ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.009РП-ЛУ

Центр выработки ключей (версия 4.0.1)

Руководство по применению

ПЕРС.26.20.40.140.009РП

Листов 126

2025

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программных и программно-аппаратных комплексов «ФПСУ». В документе содержатся сведения о программно-аппаратном комплексе «Центр выработки ключей» версии 4.0.1 (код продукта FPSUIP-CVK-KC1, FPSUIP-CVK-KC2 или FPSUIP-CVK-KC3), дано описание последовательности действий в процессе эксплуатации.

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

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

Содержание

1. Список сокращений и определений

БиоДСЧ — биологический датчик случайных чисел;

ОС — операционная система;

ПДСЧ — программный датчик случайных чисел;

ПЗУ — постоянное запоминающее устройство, твердотельный накопитель SSD (solid-state drive);

ПО — программное обеспечение;

СЗИ НСД — средство защиты информации от несанкционированного доступа;

СКЗИ — средство криптографической защиты информации;

ТМ (ТМ-идентификатор) — электронный идентификатор «touch-memory», физическим носителем ТМ-идентификатора является микроэлектронное USB-устройство «TM-Key» производства ООО «АМИКОН» (ПЕРС.466226.004, ПЕРС.466226.005, ПЕРС.466226.008, ПЕРС.466226.009) или микроэлектронное устройство контактной памяти iButton DS-1993 – DS-1996;

ЦВК — программно-аппаратный комплекс «Центр выработки ключей» версии 4.0.1 (код продукта FPSUIP-CVK-КС1, FPSUIP-CVK-КС2 или FPSUIP-CVK-КС3), программная компонента которого является одним из следующих вариантов исполнения СКЗИ «ФПСУ-IP Amigo»: «ЦВК КС1» модификация 4.0.1, «ЦВК КС2» модификация 4.0.1 или «ЦВК КС3» модификация 4.0.1;

ФПСУ (ФПСУ-IP) — криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4 или программно-аппаратный комплекс «ФПСУ-IP» версии 3;

ФПСУ-TLS – комплекс «ФПСУ-TLS» версии 3.1.20, TLS-шлюз, программная компонента которого является средством криптографической защиты информации «ФПСУ-TLS», 11485466.26.20.40.140.031.

2. Общие сведения

Руководство предназначено для работы с программно-аппаратным комплексом «Центр выработки ключей "ФПСУ"» версии 4.0.1 и распространяется на варианты поставки изделия FPSUIP-CVK-KC1, FPSUIP-CVK-KC2 или FPSUIP-CVK-KC3.

Программно-аппаратный комплекс «Центр выработки ключей "ФПСУ"» версии 4.0.1 предназначен для выработки парно-выборочных ключей, используемых ФПСУ в процессе взаимной аутентификации для организации защищенного туннеля передачи данных абонентов защищаемых фрагментов IP-сети.

Созданные ЦВК ключи выдаются на отчуждаемый носитель. В качестве носителя может выступать устройство USB-flash, SD- или MicroSD карта объемом до 32 Гб, подключаемая к ЦВК через USB-кардридер.

Ключи с носителя устанавливаются на ФПСУ локальными администраторами каждого ФПСУ, или удаленными администраторами.

Каждому ЦВК в процессе изготовления присваивается уникальный идентификатор из 6 символов.

ЦВК поставляется в соответствии с формуляром на модификации 4.0.1 вариантов исполнения «ЦВК КС1», «ЦВК КС2» или «ЦВК КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

ЦВК должен использоваться в соответствии с правилами пользования модификациями 4.0.1 вариантов исполнения «ЦВК КС1», «ЦВК КС2» или «ЦВК КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

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

СКЗИ «ФПСУ-IP Amigo» разработано ООО «АМИКОН».

СКЗИ «ФПСУ-IP Amigo» удовлетворяет:

- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для классов КС1, КС2 и КС3 в соответствии со следующей таблицей:

Класс	**Вариант исполнения**
КС1	«ЦВК КС1»
КС2	«ЦВК КС2»
КС3	«ЦВК КС3»

- «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)» по уровню $КС_{Б}$;

- «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_{Б}$.

3. Разграничение доступа и пользователи

Программное обеспечение ЦВК функционирует в собственной изолированной и функционально замкнутой операционной среде, ACCESS-TM SHELL. Среда осуществляет разграничение доступа к операционной системе ЦВК, защиту программных и информационных модулей на ПЗУ комплекса. ЦВК предлагает диалоговые средства для управления своей работой, а также для установки параметров работы.

Разграничение доступа допущенных лиц и контроль их полномочий при запуске ЦВК и управлении его работой осуществляется подсистемой ACCESS-TM SHELL по предъявляемым допущенными лицами электронным идентификаторам «touch-memory» (в качестве которых могут выступать микроэлектронные USB-устройства «TM-Key» производства ООО «АМИКОН» или устройства iButton DS1993 – DS1996) и символьному паролю (подробнее про пароли см. пункт «Окно регистрации ТМ»). Доступ выдается в соответствии с логическим разделением допущенных к управлению ЦВК лиц на четыре условных класса, представленных в таблице ниже.

Все допущенные к ЦВК лица являются администраторами СКЗИ.

Таблица 1. Роли и классы пользователей ЦВК

Класс	**Разрешенные действия**
Оператор	• запуск ЦВК - команда главного меню; • запуск ЦВК - авторизация в BIOS после холодного старта; • переинициализация ПСДЧ; • удаление лицензии; • удаление центра; • экспорт центра ЦВК; • импорт центра ЦВК; • генерация новой серии ключевых данных; • выдача ключа ПДСЧ.

Класс	**Разрешенные действия**
Инженер	Все права класса «Оператор» и дополнительно: • контроль целостности без записи результатов.
Администратор	Все права класса «Инженер» и дополнительно: • вход в пункт меню «Регистрация ТМ»; • установка пароля ТМ-идентификатора; • регистрация и удаление ТМ-идентификатора Администратора, Инженера, Оператора; • установка дополнений/изменений; • контроль целостности с записью результатов/по внешнему списку; • установка срока действия ключа запуска и ключа ПДСЧ.
Главный администратор	Все права класса «Администратор» и дополнительно: • переустановка программного обеспечения ЦВК со специального средства восстановления (USB-носителя).

Внимание! Устройство автозапуска (Включение/отключение подсистемы автоматического старта) не может быть задействовано на ЦВК, всегда находится в состоянии отключено.

4. Применимость руководства

Руководство предназначено для работы с версией 4.0.1 программного обеспечения ЦВК и распространяется на следующие указанные в таблице варианты поставки изделия и дополнительные программные модули:

Таблица 2. Варианты изделия

Код варианта изделия	**Наименование варианта изделия/дополнительного программного модуля**
FPSUIP-CVK-KC1	Программно-аппаратный комплекс «Центр выработки ключей» КС1
FPSUIP-CVK-KC2	Программно-аппаратный комплекс «Центр выработки ключей» КС2
FPSUIP-CVK-KC3	Программно-аппаратный комплекс «Центр выработки ключей» КС3

Примечание. Программно-аппаратный комплекс «Центр выработки ключей» КС1/КС2/КС3 поставляется на аппаратных платформах FPSUIP-ORD3v2 или FPSUIP-ORD4v2.

5. Условия эксплуатации и гарантийные обязательства

5. 1. Условия эксплуатации

Электропитание основных технических средств комплекса в процессе эксплуатации должно осуществляться от источников гарантированного питания, обеспечивающих автоматический переход на резервные источники при выходе из строя основной энергосистемы, а также фильтрацию от электропомех питающей сети. Напряжение в сети переменного тока должно быть 220 В ± 10%, частота тока 50 Гц ± 1%, качество электрической энергии должно соответствовать ГОСТ Р 54149.

Запрещается эксплуатация основных технических средств комплекса с неисправным шнуром питания, использование поврежденных розеток, сетевых фильтров и адаптеров.

Аппаратные средства комплекса должны размещаться в охраняемых помещениях с ограниченным доступом.

Аппаратная часть ЦВК по воздействию климатических факторов относится к 1 группе стойкости к воздействию внешних климатических факторов в процессе эксплуатации согласно ГОСТ 21552-84, и предназначена для установки в отапливаемых помещениях.

Нормальными климатическими условиями эксплуатации аппаратной части комплекса являются:

- температура окружающего воздуха - 20°(±15°) С;
- относительная влажность окружающего воздуха - 60 (±15)%;
- атмосферное давление - от 84 до 107 кПа (630–800 мм рт. ст.);
- запыленность воздуха - не более 0,75 мг/м³;
- в воздухе не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

Допускается эксплуатация ЦВК на базе аппаратной платформы FPSUIP-CVK-KC1, FPSUIP-CVK-KC2, FPSUIP-CVK-KC3 при следующих изменениях нормальных климатических условий:

- температура окружающего воздуха – от 0°С до 40°С;

- относительная влажность окружающего воздуха – от 0% до 90% (без конденсата).

Условия хранения:

- до ввода в эксплуатацию аппаратные средства комплекса должны храниться в отапливаемых помещениях при температуре воздуха от 5°С до 40°С и относительной влажности не более 80%;
- в помещениях для хранения не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

5. 2. Гарантийные обязательства

Гарантийный срок службы ЦВК указывается в паспорте на изделие.

Гарантия не распространяется на изделия, вышедшие из строя:

- по вине его владельца вследствие нарушения условий эксплуатации и/или хранения;
- из-за неправильной эксплуатации или применения в целях, не предусмотренных функциональным назначением устройства;
- из-за несоблюдения указаний, приведенных в данном документе или возникшие в результате воздействия окружающей среды (дождь, снег, град, гроза и т. п.);
- наступления форс-мажорных обстоятельств (пожар, наводнение, землетрясение и др.);
- из-за небрежного обращения и дефектов, вызванных попаданием внутрь аппаратного обеспечения посторонних предметов, веществ, жидкостей, насекомых и т. д.;
- при наличии механических внешних дефектов (явные механические повреждения, трещины, сколы на корпусе или внутри устройства, сломанные контакты разъемов);
- в случае ремонта оборудования неуполномоченными лицами.

6. Консольное подключение к ЦВК

Локальное управление ЦВК осуществляется от рабочей станции под управлением ОС Windows с помощью консольного подключения через COM-порт с помощью консольного кабеля. При этом должны выполняться требования к Терминалу, изложенные в правилах пользования на модификацию 4.0.1 вариантов исполнения «ЦВК КС1», «ЦВК КС2» или «ЦВК КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

Консольный кабель для RJ45 интерфейса входит в комплект поставки изделия.

Рисунок 1 - Консольный кабель для RJ45 интерфейса

Для консольного подключения к ЦВК, осуществляемого с Windows-станций, используется программа PuTTY сборки ООО «АМИКОН» (Далее - «Терминал»). «Терминал» можно скачать с официального сайта ООО «АМИКОН». Кроме того, «Терминал» может быть поставлен по запросу.

Подключите кабель к рабочей станции, с которой будет выполняться консольное соединение.

Скачайте с официального сайта ООО «АМИКОН» https://amicon.ru/download.php драйвер для подключения консоли к ФПСУ для вашей версии операционной системы Windows.

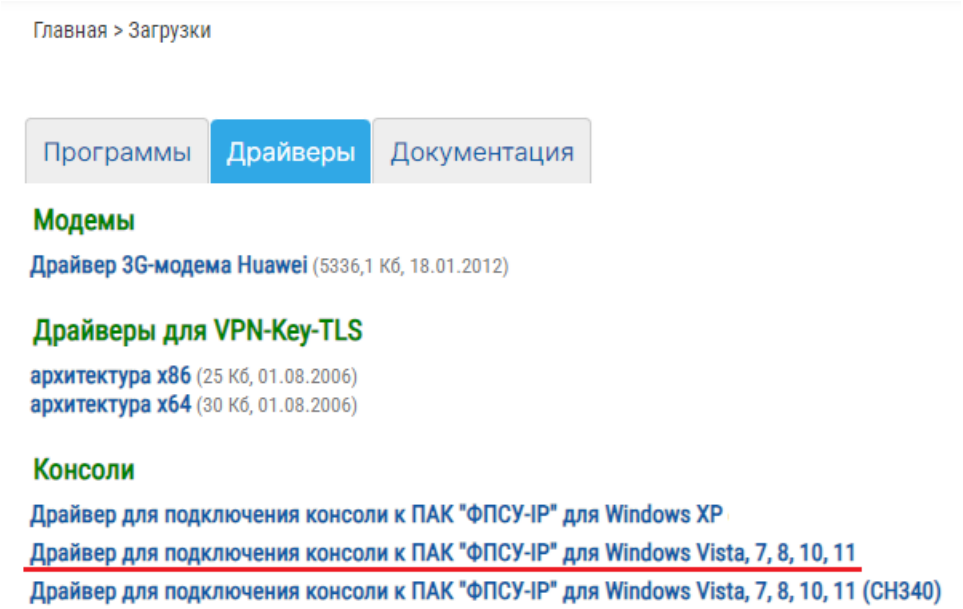

Рисунок 2 - Ссылка на скачивание

Установите драйвер кабеля в ОС рабочей станции и проверьте правильно ли консольный кабель обнаруживается в диспетчере устройств операционной системы.

Для этого:

Загрузите и распакуйте архив с файлами драйвера в отдельный каталог.

В диспетчере устройств (mmc > devmgmt.msc) выделите неопознанное устройство FT232R USB UART и по нажатию правой кнопки мыши в контекстном меню выберите пункт «Обновить драйвер для этого устройства».

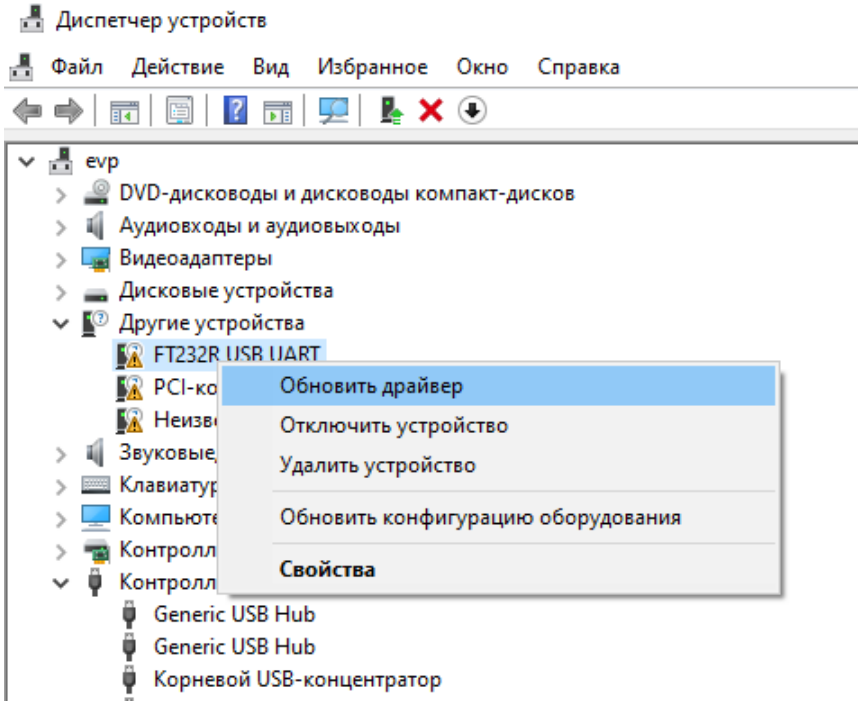

Рисунок 3 - Первое подключение консольного кабеля

В диалоговом окне мастера установки выберите поиск драйверов на этом компьютере и укажите каталог с драйвером. Система установит драйвер и выдаст сообщение об успешном обновлении. После успешной установки драйвера консольный кабель должен обнаруживаться системой как «USB Serial Port» в группе устройств «Порты (COM и LPT)».

Уточните номер COM-порта, зарегистрированного операционной системой для этого последовательного соединения в диспетчере устройств (на рисунке ниже - это COM4). Этот номер потребуется указать в «Терминале» при настройке подключения.

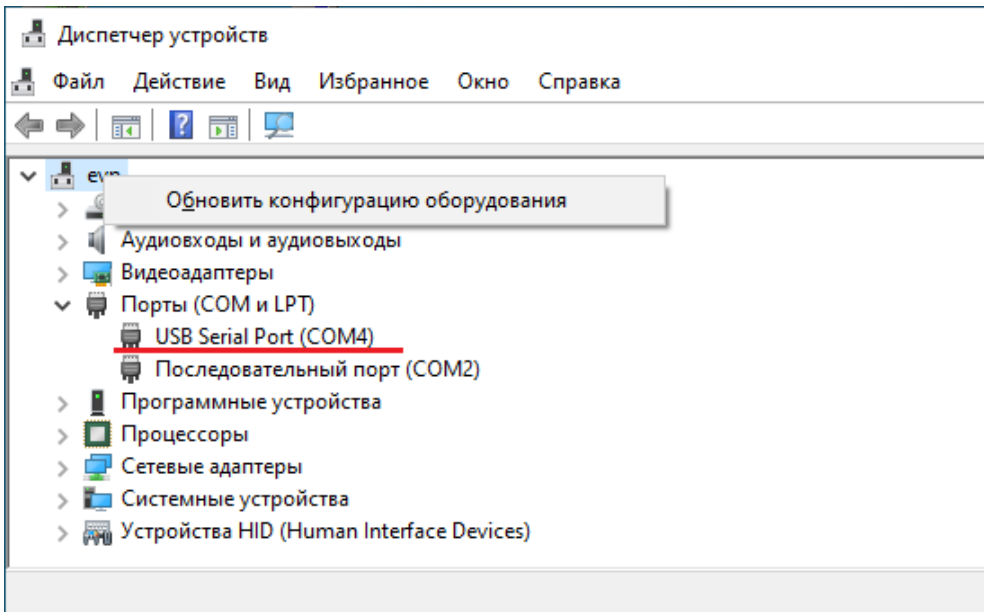

Рисунок 4 - COM порт консольного соединения в диспетчере устройств

«Терминал» доступен для загрузки с официального сайта ООО «АМИКОН» https://amicon.ru/download.php, ссылка с архивом «Терминала» имеет название «ФПСУ-терминал для Windows».

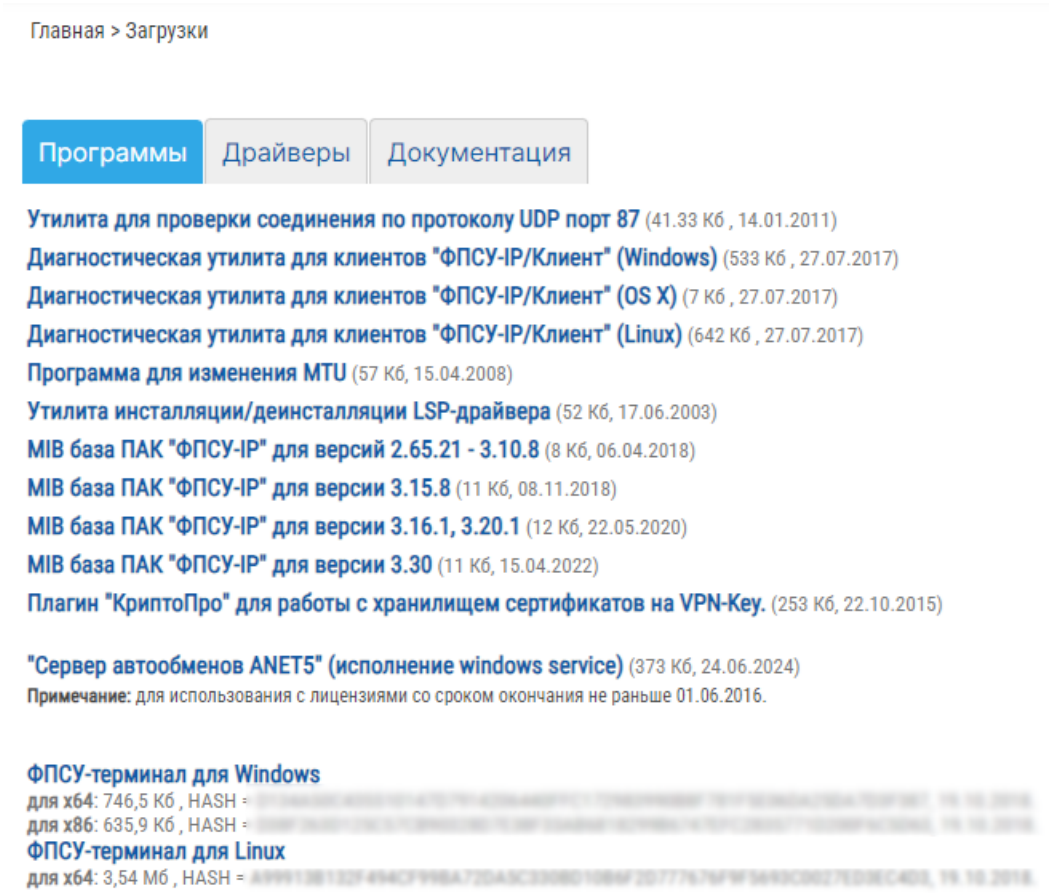

Рисунок 5 - Ссылка для скачивания

Загрузите и распакуйте архив с файлами в отдельный каталог. Запустите исполняемый файл «Терминала», PuTTY.exe, и установите указанные ниже настройки.

Выберите тип подключения Serial, укажите номер COM-порта (в примере это COM4), установите скорость (Speed) - 115200, для сохранения настроек задайте название подключения и нажмите «Save».

Примечание. В случае, если консольный кабель не переподключался к рабочей станции, при следующем подключении достаточно выбрать подключение из списка сохраненных и нажать «Load».

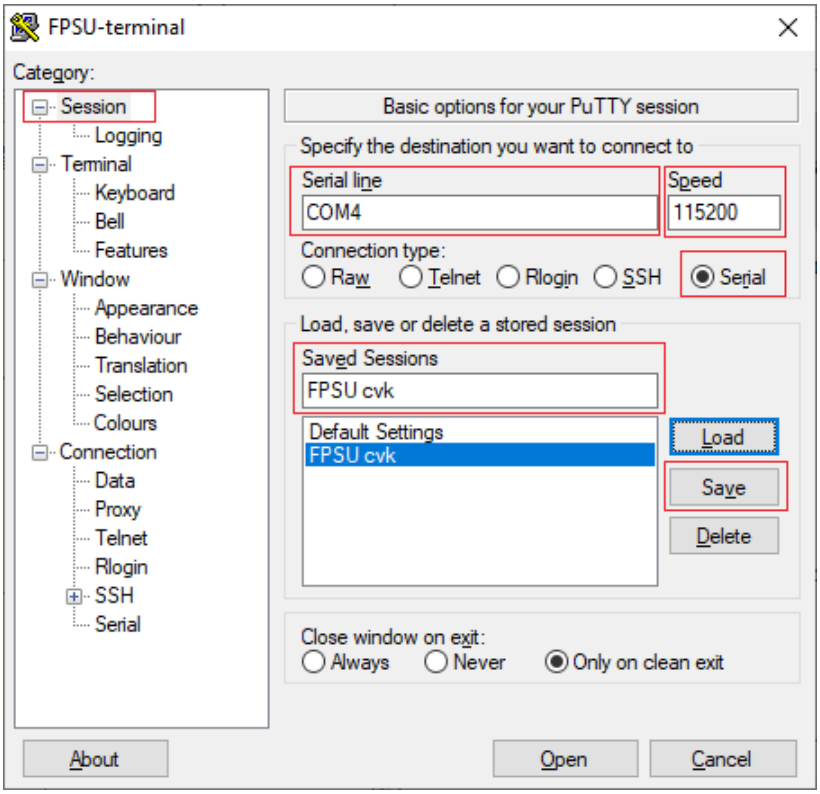

Рисунок 6 - Настройка подключения

Укажите тип используемой в терминальном соединении клавиатуры - Xterm R6 (выставляется в интерфейсе «Терминала»: Terminal-Keyboard-The Function keys and keypad).

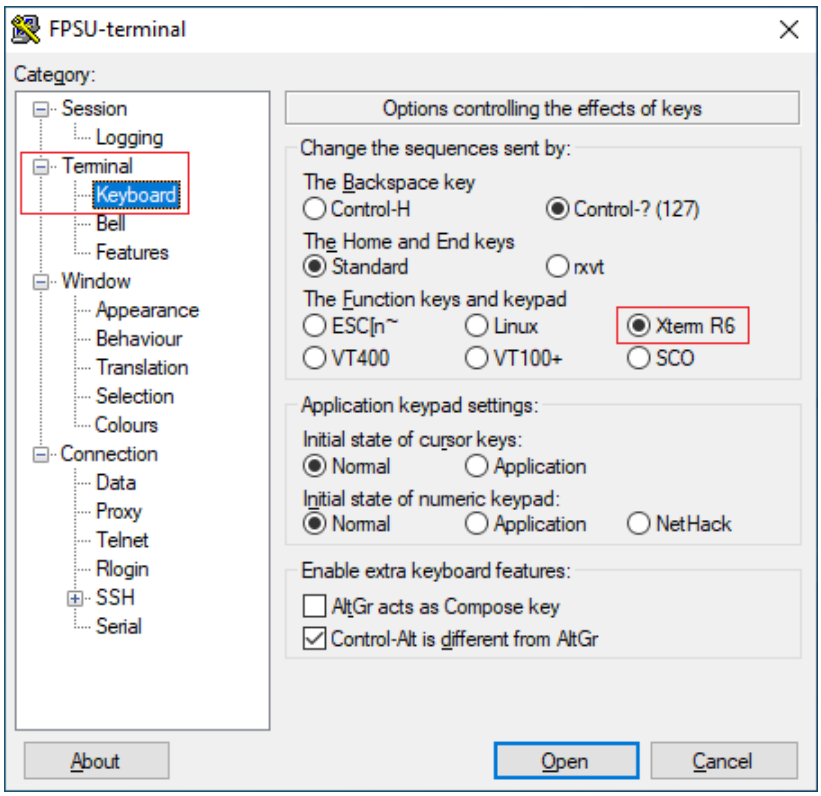

Рисунок 7 - Выбор типа клавиатуры

Выберите кодировку UTF-8 (выставляется в интерфейсе «Терминала»: Window-Translation-Remote Character Set).

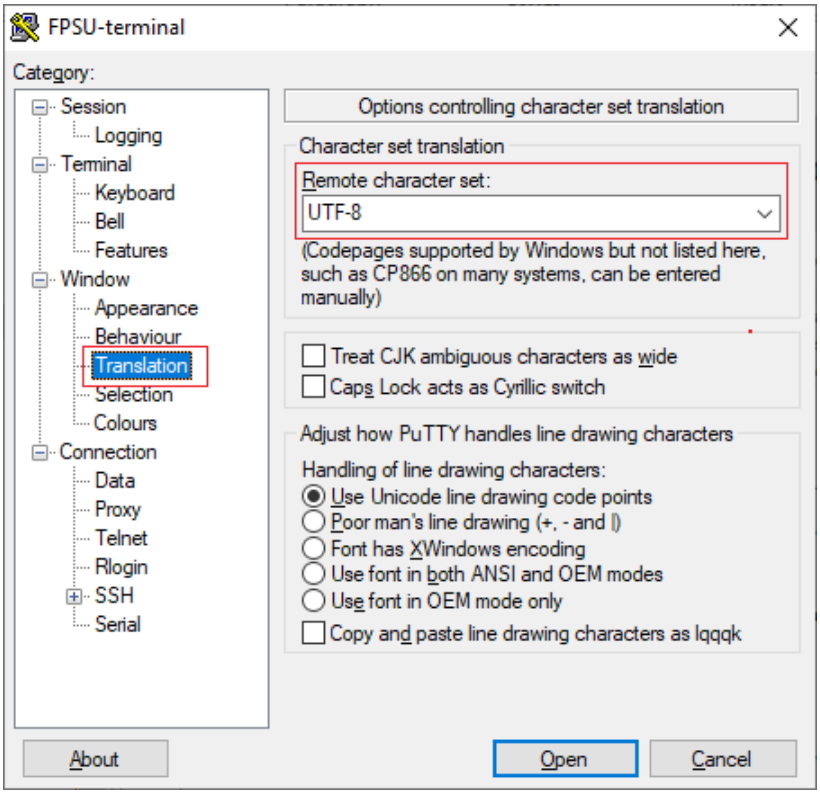

Рисунок 8 - Выбор кодировки

Задайте количество строк – 25 (выставляется в интерфейсе «Терминала»: Window–Rows).

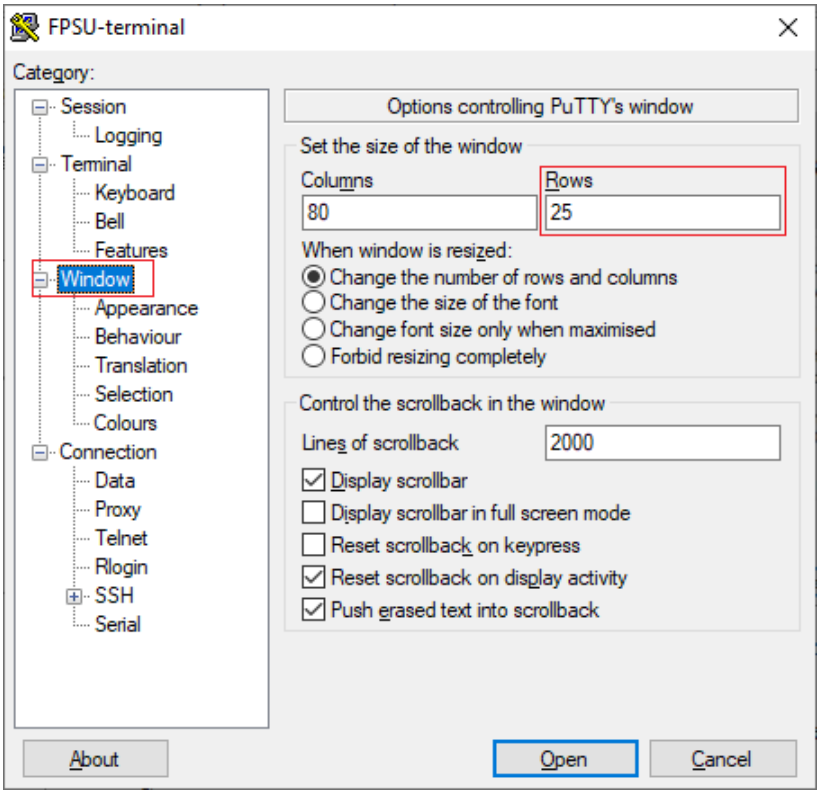

Рисунок 9 - Выбор количества строк

Запустите установку соединения с ЦВК из «Терминала», нажав «Open».

Подключите консольный кабель к консольному порту ЦВК и включите питание ЦВК.

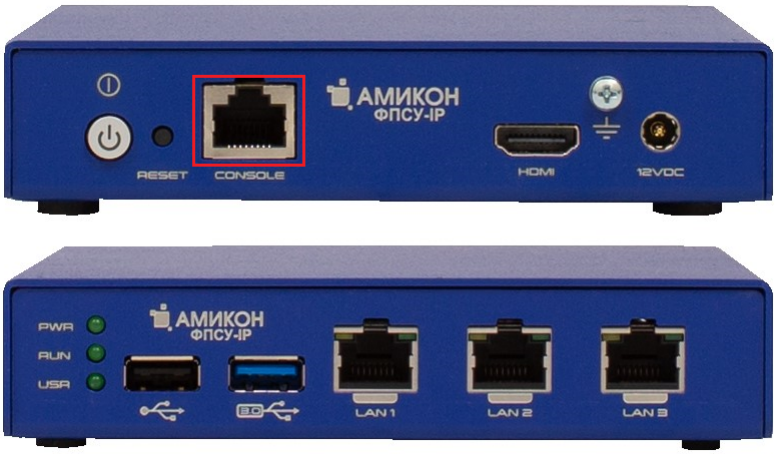

Рисунок 10 - Консольный порт ЦВК

На экране рабочей станции в окне «Терминала» отобразится главное

меню ЦВК.

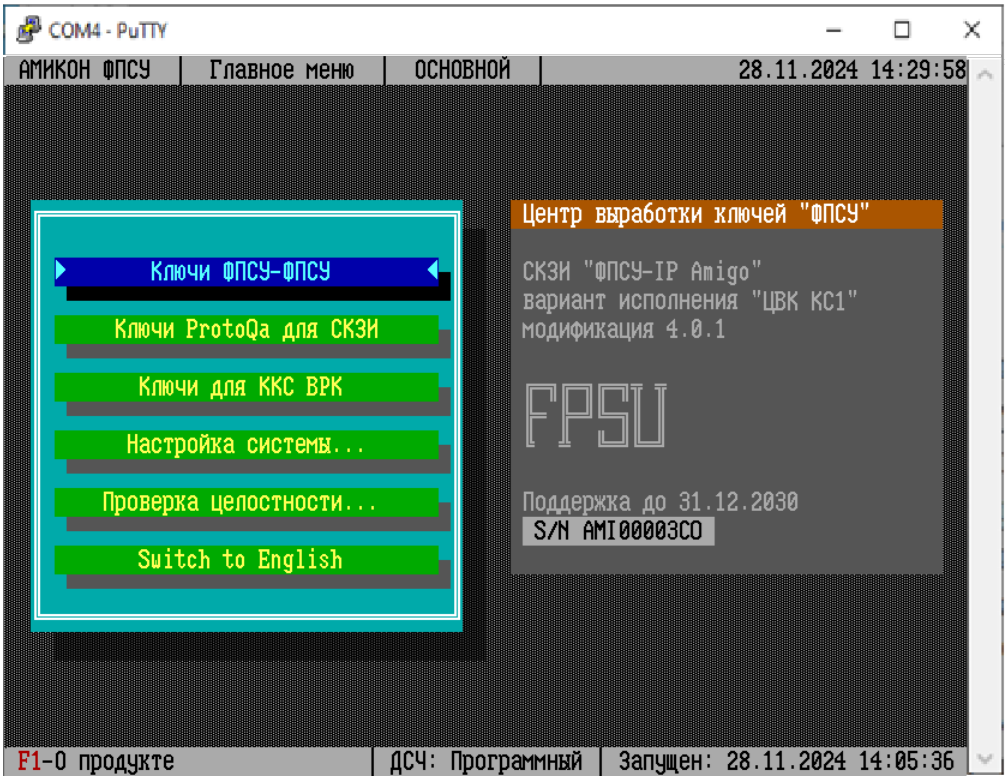

Рисунок 11 - Консольное подключение установлено

7. Запуск и настройка параметров работы ЦВК

ЦВК поставляется с установленным программным обеспечением, готовым к эксплуатации.

После подключения питания, прохождения диагностических тестов BIOS и запуска загрузчика операционной системы, на консоль будет выдан запрос на подтверждение права доступа пользователя к работе с ЦВК. Для продолжения требуется подключить ТМ-идентификатор Главного администратора к USB-порту ЦВК.

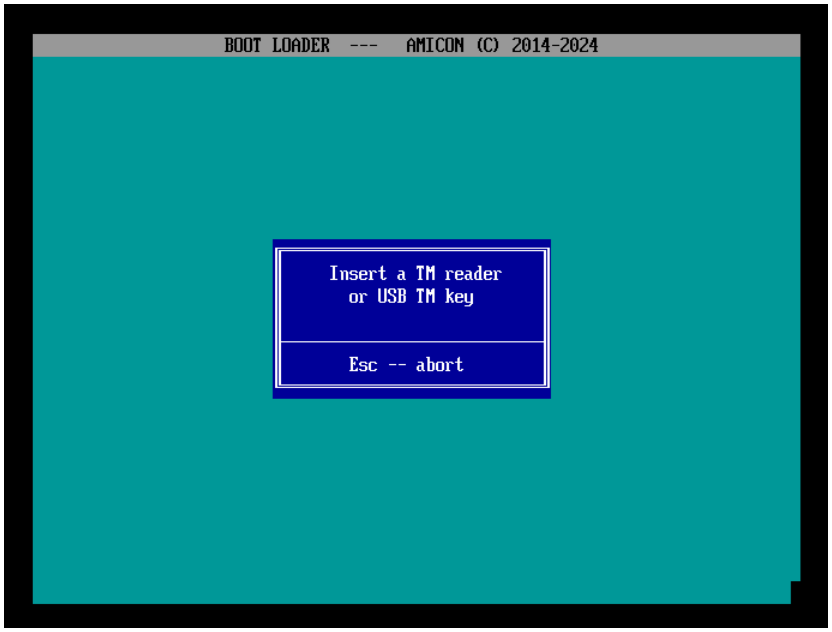

Рисунок 12 - Загрузка ЦВК

В случае успешной идентификации загрузка ЦВК продолжится. ПО ЦВК будет загружено, выдав на экран главное меню, содержащее следующие команды:

Рисунок 13 - Главное меню ЦВК

«**Ключи ФПСУ-ФПСУ**» – переход к интерфейсу генерации ключевых данных зарегистрированных на ЦВК криптосетей ФПСУ, подробнее см. пункт «Генерация и выдача ключевых данных».

«**Ключи ProtoQa для СКЗИ**» – переход к интерфейсу генерации ключевых данных СКЗИ-Потребителей, подробнее см. пункт «Ключи ProtoQa для СКЗИ».

«**Ключи для ККС ВРК**» – переход к интерфейсу генерации ключевых данных для ККС ВРК, подробнее см. пункт «Ключи для ККС ВРК».

«**Настройка системы**» – переход в окно настроек системы, подробнее см. пункты «Окно регистрации ТМ», «Установка дополнений», «Переинициализация ПДСЧ».

«**Проверка целостности**» – переход в окно запуска проверок целостности программного обеспечения ЦВК, подробнее см. пункт «Контроль целостности программного обеспечения».

«**Switch to English /Переключиться на Русский**» – смена языка в интерфейсе.

Навигация по интерфейсу ЦВК осуществляется следующим образом:

- Переход по командам меню задействуется стрелками вверх, вниз.

- Выбор команды меню или подменю осуществляется по нажатию <Enter>.
- Возврат к предыдущему окну происходит по нажатию <Esc>, либо комбинацией клавиш <Alt>+<X>.
- Переход по кнопкам в диалоговых окнах происходит по нажатию <Tab>, либо клавишами вправо, влево.
- При работе в окнах, внизу окна отображается контекстная подсказка с комбинациями клавиш.
- По нажатию <F1> можно вызвать контекстную справку, там где она доступна.

При нажатии клавиши <F1> выводится дополнительное окно со справочной информацией об изготовителе изделия, версии ЦВК, установленном обновлении.

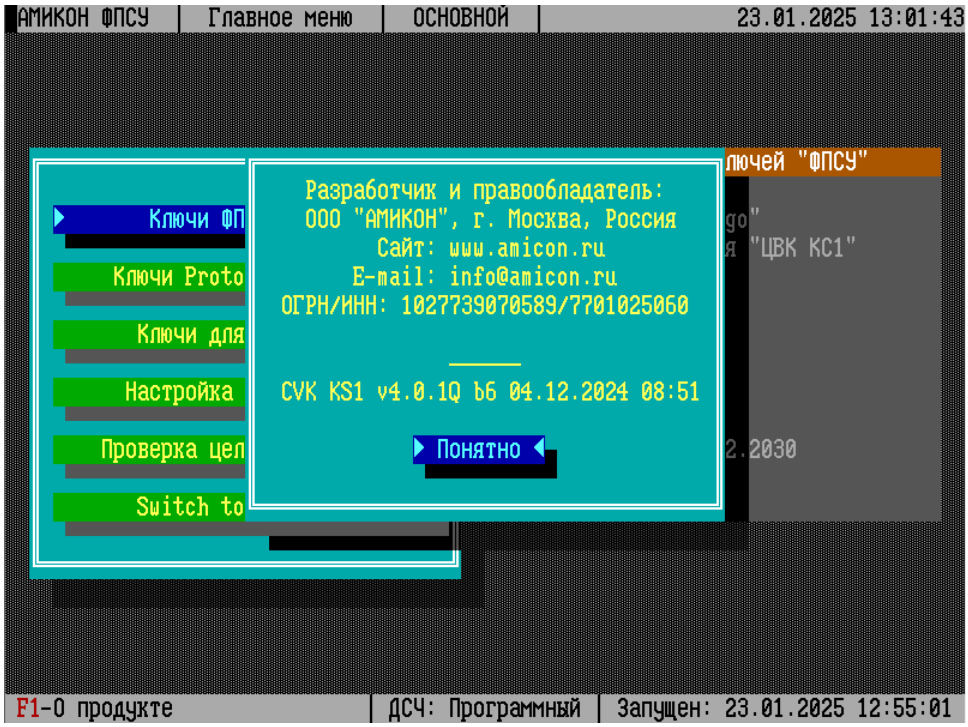

Рисунок 14 - Главное меню ЦВК

Подменю главного меню «Настройка системы» предназначено для перехода в интерфейс установки параметров и режимов работы с обслуживающими подсистемами ЦВК: подсистемой разграничения доступа и учета ТМ-идентификаторов, установки дополнений и изменений ПО ЦВК, повторной инициализации датчика случайных чисел.

Рисунок 15 - Меню настройки системы ЦВК

7. 1. Окно регистрации ТМ

Команда подменю Регистрация ТМ (ТМ-идентификаторов) предназначена для:

- регистрации и перерегистрации ТМ-идентификаторов администраторов ЦВК;
- управления паролями для учетных записей администраторов ЦВК;
- удаления записанной на потерявших актуальность или скомпрометированных ТМ-идентификаторах ключевой информации;
- проверки ТМ-идентификаторов на исправность и корректности хранимой в них информации.

Операция доступна администраторам класса «Администратор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

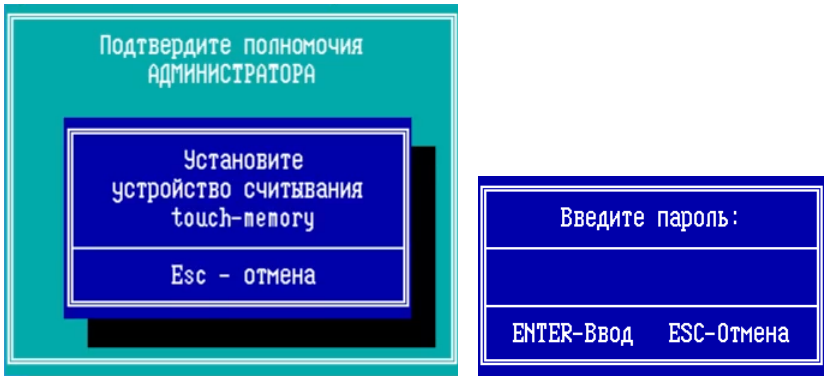

Рисунок 16 - Подтверждение полномочий и ввод пароля ТМ

После ввода пароля ТМ на экране появится таблица, показывающая наличие зарегистрированных на ЦВК ТМ-идентификаторов.

Для зарегистрированных ТМ-идентификаторов могут быть осуществлены следующие операции:

- ТМ-идентификатор Главного Администратора, может быть только проверен;
- остальные ТМ-идентификаторы – проверены, очищены (удалены) или повторно зарегистрированы, с новой ключевой информацией;
- для каждого ТМ-идентификатора может быть задан пароль.

Разрешенные для текущей записи действия выполняются при помощи клавиш, указанных в динамически меняющейся строке подсказки в нижней части экрана.

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

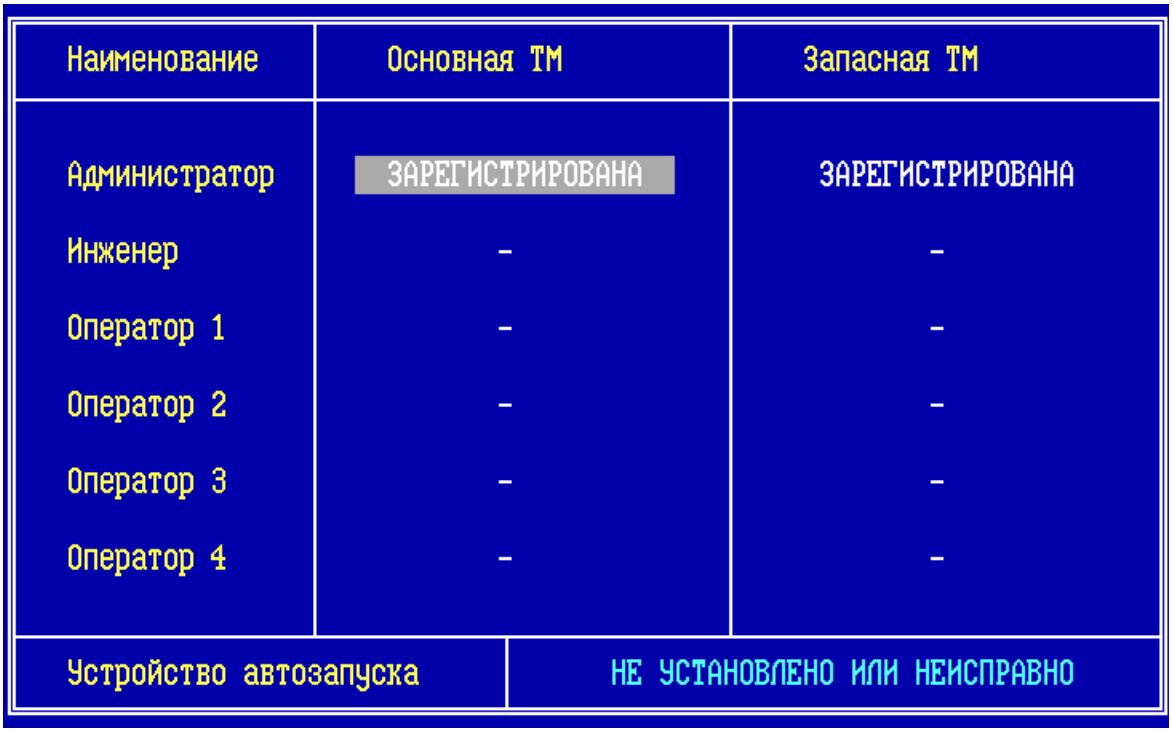

Рисунок 17 - Меню регистрации ТМ-идентификаторов администраторов ЦВК

Новый ТМ-идентификатор может быть только зарегистрирован как запасной для строки «Администратор» или основной/запасной для любого другого класса пользователей.

ТМ-идентификатор Главного Администратора зарегистрирован быть не может, он перерегистрируется только при повторной инсталляции ПО ЦВК, и только на ТМ-идентификатор, поставляемый вместе с дистрибутивом ЦВК и маркированный как ТМ-идентификатор Главного Администратора.

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

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ЦВК классов КС2 и КС3, и опциональным для ЦВК класса КС1.

Пароль основного ТМ-идентификатора выбранного класса администратора задается в окне регистрации ТМ (см. пункт «Установка пароля

Главного администратора»), пароль запасного ТМ-идентификатора выбранного класса администратора задается при перерегистрации ТМ (см. пункт «Регистрация запасного ТМ»).

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

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

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

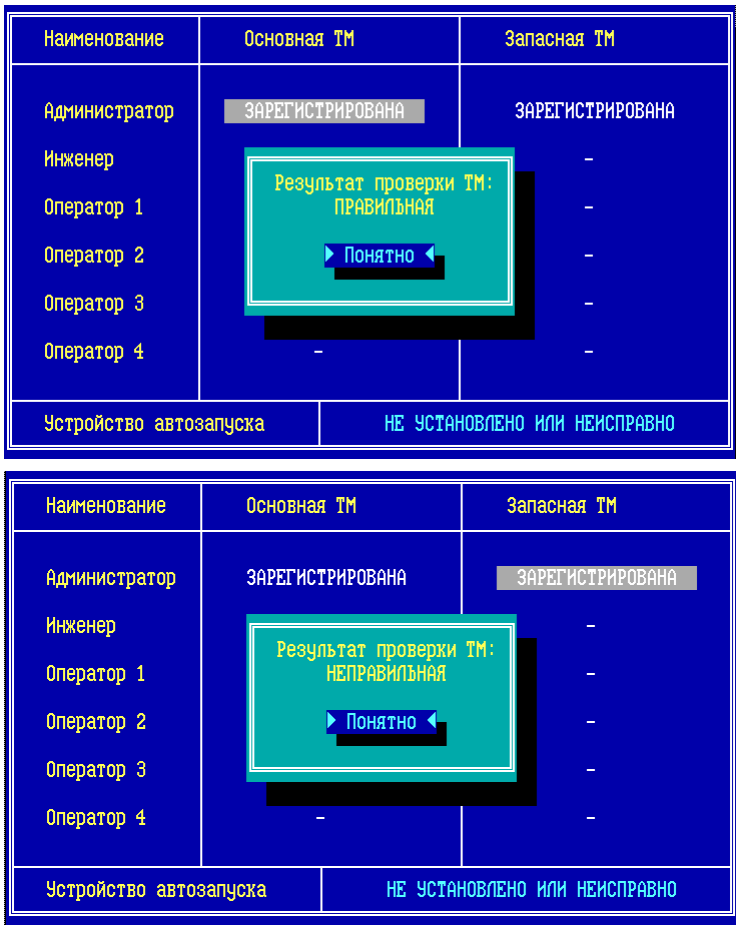

Рисунок 18 - Проверка ТМ-идентификатора администратора ЦВК

7. 1. 1. Установка пароля Главного администратора

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

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

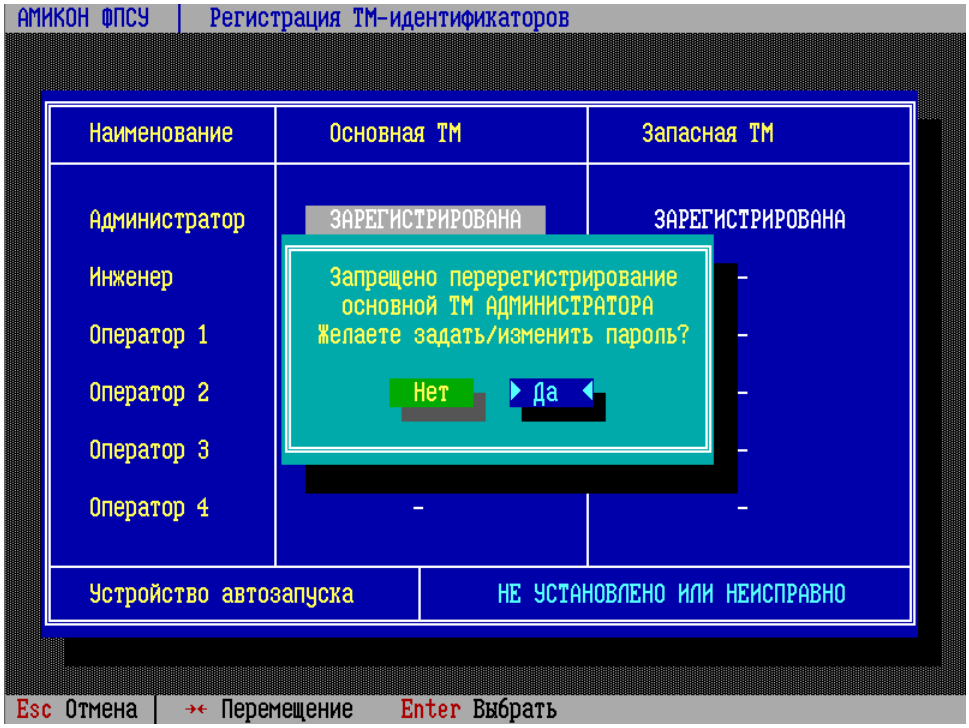

Рисунок 19 - Установка/изменение пароля ТМ

При подтверждении запроса откроется окно ввода пароля.

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

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

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

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

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-

идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ЦВК потребуется повторная установка ЦВК с дистрибутива.

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

Рисунок 20 - Ввод пароля ТМ

Пароль для основного ТМ выбранного класса администратора установлен.

7. 1. 2. Регистрация запасного ТМ

Повторная регистрация запасного ТМ-идентификатора проводится в случае замены ключевой информации ТМ-идентификатора или при компрометации ТМ-идентификатора. Операция доступна администраторам класса «Администратор» и выше.

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

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

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

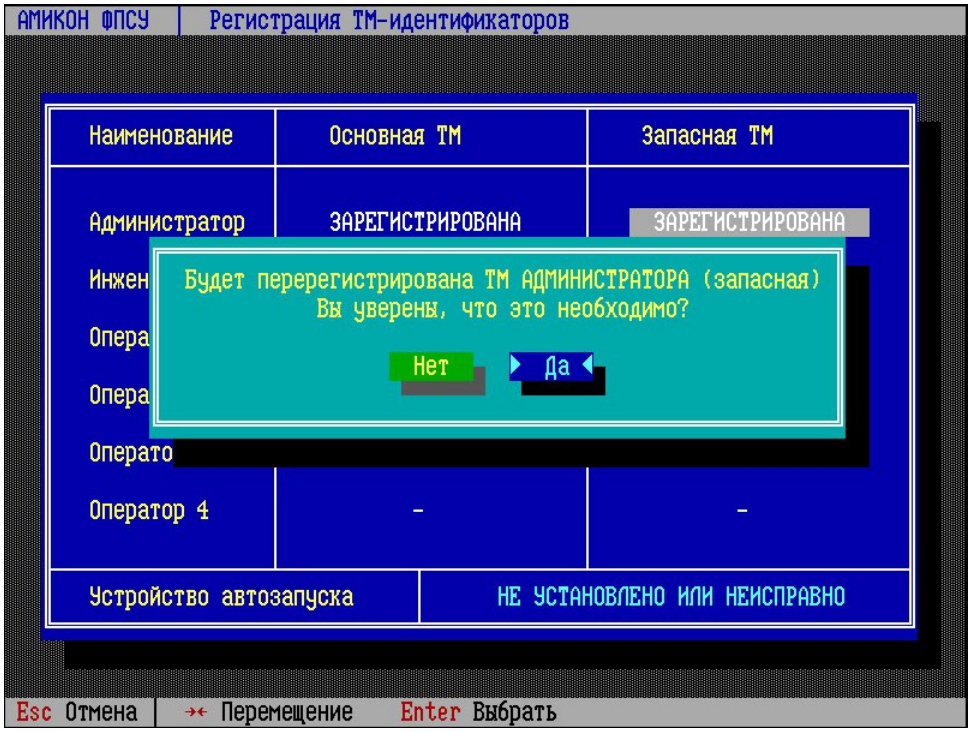

Рисунок 21 - Перерегистрация ТМ

По нажатию кнопки «Да» ТМ будет зарегистрирован заново.

Операция доступна администраторам класса «Администратор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

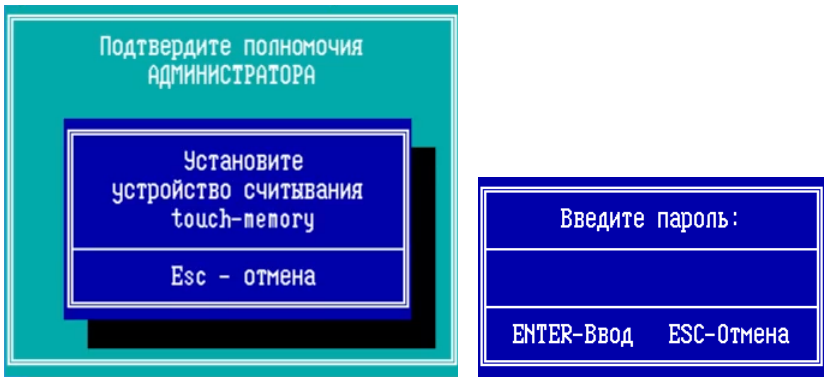

Рисунок 22 - Подтверждение полномочий и ввод пароля ТМ

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

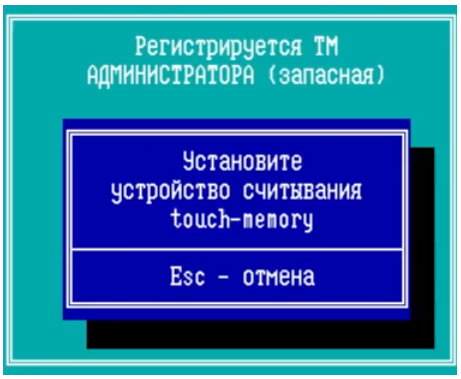

Рисунок 23 - Предъявление запасного ТМ для регистрации

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ЦВК классов КС2 и КС3, и опциональным для ЦВК класса КС1.

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

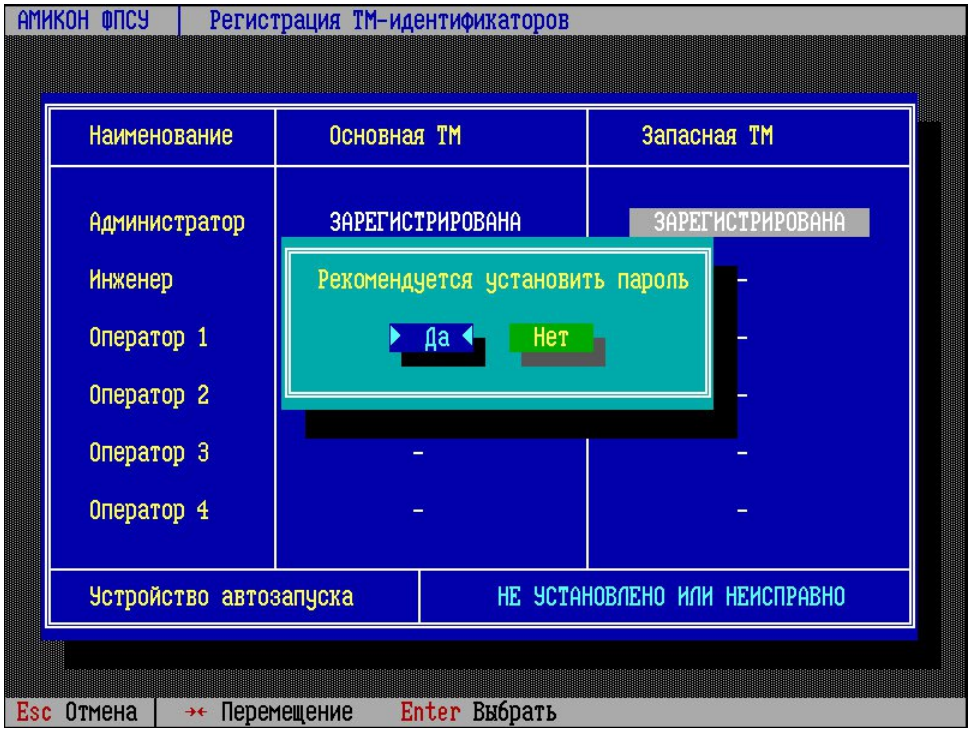

Рисунок 24 - ТМ перерегистрирован

При подтверждении запроса откроется окно ввода пароля.

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

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

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

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

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ЦВК потребуется повторная установка ЦВК с дистрибутива.

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

Рисунок 25 - Ввод пароля ТМ

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

Рисунок 26 - Предъявление запасного ТМ

После подключения запасной ТМ-идентификатор зарегистрирован с установлением пароля.

7. 1. 3. Удаление ТМ

При удалении ТМ требуется предъявить ТМ администратора и ТМ-идентификатор, который очищается, чтобы провести удаление ключевых данных. Операция доступна администраторам ЦВК класса «Администратор» и выше.

При выполнении операции по очистке ключевых данных ТМ-идентификатора система будет требовать подтверждения полномочий администратора (посредством подключения ТМ-идентификатора к USB-порту ЦВК) с целью предотвращения несанкционированных действий.

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

Выберите строку с удаляемым ТМ-идентификатором, например запасной ТМ администратора, и нажмите клавишу <Del>. На экране отобразится запрос:

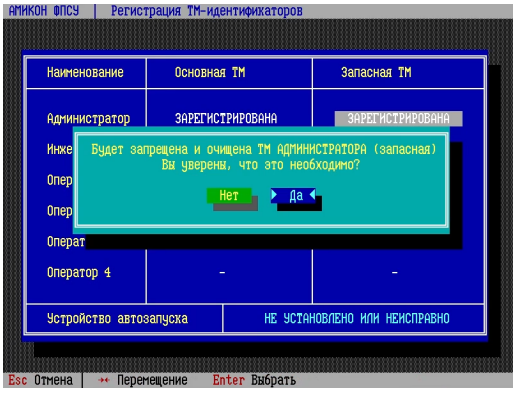

Рисунок 27 - Удаление ТМ

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

Операция доступна администраторам класса «Администратор» и выше.

При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

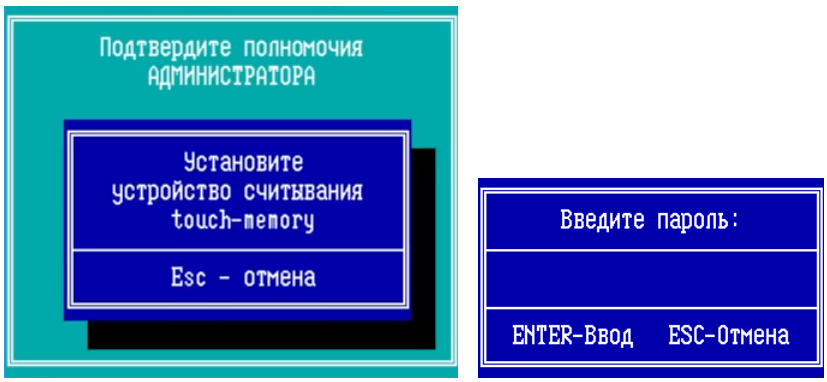

Рисунок 28 - Подтверждение полномочий и ввод пароля ТМ

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

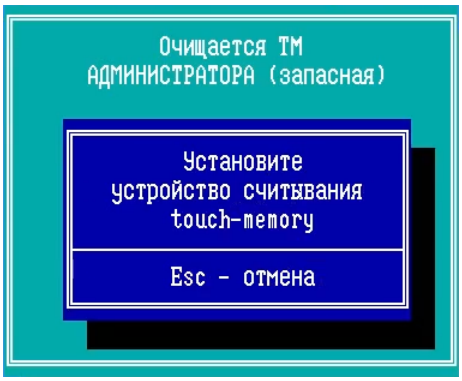

Рисунок 29 - Предъявление запасного ТМ администратора для удаления

Запасной ТМ-идентификатор администратора удален.

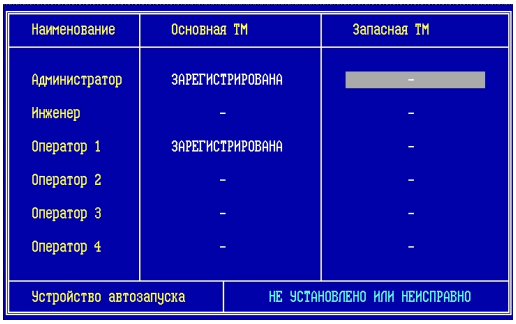

Рисунок 30 - Окно регистратора ТМ

7. 2. Установка дополнений

Команда «Установка дополнений/изменений» подменю предназначена для установки новых программных модулей, опциональных подсистем, или обновлений существующих модулей ЦВК (операции доступны пользователям классов «Главный Администратор» и «Администратор»).

Все изменения или дополнения должны быть получены от организации-поставщика ЦВК и представлены в двух файлах (в зависимости от их размера): файл списка (с расширением .up0) и файл, содержащий собственно изменения, разрешенные для данного серийного номера ЦВК (с расширением .upd).

Файлы с изменениями должны сопровождаться контрольными суммами, которые следует проверить перед установкой обновлений или дополнений, на предмет совпадения их с эталонными указанными в формуляре на СКЗИ контрольными суммами.

Операция доступна администраторам класса «Администратор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

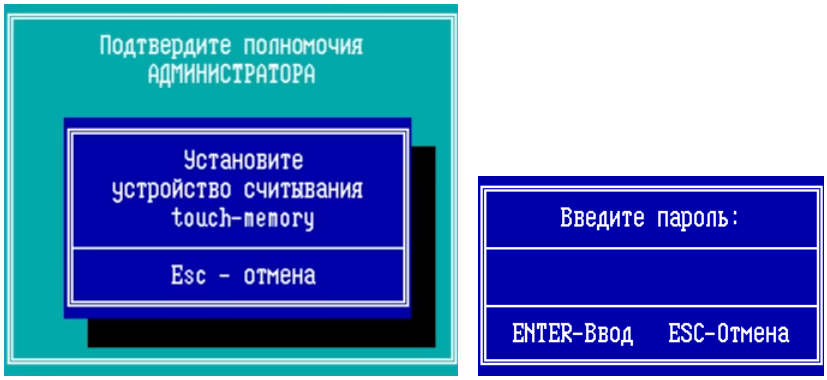

Рисунок 31 - Подтверждение полномочий и ввод пароля ТМ

Для установки обновления или дополнения, требуется:

1. Выбрать опцию «Установка дополнений/изменений» меню настройки системы ЦВК.
2. Появится сообщение подключить к ЦВК USB-носитель с файлами обновления. Файлы должны находиться в корневом каталоге USB-носителя. Подключите USB-носитель и нажмите «Понятно».

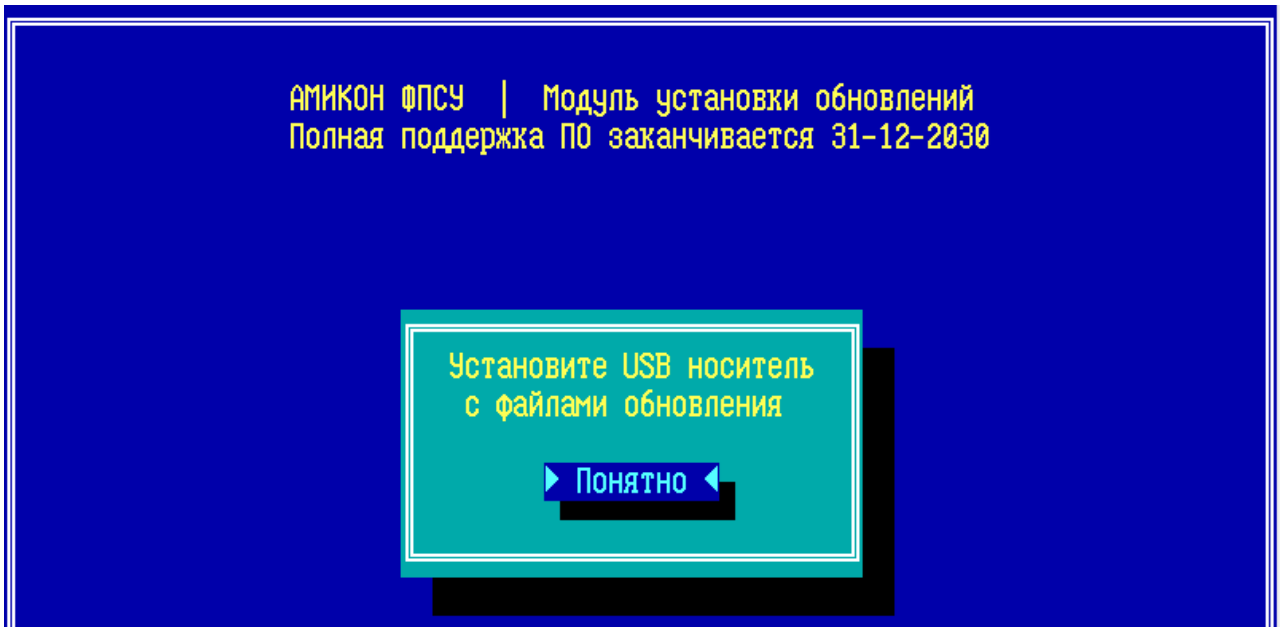

Рисунок 32 - Запрос на подключение USB-носителя

3. Отобразится окно со списком файлов обновлений для ЦВК на USB-носителе. По команде «Перечитать» при смене USB-носителя обновляется список файлов. Необходимо выбрать файл обновления в списке и выполнить команду «Установить».

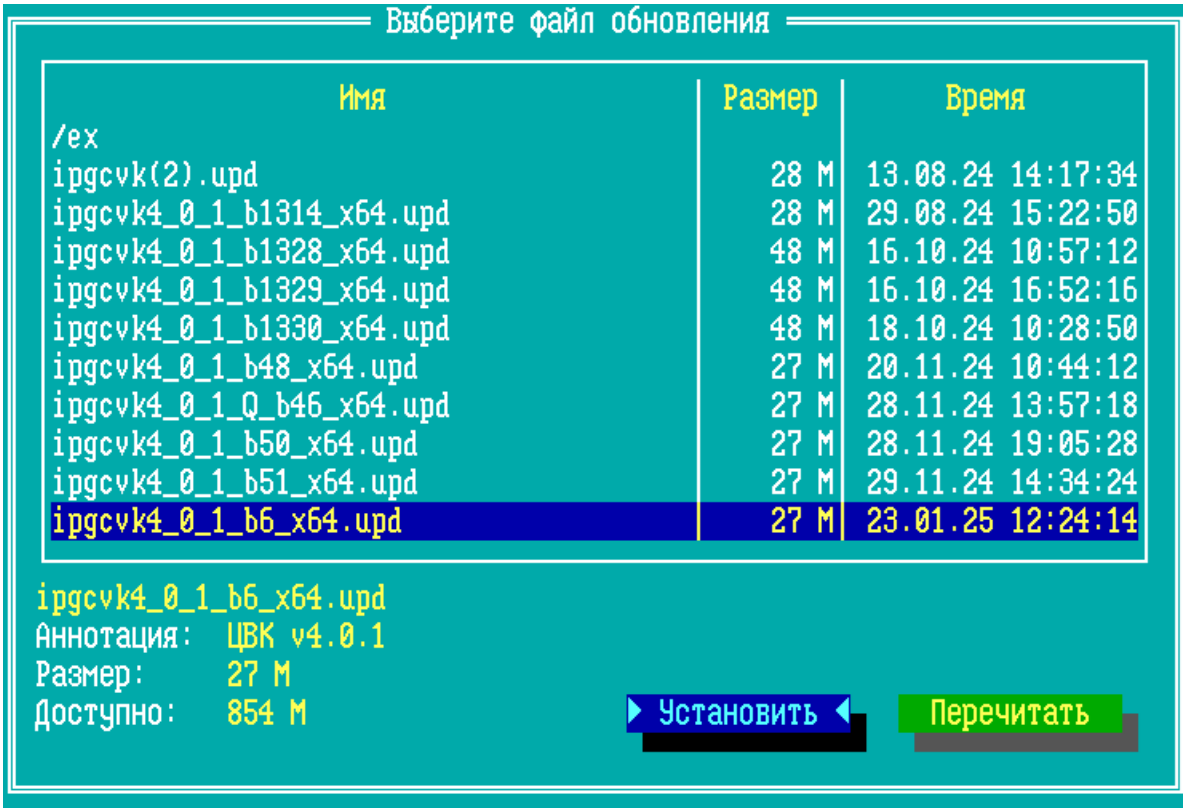

Рисунок 33 - Список файлов обновлений

4. В аннотации к выбранному файлу будет указана находящаяся в обновлении версия ЦВК. Выполните команду «Используем его» для установки обновления. Если требуется выбрать другой файл, нажмите «Выбрать другой», отобразится предыдущее окно со списком файлов обновлений.

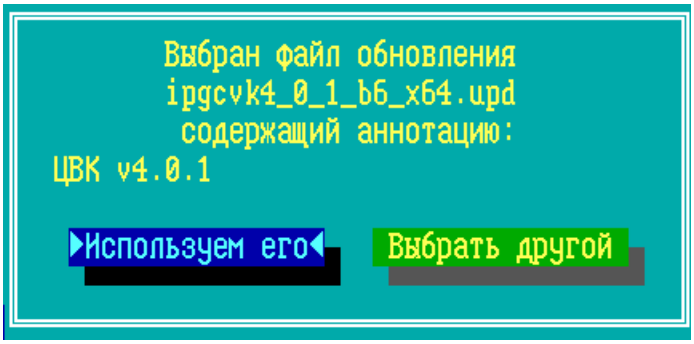

Рисунок 34 - Подтверждение обновления

5. Запустится процесс установки файла обновления. Перед обновлением считывается файл с расширением .up0 со списком обновлений, изменений, дополнений.

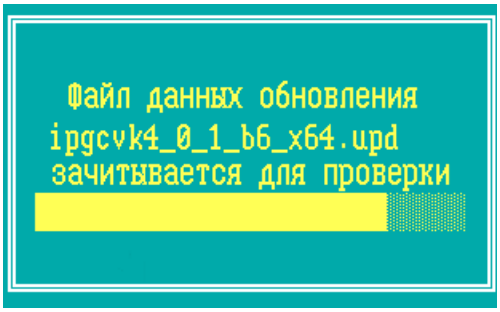

Рисунок 35 - Загрузка обновления

6. Файл обновления записывается на внутренний накопитель ЦВК.

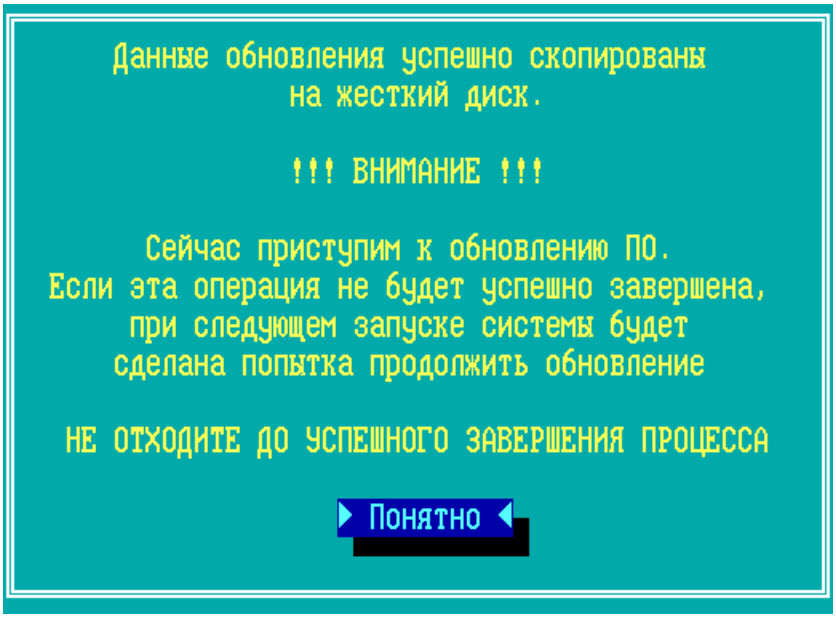

Рисунок 36 - Процесс обновления

7. После завершения установки обновлений ЦВК будет перезагружен и готов к дальнейшей эксплуатации.

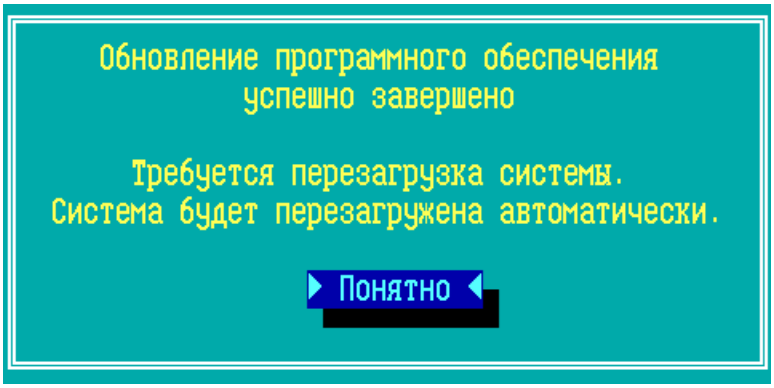

Рисунок 37 - Подтверждение успешного обновления

После перезагрузки на экран будет выдано главного меню с командами настройки и запуска ЦВК.

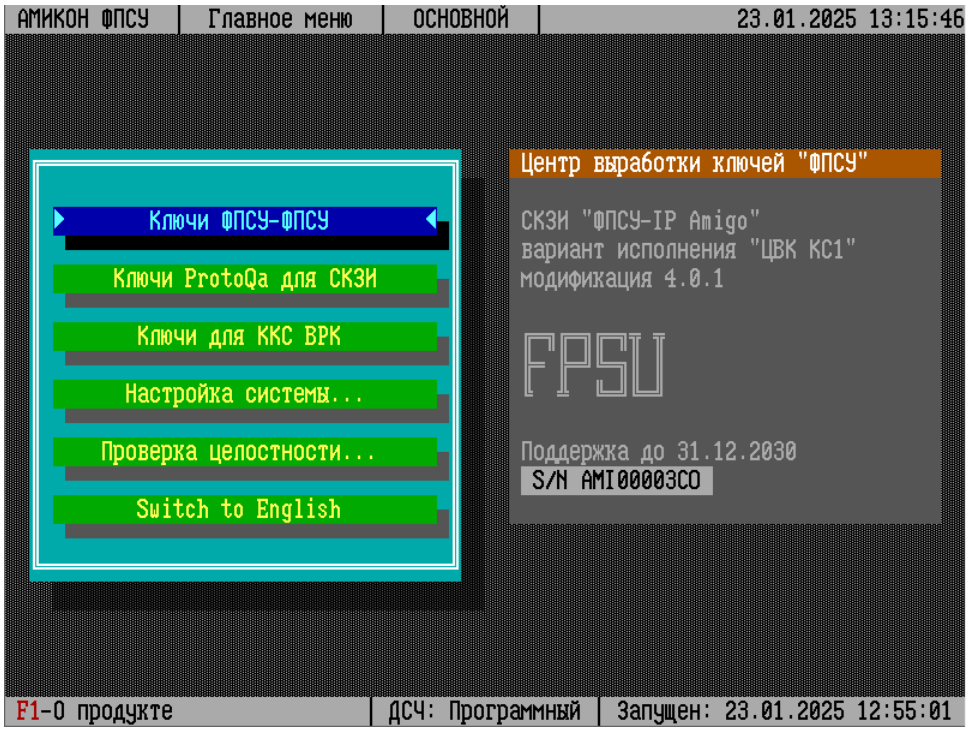

Рисунок 38 - Главное меню ЦВК

7. 3. Переинициализация ПДСЧ

Первоначальная инициализация программного датчика случайных чисел средствами биологического датчика случайных чисел происходит при установке ЦВК.

Команда «Переинициализация ключа ПДСЧ» подменю «Настройки СКЗИ» предназначена для повторной инициализации ПДСЧ ЦВК. Частота повторной инициализации ПДСЧ регулируется правилами пользования СКЗИ, в частности сроки действия ключевой информации не должны превышать 1 год и 3 месяца.

При переинициализации ПДСЧ создается новый криптографический ключ ПДСЧ, являющийся основой для генерации случайных чисел. Этот ключ используется ЦВК в процедуре генерации новой серии ключевых данных «абонентов».

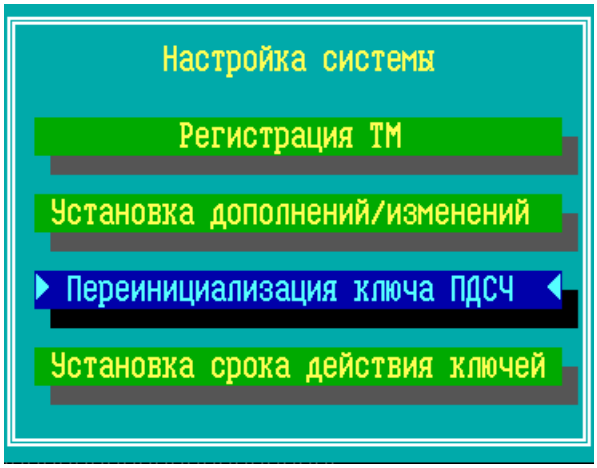

Рисунок 39 - Команда повторной инициализации ПДСЧ

Операция доступна администраторам класса «Инженер» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

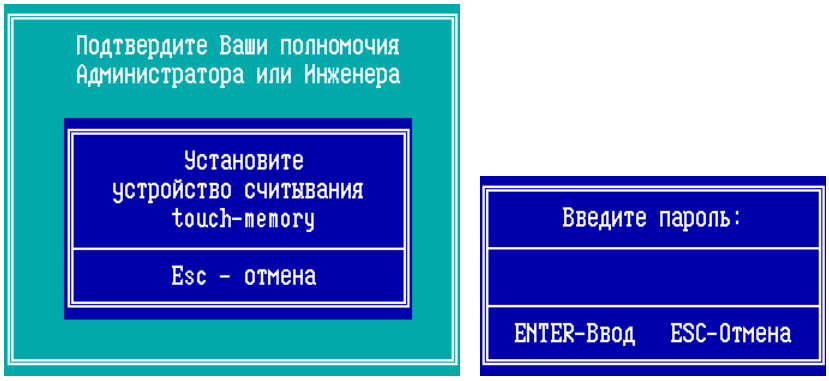

Рисунок 40 - Подтверждение полномочий и ввод пароля ТМ

При выборе команды «Переинициализация ключа ПДСЧ» запустится интерфейс БиоДСЧ. От администратора требуется двигать мышью в пределах экрана:

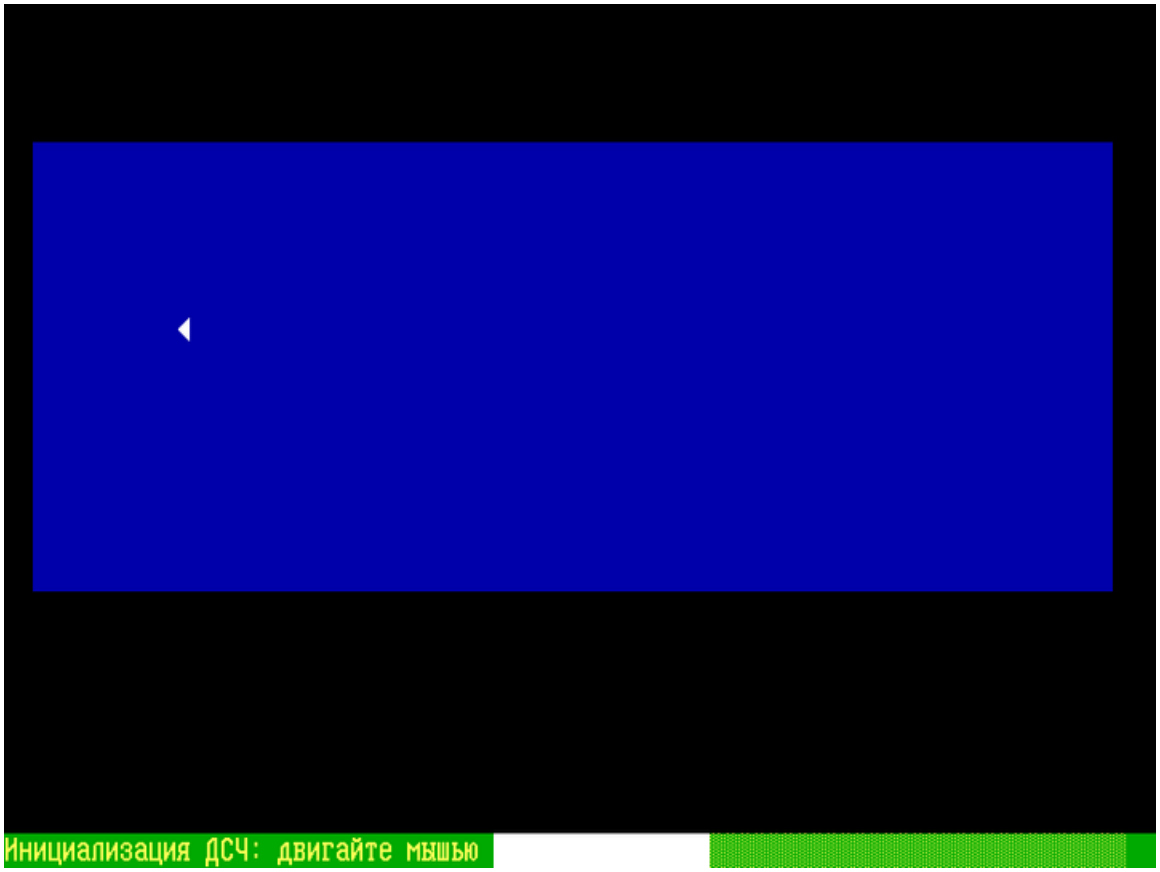

Рисунок 41 - Интерфейс БиоДСЧ

Переинициализация ПДСЧ завершится успешно, как только будет осуществлён корректный ввод достаточного числа значений. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <Esc> обратно в подменю «Настройки СКЗИ».

7. 4. Установка срока действия ключей

Команда меню «Настройка системы → Установка срока действия ключей» предназначена для доступа в интерфейс настройки срока действия ключа запуска и ключа ПДСЧ. Операции доступны администраторам класса «Администратор» и выше.

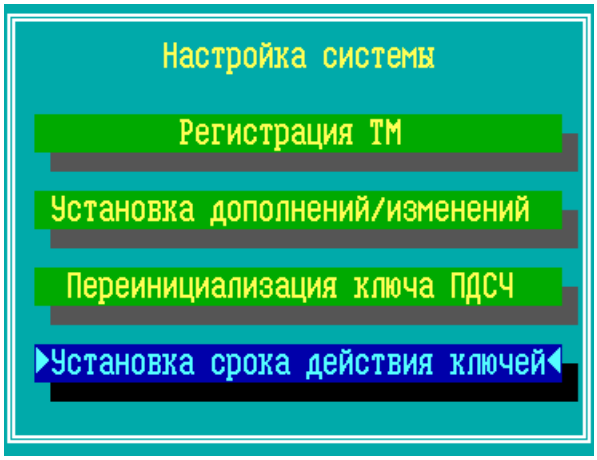

Рисунок 42 - Команда установки срока действия ключей

Операция доступна администраторам класса «Администратор» и выше. При выполнении операции необходимо подтверждение полномочий Администратора:

Рисунок 43 - Подтверждение полномочий администратора

После выполнения команды программа будет каждый раз запрашивать пароль подключенного ТМ-идентификатора для авторизации в системе, в случае если пароль установлен.

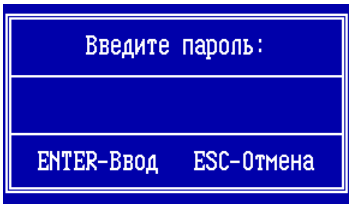

Рисунок 44 - Ввод пароля ТМ

Настройки для каждого типа ключа сохраняются отдельно:

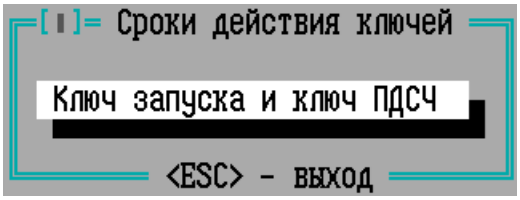

Рисунок 45 - Выбор ключей

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

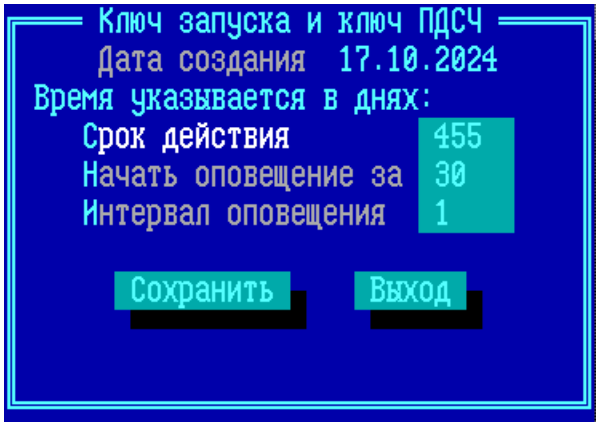

Рисунок 46 - Установка сроков действия ключей

Параметры, доступные администратору для изменения:

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

«**Начать оповещение за**» – число, обозначающее количество дней до срока прекращения действия ключа, с которого администратору ЦВК будет при запуске ЦВК выводится сообщение о приближающемся окончании срока действия ключа;

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

8. Контроль целостности программного обеспечения

ЦВК содержит ряд механизмов, обеспечивающих защиту программных модулей от НСД. В частности, автоматический контроль целостности программных модулей, находящихся на ПЗУ комплекса при запуске.

Администратор имеет возможность осуществить дополнительный контроль целостности программных и информационных частей ЦВК с использованием специальной подсистемы контроля целостности модулей, в том числе путем сравнения с эталонными контрольными суммами, указанными в формуляре на СКЗИ.

Дополнительная проверка целостности ПО ЦВК осуществляется по команде «Проверка целостности» основного меню.

Рисунок 47 - Главное меню ЦВК

У локального администратора существует три варианта выполнения проверки:

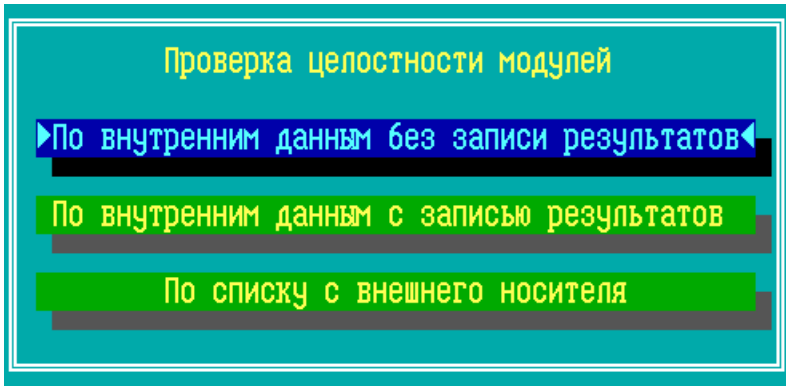

Рисунок 48 - Меню проверки целостности ПО

При выполнении операции необходимо подтверждение полномочий администратора указанного класса, а также будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе, в случае если пароль установлен.

При выборе команды «**По внутренним данным без записи результатов**» проверка ПО ЦВК происходит по хранящимся на ПЗУ (SSD) контрольным эталонным суммам, с выводом результата проверки («успешно» или «обнаружена ошибка») на экран. Операция доступна администраторам класса «Администратор» или «Инженер».

При выборе команды «**По внутренним данным с записью результатов**» проверка ПО ЦВК происходит по хранящимся на ПЗУ (SSD) контрольным эталонным суммам, с выводом результата проверки («успешно» или «обнаружена ошибка») на экран и в файл с расширением .LST на внешний носитель. Операция доступна администраторам класса «Администратор»

При выборе команды «**По списку с внешнего носителя**» проверка ПО ЦВК 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 может быть предоставлен дополнительно по запросу. Операция доступна администраторам класса «Администратор»

После активации команды главного меню «**Проверка целостности**» и опции «**По списку с внешнего носителя**» открывшегося подменю на экране

появится сообщение с приглашением вставить носитель с проверочными модулями в считывающее устройство ЦВК.

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 (CP866).

Если в результате выполнения проверки появляется сообщение о нарушении целостности контролируемых файлов, дальнейшая эксплуатация ЦВК не допускается. Следует переустановить ЦВК с дистрибутивного носителя.

В случае локального управления ЦВК с помощью консольного подключения через COM-порт от оборудованного программой «Терминал» рабочего места под управлением ОС Windows, необходимо выполнять контроль целостности программного обеспечения «Терминала» и рабочей станции в соответствии правилами пользования на модификацию 4.0.1 вариантов исполнения «ЦВК КС1», «ЦВК КС2» или «ЦВК КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

9. Ключи ФПСУ-ФПСУ

9. 1. Генерация и выдача ключевых данных

После загрузки ЦВК, переход в интерфейс генерации парно-выборочных ключей для ФПСУ осуществляется выполнением команды «Ключи ФПСУ-ФПСУ» главного меню.

Рисунок 49 - Главное меню ЦВК

Операция доступна администраторам класса «Оператор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

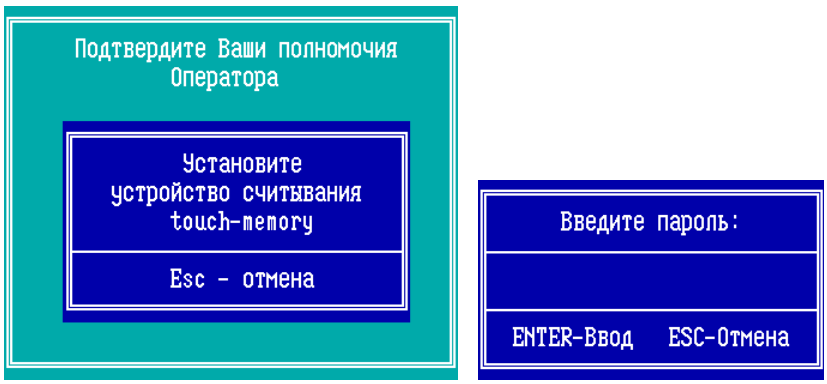

Рисунок 50 - Подтверждение полномочий и ввод пароля ТМ

После ввода пароля программа будет каждый раз предлагать скорректировать время, поскольку операционная среда функционирует изолированно от сетей передачи данных и не имеет возможности синхронизировать время. Проверьте текущее время на ЦВК, и, при необходимости, введите в поле «Новые» текущую дату и время.

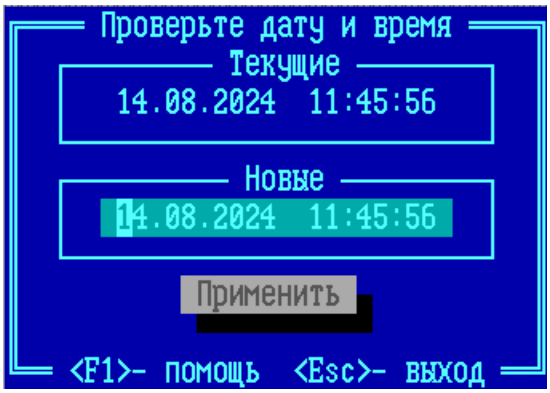

Рисунок 51 - Проверка даты и времени

До тех пор, пока время не изменено, оно автоматически повторяет текущее. После изменения оно остановится. Клавишами <Enter>, <↓> осуществляется переход на кнопку «Применить», если дата и время изменены. После установки времени кнопка станет недоступна и в строке «Новые» время опять будет следовать за текущим до нового изменения.

Выполните команду «Применить» для обновления даты и время, или нажмите клавишу <Esc> для продолжения без корректировки системного времени.

Следующим этапом работы является выбор центра – криптосети ФПСУ,

для которой генерируются ключевые данные.

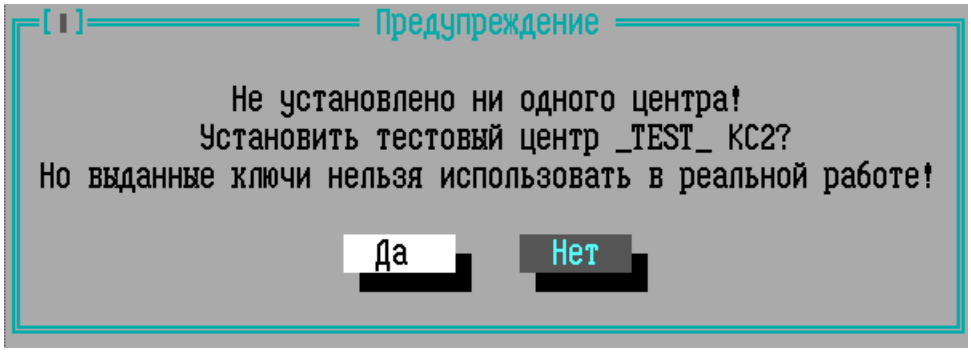

Рисунок 52 - Сообщение об установке тестового центра

Примечание. В ЦВК может быть зарегистрирован только один центр.

По умолчанию список центров пустой, и для продолжения работы требуется зарегистрировать центр, предъявив ЦВК файл с лицензией на использование центра. Команды окна списка центров:

«**Добавить**» – зарегистрировать в ЦВК новый центр, работающий с ключевыми данными класса КС1, КС2 или КС3.

«**Выбрать**» – выбрать ранее зарегистрированный в ЦВК центр для работы с ключевыми данными этого центра: генерации, выдачи на съемный носитель и удаления ключевых данных с ЦВК.

Рисунок 53 - Список центров пуст

Для перехода в окно управления (генерация, выдача, удаление с ЦВК) ключевыми данными центра, требуется выбрать центр и тип ключевых данных (КС1, КС2 или КС3). В зависимости от типа ключевых данных, порядок и параметры создания серии будут отличаться (см. пункты «Генерация новой серии ключевых данных класса КС2» и «Генерация новой серии ключевых данных классов КС1 и КС3»).

9. 1. 1. Регистрация центра в ЦВК

Для регистрации в ЦВК центра выполните команду «Добавить» окна списка центров.

Система запустит процесс регистрации лицензии на центр в ЦВК, предложив подключить USB-носитель с файлом лицензии. Подключите USB-носитель и нажмите «ОК» для продолжения.

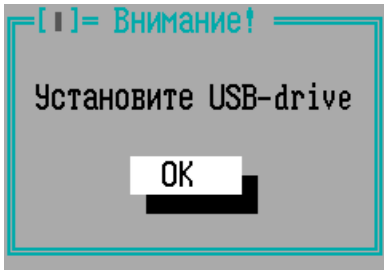

Рисунок 54 - Запрос на подключение USB-носителя с файлом лицензии

Файл лицензии - файл вида «<центр>.lsX», где X класс ключей (1 - КС1, 2 - КС2, 3 - КС3).

Будет произведен поиск в корневом каталоге подключенного к ЦВК USB-носителя, и на экран выдан список обнаруженных на носителе лицензий, также можно указать каталог с лицензией.

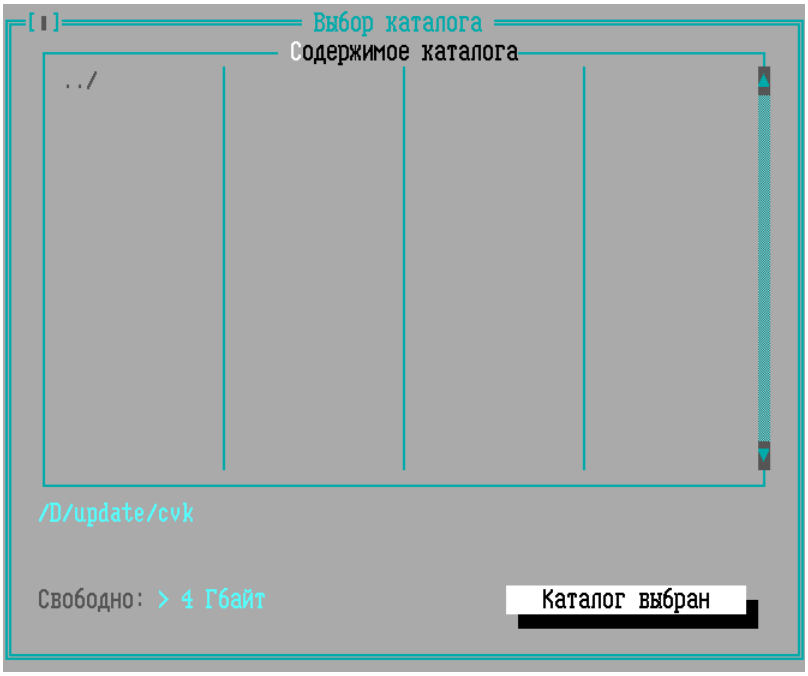

Рисунок 55 - Выбор каталога с лицензией

Каждая лицензия имеет название и тип генерируемых на основании этой лицензии ключей, относящихся к СКЗИ класса КС1, КС2 или КС3 согласно требованиям ФСБ. Если центр будет управлять ключевыми данными, применяемыми в СКЗИ нескольких классов, процедуру регистрации лицензии потребуется провести отдельно для каждого класса.

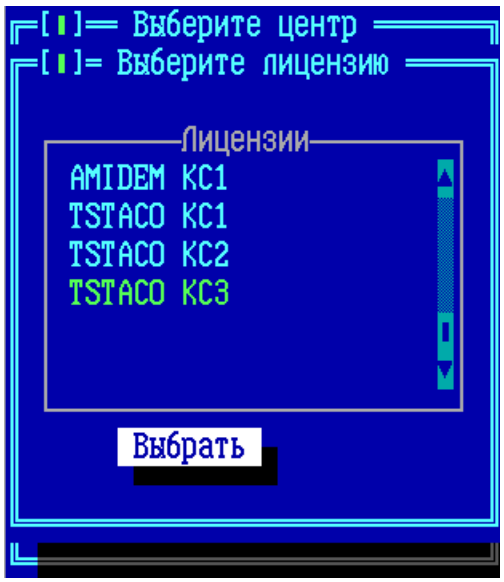

Рисунок 56 - Обнаруженные лицензии

ВНИМАНИЕ! Лицензии на центры выдаются с привязкой к определенному серийному номеру ЦВК и не могут быть установлены на другой ЦВК.

Установите курсор на требуемую лицензию в списке обнаруженных лицензий, и выполните команду «Выбрать» для регистрации указанного в лицензии центра на ЦВК. В случае корректной регистрации лицензии будет выдано служебное оповещение «Лицензия успешно установлена». Закройте оповещение, и программа осуществит возврат в окно списка центров, куда будет добавлена запись о зарегистрированном с помощью лицензии центре.

Рисунок 57 - Добавлен описатель центра

9. 1. 2. Выбор центра и типа ключей

Для перехода в окно управления (генерация, выдача, удаление с ЦВК) ключевыми данными центра, требуется выбрать центр и тип ключевых данных (КС1, КС2 или КС3). В зависимости от типа ключевых данных, порядок и параметры создания серии будут отличаться (см. пункты «Генерация новой серии ключевых данных класса КС2» и «Генерация новой серии ключевых данных классов КС1 и КС3»).

Установив курсор на центре, выполните команду «Выбрать» в окне списка зарегистрированных центров.

В появившемся окне будет приведен список типов ключевых данных, которыми центр может управлять:

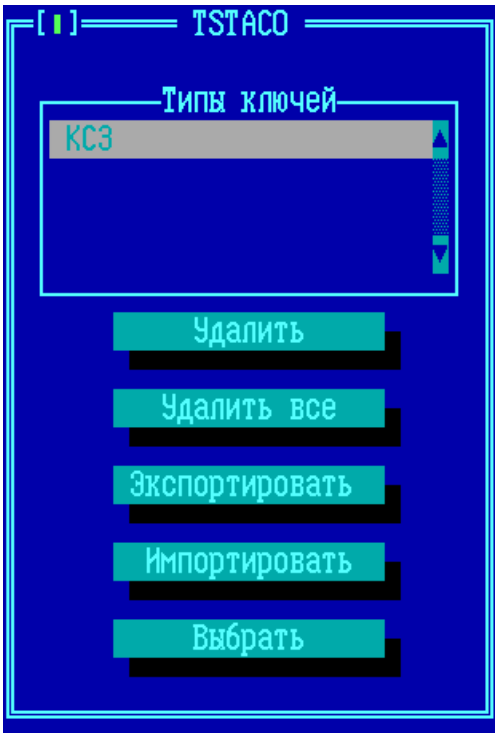

Рисунок 58 - Список типов ключевых данных

Доступные команды:

«**Удалить**» – удалить все хранящиеся на ЦВК серии ключевых данных центра, относящиеся к выбранному типу ключей. При удалении из списка последнего типа ключевых данных происходит также удаление центра из списка зарегистрированных в ЦВК центров;

«**Удалить все**» – удалить все типы ключевых данных, вместе с этим удаляется центр из списка зарегистрированных в ЦВК центров;

«**Экспортировать**» – создать и выдать на внешний носитель резервную копию центра для ключевых данных выбранного типа. Резервная копия выдается в зашифрованном виде, подробнее см. пункт «Экспорт центра ЦВК»;

«**Импортировать**» – загрузить с внешнего носителя резервную копию центра в ЦВК, подробнее см. пункт «Импорт центра ЦВК»;

«**Выбрать**» – перейти в окно управления сериями ключевых данных

выбранного типа.

9. 1. 3. Генерация новой серии ключевых данных

При выполнении команды «Выбрать» в окне выбора типа ключевых данных отобразится окно выбора серии ключевых данных.

В открывшемся окне «Выберите серию (КСХ)» список серий будет пустым при первом использовании центра с сообщением «Серии не созданы». При последующем использовании будет отображаться список ранее созданных серий.

Рисунок 59 - Пустой список серий ключевых данных

Для создания новой серии ключевых данных, нажмите клавишу <Ins>.

9. 1. 3. 1. Генерация новой серии ключевых данных класса КС2

Для генерации новой серии ключевых данных класса КС2 выберите тип ключевых данных, будет выдано окно со списком сгенерированных ранее

серий (по умолчанию, пустое) и нажмите клавишу <Ins>.

На экране отобразится окно «Новая серия». Номер новой серии присваивается автоматически, как следующий за номером последней созданной серии. Если ключевые данные генерируются первый раз, серии будет присвоен номер 1.

Рисунок 60 - Создание новой серии

В поле «Абонентов:» требуется указать максимальное количество абонентов (комплексов ФПСУ), на которое рассчитана данная серия (от 2-х до 9999 для класса КС3 и КС1). Для каждого абонента будет создан свой файл с ключевыми данными в рамках генерируемой серии.

ВНИМАНИЕ! Изменить параметры существующей серии (например, если серия рассчитывалась на имеющееся количество ФПСУ, а впоследствии в эксплуатацию были введены новые) НЕВОЗМОЖНО. Для изменения параметров потребуется создать новую серию ключевых данных.

Нажмите кнопку «Создать» для генерации серии с установленными параметрами, на экран будет выдано сообщение:

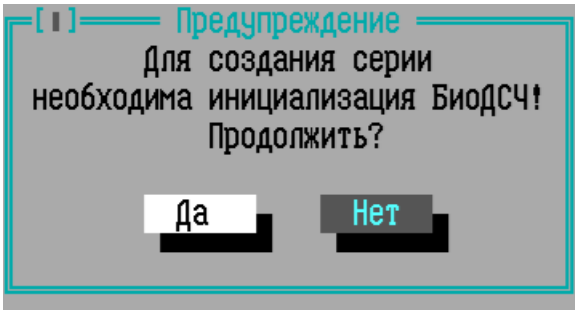

Рисунок 61 - Сообщение об инициализации БиоДСЧ

При генерации серии ключевых данных производится инициализация ПДСЧ средствами БиоДСЧ, иначе серия не будет создана, нажмите «Да» в

диалоговом окне для продолжения.

Запустится интерфейс БиоДСЧ. От администратора требуется двигать мышью в пределах экрана:

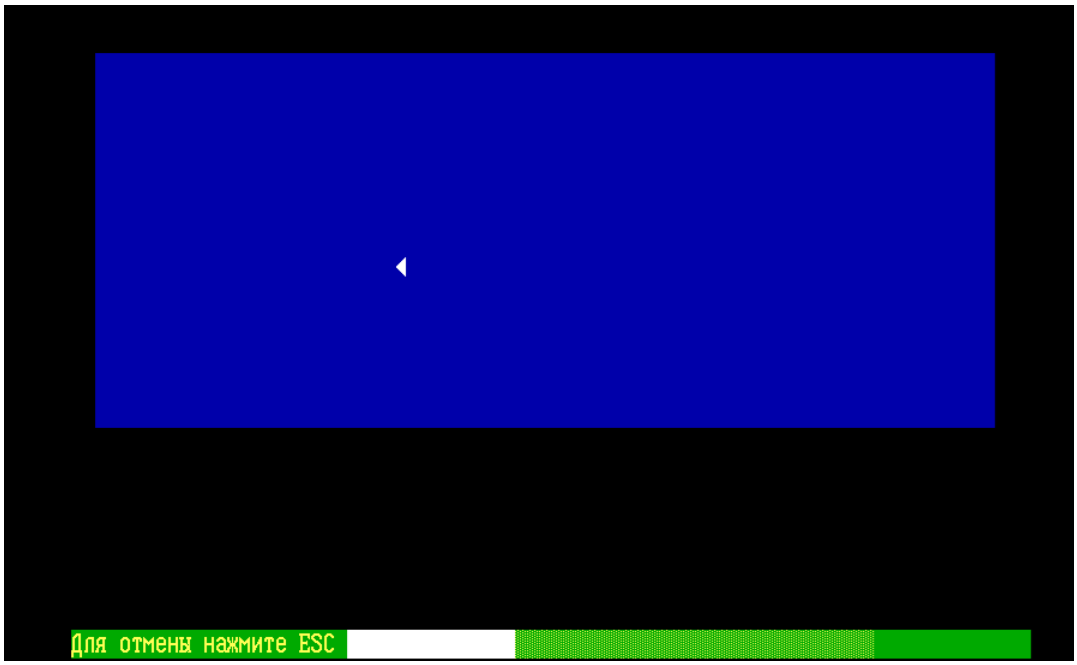

Рисунок 62 - Интерфейс БиоДСЧ

Переинициализация ПДСЧ завершится успешно, как только будет осуществлён корректный ввод достаточного числа значений. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <Esc> обратно в окно создания серии.

Затем на экран будет выдано окно выбора внешнего носителя, на который будет записан ключ хранения серии ключевых данных. Он потребуется к предъявлению каждый раз при дальнейшей работе с созданной серией, например, для выдачи парно-выборочных ключей ФПСУ на внешний носитель.

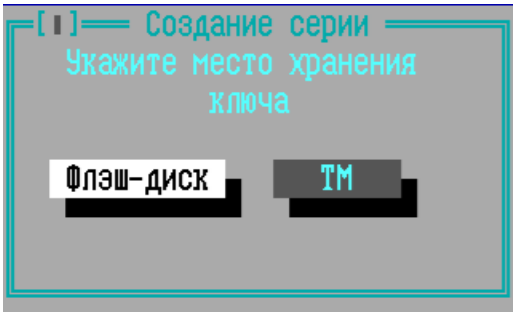

Рисунок 63 - Выбор места хранения

Местом хранения ключа может выступать файл, выдаваемый на подключенный USB-носитель, или TM-идентификатор.

ВНИМАНИЕ! Рекомендуется выбирать местом хранения «Флэш-диск». Не рекомендуется использовать TM-идентификатор в качестве носителя ключей. При использовании в качестве носителя ключа TM-идентификатора администратора ЦВК, ключ администратора на TM-идентификаторе будет перезаписан! Это приведет к потере возможности администрировать ЦВК в дальнейшем!

Если в качестве места хранения выбран TM-идентификатор, то система предложит подключить к USB порту ЦВК устройство TM-Key или приложить устройство touch-memory к TM-считывателю ЦВК для записи ключа хранения.

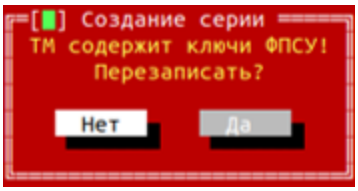

Рисунок 64 - Перезапись ключа

ВНИМАНИЕ! Для ЦВК модификации 4.0.1 TM-идентификатор «Главного Администратора» ЗАПРЕЩЕНО использовать в качестве места хранения ключа!

Если в качестве места хранения выбран «Флэш-диск», то система предложит подключить к ЦВК USB-носитель для записи на него файла с ключом хранения.

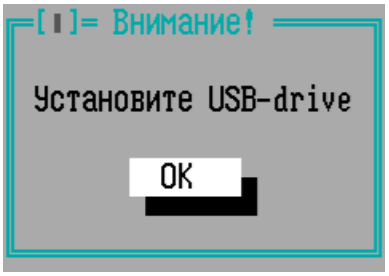

Рисунок 65 - Запись ключа хранения

Будет произведена запись файла в корневой каталог подключенного к ЦВК USB-носителя, также можно выбрать каталог для записи.

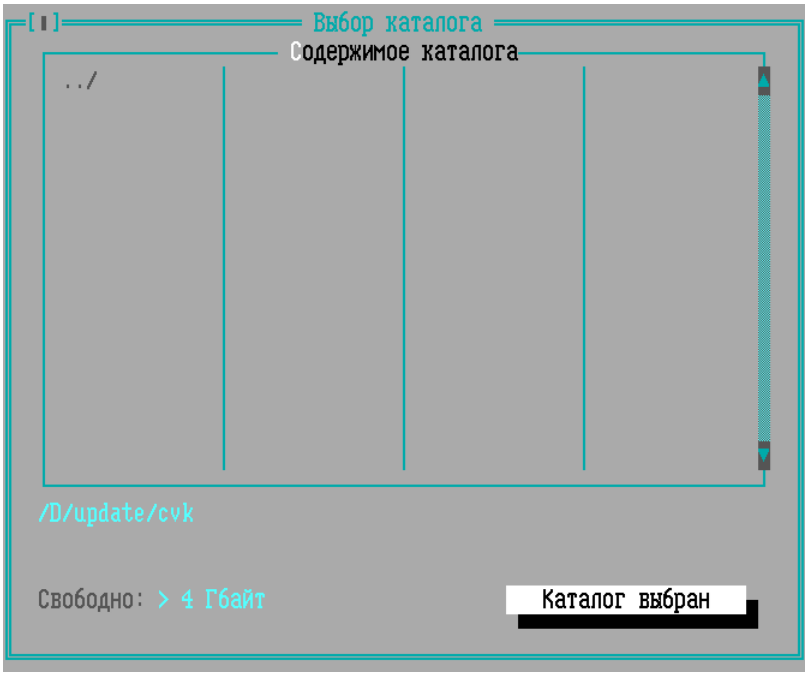

Рисунок 66 - Выбор каталога для записи файла с ключом хранения

В случае, если файл уже существует, он будет перезаписан.

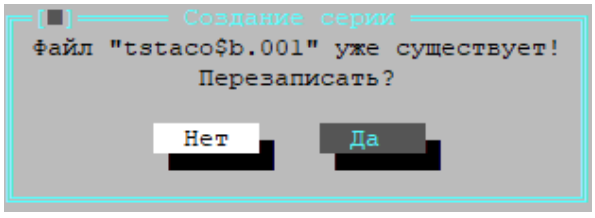

Рисунок 67 - Запись ключа хранения

По завершению будет выдано сообщение об успешном создании серии

ключевых данных.

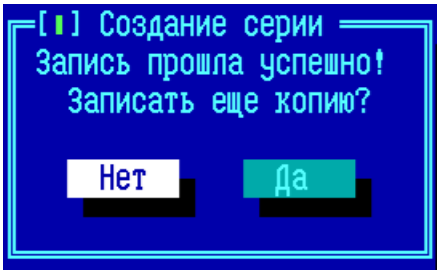

Рисунок 68 - Запись ключа хранения

После записи ключа хранения таблицы парно-выборочных ключей, будет произведен выход из окна «Создание серии» и сгенерированная серия ключевых данных ФПСУ появится в окне в списке серий.

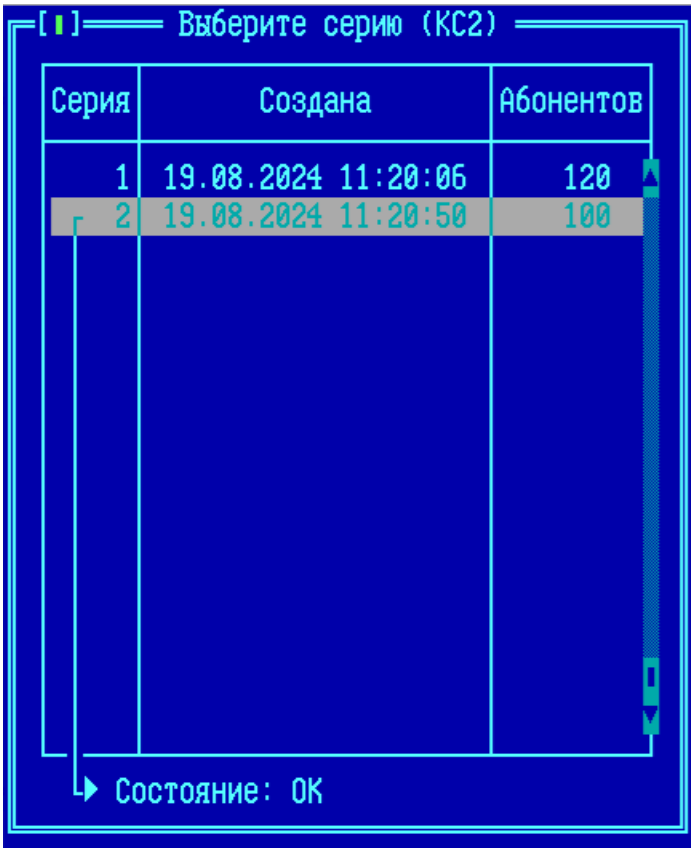

Рисунок 69 - Список серий ключевых данных

Дальнейшая работа с серией, выдача ключевых данных ФПСУ на носитель, описана в пункте «Выдача парно-выборочных ключей и ключей ПДСЧ».

9. 1. 3. 2. Генерация новой серии ключевых данных классов КС1 и КС3

Процесс генерации новой серии ключевых данных классов КС1 и КС3 отличается от генерации серии ключевых данных класса КС2 необходимостью задать дополнительные параметры серии ключевых данных. Также, как и при генерации ключей класса КС2, после выбора типа ключевых данных будет выдано окно со списком сгенерированных ранее серий (по умолчанию пустое).

Рисунок 70 - Пустой список серий ключевых данных

Для создания новой серии нажмите клавишу <Ins>. На экран будет выдано окно «Новая серия». Номер новой серии присваивается автоматически, как следующий за номером последней созданной серии. Если ключевые данные генерируются первый раз, серии будет присвоен номер 1.

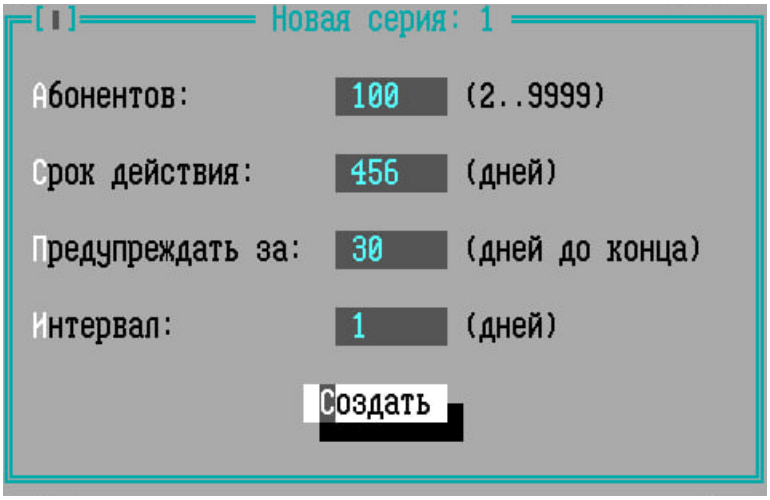

Рисунок 71 - Создание новой серии ключей КС3

При создании серии, в поле «Абонентов:» требуется указать максимальное количество абонентов (комплексов ФПСУ), на которое рассчитана данная серия (от 2-х до 9999 для КС1, от 2-х до 9999 для КС3). Для каждого абонента будет создан свой файл с ключевыми данными в рамках генерируемой серии.

Дополнительными параметрами являются срок действия ключевых данных, в днях (по умолчанию 456 дней, 15 месяцев), начало и интервал повторения предупреждения о завершении срока действия ключей.

ВНИМАНИЕ! Изменить параметры существующей серии (например, если серия рассчитывалась на имеющееся количество ФПСУ, а впоследствии в эксплуатацию были введены новые) НЕВОЗМОЖНО. Для изменения параметров потребуется создать новую серию ключевых данных.

Дальнейшая процедура генерации ключевых данных классов КС1 и КС3, начинающаяся после нажатия кнопки «Создать», совпадает с процедурой генерации ключевых данных класса КС2 (см. пункт «Генерация новой серии ключевых данных класса КС2»).

Дальнейшая работа с серией, выдача ключевых данных ФПСУ на носитель, описана в пункте «Выдача парно-выборочных ключей и ключей ПДСЧ».

9. 1. 3. 3. Смена серии ключевых данных

Срок действия серии ключевых данных отсчитывается с момента генерации и не должен превышать 15 месяцев. До истечения срока действия текущей серии ключевых данных требуется повторно сгенерировать и установить новую серию ключевых данных на местах использования СКЗИ.

Для смены серии ключевых данных на ЦВК необходимо сгенерировать новую серию ключевых данных (см. пункты «Генерация новой серии ключевых данных класса КС2», «Генерация новой серии ключевых данных классов КС1 и КС3»).

При смене серии ключевых данных требуется сменить парно-выборочные ключи. Для этого на ЦВК генерируются парно-выборочные ключи с тем же номером для новой старшей серии ключевых данных и выдаются на внешний носитель (см. пункт «Выдача парно-выборочных ключей и ключей ПДСЧ»).

На ФПСУ могут быть установлены две серии ключевых данных одновременно на период перехода с младшей серии на старшую.

На ФПСУ необходимо сменить парно-выборочные ключи на новые, выданные ЦВК. После того как, все ключи заменены на новые со старшей серией ключевых данных, младшая серия ключевых данных может быть удалена с ЦВК.

9. 1. 4. Выдача парно-выборочных ключей и ключей ПДСЧ

Список всех сгенерированных на ЦВК серий ключевых данных центра находится в окне списка серий центра, вызываемом по команде «Выбрать» (см. пункт «Выбор центра и типа ключей»). Выдача ключей для всех классов КС происходит одинаково.

В появившемся окне каждая сгенерированная и не удаленная серия ключевых данных помечена состоянием «ОК» – это означает, что ключевые данные сгенерированы и их можно выдать на внешний носитель.

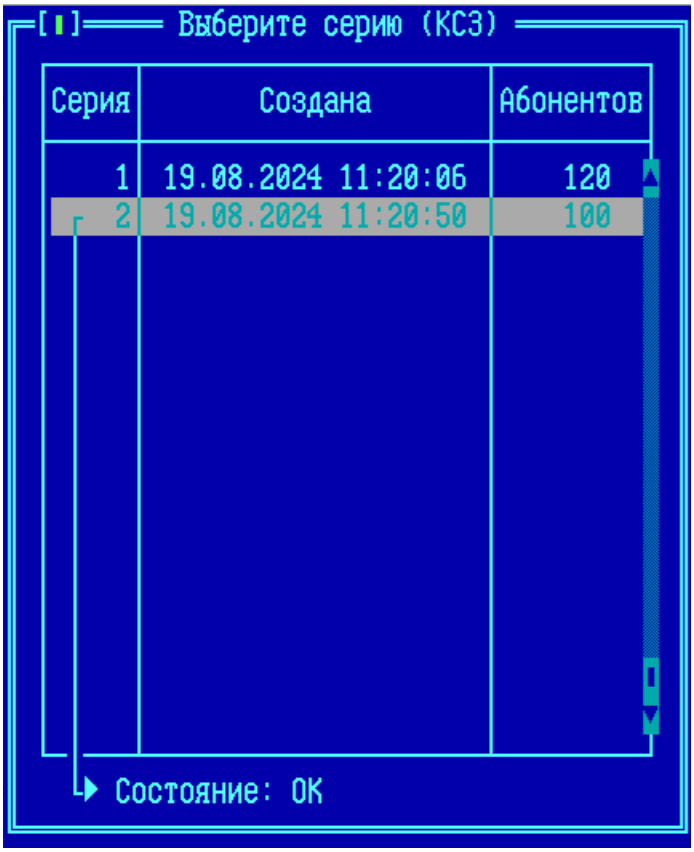

Рисунок 72 - Отображение серии, выдаваемой на внешний носитель

Если ранее сгенерированная серия больше не требуется – её можно удалить при помощи клавиши <Del>. В этом случае состояние серии будет помечено как «Удалена по команде оператора», а сгенерированные в её рамках ключевые данные удалены и недоступны для выдачи на внешний носитель. Запись об удаленной серии не удаляется из списка серий.

Рисунок 73 - Отображение удаленной серии

Для перехода в окно списка ключей данной серии, следует установить курсор на требуемой серии и нажать <Enter>. Программа потребует предъявления с носителя ключа хранения (ключа таблицы парно-выборочных ключей) этой серии, созданного на этапе генерации серии ключевых данных.

Файл серии ключевых данных - файл вида «<центр>$b.00N», где N - номер серии ключевых данных.

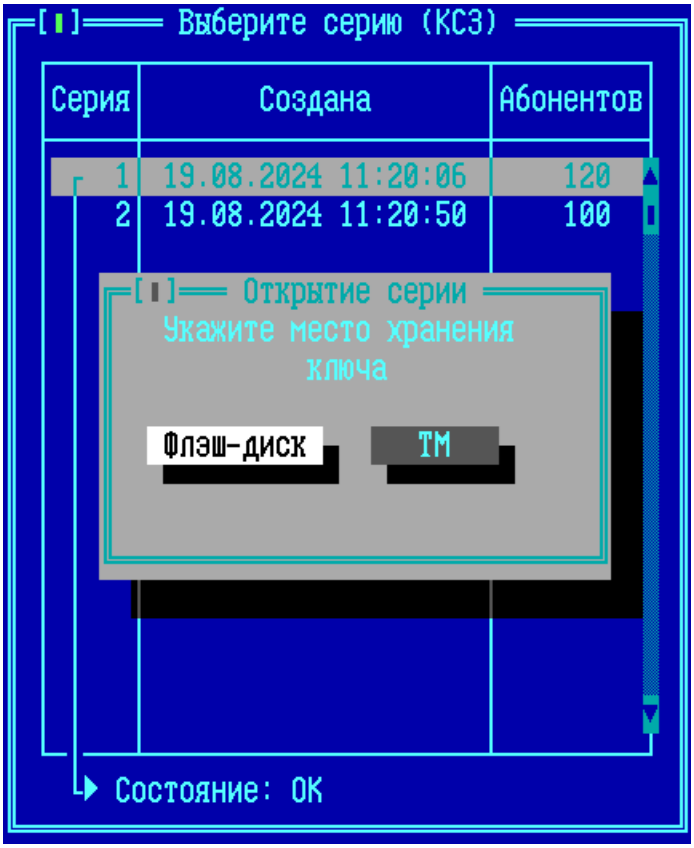

Рисунок 74 - Открытие ключа серии

После того, как будет установлен и указан внешний носитель с серией ключевых данных, отобразится следующее окно:

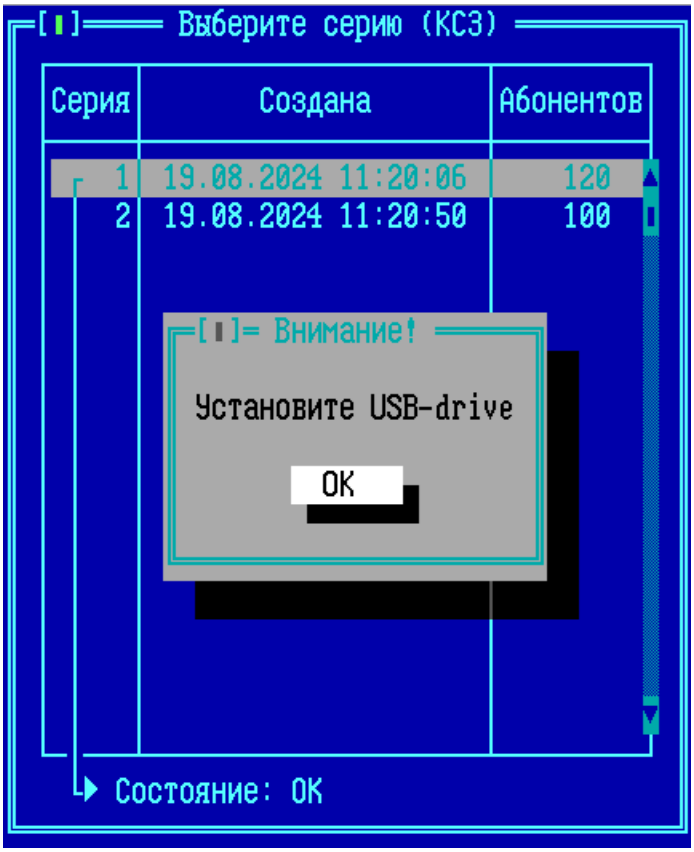

Рисунок 75 - Чтение ключа серии

Если указано неверное место хранения ключа, на экране появится сообщение об ошибке:

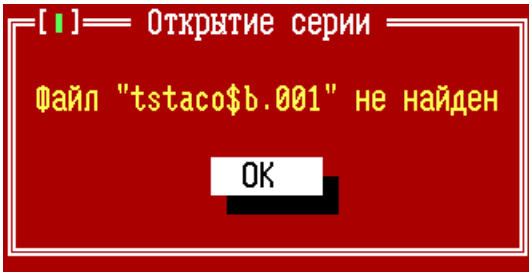

Рисунок 76 - Неверно указано место хранения ключа

Если предъявленный ключ хранения будет неверным, на экране появится сообщение об ошибке:

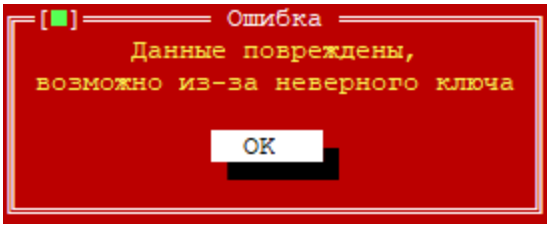

Рисунок 77 - Данные серии повреждены

Если предъявленный ключ хранения будет верным, на экране появится окно с заданными дополнительными параметрами для этой серии.

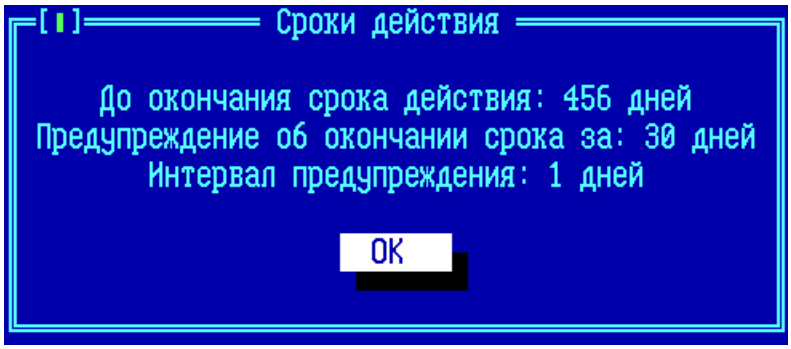

Рисунок 78 - Дополнительные параметры серии

Далее на экране появится окно, содержащее нумерованный список ключевых данных серии.

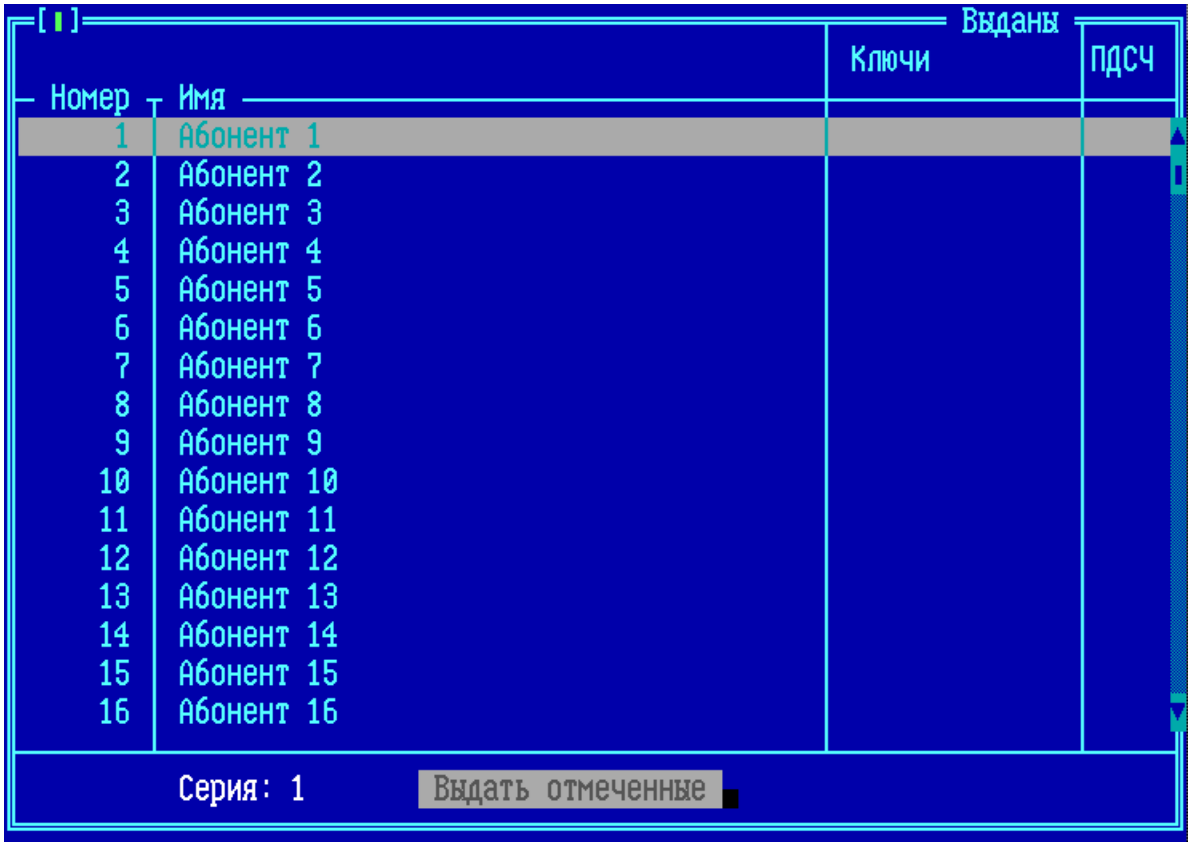

Рисунок 79 - Список ключей выбранной серии

В списке ключевые данные представлены номерами и именами ФПСУ, для которых они были созданы. Для удобства администратор может дать каждому ключу имя (например, по географическому или административному признаку ФПСУ, которому ключ предназначен. По умолчанию, имя состоит из слова «Абонент» и порядкового номера ключевых данных в серии).

Имя можно изменить, установив на конкретный пункт списка курсор и нажав клавишу <Пробел>. В появившемся поле следует ввести имя (от 1 до 39 символов) и подтвердить изменение нажатием клавиши <Enter>.

Ключи можно выдавать по одному или в массовом порядке.

9. 1. 4. 1. Выдача одного парно-выборочного ключа

Если требуется выдать из ЦВК ключ для абонента с определенным номером, то в окне списка парно-выборочных ключей серии следует установить курсор на строке с требуемым номером и нажать клавишу <Enter>.

Ключи выдаются на USB-носитель. В появившемся информационном окне, где находятся сведения об имени абонента и номере выдаваемого парно-выборочного ключа, установите флаг «Выдать ключ» по нажатию клавиши <Пробел> на строке с флагом, продолжите операцию, нажав кнопку «Выдать».

Парно-выборочный ключ можно выдать как отдельно, так и вместе с ключом ПДСЧ.

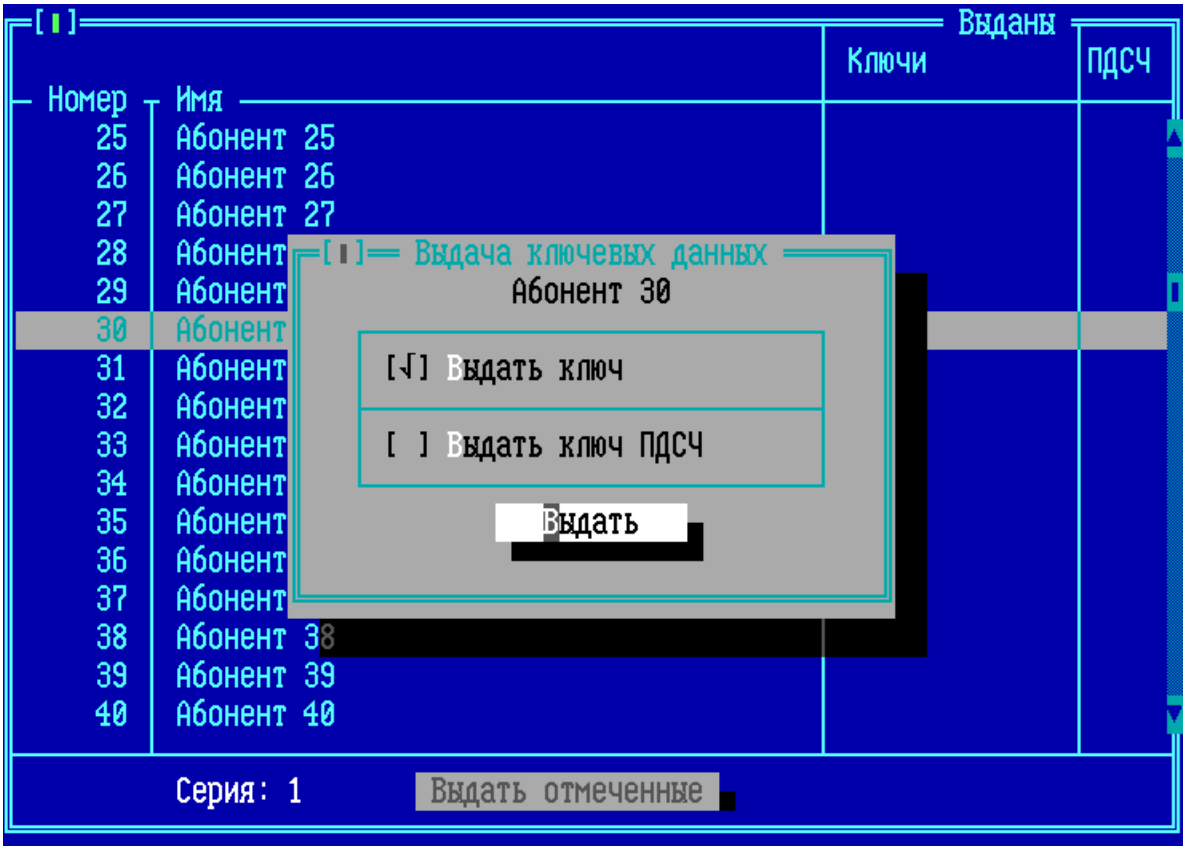

Рисунок 80 - Подтверждение выдачи ключа

Если выдаваемый ключ ранее был выдан, то в окне выдачи этот ключ будет отмечен знаком «+». Для повторно выдачи необходимо выбрать флаг «Выдать ключ» и установить знак «√» по нажатию клавиши <Пробел>, затем выдать ключ заново.

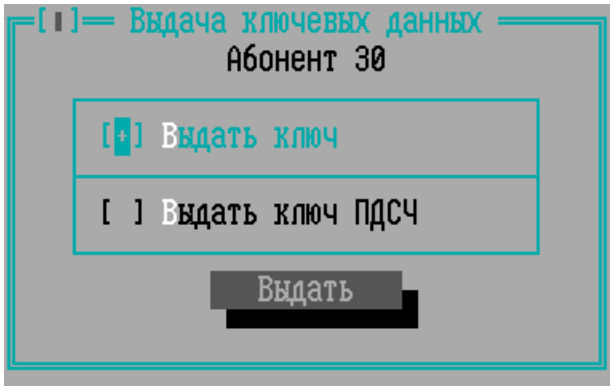

Рисунок 81 - Ранее выданный ключ

Подключите USB-носитель к ЦВК и подтвердите готовность записи ключа на носитель.

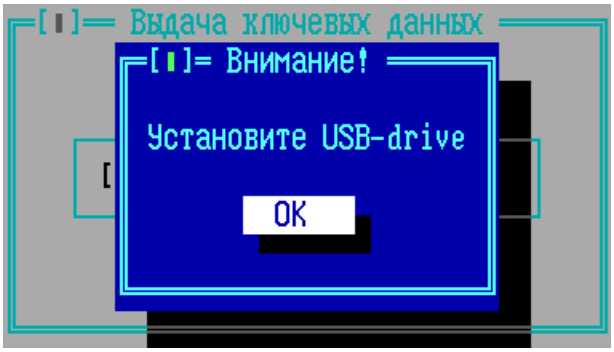

Рисунок 82 - Запрос на подключение USB-носителя

Будет произведена запись файла в корневой каталог подключенного к ЦВК USB-носителя, также можно выбрать каталог для записи.

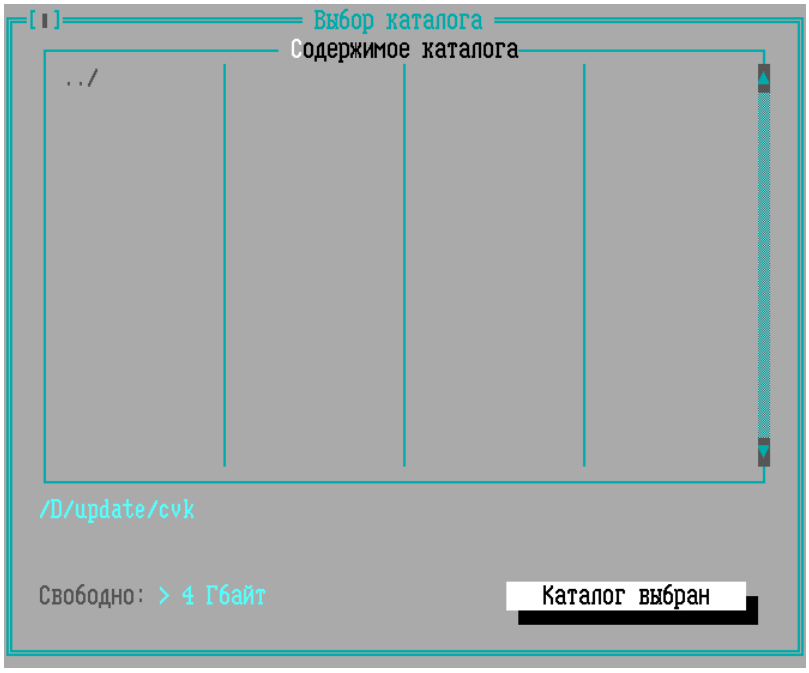

Рисунок 83 - Выбор каталога для записи файла парно-выборочного ключа

В случае, если файл уже существует, он будет перезаписан.

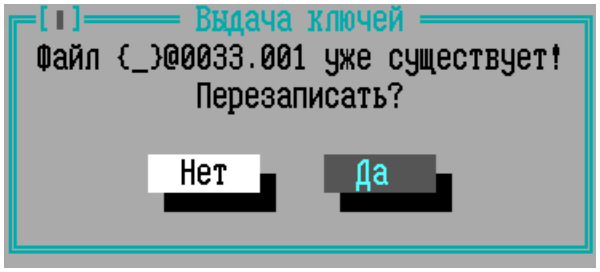

Рисунок 84 - Запись парно-выборочного ключа

Для отмены выдачи и возврата в окно списка ключевых данных серии, нажмите <Esc>.

После нажатия кнопки «ОК» и выбора каталога парно-выборочный ключ указанного номера будет записан на USB-носитель, а в списке ключевых данных серии появится запись о выдаче ключа на носитель. Выданный ключ отмечается знаком «+» в списке.

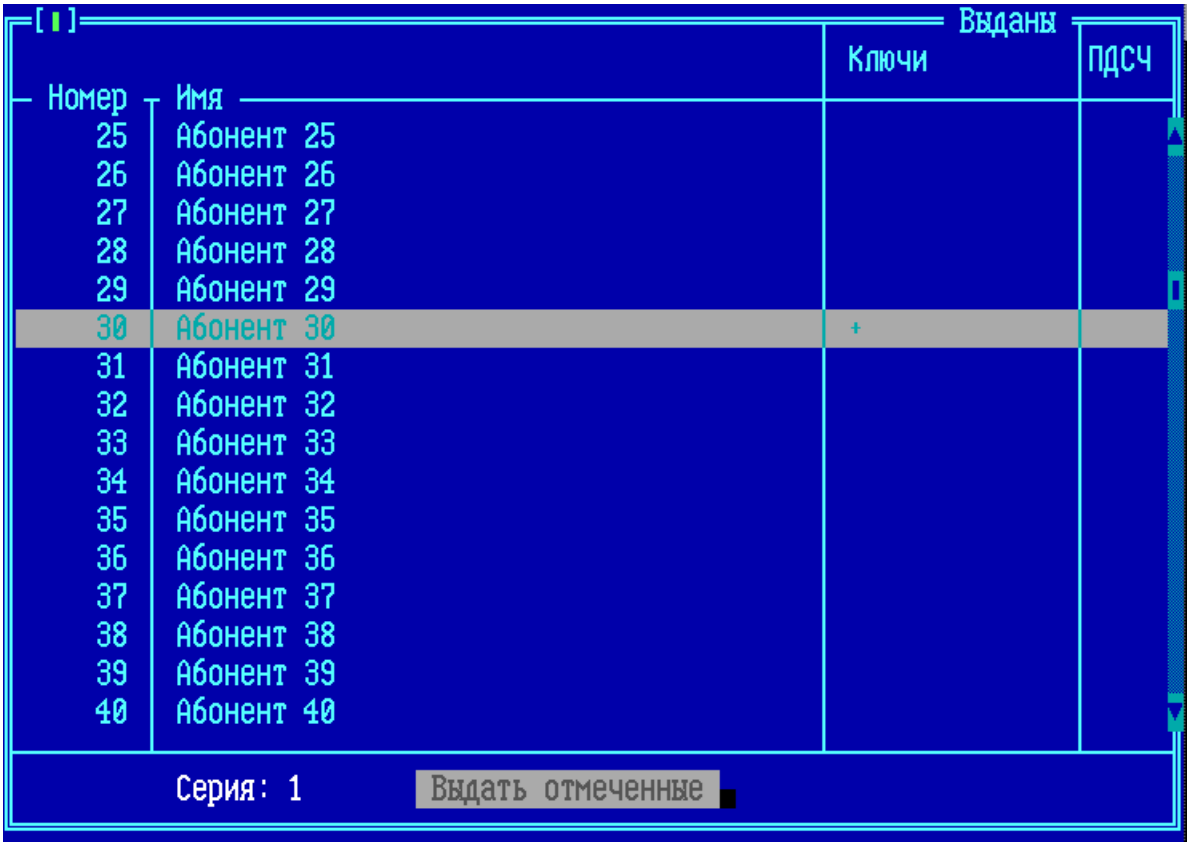

Рисунок 85 - Выданный ключ отмечается знаком «+»

Файл парно-выборочного ключа на внешнем носителе - файл вида «{_} @X+3.00N», где X - четырехразрядный номер абонента, N - серия ключа.

9. 1. 4. 2. Массовая выдача парно-выборочных ключей

Ключевые данные могут быть выданы не только по одному, но и сразу группой. Для этого следует:

- отметить в списке окна абонентов, ключи для которых требуется выдать. Абонент отмечается знаком «√» на выбранной курсором строке по нажатию клавиши <Пробел>;
- выполнить команду «Выдать отмеченные», переход на которую из списка ключевых данных серии осуществляется нажатием клавиши <Tab>.

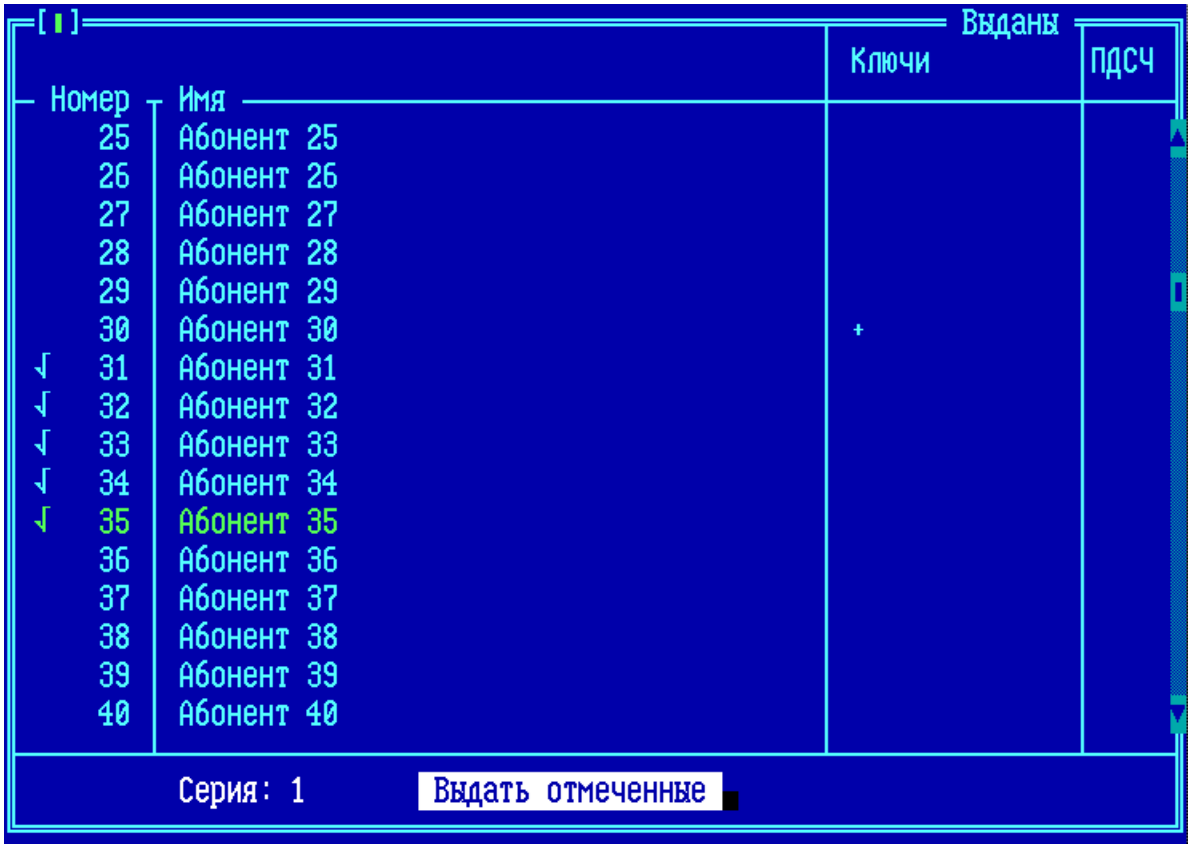

Рисунок 86 - Отмеченные для выдачи ключи серии

После выполнения команды «Выдать отмеченные» в окне выдачи ключевых данных для отмеченных абонентов необходимо активировать флаг «Выдать ключ» по нажатию клавиши <Пробел>. Для отмеченных абонентов можно выдать как одни парно-выборочные ключи, так и вместе с ключами ПДСЧ. Если требуется выдать парно-выборочные ключи вместе с ключами ПДСЧ, дополнительно активируйте флаг «Выдать ключ ПДСЧ».

Нажмите кнопку «Выдать» для продолжения.

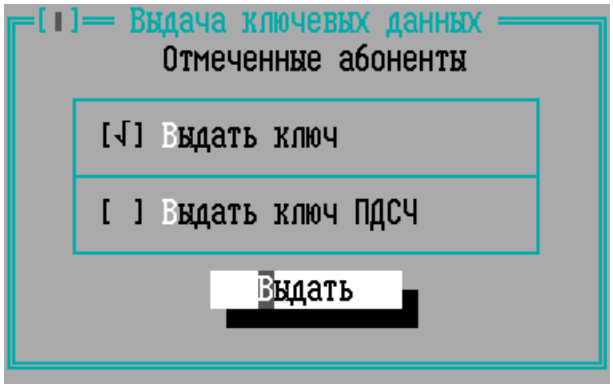

Рисунок 87 - Окно выдачи ключей ПДСЧ

Система предложит подключить к ЦВК USB-носитель, на который будут записаны ключевые данные. Подключите USB-носитель к ЦВК и нажмите «ОК»:

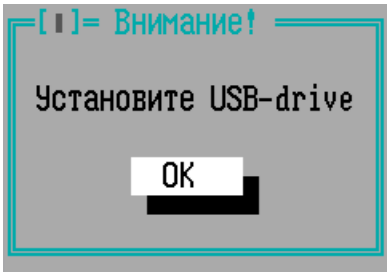

Рисунок 88 - Запрос на подключение USB-носителя

Будет произведена запись файлов парно-выборочных ключей в корневой каталог подключенного к ЦВК USB-носителя, также можно выбрать каталог для записи.

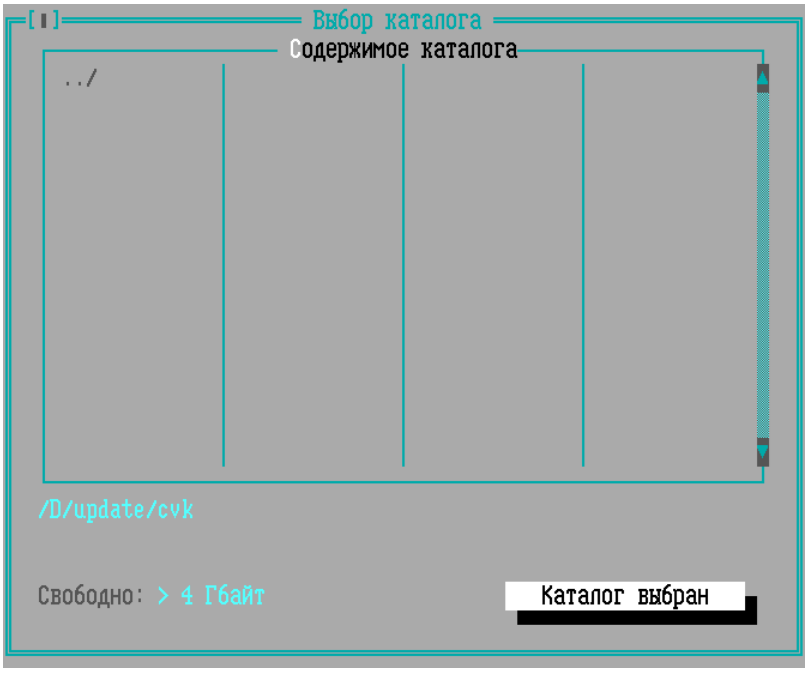

Рисунок 89 - Выбор каталога для записи файлов парно-выборочных ключей

По завершению процесса записи парно-выборочных ключей на USB-носитель, будет осуществлен возврат к окну списка парно-выборочных ключей данной серии, абоненты с выданными для них ключами будут отмечены знаком «+».

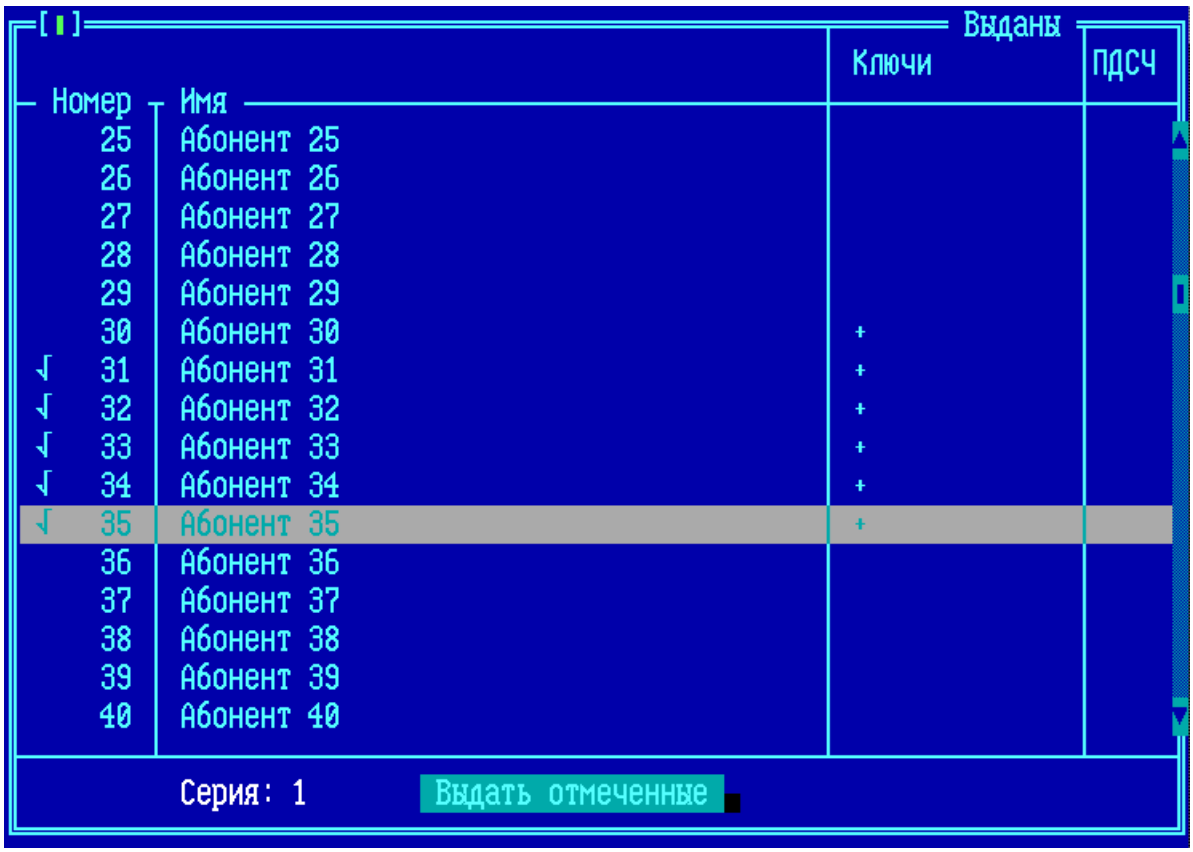

Рисунок 90 - Выданные ключи серии

9. 1. 4. 3. Выдача ключа ПДСЧ

Ключ ПДСЧ выдается на USB-носитель по команде администратора из окна списка парно-выборочных ключей. В окне списка парно-выборочных ключей серии следует установить курсор на строке с выбранным абонентом и нажать клавишу <Enter>.

В появившемся информационном окне, где находятся сведения об имени абонента, выделите флаг «Выдать ключ ПДСЧ» и нажмите клавишу <Пробел>, подтвердите операцию, нажав кнопку «Выдать».

Ключ ПДСЧ можно выдать как отдельно, так и вместе с парно-выборочным ключом.

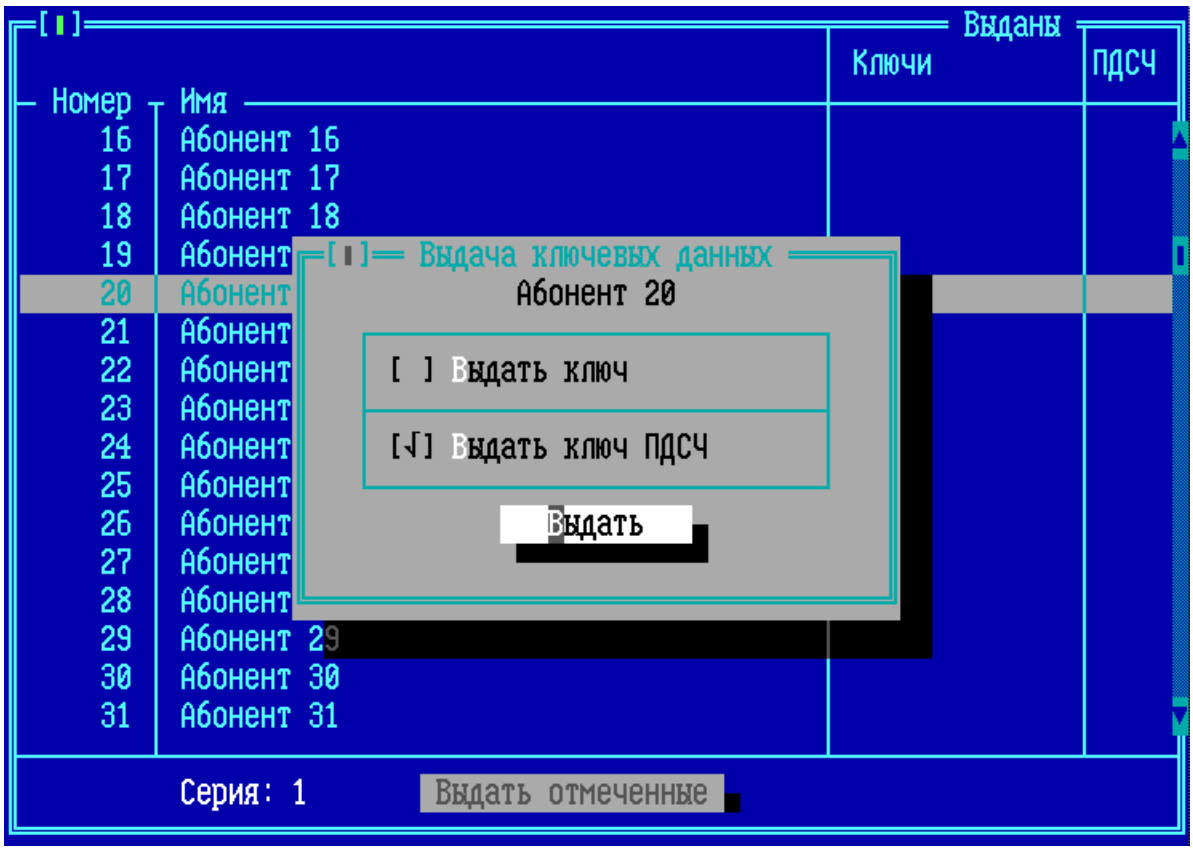

Рисунок 91 - Подтверждение выдачи ключа

Каждый раз генерируется и выдается новый ключ ПДСЧ.

Если выдаваемый ключ ранее был выдан, то в окне выдачи этот ключ будет отмечен знаком «+». Для повторной выдачи необходимо выбрать флаг «Выдать ключ ПДСЧ» и установить знак «√» по нажатию клавиши <Пробел>, затем выдать ключ заново.

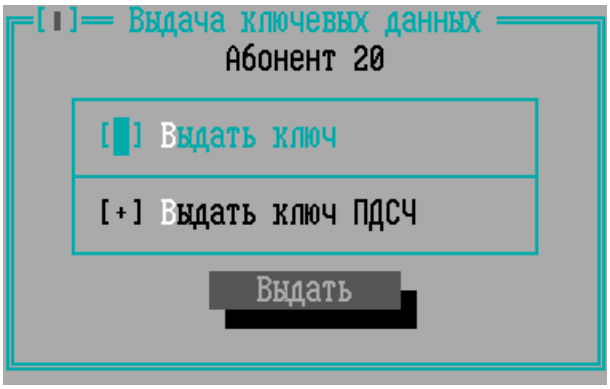

Рисунок 92 - Ранее выданный ключ

Подключите USB-носитель к ЦВК и подтвердите готовность записи ключа ПДСЧ на носитель, нажав кнопку «ОК».

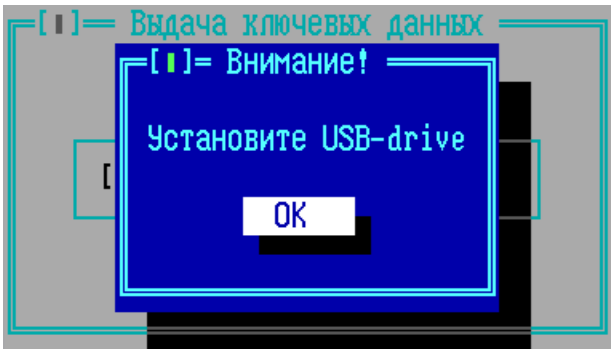

Рисунок 93 - Запрос на подключение USB-носителя

Будет произведена запись файлов в корневой каталог подключенного к ЦВК USB-носителя, также можно выбрать каталог для записи.

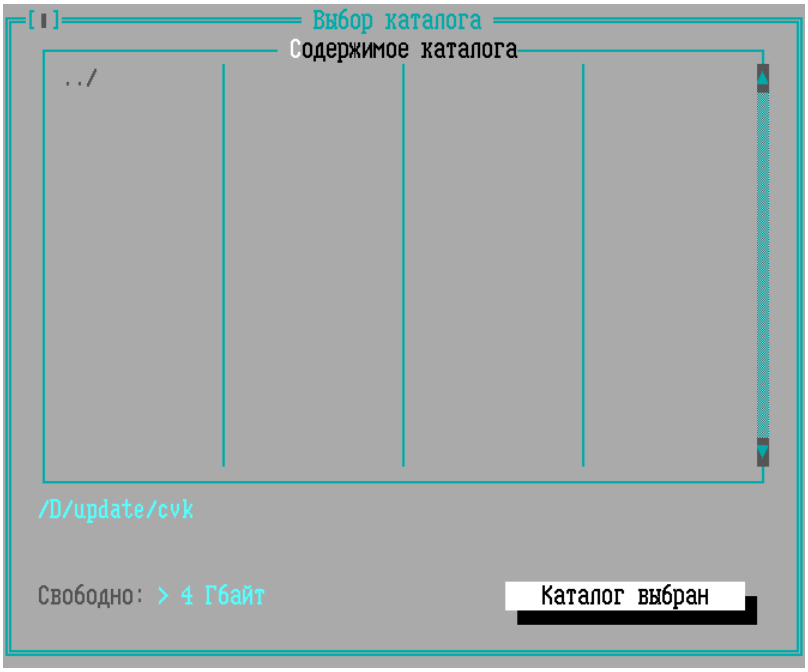

Рисунок 94 - Выбор каталога для записи файла парно-выборочного ключа

В случае, если файл с таким именем в указанном каталоге уже существует, будет предложено его перезаписать.

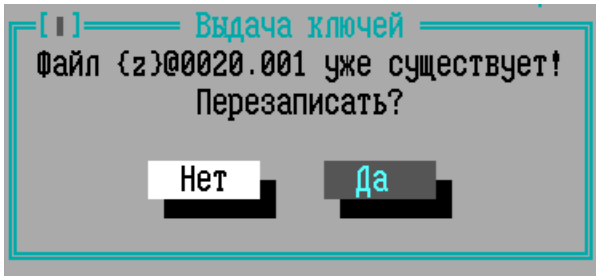

Рисунок 95 - Запись парно-выборочного ключа

Для отмены выдачи и возврата в окно списка ключевых данных серии, нажмите <Esc>.

После нажатия кнопки «ОК» и выбора каталога ключ ПДСЧ для указанного номера абонента будет записан на USB-носитель.

В списке ключевых данных серии появится запись о выдаче ключа ПДСЧ на носитель. Выданный ключ отмечается знаком «+» в списке:

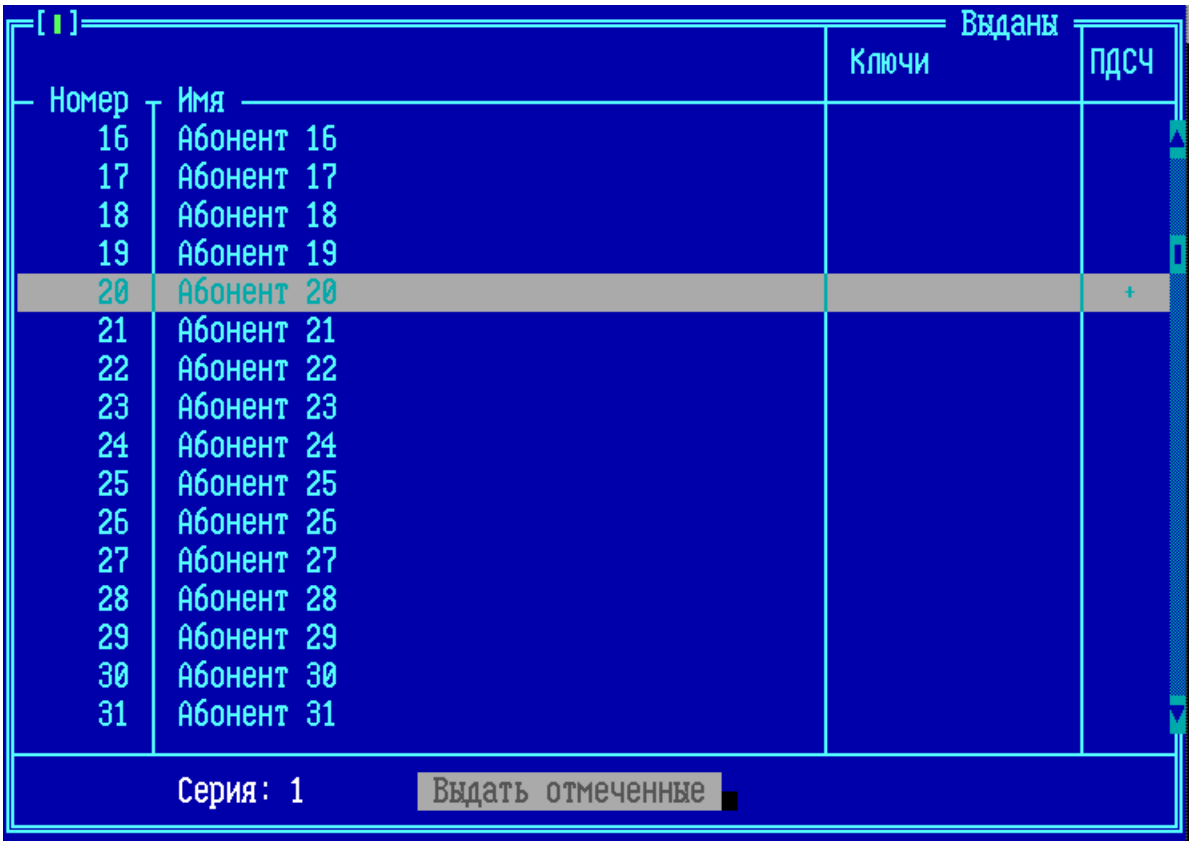

Рисунок 96 - Выданный ключ отмечается знаком "+"

Файл ключа ПДСЧ на внешнем носителе - файл вида «{z}@XXXX.00N»,

где «{z}@X» - служебный текст, признак файла с ключом ПДСЧ; «XXXX» - четырехразрядный номер абонента; «N» - серия ключа.

9. 1. 4. 4. Массовая выдача ключей ПДСЧ

Ключи ПДСЧ выдаются на USB-носитель. Ключи ПДСЧ могут быть выданы не только по одному, но и группой. Для этого следует:

- установить курсор на список абонентов нажатием клавиши <Tab>;
- отметить абонентов, ключи для которых требуется выдать. Абонент отмечается знаком «√» на выбранной курсором строке по нажатию клавиши <Пробел>;
- выполнить команду «Выдать отмеченные», переход на которую из списка абонентов осуществляется нажатием клавиши <Tab>.

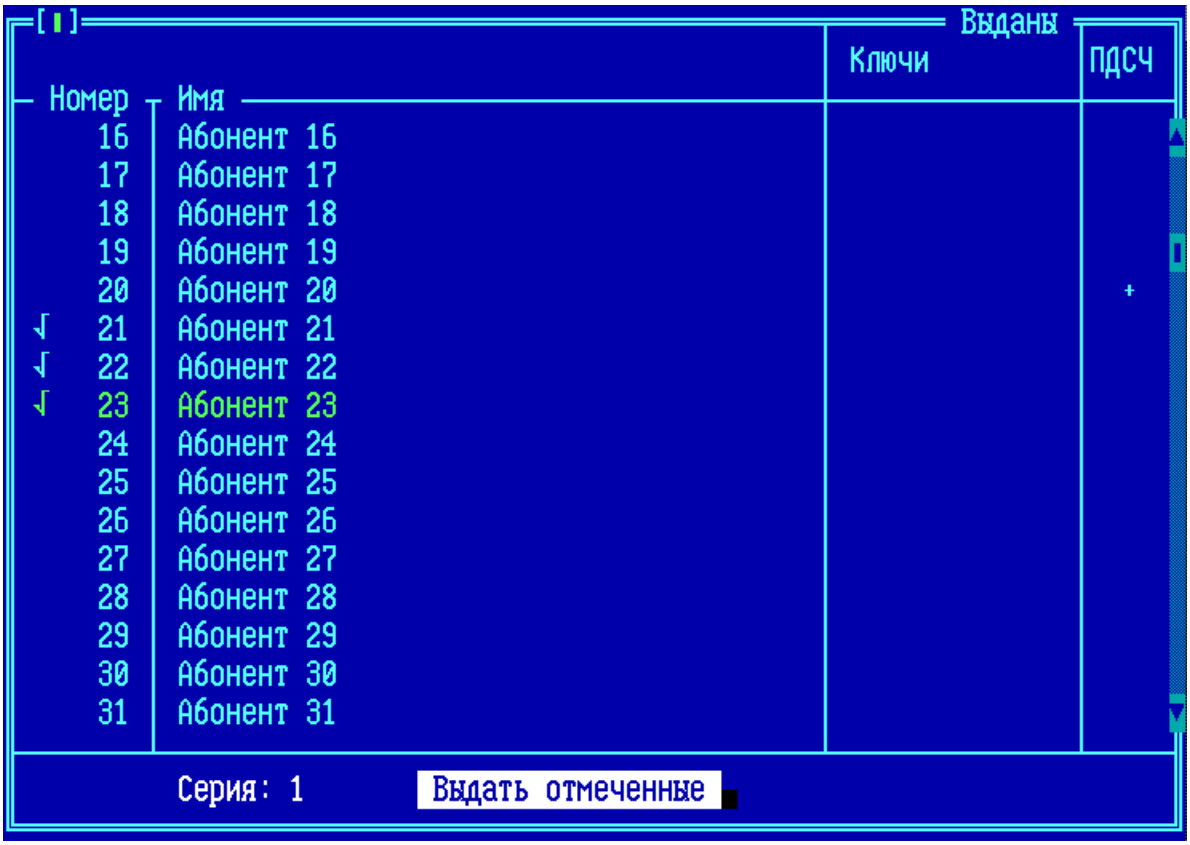

Рисунок 97 - Отмеченные для выдачи ключи серии

После выполнения команды «Выдать отмеченные» в окне выдачи ключевых данных необходимо активировать флаг «Выдать ключ ПДСЧ». Ключ ПДСЧ можно выдать как отдельно, так и вместе с парно-выборочным ключом.

Установите флаг «Выдать ключ ПДСЧ» по нажатию клавиши <Пробел> и нажмите кнопку «Выдать».

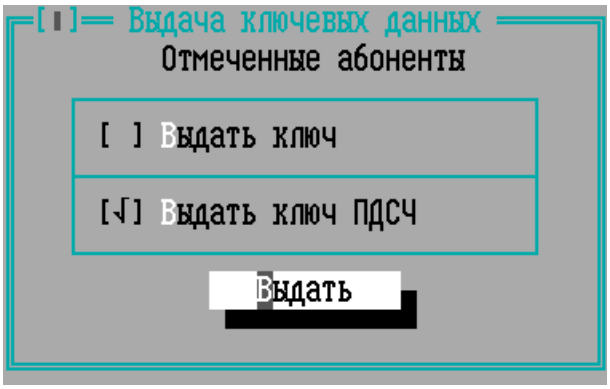

Рисунок 98 - Окно выдачи ключей ПДСЧ

Система предложит подключить к ЦВК USB-носитель, на который будут записаны ключи ПДСЧ. Подключите USB-носитель к ЦВК и нажмите «ОК».

Каждый раз генерируется и выдается новый ключ ПДСЧ.

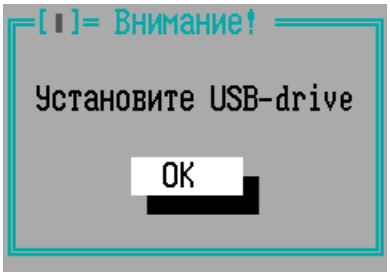

Рисунок 99 - Запрос на подключение USB-носителя

Будет произведена запись файлов ключей ПДСЧ в корневой каталог подключенного к ЦВК USB-носителя, также можно выбрать каталог для записи.

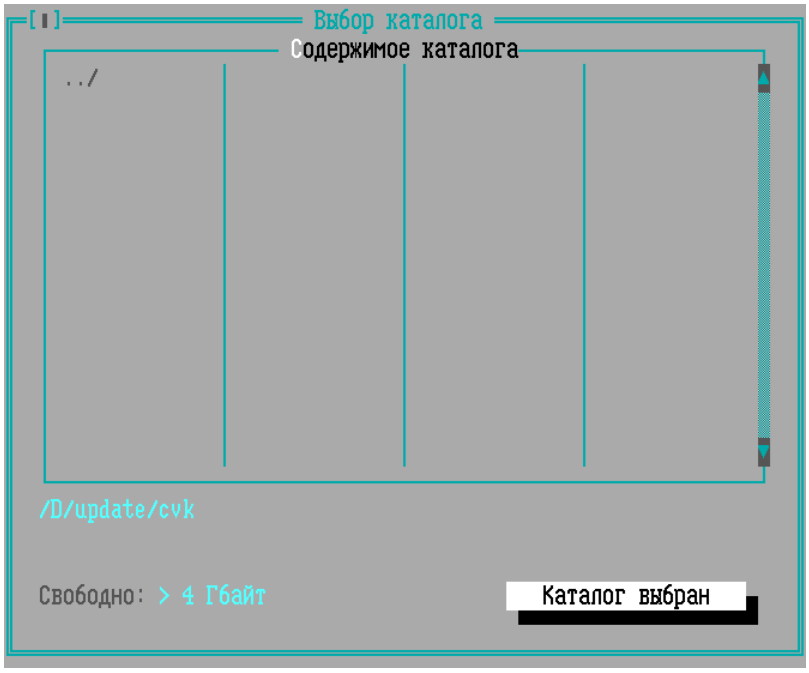

Рисунок 100 - Выбор каталога для записи файлов парно-выборочных ключей

По завершению процесса записи ключей ПДСЧ на USB-носитель, будет осуществлен возврат к окну списка парно-выборочных ключей данной серии, а записи выданных ключей будут отмечены знаком «+».

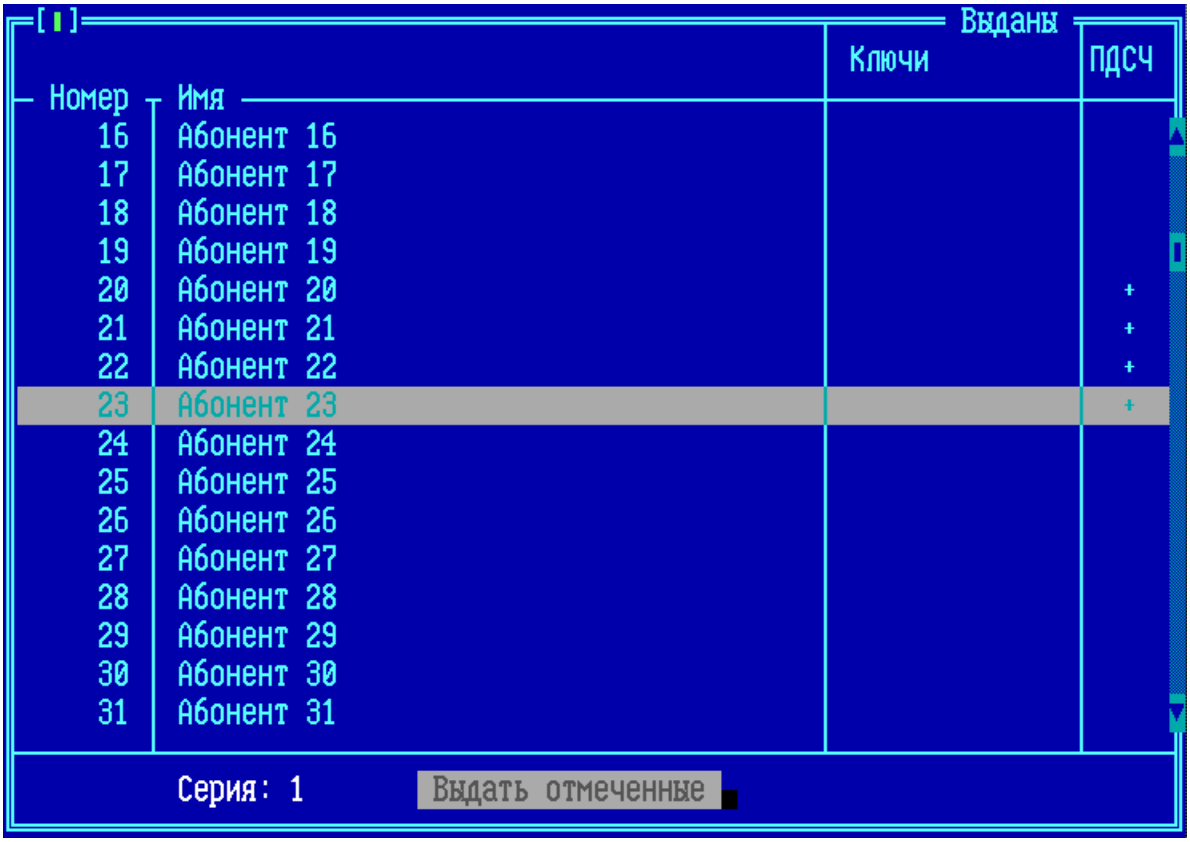

Рисунок 101 - Выданные ключи ПДСЧ

9. 2. Импорт и экспорт серий ключевых данных

Зарегистрированные в ЦВК центры криптосетей ФПСУ вместе со всеми созданными в них сериями парно-выборочных ключей могут быть экспортированы из ЦВК на внешний носитель, в зашифрованном на ключе экспорта виде.

Экспорт осуществляется в файл формата «<центр>.asX», где X может быть 1, 2 или 3, обозначая класс ключей СКЗИ, КС1, КС2 или КС3 соответственно (см. пункт «Экспорт центра ЦВК»). Ключ экспорта может быть записан на USB-носитель или ТМ-идентификатор, и обязателен для предъявления при импорте центра обратно в ЦВК (см. пункт «Импорт центра ЦВК»).

Экспортированные таким образом центры криптосетей могут быть, при наличии ключа экспорта, импортированы обратно на ЦВК. В процессе импорта имеющиеся в ЦВК данные центра будут полностью перезаписаны

импортируемыми.

ВНИМАНИЕ! Для ПО ЦВК не рекомендуется использовать ТМ-идентификатор в качестве носителя ключей. При использовании в качестве носителя ключа экспорта ТМ-Идентификатора Главного Администратора, ключ Главного Администратора на ТМ-Идентификаторе будет перезаписан! Это приведет к потере возможности администрировать ЦВК в дальнейшем! ТМ-идентификатор Главного Администратора ЗАПРЕЩЕНО использовать в качестве места хранения ключа экспорта!

9. 2. 1. Экспорт центра ЦВК

Экспорт центра ЦВК может быть выполнен в целях создания резервной копии ключевых и лицензионных данных, а также для переноса центра на другой ЦВК.

Для экспорта серий ключевых и лицензионных данных центра, следует выполнить команду «Экспортировать» окна списка типов ключей центра. Экспортируемые данные будут зашифрованы на специальном ключе экспорта.

Рисунок 102 - Список типов ключей центра

При экспорте центра производится инициализация ПДСЧ средствами биологического датчика случайных чисел, нажмите «Да» в диалоговом окне для продолжения.

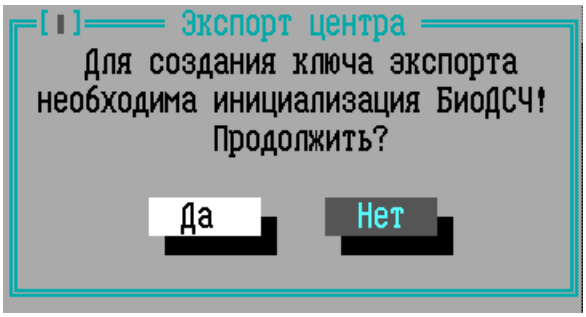

Рисунок 103 - Сообщение об инициализации БиоДСЧ

Запустится интерфейс БиоДСЧ. От администратора требуется двигать мышью в пределах экрана:

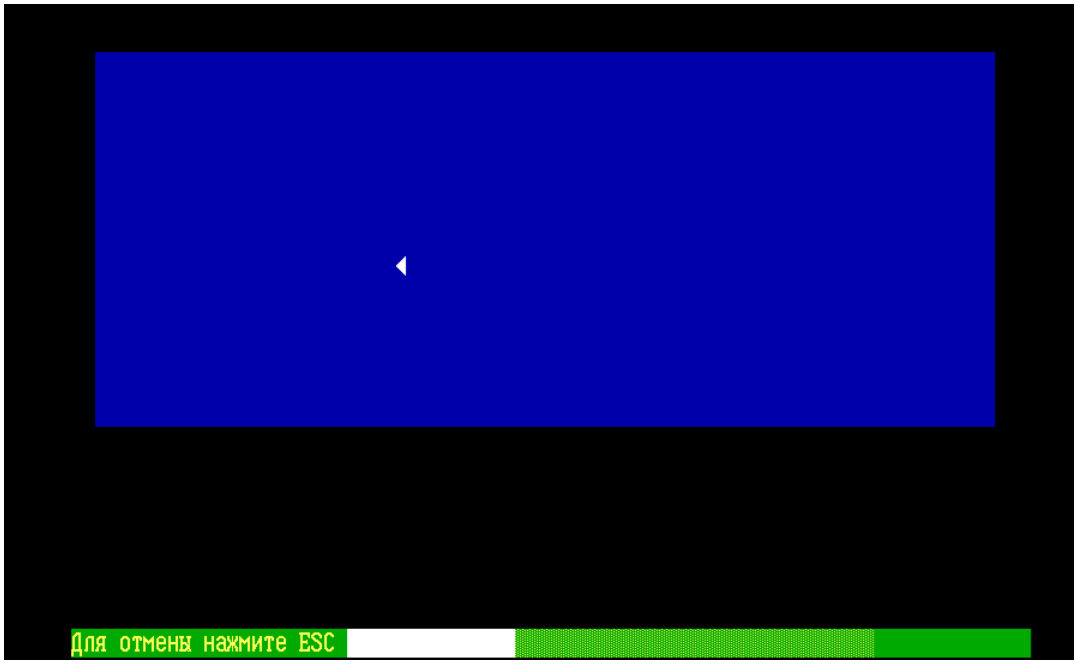

Рисунок 104 - Интерфейс БиоДСЧ

Переинициализация ПДСЧ завершится успешно, как только будет считано достаточное число случайных движений мыши. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <Esc> обратно в окно центра.

При экспорте центра КСЗ запрашивается срок действия ключа экспорта:

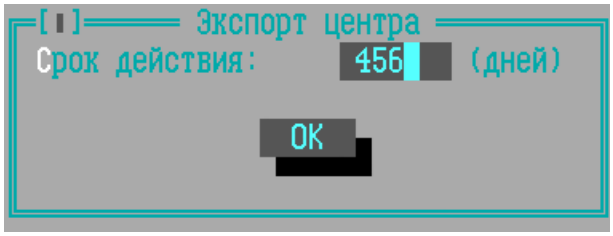

Рисунок 105 - Установка срока действия ключа экспорта

Затем на экран будет выдано окно выбора внешнего носителя, на который будет записан ключ экспорта, USB-носитель или ТМ-идентификатор.

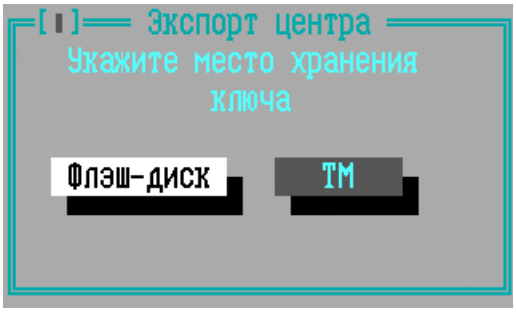

Рисунок 106 - Выберите место хранения ключа экспорта

Если в качестве места хранения выбран ТМ-идентификатор, то система предложит приложить его к ТМ-считывателю ЦВК для записи ключа экспорта.

Если в качестве места хранения выбран «Флэш-диск», то система предложит подключить к ЦВК USB-носитель для записи на него файла с ключом экспорта.

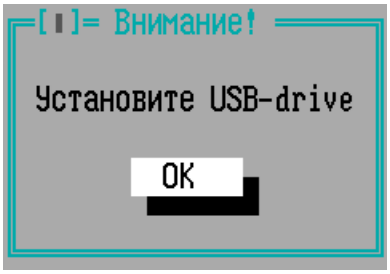

Рисунок 107 - Подтверждение подключения внешнего носителя

Файл записывается в корневую папку носителя, и в случае конфликта имен перезаписывает файл.

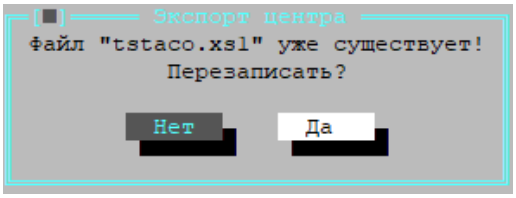

Рисунок 108 - Подтверждение перезаписи файла ключа экспорта

Критерием успешности экспорта ключа является системное оповещение «Запись прошла успешно!». Можно записать копию ключа экспорта на другой носитель, выбрав кнопку «Да».

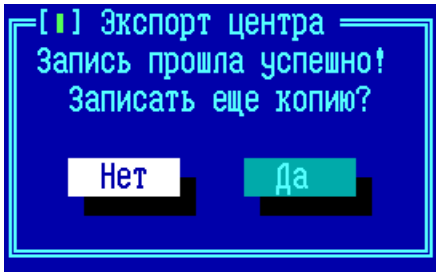

Рисунок 109 - Экспорт центра

После записи всех копий ключа экспорта на внешние носители, система предложит подключить USB-носитель, на который будет выдан зашифрованный файл с лицензией и парно-выборочными ключами экспортируемого центра:

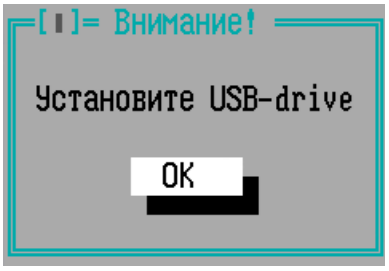

Рисунок 110 - Подключите USB-носитель к ЦВК

После успешной записи система выдаст сообщение «Выполнено». После этого можно отключать USB-носитель и продолжить работу с ЦВК в штатном режиме.

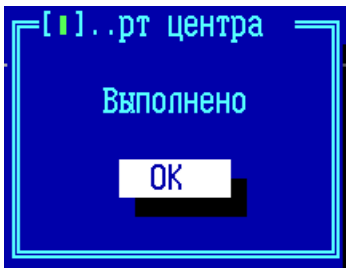

Рисунок 111 - Экспорт центра прошел успешно

9. 2. 2. Импорт центра ЦВК

Экспортированные ранее центры ЦВК могут быть импортированы обратно. При импорте, находящаяся в ЦВК информация о центре, включающая сгенерированные серии парно-выборочных ключей, будут полностью заменены импортируемыми данными.

Для импорта серий ключевых и лицензионных данных центра, следует выполнить команду «Импортировать» окна списка типов ключей центра:

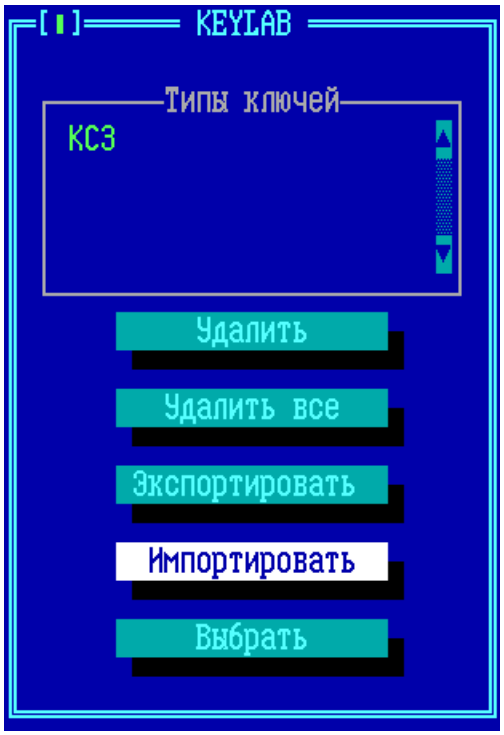

Рисунок 112 - Список типов ключей центра

После выполнения команды, система потребует предъявить ключ экспорта, на котором зашифрованы импортируемые данные. Во время

экспорта ключ мог быть сохранен и на ТМ-идентификатор, и в файл на внешний носитель.

Рисунок 113 - Выберите место хранения ключа экспорта

Если ключ экспорта был ранее сохранен в ТМ-идентификатор, то нажмите кнопку «ТМ». По предложению системы предъявите ТМ-идентификатор: в зависимости от типа носителя, приложите устройство touch-memory с ключом экспорта к ТМ-считывателю ЦВК или подключите к USB порту ЦВК устройство TM-Key.

Если ключ экспорта был ранее сохранен в файл, то нажмите кнопку «Флэш-диск», и по предложению системы, подключите USB-носитель к ЦВК для прочтения файла с ключом экспорта. Файл должен находиться в корневой папке носителя.

После уточнения места хранения ключа система предложит подключить к ЦВК USB-носитель для получения файла с ключом экспорта.

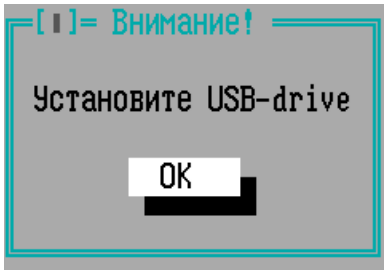

Рисунок 114 - Подтверждение получения ключа импорта

Далее выдается окно с подтверждением получения лицензии и парно-выборочных ключей импортируемого центра.

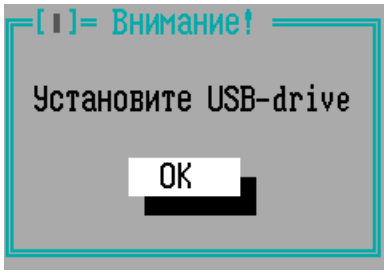

Рисунок 115 - Импорт данных

Если в ЦВК уже был зарегистрирован центр с тем же именем и тем же типом лицензии на ключи (КС1, КС2 или КС3), то при импорте будет выдано оповещение о перезаписи хранящихся в ЦВК данных импортируемыми.

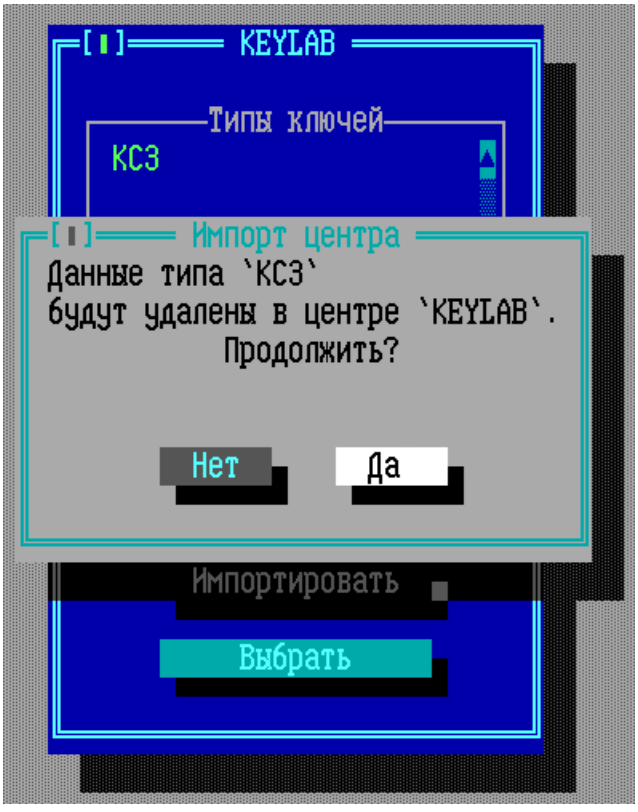

Рисунок 116 - Данные центра будут удалены

При штатном завершении процедуры импорта будет выдано сообщение «Выполнено».

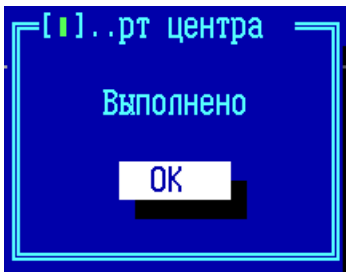

Рисунок 117 - Импорт центра

9. 3. Удаление ключевой информации

Серии парно-выборочных ключей, созданных на ЦВК, могут быть удалены. Для этого следует воспользоваться командами «Удалить» или «Удалить все» окна списка типа ключей центра:

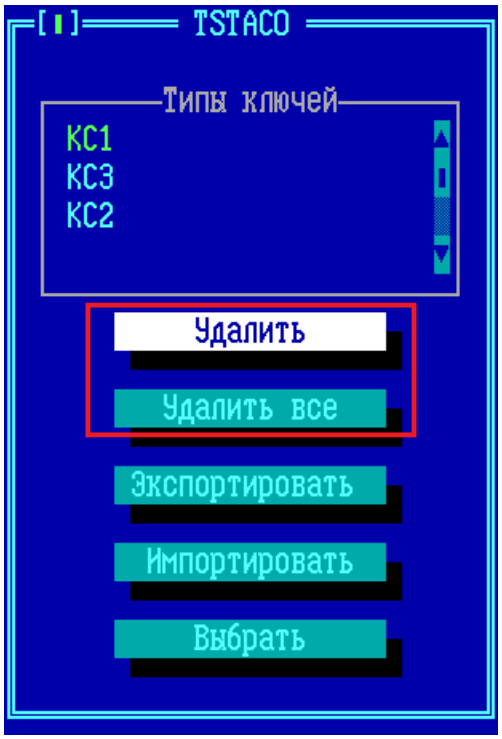

Рисунок 118 - Список типов ключей центра

Команда «Удалить» запускает процесс удаления ключевых данных центра одного выбранного типа (КС1, КС2 или КС3) с ЦВК. Обратите внимание, что в случае удаления всех типов ключевых данных из списка, происходит удаление записи центра из ЦВК:

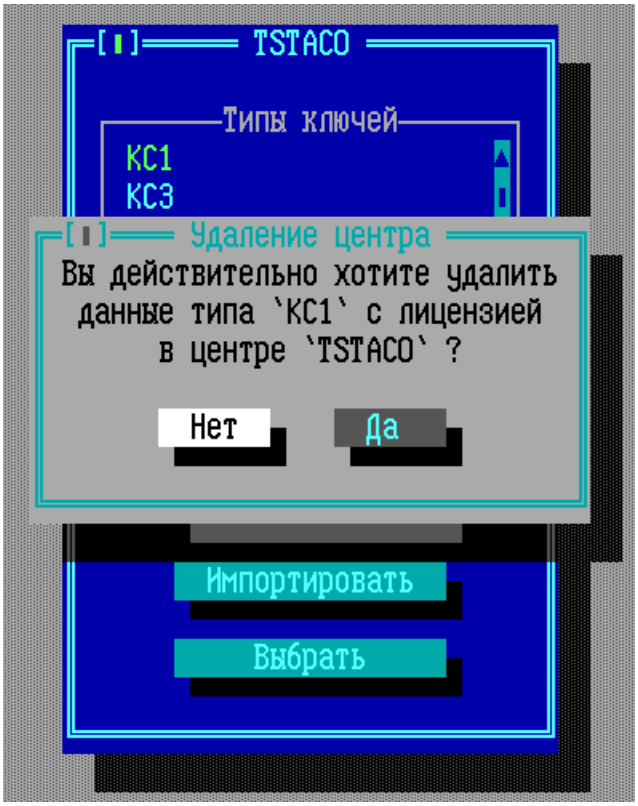

Рисунок 119 - Удаление ключей одного типа

Нажмите кнопку «Да» в появившемся окне для удаления с ЦВК всех серий выбранного типа ключевых данных. В случае успешного удаления будет выдано служебное оповещение «Выполнено», в случае если был удален последний тип ключевых данных будет выдано оповещение «В центре '% Имя_центра%' удалены данные типа "КСХ"» или «В центре '%Имя_центра%' удалены данные типа "КСХ" с лицензией».

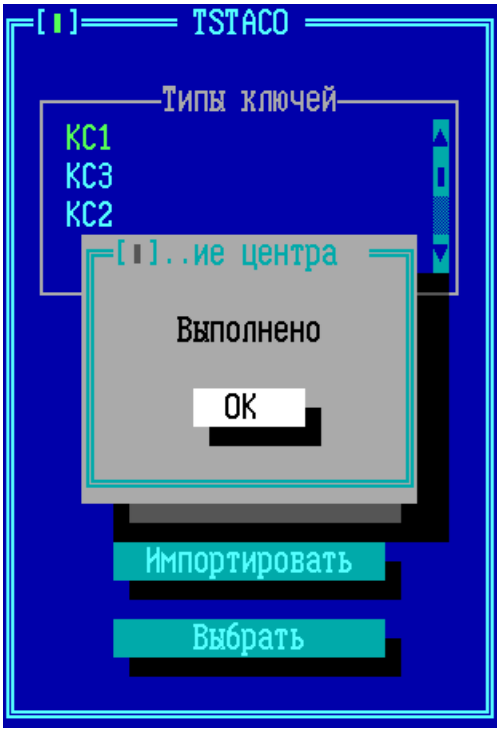

Рисунок 120 - Удаление ключей одного типа

Команда «Удалить все» окна списка типов ключевых данных удаляет с ЦВК и все серии ключевых данных всех зарегистрированных типов, и запись об удаляемом центре вместе с лицензией. Для повторного использования центра его придётся заново зарегистрировать на ЦВК (см. пункт «Регистрация центра в ЦВК»).

10. Ключи ProtoQa для СКЗИ

Генерация парно-выборочных ключей для СКЗИ-Потребителей доступна по команде главного меню «Ключи ProtoQa для СКЗИ».

Рисунок 121 - Главное меню ЦВК

Операция доступна администраторам класса «Оператор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

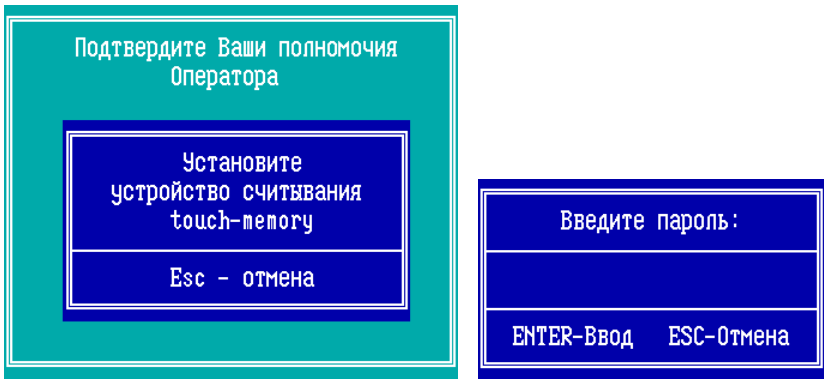

Рисунок 122 - Подтверждение полномочий и ввод пароля ТМ

В открывшемся окне отображается информация о зарегистрированных СКЗИ-Потребителях, при первом открытии список пуст. В окне «Список СКЗИ-Потребителей» задаются абоненты квантовой сети, которым ФПСУ распределяет квантовые ключи и с которыми ФПСУ строит квантовые туннели.

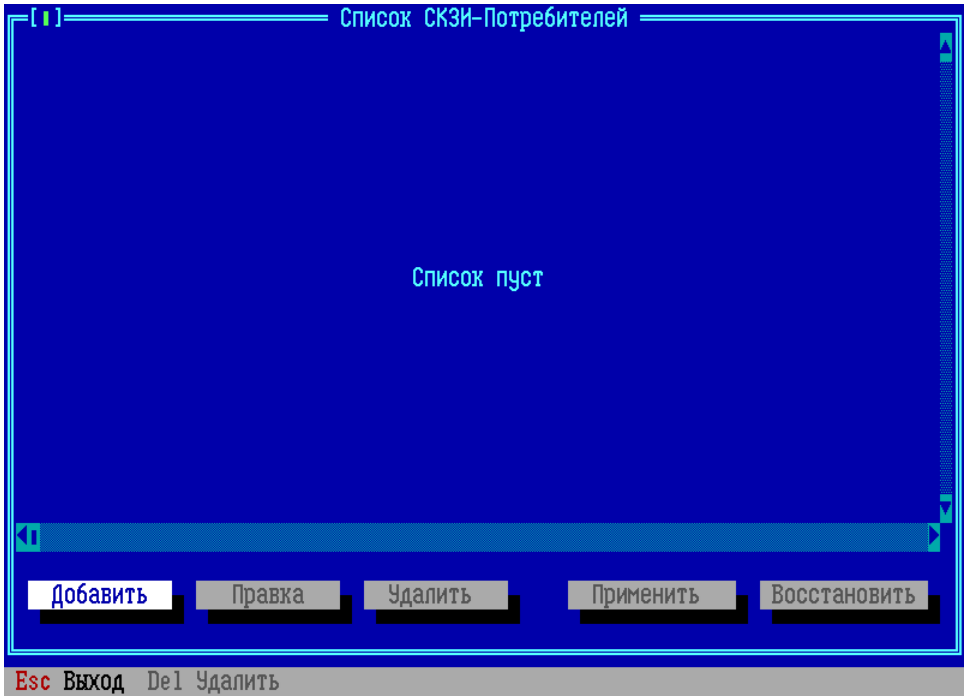

Рисунок 123 - Список СКЗИ-Потребителей

По кнопке «Добавить» или по нажатию клавиши <Ins> открывается окно «СКЗИ-Потребителей»:

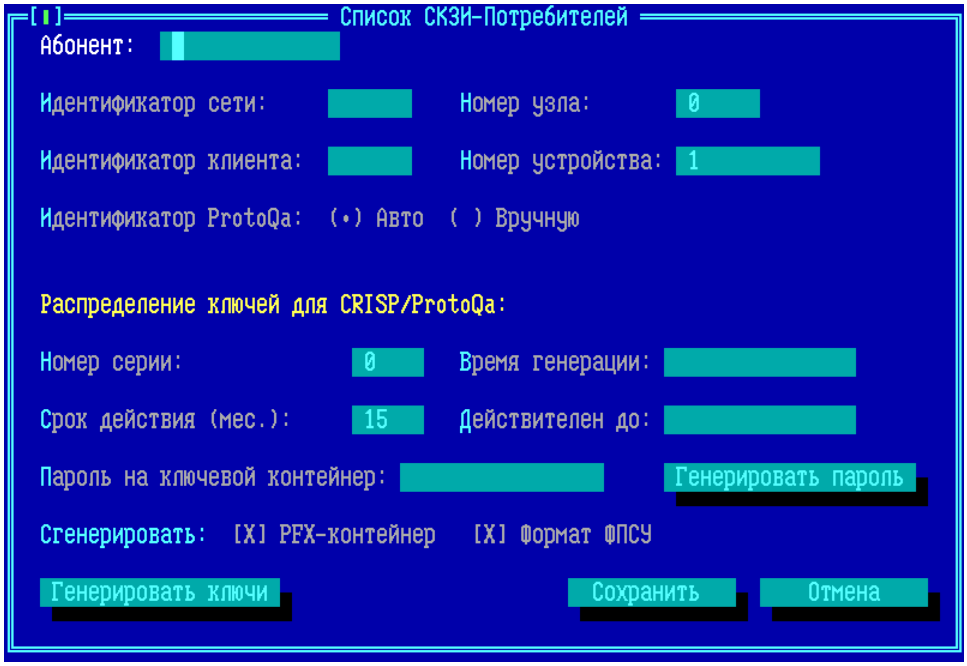

Рисунок 124 - Добавление абонента

Установите следующие параметры:

«**Абонент**» – текстовое описание СКЗИ-Потребителя.

Абонент получает пару ключей для обмена сообщениями между указанными узлами квантовой сети. Узел данного ФПСУ будет являться локальным СКЗИ для этого абонента, удаленный квантовый узел будет являться парным СКЗИ для этого абонента. На удаленном узле требуется выполнить зеркальные настройки для данного абонента, локальным СКЗИ будет являться парный СКЗИ.

Идентификатор сети и Номер узла составляют уникальный идентификатор узла в квантовой сети.

«**Идентификатор сети**» – Идентификатор сети содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры. Идентификатор сети назначается администратором квантовой сети. Внутри одного идентификатора сети объединяются узлы с общим технологическим устройством, правилами подключения и тарификации. Это могут быть узлы внутри сегмента сети или всей сети одного оператора.

«**Номер узла**» – уникальный в пределах указанной сети номер, присваиваемый данному ФПСУ, число от 1 до 64999. Номер согласуется с администратором безопасности квантовой сети и не должен быть произвольным.

«**Идентификатор клиента**» – уникальный 4-х-символьный идентификатор клиента (абонента) в квантовой сети. Присваивается администратором квантовой сети. Идентификатор клиента, содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры.

«**Номер устройства**» – идентификатор клиентского устройства. Уникальный в пределах указанного узла номер, присваиваемый устройству, являющемуся потребителем ключей. Значение по умолчанию - «1». Другие значения выставляются, если данный клиент имеет несколько различных устройств на указанном узле.

«**Идентификатор ProtoQa**» – идентификатор формируется автоматически из атрибутов узла при установлении флага «Авто», либо вводится в отдельное поле при установлении флага «Вручную». для СКЗИ-Потребителей производства ООО «АМИКОН», либо совместимых с ними в части адресации на квантовой сети, переключатель следует оставить в положении «Авто». В ином случае следует перевести переключатель в положение «вручную» и заполнить вручную идентификатор в виде 32-значного числа в hex-формате (используются цифры от «0» до «9» и латинские буквы от «a» до «f».

Для генерации ключевых данных следует задать обязательный параметр «**Срок действия**» ключей.

«**Срок действия (мес.)**» – срок действия парно-выборочного ключа отсчитывается с момента генерации, по умолчанию составляет 15 месяцев. До истечения срока действия текущих ключевых данных требуется повторно сгенерировать и установить новые ключевые данные на местах использования СКЗИ. Допустимые сроки действия ключей указываются в правилах пользования СКЗИ.

Далее требуется заполнить «**Пароль на ключевой контейнер**»

вручную, либо сгенерировать пароль автоматически, нажав на кнопку «Генерировать пароль».

Далее следует указать в каком из форматов генерировать ключи: «**PFX-контейнер**» имеет парольную защиту и подходит для произвольных СКЗИ, поддерживающих протокол ProtoQa; «**Формат ФПСУ**» подходит только для СКЗИ производства ООО «АМИКОН» и не требует ввода пароля, использования такого формата регулируется правилами безопасности квантовой сети.

При нажатии кнопки «Генерировать ключи» происходит запись ключей на внешний USB-носитель.

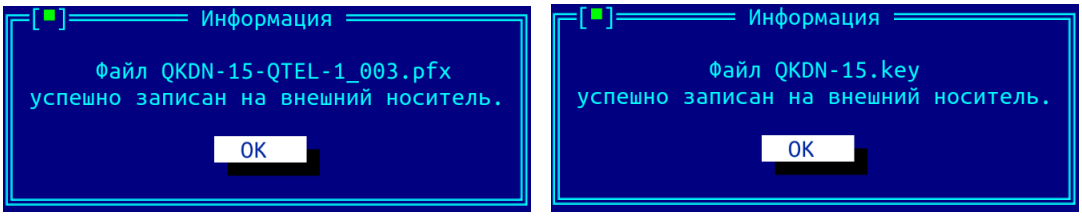

Рисунок 125 - Парно-выборочный ключ в выбранном формате записан на USB-носитель

Имя файла «PFX-контейнера» состоит из полного адреса СКЗИ-Потребителя и из номера серии, в адрес входят идентификатор узла, идентификатор клиента и номер устройства.

Имя файла в «формате ФПСУ» состоит только из идентификатора узла. Система позволяет накопить в одном файле несколько ключей для различных СКЗИ-Потребителей, расположенных на одном узле.

После записи ключей номер серии увеличивается автоматически.

По нажатию кнопки «Сохранить» запись о сгенерированных ключах сохраняется в список СКЗИ-Потребителей.

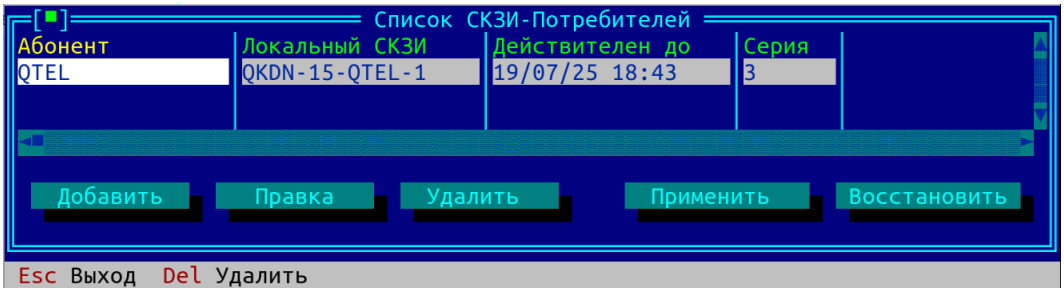

Рисунок 126 - Список СКЗИ-Потребителей

«**Номер серии**» – уникальный числовой идентификатор парно-выборочного ключа для протокола ProtoQa. При смене ключа увеличивается на 1. В случае компрометации парно-выборочного ключа ProtoQa необходимо сменить парно-выборочный ключ, для этого сгенерировать новый ключ, при генерации повысится номер серии.

«**Время генерации**» – дата и время генерации ключевых данных, проставляется автоматически в момент создания.

«**Действителен до**» – дата и время срока окончания действия ключевых данных, проставляется автоматически в момент создания.

Для просмотра сведений о парно-выборочном ключе абонента и для повторной генерации ключа следует выделить строку и нажать клавишу <Enter> или кнопку «Правка».

Для удаления парно-выборочного ключа абонента следует выделить строку абонента в списке и нажать клавишу <Del> или кнопку «Удалить».

Переход в таблице по строкам абонентов осуществляется клавишами <↑> и <↓>.

Для сохранения списка нажмите клавишу «Применить». Сохранение изменений с выходом в главное меню осуществляется по нажатии клавиши <F2>.

Выход с отменой внесенных изменений осуществляется по нажатию клавиши <Esc>, кнопка «Восстановить» отменяет внесенные за последний сеанс администрирования изменения без выхода из окна «Список СКЗИ-Потребителей».

11. Ключи для ККС ВРК

Генерация ключевых данных для защиты данных при передаче между сопряженными ККС ВРК и ФПСУ доступна по команде главного меню «Ключи для ККС ВРК».

Рисунок 127 - Главное меню ЦВК

Операция доступна администраторам класса «Оператор» и выше. При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ЦВК, кроме того вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

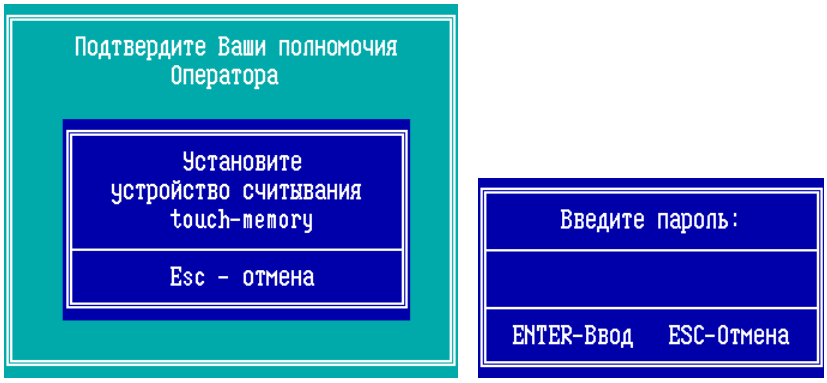

Рисунок 128 - Подтверждение полномочий и ввод пароля ТМ

В открывшемся окне отображается информация о зарегистрированных ККС ВРК, при первом открытии список пуст. В окне «Список ККС ВРК» задаются соседние узлы в топологии сети, которые будут являться источниками квантовых ключей для ФПСУ.

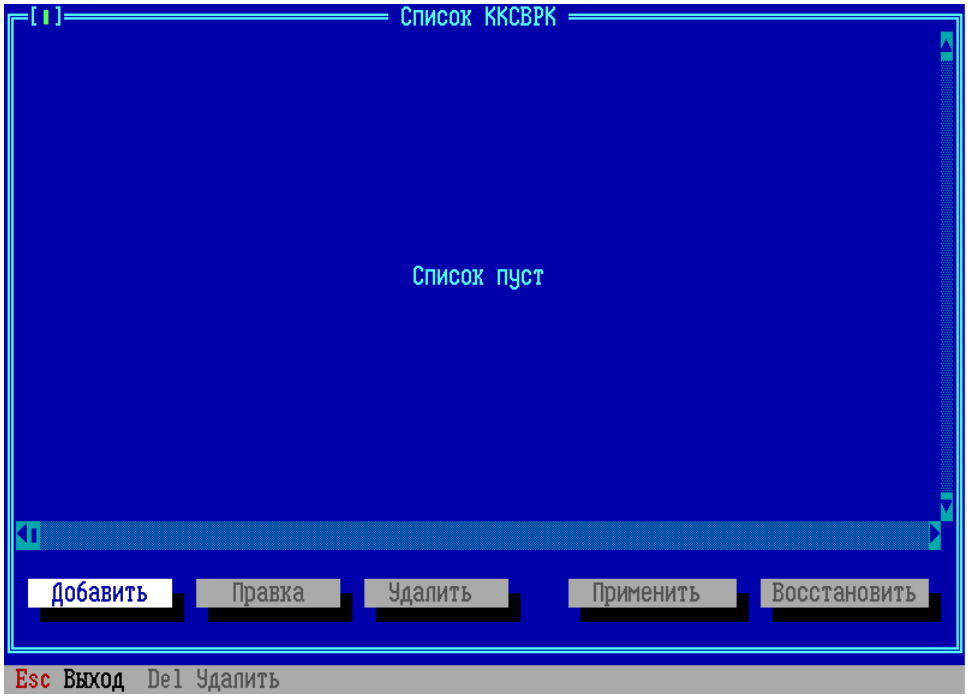

Рисунок 129 - Список ККС ВРК

По кнопке «Добавить» или по нажатию клавиши <Ins> открывается окно с настройками.

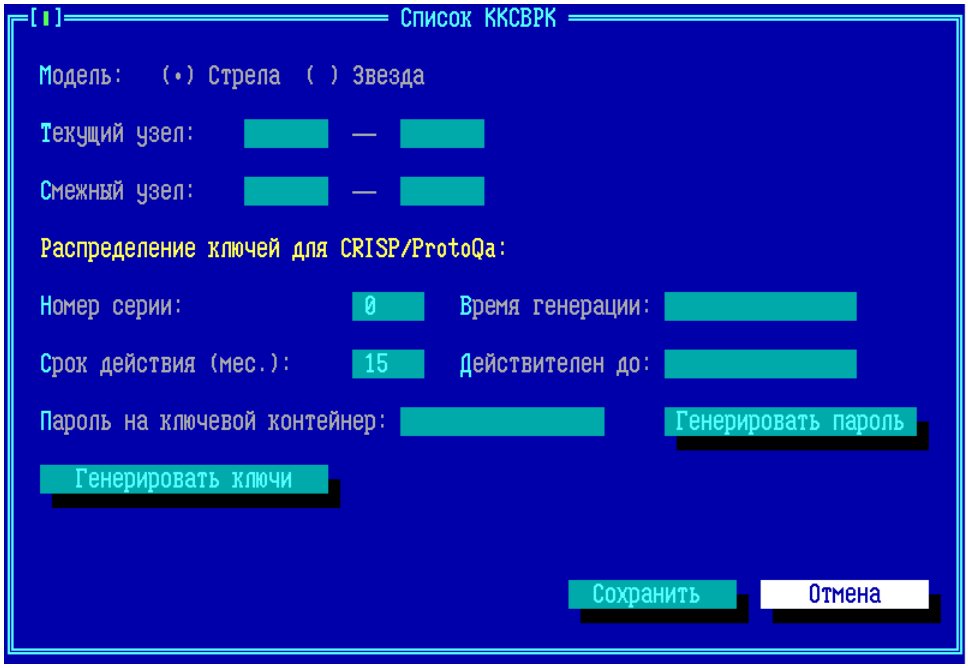

Рисунок 130 - Список ККС ВРК

«**Модель**» **–** переключатель, указывающий модель установленного на узле модуля КРК. Выбор из двух вариантов: «Стрела» для топологии точка-точка, либо «Звезда».

«**Текущий узел**» – идентификатор квантовой сети и номер узла ФПСУ, к которому подключена данная ККС ВРК.

«**Смежный узел**» – параметр модели «Стрела». Идентификатор квантовой сети и номер соседнего узла, с которым текущий узел вырабатывает квантовые ключи и строит квантовый туннель. Номер узла согласовывается с администратором безопасности квантовой сети.

«**Номер системы**» – параметр модели «Звезда». Получается от администратора безопасности квантовой сети.

Для генерации ключевых данных следует задать обязательный параметр «**Срок действия**» ключей.

«**Срок действия (мес.)**» – срок действия парно-выборочного ключа отсчитывается с момента генерации, по умолчанию составляет 15 месяцев. До истечения срока действия текущих ключевых данных требуется повторно сгенерировать и установить новые ключевые данные на местах использования

СКЗИ.

Далее следует заполнить «**Пароль на ключевой контейнер**» вручную, либо сгенерировать пароль автоматически, нажав на кнопку «Генерировать пароль».

При нажатии на кнопку «Генерировать ключи» происходит непосредственно генерация и запись ключей на внешние носители:

- для ККС ВРК модели «Стрела» происходит запись на Micro-SD карту;
- для ККС ВРК модели «Звезда» происходит запись на USB-токен производства ООО «АМИКОН»;
- для ФПСУ генерируется файл с названием «<идент. узла>.key».

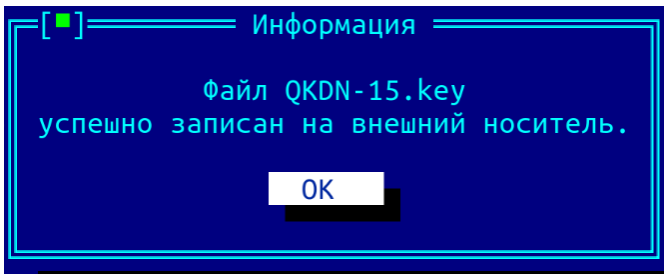

Рисунок 131 - Парно-выборочный ключ записан на USB-носитель

После записи ключей номер серии увеличивается автоматически.

По нажатию кнопки «Сохранить» запись о сгенерированных ключах сохраняется в список ККС ВРК.

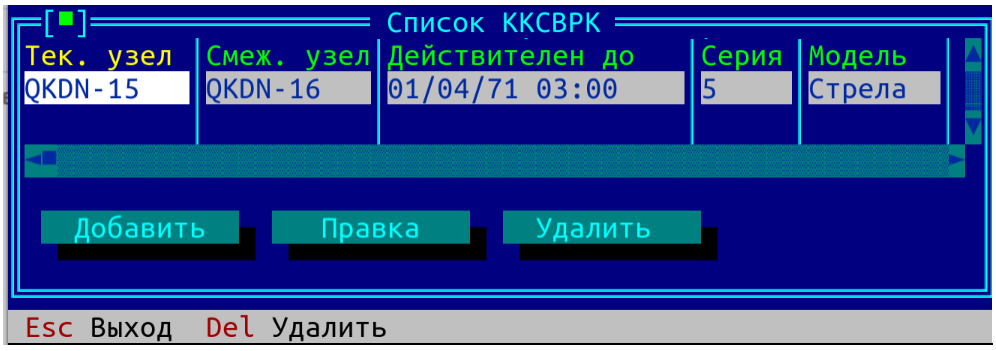

Рисунок 132 - Список ККС ВРК

«**Номер серии**» – уникальный числовой идентификатор парно-выборочного ключа. При смене ключа увеличивается на 1. В случае компрометации ключа необходимо сменить ключ, для этого сгенерировать

новый ключ, при генерации повысится номер серии.

«**Время генерации**» – дата и время генерации ключевых данных, проставляется автоматически в момент создания.

«**Действителен до**» – дата и время срока окончания действия ключевых данных, проставляется автоматически в момент создания.

Для просмотра сведений о парно-выборочном ключе ККС ВРК и для повторной генерации ключа следует выделить строку и нажать клавишу <Enter> или кнопку «Правка».

Для удаления парно-выборочного ключа ККС ВРК следует выделить строку ККС ВРК в списке и нажать клавишу <Del> или кнопку «Удалить».

Переход в таблице по строкам осуществляется клавишами <↑> и <↓>.

Для сохранения списка нажмите кнопку «Применить». Сохранение изменений с выходом в главное меню осуществляется по нажатии клавиши <F2>.

Выход с отменой внесенных изменений осуществляется по нажатию клавиши <Esc>, кнопка «Восстановить» отменяет внесенные за последний сеанс администрирования изменения без выхода из окна «Список ККС ВРК».

12. Выдача ключа ПДСЧ для ФПСУ-TLS

ЦВК можно применять для генерации и выдачи ключа ПДСЧ для программных и программно-аппаратных комплексов ФПСУ-TLS.

Сгенерированный ЦВК ключ ПДСЧ может быть использован на комплексе ФПСУ-TLS для инициализации ПДСЧ. Для программных комплексов ФПСУ-TLS, функционирующим под управлением виртуальных машин, использование выданного ЦВК ключа ПДСЧ при инициализации ПДСЧ обязательно.

Для выдачи ключа ПДСЧ для ФПСУ-TLS следует:

1. Выбрать класс центра ЦВК в соответствии с классом СКЗИ ФПСУ-TLS, для которого предназначается ключ ПДСЧ (см. пункт «Выбор центра и типа ключей»). Для программных комплексов ФПСУ-TLS, функционирующим под управлением виртуальных машин, разрешено использовать центр любого класса при генерации ключа ПДСЧ: КС1, КС2 или КС3;

2. Создать в выбранном центре новую серию ключевых данных (см. пункт «Генерация новой серии ключевых данных»). Каждый ФПСУ-TLS считается отдельным абонентом, так что при указании размера серии следует учитывать количество ФПСУ-TLS, которым требуется выдать ключ ПДСЧ;

3. Выдать из окна управления созданной серией ключевых данных ключи ПДСЧ для ФПСУ-TLS в файл на внешний носитель (см. пункты «Выдача ключа ПДСЧ» и «Массовая выдача ключей ПДСЧ»).

Внешний носитель с файлами ключей ПДСЧ должен быть доверенным образом передан администратору ФПСУ-TLS.

13. Переустановка ЦВК

ЦВК поставляется с предустановленным программным обеспечением. Переустановка программного обеспечения ЦВК может потребоваться в случаях неуспешной проверки целостности контролируемых файлов, замене внутреннего накопителя ЦВК, утере ТМ-идентификатора Главного администратора и/или пароля Главного администратора. Операция доступна администратору класса «Главный Администратор».

При переустановке все хранящиеся на внутреннем накопителе ЦВК данные, в том числе ключи, будут стерты. Рекомендуется перед переустановкой сделать экспорт данных ЦВК (см. пункт «Экспорт центра ЦВК»).

Для переустановки необходимы USB-носитель с дистрибутивом ЦВК, ТМ-идентификатор Главного Администратора, запасной ТМ-идентификатор, USB-flash с лицензиями криптосетей центров ЦВК.

Переустановка ЦВК заключается в подключении загрузочного USB-носителя к аппаратной платформе, выборе варианта загрузки с USB-носителя при старте ЦВК, и дальнейшего следования указаниям мастера установки. В процессе установки система будет несколько раз перезагружена.

Для переустановки программного обеспечения ЦВК:

Выключите питание аппаратной платформы ЦВК. Подключите загрузочный USB-носитель к аппаратной платформе ЦВК.

Включите питание аппаратной платформы, на которую ставится ПО ЦВК.

Рисунок 133 - Окно автостарта

При загрузке ЦВК после стартовых тестов в окне оповещения необходимо в течение первых секунд нажимать стрелку вниз на клавиатуре, чтобы отобразилось стартовое окно загрузчика:

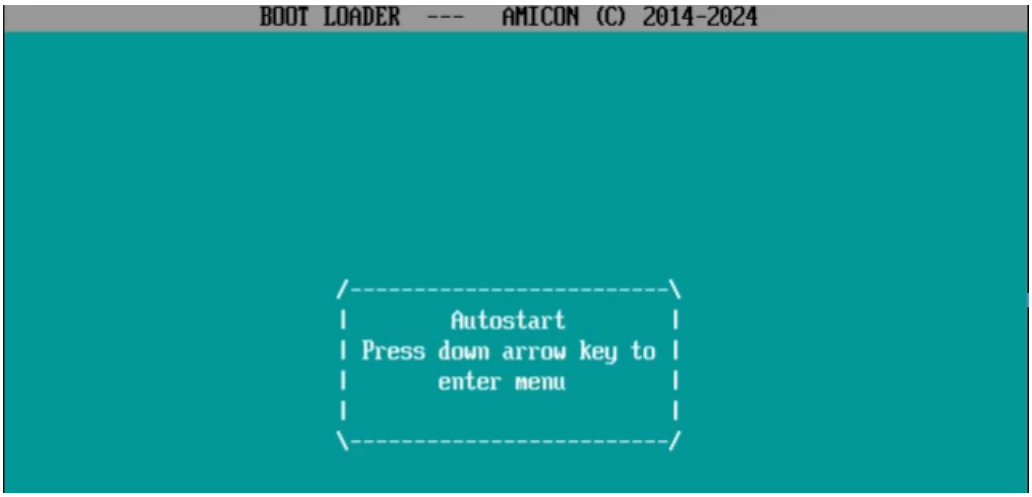

Рисунок 134 - Окно автостарта

Откроется меню установки, в котором можно проверить найденный на USB-носителе серийный номер ЦВК. Серийный номер ЦВК в формате «XXX00000XX» можно посмотреть на аппаратной платформе ЦВК. Если серийный номер совпадает с ожидаемым, выполните команду «Install FPSU»:

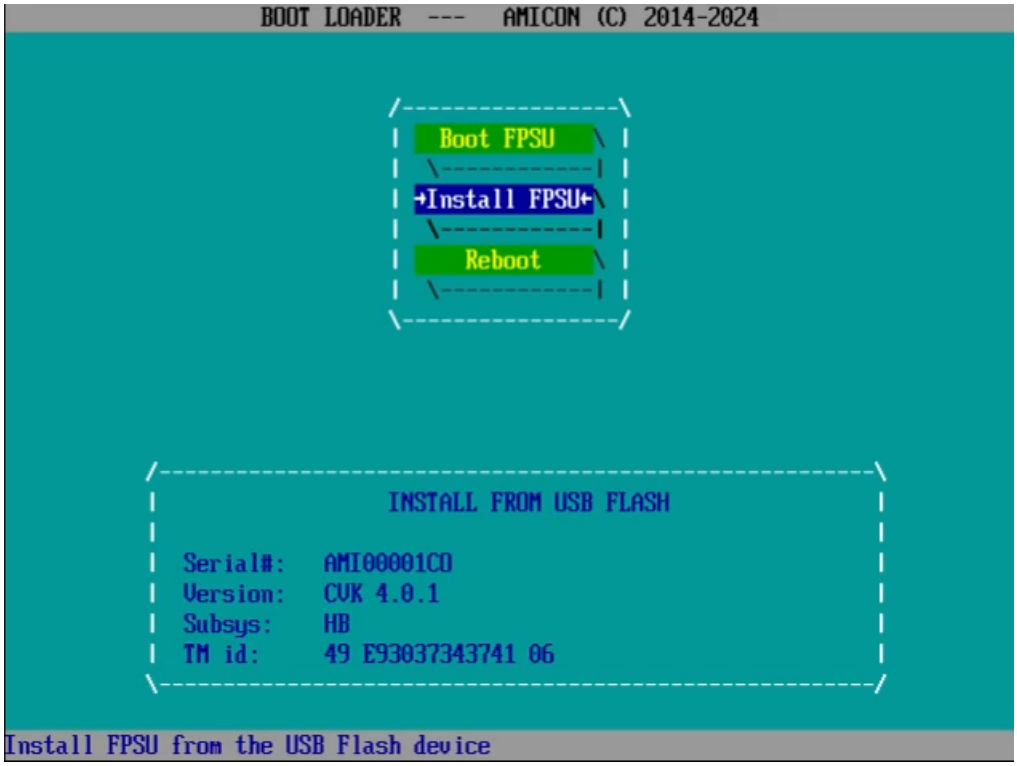

Рисунок 135 - Окно загрузчика ЦВК

Необходимо предъявить ТМ-идентификатор Главного Администратора (посредством подключения ТМ-идентификатора к USB-порту ЦВК) для продолжения переустановки.

Рисунок 136 - Необходимо подключить к ЦВК устройство TM-Key или USB TM-считыватель

В случае, если ЦВК переустанавливается по причине нарушения целостности контролируемых файлов, на экран будет выдано сообщение о ранее установленном ПО ЦВК. Выберите действие.

Рисунок 137 - Ожидание ответа пользователя

Подтвердите переустановку комплекса.

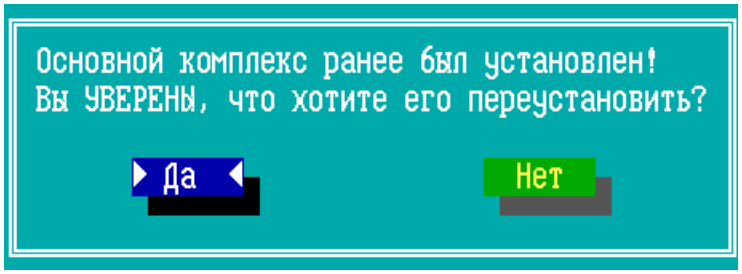

Рисунок 138 - Подтверждение ответа пользователя

При переустановке система отформатирует внутренний накопитель, сформирует логические разделы и выдаст сообщение.

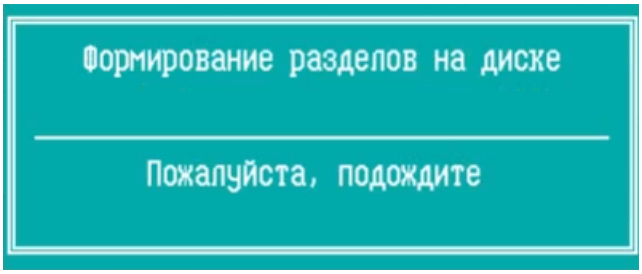

Рисунок 139 - Формирование разделов

При успешном завершении переустановки выдается сообщение, содержащее в том числе информацию о серийном номере ЦВК, и следующем шаге: перезагрузке ЦВК.

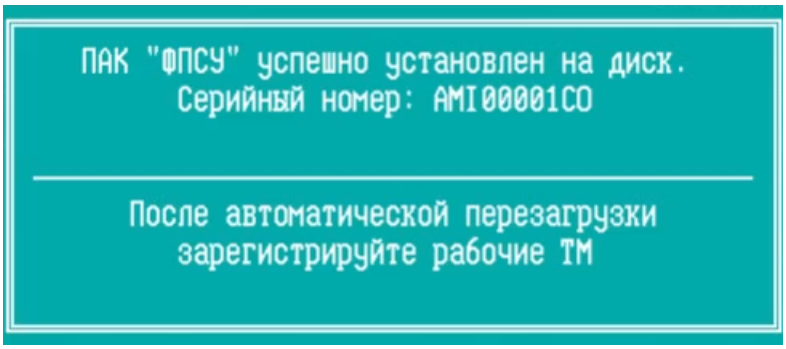

Рисунок 140 - Серийный номер

После перезагрузки ЦВК отобразится окно загрузчика. После выполнения начальной подготовки, система перейдет к обязательной процедуре инициализации ПДСЧ и перерегистрации ТМ-идентификаторов администраторов ЦВК.

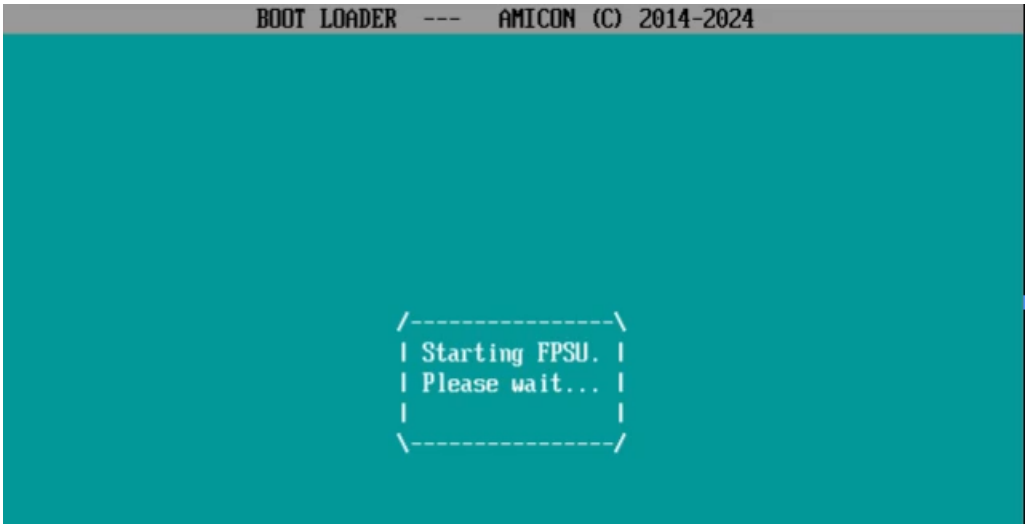

Рисунок 141 - Перезагрузка

Для инициализации ПДСЧ будет запущен интерфейс биологического датчика случайных чисел. От администратора требуется двигать мышью в пределах экрана до появления сообщения что процедура инициализации ПДСЧ завершена успешно:

Рисунок 142 - Инициализация ПДСЧ

После инициализации ПДСЧ отобразится окно с таблицей зарегистрированных ТМ-идентификаторов. Требуется перерегистрировать ТМ-идентификатор Главного Администратора, для продолжения нажмите кнопку «Понятно».

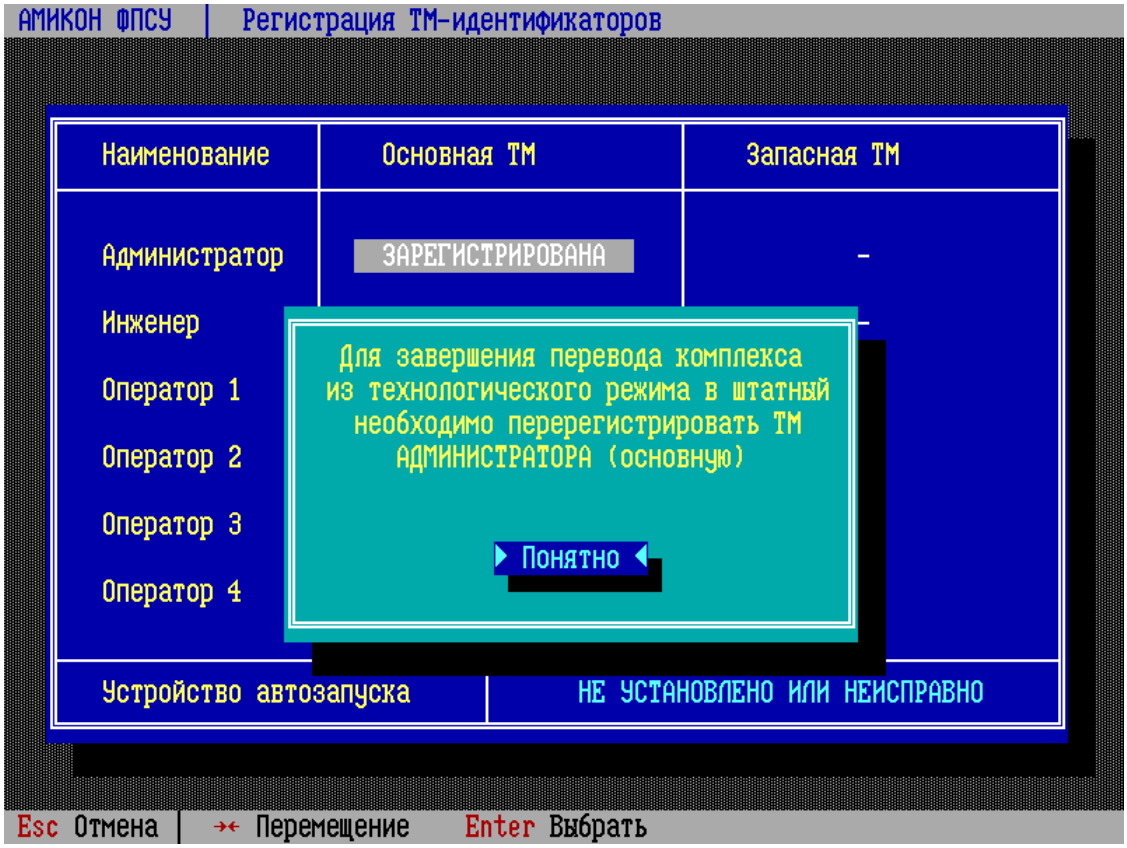

Рисунок 143 - Переход в штатный режим

Предъявите ТМ-идентификатор Главного администратора, на который будет записана новая ключевая информация:

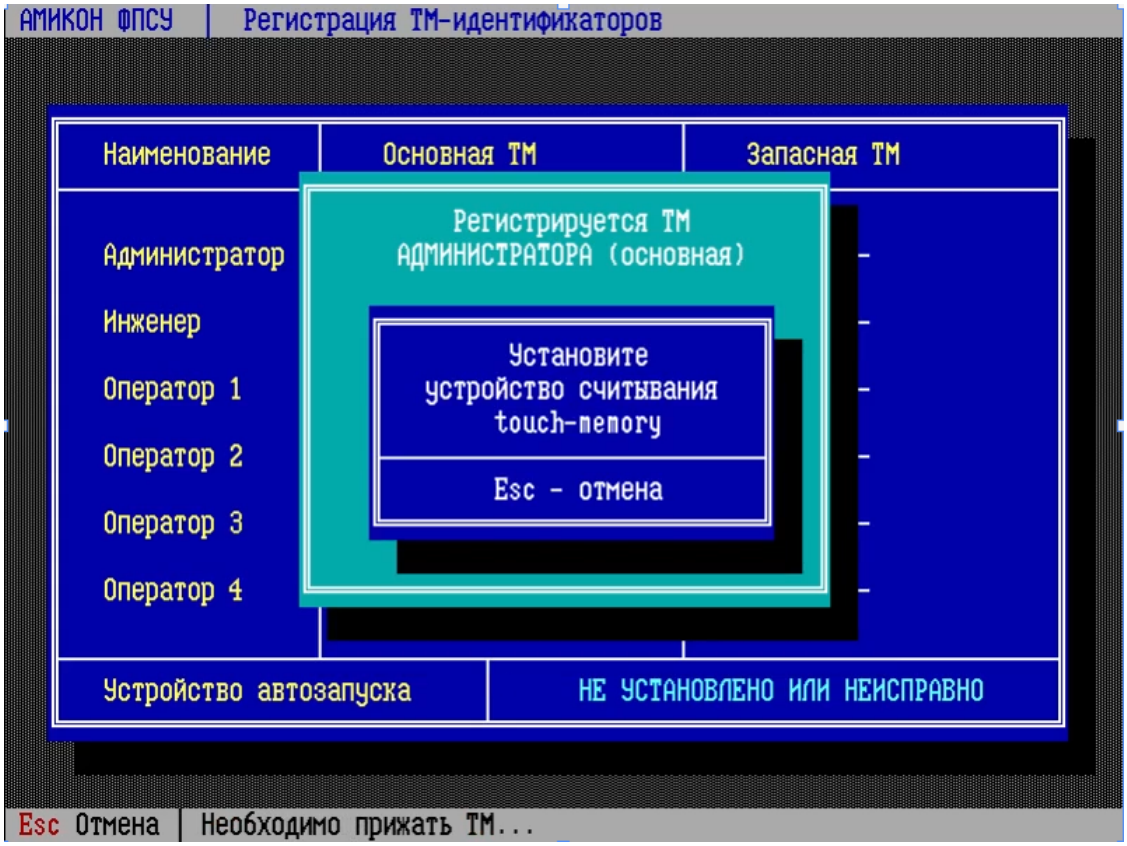

Рисунок 144 - Предъявление ТМ Главного администратора для перерегистрации

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

ВНИМАНИЕ! Установка пароля для каждого ТМ-идентификатора обязательна для ЦВК классов КС2 и КС3, и опциональна для ЦВК класса КС1.

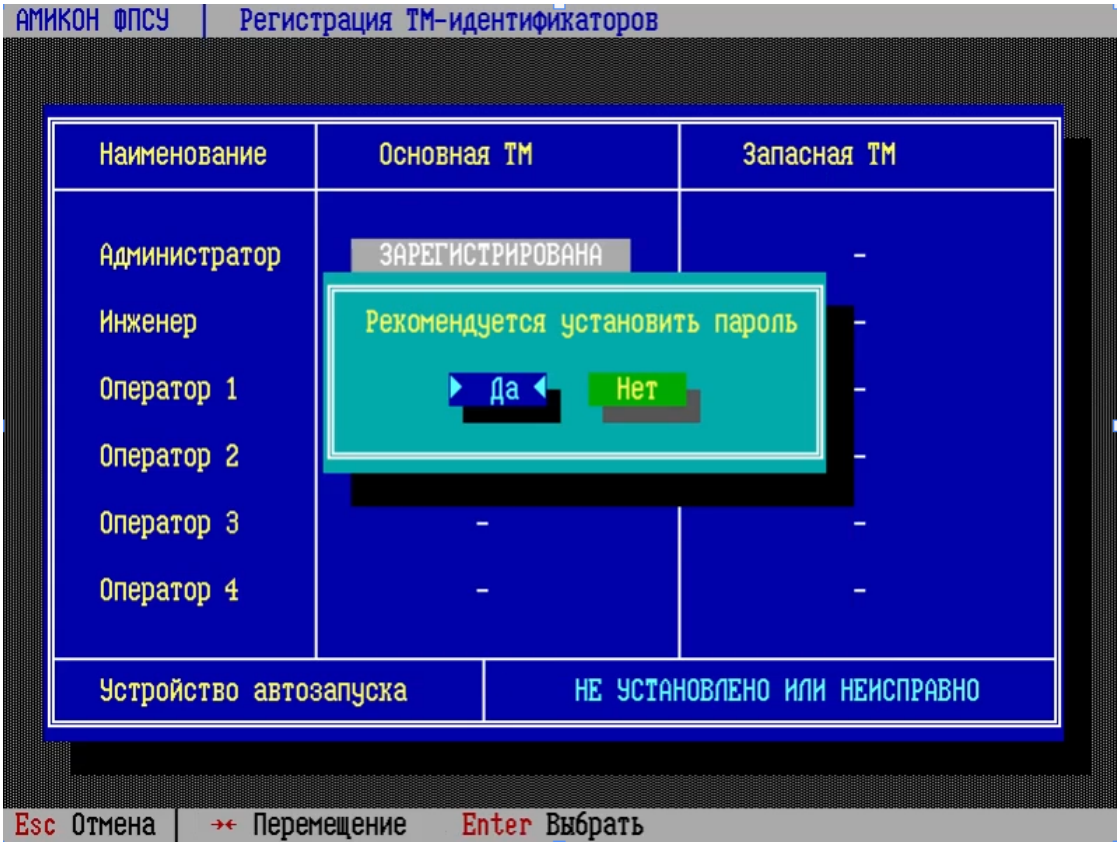

Рисунок 145 - ТМ перерегистрирован

При подтверждении запроса откроется окно ввода пароля.

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

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

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

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

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ЦВК потребуется повторная установка ЦВК с дистрибутива.

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

Рисунок 146 - Ввод пароля ТМ

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

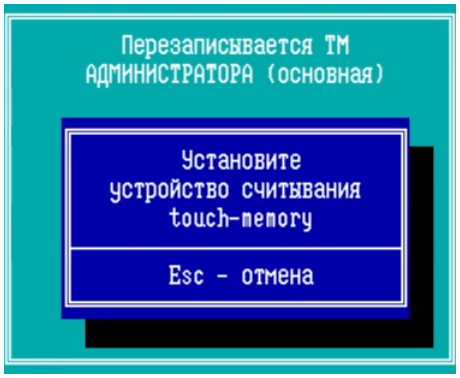

Рисунок 147 - Предъявление ТМ Главного администратора для установления пароля

ТМ-идентификатор Главного администратора перерегистрирован с установлением пароля. Комплекс переведен в штатный режим. ЦВК будет перезагружен.

ВНИМАНИЕ! На ЦВК должны быть зарегистрированы минимум два ТМ-идентификатора, один из которых ТМ Главного администратора.

Обязательным условием для продолжения работы является регистрация второго ТМ-идентификатора, запасного ТМ администратора или ТМ-идентификатора любого другого класса, иначе при закрытии регистратора ТМ-идентификаторов он будет открываться снова, блокируя дальнейшую работу.

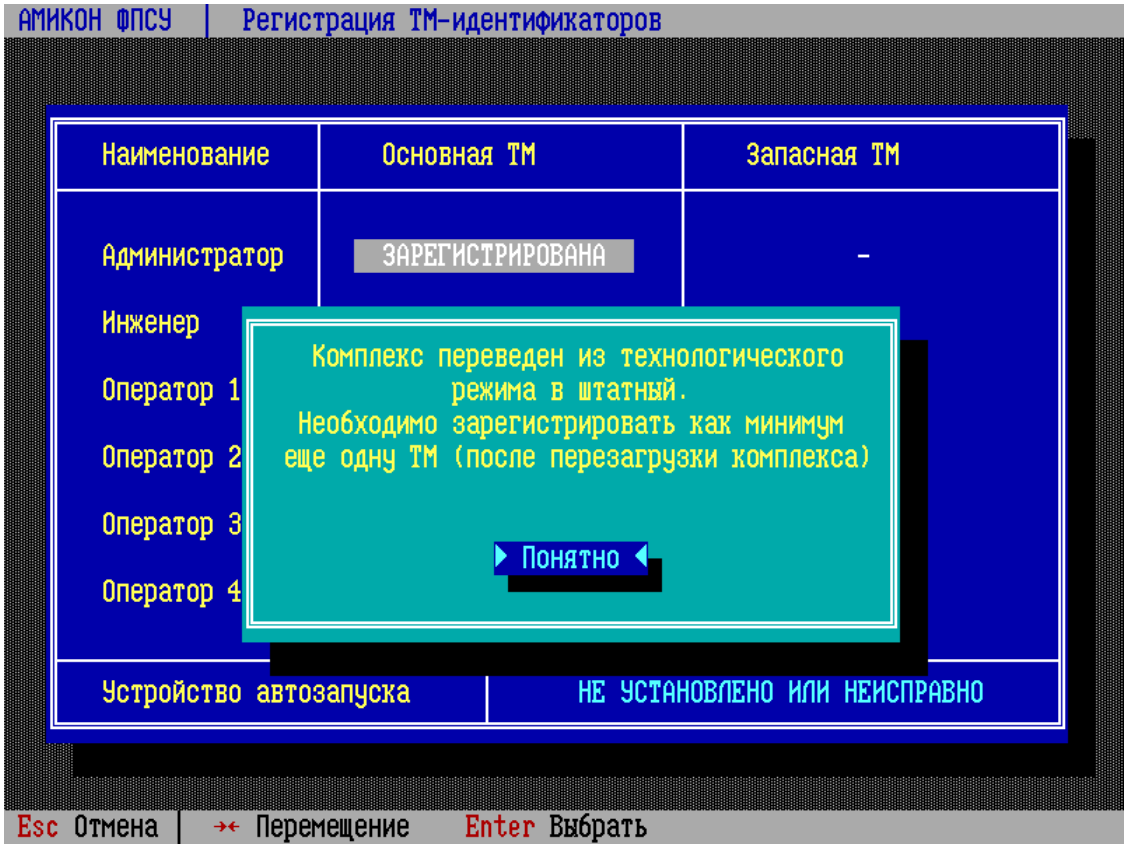

Рисунок 148 - ЦВК переведен в штатный режим работы

После перезагрузки ЦВК потребуется авторизация для запуска, необходимо подтвердить полномочия пользователя класса «Оператор» или выше. При переустановке ЦВК все зарегистрированные ранее ТМ требуется перерегистрировать, поэтому авторизация для запуска выполняется с помощью вновь зарегистрированного ТМ-идентификатора Главного администратора.

Рисунок 149 - Авторизация на запуск ЦВК

После перезагрузки отобразится таблица с уже зарегистрированным ТМ-идентификатором Главного администратора.

Далее потребуется регистрация ещё одного ТМ-идентификатора, например, запасного ТМ-идентификатора администратора.

При регистрации второго ТМ-идентификатора требуется ТМ администратора для подтверждения права регистрации и другой ТМ для регистрации выбранного класса пользователя ЦВК.

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

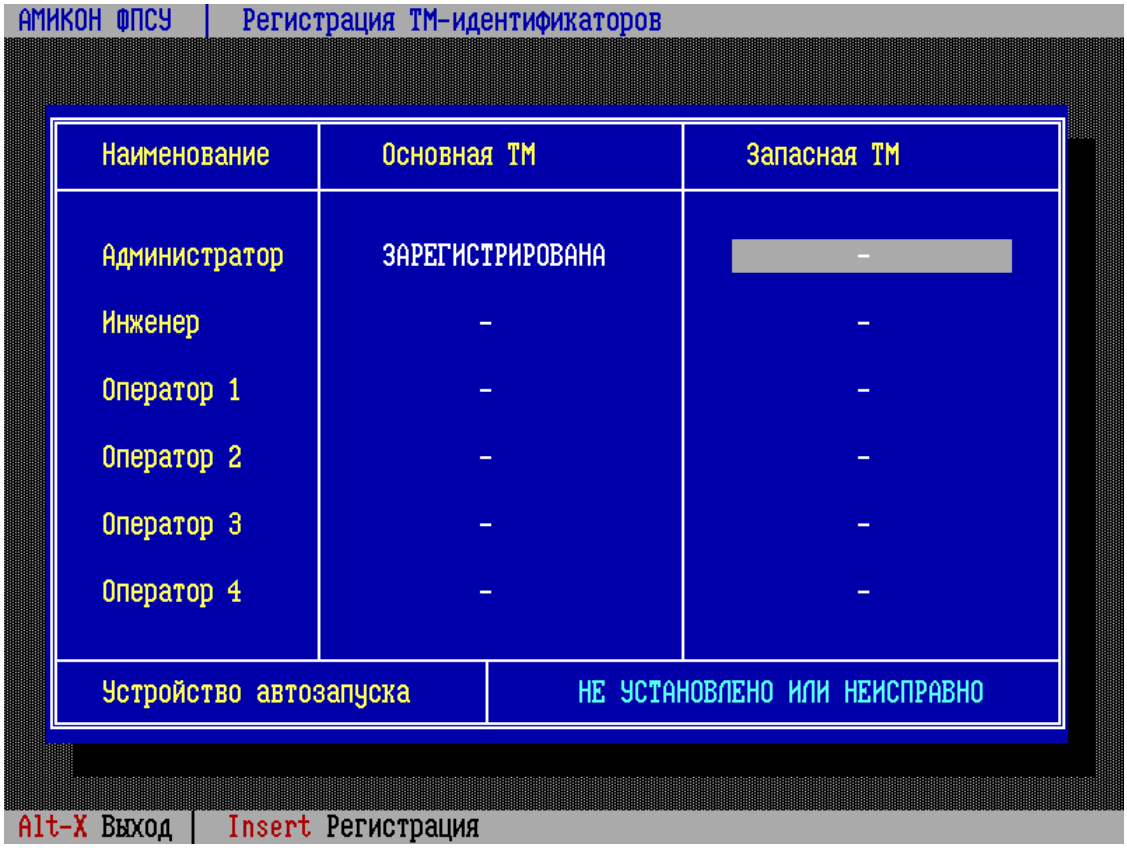

Рисунок 150 - Таблица зарегистрированных ТМ-идентификаторов

Выберите в таблице ячейку «Администратор-Запасная ТМ» и нажмите клавишу <Insert>. Отобразится запрос на регистрацию запасного ТМ-идентификатора администратора.

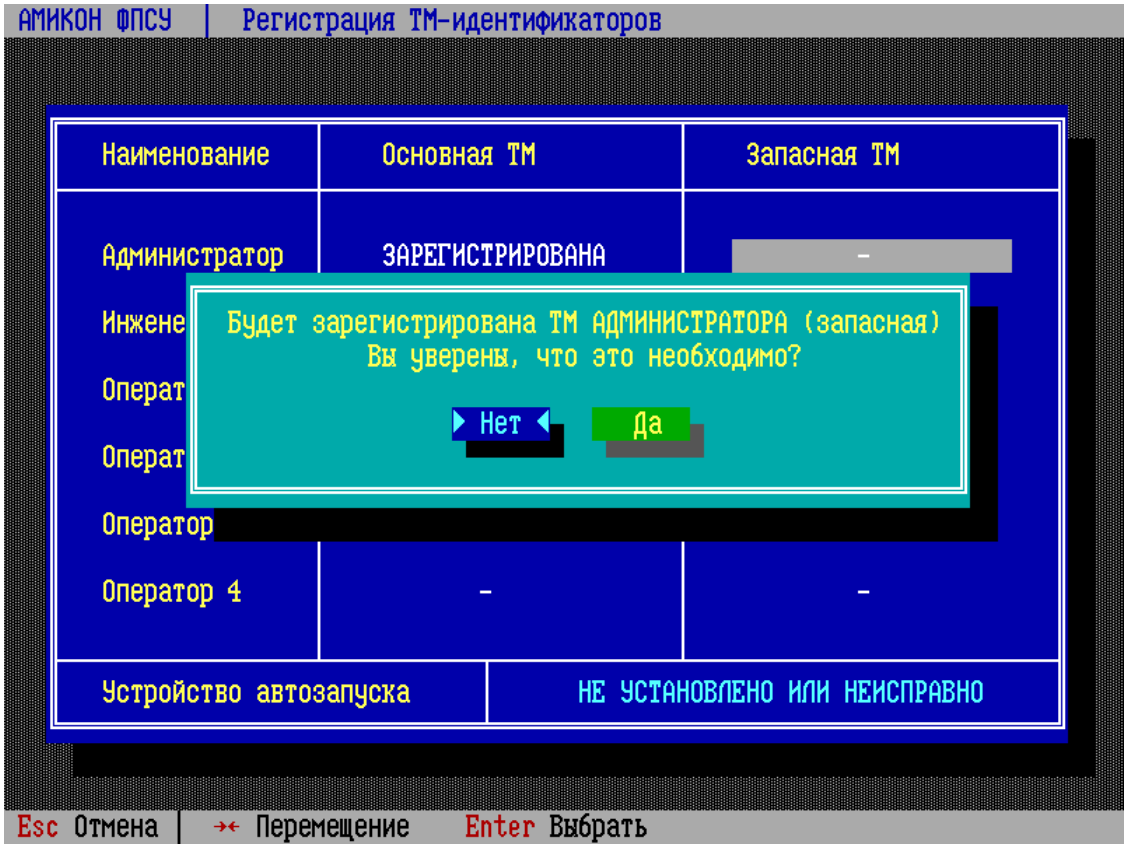

Рисунок 151 - Регистрация запасного ТМ

При подтверждении запроса по нажатию кнопки «Да» ТМ будет зарегистрирован заново, потребуется подтверждение полномочий администратора посредством подключения ТМ-идентификатора Главного администратора к USB-порту ЦВК.

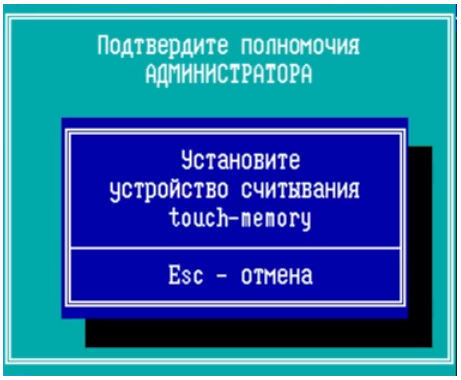

Рисунок 152 - Подтверждение полномочий администратора

Также запрашивается пароль подключенного ТМ-идентификатора

Главного администратора для авторизации в системе, в случае если пароль установлен.

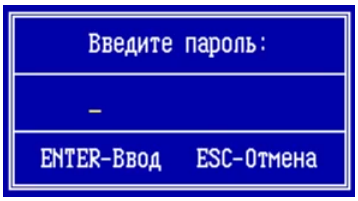

Рисунок 153 - Ввод пароля ТМ Главного администратора

Далее необходимо убрать ТМ-идентификатор Главного администратора, в случае если ТМ остается подключен, на экран будет выдано сообщение:

Рисунок 154 - ТМ-идентификатор считан

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

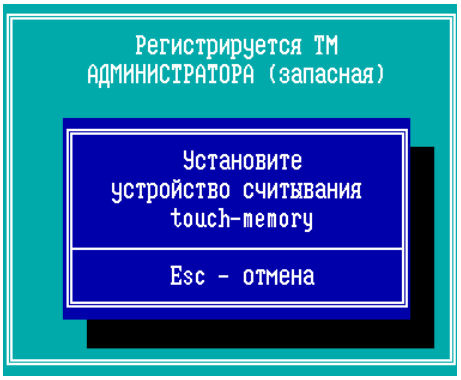

Рисунок 155 - Регистрация запасной ТМ

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

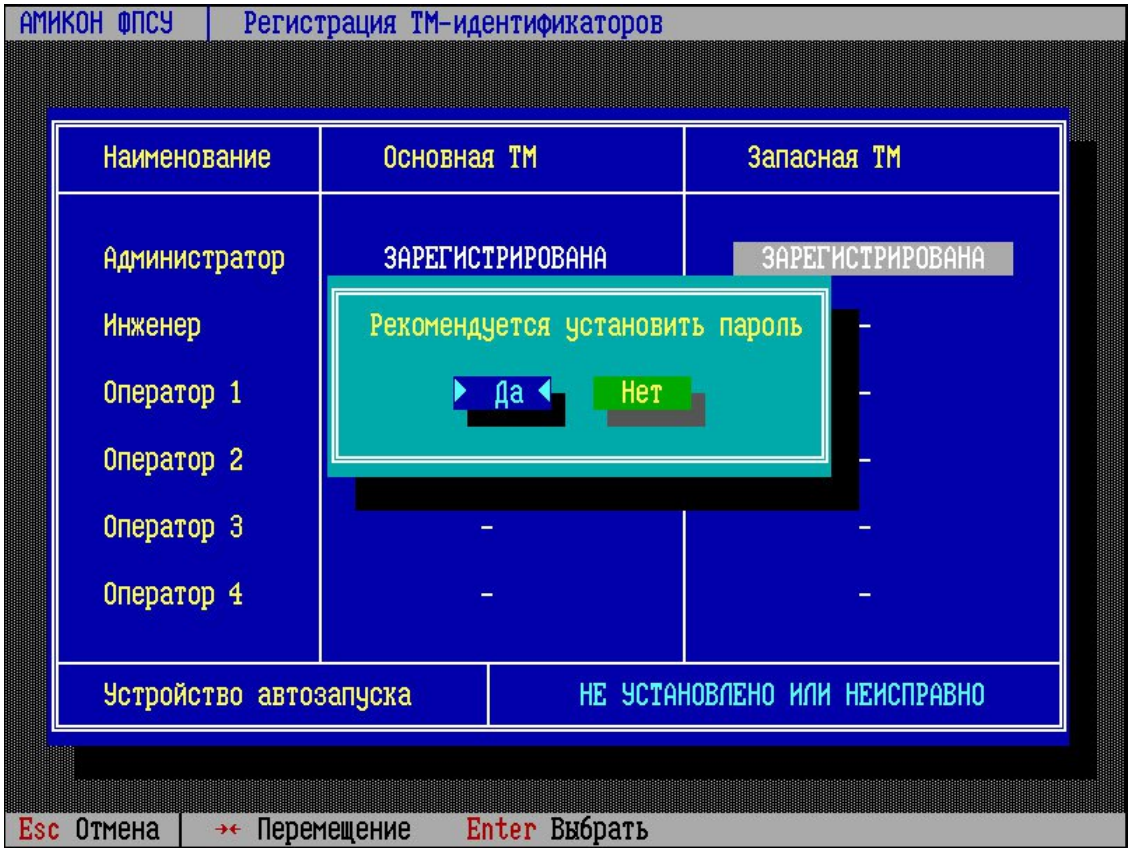

Рисунок 156 - Запасной ТМ зарегистрирован

При подтверждении запроса откроется окно ввода пароля. Все требования к паролю изложены выше (см. установка пароля ТМ Главного администратора).

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

Рисунок 157 - Ввод пароля ТМ

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

Рисунок 158 - Предъявление запасного ТМ

Запасной ТМ-идентификатор администратора зарегистрирован с установлением пароля.

После того, как запасной ТМ-идентификатор администратора зарегистрирован, отключите USB-носитель с дистрибутивом.

Для восстановления ключевых данных, подключите USB-flash с лицензиями криптосетей (центров) ЦВК и используйте команду «Импортировать» (см. пункт «Импорт и экспорт серий ключевых данных»).

Рекомендуется настройки автозапуска оставить по умолчанию.

При возврате в главное меню будет выдано предупреждение об отсутствии установленных центров. Не рекомендуется устанавливать тестовый центр. Криптографические ключи тестового центра нельзя использовать в рабочем режиме на ФПСУ. Нажмите кнопку «Нет».

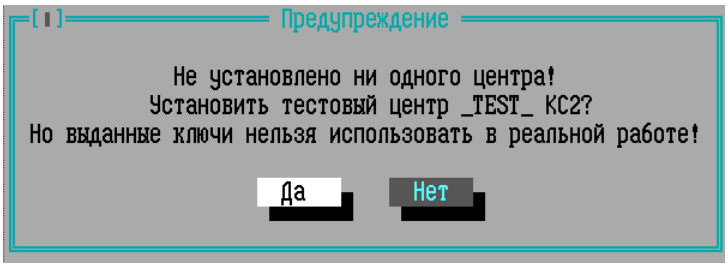

Рисунок 159 - Предупреждение

После отказа от установки тестового центра на экран будет выдано главное меню ЦВК. Процесс переустановки завершен. Дальнейшая работа с ЦВК происходит в штатном режиме, работа с ключевыми данными описана в пункте «Генерация и выдача ключевых данных».