ООО "АМИКОН"

УТВЕРЖДЕН

ПЕРС.26.20.40.140.006РП-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

"Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP" Магма

Центр выработки ключей

Руководство по применению

ПЕРС.26.20.40.140.006РП

Листов 59

2023

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программно-аппаратных комплексов шифрования "ФПСУ-IP". В документе содержатся общие сведения об изделии "Центр выработки ключей", приведен перечень необходимых организационно-технических мер и 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 подробные консультации по телефону или электронной почте.

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

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

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

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

Электронная почта: info@amicon.ru

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

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

Содержание

1. Список сокращений и определений

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

ПДСЧ — программно-клавиатурный датчик случайных чисел;

ОС — операционная система;

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 устройство контактной памяти iButton DS-1993 – DS-1996 (Dallas Semiconductor) или микроэлектронное USB-устройство "TM-Key" ПЕРС.466226.004 (ООО "АМИКОН");

ЦВК — программно-аппаратный комплекс "Центр выработки ключей", являющийся СКЗИ "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма", модификация "Центр выработки ключей 1.3" изделия Центр выработки ключей;

ФПСУ-IP — программно-аппаратный комплекс "ФПСУ-IP" (Фильтр Пакетов Сетевого Уровня), являющийся СКЗИ "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма" изделием "Криптомаршрутизатор".

2. Общие сведения

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

Созданные ЦВК ключи выдаются на отчуждаемый носитель. Ключи с носителя устанавливаются на ФПСУ-IP локальными администраторами каждого ФПСУ-IP, или удаленными администраторами.

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

ЦВК является изделием Центр выработки ключей (модификацией "Центр выработки ключей 1.3") СКЗИ "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма", поставляется в соответствии с формуляром на СКЗИ "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма", и должен использоваться в соответствии с правилами пользования СКЗИ "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма".

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" имеет сертификат соответствия «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений составляющих государственную тайну» для классов КС1/КС2/КС3 и «Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведения, составляющих государственную тайну, и эксплуатируемых на территории Российской Федерации» по уровню КС.

3. Условия эксплуатации и гарантийные обязательства

3. 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.

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.

3. 2. Гарантийные обязательства

Гарантийный срок на ЦВК составляет 12 месяцев со дня поставки комплекса.

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.

4. Подключение к ЦВК

Локальное управление ЦВК осуществляется от рабочей станции под управлением ОС Windows с помощью консольного подключения через COM-порт. При этом должны выполняться требования к Терминалу, изложенные в документе "Правила пользования" изделия ИНФК.11485466.4012.024 "Средство криптографической защиты информации "Программно-аппаратный комплекс шифрования "ФПСУ-IP" модификация "ФПСУ-IP Магма".

В комплект поставки входит консольный кабель для RJ45 интерфейса (см. рисунок ниже).

Рисунок 1 - Консольный кабель для RJ45 интерфейса

Для консольного подключения к ЦВК, осуществляемого с Windows-станций, используется утилита PuTTY. Утилиту PuTTY версии 0.70 сборки ООО "АМИКОН" можно скачать с официального сайта ООО "АМИКОН". Кроме того, утилита может быть поставлена по запросу.

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

Скачайте с официального сайта Амикон https://amicon.ru/download.php драйвер для подключения консоли к ФПСУ-mini для Windows (см. рисунок ниже).

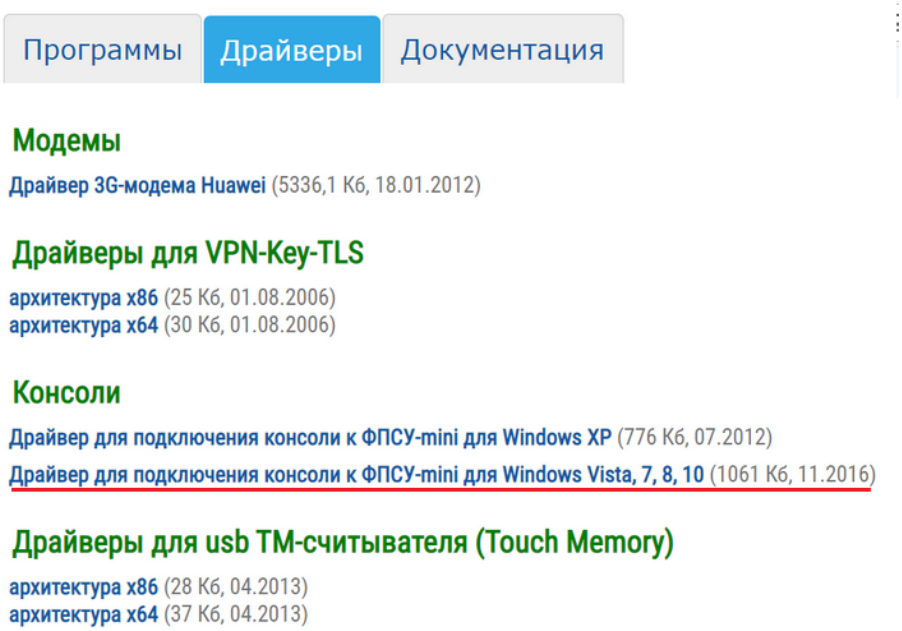

Рисунок 2 - Ссылка на скачивание

Установите драйвер кабеля в ОС рабочей станции и проверьте правильно ли кабель обнаруживается в диспетчере устройств. 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" (см. рисунок ниже).

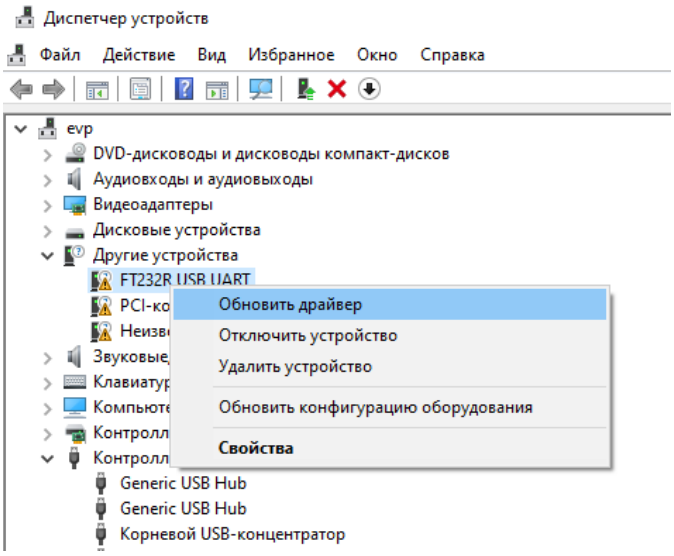

Рисунок 3 - Отображение консольного кабеля для RJ45 интерфейса при первом подключении в диспетчере устройств

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 PuTTY при настройке подключения.

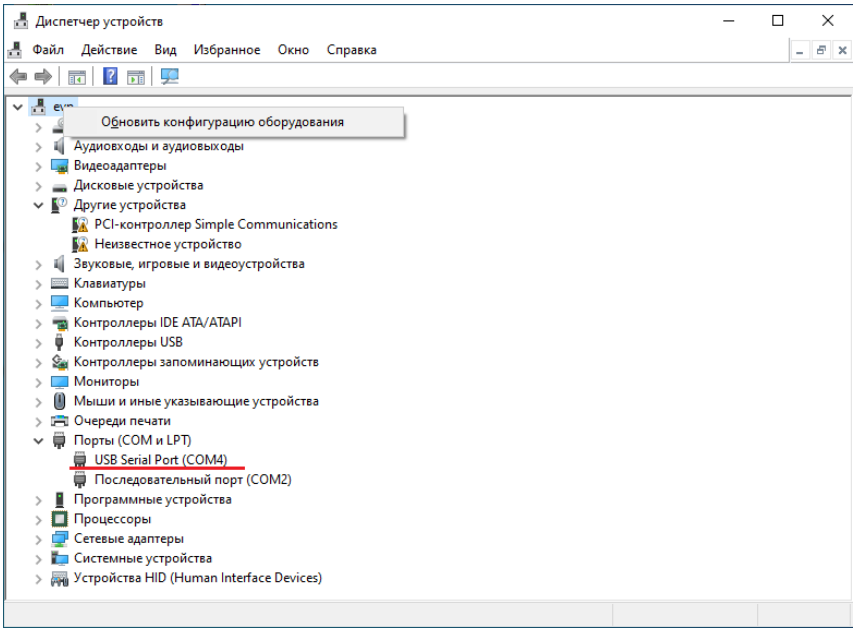

Рисунок 4 - COM порт консольного соединения в диспетчере устройств

Для запуска утилиты PuTTY скачайте с официального сайта Амикон https://amicon.ru/download.php ФПСУ-терминал для Windows (см. рисунок ниже).

Рисунок 5 - Ссылка для скачивания

Загрузите и распакуйте архив с файлами в отдельный каталог. Запустите файл PuTTY.exe и установите указанные ниже настройки (см. рисунки ниже в данном пункте).

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".

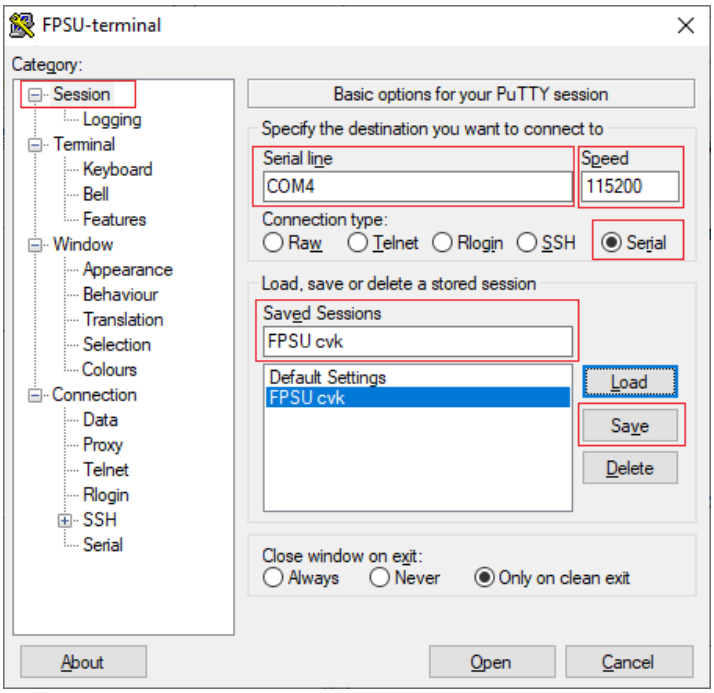

Рисунок 6 - Настройка подключения

Укажите тип используемой в терминале клавиатуры - Xterm R6 (выставляется в интерфейсе PuTTY: Terminal-Keyboard-The Function keys and keypad).

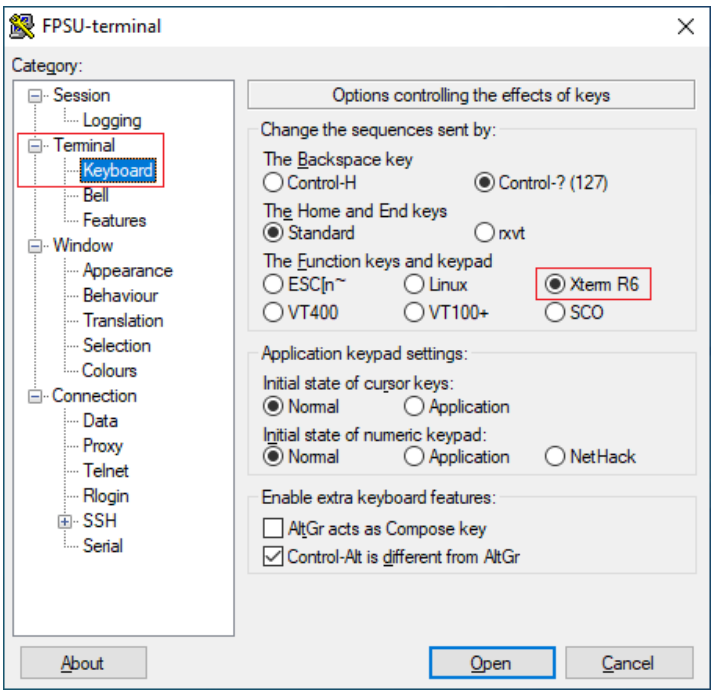

Рисунок 7 - Выбор типа клавиатуры

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

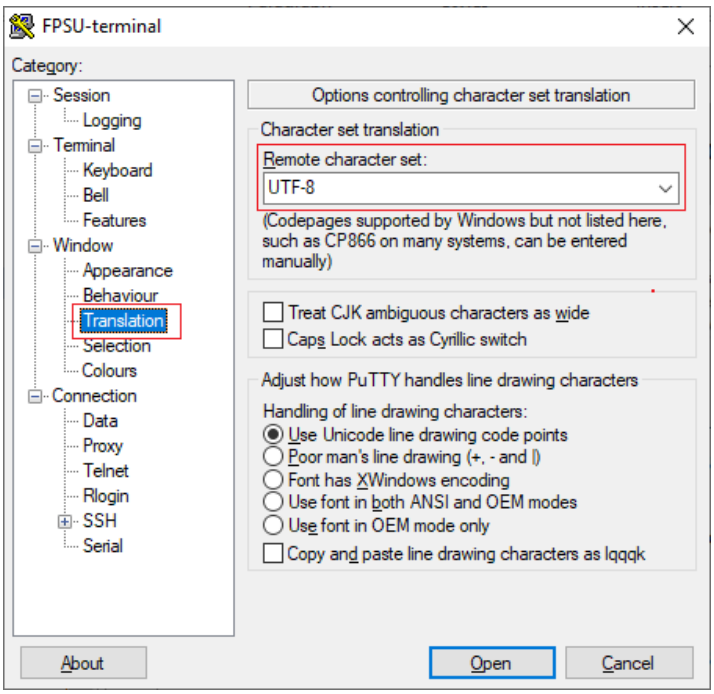

Рисунок 8 - Выбор кодировки

Задайте количество строк – 25 (выставляется в интерфейсе PuTTY: Window–Rows).

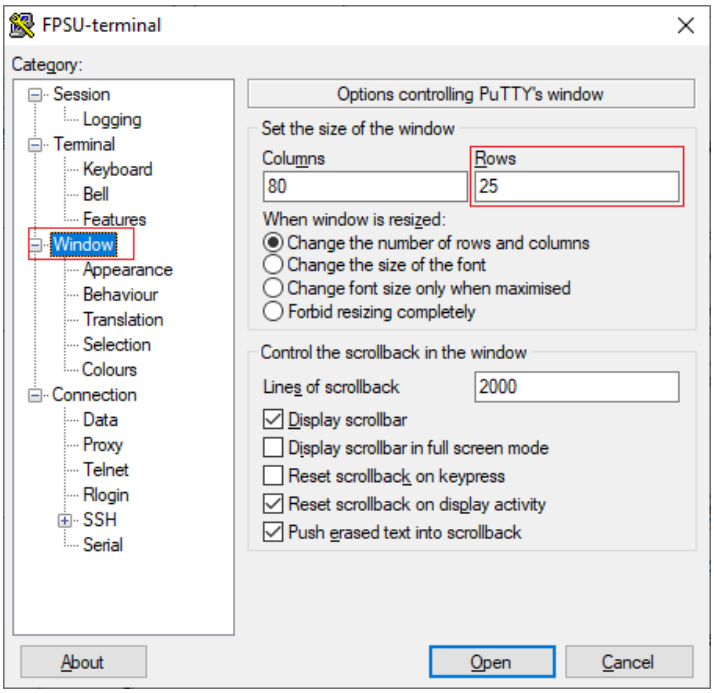

Рисунок 9 - Выбор количества строк

Запустите терминал, нажав "Open".

Подключите консольный кабель к ЦВК (см. рисунок ниже) и включите питание ЦВК.

Рисунок 10 - Консольный порт ЦВК

На экране отобразится главное меню ЦВК (см. рисунок ниже).

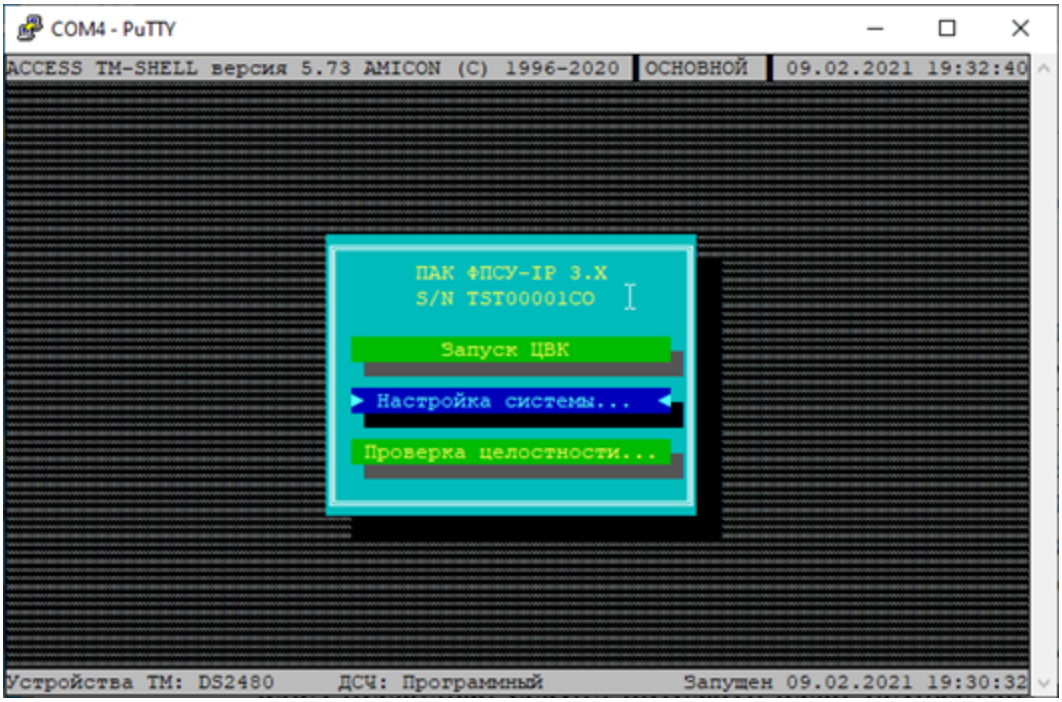

Рисунок 11 - Консольное подключение установлено

5. 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 ФПСУ, на консоль будет выдан запрос на подтверждение права доступа пользователя к работе с ЦВК (см. рисунок ниже). Для продолжения требуется подключить ТМ-идентификатор Главного Администратора к USB-порту ЦВК.

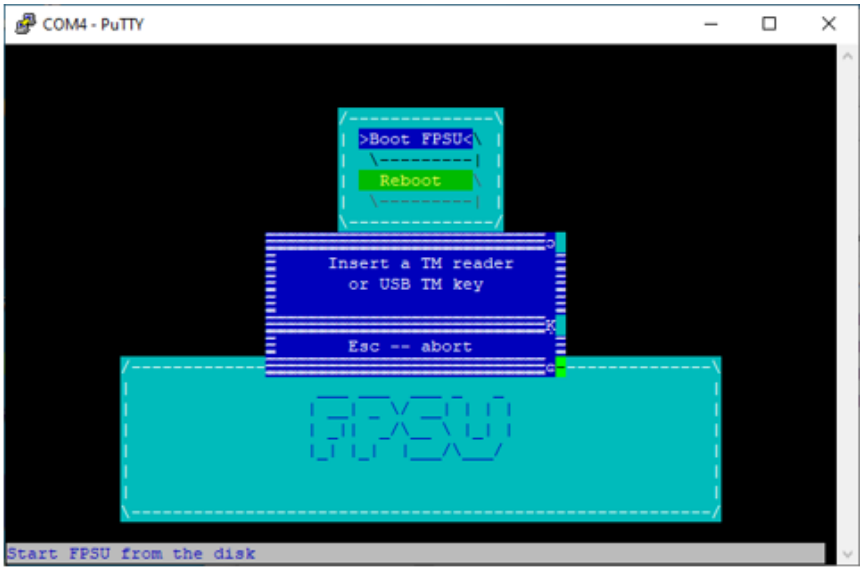

Рисунок 12 - Загрузка ЦВК

В случае успешной идентификации загрузка ОС продолжится. ПО ЦВК будет загружено, выдав на экран главное меню, содержащее следующие команды (см. рисунок ниже):

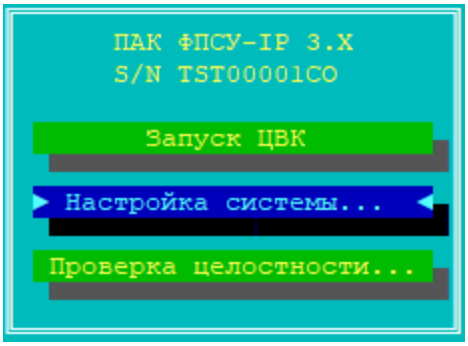

Рисунок 13 - Главное меню ЦВК

"Запуск ЦВК" – переход к интерфейсу генерации ключевых данных зарегистрированных на ЦВК криптосетей ФПСУ-IP, подробнее см. пункт Генерация и выдача ключевых данных.

"Настройка системы" – переход в окно настроек системы, подробнее см. пункты Регистрация ТМ, Установка дополнений, Переинициализация ПДСЧ.

"Проверка целостности" – переход в окно запуска проверок целостности программного обеспечения ЦВК, подробнее см. пункт Контроль целостности ПО.

Навигация по интерфейсу ЦВК осуществляется следующим образом:

- Переход по командам меню осуществляется клавишами 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.

Подменю главного меню "Настройка системы" (см. рисунок ниже) 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.

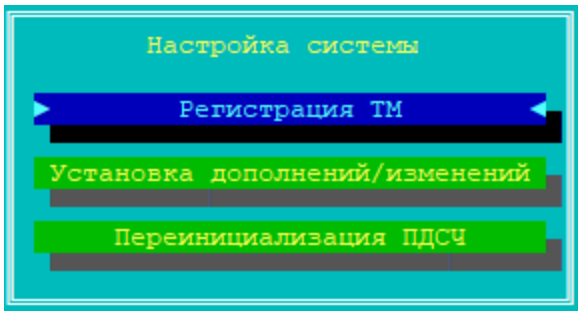

Рисунок 14 - Меню настройки системы ЦВК

5. 1. Регистрация ТМ

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

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

При выборе опции на экране появится таблица (см. рисунок ниже), показывающая наличие зарегистрированных ТМ-идентификаторов.

Для зарегистрированных ТМ-идентификаторов могут быть осуществлены следующие операции:

- ТМ-идентификатор Главного Администратора, может быть только проверен;
- остальные ТМ-идентификаторы – проверены, очищены или повторно зарегистрированы, с новой ключевой информацией.

Новый ТМ-идентификатор может быть только зарегистрирован как запасной для строки администратора 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.

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

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

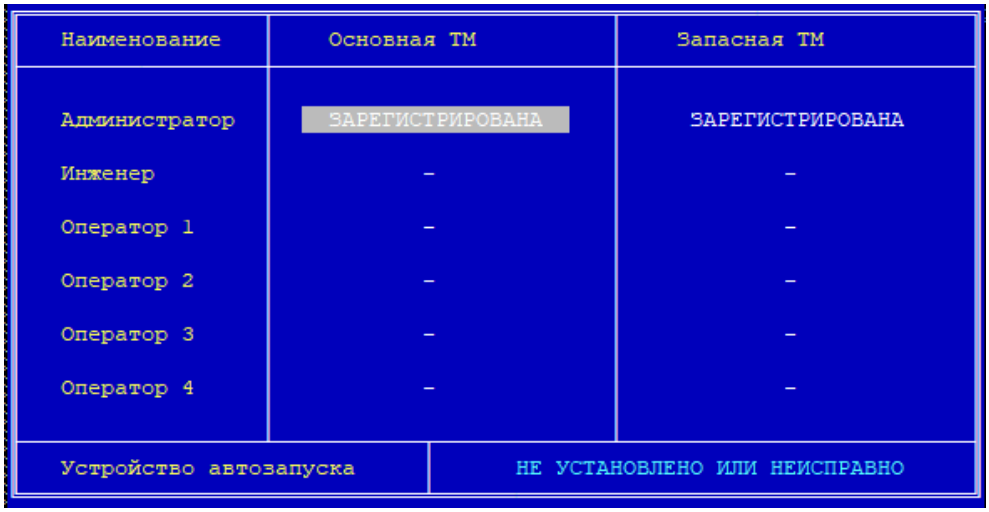

Рисунок 15 - Меню регистрации ТМ-идентификаторов администраторов ЦВК

5. 2. Установка дополнений

Опция "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 указанными в формуляре на СКЗИ контрольными суммами.

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 находится в корневом каталоге USB-носителя. Подключите USB-носитель и нажмите "Понятно" (см. рисунок ниже).

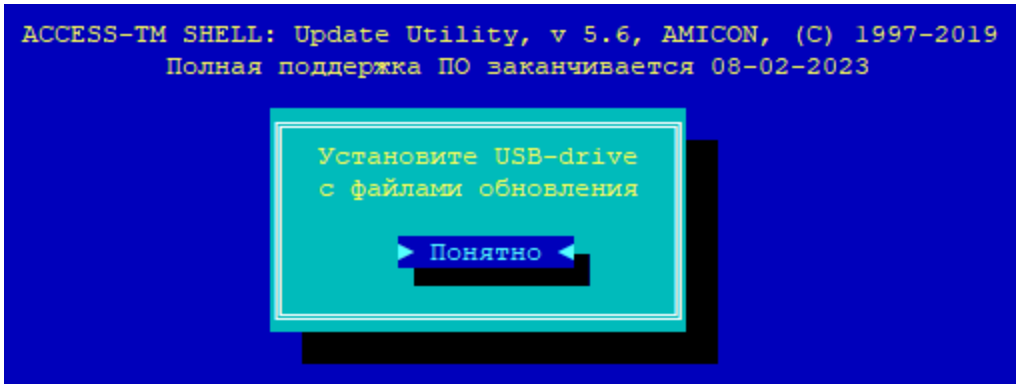

Рисунок 16 - Запрос на подключение USB-носителя

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" (см. рисунок ниже).

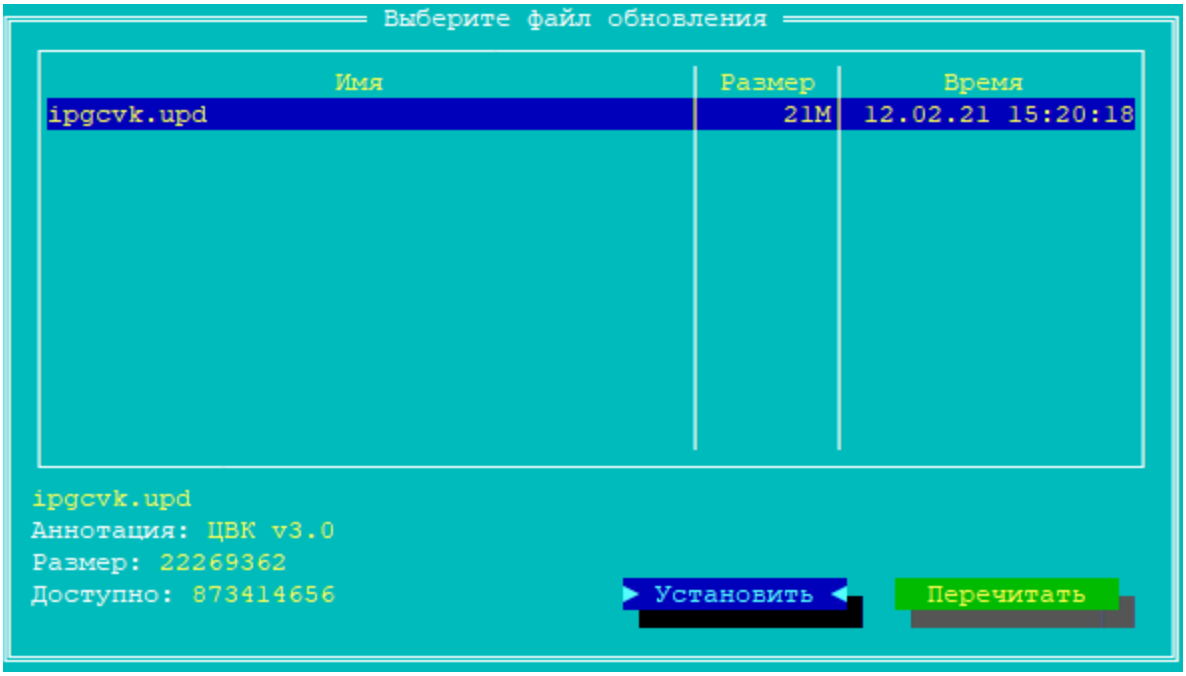

Рисунок 17 - Список файлов обновлений

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

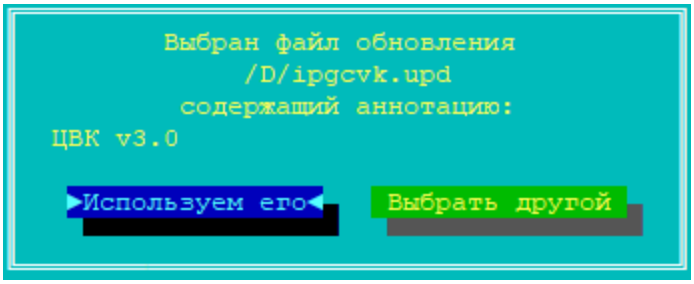

Рисунок 18 - Подтверждение обновления

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

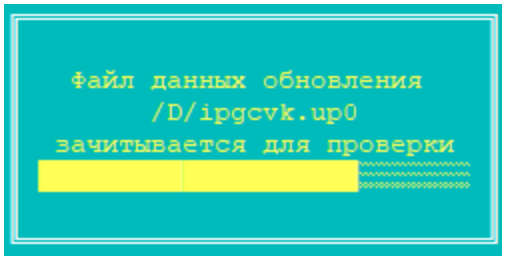

Рисунок 19 - Загрузка обновления

6. Файл обновления записывается на внутренний накопитель ЦВК (см. рисунок ниже).

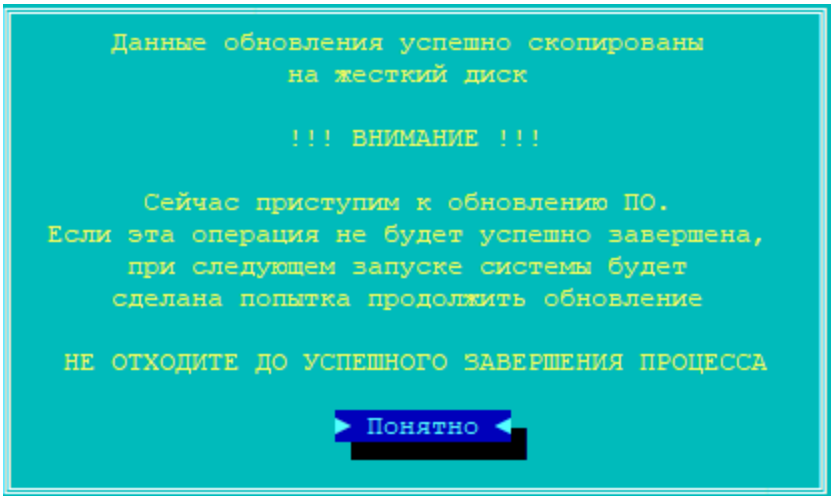

Рисунок 20 - Процесс обновления

7. После завершения установки обновлений ЦВК будет перезагружен и готов к дальнейшей эксплуатации (см. рисунок ниже).

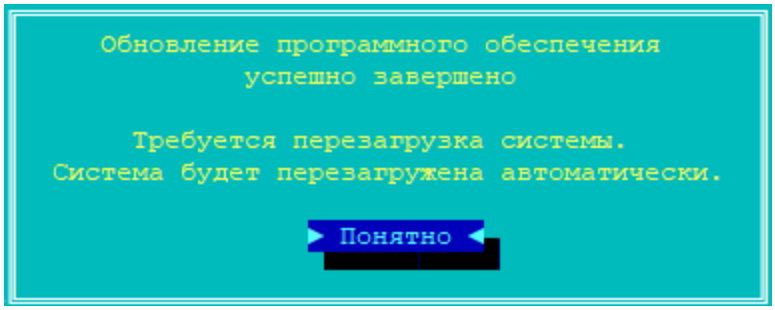

Рисунок 21 - Подтверждение успешного обновления

5. 3. Переинициализация ПДСЧ

Первоначальная инициализация программно-клавиатурного датчика случайных чисел (ПДСЧ) происходит при установке ЦВК.

Команда "Переинициализация ПДСЧ" подменю предназначена для повторной инициализации ПДСЧ ЦВК (см. рисунок ниже). Частота повторной инициализации программного датчика случайных чисел ЦВК 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".

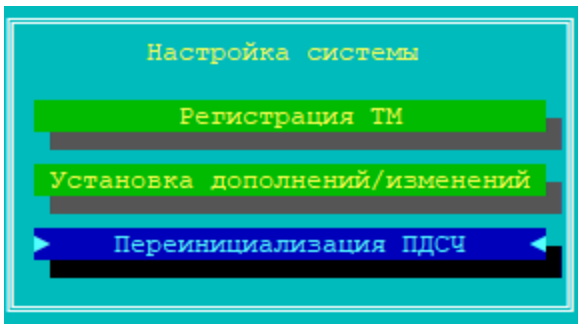

Рисунок 22 - Команда повторной инициализации ПДСЧ

При выборе команды "Переинициализация ПДСЧ" запустится интерфейс программно-клавиатурного датчика случайных чисел. От пользователя требуется ввести указываемые на экране цифры (см. рисунок ниже).

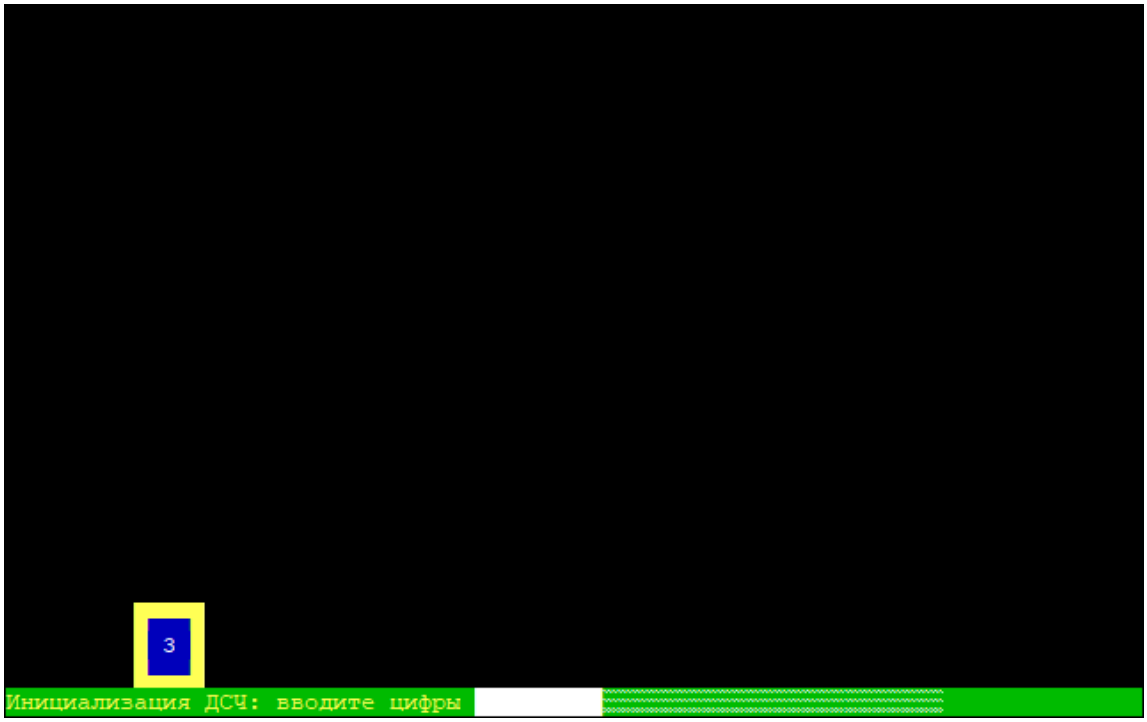

Рисунок 23 - Программно-клавиатурный датчик случайных чисел

Переинициализация ПДСЧ завершится успешно, как только будет осуществлён корректный ввод достаточного числа символов. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <Esc> обратно в главное меню "Настройки системы".

6. Контроль целостности ПО

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 "ФПСУ-IP".

Дополнительная проверка целостности ПО ЦВК осуществляется по команде "Проверка целостности" основного меню (см. рисунок ниже).

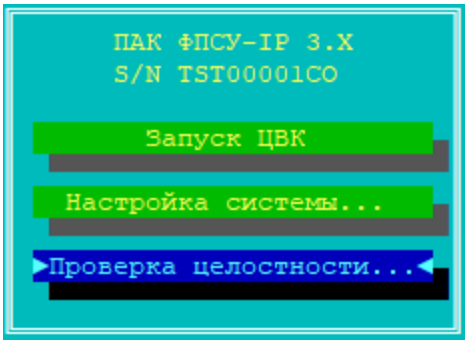

Рисунок 24 - Главное меню ЦВК

У локального администратора существует три варианта выполнения проверки (см. рисунок ниже):

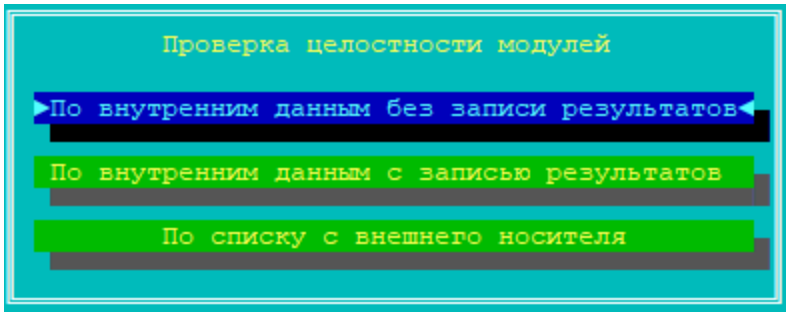

Рисунок 25 - Меню проверки целостности ПО

При выборе опции "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.

При выборе опции "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.

При выборе опции "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.

После активизации 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 PuTTy версии 0.70 сборки ООО "АМИКОН" рабочего места под управлением ОС Windows (далее - Терминалом), необходимо выполнять контроль целостности программного обеспечения Терминала.

Первоначальный контроль целостности после установки

Непосредственно после установки ПО Терминала на ПЭВМ следует выполнить первоначальный контроль целостности программных модулей Терминала.

Контроль целостности осуществляется при помощи входящей в состав СКЗИ "Программы контроля целостности файлов" WINFPSUHASH.EXE.

Для выполнения первоначального контроля целостности после установки следует рассчитать с помощью WINFPSUHASH.EXE контрольные суммы на программное обеспечение Терминала и сравнить полученные результаты с эталонными контрольными суммами из формуляра на СКЗИ (подробнее об использовании WINFPSUHASH.EXE см.

инструкцию по применению программы контроля целостности файлов).

При нарушении целостности программного модуля Терминала, необходимо повторно установить программу с инсталляционного носителя.

Контроль целостности в процессе эксплуатации

Для использования Терминала для управления ЦВК как СКЗИ класса КС2 или КС3, контроль целостности программы в процессе эксплуатации следует осуществлять средствами сертифицированного по Требованиям ФСБ АПМДЗ с действующим сертификатом соответствия.

В остальных случаях, контроль целостности Терминала в процессе эксплуатации следует осуществлять программой WINFPSUHASH.EXE.

Контролю целостности в процессе эксплуатации подлежат программные модули Терминала (putty_x86.exe и putty_amd64.exe) и исполняемые файлы ОС.

При нарушении целостности контролируемых программных модулей необходимо прекратить работу с Терминалом до восстановления целостности файлов.

7. Генерация и выдача ключевых данных

После загрузки ОС ЦВК, переход в интерфейс генерации ключевых данных осуществляется выполнением команды "Запуск ЦВК" главного меню (см. рисунок ниже).

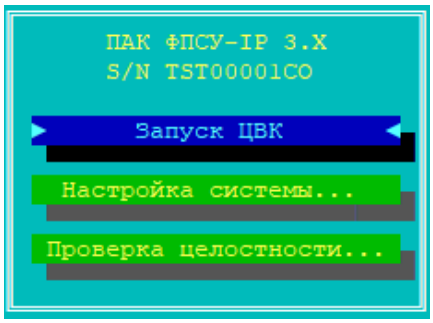

Рисунок 26 - Главное меню ЦВК

После выполнения команды "Запуск ЦВК" программа будет каждый раз предлагать скорректировать время, поскольку операционная среда функционирует изолированно от общей сети передачи данных и не имеет возможности синхронизировать время. Проверьте (см. рисунок ниже) текущее время на ЦВК, и, при необходимости, введите в поле "Новые" текущую дату и время. Выполните команду "Установить" для обновления даты и время, или нажмите клавишу <Esc> для продолжения без корректировки системного времени.

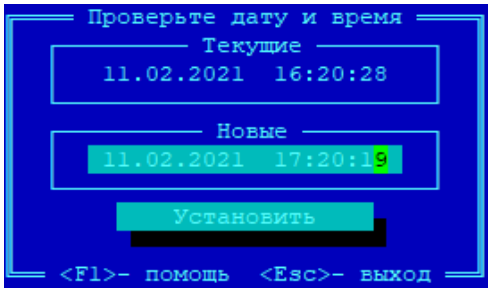

Рисунок 27 - Проверка даты и времени

Следующим этапом работы является выбор центра – криптосети ФПСУ-IP, для которой генерируются ключевые данные.

Примечание. Для ЦВК может быть зарегистрирован только один центр.

По умолчанию список центров пустой (см. рисунок ниже), 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.

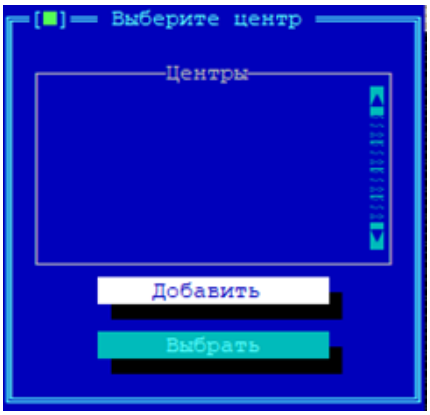

Рисунок 28 - Список центров пуст

7. 1. Регистрация центра в ЦВК

Для регистрации в ЦВК центра выполните команду "Добавить" окна списка центров (см. рисунок выше).

Система запустит процесс регистрации лицензии на центр в ЦВК, предложив подключить USB-носитель с файлом лицензии (см. рисунок ниже). Подключите USB-носитель и нажмите "ОК" для продолжения.

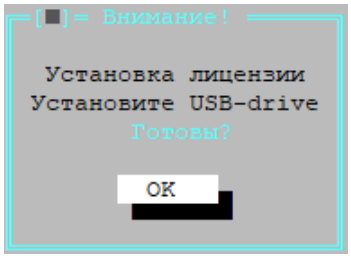

Рисунок 29 - Запрос на подключение USB-носителя с файлом лицензии

Будет произведен поиск в корневом каталоге подключенного к ЦВК USB-носителя, и на экран выдан список обнаруженных на носителе лицензий (см. рисунок ниже). 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.

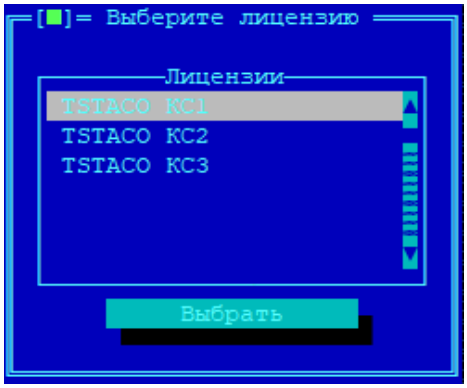

Рисунок 30 - Обнаруженные лицензии

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 (см. рисунок ниже).

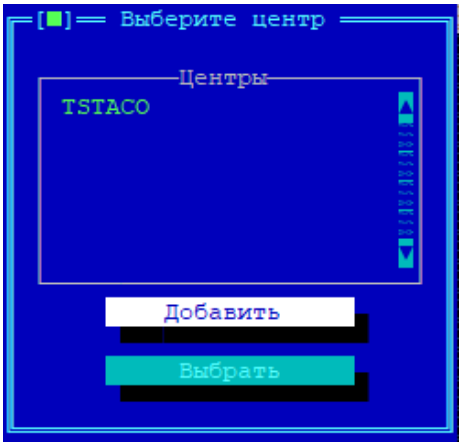

Рисунок 31 - Добавлен описатель центра

7. 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 (см. рисунок выше).

В появившемся окне будет приведен список типов ключевых данных, которыми центр может управлять (см. рисунок ниже):

Рисунок 32 - 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.

7. 3. Генерация новой серии ключевых данных

При выполнении команды на экране появится диалоговое окно "Выберите серию (КСХ)" (см. рисунок ниже), которое будет пустым при первом использовании центра, а при последующих будет отображать список ранее созданных серий.

Рисунок 33 - Пустой список серий ключевых данных

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

7. 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> (см. рисунок выше).

На экране отобразится окно "Новая серия" (см. рисунок ниже). Номер новой серии присваивается автоматически, как следующий за номером последней созданной серии. Если ключевые данные генерируются первый раз, серии будет присвоен номер 1.

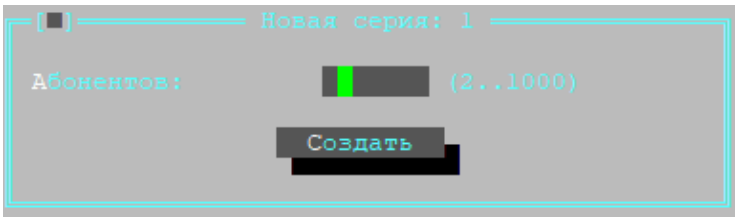

Рисунок 34 - Создание новой серии

В поле "Абонентов:" требуется указать максимальное количество абонентов (программно-аппаратных комплексов ФПСУ-IP), на которое рассчитана данная серия (от 2-х до 1000 для класса КС2). 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-IP, 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 окно выбора внешнего носителя, на который будет записан ключ хранения серии ключевых данных (см. рисунок ниже). Он потребуется к предъявлению каждый раз при дальнейшей работе с созданной серией, например, для выдачи парно-выборочных ключей ФПСУ-IP на внешний носитель.

Рисунок 35 - Выбор места хранения

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

Примечание. Рекомендуется выбирать местом хранения "Флеш-диск". Не рекомендуется использовать ТМ-идентификатор в качестве носителя ключей (см. рисунок ниже). При использовании в качестве носителя ключа ТМ-идентификатора администратора ЦВК, ключ администратора на ТМ-идентификаторе будет перезаписан! Это приведет к потере возможности администрировать ЦВК в дальнейшем!

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

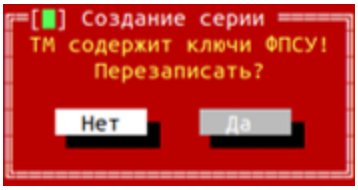

Рисунок 36 - Перезапись ключа

ВНИМАНИЕ! Для ЦВК модификации 1.3 ТМ-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 (см. рисунок ниже).

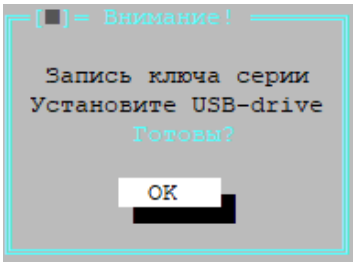

Рисунок 37 - Запись ключа хранения

В случае, если файл уже существует, он будет перезаписан (см. рисунок ниже).

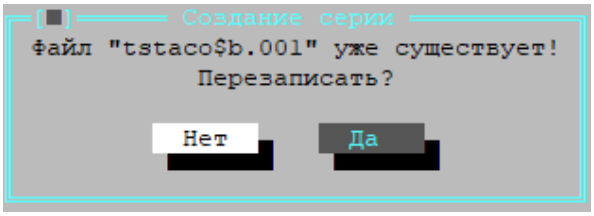

Рисунок 38 - Запись ключа хранения

По завершению будет выдано сообщение об успешном создании серии ключевых данных (см. рисунок ниже).

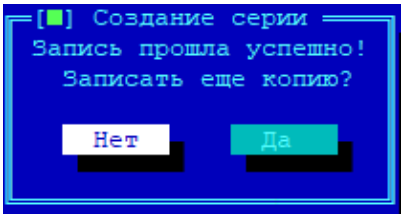

Рисунок 39 - Запись ключа хранения

После записи ключа хранения таблицы парно-выборочных ключей, будет произведен выход из окна "Создание серии" и сгенерированная серия ключевых данных ФПСУ-IP появится в окне в списке серий (см. рисунок ниже).

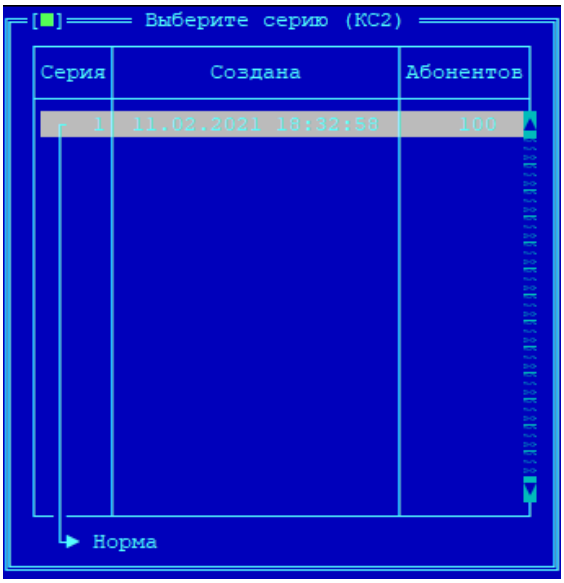

Рисунок 40 - Список серий ключевых данных

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

7. 3. 2. Генерация новой серии ключевых данных классов КС1 и КС3

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

Рисунок 41 - Пустой список серий ключевых данных

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

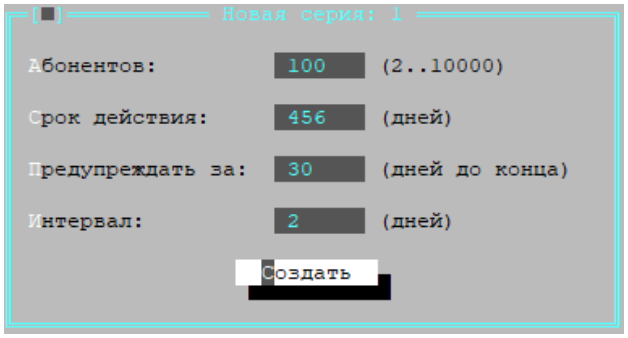

Рисунок 42 - Создание новой серии ключей КС3

При создании серии, в поле "Абонентов:" требуется указать максимальное количество абонентов (программно-аппаратных комплексов ФПСУ-IP), на которое рассчитана данная серия (от 2-х до 1000 для КС1, от 2-х до 10000 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-IP, 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-IP на носитель, описана в пункте Выдача парно-выборочных ключей.

7. 4. Выдача парно-выборочных ключей

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 (см. рисунок ниже) каждая сгенерированная и не удаленная серия ключевых данных помечена состоянием "Норма" – это означает, что ключевые данные сгенерированы и их можно выдать 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", а сгенерированные в её рамках ключевые данные удалены и недоступны для выдачи на внешний носитель. Запись об удаленной серии не удаляется из списка серий.

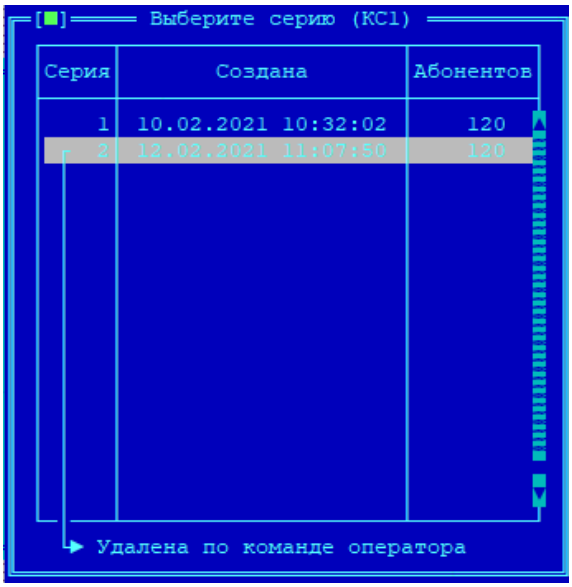

Рисунок 43 - Отображение удаленной серии

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 (см. рисунок ниже), созданный на этапе генерации серии ключевых данных.

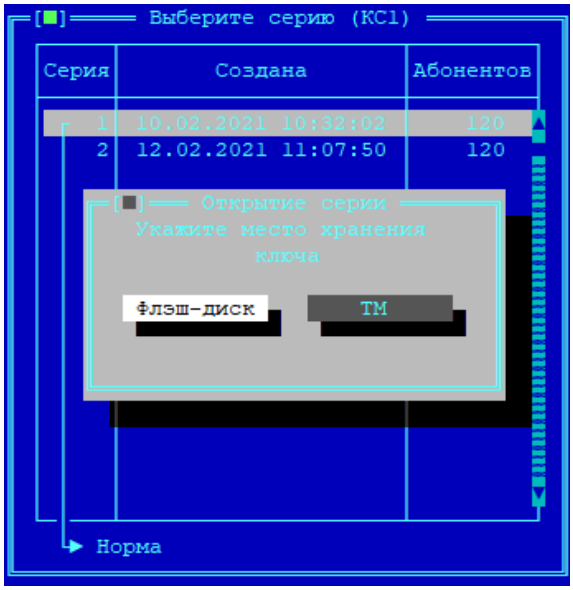

Рисунок 44 - Открытие ключа серии

После того, как будет установлен и указан внешний носитель с серией ключевых данных, отобразится следующее окно (см. рисунок ниже):

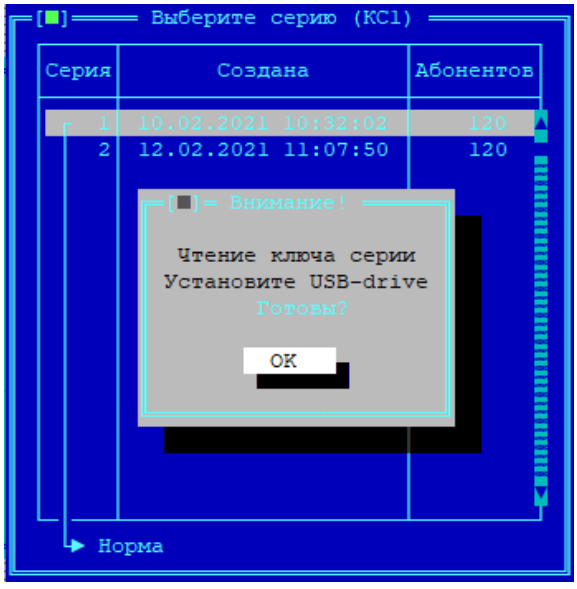

Рисунок 45 - Чтение ключа серии

Если предъявленный ключ хранения будет неверным, на экране появится сообщение об ошибке (см. рисунок ниже).

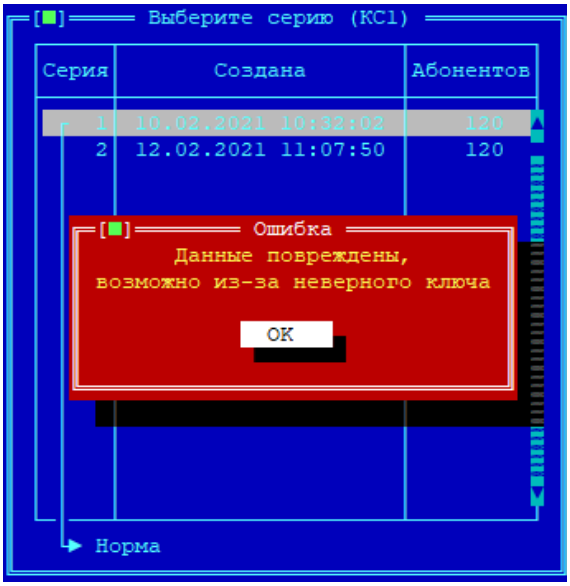

Рисунок 46 - Данные серии повреждены

Если предъявленный ключ хранения будет верным, на экране появится окно с заданными дополнительными параметрами для этой серии (см. рисунок ниже).

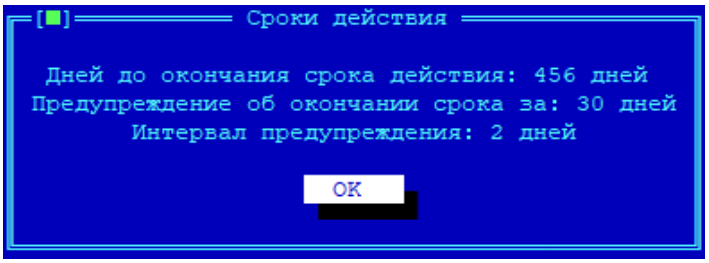

Рисунок 47 - Дополнительные параметры серии

Далее на экране появится окно (см. рисунок ниже), содержащее нумерованный список ключевых данных серии.

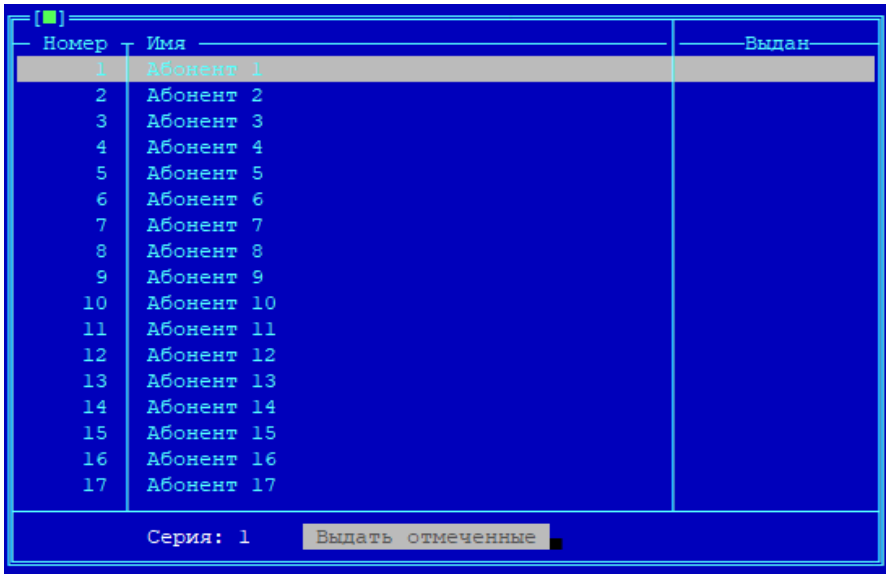

Рисунок 48 - Список ключей выбранной серии

В списке ключевые данные представлены номерами и именами ФПСУ-IP, для которых они были созданы. Для удобства администратор может дать каждому ключу имя (например, по географическому или административному признаку ФПСУ-IP, 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.

7. 4. 1. Выдача одного парно-выборочного ключа

Если требуется выдать из ЦВК ключ 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-flash носитель. В появившемся информационном окне, где находятся сведения об имени и номере выдаваемого парно-выборочного ключа (см. рисунок ниже), подтвердите продолжение, нажав кнопку "Выдать".

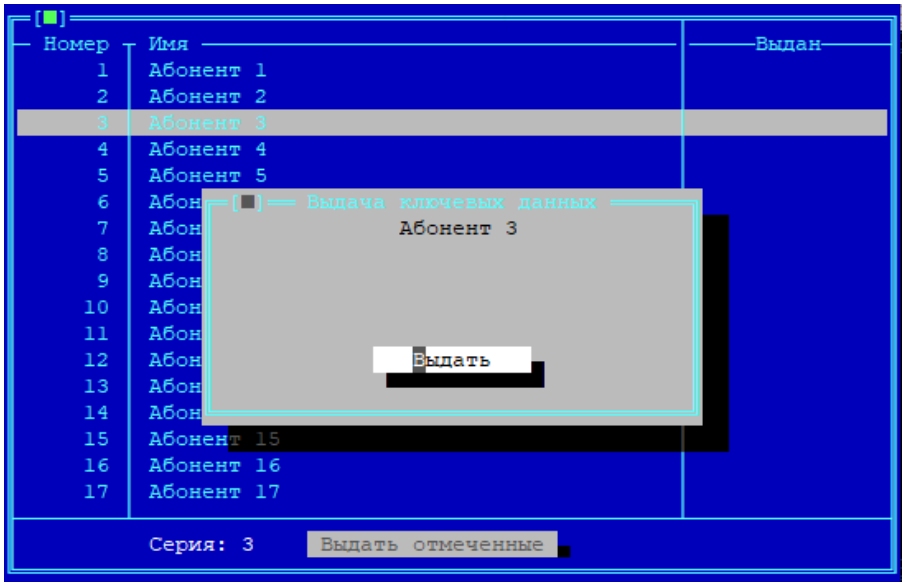

Рисунок 49 - Подтверждение выдачи ключа

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

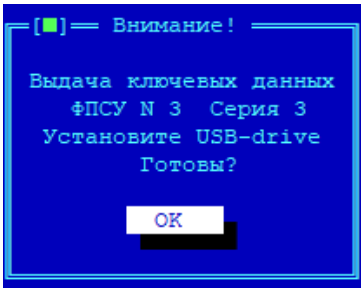

Рисунок 50 - Запрос на подключение USB-носителя

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

После нажатия кнопки "ОК" парно-выборочный ключ указанного номера (см. рисунок выше) будет записан на USB-носитель, а в списке ключевых данных серии появится запись о выдаче ключа на носитель (см. рисунок ниже).

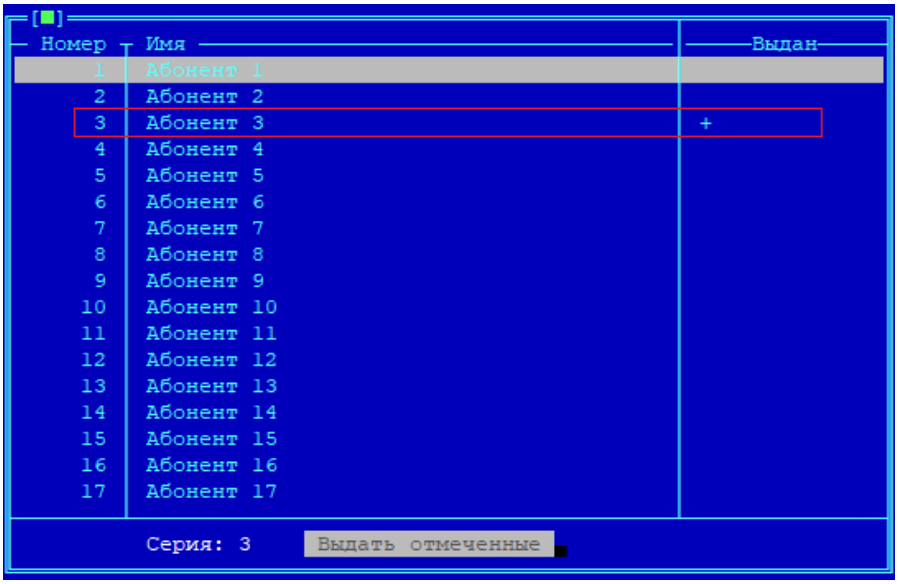

Рисунок 51 - Выданный ключ отмечается знаком "+"

7. 4. 2. Массовая выдача парно-выборочных ключей

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

- отметить положенные к выдаче ключи в списке окна. Ключ отмечается знаком "v" на выбранной курсором строке по нажатию клавиши <Пробел> (см. рисунок ниже);
- выполнить команду "Выдать отмеченные", переход на которую из списка ключевых данных серии осуществляется нажатием клавиши <Tab>.

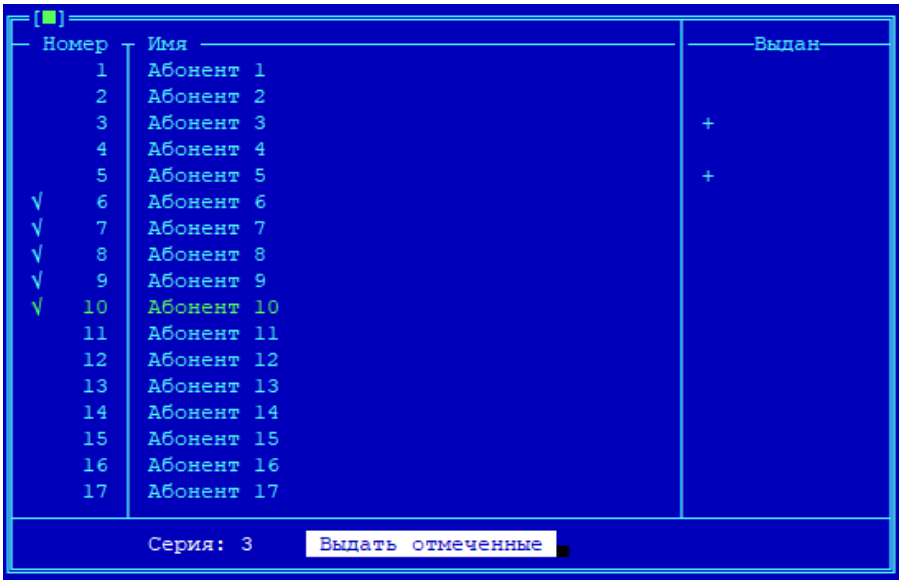

Рисунок 52 - Отмеченные для выдачи ключи серии

После выполнения команды "Выдать отмеченные", система предложит подключить к ЦВК USB-носитель, на который будут записаны ключевые данные (см. рисунок ниже). Подключите USB-носитель к ЦВК и нажмите "ОК".

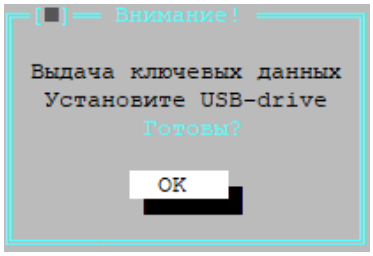

Рисунок 53 - Запрос на подключение USB-носителя

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

8. Импорт и экспорт серий ключевых данных

Зарегистрированные в ЦВК центры криптосетей ФПСУ-IP 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 "Имя_центра.asX", где "X" может быть 1, 2 или 3, обозначая класс ключей как 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!

8. 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 (см. рисунок ниже). Экспортируемые данные будут зашифрованы на специальном ключе экспорта.

Рисунок 54 - Список типов ключей центра

На экран будет выдано окно выбора внешнего носителя, на который будет записан ключ экспорта, USB-носитель или ТМ-идентификатор (см. рисунок ниже).

Рисунок 55 - 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 (см. рисунок ниже).

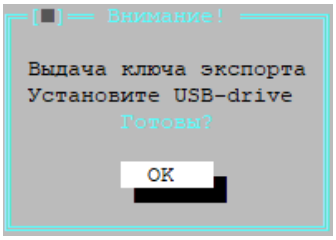

Рисунок 56 - Подтверждение подключения внешнего носителя

Файл записывается в корневую папку носителя, и в случае конфликта имен

перезаписывает файл (см. рисунок ниже).

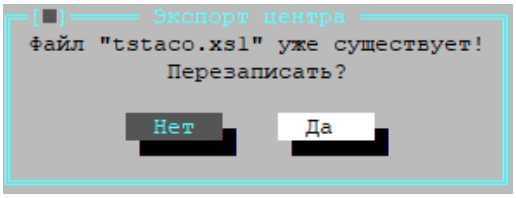

Рисунок 57 - Подтверждение перезаписи файла ключа экспорта

Критерием успешности экспорта ключа является системное оповещение "Запись прошла успешно!" (см. рисунок ниже). Можно записать копию ключа экспорта на другой носитель, выбрав команду "Да".

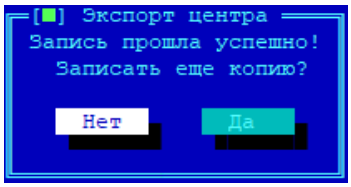

Рисунок 58 - Экспорт центра

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 (см. рисунок ниже):

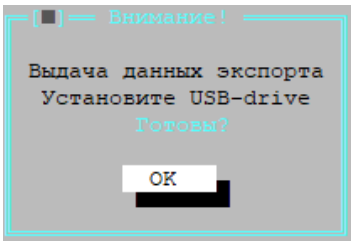

Рисунок 59 - Подключите USB-носитель к ЦВК

После успешной записи система выдаст сообщение "Экспорт центра прошел успешно" (см. рисунок ниже). После этого можно отключать USB-носитель и продолжить работу с ЦВК в штатном режиме.

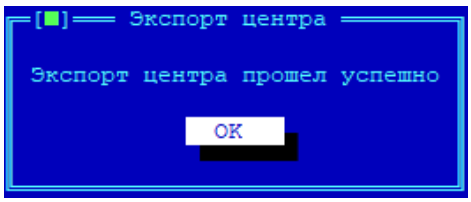

Рисунок 60 - Экспорт центра прошел успешно

8. 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 (см. рисунок ниже):

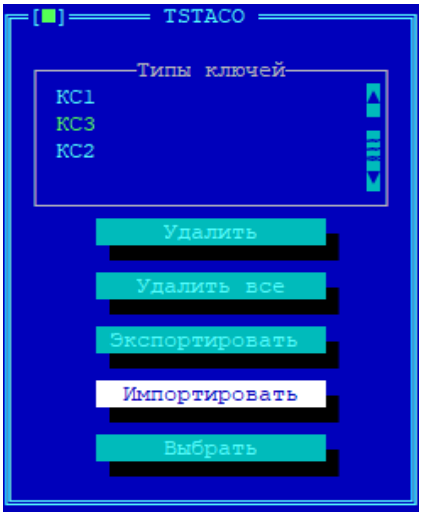

Рисунок 61 - Список типов ключей центра

После выполнения команды, система потребует предъявить ключ экспорта, на котором зашифрованы импортируемые данные (см. рисунок ниже). Во время экспорта ключ мог быть сохранен и на ТМ-идентификатор, и в файл на внешний носитель.

Рисунок 62 - Выберите место хранения ключа экспорта

Если ключ экспорта был ранее сохранен в TM-идентификатор, то нажмите кнопку "TM". По предложению системы предъявите TM-идентификатор: в зависимости от типа носителя, приложите устройство touch-memory с ключом экспорта к TM-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 находится в корневой папке носителя.

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

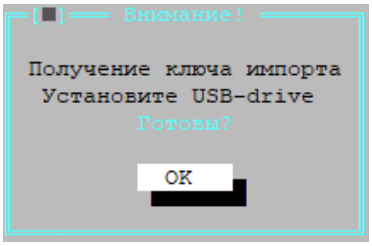

Рисунок 63 - Подтверждение получения ключа импорта

Далее выдается окно с подтверждением получения лицензии и парно-выборочных ключей импортируемого центра (см. рисунок ниже).

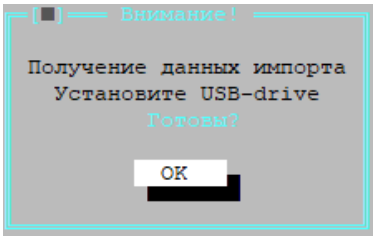

Рисунок 64 - Импорт данных

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 (см. рисунок ниже).

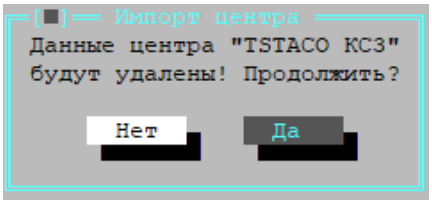

Рисунок 65 - Данные центра перезаписываются

При штатном завершении процедуры импорта будет выдано сообщение "Импорт центра прошел успешно" (см. рисунок ниже).

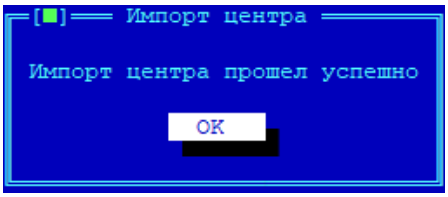

Рисунок 66 - Импорт центра

9. 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 (см. рисунок ниже):

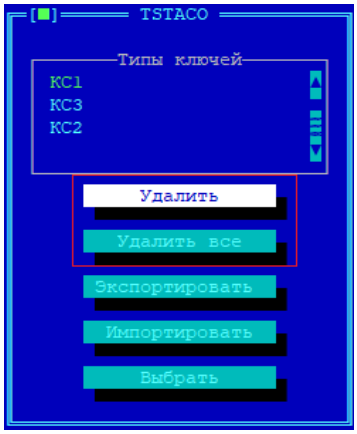

Рисунок 67 - Список типов ключей центра

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 (см. рисунок ниже):

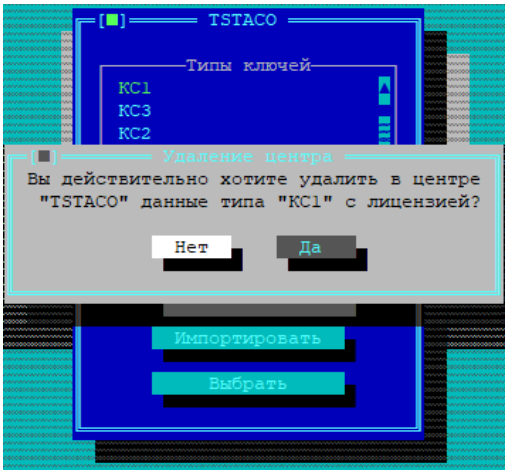

Рисунок 68 - Удаление ключей одного типа

Нажмите кнопку "Да" в появившемся окне для удаления с ЦВК всех серий выбранного типа ключевых данных. В случае успешного удаления будет выдано служебное оповещение "В центре Имя_центра удалены данные типа "КС1" или "В центре Имя_центра удалены данные типа "КС1" с лицензией", если был удален последний тип ключевых данных.

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. Переустановка ЦВК

ЦВК поставляется с предустановленным программным обеспечением. Переустановка требуется только в случае неуспешной проверки целостности контролируемых файлов, либо при замене жесткого диска.

При переустановке все хранящиеся на внутреннем накопителе ЦВК ключи будут стерты. Рекомендуется перед переустановкой сделать экспорт ключевых данных.

Для переустановки необходимы USB-носитель с дистрибутивом, 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, и дальнейшего следования указаниям мастера установки. В процессе установки система будет несколько раз перезагружена.

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

Включите питание аппаратной платформы, на которую ставится ПО ЦВК. При загрузке ЦВК после стартовых тестов в окне оповещения необходимо в течении первых секунд нажимать стрелку вниз на клавиатуре, чтобы отобразилось стартовое окно загрузчика (см. рисунок ниже).

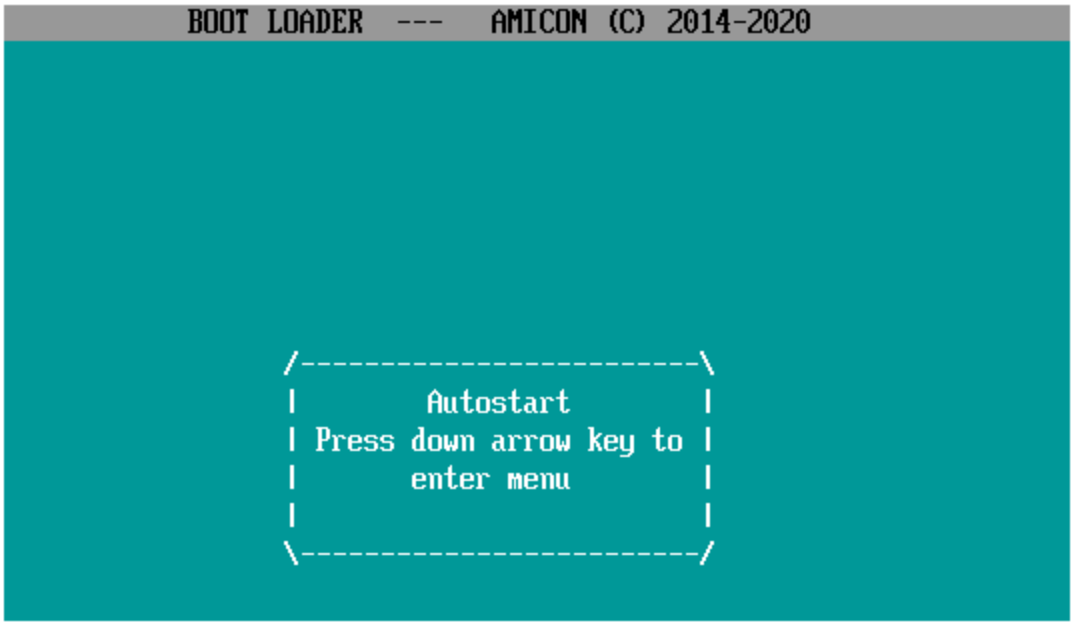

Рисунок 69 - Окно автостарта

На экран будет выдано стартовое окно загрузчика (см. рисунок ниже).

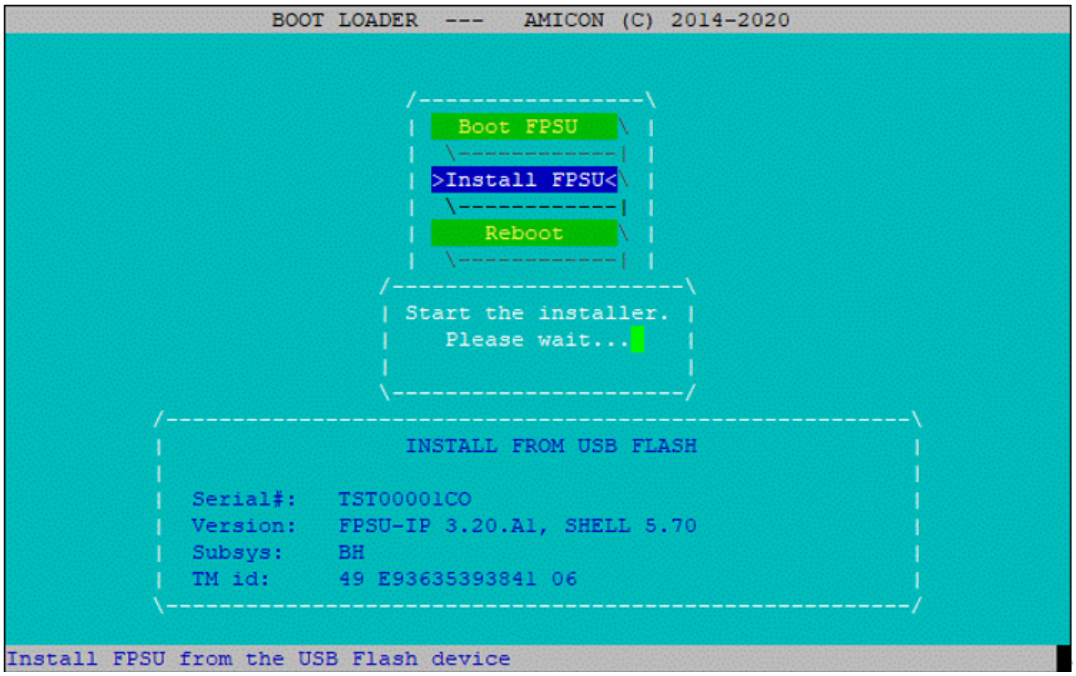

Рисунок 70 - Окно загрузчика ЦВК

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".

Необходимо предъявить ТМ-идентификатор (посредством подключения ТМ-идентификатора к USB-порту ЦВК) для продолжения переустановки (см. рисунок ниже).

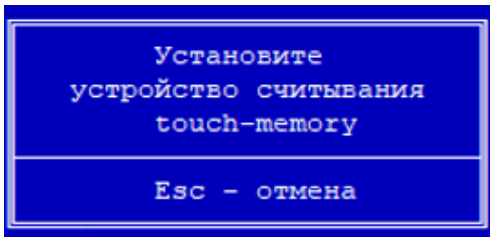

Рисунок 71 - Необходимо подключить к ЦВК устройство TM-Key или USB TM-считыватель

В случае, если ЦВК переустанавливается по причине нарушения целостности контролируемых файлов, на экран будет выдано сообщение о ранее установленном ПО ЦВК. Подтвердите выбранное действие (см. рисунок ниже).

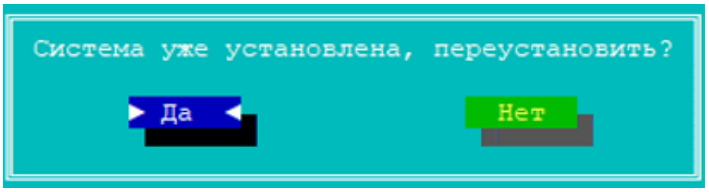

Рисунок 72 - Ожидание ответа пользователя

При переустановке система отформатирует диск, сформирует разделы на диске и выдаст сообщение (см. рисунок ниже).

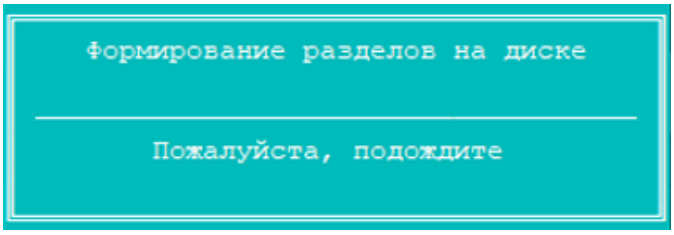

Рисунок 73 - Формирование разделов

При успешном завершении переустановки выдается сообщение о серийном номере и дальнейшей перезагрузке (см. рисунок ниже).

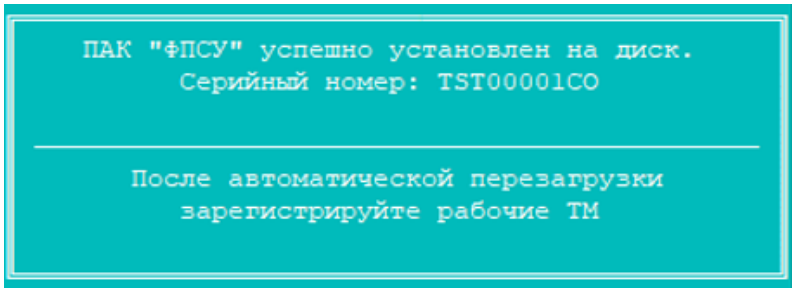

Рисунок 74 - Серийный номер

При перезагрузке отобразится окно загрузчика (см. рисунок ниже), потребуется обязательная инициализация ПДСЧ и перерегистрация ключей администратора.

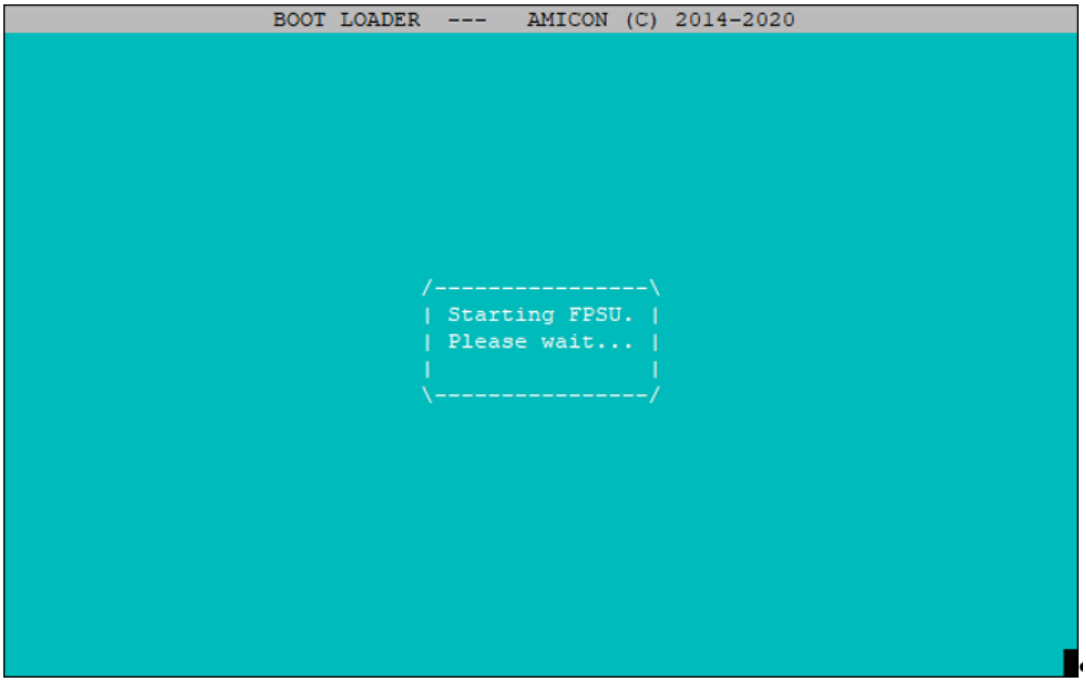

Рисунок 75 - Перезагрузка

В окне инициализации ПДСЧ необходимо последовательно вводить указываемые на экране цифры (см. рисунок ниже). При этом будет сформирован криптографический ключ для генерации новых серий ключевых данных.

Рисунок 76 - Инициализация ПДСЧ

После инициализации ПДСЧ отобразится окно с таблицей зарегистрированных ТМ-идентификаторов. Требуется перейти в штатный режим и перерегистрировать ТМ-идентификатор Главного Администратора по кнопке "Понятно" (см. рисунок ниже).

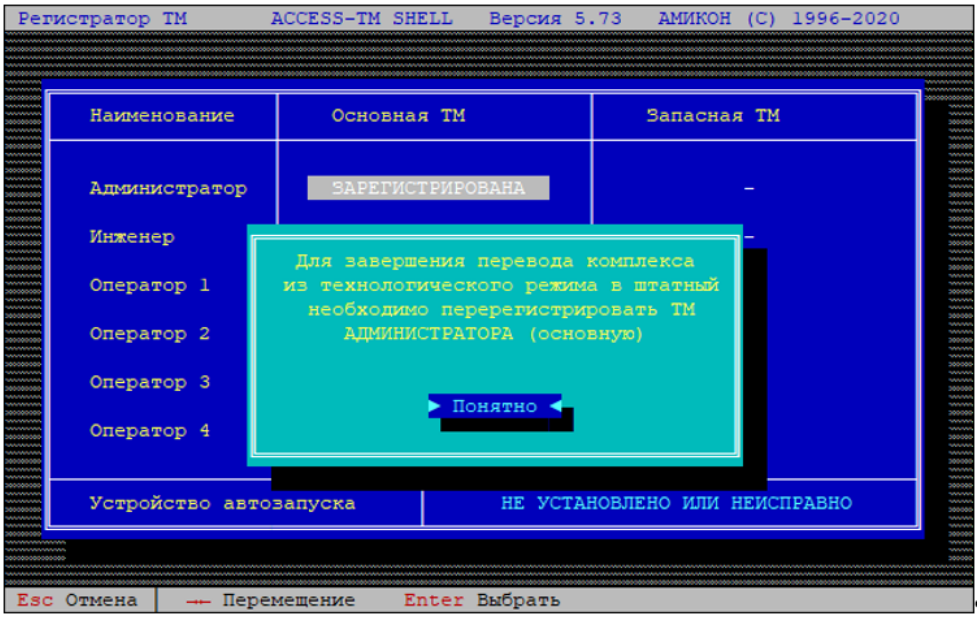

Рисунок 77 - Переход в штатный режим

Далее потребуется ещё одна перезагрузка и регистрация запасного ТМ-идентификатора (см. рисунок ниже).

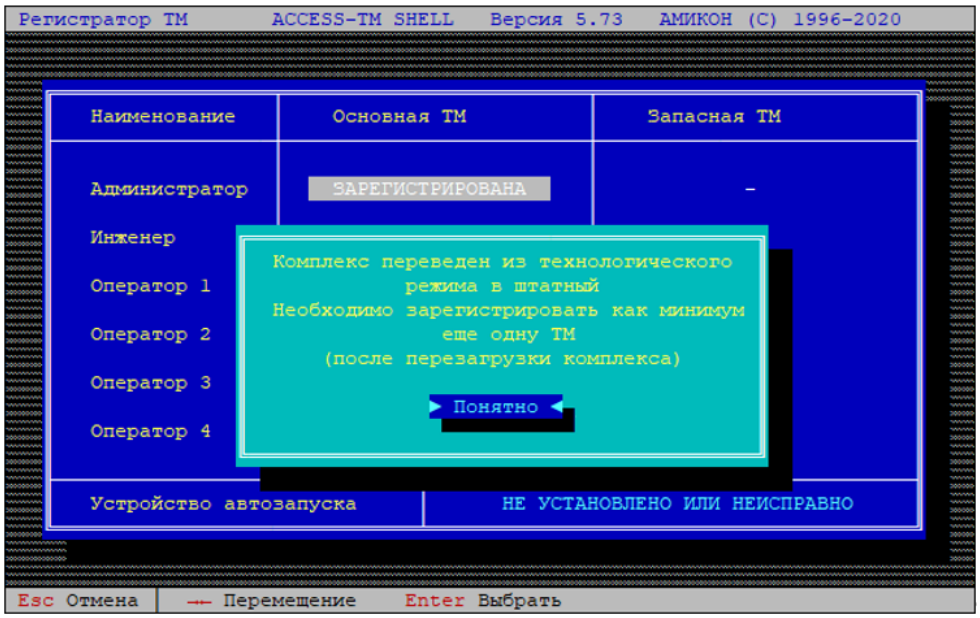

Рисунок 78 - ЦВК переведен в штатный режим работы

После перезагрузки отобразится таблица с уже зарегистрированным ТМ-идентификатором Главного Администратора (см. рисунок ниже).

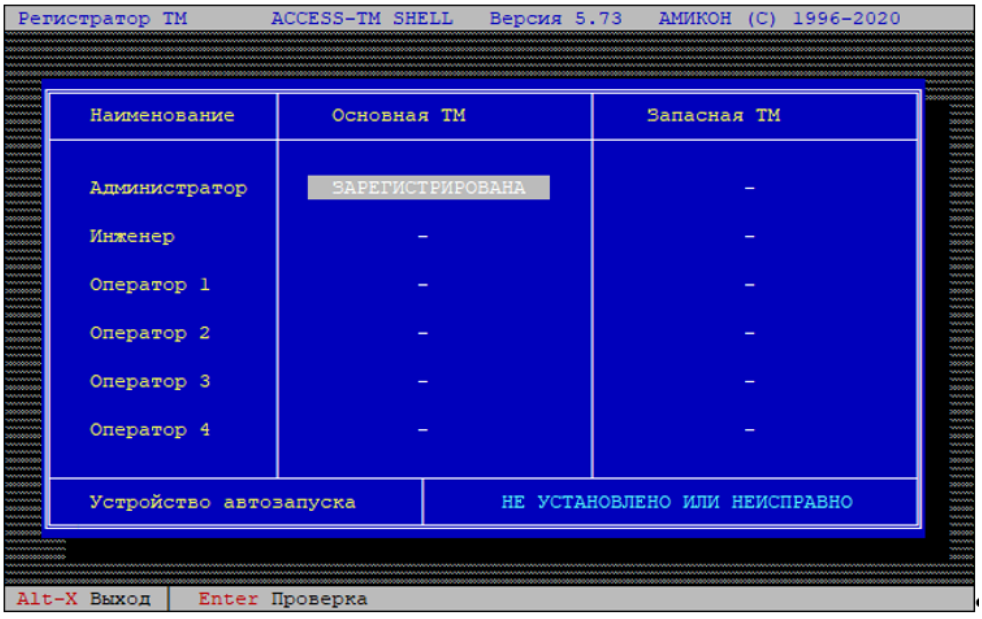

Рисунок 79 - Таблица зарегистрированных ТМ-идентификаторов

Выберите в таблице в строке "Администратор" поле "Запасная ТМ" и нажмите клавишу <Ins>. Отобразится запрос на регистрацию запасного ТМ-идентификатора администратора, который необходимо подтвердить по кнопке "Да" (см. рисунок ниже).

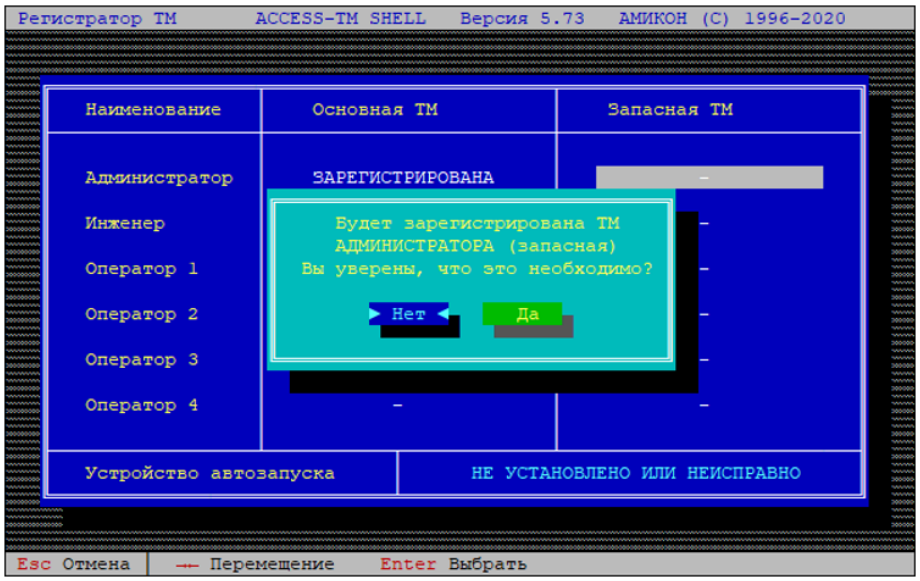

Рисунок 80 - Регистрация запасной ТМ

Для этого необходимо убрать ТМ-идентификатор Главного Администратора и предъявить запасной ТМ-идентификатор администратора для его регистрации (см. рисунок ниже).

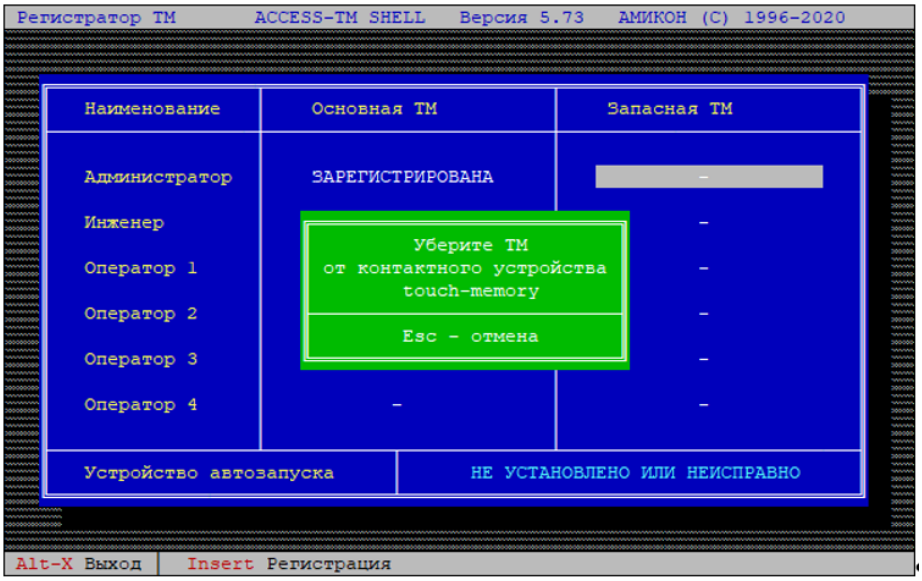

Рисунок 81 - Регистрация запасной ТМ

После того, как запасной ТМ-идентификатор администратора зарегистрирован (см. рисунок ниже), отключите USB-носитель с дистрибутивом.

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

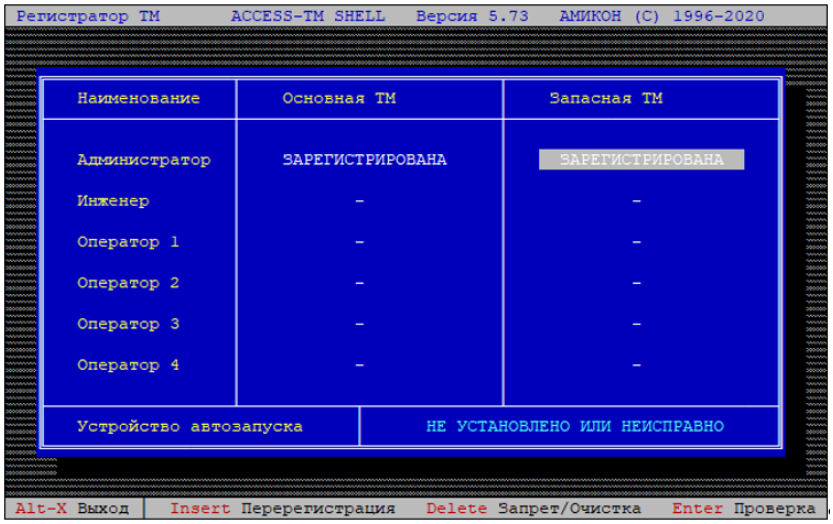

Рисунок 82 - Регистрация запасной ТМ

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-IP. Нажмите кнопку "Нет" (см. рисунок ниже).

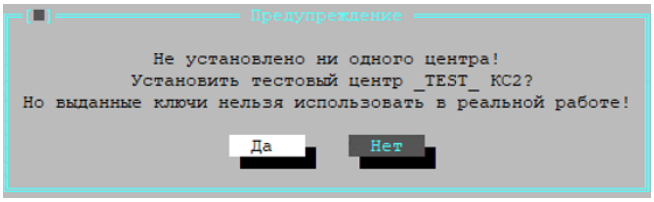

Рисунок 83 - Предупреждение

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.