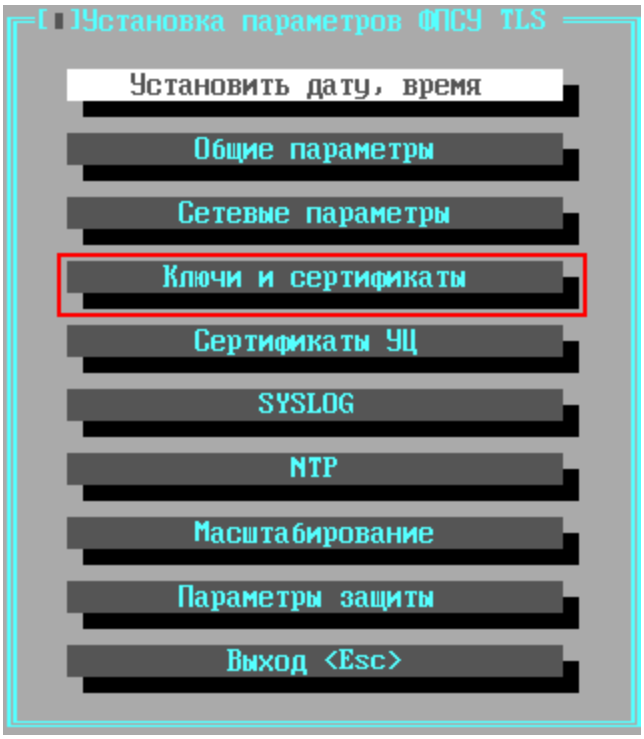

Рисунок 25 - Меню установки параметров ФПСУ-TLS

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

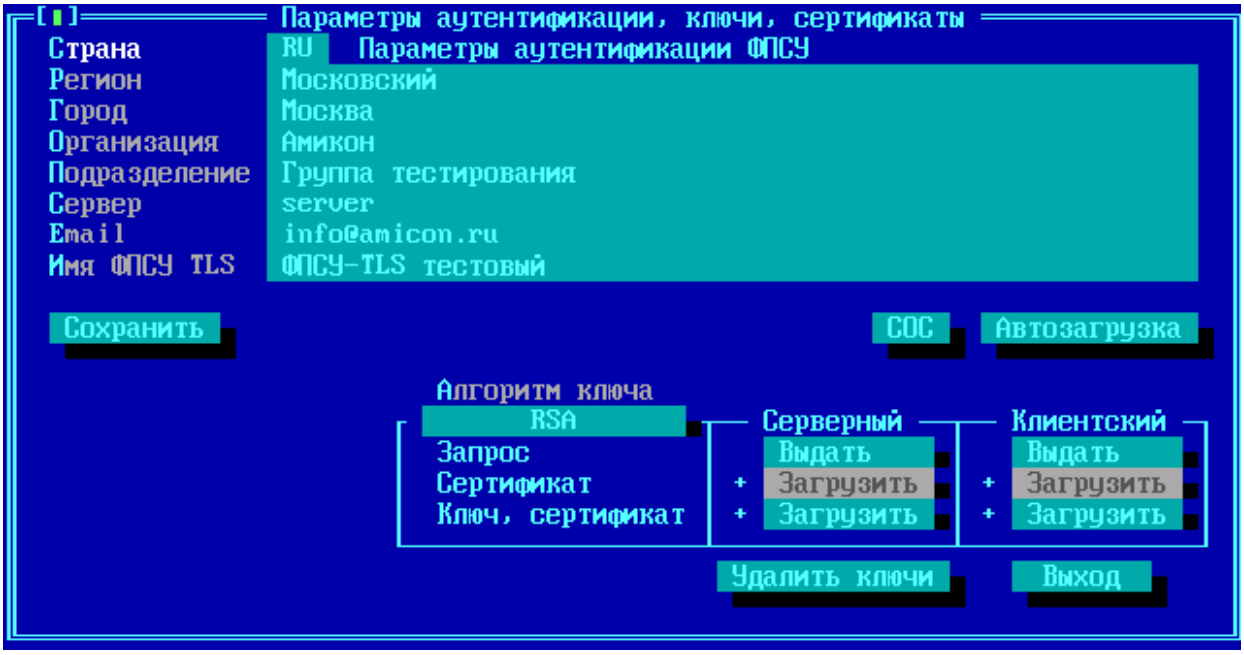

Рисунок 26 - Параметры аутентификации, ключи, сертификаты

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»;
- ***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:

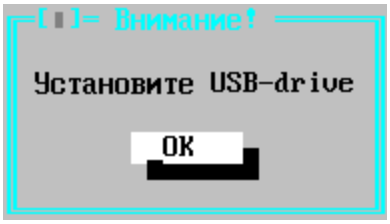

Рисунок 27

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».

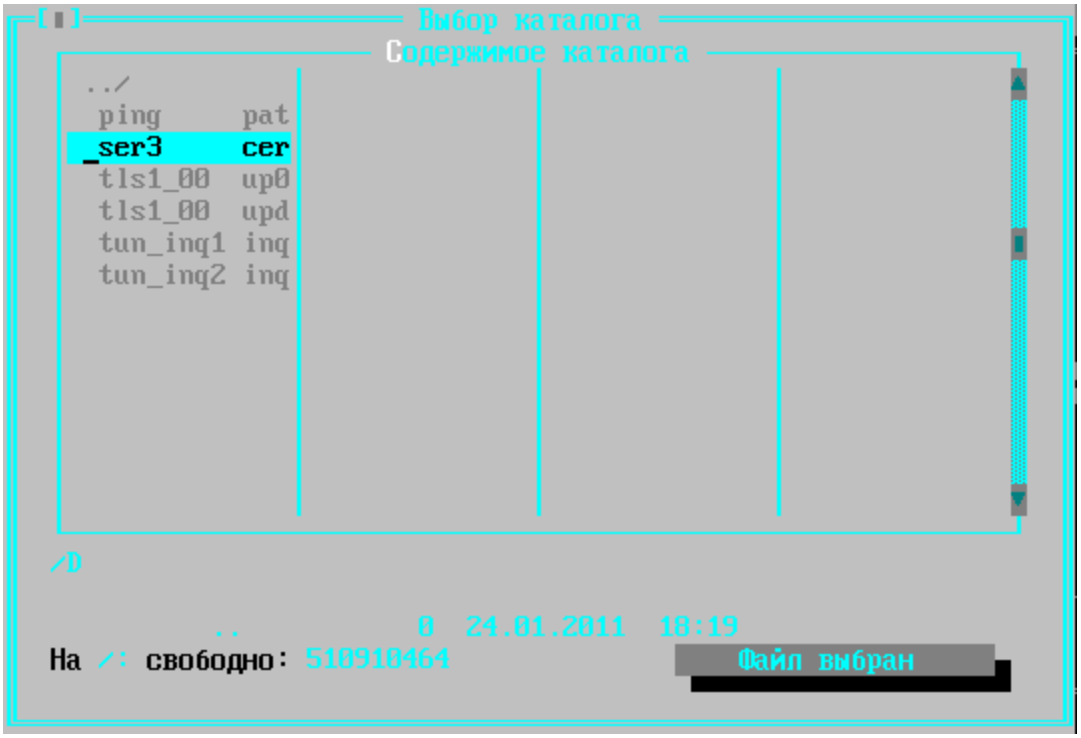

Рисунок 28 - Окно диалога выбора файла

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

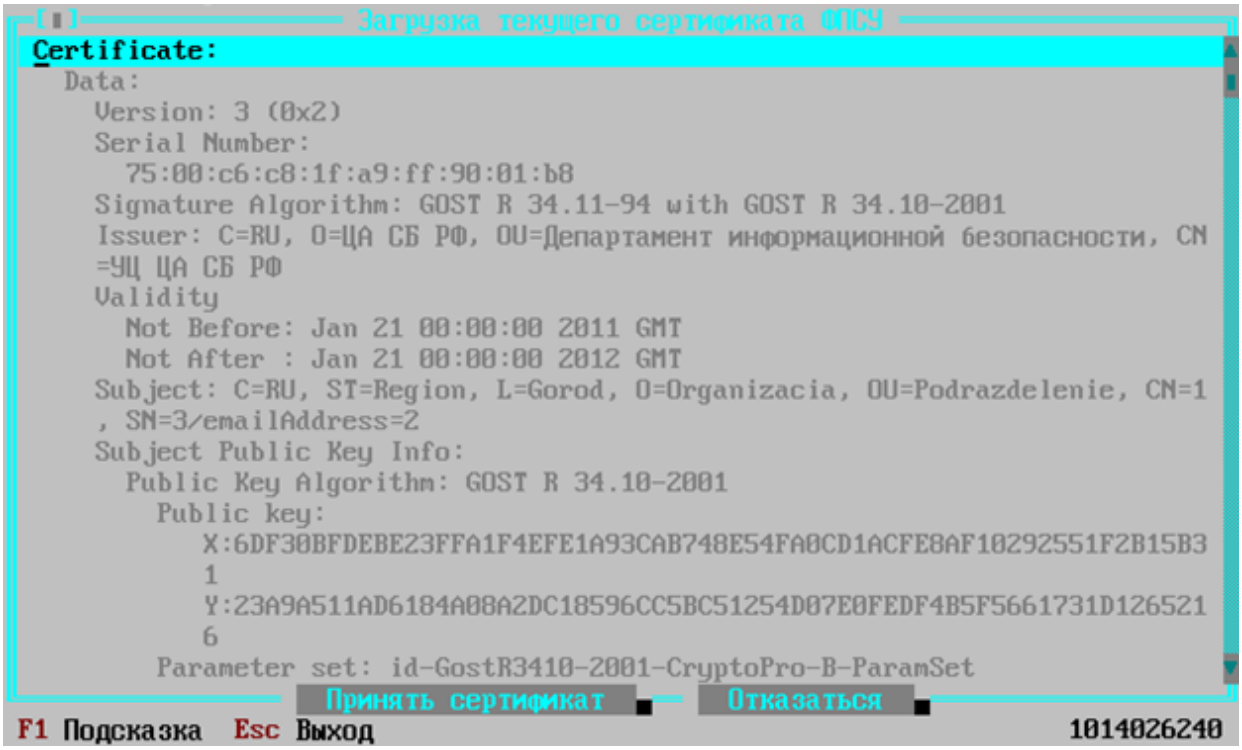

Рисунок 29 - Просмотр устанавливаемого сертификата

Поддерживаемые криптографические наборы указываются в тексте сертификата в строке, начинающейся со слов «Signature Algorithm:».

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

После принятия или отказа от сертификата будет выполнен возврат в окно управления личными сертификатами ФПСУ-TLS.

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. 5. 5. 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 «Ключи и Сертификаты» меню установки параметров ФПСУ-TLS:

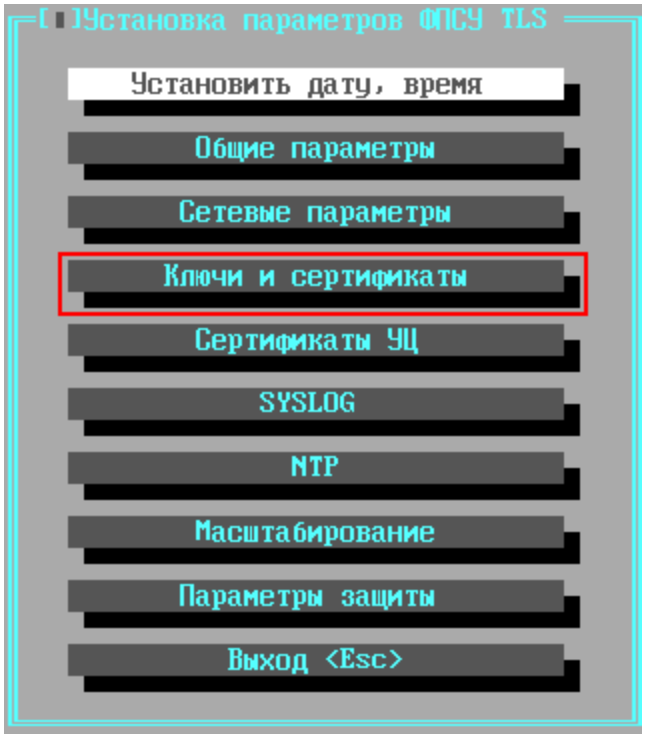

Рисунок 30 - Меню установки параметров ФПСУ-TLS

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

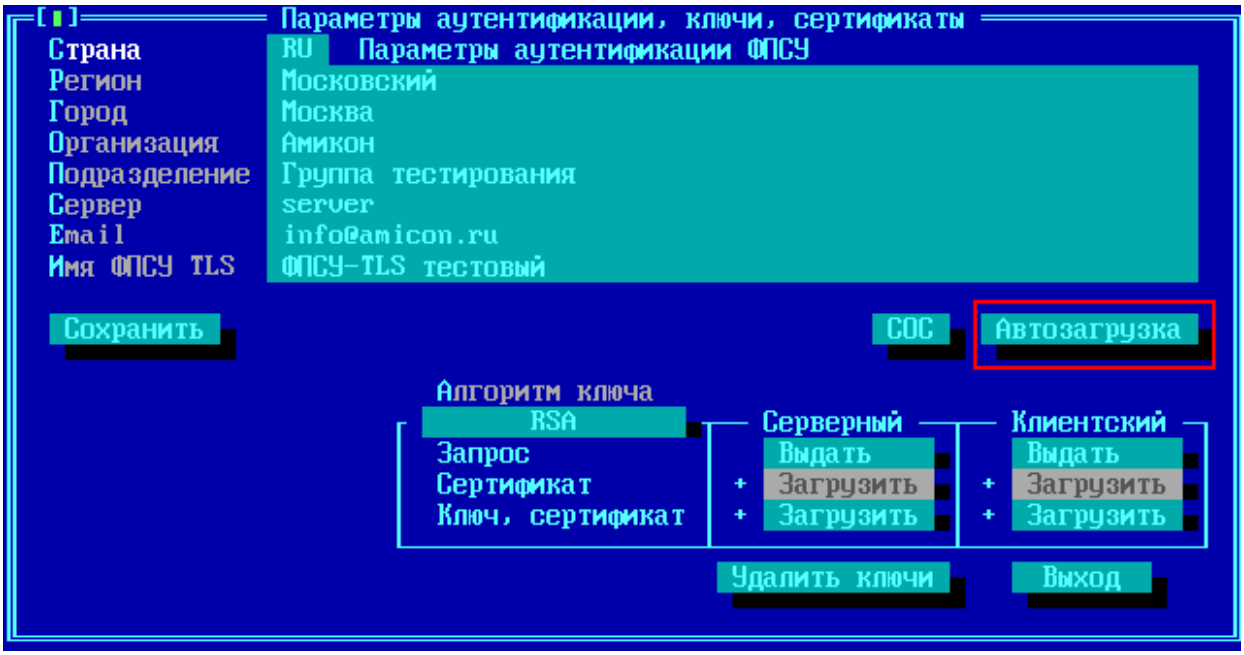

Рисунок 31 - Вызов окна автозагрузки сертификатов

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.

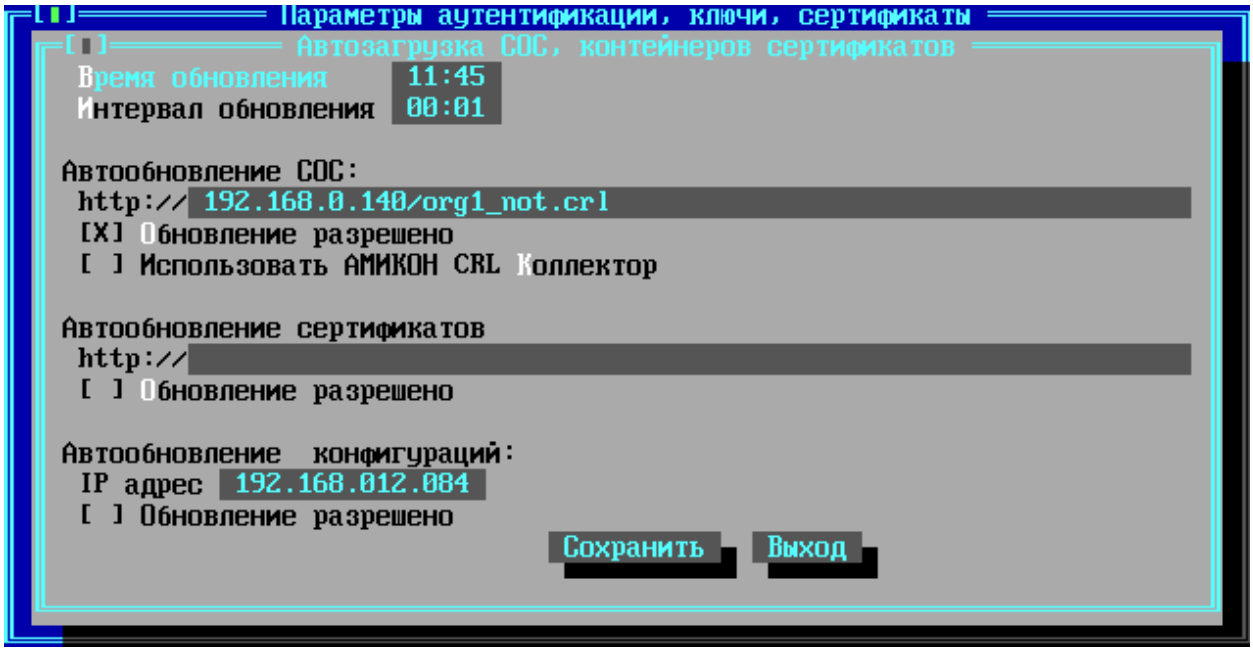

Рисунок 32 - Окно управления автоматической загрузкой

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. 6. 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» основного меню ФПСУ-TLS:

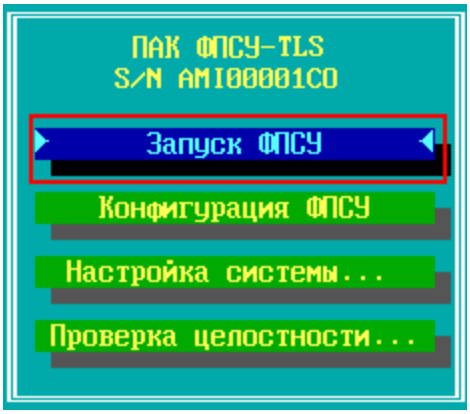

Рисунок 33 - Перевод в рабочий режим

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,
- SYSLOG и SNMP,
- Дата и время ФПСУ-TLS,
- Просмотр установленных сертификатов.

6. Эксплуатация ФПСУ-TLS

Минимальные обязательные настройки ФПСУ-TLS, позволяющие выполнять основные функции по защите http-трафика к web-серверам локальной сети, описаны в пункте Первоначальная настройка и запуск 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+F4> - экран текущего состояния ФПСУ-TLS рабочего режима.

6. 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.

6. 1. 1. Экран текущего состояния ФПСУ-TLS

По умолчанию, на экран выдается информативное окно текущего состояния ФПСУ-TLS, открывается по нажатию клавиш <Alt+F4>:

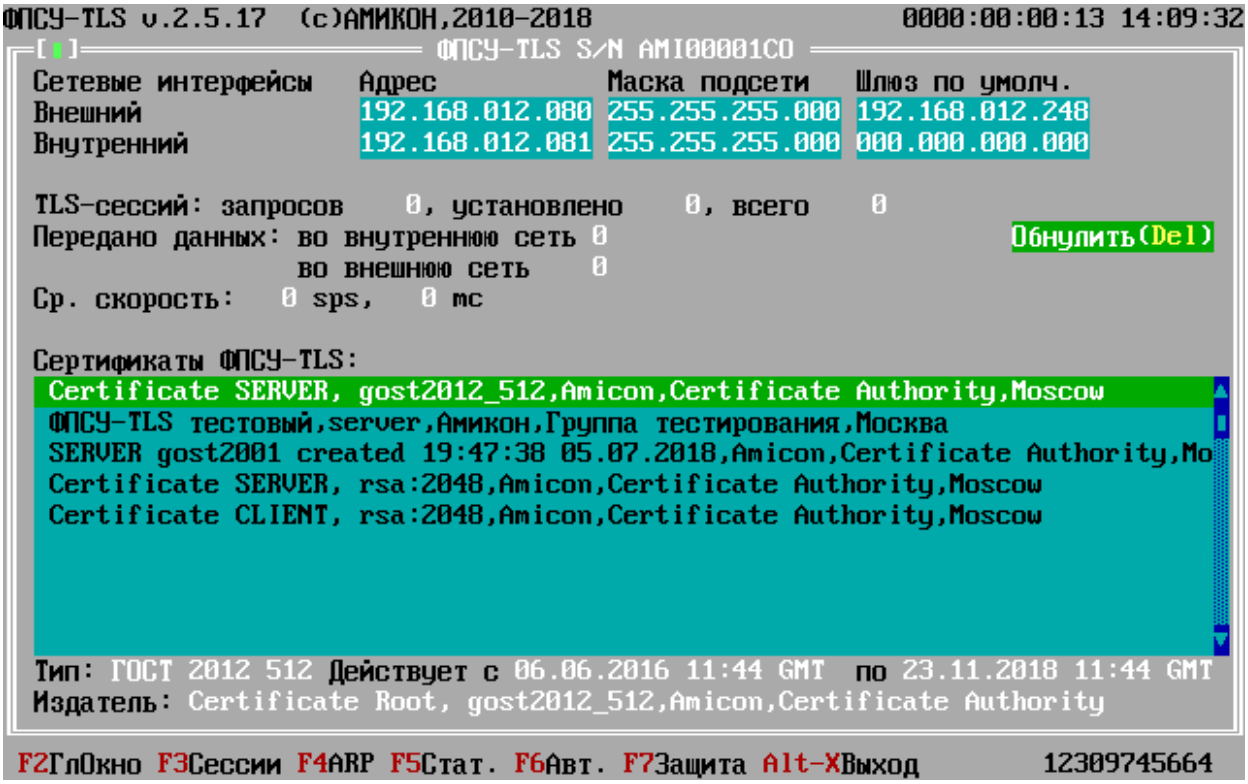

Рисунок 34 - Окно текущего состояния ФПСУ-TLS

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.

6. 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>:

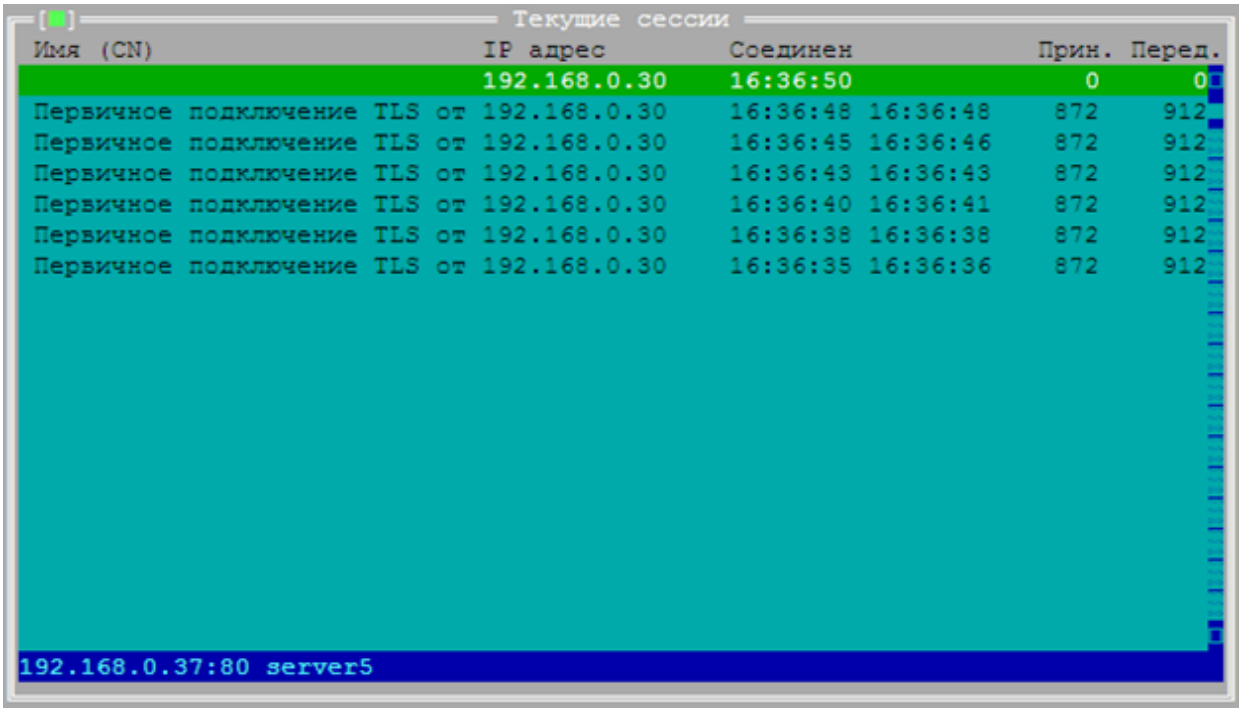

Рисунок 35 -Окно текущих сессий TLS-клиентов

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.

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.

6. 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.

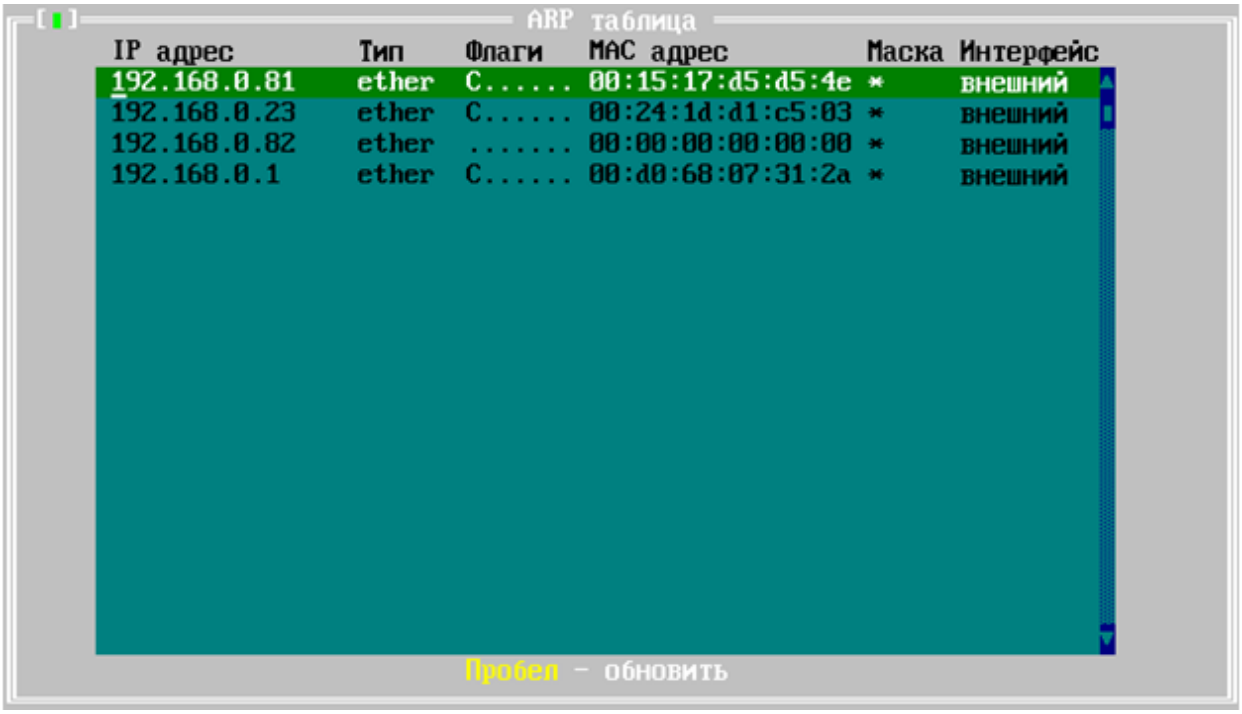

Рисунок 36 -ARP таблица

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

6. 1. 4. Просмотр статистики

При нажатии клавиши <F5>, ФПСУ-TLS перейдёт в окно установки условий поиска накопленной регистрационной информации.

Для получения необходимых данных сначала отметьте нужный тип, выделив курсором соответствующую строку, и нажмите <Пробел>. При этом строка будет отмечена слева знаком «v», 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.

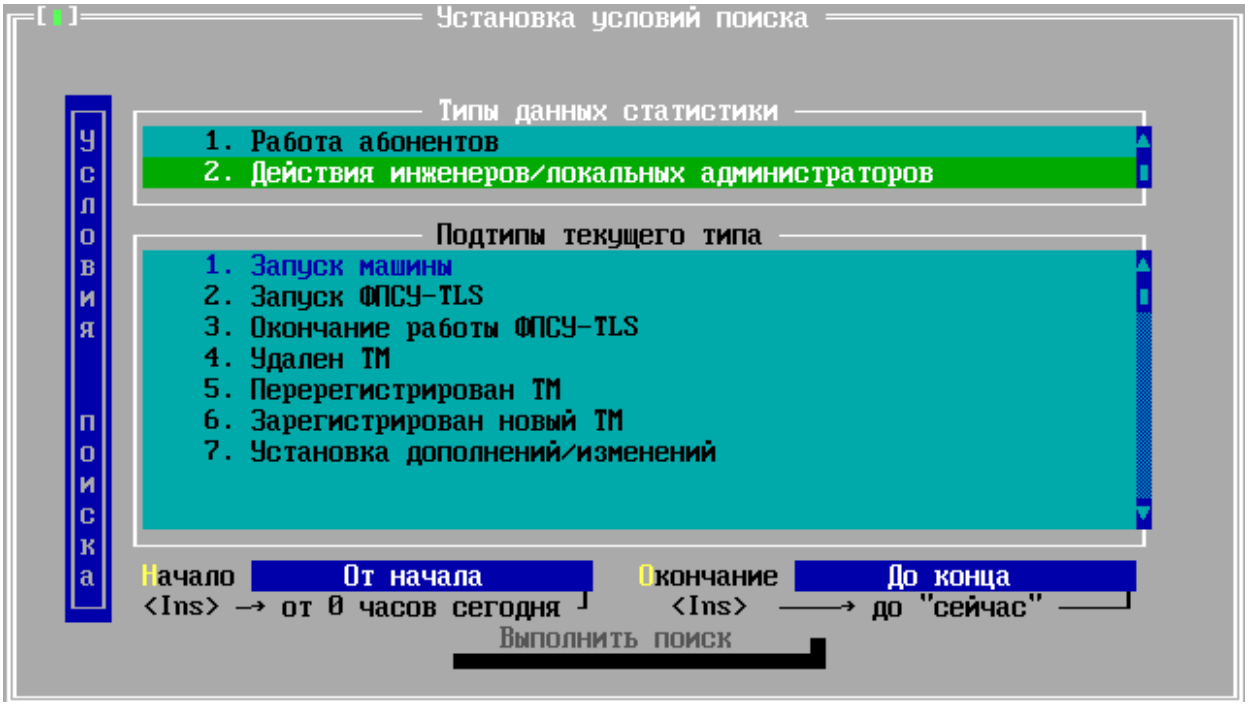

Рисунок 37 -Окно поиска статистики

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>.

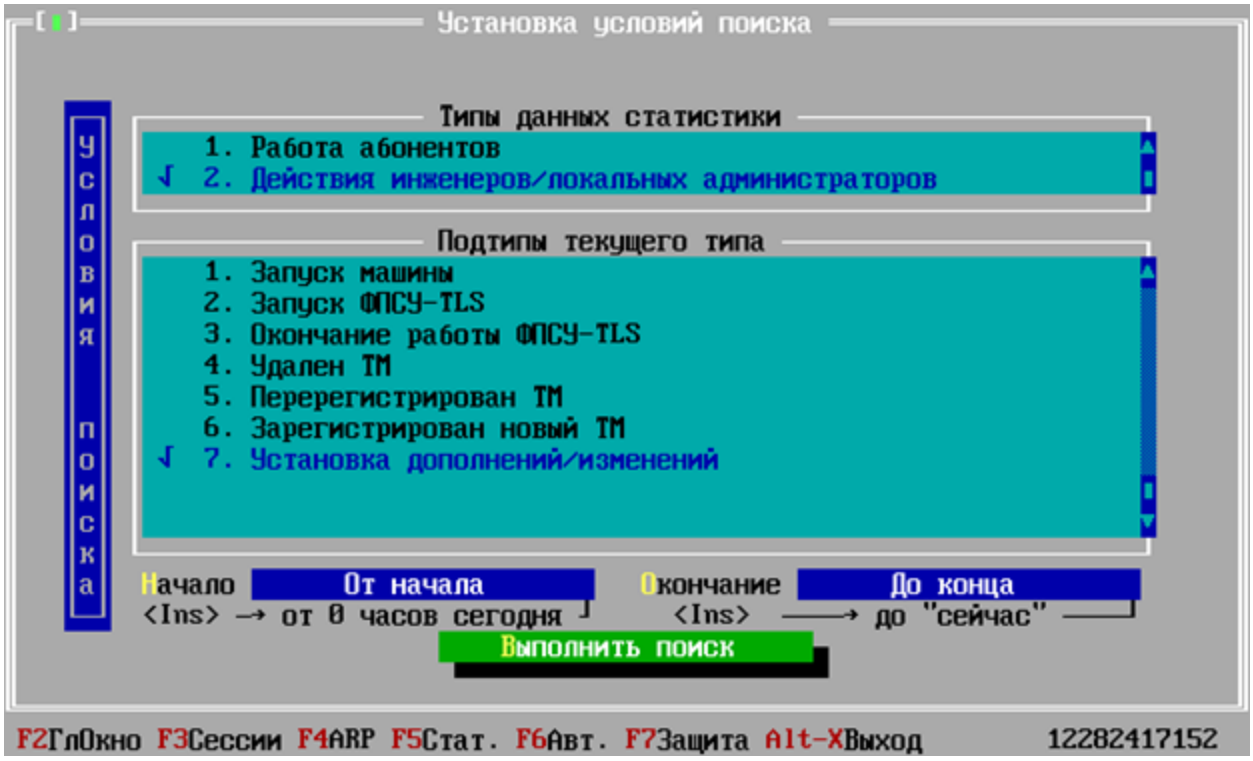

Рисунок 38 -Выбор выводимых данных статистики

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.

6. 1. 5. 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:

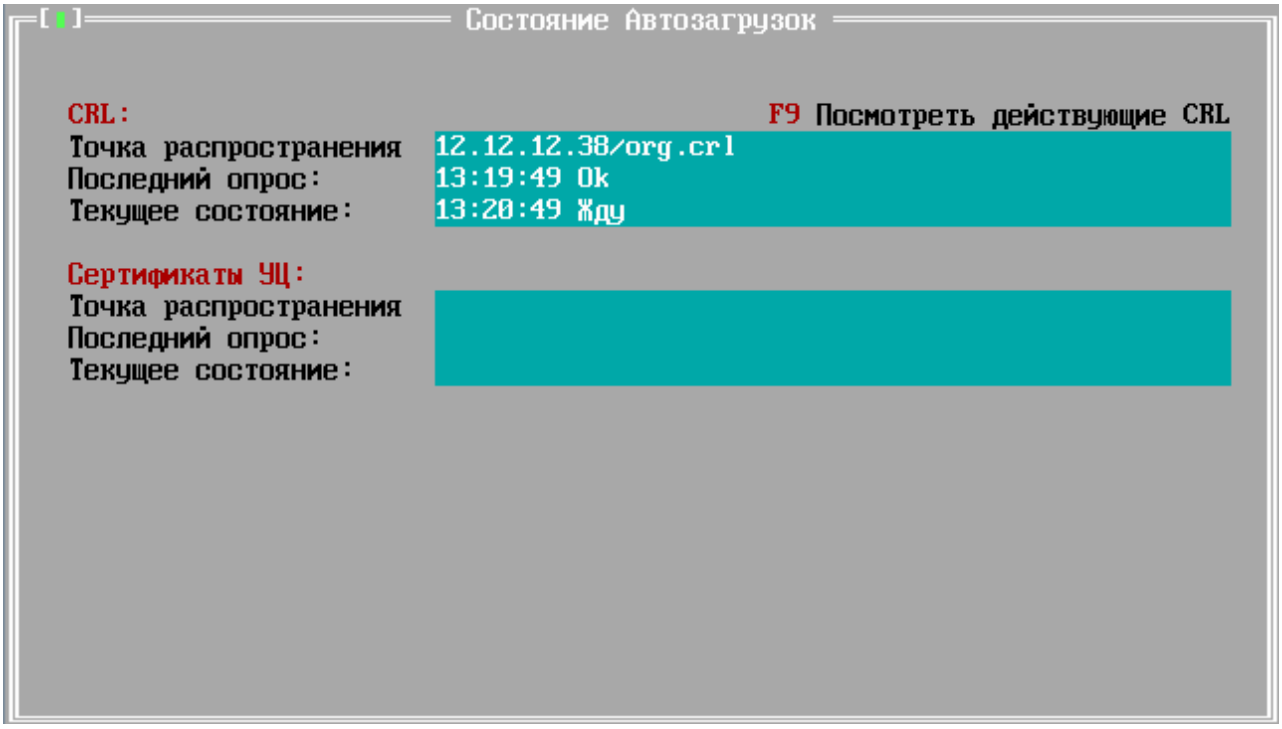

Рисунок 39 - Окно состояния автоматических загрузок сертификатов

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>.

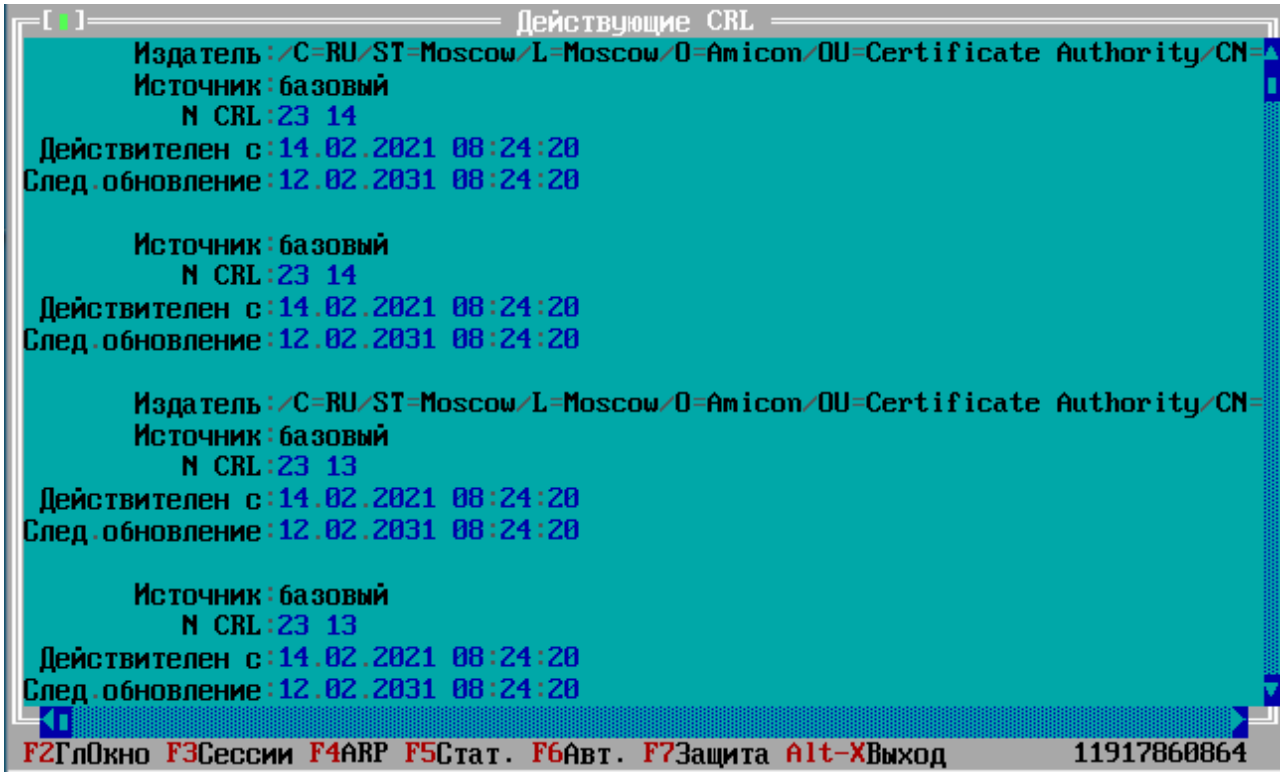

Рисунок 40 - Просмотр действующих CRL

6. 1. 6. 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. Список по умолчанию пустой. Если в него попадают IP-адреса, то указывается следующие данные для соединений с заблокированного IP-адреса:

- IP-адрес заблокированного хоста;
- Тип соединения (если определен), исходящий с заблокированного хоста;
- Время блокировки;
- количество заблокированных данных;
- количество заблокированных пакетов.

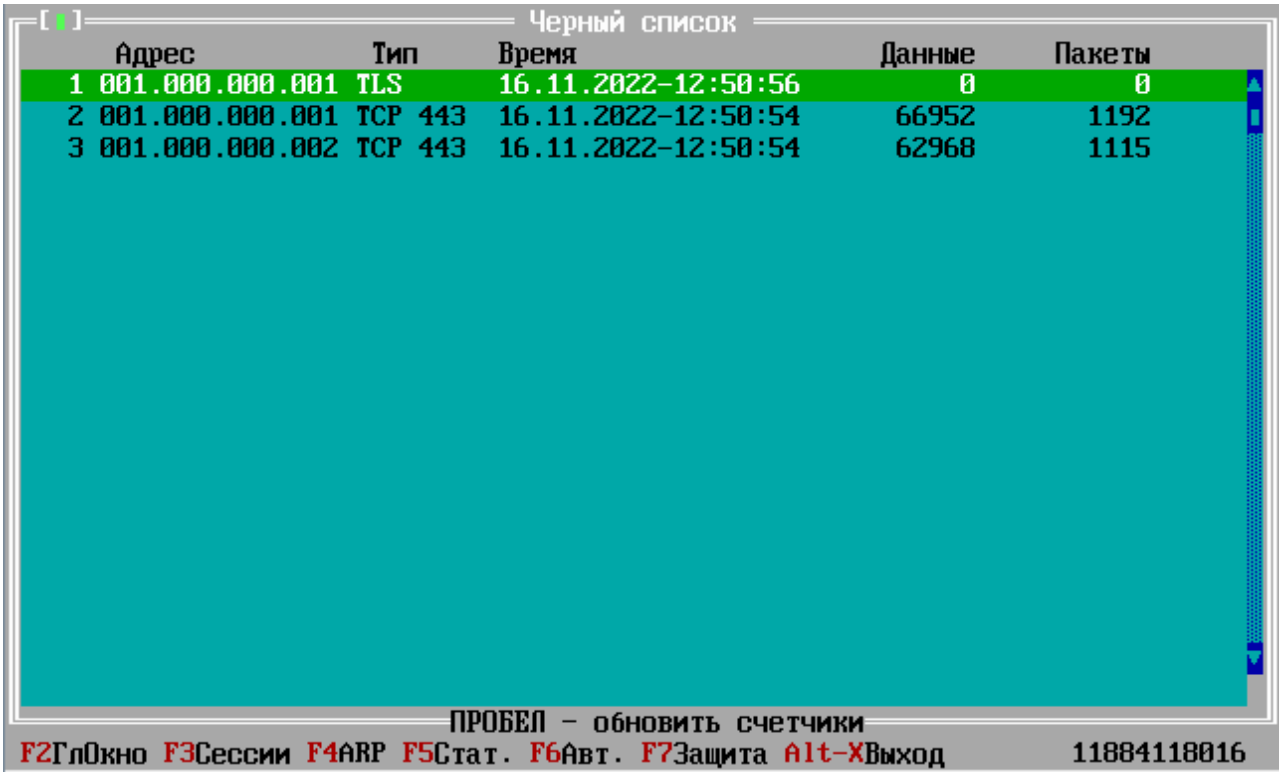

Рисунок 41 - Список IP адресов, соединение которых с ФПСУ-TLS блокируется

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

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

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.

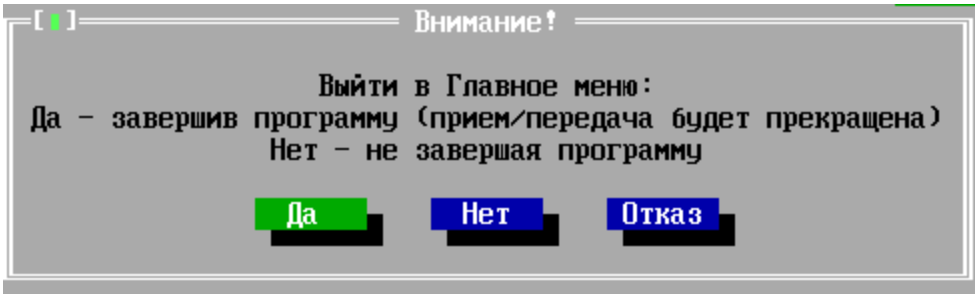

Рисунок 42 - Выбор выхода из рабочего режима

6. 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.

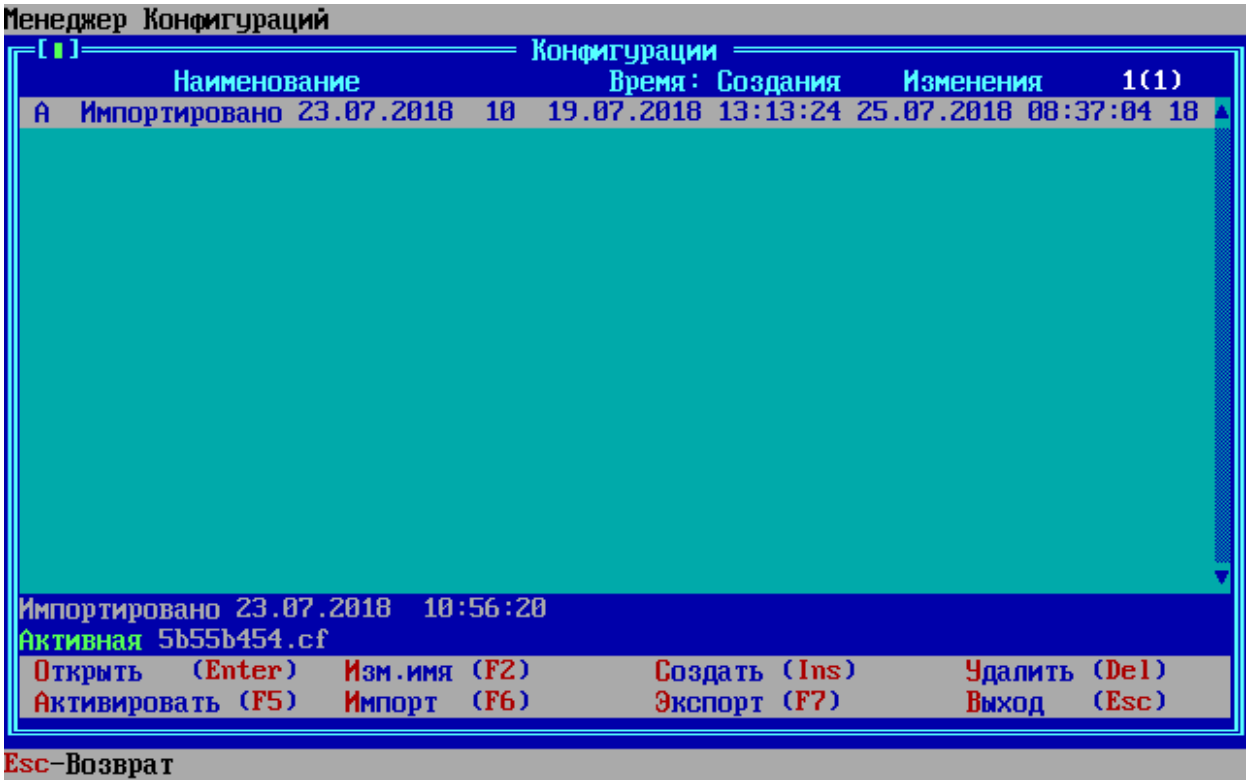

Рисунок 43 - Окно менеджера конфигураций

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

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:

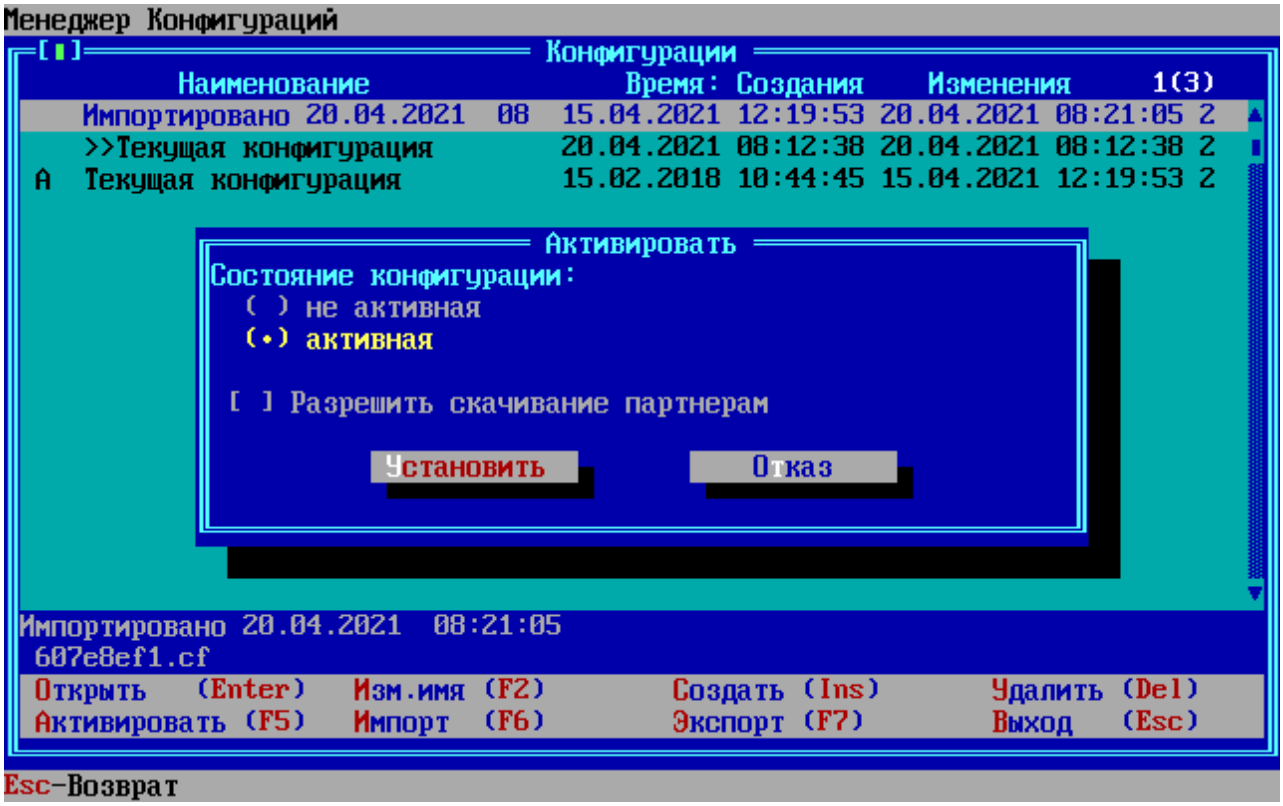

Рисунок 44 - Окно активации конфигурации

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 (подробнее см. «Управление сертификатами администраторов ФПСУ-TLS»). В статус конфигурации добавится символ ***«S»*** - ФПСУ-TLS становится сервером, с которого партнерами скачивается данная конфигурация.

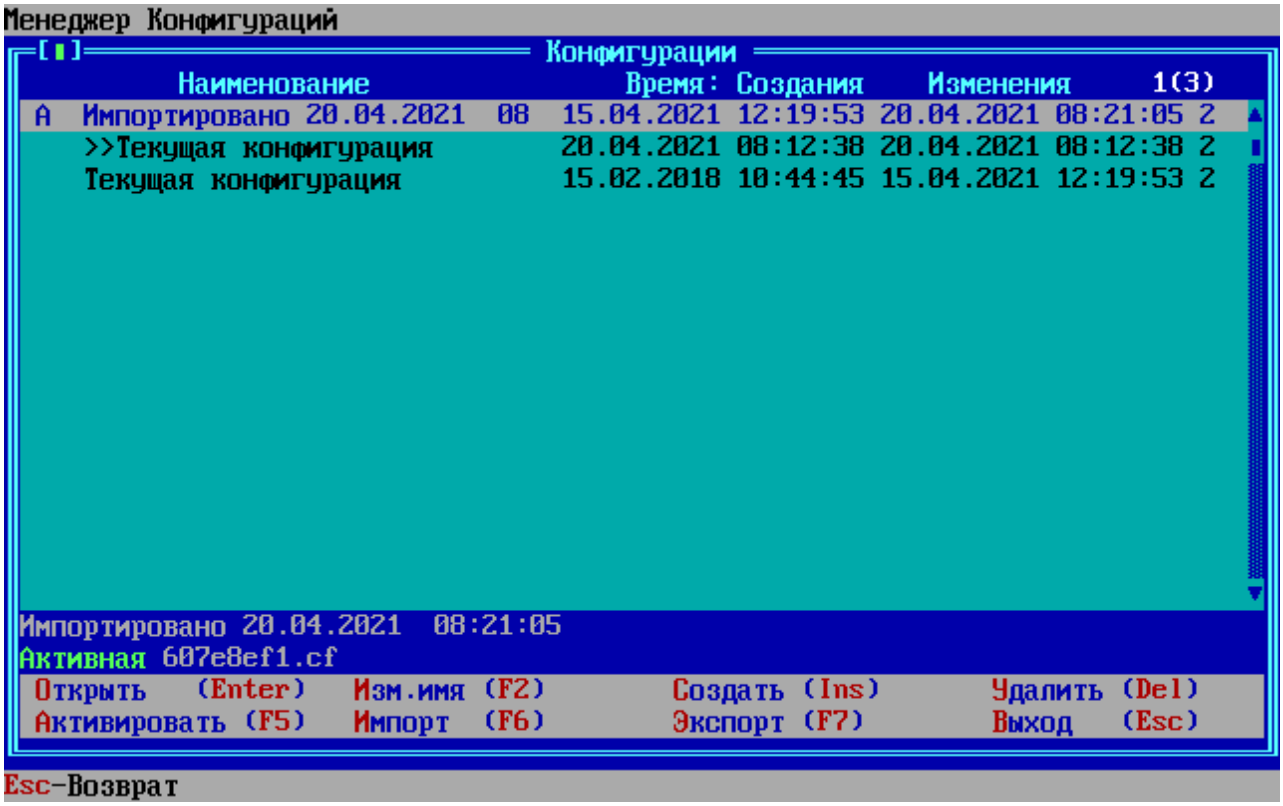

Рисунок 45 - Рабочая конфигурация

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>.

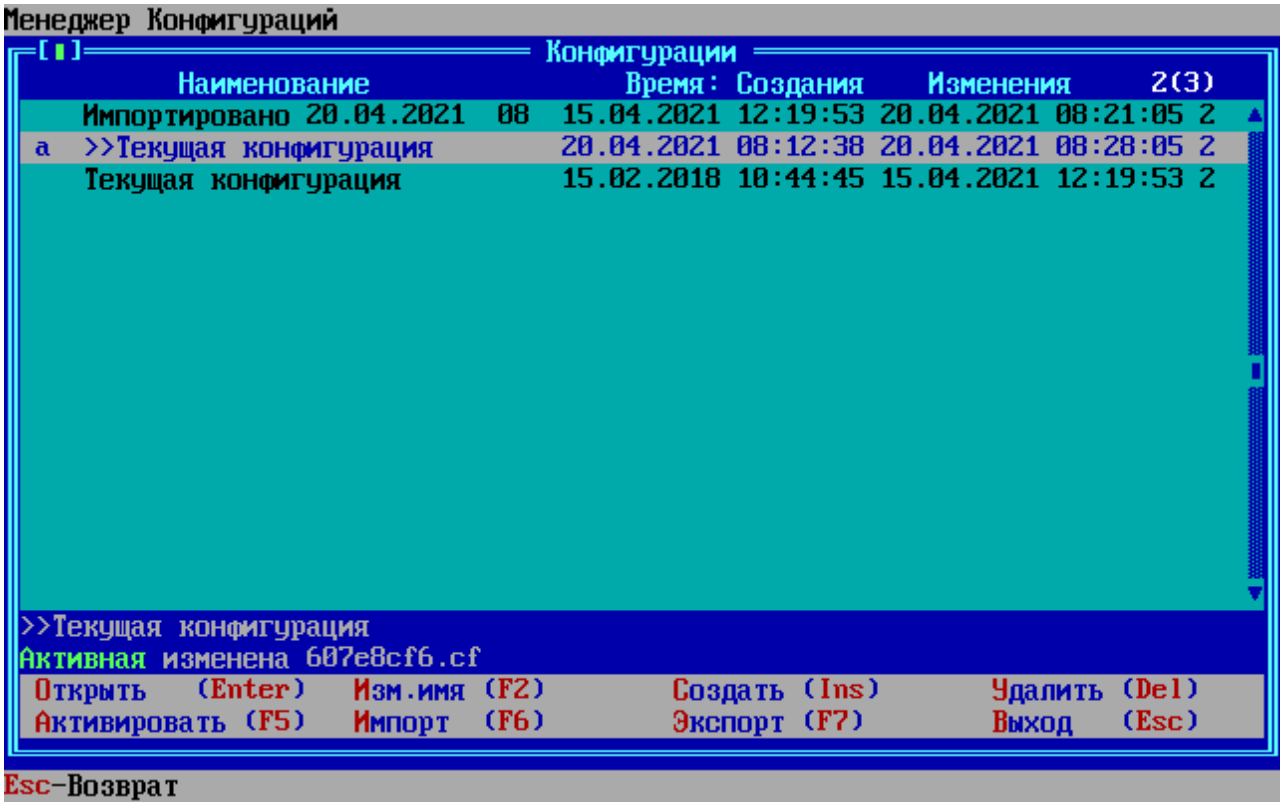

Рисунок 46 - Рабочая конфигурация с внесенными изменениями

Экспорт конфигурации

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

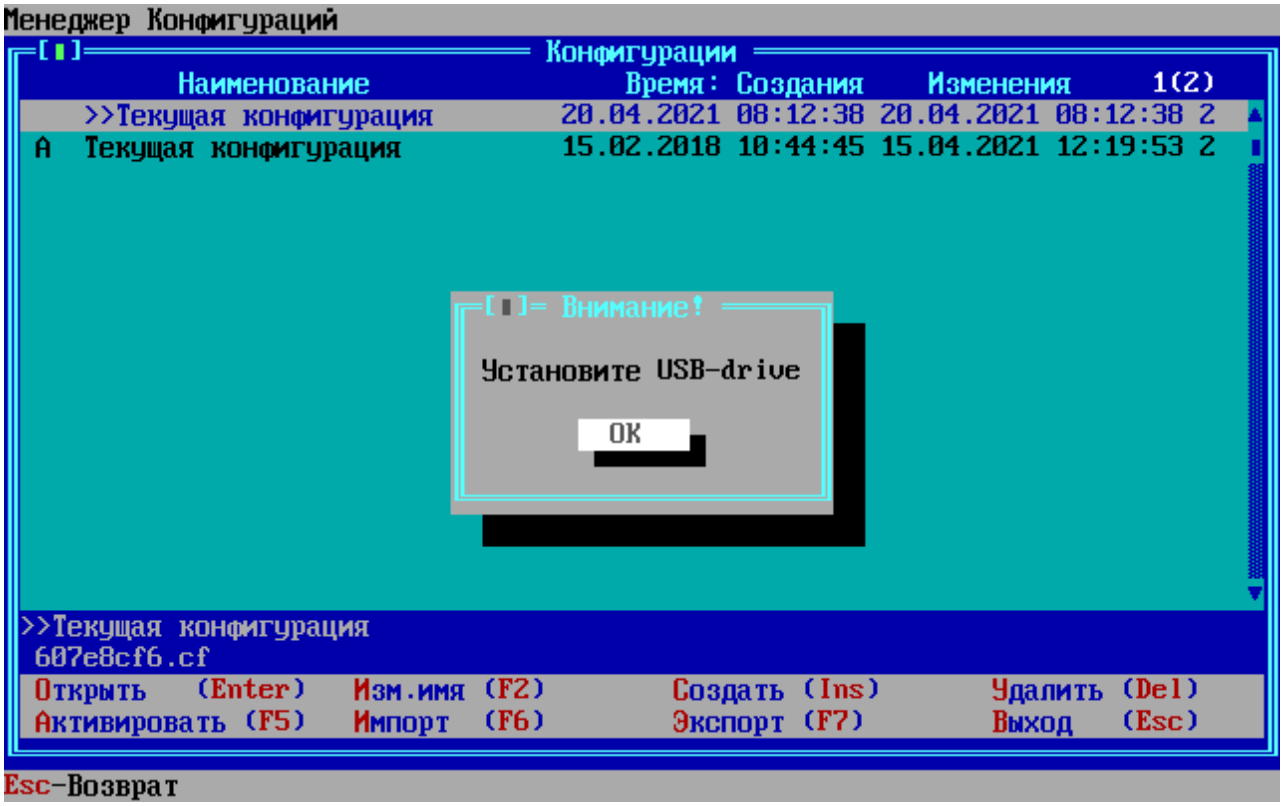

Рисунок 47 - Носитель для экспорта конфигурации

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

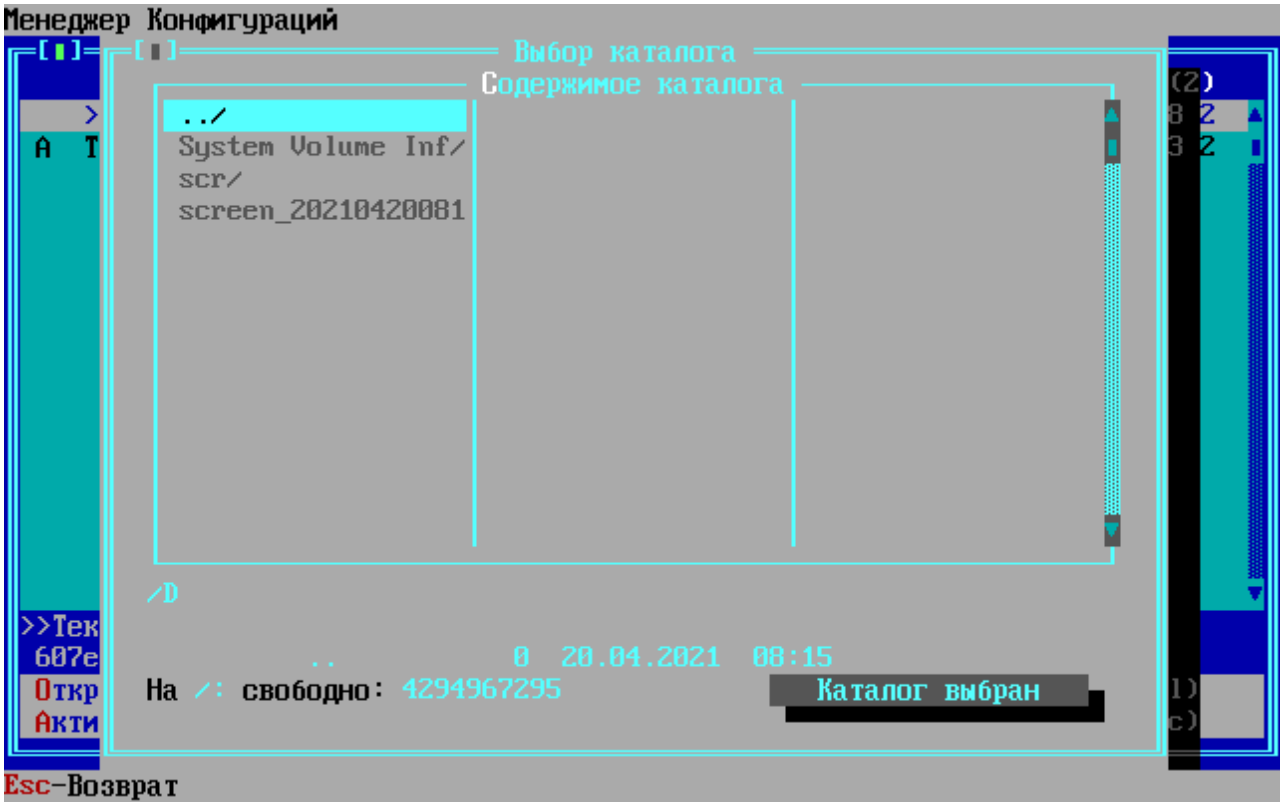

Рисунок 48 - Выбор каталога для экспорта

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

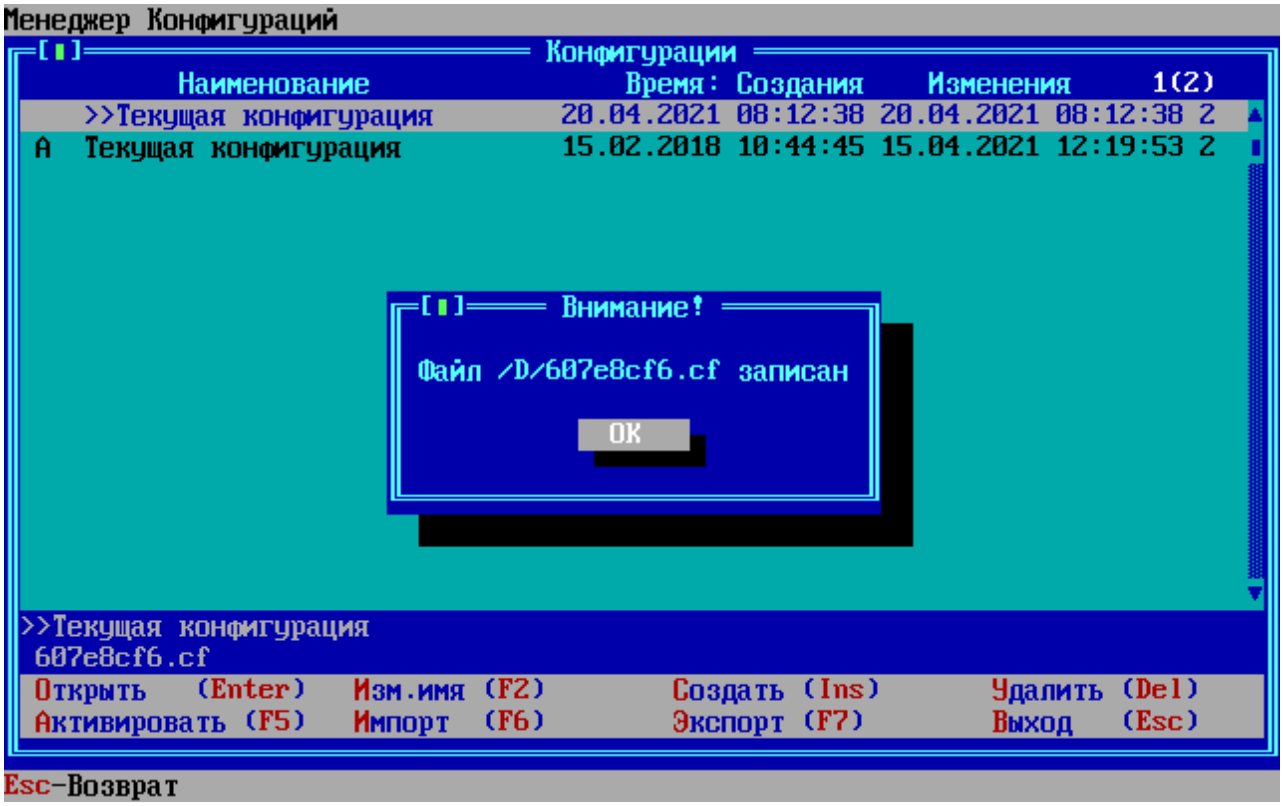

Рисунок 49 - Экспорт конфигурации в файл

Импорт конфигурации

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

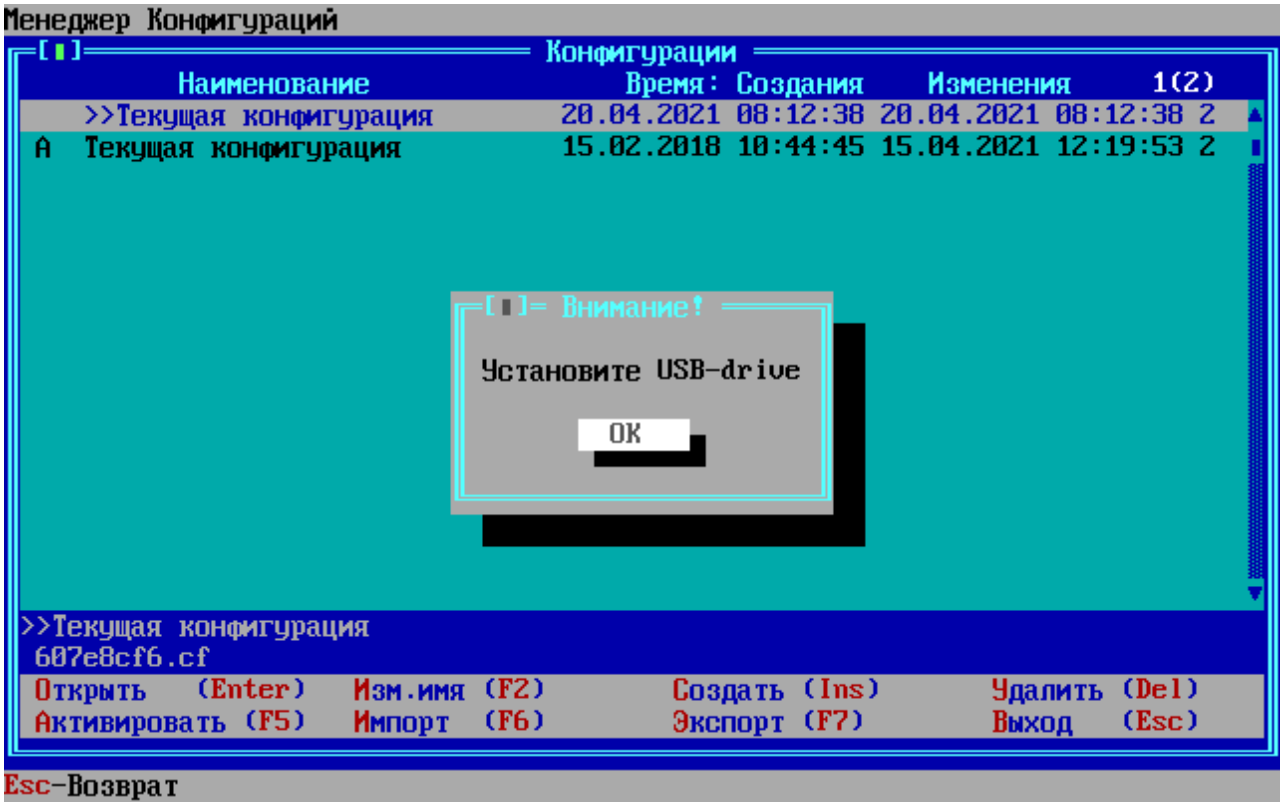

Рисунок 50 Носитель с конфигурацией

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

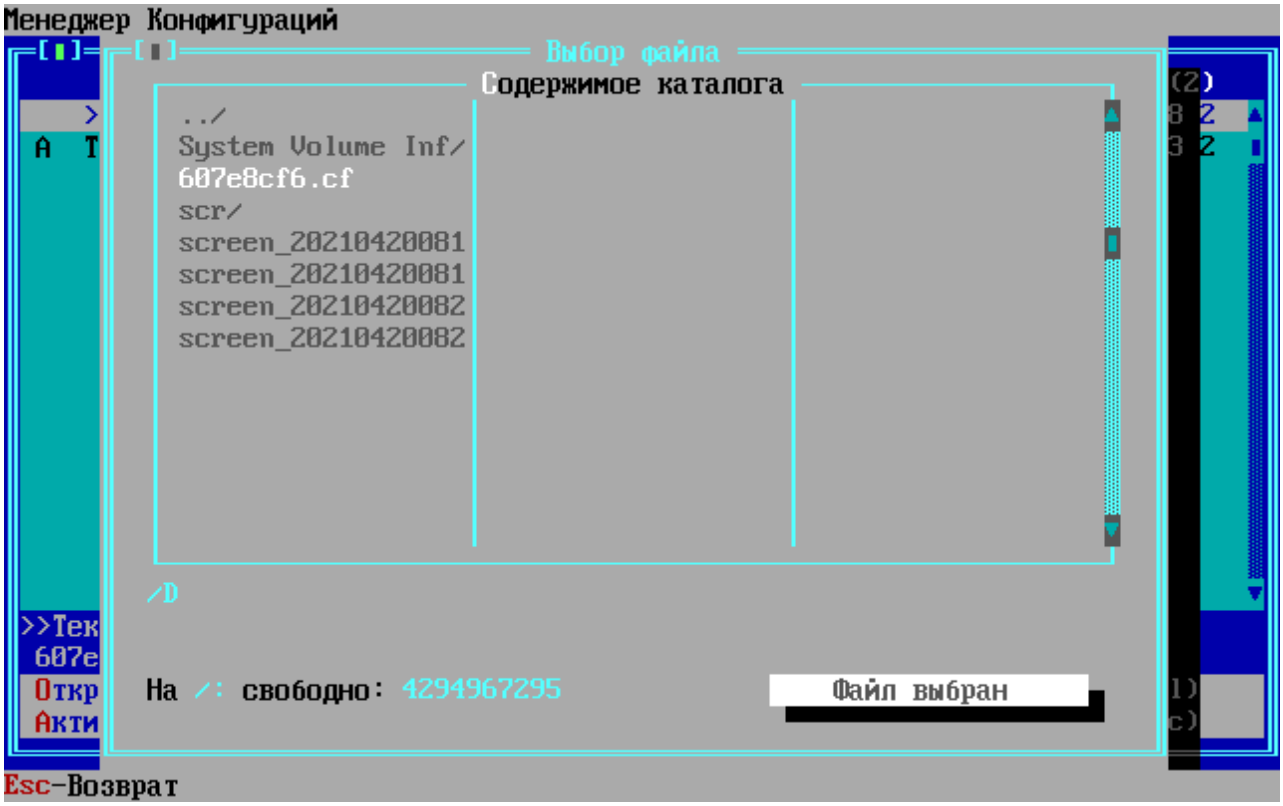

Рисунок 51 - Выбор файла для импорта

Конфигурация получит наименование «Импортировано» с датой изменения.

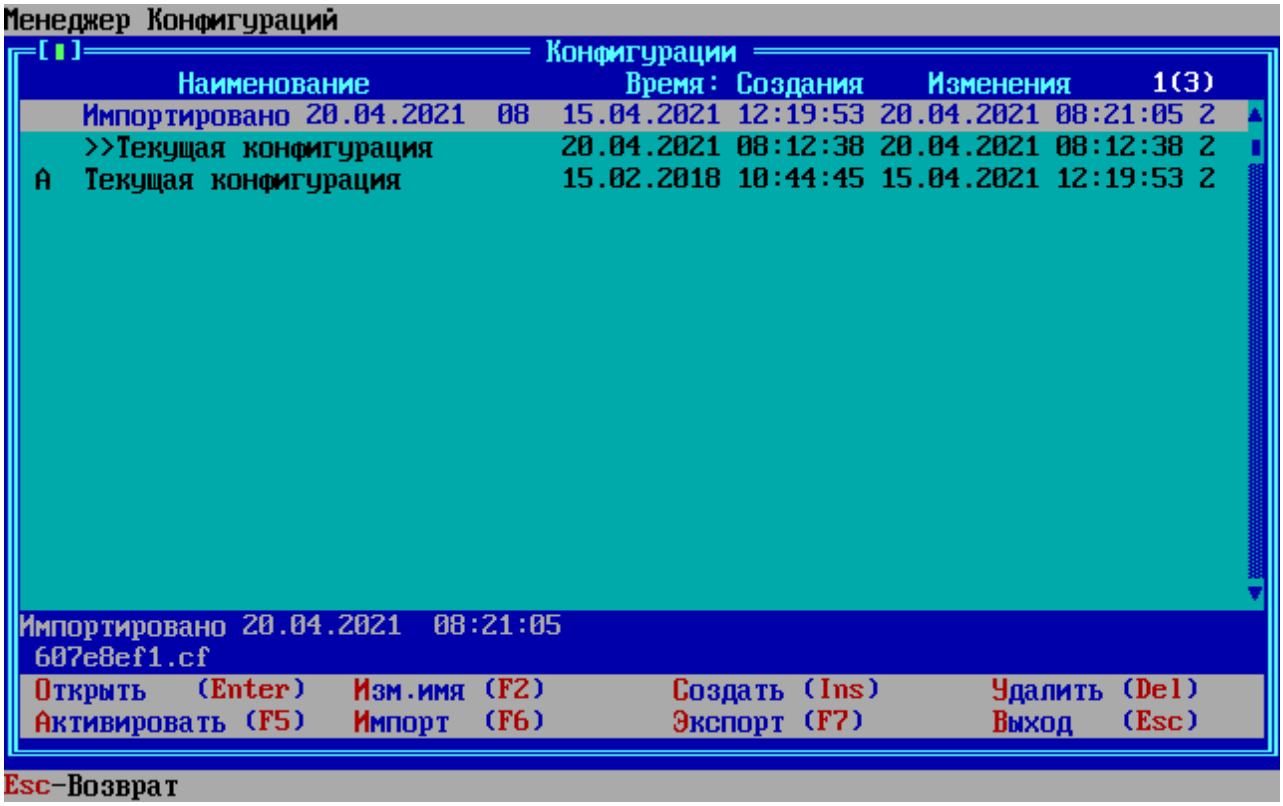

Рисунок 52 - Импортированная конфигурация

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.

6. 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 инициализирующим соединение клиентом, а добавляемый сервер – в роли TLS-сервера.

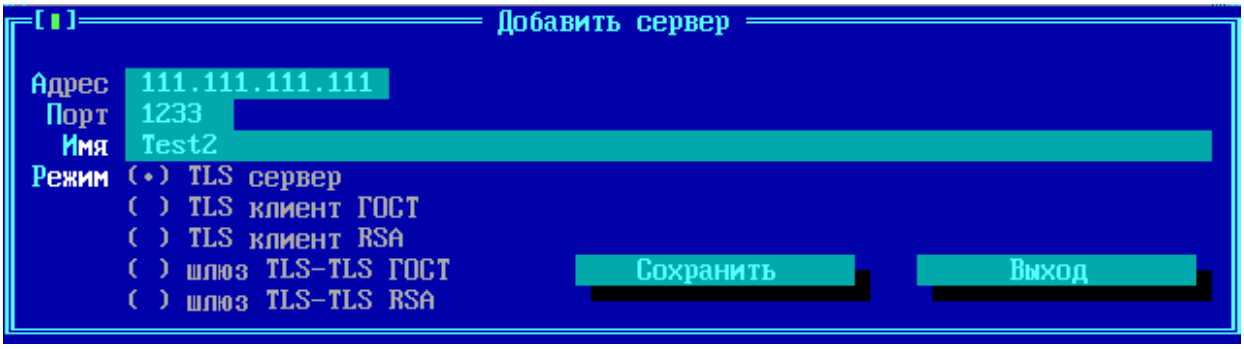

Рисунок 53 - Параметры соединения с защищаемым сервером

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 к Веб-Сервису:

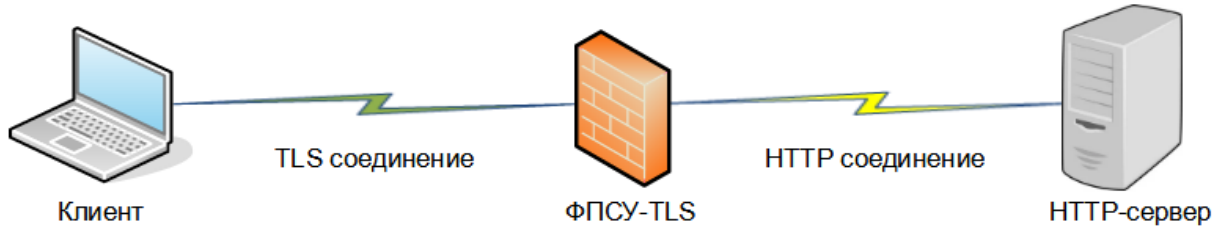

Рисунок 54 - Режим работы по умолчанию, «TLS-сервер»

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).

Режим «TLS-клиент»

Опции «TLS-клиент ГОСТ» и «TLS-клиент RSA» используют одну и ту же схему работы, отличаясь только используемым в TLS соединении криптографическим протоколом. Эти режимы работы предполагают незащищенное http-соединение с ФПСУ-TLS от клиента из внешней сети, и защищенное TLS-соединение с защищаемым сервером:

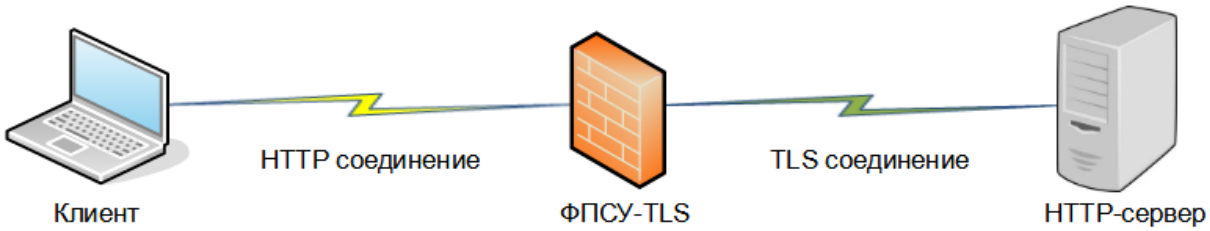

Рисунок 55 - Режимы работы «TLS-клиент»

Такая схема может быть использована, когда подключающийся с внешнего порта клиент не имеет возможности использовать TLS-протокол, или находящаяся на внешнем порту сеть передачи данных считается доверенной.

Для организации соединения ФПСУ-TLS с защищаемым сервером потребуются установленный на ФПСУ-TLS клиентский личный сертификат, а на защищаемый сервер – серверный личный сертификат, выданные УЦ. Корневые сертификаты таких УЦ должны быть установлены на ФПСУ-TLS и на защищаемый сервер.

Режим «шлюз TLS-TLS»

Опции «шлюз TLS ГОСТ» и «шлюз TLS RSA» используют одну и ту же схему работы, отличаясь только используемым в TLS соединении криптографическим протоколом. Эти режимы работы предполагают защищенное TLS-соединение с ФПСУ-TLS от клиента из внешней сети, и защищенное TLS-соединение с защищаемым сервером:

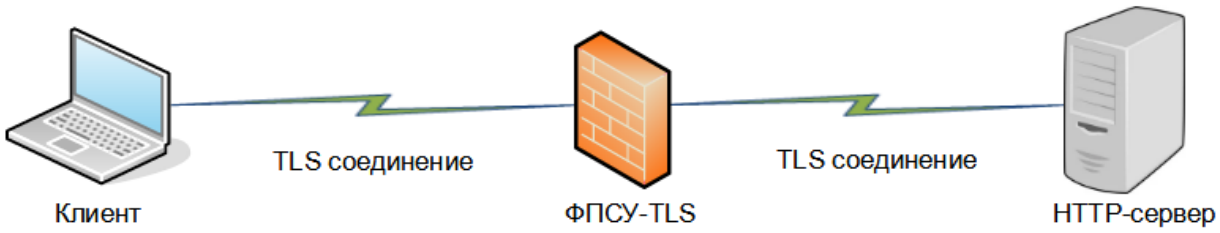

Рисунок 56 - Режимы работы «TLS-шлюз»

Для организации соединения ФПСУ-TLS с защищаемым сервером потребуются установленный на ФПСУ-TLS клиентский личный сертификат, а на защищаемый сервер – серверный личный сертификат, выданные УЦ. Корневые сертификаты таких УЦ должны быть установлены на ФПСУ-TLS и на защищаемый сервер.

6. 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).

6. 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 Source Hash Scheduling. 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.

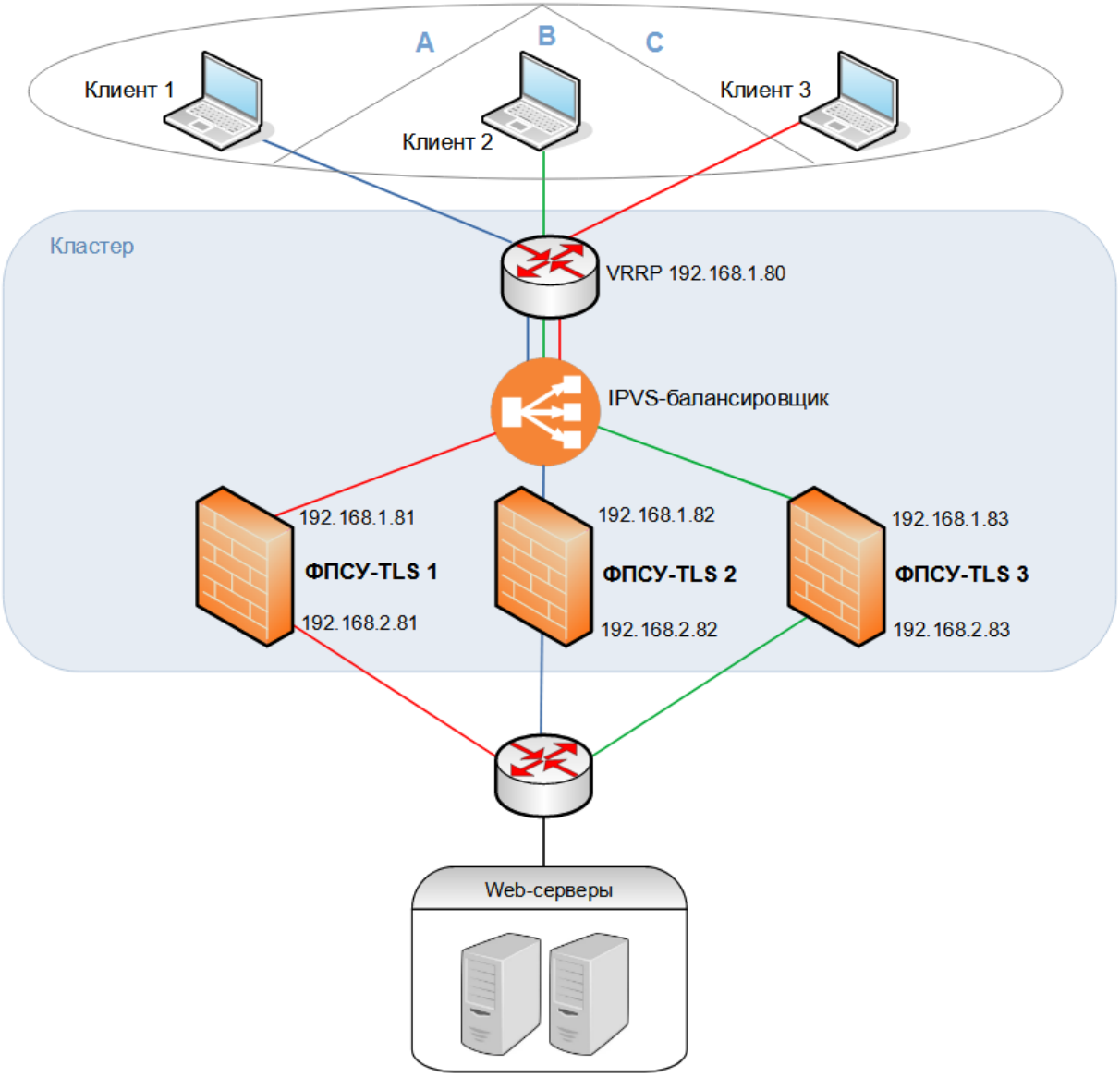

Рисунок 57 - Схема работы кластера ФПСУ-TLS

6. 4. 2. Настройка подсистемы масштабирования

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

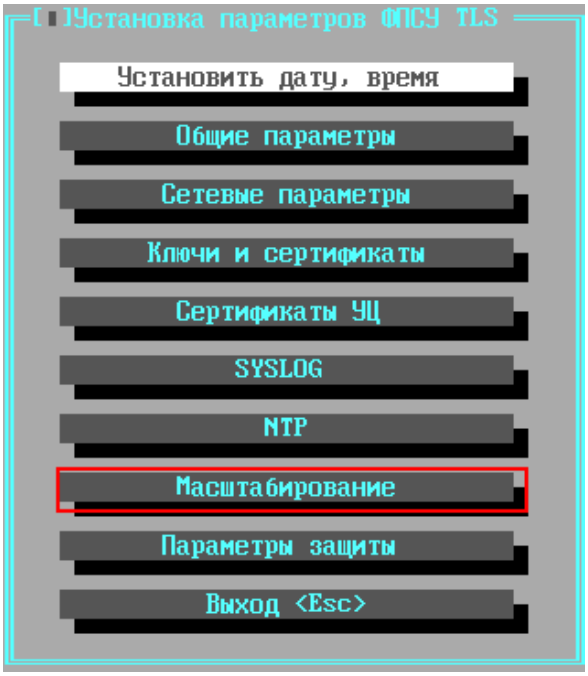

Рисунок 58 - Меню установки параметров ФПСУ-TLS

В открывшемся окне будут указаны следующие параметры работы подсистемы:

Рисунок 59 - Настройка масштабирования

Статус ФПСУ – 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, 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.

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»***.

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.

6. 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:

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.

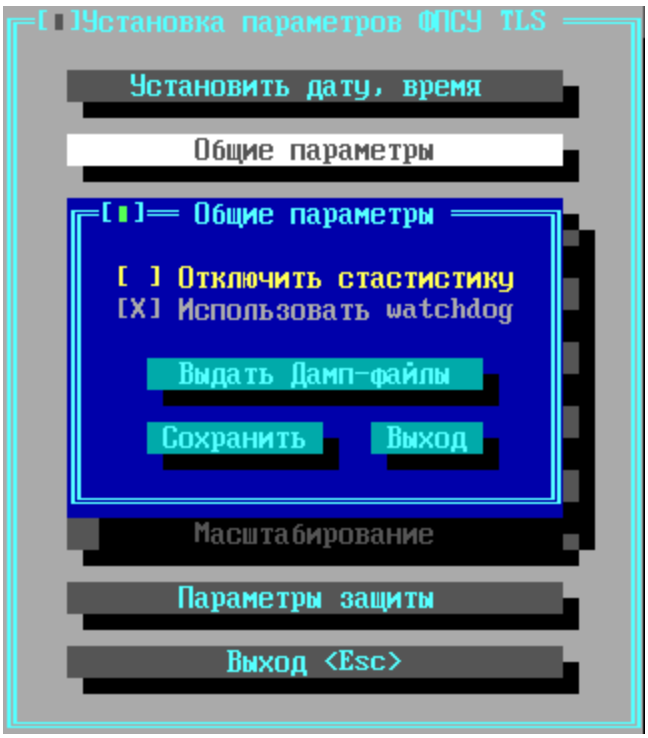

Рисунок 60 - Общие параметры

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

Выдать Дамп-файлы – 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.

6. 6. SYSLOG и SNMP

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» меню установки параметров ФПСУ-TLS:

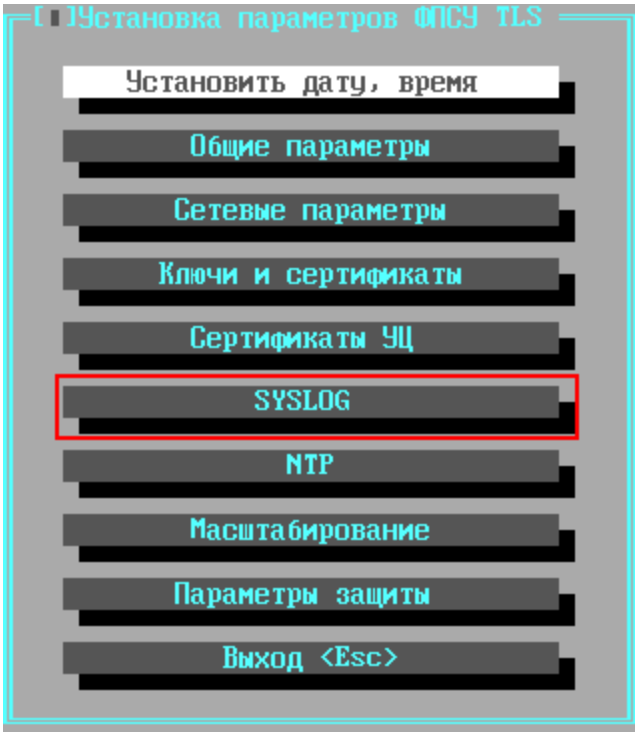

Рисунок 61 - Меню установки параметров ФПСУ-TLS

Для активации подсистемы Syslog, в открывшемся окне укажите следующие параметры:

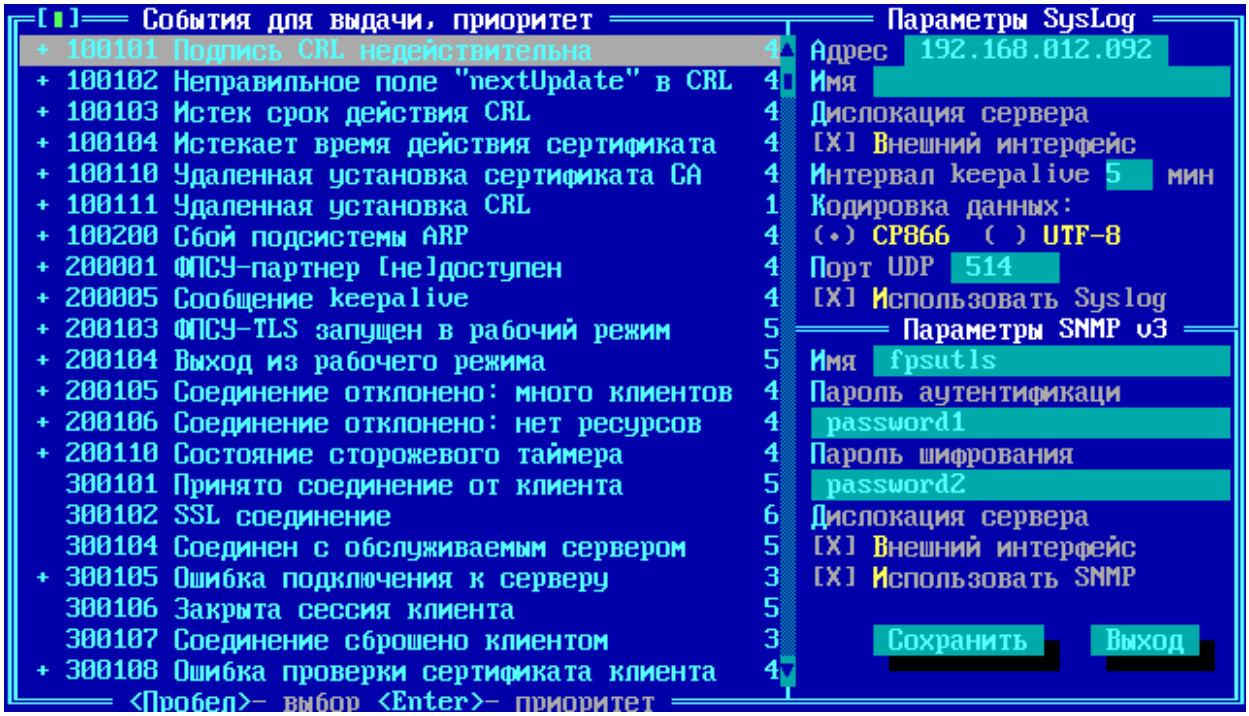

Рисунок 62 - Параметры Syslog и SNMP

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>;

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

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).

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

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 2. Оповещения о событиях

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

Приоритет	Код события	Причина
5	200001	ФПСУ-партнер недоступен
4	200005	Сообщение keepalive
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. Формат: соединение <система> от <IP-адрес> сброшено клиентом

Приоритет	Код события	Причина
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 3. 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;
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.

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

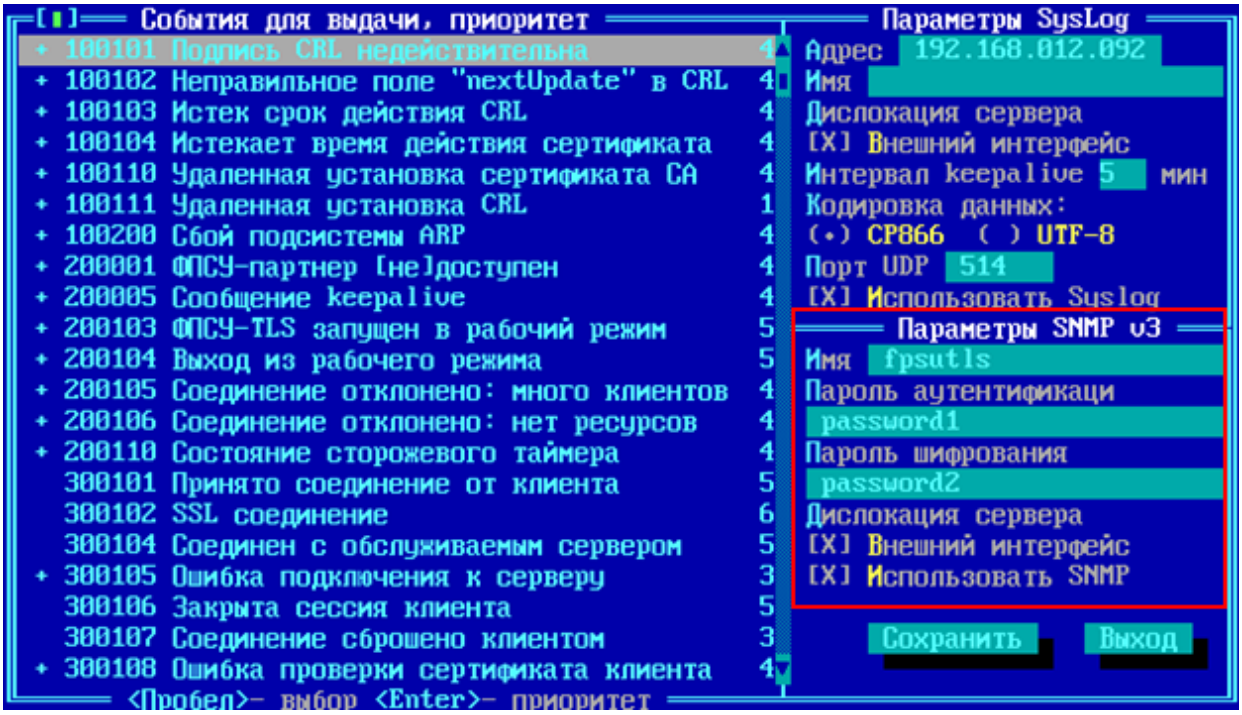

Рисунок 63 - Параметры SNMP

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>;

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.

6. 7. 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.

6. 7. 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»:

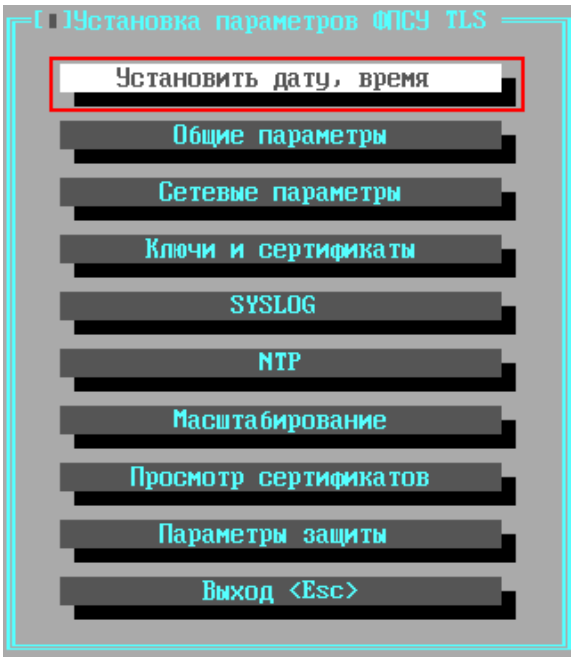

Рисунок 64 - Меню установки параметров ФПСУ-TLS

На экран будет выдано диалоговое окно установки:

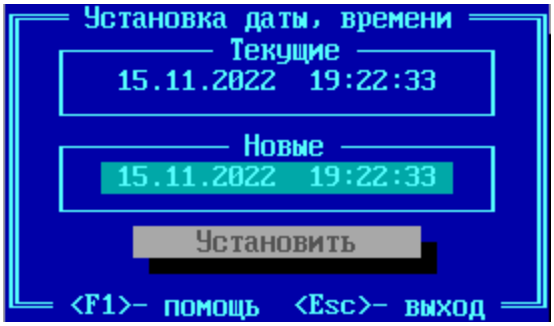

Рисунок 65 - Диалог установки времени на ФПСУ-TLS

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>.

6. 7. 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:

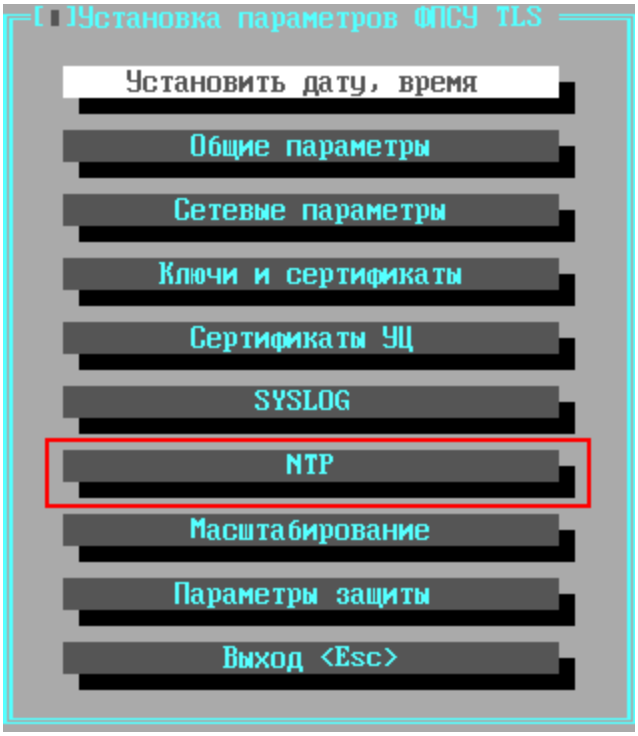

Рисунок 66 - Меню установки параметров ФПСУ-TLS

На экран будет выдано диалоговое окно установки параметров:

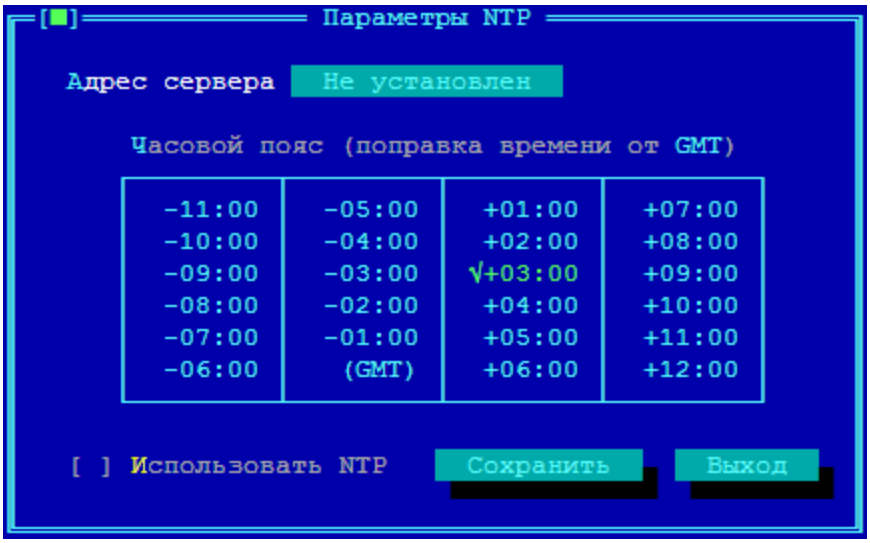

Рисунок 67 - Установка параметров взаимодействия с NTP-сервером

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.

6. 8. Просмотр и удаление установленных сертификатов

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

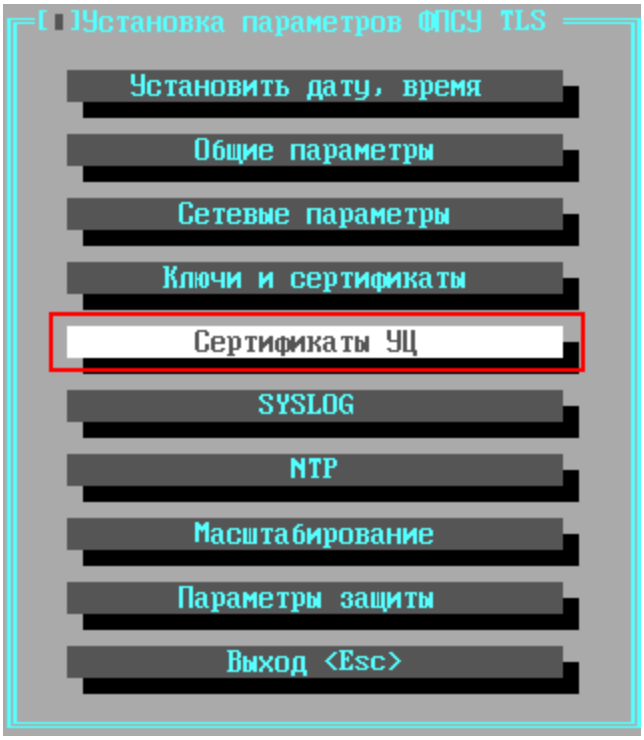

Рисунок 68 - Меню установки параметров ФПСУ-TLS

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.

ВНИМАНИЕ! Перед эксплуатацией ФПСУ-TLS следует просмотреть параметры сертификатов, обозначенных как SERVER или CLIENT, и удалить сертификаты с записью «Signature Algorithm: GOST R 34.11-94 with GOST R 34.10-2001»:

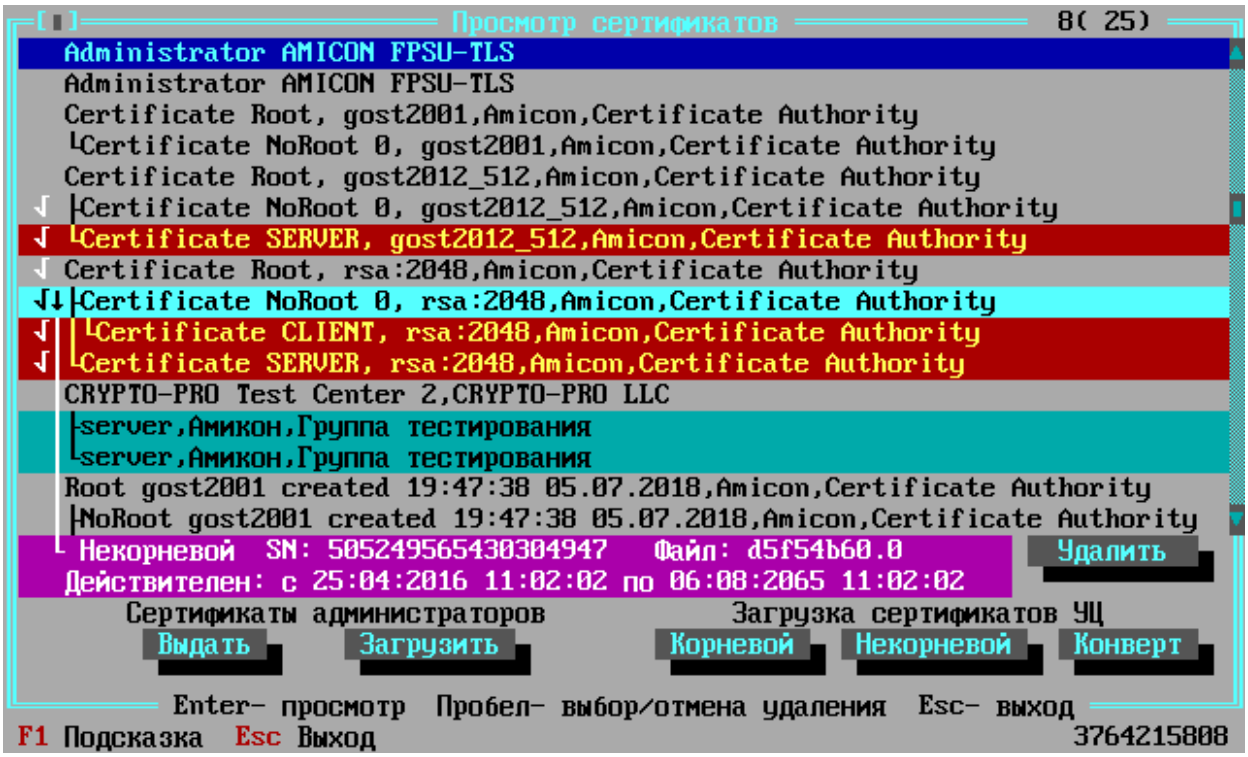

Рисунок 69 - Просмотр списка сертификатов

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

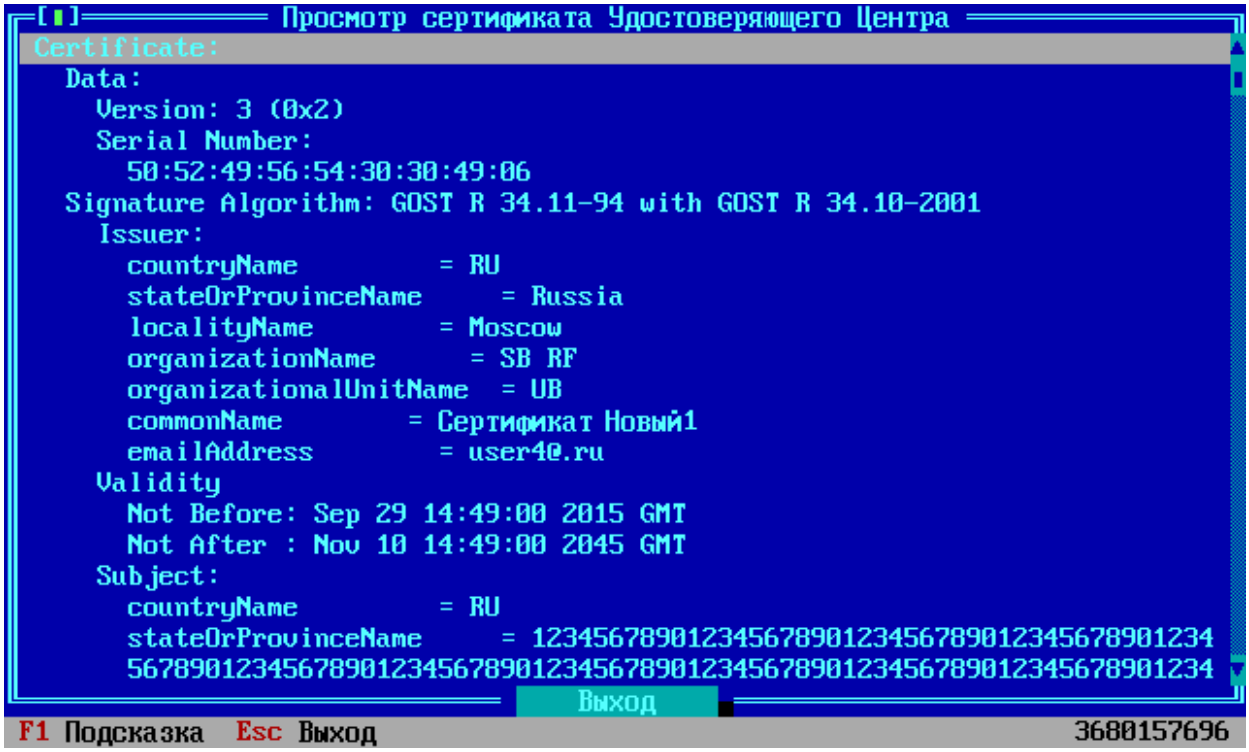

Рисунок 70 - Просмотр сертификата

В строке Signature Algorithm после двоеточия указываются поддерживаемые ФПСУ-TLS крипрографические криптонаборы находятся в поле

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

Для удаления сертификата выделите его курсором и нажмите кнопку <Удалить>.

6. 9. 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:

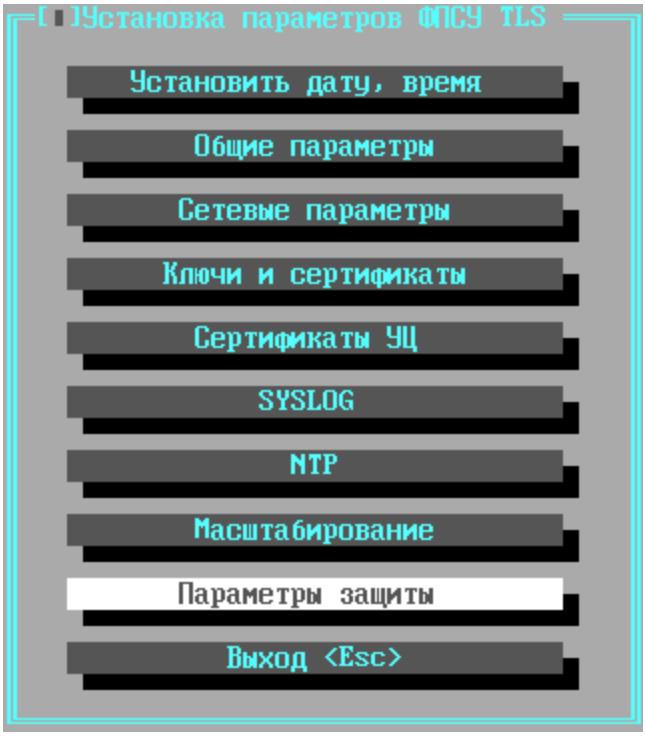

Рисунок 71 - Меню конфигурации ФПСУ-TLS

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

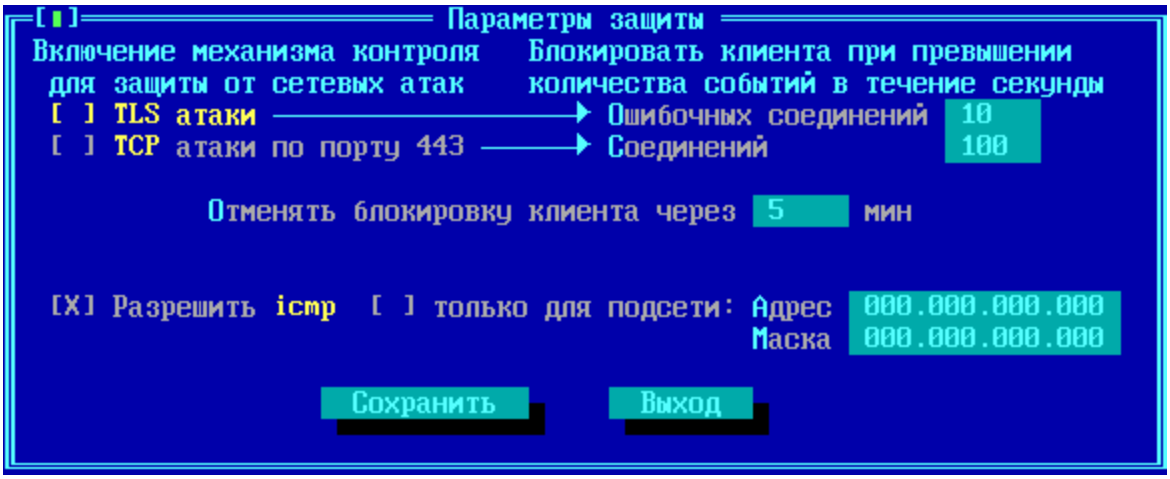

Рисунок 72 - Параметры защиты

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.

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.

6. 10. 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.

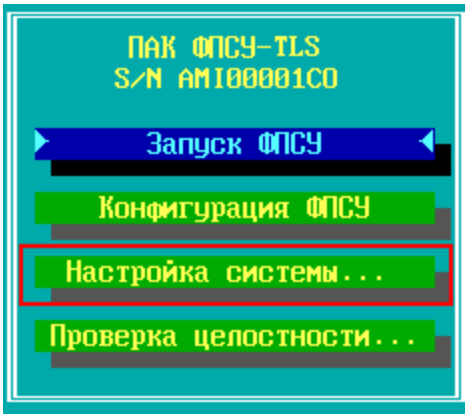

Рисунок 73 - Вызов меню настройки системы

При выборе опции «Настройка Системы» откроется ее подменю, содержащее две команды, «Регистрация ТМ-идентификаторов» (см. пункт Регистрация ТМ-

идентификаторов) и «Установка дополнений/изменений» (см. пункт Обновление программного обеспечения).

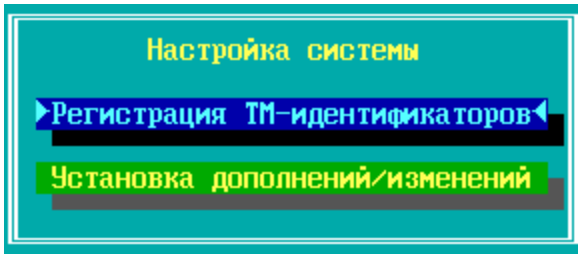

Рисунок 74 - Меню настройки системы

6. 10. 1. Регистрация ТМ-идентификаторов

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

- регистрации новых локальных администраторов ФПСУ-TLS (из записи их идентификационной информации на ТМ);
- 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.

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.

Рисунок 75 - Меню регистрации администраторов

6. 10. 1. 1. Регистрация нового администратора

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.

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

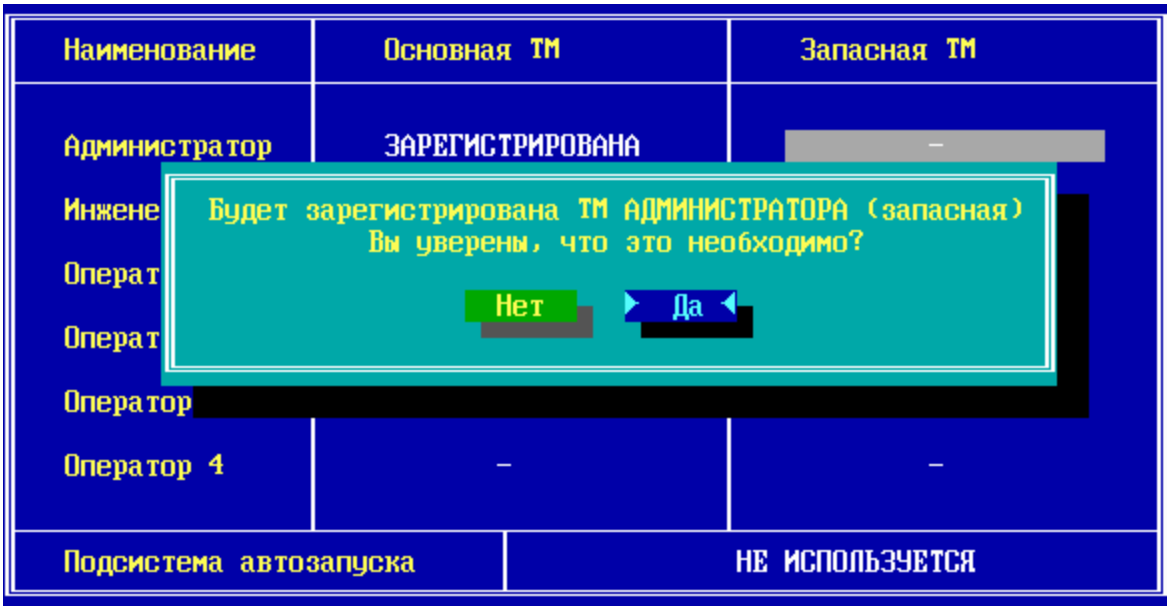

Рисунок 76 - Регистрация запасного ТМ администратора

При выполнении операции по регистрации система будет требовать подтверждения полномочий администратора прижатием основного ТМ-идентификатора учетной записи «Администратор» к считывателю ТМ.

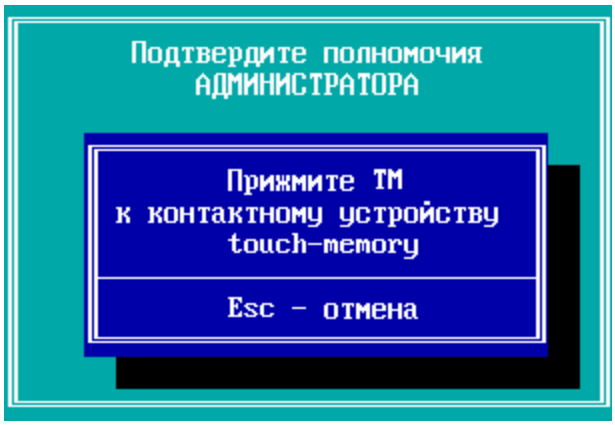

Рисунок 77 - Подтверждение прав администратора

Затем потребуется прижать ТМ-идентификатор к считывателю, на который будет записываться запасной ТМ администратора, для регистрации.

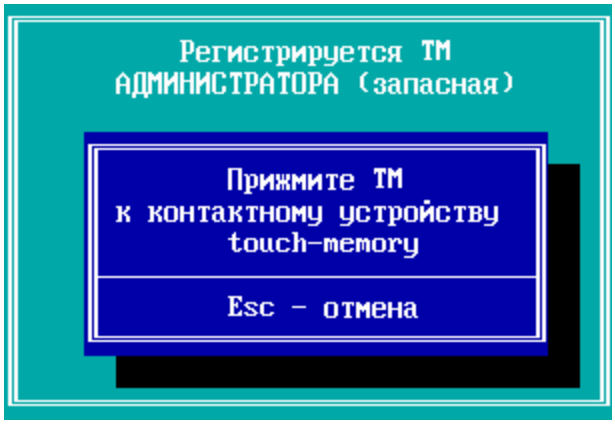

Рисунок 78 - Запись запасного ТМ администратора

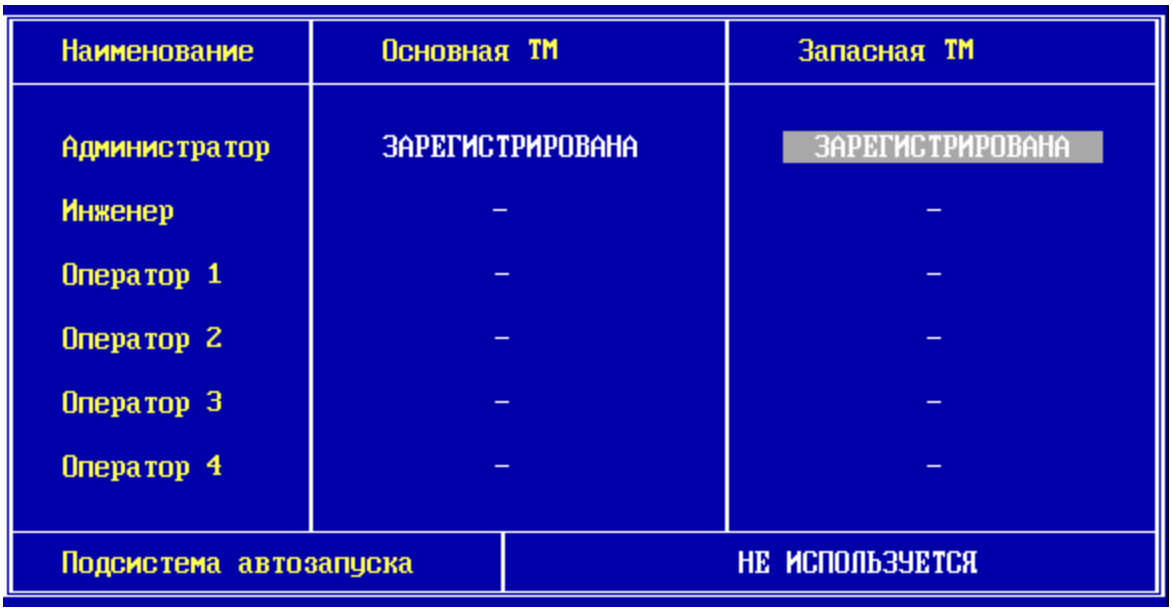

Рисунок 79 - Запасной ТМ администратора создан

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.

Разрешенные для текущей записи действия выполняются при помощи следующих клавиш:

- <Ins> – регистрация или перерегистрация ТМ выбранной учетной записи;
- <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.

6. 10. 1. 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»;

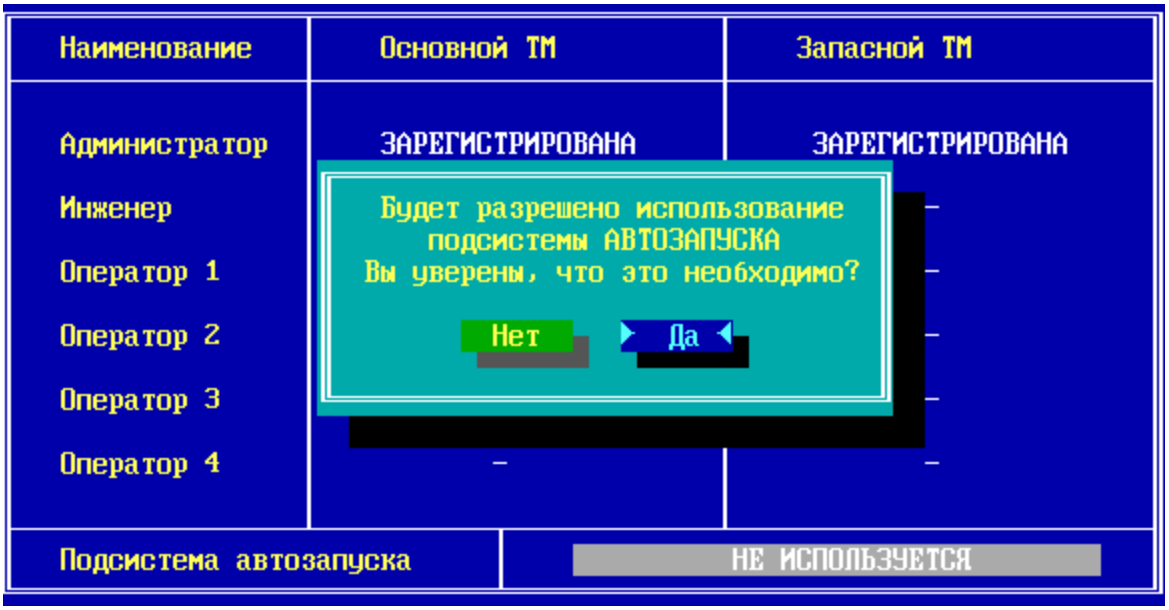

Рисунок 80 - Включение подсистемы автозапуска ФПСУ-TLS

- подтвердите полномочия администратора ФПСУ-TLS, приложив ТМ-идентификатор к считывателю;

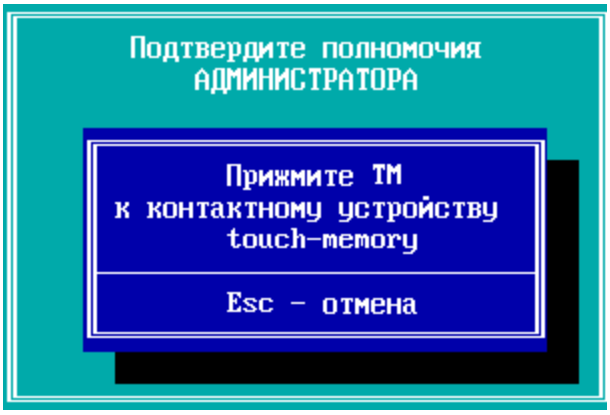

Рисунок 81 - Подтверждение прав администратора

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

Наименование	Основная ТМ	Запасная ТМ
Администратор	ЗАРЕГИСТРИРОВАНА	ЗАРЕГИСТРИРОВАНА
Инженер	-	-
Оператор 1	-	-
Оператор 2	-	-
Оператор 3	-	-
Оператор 4	-	-
Подсистема автозапуска	ИСПОЛЬЗУЕТСЯ	

Рисунок 82 - 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.

6. 10. 2. Обновление программного обеспечения

Опция подменю «Настройка подсистемы > Установка дополнений/изменений» предназначена для установки новых программных модулей или обновлений существующих модулей ФПСУ-TLS (операции доступны администратору класса «Главный Администратор»).

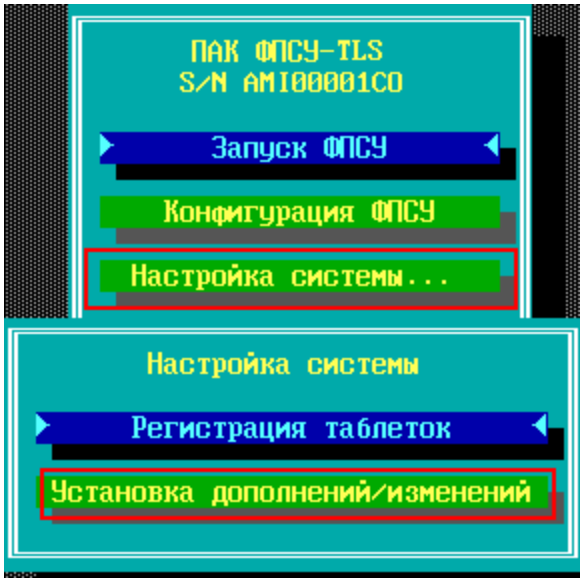

Рисунок 83 - Переход в меню установки дополнений/изменений

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 WINFPSUHASH.EXE хэш-функции от файла с обновлениями и сравнением полученного результата с контрольными данными. Программа WINFPSUHASH.EXE 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 основного меню ФПСУ-TLS, «Настройка подсистемы > Установка дополнений/изменений». Для выполнения команды потребуется предъявить ТМ-идентификатор Главного администратора.

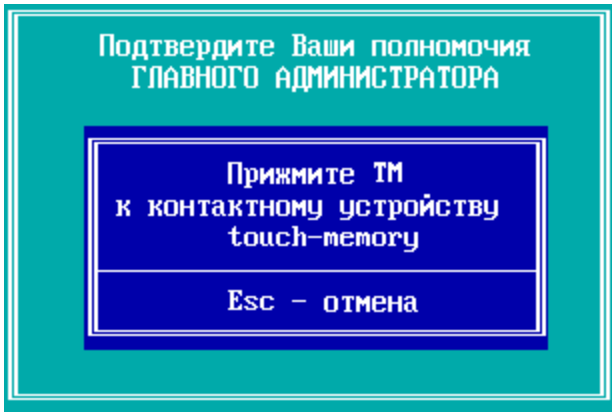

Рисунок 84 - Требуется ТМ-идентификатор Главного администратора

В появившемся служебном окне нажмите клавишу <Enter> для продолжения, проверив корректность подключения внешнего носителя к USB-порту ФПСУ-TLS. Файлы обновления должны лежать в корне USB-носителя!

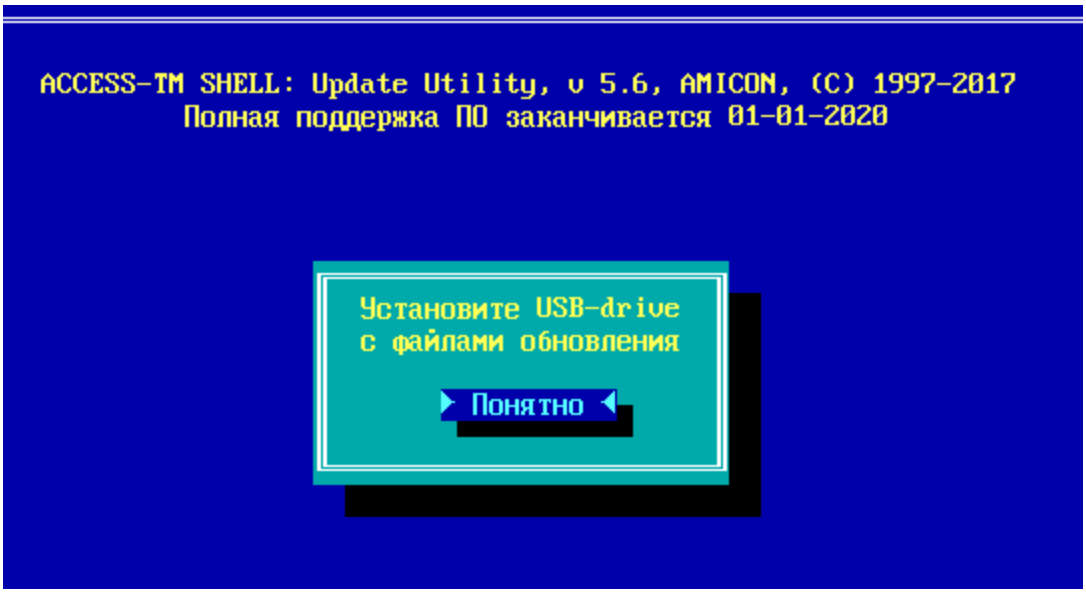

Рисунок 85 - Подсистема обновления, запрос на подключение USB

Если внешний носитель исправен и содержит файлы обновления программного обеспечения для ФПСУ-TLS с таким серийным номером, то в диалоге установки будет

предложено установить обновления из первого найденного файла обновления программного обеспечения, либо попытаться найти другой файл. Для установки найденного обновления выберите ответ «Используем его» и нажмите клавишу <Enter>.

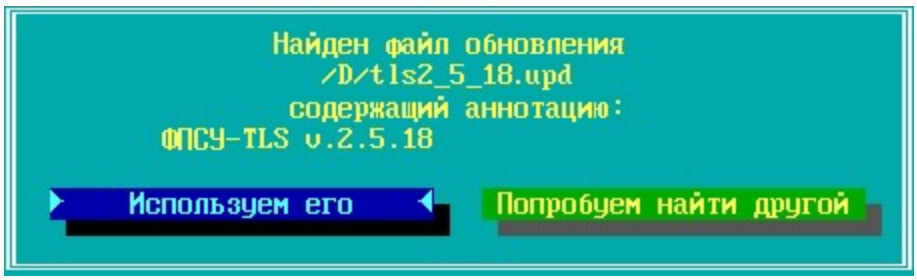

Рисунок 86 - Найден файл обновления

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.

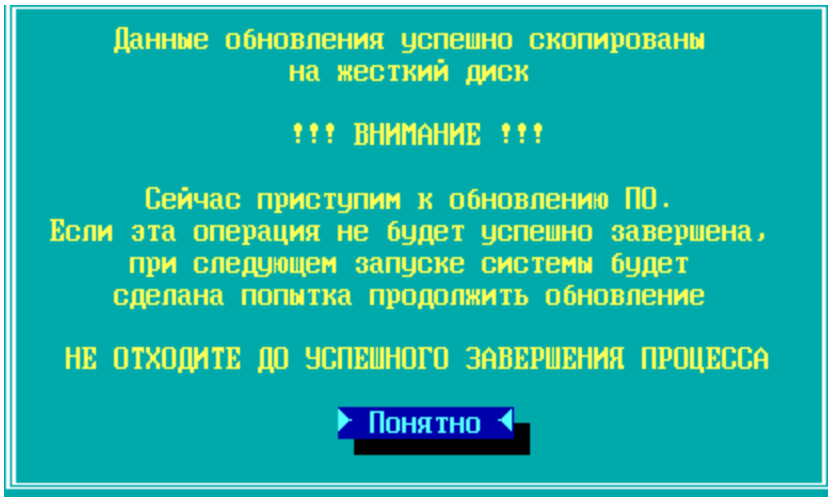

Рисунок 87 - Файлы скопированы, можно запускать обновление

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

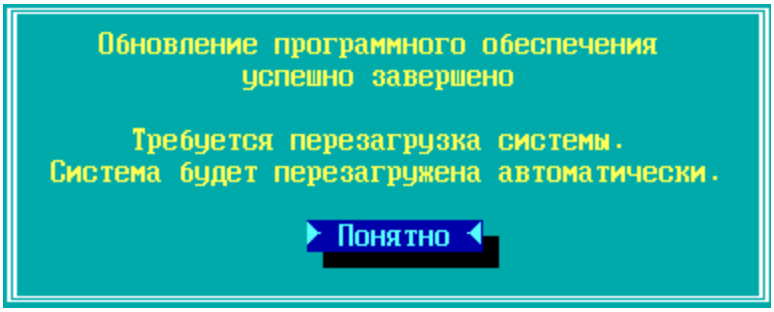

Рисунок 88 - Установка завершена, требуется перезагрузка

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

Рисунок 89 - Основное меню ФПСУ-TLS

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

7. 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, bmon.

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

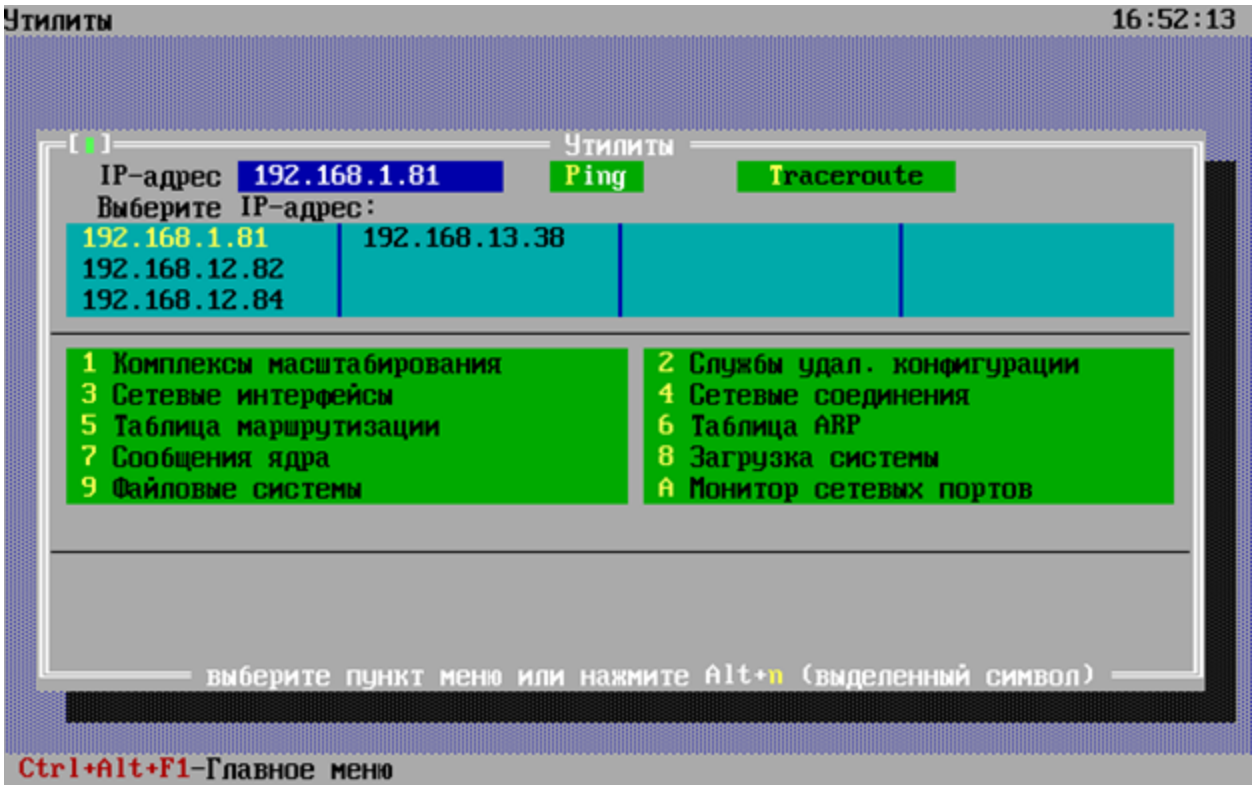

Рисунок 90 - Окно с утилитами ФПСУ-TLS

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.

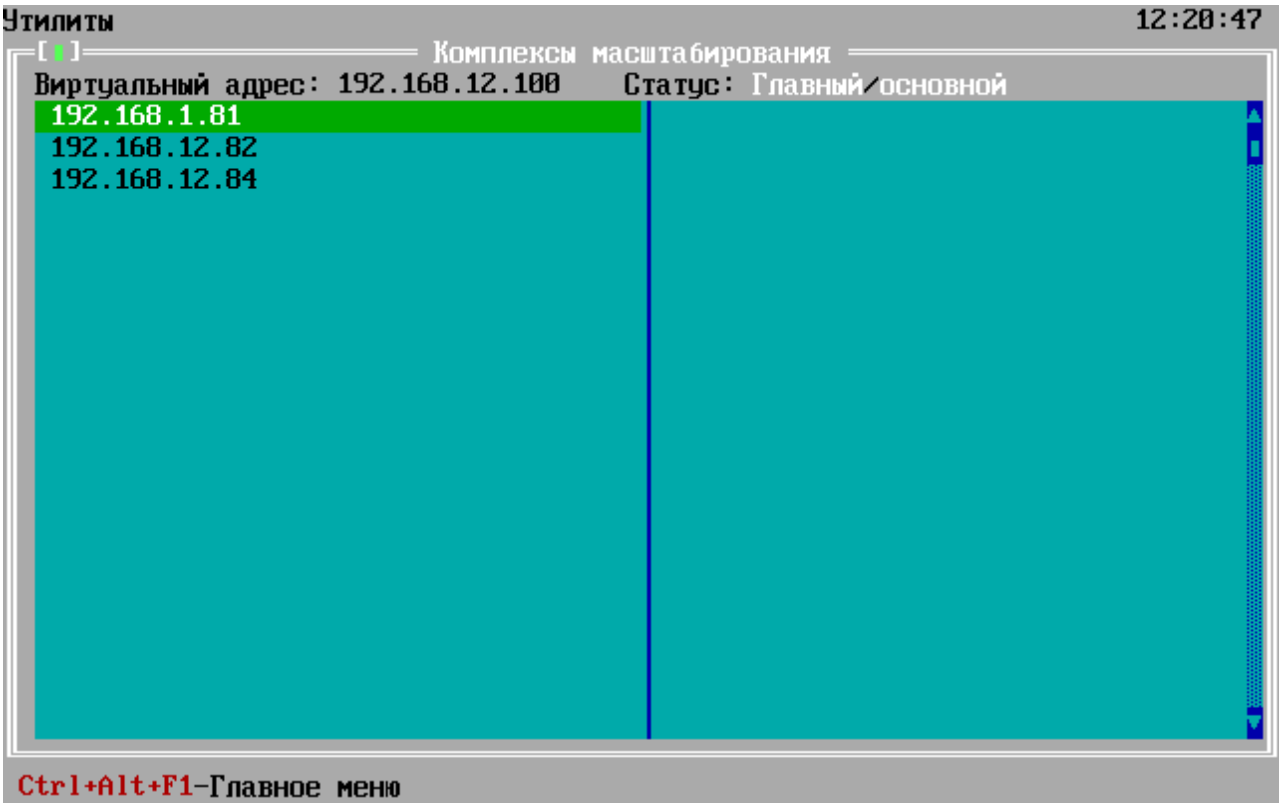

Рисунок 91 - Окно «Комплексы масштабирования»

2 Службы удаленной загрузки конфигурации

Опция «Службы удал. конфигурации» вызывается по нажатию клавиш <Alt+2> или <2>. Для выбранного IP-адреса на экран выдается информация о службе удаленной загрузки конфигурации, с указанием IP-адреса точки распространения.

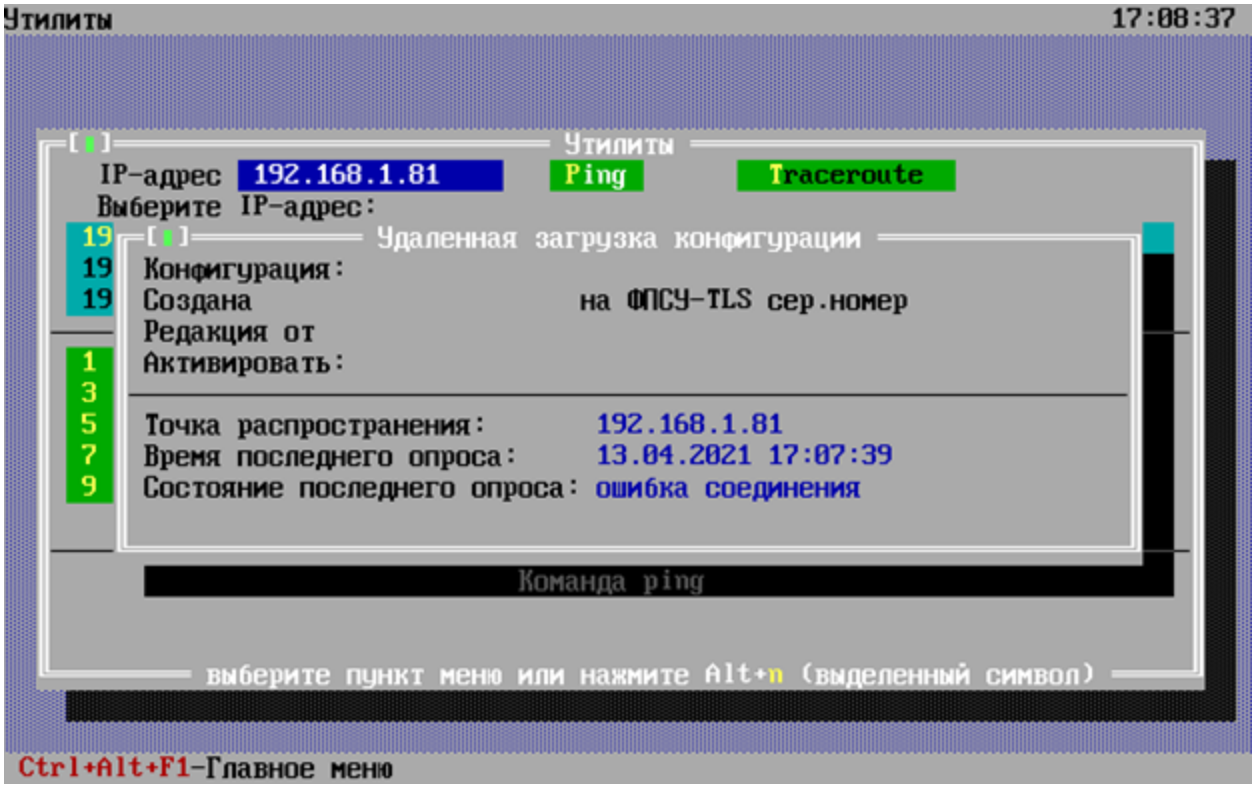

Рисунок 92 - Окно «Службы удал. конфигурации»

3 Сетевые интерфейсы

Опция «Сетевые интерфейсы» вызывается по нажатию клавиш <Alt+3> или <3>, 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.

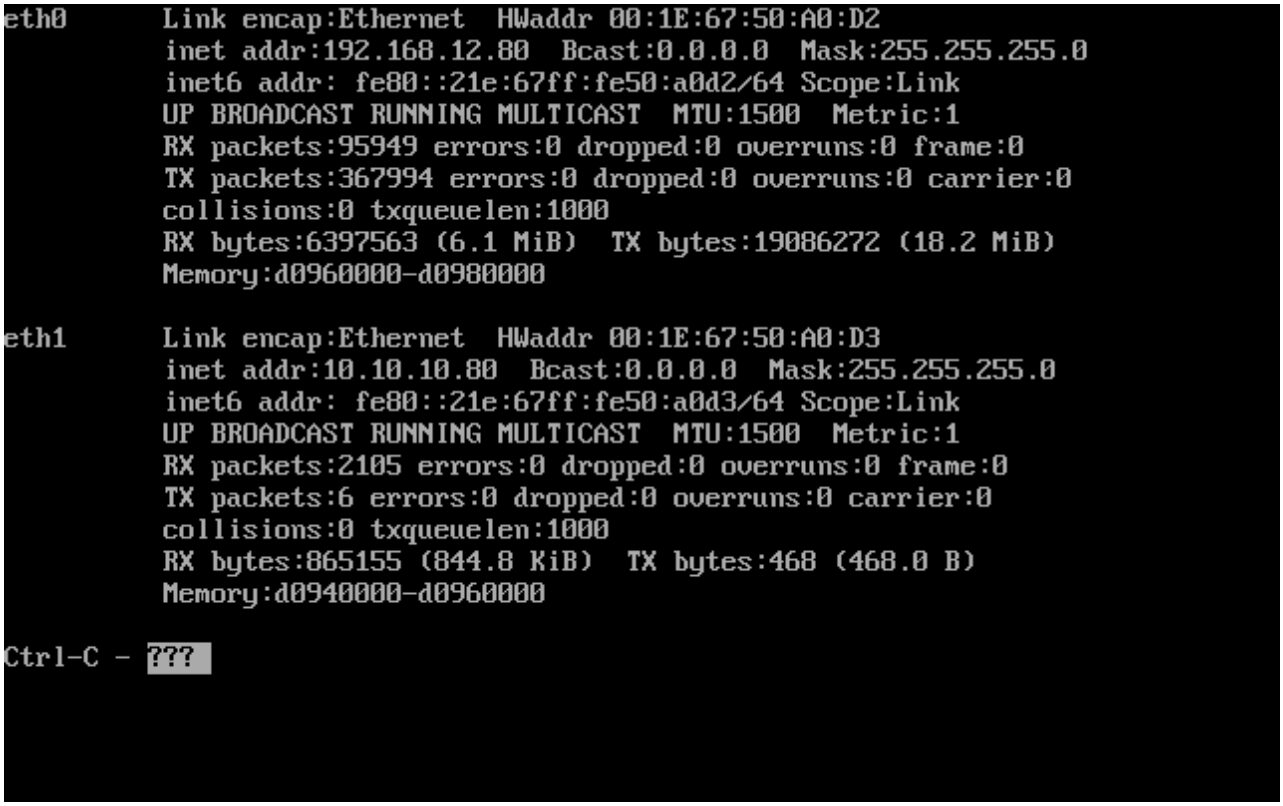

Рисунок 93 - Окно «Сетевые интерфейсы»

4 Сетевые соединения

Опция «Сетевые соединения» вызывается по нажатию клавиш <Alt+4> или <4>, выполняет команду `netstat` для поиска сетевых проблем и определения производительности сети. На экране выводится список активных соединений.

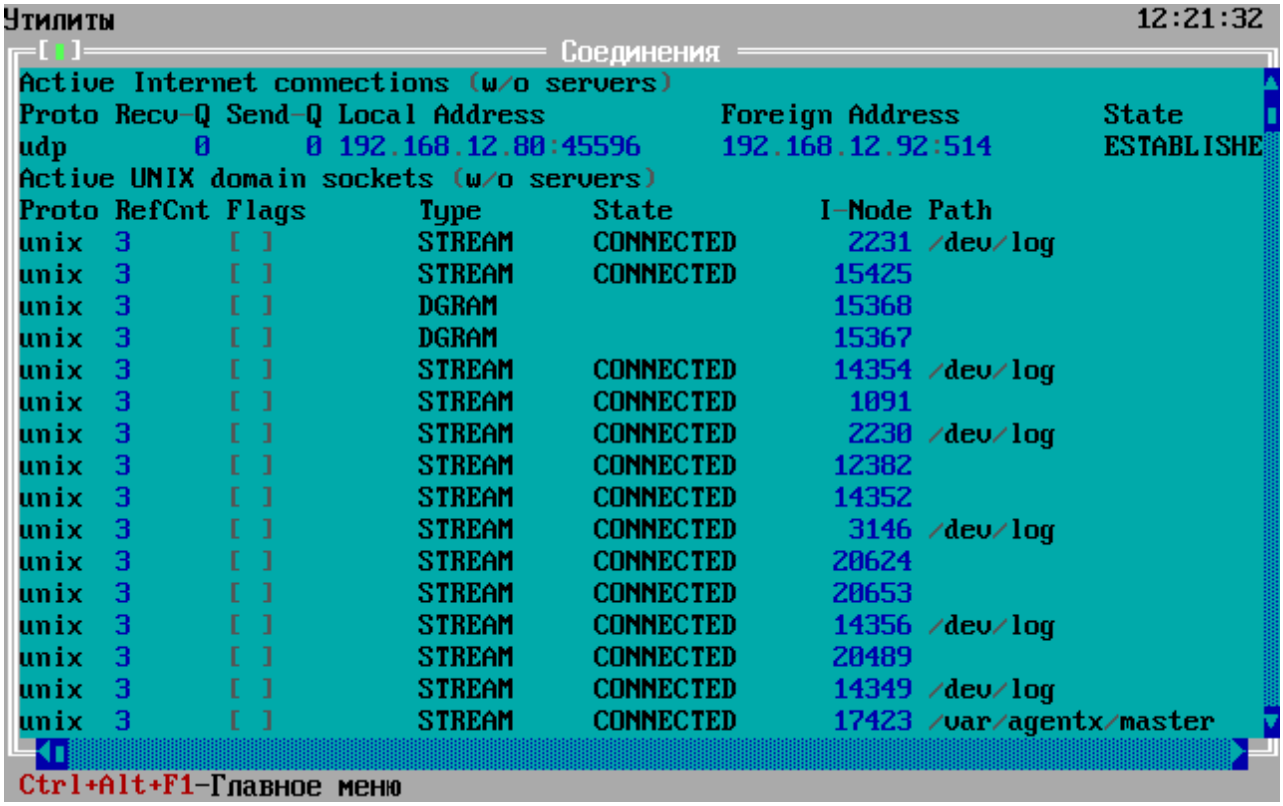

Рисунок 94 - Окно «Сетевые соединения»

5 Таблица маршрутизации

Опция «Сетевые соединения» вызывается по нажатию клавиш <Alt+5> или <5>, выполняет команду `route` для просмотра таблицы маршрутизации.

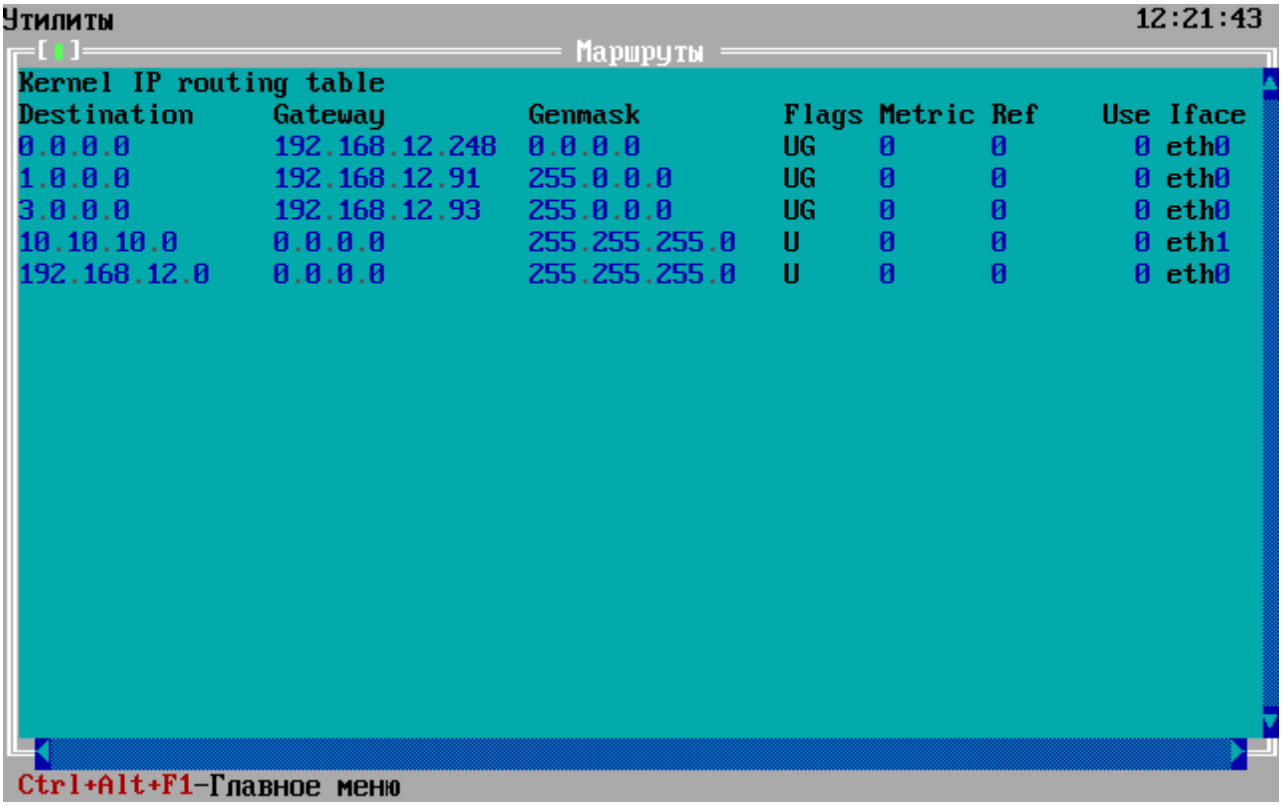

Рисунок 95 - Окно «Таблица маршрутизации»

6 Таблица ARP

Опция «Таблица ARP» вызывается по нажатию клавиш <Alt+6> или <6>, выполняет команду `arp` для вывода записей ARP-таблицы. Запись ARP-таблицы включает IP-адрес, соответствующий ему MAC-адрес с указанием интерфейса.

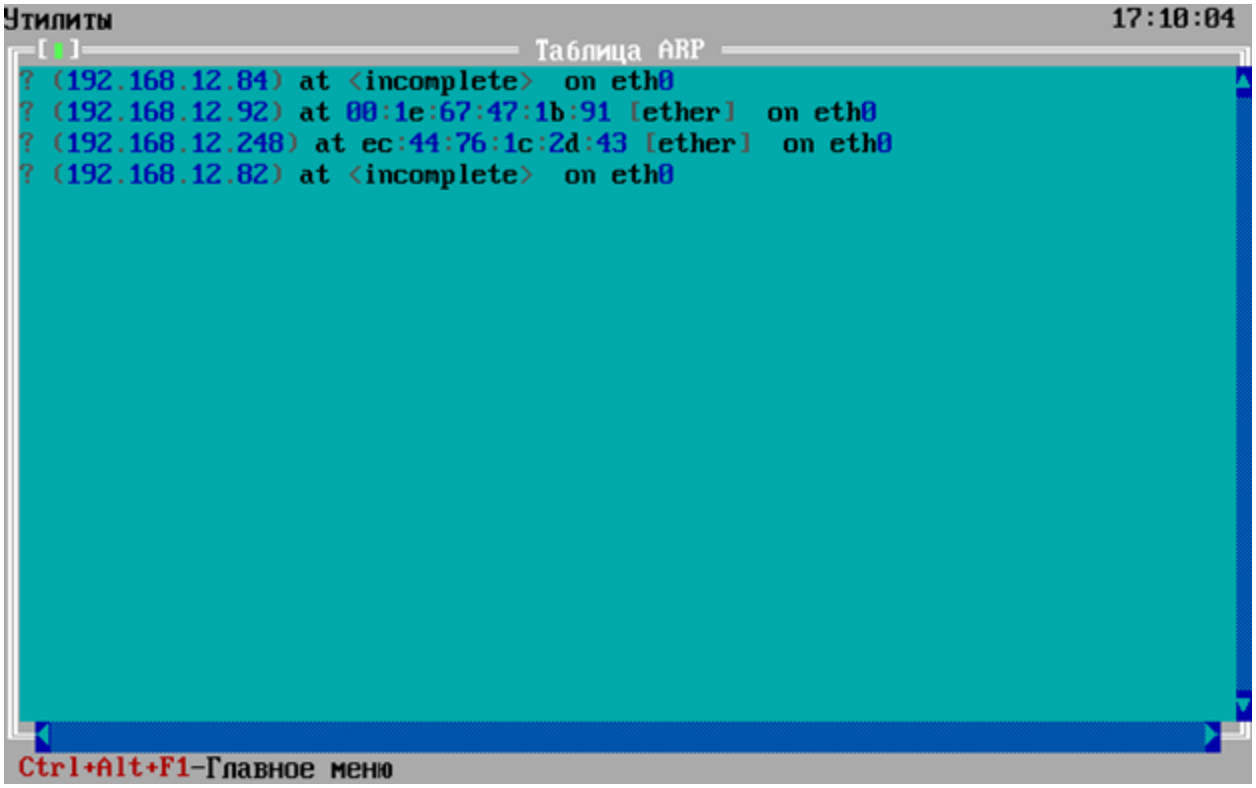

Рисунок 96 - Окно «Таблица ARP»

7 Сообщения ядра

Опция «Сообщения ядра» вызывается по нажатию клавиш <Alt+7> или <7>, 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.

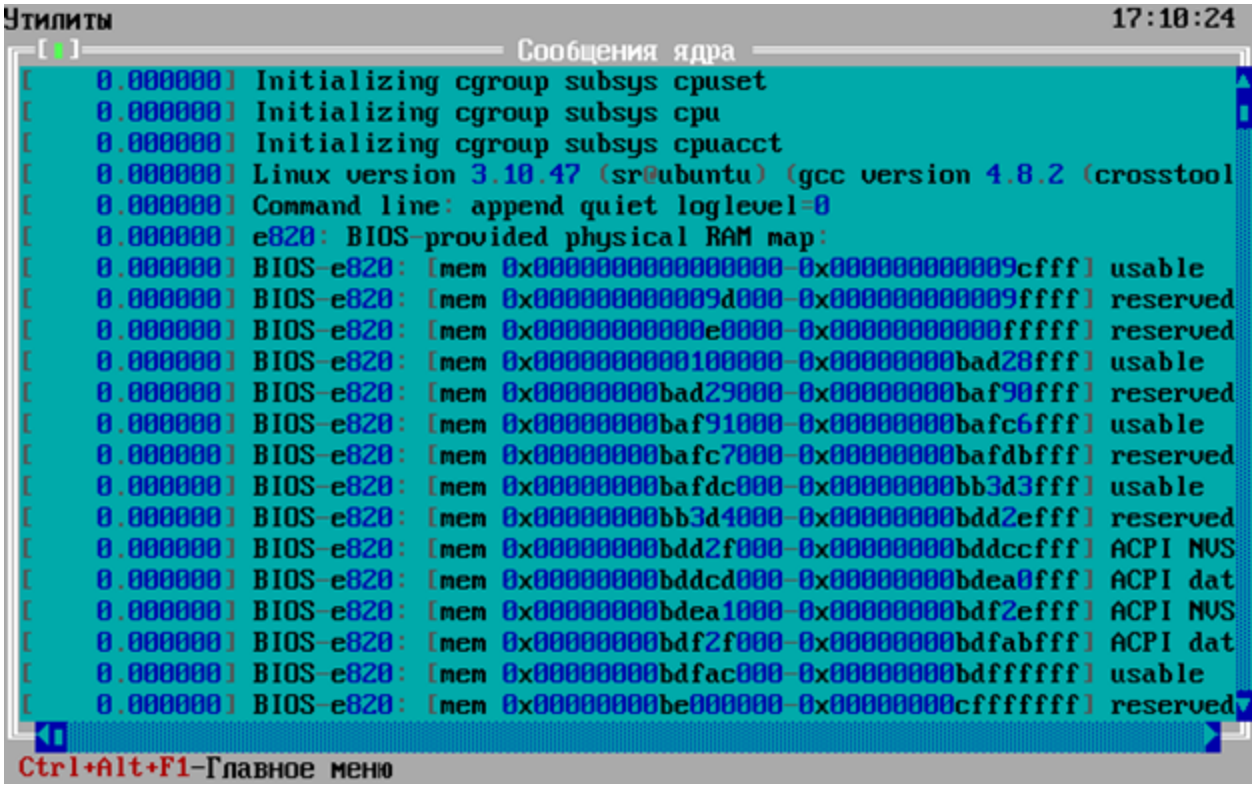

Рисунок 97 - Окно «Сообщения ядра»

8 Загрузка системы

Опция «Загрузка системы» вызывается по нажатию клавиш <Alt+8> или <8>, выполняет команду `top`, выводит список работающих в операционной системе процессов и информацию о них.

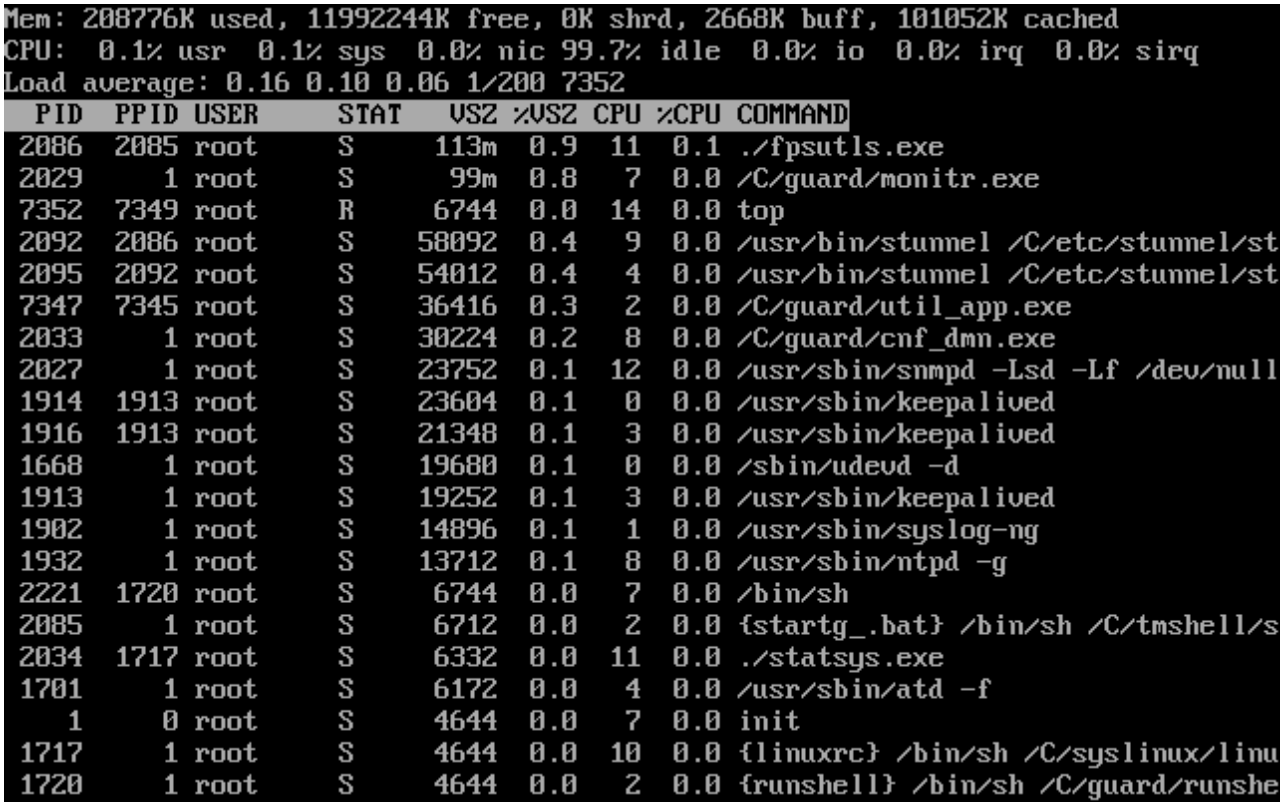

Рисунок 98 - Окно «Загрузка системы»

9 Файловые системы

Опция «Файловые системы» вызывается по нажатию клавиш <Alt+9> или <9>, выполняет команду `df`, выдаёт отчёт о доступном и использованном дисковом пространстве на файловых системах.

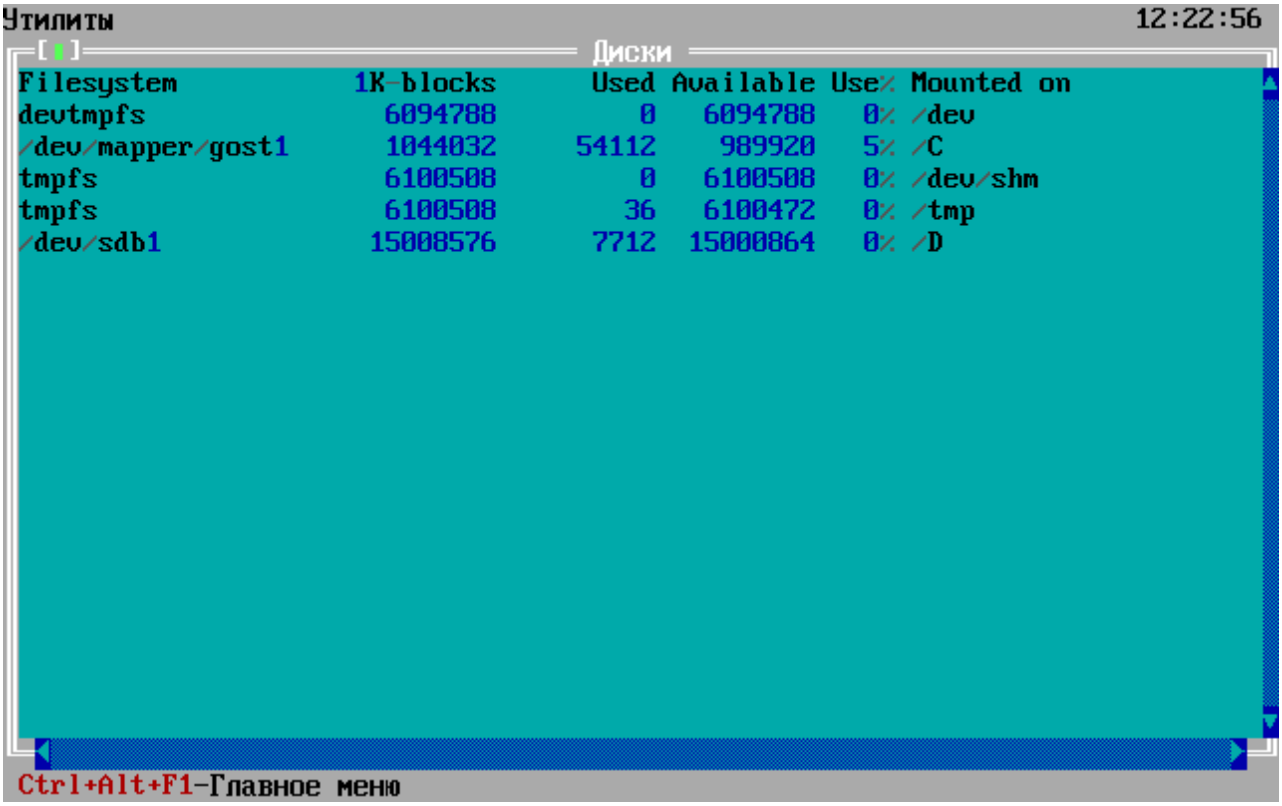

Рисунок 99 - Окно «Файловые системы»

A Монитор сетевых портов

Опция «Монитор сетевых портов» вызывается по нажатию клавиш <Alt+A>, выполняет команду `bmon` для мониторинга трафика сетевых интерфейсов. Для каждого интерфейса отображается скорость передачи информации и число пакетов за единицу времени.

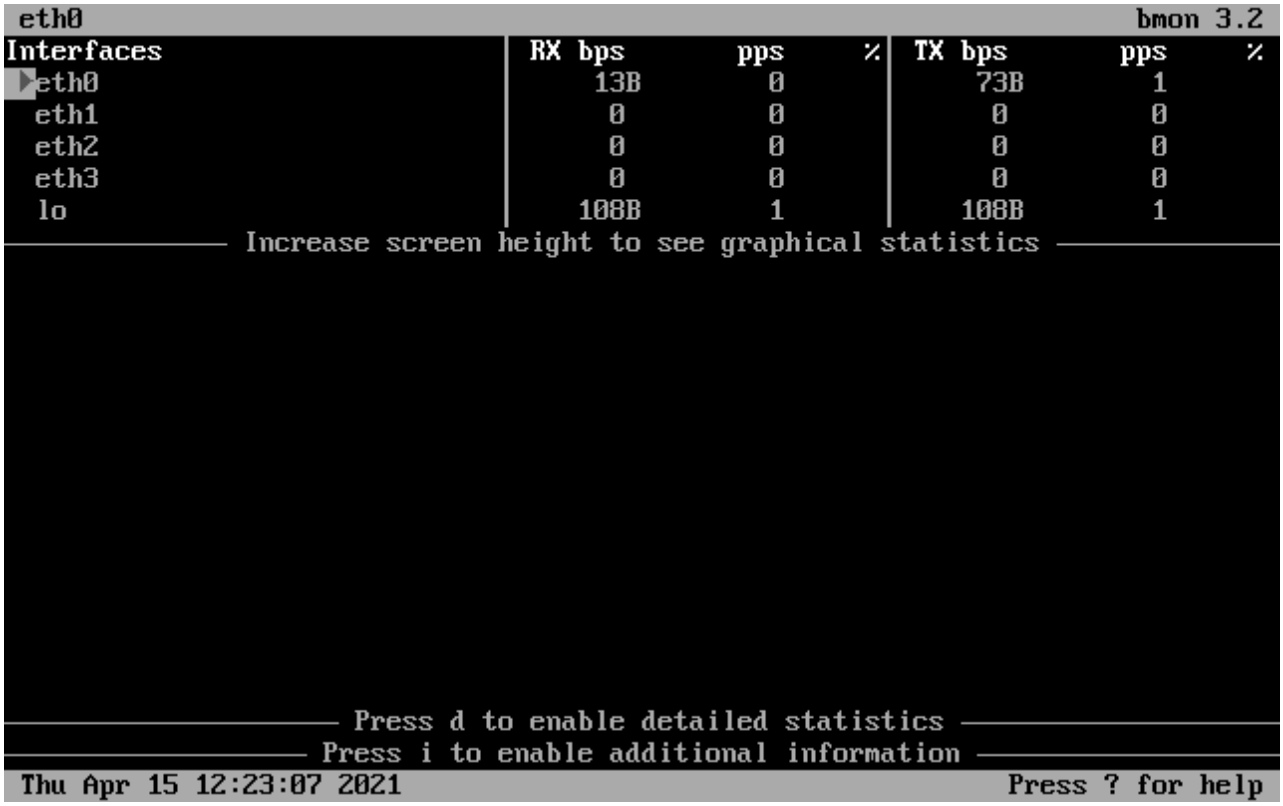

Рисунок 100 - Окно «Монитор сетевых портов»

8. Резервирование и восстановление

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.

9. 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.

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

Рисунок 101 - Основное меню ФПСУ-TLS

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

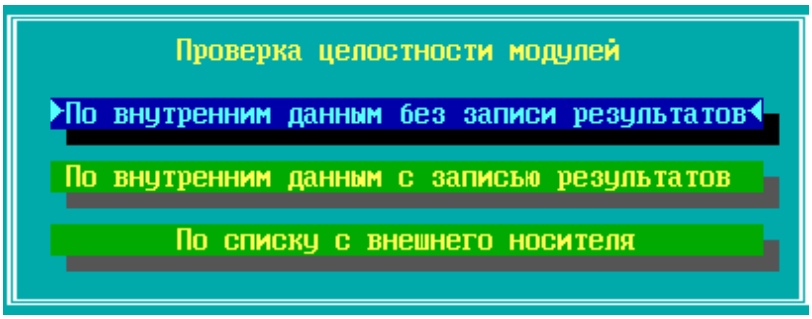

Рисунок 102 - Меню проверки целостности

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.

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.

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.

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

10. Инсталляция ПО ФПСУ-TLS

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

- аппаратная основа ФПСУ-TLS (АО);
- 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 АО 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.

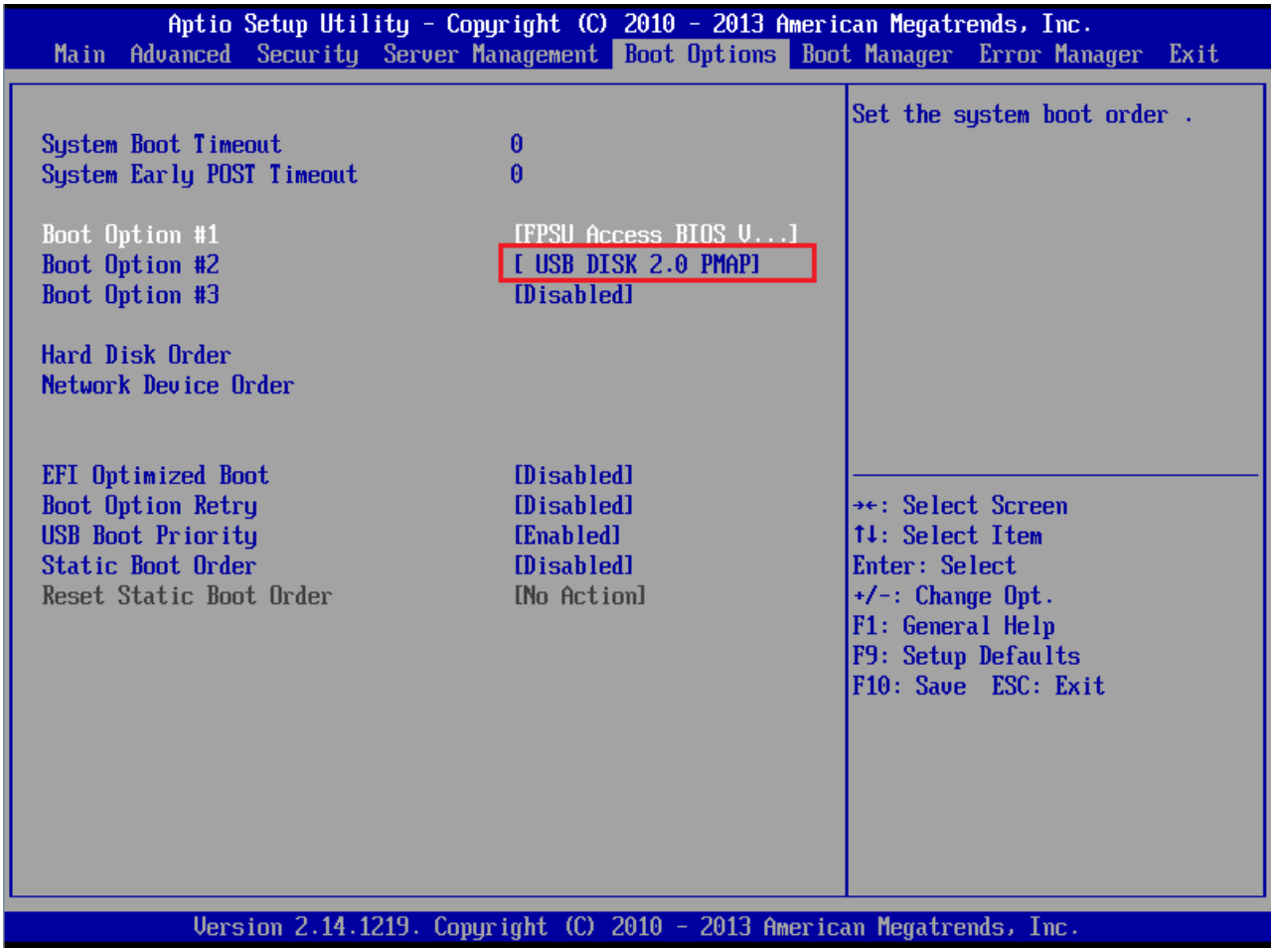

Рисунок 103 - Выбор загрузки с USB

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:

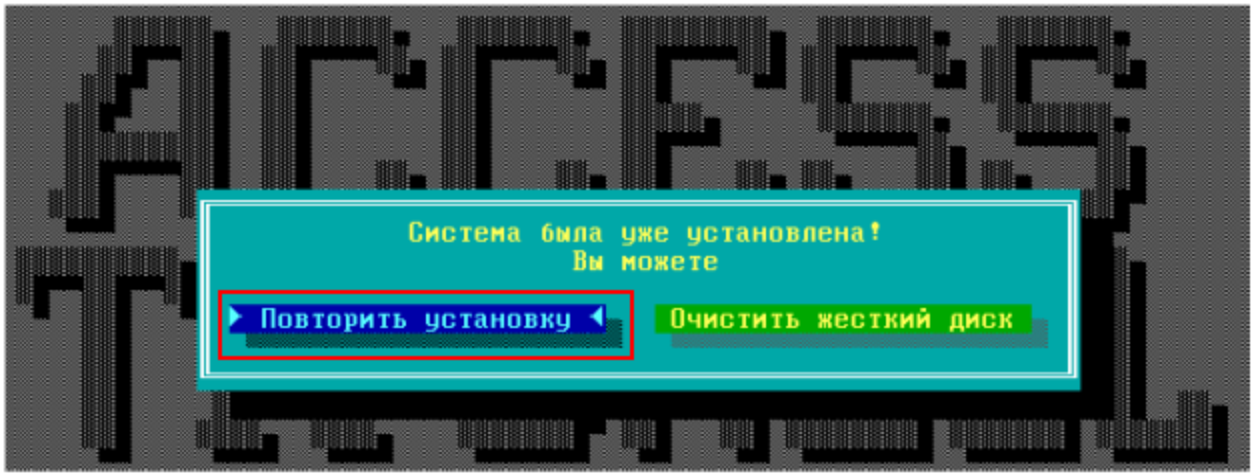

Рисунок 104 - Сообщение при повторной установке

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.

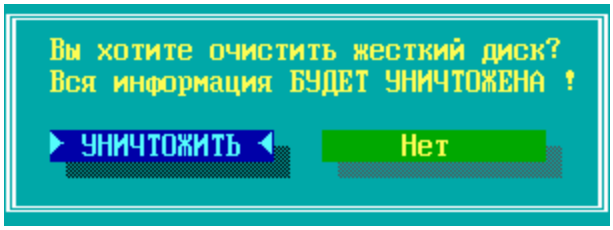

Рисунок 105 - Очистка ПЗУ ФПСУ-TLS

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.

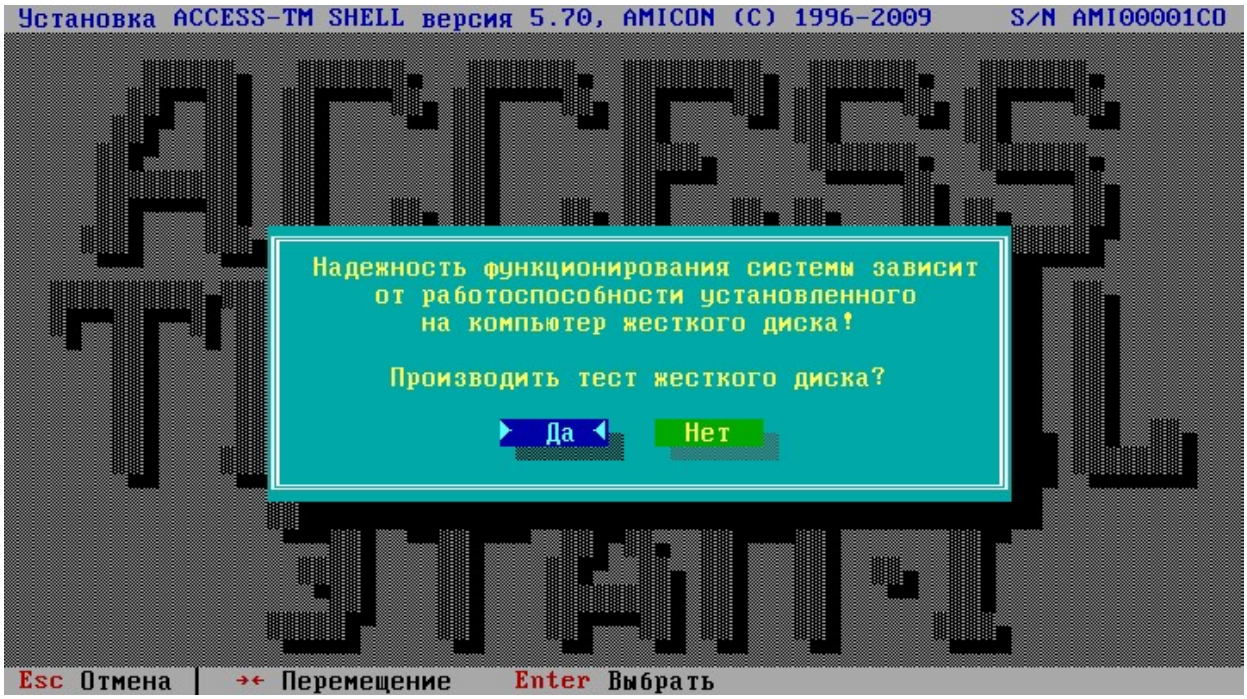

Рисунок 106 - Тест ПЗУ ФПСУ-TLS

Необходимо дождаться завершения теста.

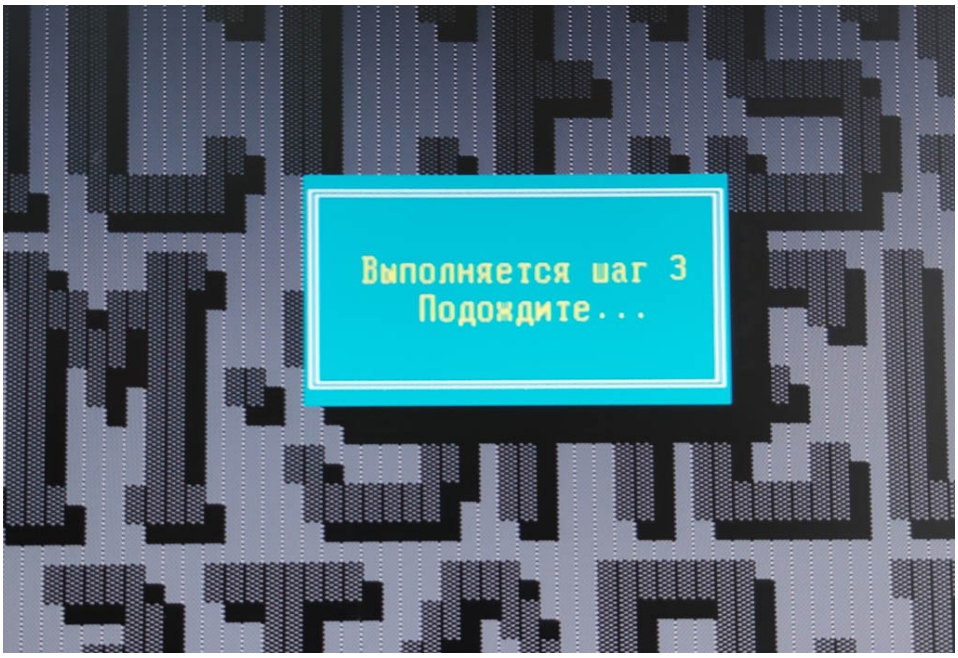

Рисунок 107 - Тест ПЗУ ФПСУ-TLS

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

Рисунок 108 - 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.

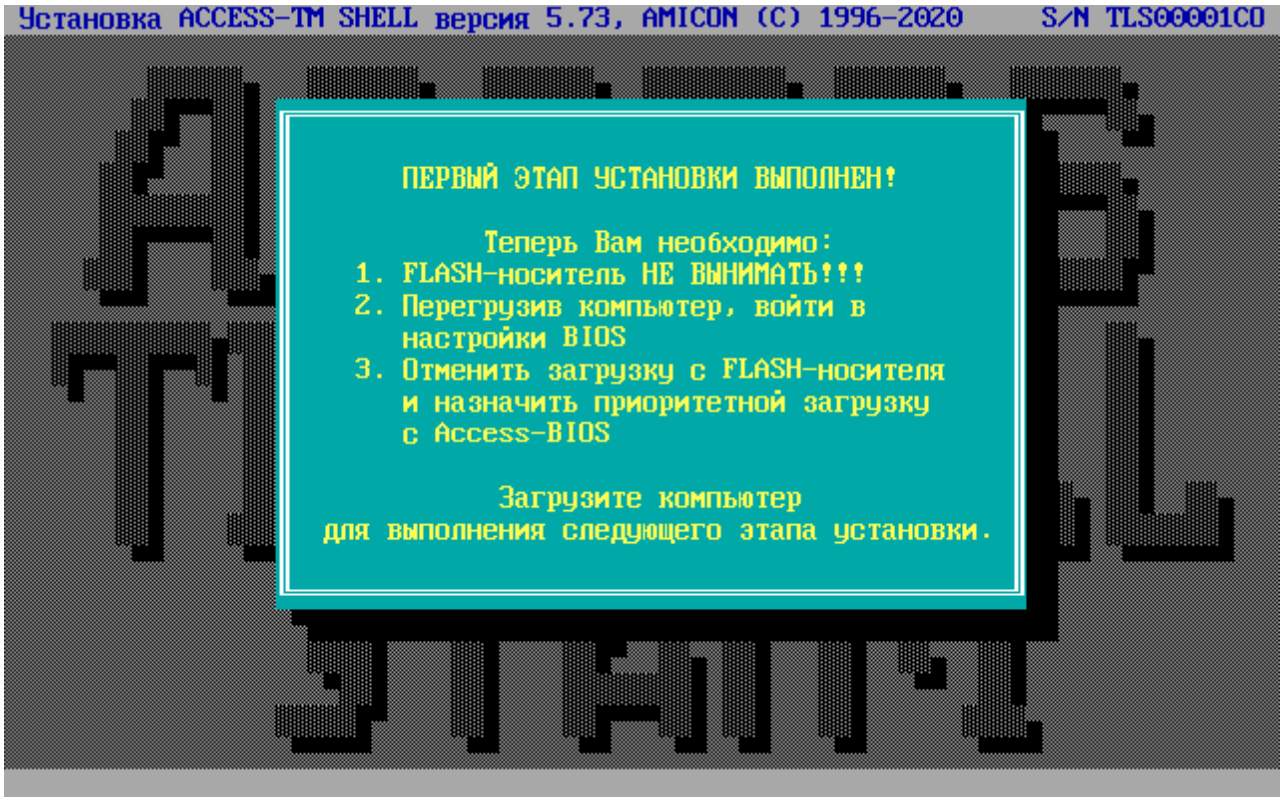

Рисунок 109 - Завершение первого этапа установки

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).

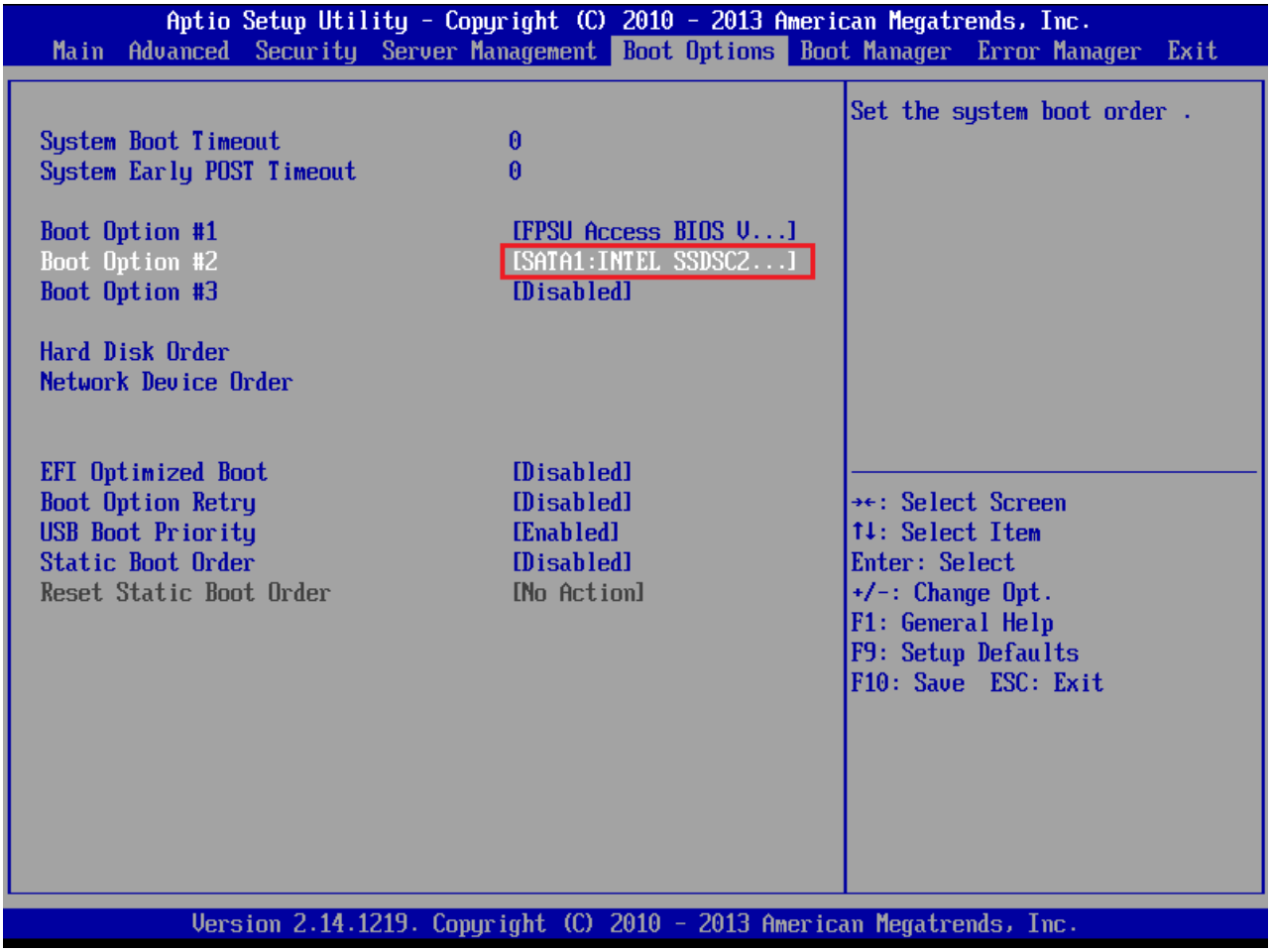

Рисунок 110 - Выбор загрузки с Access BIOS/PnP

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:

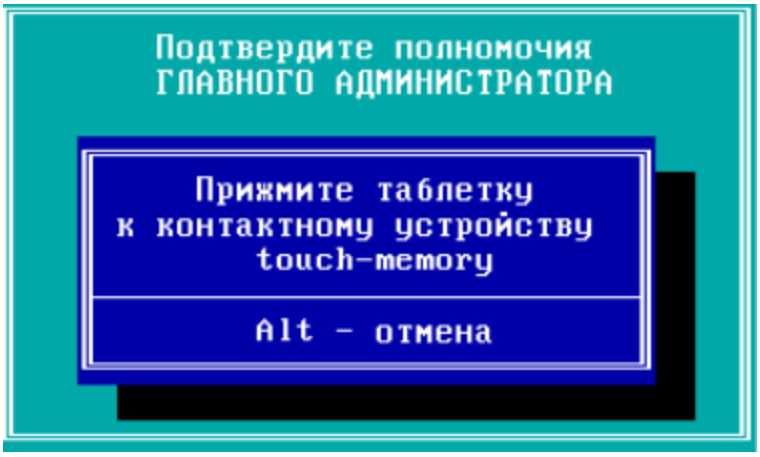

Рисунок 111 - Проверка полномочий Главного администратора

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.

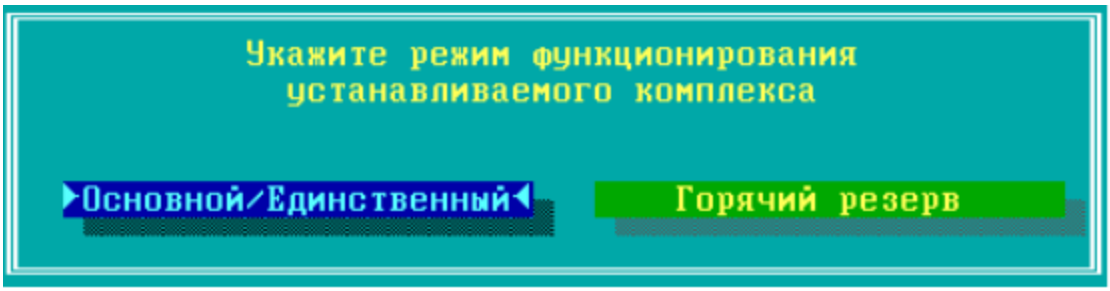

Рисунок 112 - Выбор режима функционирования ФПСУ-TLS

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

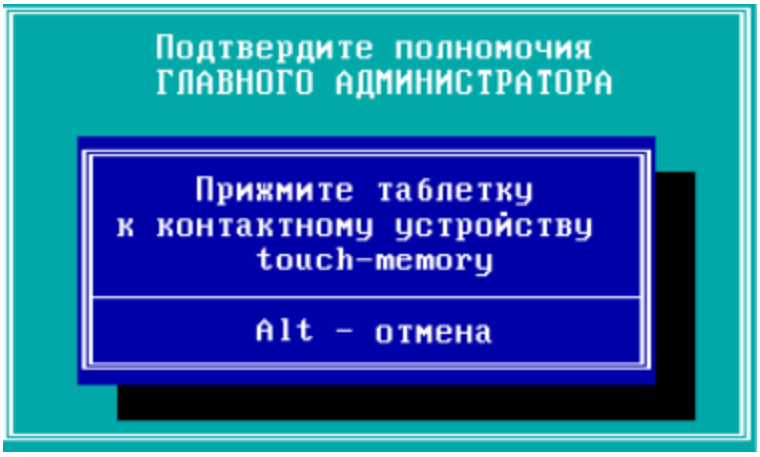

Рисунок 113 - Проверка полномочий Главного администратора

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

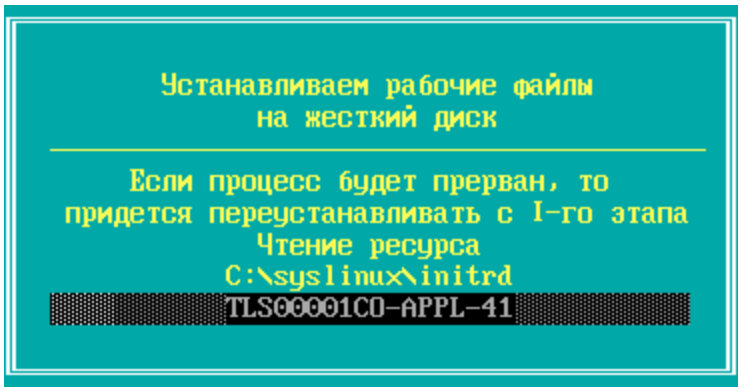

Рисунок 114 - Копирование файлов ФПСУ-TLS на ПЗУ

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).

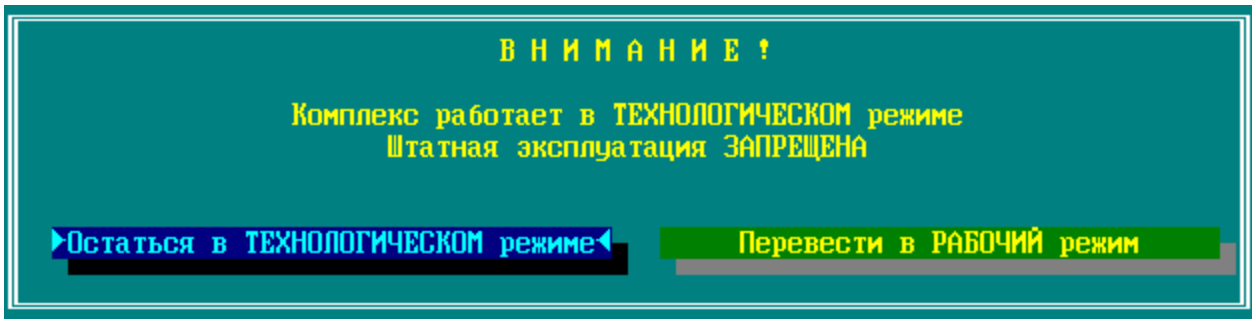

Рисунок 115 - Выбор режима функционирования ФПСУ-TLS

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

14. Для перевода ФПСУ-TLS в рабочий режим требуется инициализировать программно-клавиатурный датчик случайных чисел. От администратора требуется вводить указываемые программой цифры в зависимости от запрашиваемого символа. Дальнейшая работа будет возможна, как только будет осуществлён корректный ввод достаточного количества цифр.

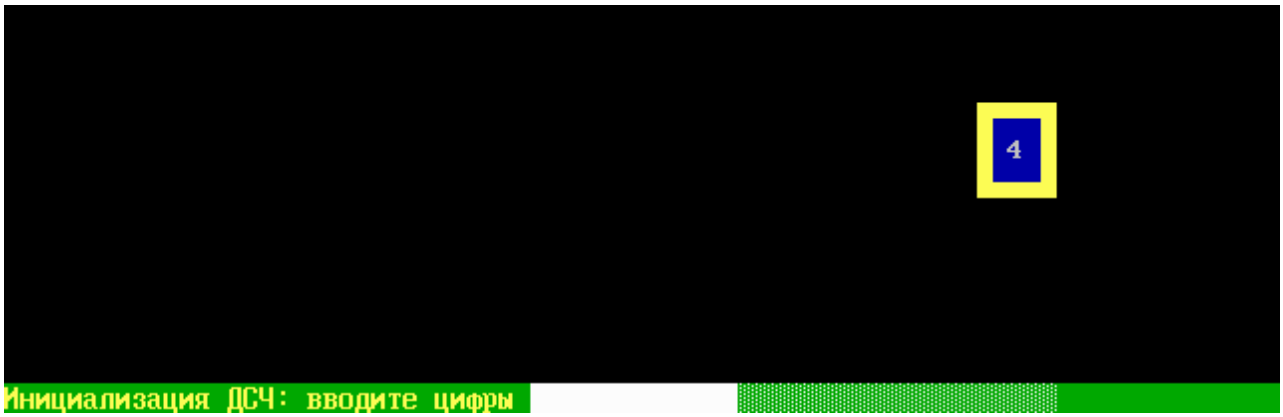

Рисунок 116 - Программно-клавиатурный датчик случайных чисел

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

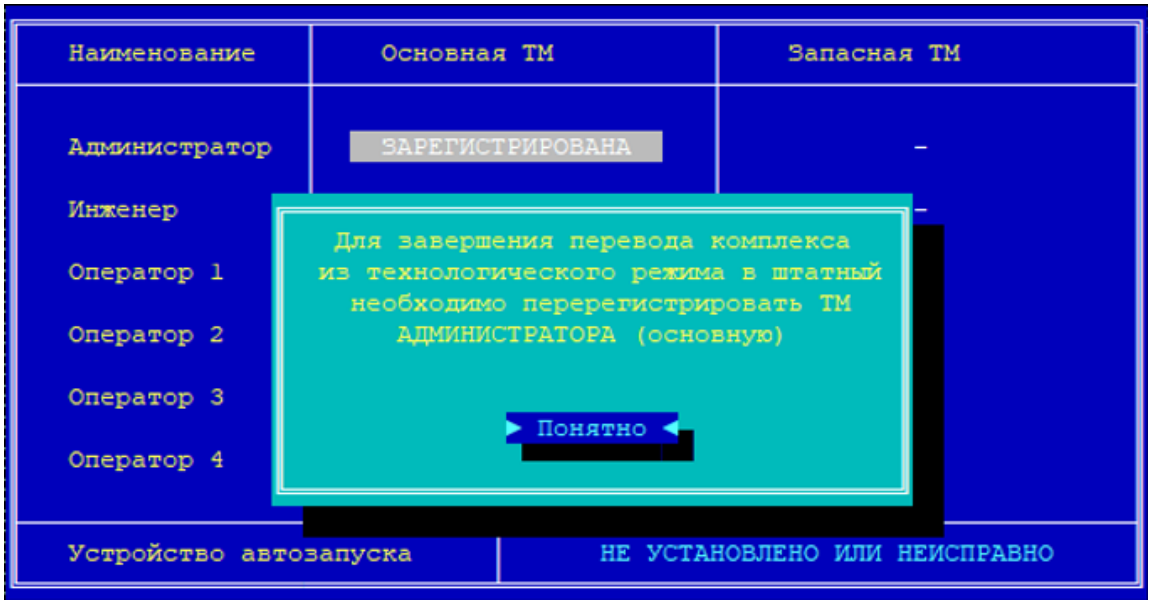

Рисунок 117 - Служебное оповещение о переходе в рабочий режим

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

ТМ-считывателю ФПСУ-TLS.

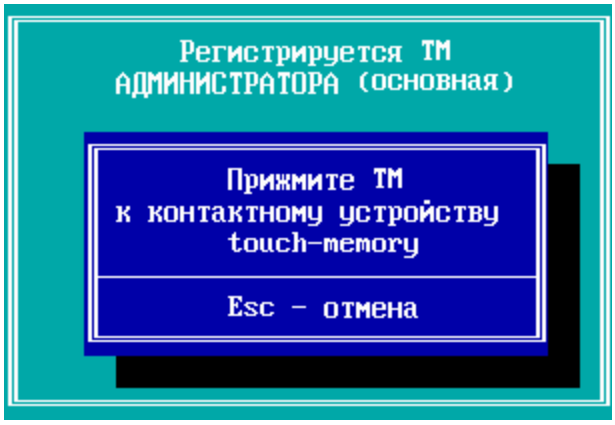

Рисунок 118 - Перерегистрация Главного администратора

17. При успешной перерегистрации ТМ-идентификатора Главного администратора комплекс будет принудительно перезагружен.

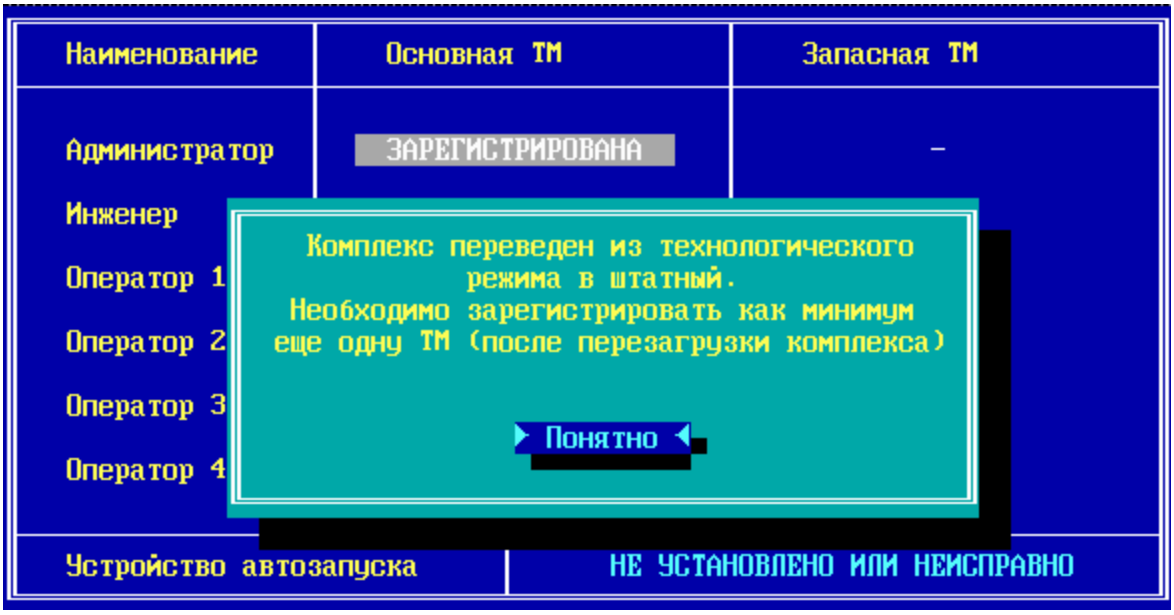

Рисунок 119 - Перезагрузка комплекса

18. Во время перезагрузки необходимо подтвердить права допущенного лица класса Главный администратор, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS:

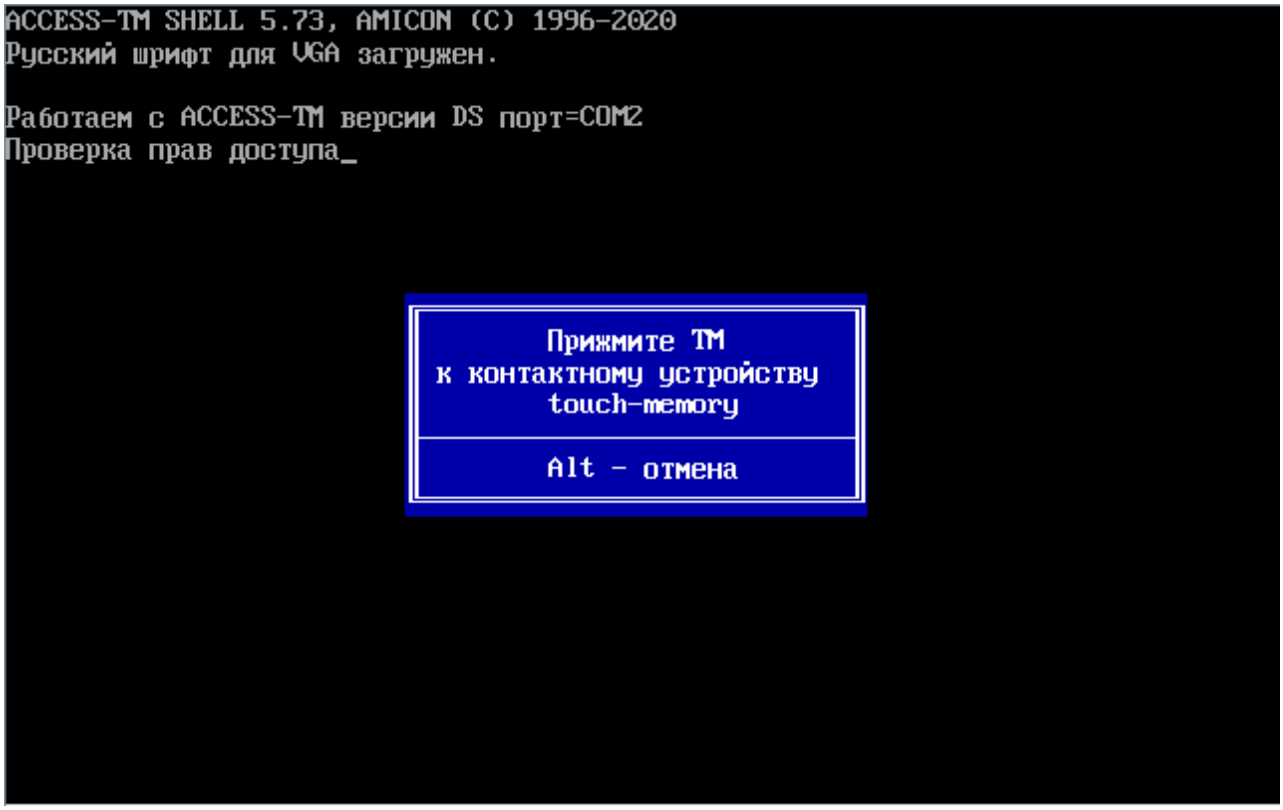

Рисунок 120 - Перезагрузка ФПСУ-TLS

По завершению регистрации TM-идентификатор Главного администратора отображается в таблице TM-идентификаторов в строке «Администратор» в столбце «Основной TM».

Наименование	Основная TM	Запасная TM
Администратор	ЗАРЕГИСТРИРОВАНА	
Инженер	-	-
Оператор 1	-	-
Оператор 2	-	-
Оператор 3	-	-
Оператор 4	-	-
Подсистема автозапуска	НЕ ИСПОЛЬЗУЕТСЯ	

Рисунок 121 - ТМ-идентификатор Главного администратора зарегистрирован

19. Далее зарегистрируйте запасной ТМ-идентификатор администратора. В строке «Администратор» перейдите в столбец «Запасной ТМ» и нажмите <Ins>.

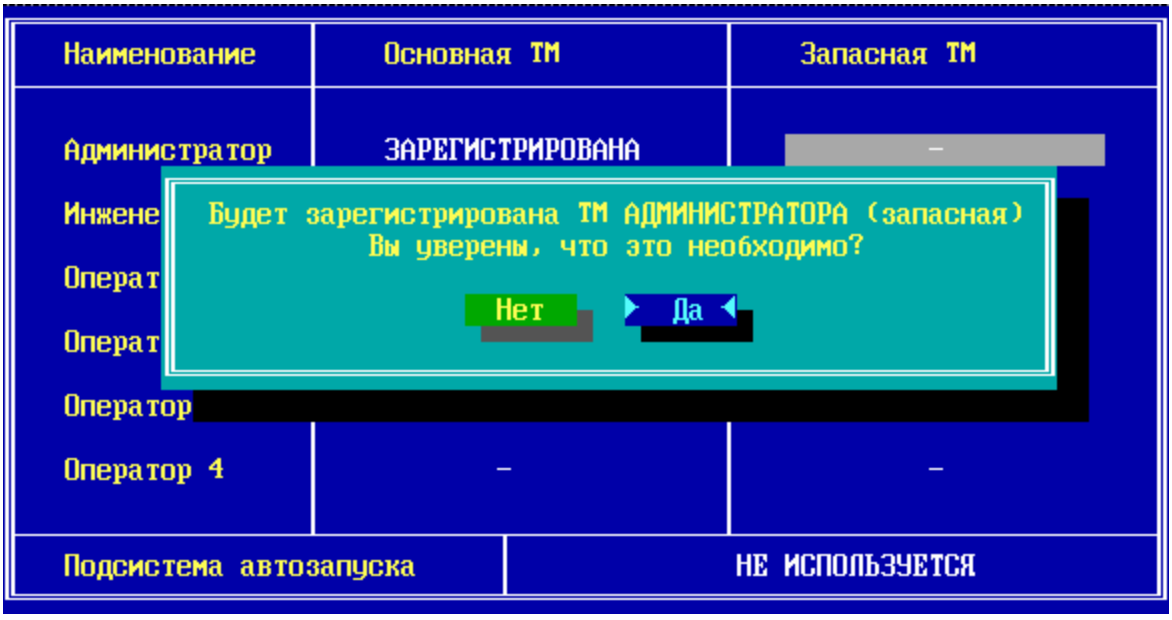

Рисунок 122 - Регистрация запасного ТМ-идентификатора администратора ФПСУ-TLS

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:

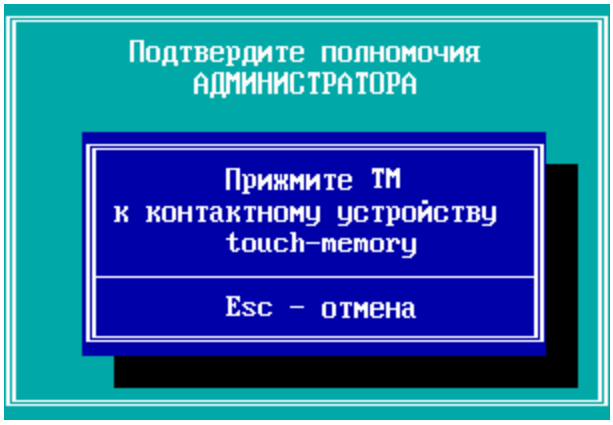

Рисунок 123 - Проверка полномочий Главного администратора

21. Приложите ТМ-идентификатор, на который будет записана ключевая информация запасного ТМ-идентификатора администратора, к ТМ-считывателю ФПСУ-TLS.

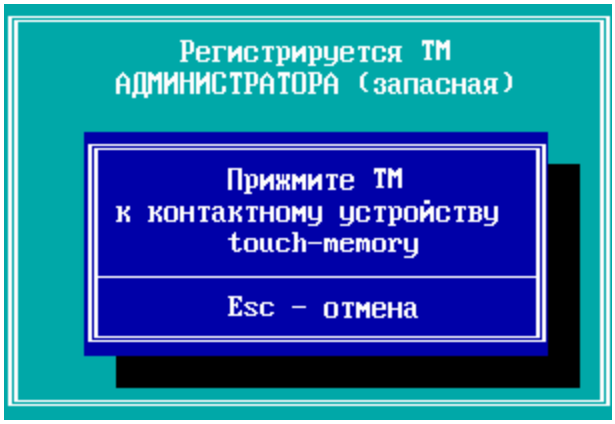

Рисунок 124 - Регистрация запасного ТМ-идентификатора администратора

При успешном завершении регистрации запасной ТМ-идентификатор администратора будет зарегистрирован и отобразится в таблице ТМ-идентификаторов.

Рисунок 125 - 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>.

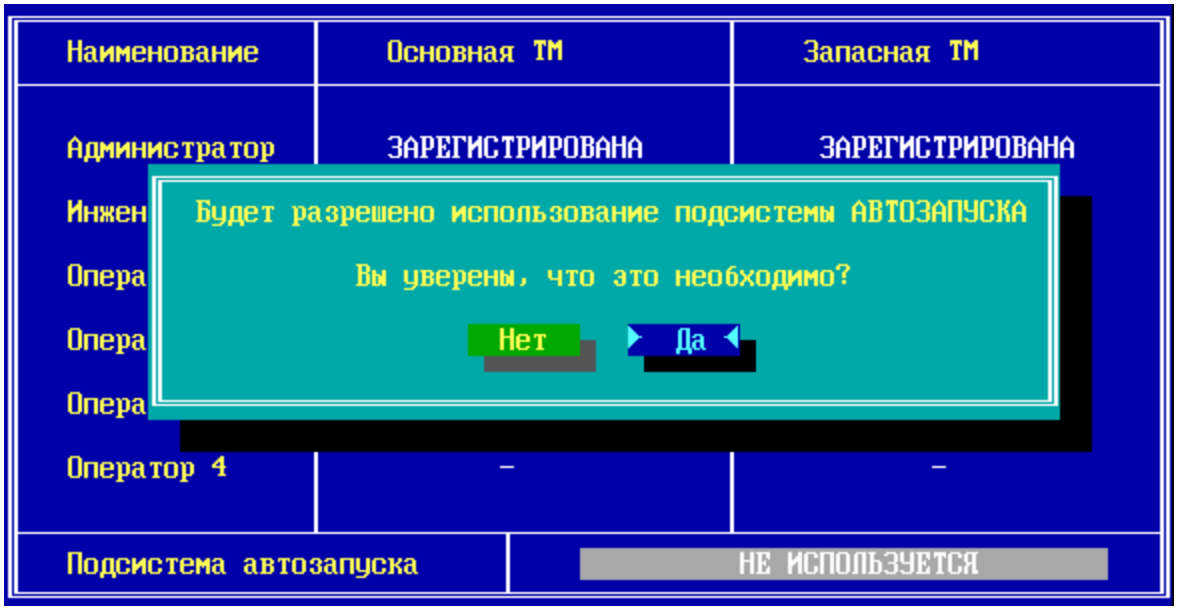

Рисунок 126 - Настройка подсистемы автозапуска

23. Для подтверждения включения подсистемы автозапуска выберите команду «Да» и нажмите <Enter>. Подтвердите права допущенного лица класса Главный администратор, приложив основной ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-TLS.

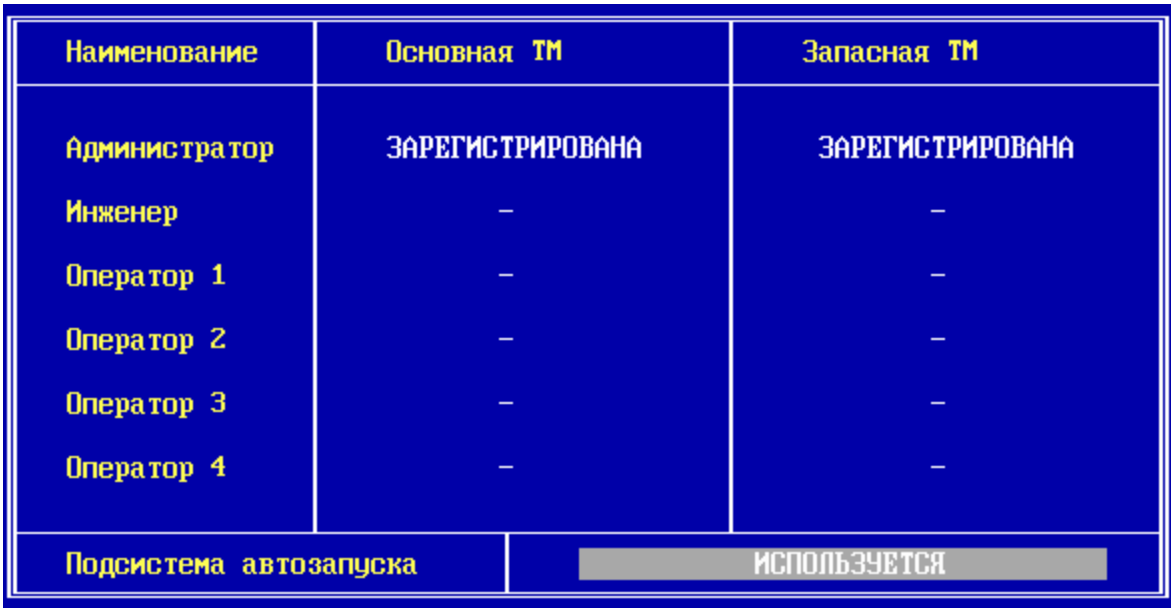

Рисунок 127 - Подсистема автозапуска включена

Выход в основное меню осуществляется по нажатию сочетания клавиш <Alt+X>.

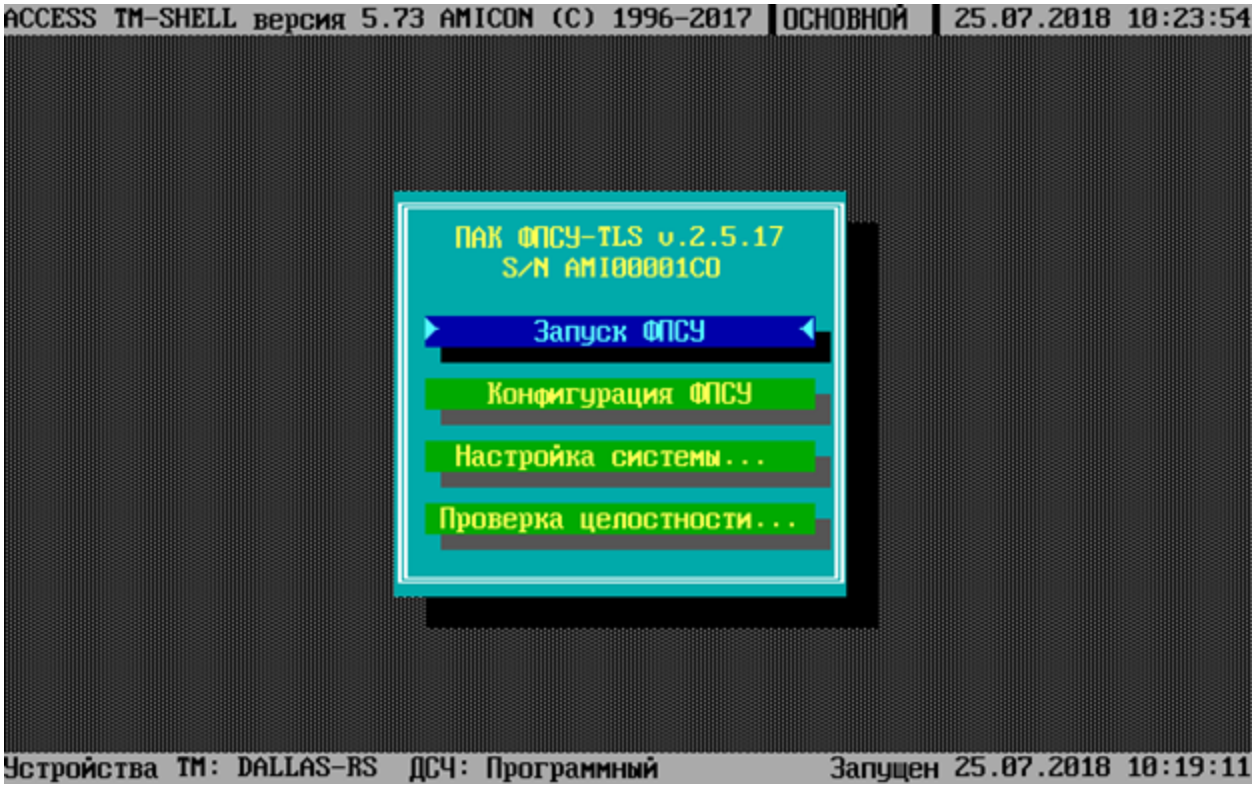

Рисунок 128 - Главное меню ФПСУ-TLS

Переустановка ПО ФПСУ-TLS завершена, ПО запущено в штатном рабочем режиме.