ООО «АМИКОН»

Утверждено
РОФ. ПЕРС. 00114-01 34 01-ЛУ

Центр генерации ключей клиентов версии 7.0

Руководство по применению

РОФ. ПЕРС. 00114-01 34 01

Количество листов 90

2026

Аннотация

Документ предназначен для администраторов безопасности организаций, использующих для построения систем защиты от несанкционированного доступа к информации средства криптографической защиты информации «ФПСУ-IP Amigo». В документе содержатся общие сведения о программе генерации ключевой информации, необходимой для организации защищен-ных каналов связи между рабочими местами пользователей, оснащенных ФПСУ-IP/Клиентами, и ФПСУ-IP, приведен перечень необходимых организационно-технических мер и дано описание последовательности действий при установке программы, создании и настройки логической структуры VPN сети.

Содержание

1. Список используемых терминов и определений

PIN-код пользователя VPN-профиля	цифровой код, требующийся для работы ФПСУ-IP/Клиента с этим VPN-профилем;
Администратор ЦГКК	физический пользователь ЦГКК, для которого заданы логин и пароль;
АРМ	автоматизированное рабочее место;
АРМ пользователя ФПСУ-IP/Клиент, АРМ Клиента	автоматизированное рабочее место, ПЭВМ или мобильное устройство, на которое установлено программное обеспечение ФПСУ-IP/Клиента;
АПМДЗ	аппаратно-программный модуль доверенной загрузки;
ДСЧ	датчик случайных чисел;
Ключ	изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование;
Ключевая информация	специальным образом организованная совокупность ключей, предназначенная для осуществления криптографической защиты информации определенного пользователя;
Ключевой носитель	физический носитель, предназначенный для размещения и хранения на нем ключевой информации;
Криптосеть	совокупность ФПСУ-IP/Клиентов, использующих для построения VPN-туннеля ключи, выработанные в ЦГКК на основе единого общесистемного ключа. Каждая Криптосеть имеет собственное имя и уникальный номер, присвоенные производителем;
Номер генерации	числовой счетчик-идентификатор сгенерированных ЦГКК ключевых данных пользователя Криптосети ФПСУ-IP/Клиентов (изменяется от 1 до 256, по умолчанию равен 1), может быть изменен администратором ЦГКК. Записывается в VPN-профиль ФПСУ-IP/Клиента при инициализации VPN-Key или выдаче VPN-профиля

	в файл. Номер генерации, записанный в VPN-профиль ФПСУ-IP/Клиента, должен соответствовать тому, что указан на ФПСУ-IP, иначе ФПСУ-IP/Клиент не сможет соединиться с ФПСУ-IP;
НСД	несанкционированный доступ к информации;
ОС	операционная система;
ПЗУ	постоянное запоминающее устройство (НЖМД, SSD-диск и т.п.); используется для хранения массива данных;
ПО	программное обеспечение;
ПЭВМ	персональная электронная вычислительная машина;
Пользователь	в рамках данного документа: пользователь Криптосети, учетная запись из состава одной из групп Криптосети. Необходимые для создания VPN-туннеля VPN-профили генерируются ЦГКК с привязкой к конкретному пользователю Криптосети;
Программно-аппаратный Клиент	модификации 7.1 следующих вариантов исполнения СКЗИ «ФПСУ-IP Amigo»: • «ФПСУ-IP/Клиент КС1», • «ФПСУ-IP/Клиент АТМ КС1», • «ФПСУ-IP/Клиент КС2», • «ФПСУ-IP/Клиент АТМ КС2», используется для создания VPN-туннеля с применением устройства «VPN-Key/Client»;
Программный Клиент	модификации 7.1 следующих вариантов исполнения СКЗИ «ФПСУ-IP Amigo»: • «Программный клиент Win КС1», • «Программный клиент Win АТМ КС1», • «Программный клиент Win КС2», • «Программный клиент Win АТМ КС2», • «Программный клиент Linux КС1» • «Программный клиент Linux АТМ КС1» • «Программный клиент Linux КС2», • «Программный клиент Linux АТМ КС2»,

	используется для создания VPN-туннеля без применения устройства «VPN-Key/Client»;
СКЗИ	средство криптографической защиты информации;
СЗИ МДЗ	средство защиты информации, реализующее механизмы доверенной загрузки
ФПСУ-IP/Клиент	общее название для Программных и Программно-аппаратных клиентов;;
ФПСУ-IP	одно из следующих изделий производства ООО «АМИКОН»: • «Криптомаршрутизатор и межсетевой экран «ФПСУ-IP Amigo» версии 4», программный или программно-аппаратный комплекс, программная компонента которого является вариантом исполнения «ФПСУ-IP Int КС1», «ФПСУ-IP Int КС2», «ФПСУ-IP Int КС3», «ФПСУ-IP КС1», «ФПСУ-IP Q КС1», «ФПСУ-IP КС2», «ФПСУ-IP Q КС2», «ФПСУ-IP КС3» или «ФПСУ-IP Q КС3» СКЗИ «ФПСУ-IP Amigo»; • «Программно-аппаратный комплекс «ФПСУ-IP» версии 3», программный или программно-аппаратный комплекс «ФПСУ-IP» версии 3, программная компонента которого является изделием Криптомаршрутизатор из состава СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP»; • ««ФПСУ-IP Int» версии 3», программно-аппаратный комплекс, программная компонента которого является изделием Криптомаршрутизатор из состава СКЗИ «ФПСУ-IP Int».
ФПСУ-IP/Клиент	общее название для Программных и Программно-аппаратных Клиентов;;
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую;
ЦГКК	Модификации 7.0 следующих вариантов исполнений СКЗИ «ФПСУ-IP Amigo»: • «ЦГКК КС1», • «ЦГКК КС2».
PIN-код	цифровой код, требующийся для работы ФПСУ-IP/Клиента с этим

администратора VPN-профиля	VPN-профилем и системной настройки VPN-профиля;
VPN	Virtual Private Network, виртуальная частная сеть передачи данных, создаваемая поверх существующей общедоступной или частной сети передачи данных;
VPN-профиль	создаваемый ЦГКК набор служебных данных и ключевой информации, необходимый для работы криптографического сервиса ФПСУ-IP/Клиента. VPN-профиль содержит настройки, которые позволяют ФПСУ-IP/Клиенту соединиться с ФПСУ-IP, в частности содержит IP-адреса ФПСУ-IP и ключевые данные пользователя ФПСУ-IP/Клиента;
VPN-туннель	виртуальный канал связи, защищенный криптографическими методами (двусторонней аутентификацией и шифрованием передаваемых данных);
VPN-Key	программно-аппаратное устройство «VPN-Key/Client», являющееся ключевым носителем и реализующее алгоритмы криптографических преобразований и выработки случайных последовательностей, в которое установлен микрокод из состава модификации 7.1 следующих вариантов исполнений СКЗИ «ФПСУ-IP Amigo»: • «ФПСУ-IP/Клиент КС1», • «ФПСУ-IP/Клиент КС2», • «ФПСУ-IP/Клиент АТМ КС2», • «ФПСУ-IP/Клиент АТМ КС2».

2. Общие сведения

Программа «Центр генерации ключей клиентов», предназначена для создания ключевой информации для защиты обмена данными между АРМ пользователя ФПСУ-IP/Клиента и ФПСУ-IP.

Руководство предназначено для работы с программой «Центр генерации ключей клиентов» версии 7.0.

Каждая Криптосеть, созданная при помощи программы ЦГКК, предназначена для работы с ограниченным, указанным в лицензии на Криптосеть, количеством VPN-профилей. Криптосеть имеет собственное имя и уникальный номер, характеризующие данную Криптосеть, а также определённый срок действия (эти параметры фиксируются в специальном файле-лицензии).

Одна программа ЦГКК может использоваться для организации работы нескольких Криптосетей.

Основными функциями программы ЦГКК являются:

- регистрация Криптосетей на основе предъявленных лицензий на использование Криптосетей;
- генерация общесистемного ключа Криптосети и запись его на ТМ-идентификатор или в файл;
- создание логической структуры пользователей Криптосети;
- запись ключевой информации пользователя и системной информации (VPN-профиля) в устройства «VPN-Key» для работы с программно-аппаратным ФПСУ-IP/Клиентом (инициализация «VPN-Key»);
- генерация ключевой информации для работы с программным ФПСУ-IP/Клиентом.

Вырабатываемый программой ЦГКК общесистемный ключ Криптосети может храниться в распределенном виде на нескольких ТМ-идентификаторах (в качестве ТМ-идентификатора используются электронные устройства iButton DS1993 – DS1996 или микроэлектронные USB-устройства «TM-Key» разработки ООО «АМИКОН»), в этом случае общесистемный ключ может быть воссоздан на ЦГКК только в том случае, если будут предъявлены все первичные ключи.

Внутри одной Криптосети пользователи подразделяются на логические группы с уникальными номерами. Пользователю присваивается уникальный в пределах его группы Криптосети номер.

На основе общесистемного ключа Криптосети ЦГКК вырабатывает ключевую

информацию пользователя, которая записывается в устройство «VPN-Key» для программноаппаратного комплекса и в бинарный файл для программного ФПСУ-IP/Клиента.

Одновременно с ключевой информацией ЦГКК записывает системные идентификаторы пользователя (номер Криптосети Клиентов, номер группы и индивидуальный номер пользователя в группе) и его персональные коды доступа к ключевой информации.

Программа ЦГКК входит в состав модификации 7.0 следующих вариантов исполнений СКЗИ «ФПСУ-IP Amigo»:

- «ЦГКК КС1»,
- «ЦГКК КС2»,

поставляется в соответствии с документом «Средство криптографической защиты информации «ФПСУ-IP Amigo». Формуляр» и должна использоваться в соответствии с документом «Средство криптографической защиты «ФПСУ-IP Amigo». Правила пользования» .

3. Защита от НСД

Под защитой информации от несанкционированного доступа подразумевается деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником прав или правил доступа к защищаемой информации.

3. 1. При инсталляции

Перед инсталляцией ПО ЦГКК:

1. В обязательном порядке произвести мероприятия по обеспечению сохранности и целостности системного блока ПЭВМ (опечатать крышку системного блока и разъёмы ПЭВМ);
2. В обязательном порядке произвести проверку ПЭВМ на наличие компьютерных «вирусов»;
3. Рекомендуется осуществить контроль целостности инсталляционного файла посредством использования программного модуля WinFPSUHash.exe, входящего в состав поставки ЦГКК (см. пункт «Контроль целостности до установки»);
4. Сразу после установки ПО ЦГКК на ПЭВМ (см. пункт «Первоначальный контроль целостности после установки») в обязательном порядке осуществить контроль целостности ПО ЦГКК с помощью программного модуля WinFPSUHash.exe.

Не допускается установка ПО ЦГКК в ПЗУ ПЭВМ в случае обнаружения «вирусов» или нарушения целостности программных модулей ЦГКК.

3. 2. При эксплуатации

Не допускается непрерывная работа ПЭВМ с установленным ЦГКК дольше 24 часов.

Контроль целостности программы после инсталляции должен осуществляться утилитой WinFPSUHash.exe, входящей в поставку ЦГКК (см. пункт «Контроль целостности в процессе эксплуатации»). При использовании ЦГКК как СКЗИ класса КС2, контроль целостности программы может осуществляться средствами АПМДЗ или СЗИ МДЗ. Установка и настройка АПМДЗ или СЗИ МДЗ должна производиться в соответствии с эксплуатационной документацией на используемое средство. Настройка должна исключать возможность вмешательства в процессы загрузки операционной системы и прикладного ПО.

Перед каждым запуском ЦГКК необходимо:

1. Осуществить контроль сохранности и целостности системного блока ПЭВМ;

2. Произвести контроль целостности ПО ЦГКК (см. пункт «Контроль целостности в процессе эксплуатации»);
3. Осуществить проверку ПЭВМ на наличие программ «вирусов» и «посторонних» программ;
4. При нарушении целостности программных модулей ЦГКК, программу необходимо повторно установить с инсталляционного носителя.

В случае обнаружения «посторонних» программ или «вирусов», выявления факта нарушения целостности системного блока, нарушения целостности проверяемых файлов ОС или совместно работающих с ЦГКК программ, дальнейшая эксплуатация ЦГКК не допускается до устранения проблемы.

4. Установка программного обеспечения

«Центр генерации ключей клиентов» устанавливается на специально выделенную, не подключенную к сетям передачи данных ПЭВМ.

Общесистемный ключ, вырабатываемый ЦГКК, не хранится в ПЗУ ПЭВМ, однако в базу данных записываются персональные идентификационные коды пользователей Клиентов, поэтому доступ к рабочему месту посторонних лиц должен быть строго ограничен.

В комплект поставки ЦГКК входят следующие файлы:

- CGKK_7_0.exe − установочный файл программы ЦГКК 7-й версии;
- KG_NNNNN.lic − файл-лицензия на использование одной Криптосети Клиентов с уникальным номером №№№№№. Срок действия лицензии и максимальное количество пользователей, обслуживаемых данной Криптосетью Клиентов, задаются при поставке лицензии;
- WinFPSUHash.exe − программа для проведения контроля целостности (см. пункт «Контроль целостности программы ЦГКК»);
- install.hsh − файл программы WinFPSUHash.exe, содержащий контрольные данные файла CGKK_7_0.exe;
- CGKK.hsh − файл программы WinFPSUHash.exe, содержащий контрольные данные модулей программы ЦГКК.

Перед установкой программы рекомендуется выполнить контроль целостности файла установки CGKK_7_0.exe. (см. пункт «Контроль целостности до установки»).

Для установки ПО ЦГКК в операционную систему необходимо выполнить следующие действия:

1. Запустить ПЭВМ;
2. Установить инсталляционный носитель в ПЭВМ и запустить CGKK_7_0.exe;
3. Принять условия лицензионного соглашения:

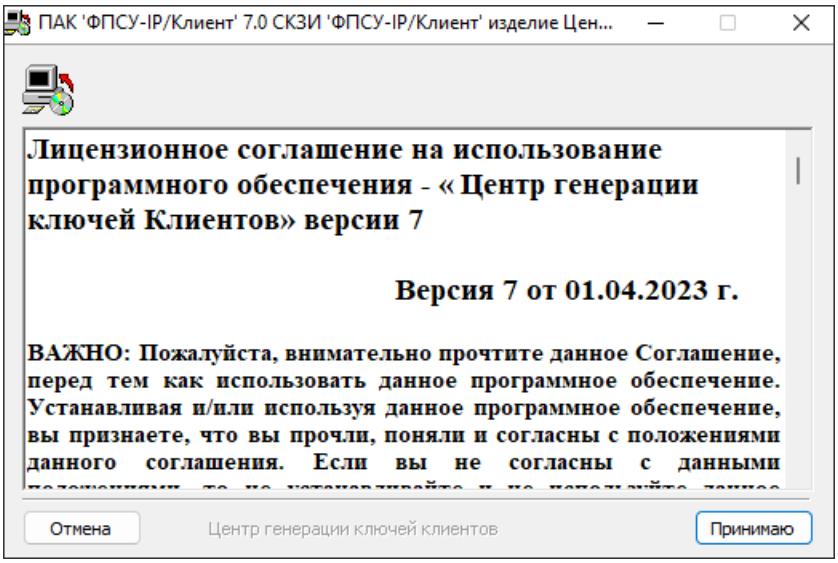

Рисунок 1 - Лицензионное соглашение

4. Выбрать опциональные компоненты устанавливаемого программного обеспечения:

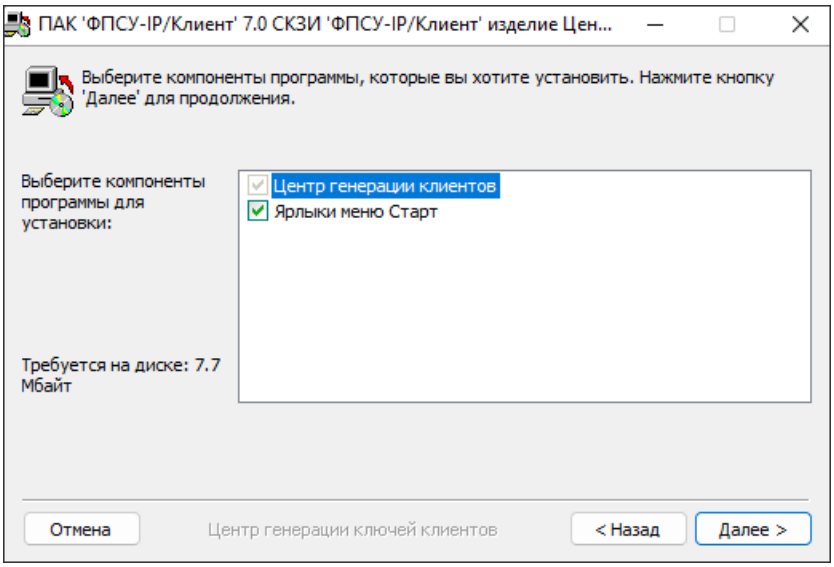

Рисунок 2 - Выбор опциональных компонентов

4. По запросу операционной системы выбрать место для установки программы ЦГКК (по умолчанию ЦГКК будет установлена в каталог %Program Files% \AMICON\Centre FPSU-IP):

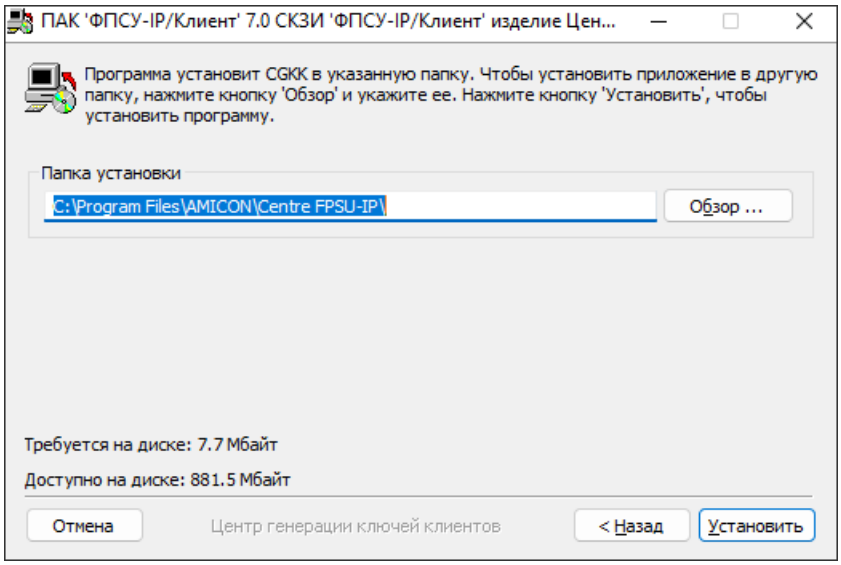

Рисунок 3 - Выбора каталога установки

Если в указанном каталоге находилась более ранняя версия программы ЦГКК, установщик предложит обновить её, сохранив логическую структуру пользователей.

5. После установки программных модулей, провести контроль целостности ПО ЦГКК с помощью программы WinFPSUHash.exe (см. пункт «Первоначальный контроль целостности после установки»);
6. Перезагрузить ПЭВМ.

Для проверки корректности установки драйверов для работы с устройством «VPN-Key» необходимо вставить в USB-порт одно из устройств «VPN-Key», открыть «Диспетчер устройств» и найти объект «USB Smart Card reader» в списке установленных устройств.

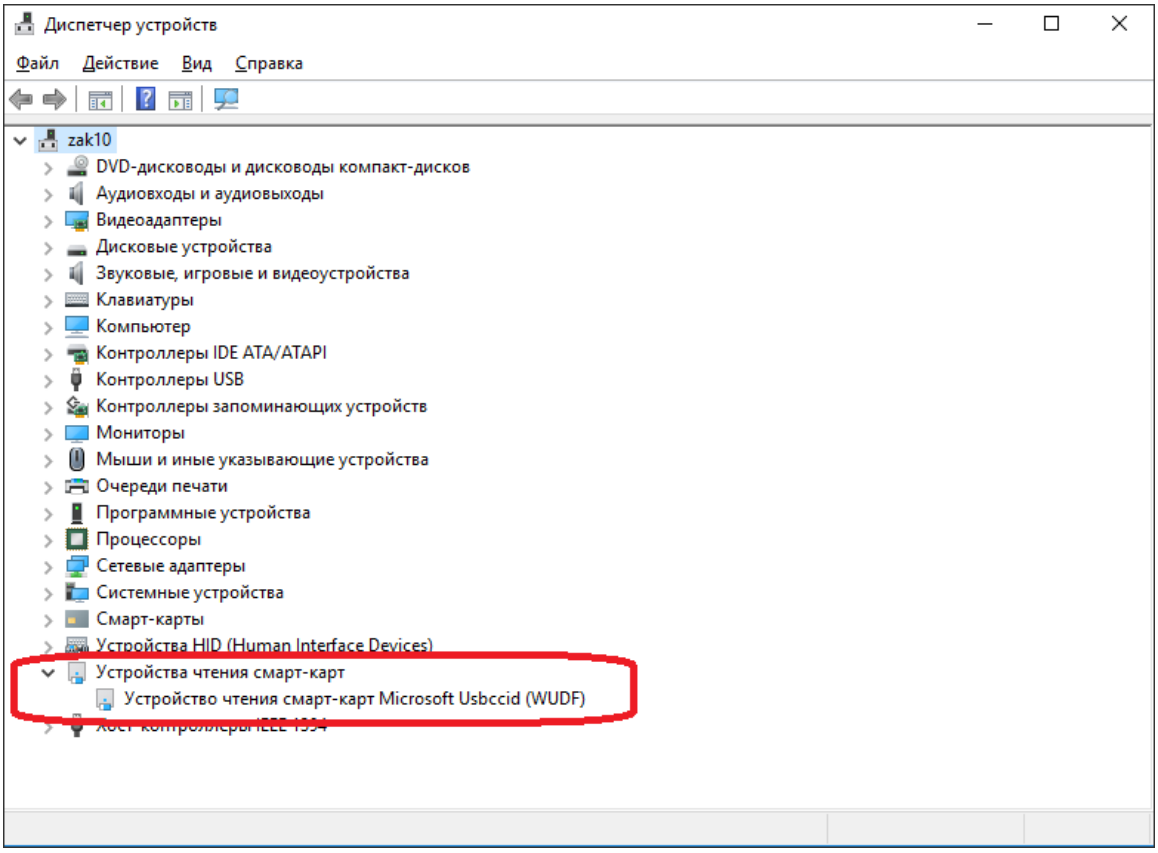

Рисунок 4 - Драйвер USB Smart Card reader установлен

Если операционная система выдаёт сообщение о том, что обнаруженное новое устройство не опознано, необходимо установить нужный драйвер с инсталляционного носителя вручную.

5. Эксплуатация ЦГКК

После установки на ПЭВМ программного обеспечения ЦГКК, в меню «Пуск» операционной системы WINDOWS будет создан пункт «АМИКОН», в котором должно отображаться название «Центр генерации ключей клиентов».

Запустить программу можно напрямую из каталога, приложение «%Program Files% AMICON\Centre FPSU-IP\KeyGen.exe».

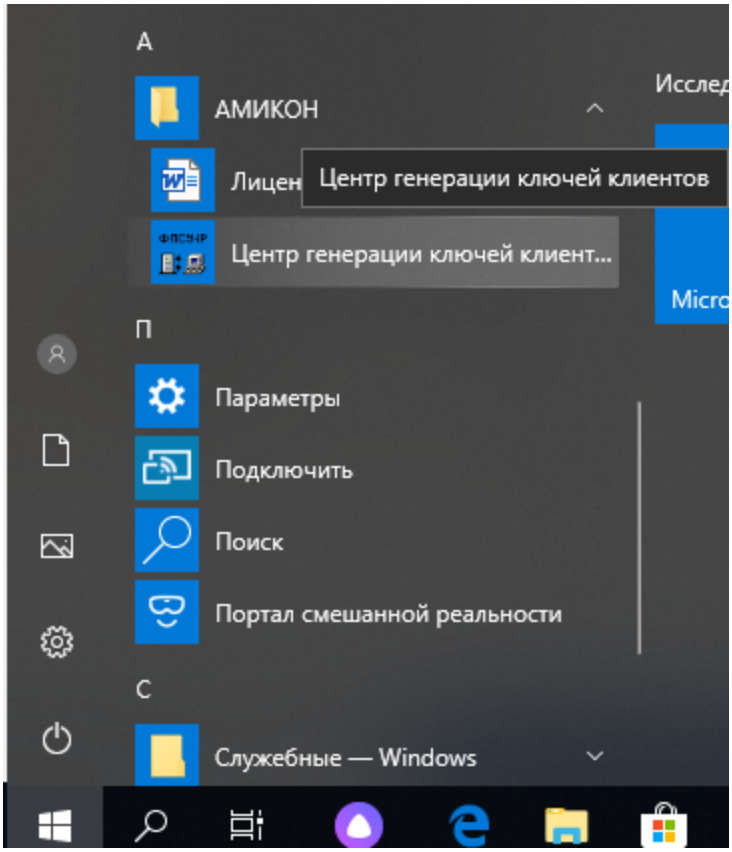

Рисунок 5 - Ярлыки на запуск программы

5. 1. Вход в программу с использованием пароля

В ЦГКК предусмотрена возможность добавления нескольких администраторов ЦГКК с заведением паролей для каждого из них.

Для добавления возможности входа по паролю необходимо:

1. Выбрать пункт меню «Настройка →Безопасность».

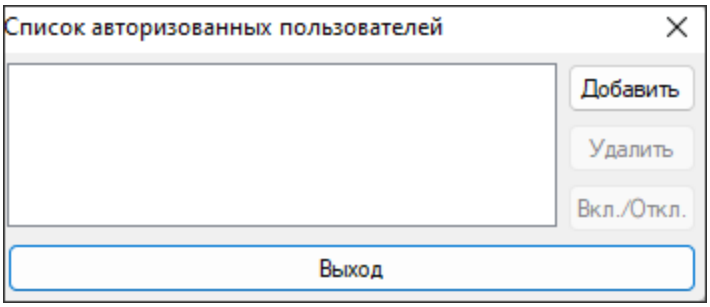

Рисунок 6 - Добавление списка администраторов

2. Для добавления администратора ЦГКК и заведения для него пароля нажать кнопку «Добавить» в окне «Список авторизованных пользователей».

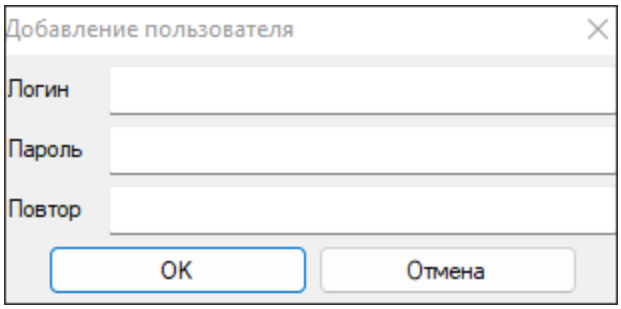

Рисунок 7 - Добавление пользователя

3. В открывшемся окне «Добавление пользователя» ввести логин администратора ЦГКК для входа в систему, а так же создать и продублировать его пароль.

После нажатия клавиши «ОК» администратор ЦГКК отобразится в окне «Список авторизованных пользователей».

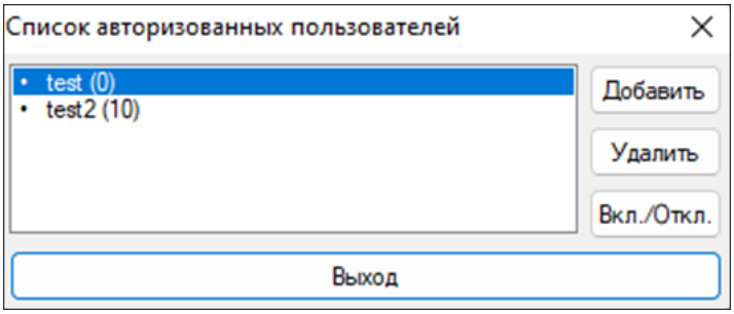

Рисунок 8 - Пользователь добавлен

По умолчанию администратор ЦГКК создается активированным, т.е. имеющим право на вход в систему при вводе своего логина и пароля (помечен точкой). В скобках отображается оставшееся количество попыток ввода пароля (максимальное количество

– 10 раз). Для деактивации администратора ЦГКК (может быть произведена любым из зарегистрированных администраторов) необходимо выбрать его в общем списке и нажать кнопку «Вкл./Откл.» в окне «Список авторизованных пользователей». После этого в открывшемся окне настроек авторизации следует подтвердить или отменить выбранное действие путем нажатия кнопок «Да» или «Нет» соответственно.

В дальнейшем после запуска ПО на экран будет выводиться окно для ввода данных администратора ЦГКК, в котором будет необходимо ввести логин и пароль для него.

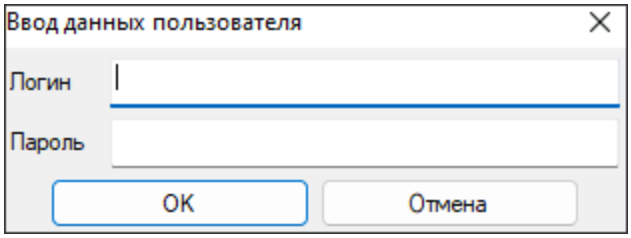

Рисунок 9 - Окно ввода данных пользователя

В том случае, если администратор ЦГКК был деактивирован, авторизоваться по его логину и паролю будет невозможно.

При необходимости администратора ЦГКК можно удалить путем выбора его в общем списке нажатия одноименной кнопки в окне «Список авторизованных пользователей» с последующим подтверждением действия. Для смены пароля администратора его так же необходимо удалить и создать заново с тем же логином и новым паролем.

Следует иметь в виду, что пароль должен состоять из 6 символов минимально.

5. 2. Регистрация Криптосетей Клиентов

При первом запуске программа потребует зарегистрировать хотя бы одну Криптосеть, выдав служебное сообщение. Без этого этапа дальнейшая работа с ЦГКК невозможна.

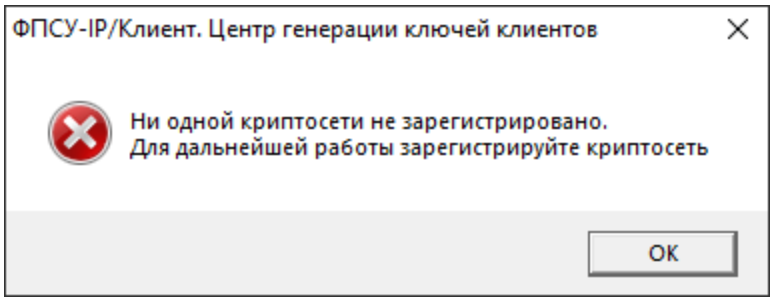

Рисунок 10 - Первый этап работы

Регистрация Криптосети – первый этап работы по выработке и изготовлению ключей. Для регистрации Криптосети необходимо предъявить лицензию на использование ЦГКК, в которой указаны имя, уникальный номер, период действия лицензии и максимальное количество обслуживаемых Клиентов. Все эти данные содержатся в файле вида KG_NNNNN.lic (NNNNN - номер Криптосети Клиентов).

При регистрации Криптосети Клиентов определяется количество первичных ключей (ТМ-идентификаторов или файлов формата *.tm), на которые будет распределён общесистемный ключ. По окончании регистрации программа ЦГКК создаст информационный файл формата *.tmk, который будет использован при выработке общесистемного ключа (см. пункт «Генерация и запись на ТМ-носитель общесистемных ключей»).

Для регистрации каждой следующей Криптосети Клиентов необходимо выполнить следующие действия:

1. Войти в меню «Операции» и выполнить команду «Зарегистрировать криптосеть ФПСУ-IP/Клиентов».

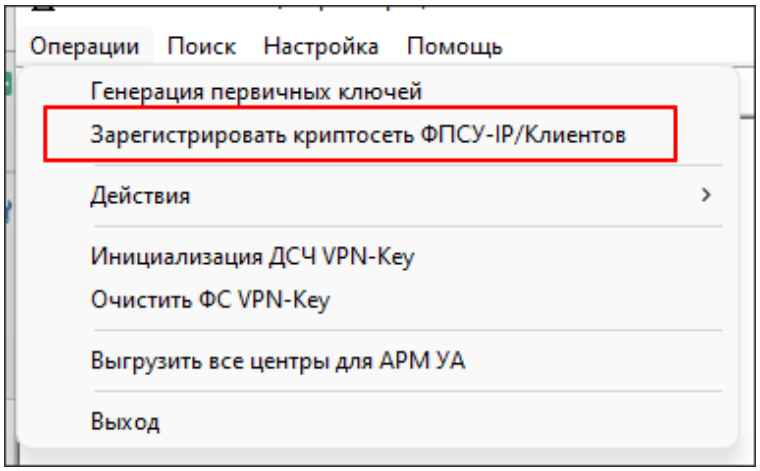

Рисунок 11 - Регистрация криптосети

2. В ответ на запрос программы указать путь к файлу-лицензии на создание Криптосети Клиентов (KG_NNNNN.lic).
3. В появившемся служебном окне указать количество первичных ключей (ТМ-идентификаторов или файлов формата *.tm), на которые должен быть распределен общесистемный ключ (от 1 до 16) и нажать ОК;

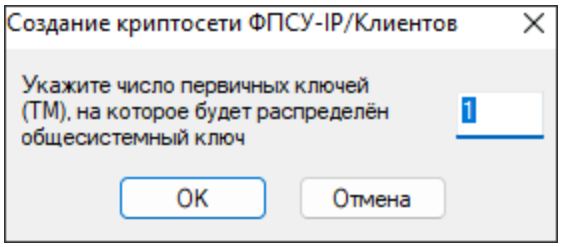

Рисунок 12 - Указание количества первичных ключей

4. После выдачи служебного окна с сообщением о создании файлов формата *.tmk, необходимых для генерации общесистемного ключа, Криптосеть Клиентов будет зарегистрирована, после чего ее имя появится в списке в левой части окна программы.

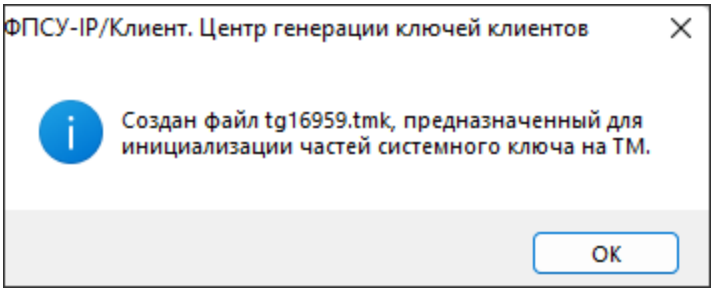

Рисунок 13 - Созданы файлы tmk

В случае необходимости – например, для увеличения количества доступных пользователей Криптосети, – лицензию можно обновить. Для этого необходимо:

1. Получить новый файл с новой лицензией на использование Криптосети Клиентов с данными номером и именем;
2. Войти в меню «Операции» и активизировать строку «Зарегистрировать криптосеть ФПСУ-IP/Клиентов»;
3. В ответ на запрос программы, указать месторасположение и имя нового файла лицензии (KG_*.lic);
4. Нажать кнопку «Да» в окне с предложением обновить лицензию.

В одной программе ЦГКК могут быть зарегистрированы несколько Криптосетей Клиентов при условии, что имеется соответствующее количество лицензий на их использование (одна Криптосеть – одна лицензия).

В контекстном меню для каждой Криптосети отображается список операций, которые можно производить с зарегистрированной Криптосетью Клиентов, а именно:

- «Свойства» - информация о Криптосети Клиентов, включающая в себя:
  - имя Криптосети Клиентов; номер Криптосети Клиентов;
  - максимальное количество пользователей Криптосети Клиентов; количество пользователей; количество оставшихся лицензий на инициализацию пользователя;
  - дата окончания срока лицензии; кем выдана лицензия;
  - количество ТМ, на которые записан общесистемный ключ;
  - серия ключа; тип ключа; срок действия ключа;
  - базовая конфигурация (если установлена).
- «Создать группу» - операция создания внутри Криптосети Клиентов логической группы пользователей;
- «Удалить» - операция удаления Криптосети Клиентов из списка.
- «Загрузить ключ» - операция последовательной загрузки первичных ключей с ТМ идентификаторов в оперативную память ПЭВМ с объединением их в общесистемный ключ. Ключ будет храниться в оперативной памяти ПЭВМ либо до завершения работы программы, либо до принудительной выгрузки ключа из памяти;
- «Очистить ключ» - принудительная запись случайной последовательности на место общесистемного ключа в оперативной памяти ПЭВМ;
- «Экспортировать *.tmk файл» - запись файлов *.tmk для данной Криптосети Клиентов (по умолчанию файл размещается в папке %Program Files% \AMICON\Centre FPSU-IP\Tmk). Команда может потребоваться для повторного размещения первоначально созданных при регистрации Криптосети *.tmk-файлов в папке «Tmk» каталога установки (например, в случае их случайного удаление);
- «Выбрать базовую конфигурацию» - операция выбора для данной Криптосети Клиентов или данной группы пользователей конфигурации по умолчанию. При инициализации пользователя из данной Криптосети Клиентов или группы или при выдаче QR-кода указанная конфигурация будет предлагаться по умолчанию;
- «Выгрузить центр для АРМ УА» - операция создания списка активных пользователей из центра, который в дальнейшем можно загрузить в АРМ УА с целью автоматизации внесения информации о разрешении или запрете работы для групп клиентов в конфигурации (т.е. для пакетного изменения блокировок клиентов). Этот список представляет собой файл формата *.exc, содержащий следующие сведения:
  - общие сведения о файле экспорта (описание версия, кодировка, система);

- информация о группе пользователей (наименование, ID, тип группы (мобильная или нет), признак наличия блокировки группы);
- информация о пользователях (наименование, ID, тип пользователя (мобильный или нет), признак наличия блокировки пользователя).

Следует иметь в виду, что переименовать Криптосеть Клиентов нельзя, поскольку ее имя определяется один раз и является частью лицензии на использование.

5. 3. Интерфейс программы ЦГКК

Главное меню программы расположено вверху экрана и содержит следующие команды:

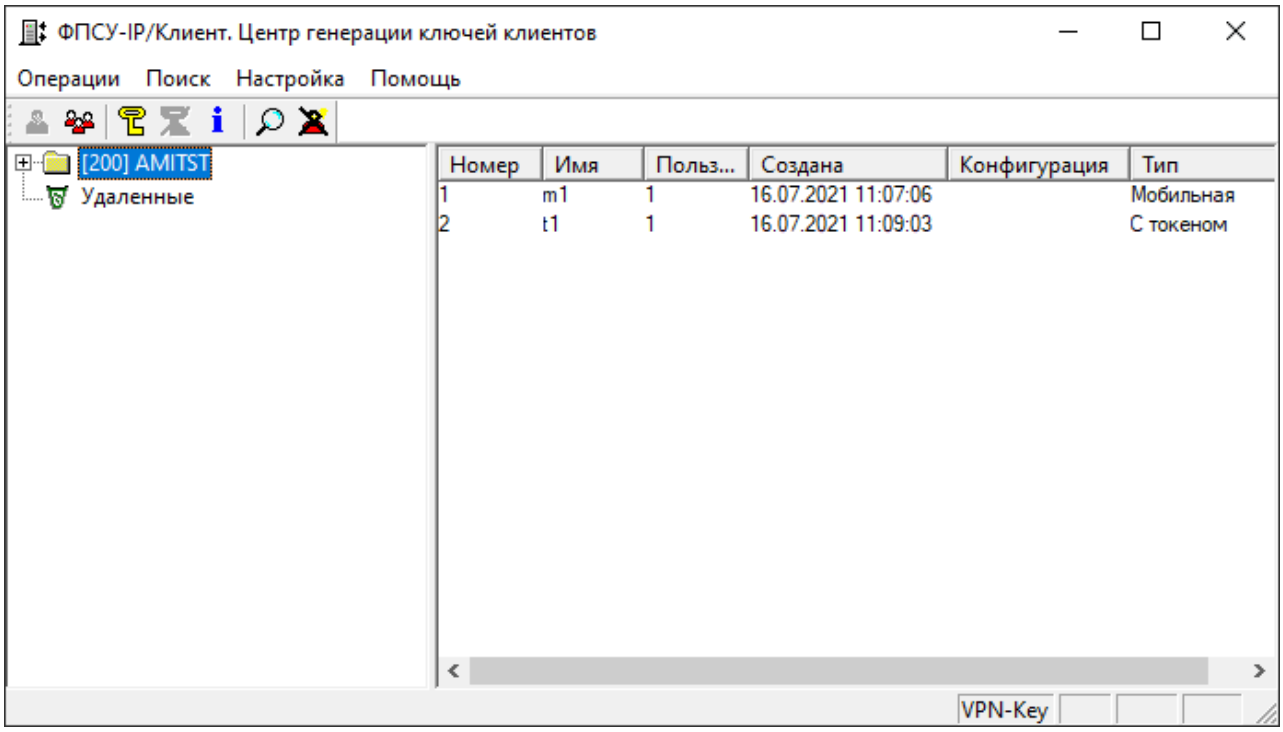

Рисунок 14 - Окно программы

- «Операции» - пункт меню, предназначенный для:
  - регистрации Криптосетей Клиентов, генерации первичных ключей,
  - доступа к контекстному меню выбранного курсором объекта в разделе «Действия»;
  - повторной инициализации ДСЧ устройства «VPN-Key»;
  - форматирования файловой системы подключенного устройства «VPN-Key». Следует учитывать, что при форматировании вся хранящаяся на устройстве информация (ключевая информация, данные о пользователях и настройки

работы с хостами и ФПСУ-IP) будет уничтожена.

- «Поиск» - пункт меню для поиска зарегистрированного пользователя Криптосети Клиентов. Поиск производится либо по символьному имени пользователя, либо по учетным данным — номеру Криптосети Клиентов, группы и пользователя.
- «Настройка» - пункт меню для установки конфигурации пользователей, то есть определения режима и параметров их работы с конкретными ФПСУ-IP. Так же в этом пункте есть настройки порядка сортировки записей пользователей в иерархическом дереве и автоматическому выводу информации о подключаемом устройстве «VPN-Key» на экран и печать при инициализации (см. ниже).
- «Помощь» - пункт меню для получения справочной информации.

Ниже строки главного меню расположена панель инструментов, сопровождаемая всплывающими подсказками о назначении своих элементов:

 - инструмент создания пользователя Криптосети Клиентов. Если операция доступна, картинка на кнопке будет цветной, в противном случае — черно-белой;

 - инструмент создания логической группы пользователей Криптосети Клиентов;

 - инструмент загрузки общесистемного ключа выбранной Криптосети Клиентов в оперативную память ПЭВМ;

 - инструмент очистки общесистемного ключа в оперативной памяти ПЭВМ;

 - инструмент получения информации о подключенном устройстве «VPN-Key». Если устройство подключено, операция будет доступна, а картинка на кнопке будет цветной, в противном случае — чёрно-белой. Следует иметь в виду, что при работе с ЦГКК в определенный момент времени может быть подключено только одно устройство VPN-Key;

 - инструмент для быстрого перехода к окну поиска пользователя;

 - инструмент включения/выключения режима отображения заблокированных пользователей.

Левая половина экрана предназначена для отображения структурного дерева Криптосетей Клиентов, обслуживаемых данной программой ЦГКК, правая — для отображения информации о группах и пользователях, отмеченных строкой выбора.

В статусную строку внизу экрана выводится краткая информация о выбранной в общем списке Криптосети Клиентов и (или) входящих в ее состав логических группах/пользователях. Кроме того, при подключении к USB-порту устройства «VPN-Key», в

статусной строке появляется соответствующая отметка, VPN-KEY.

5. 4. Настройки ЦГКК

При выборе пункта «Общие» пункта меню «Настройка» открывается окно, содержащее следующий ряд опций:

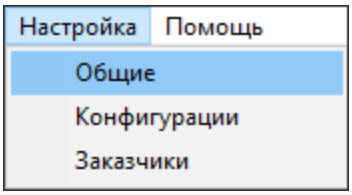

Рисунок 15 - Меню «Настройка»

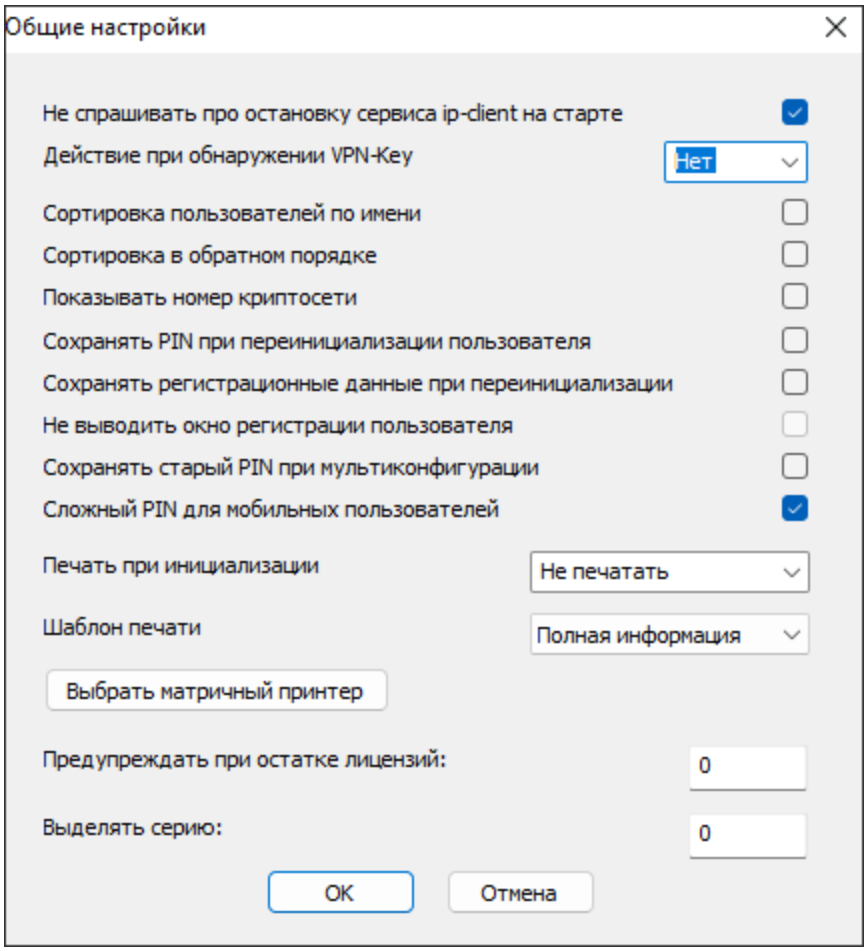

Рисунок 16 - Окно общих настроек программы ЦГКК

- «Не спрашивать про остановку сервиса ip-client на старте» — при установке этого

флага не будет выдаваться запрос на остановку сервиса ФПСУ-IP/Клиент (см. п. «Эксплуатация ЦГКК»).

- «Действие при обнаружении VPN-Key» — возможен выбор трёх вариантов работы программы после подключения к USB порту компьютера устройства «VPN-Key»:
  - «Инфо» - при выборе этого варианта во всплывающем окне будет выведена полная информация о подключенном устройстве (серийный и учетный номера устройства «VPN-Key», версии ПО устройства, инициализированные в нём пользователи с номерами Криптосетей Клиентов, групп и логических пользователей, число оставшихся попыток ввода PIN и PUK кодов);
  - «Поиск» при выборе этого варианта в основном окне программы будет выбран пользователь, который был инициализирован в подключенное устройство «VPN-Key»;
  - «Нет» - вариант по умолчанию. Если выбран, то никаких действий программа выполнять не будет.
- «Сортировка пользователей по имени/в обратном порядке» — установка порядка сортировки пользователей Криптосети внутри группы по символьному имени.
- «Показывать номер Криптосети» — при установке флага в этом поле в основном окне программы ЦГКК рядом с именем Криптосети будет отображаться и её уникальный номер.
- «Сохранять PIN при переинициализации пользователя» — установка флага в этом поле означает, что при повторной инициализации пользователя для доступа к устройству «VPN-Key» будет использоваться тот же набор PIN и PUK кодов пользователя и администратора, который использовался при первой инициализации пользователя.
- «Сохранять регистрационные данные при переинициализации» — установка флага в этом поле означает, что при повторной инициализации пользователя регистрационные данные (владелец, учетный номер устройства, организация, и т. п.) будут взяты из хранящихся в программе ЦГКК данных, оставшихся после первой инициализации данного пользователя.
- «Не выводить окно регистрации пользователя» — при установленном флаге «Сохранять регистрационные данные при переинициализации» не будет отображаться окно, позволяющее изменить регистрационные данные.
- «Сохранять старый PIN при мультиконфигурации» — при инициализации в устройство «VPN-Key» дополнительного пользователя из другой Криптосети для доступа к конфигурации дополнительного пользователя будут использоваться те же наборы PIN и PUK кодов, что и для доступа к конфигурации первого инициализированного в устройство «VPN-Key» пользователя.

- «Сложный PIN для мобильных пользователей» - установка этого флага означает, что при генерации QR-кода для работы с мобильным приложением «ФПСУ-IP/Клиент» PIN-код VPN-профиля может содержать как цифровые, так и буквенные обозначения. В настоящий момент следует формировать исключительно цифровой PIN для корректной работы ФПСУ-IP/Клиента с выданным ЦГКК профилем.
- «Печать при инициализации» — если выбрана опция «Спрашивать», то после генерации ключевой информации будет выдаваться системное окно: «Печатать PIN-конверт?». По нажатию кнопки «Да» сведения о пользователе (в зависимости от опции, выбранной в шаблоне печати (см. ниже) будут сохранены в файл формата *.pdf. При выборе опции «После инит. ФПСУ» или «После инит. КА» информация о пользователе будет направляться на печать в момент загрузки общесистемного ключа.
- «Шаблон печати» — выпадающий список выбора печати по умолчанию. В нем производится выбор того, какие сведения будут выводиться на печать: полная информацию о пользователе, PIN-конверт (имя пользователя, отметка инициализации, серийный номер, учетный номер, PIN и PUK коды).
- Предупреждать при остатке лицензий — при включении этой опции программа будет выдавать администратору предупреждающее служебное сообщение, если количество лицензий на инициализацию пользователей станет меньше указанного в этом окне.
- Выделять серию — у пользователей, которые были инициализированы с указанной серией ключа, иконки в окне списка программы будут отмечены синим цветом, вместо обычного красного. Если указана серия 0 (ноль), механизм пометки иконки пользователя разными цветами отключен.

Пункт «Заказчики» меню «Настройка» позволяет сформировать список заказчиков (организаций, частных лиц, например), из которого будет предложено выбрать при инициализации пользователя в устройство «VPN-Key» (см. пункт «Создание пользователя»).

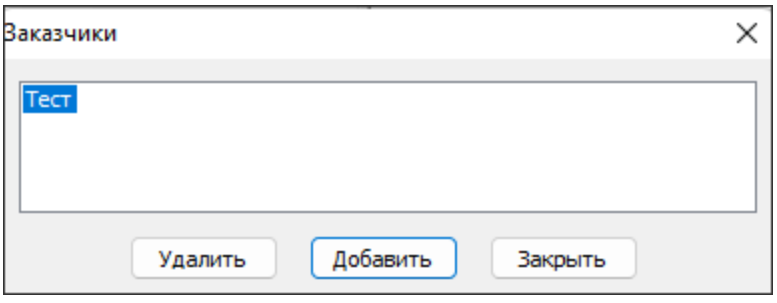

Рисунок 17 - Формирование списка заказчиков

5. 5. Настройка шаблона конфигурации VPN-профилей

Администратор программы ЦГКК может заранее создать шаблоны конфигураций для пользователей зарегистрированных Криптосетей Клиентов. Шаблоны могут быть выбраны для записи в устройство «VPN-Key» при инициализации пользователя или в файл как в двоичном виде, так и в формате графического файла, и служат для упрощения процесса создания большого числа пользователей с одинаковыми конфигурациями подключения к ФПСУ-IP.

Выбор пункта основного меню «Настройка → Конфигурации» выводит на экран окно со списком конфигураций.

В окне списка конфигураций следует создать шаблон конфигурации (см. пункт «Создание шаблона конфигурации VPN-профиля»). Окно со списком конфигураций содержит следующие командные кнопки:

- Выбрать - команда для записи текущей конфигурации в подключенное в данный момент устройство «VPN-Key» или в файл с ключевыми сведениями;
- Изменить - команда для изменения текущей конфигурации списка;
- Создать - команда для создания нового пустого описателя типовой конфигурации;
- Удалить - команда для удаления текущей конфигурации;
- Закрыть - команда для выхода из режима настройки без установки параметров.

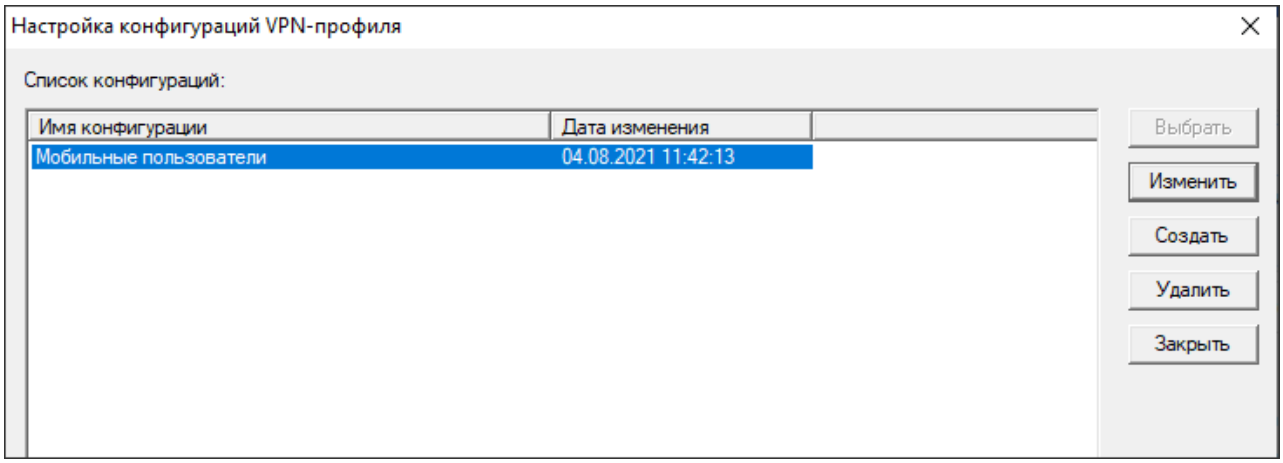

Рисунок 18 - Выбор конфигурации

При настройке шаблона созданной конфигурации открывается окно установки параметров конфигурации.

Окно параметров имеет несколько вкладок для формирования настроек:

- Вкладка «ФПСУ» предназначена для настройки подключения к ФПСУ-IP.

- Вкладка «Хосты» предназначена для настройки рабочих станций через ФПСУ-IP.
- Вкладка «Блокировки» предназначена для настройки блокировок пакетов при установленном VPN-туннеле с ФПСУ-IP.

Если для текущей Криптосети Клиентов или группы была установлена конфигурация по умолчанию, то будет предложено установить выбранную базовую конфигурацию.

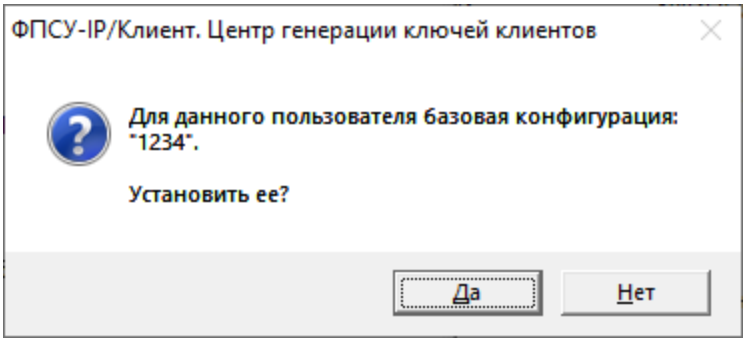

Рисунок 19 - Сообщение о наличии базовой конфигурации

В противном случае при выдаче ключей в файл или при инициализации пользователя на экране появляется окно настройки, содержащее список шаблонных конфигураций, описанных администратором ЦГКК заранее, посредством выбора пункта «Конфигурации» меню «Настройка».

5. 5. 1. Создание шаблона конфигурации VPN-профиля

Установка параметров взаимодействия ФПСУ-IP/Клиентов с ФПСУ-IP (конфигурирование) может производиться как администратором ЦГКК, так и самими пользователями ФПСУ-IP/Клиентов. Пользователи ФПСУ-IP/Клиент, имеющие права администратора, могут также изменять рабочие установки, предварительно сделанные администратором ЦГКК (см. «Руководство пользователя ФПСУ-IP/Клиента»).

Для создания шаблона конфигурации VPN-профиля выбрать пункт меню «Настройка → Конфигурации».

В открывшемся окне нажать кнопку «Создать» и ввести название конфигурации.

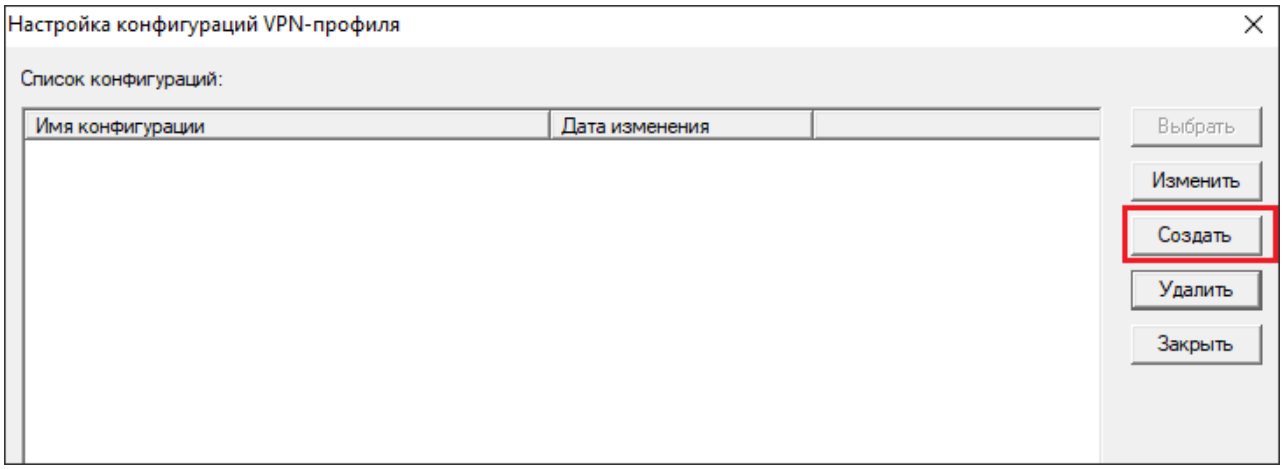

Рисунок 20 - Окно со списком конфигураций

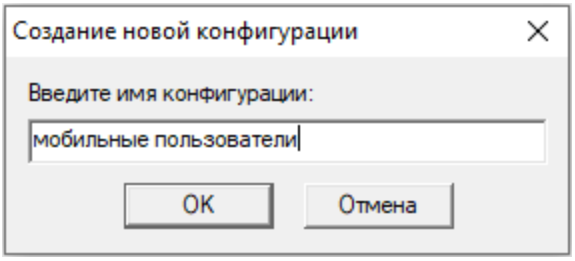

Рисунок 21 - Сохранение конфигурации

По нажатию кнопки «ОК» название шаблона конфигурации сохраняется в список конфигураций.

5. 5. 2. Настройка подключения к ФПСУ-IP

Для изменения шаблона конфигурации VPN-профиля выбрать пункт меню «Настройка → Конфигурации».

В открывшемся окне списка конфигураций выбрать конфигурацию и нажать кнопку «Изменить».

Откроется окно установки параметров конфигурации. Настройка подключения к ФПСУ-IP осуществляется на вкладке «ФПСУ».

В поле «IP-адрес» следует ввести IP-адрес ближайшего порта ФПСУ-IP, через который будет осуществляться доступ ФПСУ-IP/Клиента к запрашиваемым абонентам.

Если в сети имеется ещё один ФПСУ-IP, который может предоставить доступ ФПСУ-IP/Клиенту в случае отсутствия связи с основным ФПСУ-IP, выставьте флажок в поле

«Дополнительный» и укажите его IP-адрес в окне справа.

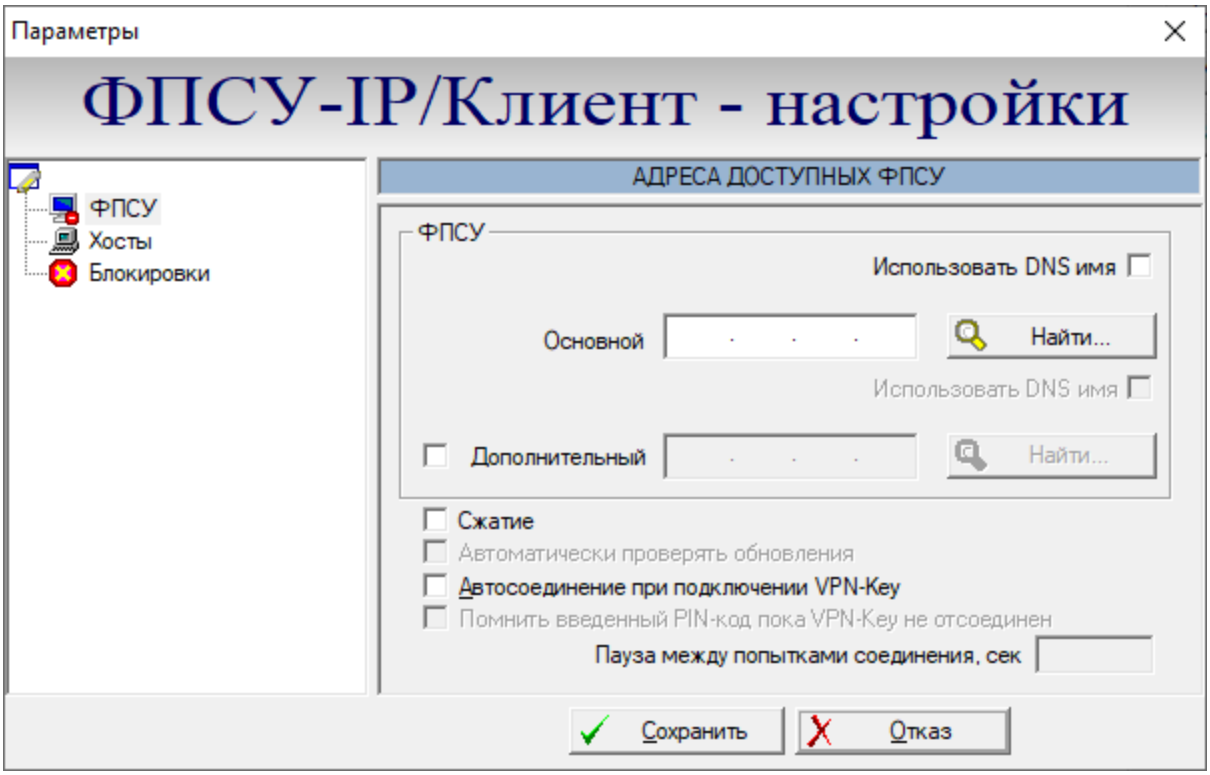

Рисунок 22 - Вкладка ФПСУ

Если канал связи с ФПСУ-IP обеспечивает скорости передачи данных не выше 5 Мбит/с, рекомендуется указать на необходимость сжатия данных перед передачей их в VPN-туннель (выставить флаг «Сжатие данных»). Для более высоких скоростей соединения эта опция неэффективна.

При установленном флаге «Автосоединение при подключении VPN-Key» в момент подключения устройства «VPN-Key» в USB-порт ФПСУ-IP/Клиент автоматически будет пытаться идентифицировать пользователя и соединиться с ФПСУ-IP.

5. 5. 3. Доступные через ФПСУ-IP рабочие станции

Для изменения шаблона конфигурации VPN-профиля выбрать пункт меню «Настройка → Конфигурации».

В открывшемся окне списка конфигураций выбрать конфигурацию и нажать кнопку «Изменить».

Откроется окно установки параметров конфигурации. Настройка рабочих станций

осуществляется на вкладке «Хосты».

В поле «IP-адреса хостов» необходимо указать IP-адреса доступных через ФПСУ-IP хостов. IP-пакеты, отправляемые рабочей станцией ФПСУ-IP/Клиента в адрес указанных IP-адресов, будут зашифровываться и направляться на ФПСУ-IP.

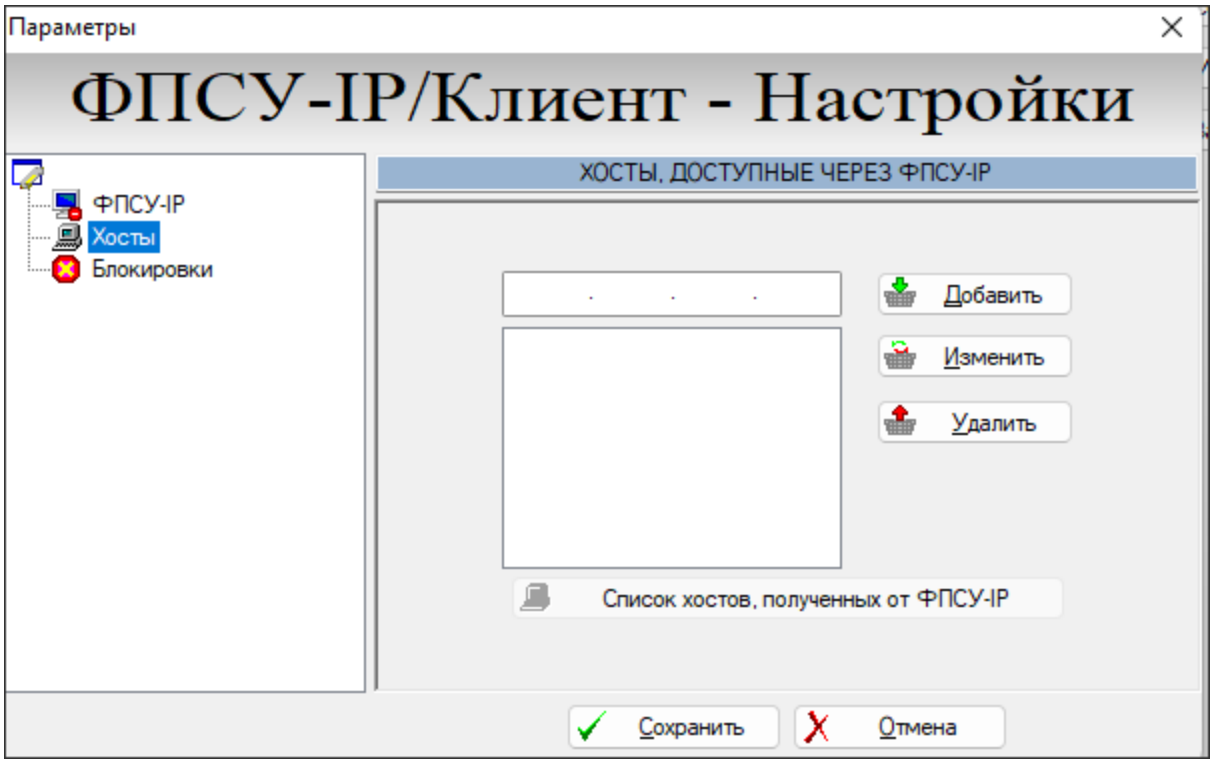

Рисунок 23 - Список хостов

Нажатие кнопки «Добавить» включает находящийся в поле ввода IP-адрес в список хостов. С помощью кнопки «Изменить» можно изменить IP-адрес имеющийся в конфигурации хоста.

5. 5. 4. Настройка блокировок пакетов при установленном VPN-туннеле с ФПСУ-IP

Для изменения шаблона конфигурации VPN-профиля выбрать пункт меню «Настройка → Конфигурации».

В открывшемся окне списка конфигураций выбрать конфигурацию и нажать кнопку «Изменить».

Откроется окно установки параметров конфигурации. Настройка блокировок осуществляется на вкладке «Блокировки».

В данной вкладке можно установить правила фильтрации входящих и исходящих пакетов данных. Блокировки будут активны на время взаимодействия ФПСУ-IP/Клиента и ФПСУ-IP.

Примечание. Блокировки не могут быть установлены для ФПСУ-IP/Клиента под управлением операционных систем Android и iOS.

В группе переключателей следует установить флаги для тех соединений, которые будут запрещены во время сеансов с ФПСУ-IP. Ограничения на приём и передачу пакетов могут быть установлены как для сетевого адаптера, связанного с ФПСУ-IP, так и для других сетевых адаптеров АРМ пользователя ФПСУ-IP/Клиента.

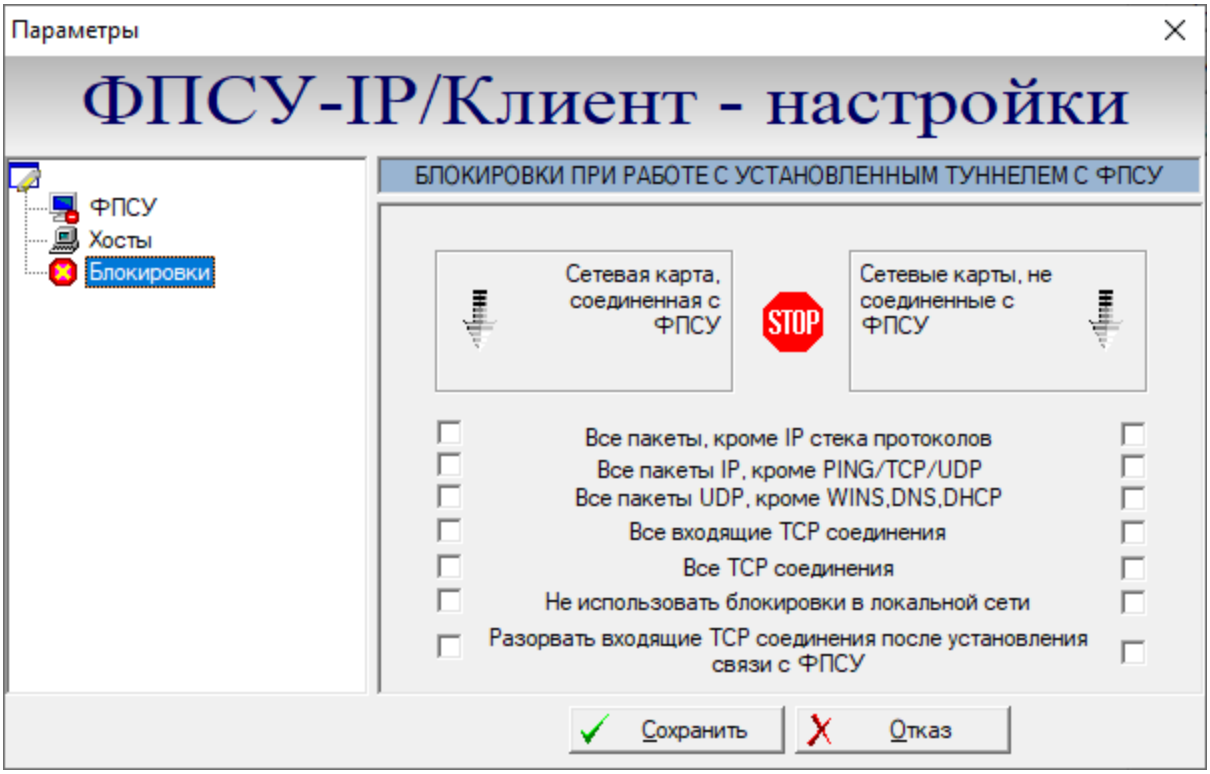

Рисунок 24 - Блокировки

Во время установки VPN-туннеля с ФПСУ-IP правила фильтрации, возможно, будут принудительно дополнены в соответствии с указаниями администратора ФПСУ-IP. Эти правила имеют приоритет выше, чем настройки устройства «VPN-Key».

Произведенные установки необходимо сохранить путем нажатия на одноименную кнопку.

5. 6. Генерация общесистемных ключей

После регистрации Криптосети в программе ЦГКК, требуется сгенерировать и записать серию общесистемного ключа этой Криптосети на ТМ-носители или в двоичный файл, опционально – в распределенном на разные ТМ-носители или файлы виде.

5. 6. 1. Генерация и запись на ТМ-носитель общесистемных ключей

Находящиеся на ТМ-идентификаторах и в файлах формата *.tm части общесистемного ключа называются первичными ключами.

С помощью общесистемного ключа для каждого ФПСУ-IP/Клиента вырабатываются пользовательские ключевые данные, которые записываются в устройство «VPN-Key» или в бинарный файл.

Окно генерации серии общесистемного ключа, распределенного в виде набора первичных ключей, запускается выбором пункта «Генерация первичных ключей» меню «Операции».

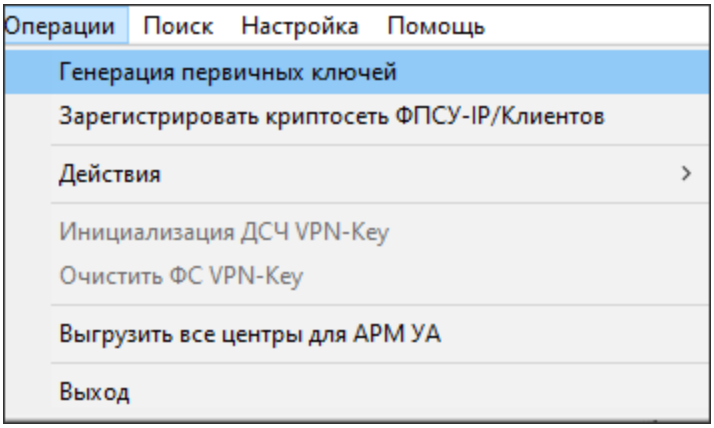

Рисунок 25 - Запуск генерации первичных ключей

В появившемся окне для генерации первичных ключей требуется:

1. Нажать кнопку «Загрузить данные о ключевой ТМ» и указать местонахождение данных о Криптосети Клиентов, для которой генерируются первичные ключи (файла формата *.tmk, сформированного при регистрации Криптосети - см. пункт «Регистрация Криптосетей Клиентов»).

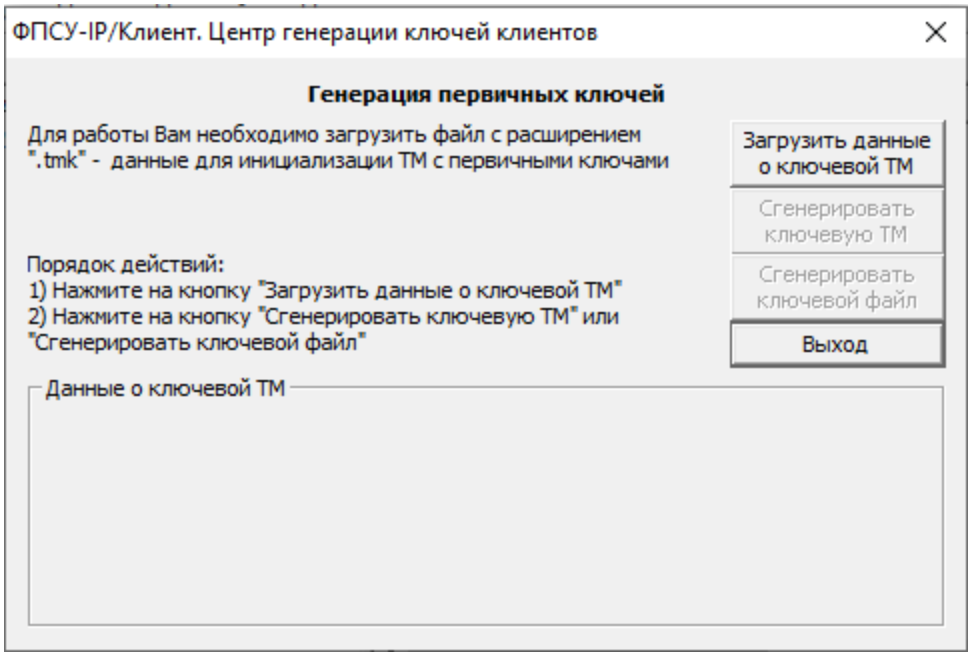

Рисунок 26 - Генерация первичных ключей

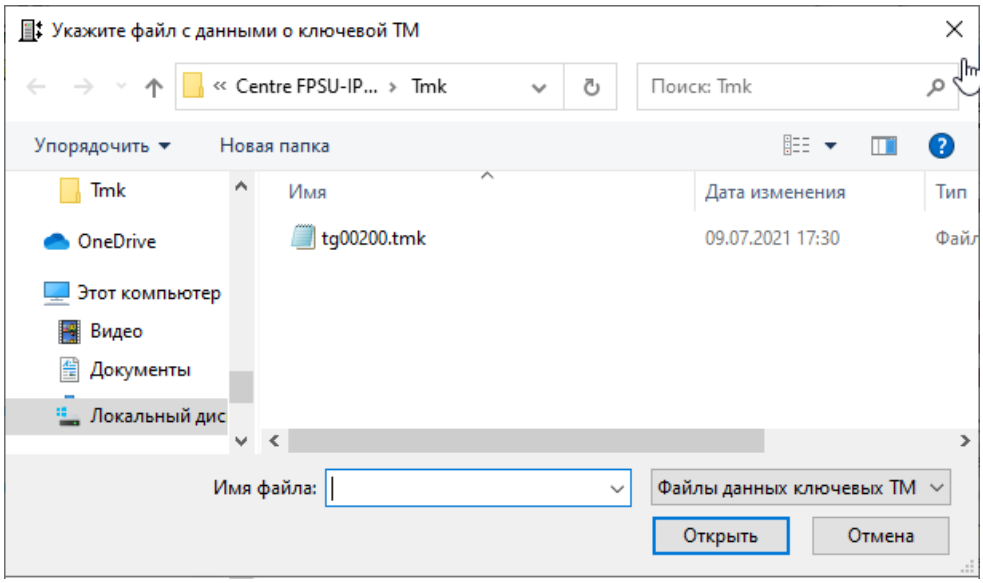

Рисунок 27 - Выбор файла формата *.tmk

2. После указания местоположения файла формата *.tmk, становятся активными кнопки «Сгенерировать ключевую ТМ» и «Сгенерировать ключевой файл», отвечающие за продолжение процесса генерации ключей и записи их на ТМ-идентификаторы или в двоичные файлы соответственно.

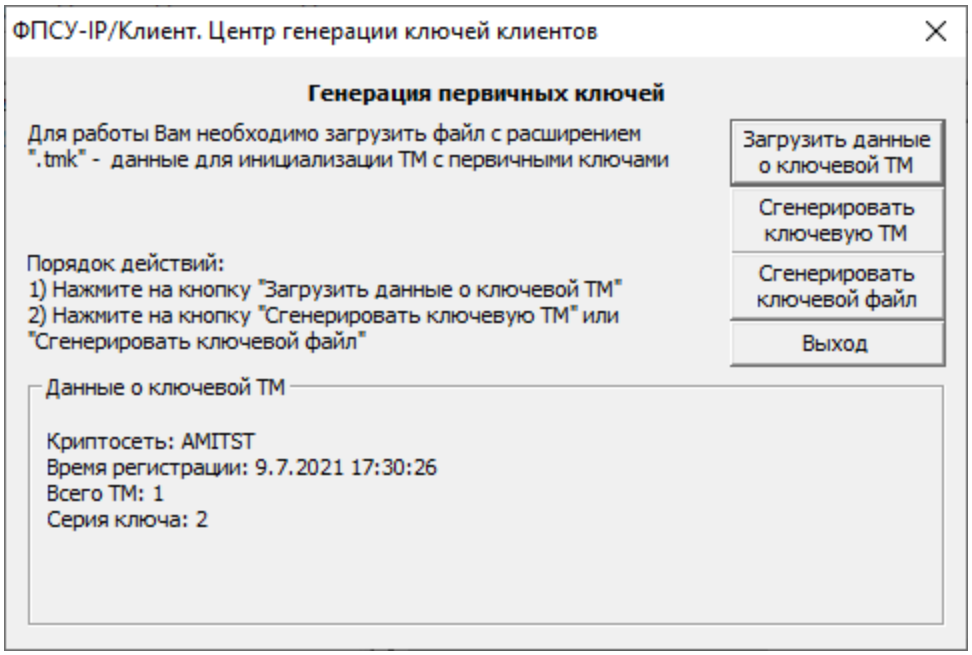

Рисунок 28 - Генерация первичных ключей

3. Нажать на кнопку «Сгенерировать ключевую ТМ». По нажатию кнопки «Да» ключ записывается в файл с признаком поддержки алгоритмов шифрования в соответствии с ГОСТ 34.12–2015 (блочный шифр «Магма»), по нажатию кнопки «Нет» - с признаком поддержки алгоритмов шифрования в соответствии с ГОСТ 28147-89.

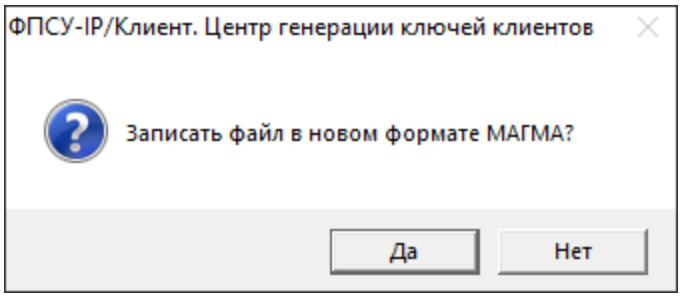

Рисунок 29 - Выбор криптографического протокола

4. В появившемся окне необходимо указать номер серии генерируемых ключевых данных и нажать «ОК». По умолчанию предлагается номер серии, следующий за номером последней созданной серии, начиная с 2.

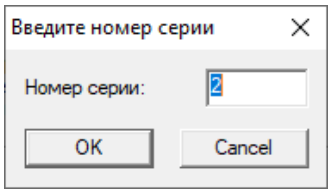

Рисунок 30 - Ввод номера серии

5. Произойдет вызов датчика случайных чисел, в котором требуется сформировать случайное число путем перемещения указателя мыши в пределах окна.

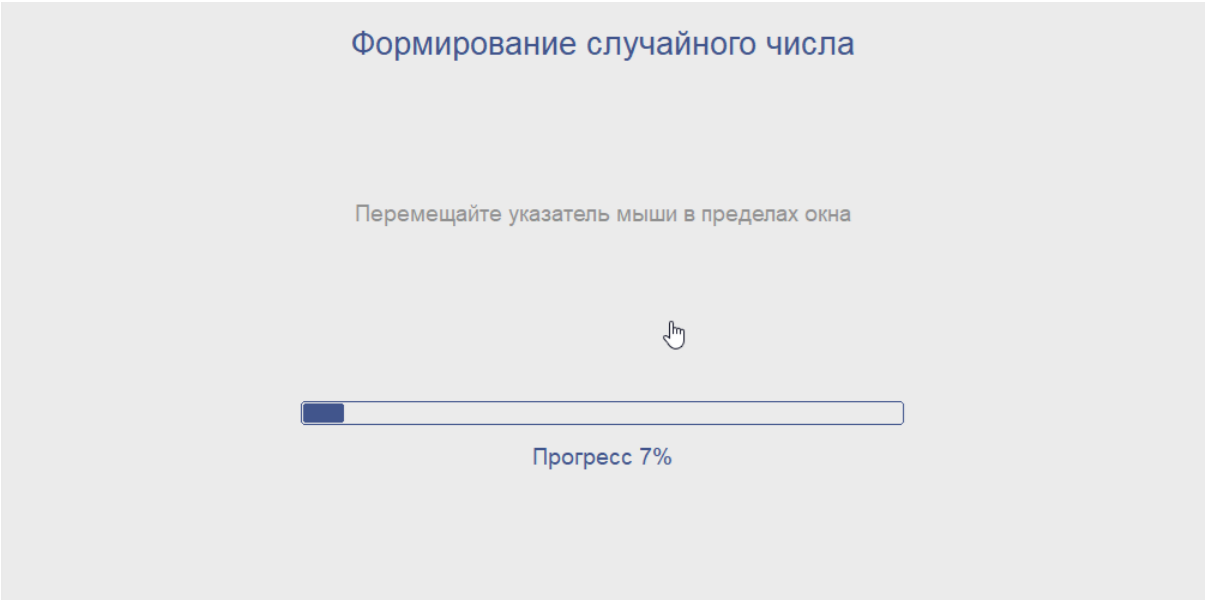

Рисунок 31 - Формирование случайного числа

6. После инициализации датчика случайных чисел в случае формирования ключевых ТМ-носителей программа предложит начать запись первичных ключей в ТМ-идентификатор, предлагая прислонить к ТМ-считывателю или подключить к USB-порту носители в указанном порядке. Критерием успешности записи первичного ключа на ТМ является служебное оповещение «Ключевая ТМ № *XX* записана успешно».

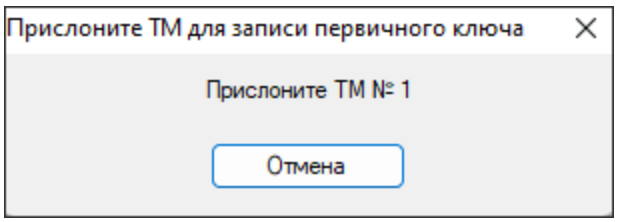

Рисунок 32 - Предложение прислонить ТМ №1

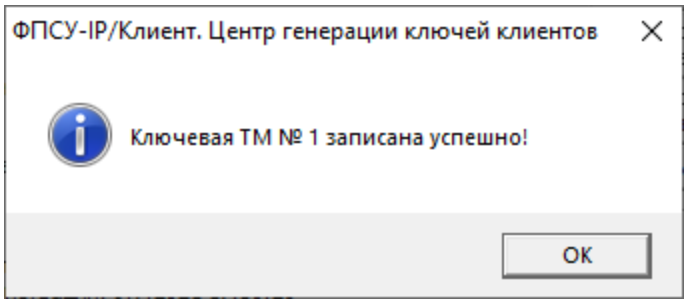

Рисунок 33 - Сообщение об успешной записи ключевой ТМ

7. Повторить п. 6 для каждого первичного ключа (см. пункт «Регистрация Криптосетей Клиентов»). Не следует допускать записи на один ТМ-идентификатор более одного первичного ключа. Когда все первичные ключи будут записаны, программа выдаст служебное оповещение о завершении процедуры генерации и записи первичных ключей.

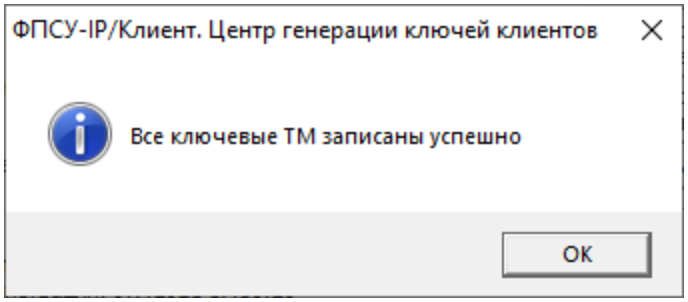

Рисунок 34 - Завершение генерации и записи первичных ключей

Записанные на ТМ-идентификаторы первичные ключи потребуются, когда возникнет необходимость инициализировать пользователя этой Криптосети Клиентов.

5. 6. 2. Генерация и запись общесистемных ключей в виде файла

Находящиеся в файлах формата *.tm части общесистемного ключа также называются первичными ключами.

С помощью общесистемного ключа для каждого ФПСУ-IP/Клиента вырабаты-ваются пользовательские ключевые данные, которые записываются в устройство «VPN-Key» или в бинарный файл.

Окно генерации серии общесистемного ключа, распределенного в виде набора первичных ключей, запускается выбором пункта «Генерация первичных ключей» меню «Операции».

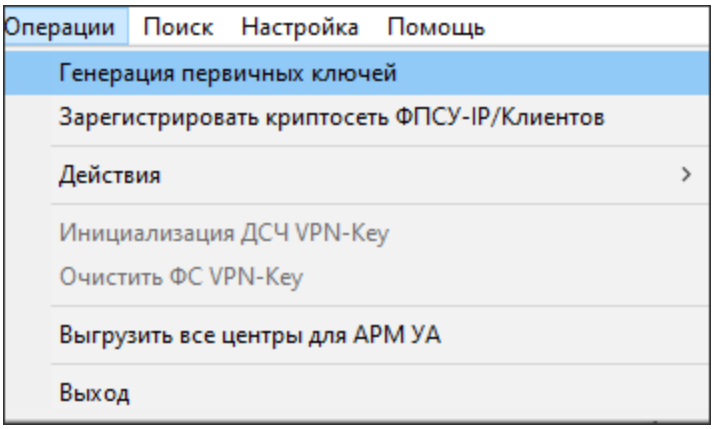

Рисунок 35 - Запуск генерации первичных ключей

В появившемся окне для генерации первичных ключей требуется:

1. Нажать кнопку «Загрузить данные о ключевой ТМ» и указать местонахождение данных о Криптосети Клиентов, для которой генерируются первичные ключи (файла формата *.tmk, сформированного при регистрации Криптосети - см. пункт «Регистрация Криптосетей Клиентов»).

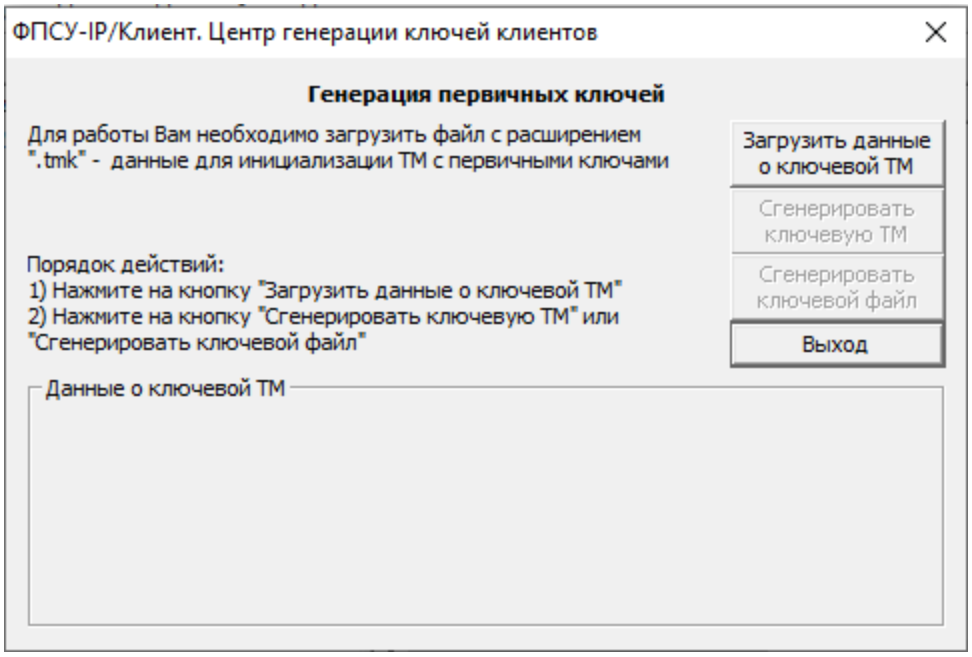

Рисунок 36 - Генерация первичных ключей

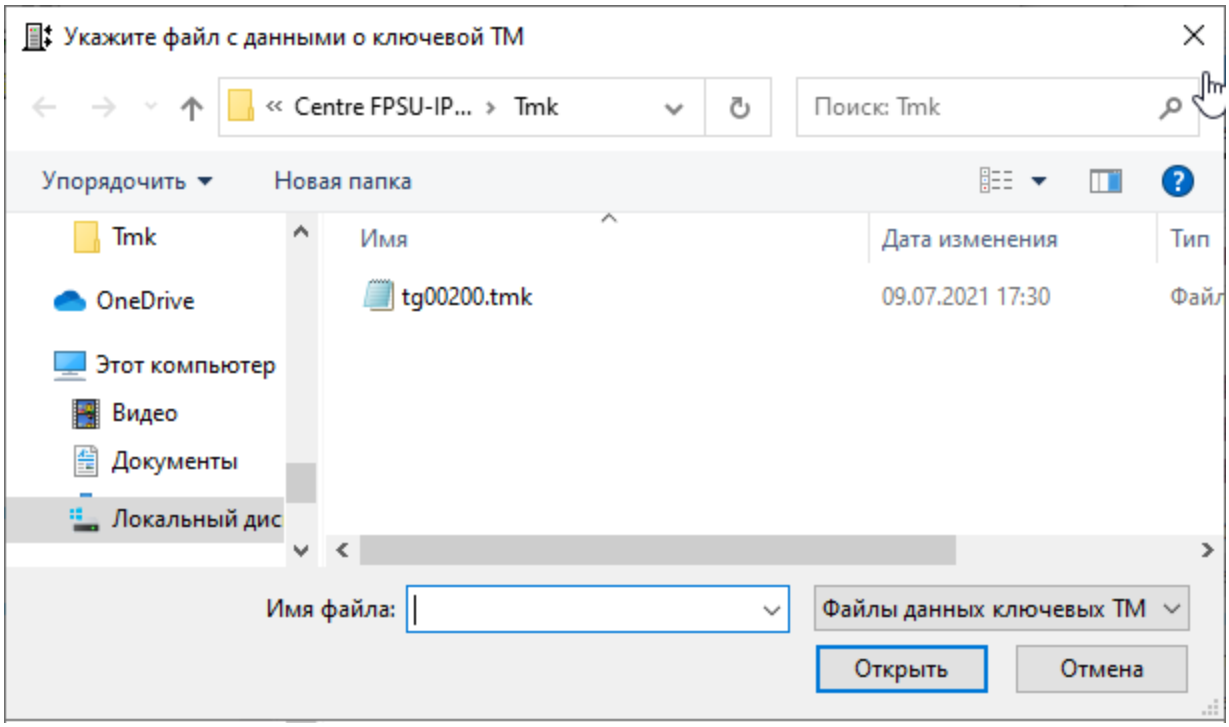

Рисунок 37 - Выбор файла формата *.tmk

2. После указания местоположения файла формата *.tmk, становятся активными кнопки «Сгенерировать ключевую ТМ» и «Сгенерировать ключевой файл», отвечающие за продолжение процесса генерации ключей и записи их на ТМ-носители или в двоичные файлы соответственно.

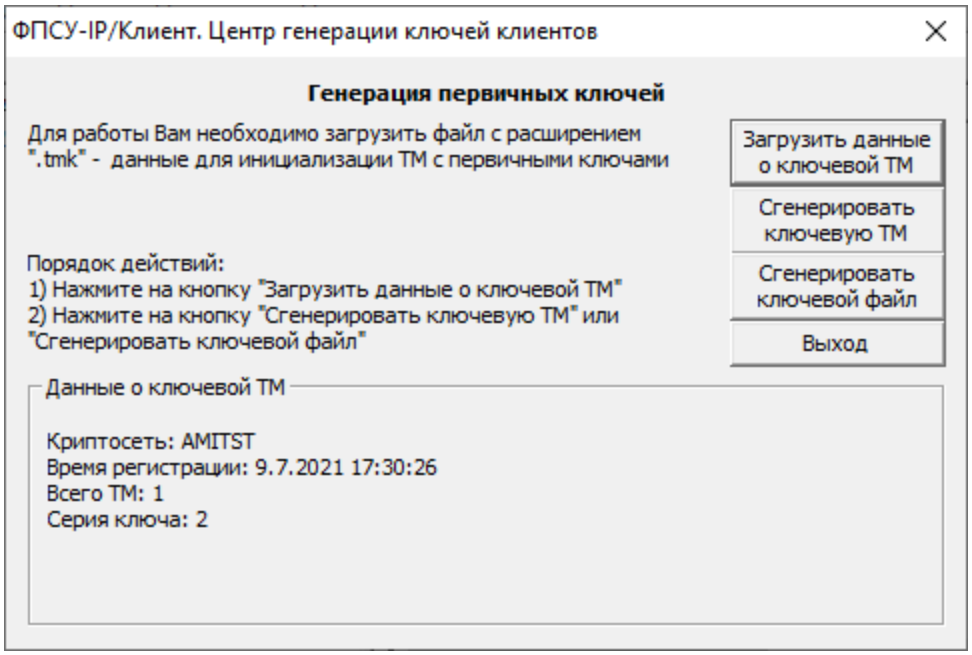

Рисунок 38 - Генерация первичных ключей

3. Нажать на кнопку «Сгенерировать ключевую ТМ». По нажатию кнопки «Да» ключ записывается в файл с признаком поддержки алгоритмов шифрования в соответствии с ГОСТ 34.12–2015 (блочный шифр «Магма»), по нажатию кнопки «Нет» - с признаком поддержки алгоритмов шифрования в соответ-ствии с ГОСТ 28147-89.

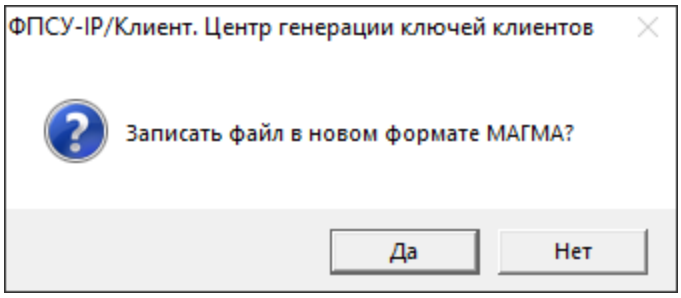

Рисунок 39 - Выбор криптографического протокола

4. В появившемся окне указать номер серии генерируемых ключевых данных и нажать «ОК». По умолчанию предлагается номер серии, следующий за номером последней созданной серии, начиная с 2.

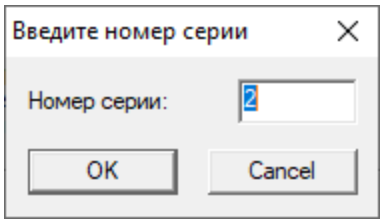

Рисунок 40 - Ввод номера серии

5. Выбрать место хранения файлов с ключевой информацией. Рекомендуется выбирать в качестве места хранения отчуждаемый носитель. В случае хранения ключевой информации в файловой системе ПЭВМ, внутренний носитель данных ПЭВМ становится ключевым носителем (подробнее требования к ключевым носителям см. документ «Правила пользования» на СКЗИ).
6. Произойдет вызов датчика случайных чисел, в котором требуется сформировать случайное число путем перемещения указателя мыши в пределах окна.

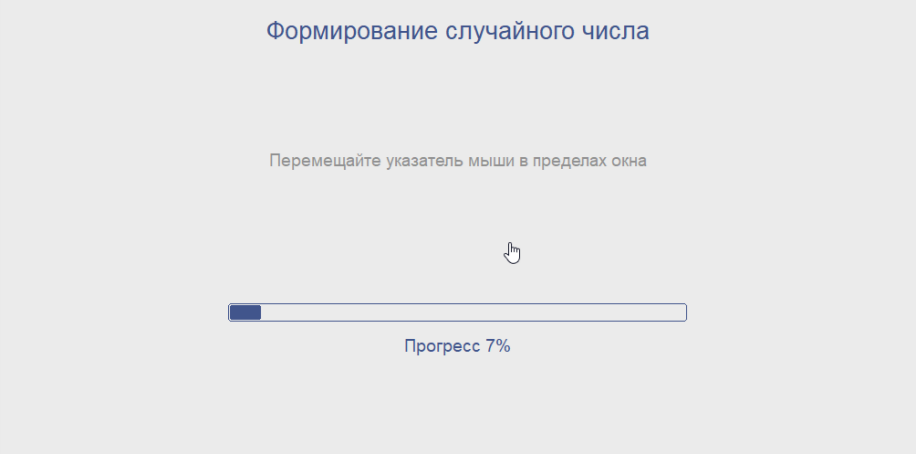

Рисунок 41 - Формирование случайного числа

7. После инициализации датчика случайных чисел на экран будет выведено сообщение об успешно записанном ключевом файле.

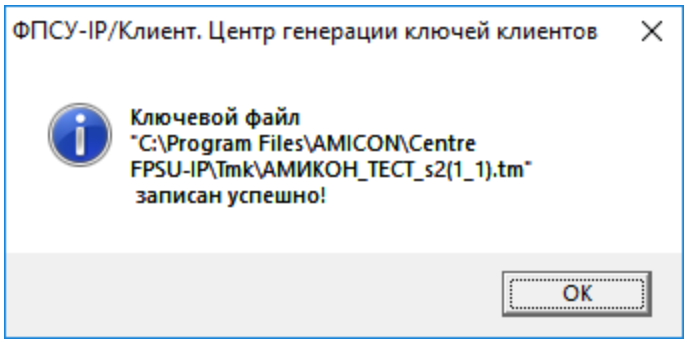

Рисунок 42 - Сообщение об успешной записи ключевого файла

8. Повторить п. 5 для каждого первичного ключа (см. пункт «Регистрация Криптосетей Клиентов»). Когда все первичные ключи будут записаны, программа выдаст служебное оповещение о завершении процедуры генерации и записи первичных ключей.

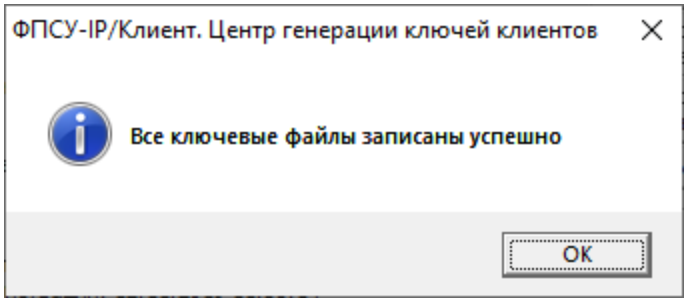

Рисунок 43 - Сообщение об успешной записи всех ключевых файлов

Записанные в двоичные файлы первичные ключи потребуются, когда возникнет необходимость инициализировать пользователя этой Криптосети Клиентов или выдать QR-код.

5. 6. 3. Смена общесистемных ключей

Срок действия серии общесистемного ключа Криптосети отсчитывается с момента генерации и не должен превышать 15 месяцев. До истечения срока действия текущего общесистемного ключа требуется повторно сгенерировать и установить новый общесистемный ключ на местах использования СКЗИ.

Для смены серии общесистемного ключа Криптосети Клиентов на ЦГКК необходимо заново сгенерировать первичные ключи, которые записываются в виде файла формата *.tm. Ключевая информация может быть опционально распределена в несколько файлов. Генерация и запись общесистемных ключей описана в пунктах «Генерация и запись на ТМ-носитель общесистемных ключей» и «Генерация и запись общесистемных ключей в виде

файла».

При смене серии общесистемного ключа Криптосети требуется сменить ключевую информацию каждого VPN-профиля. На ЦГКК генерируются ключи и выдаются в виде QR-кода или в виде файла формата *.bin (см. пункт «Выдача ключей для смены ключевой информации VPN-профиля»).

На программном Клиенте или в мобильном приложении «ФПСУ-IP/Клиент» могут быть установлены две серии общесистемных ключей одновременно на период перехода с текущей (младшей) серии на новую (старшую).

На программном Клиенте или в мобильном приложении «ФПСУ-IP/Клиент» необходимо сменить ключи каждого VPN-профиля на новые, выданные ЦГКК. После того как, все ключи заменены на новые со старшей серией общесистемного ключа, младшая серия общесистемного ключа может быть удалена с ЦГКК.

5. 7. Создание групп пользователей

Для удобства обслуживания и настройки политик доступа, все пользователи Криптосети Клиентов подразделяются на логические группы. Логические группы могут объединять пользователей по территориальному или функциональному признакам, а также по режиму доступа к информации при работе через ФПСУ-IP.

В Криптосети Клиентов должна быть создана по крайней мере одна логическая группа.

В каждой группе может быть создано до 1024 пользователей, однако общее число пользователей всех групп не может превышать максимальное количество, указанное в лицензии на использование данной Криптосети Клиентов.

Следует обратить внимание на то, что при создании логической структуры пользователей ЦГКК необходимо учитывать специфику обслуживания ФПСУ-IP/Клиентов программно-аппаратными комплексами ФПСУ-IP.

Каждый из ФПСУ-IP, через которые будут работать ФПСУ-IP/Клиенты, может обслуживать ограниченное количество групп (от одной или разных Криптосетей), причём число ФПСУ-IP/Клиентов от каждой группы также ограничивается (в настоящий момент через один ФПСУ-IP могут работать не более 1024 ФПСУ-IP/Клиентов в группе от не более чем 128 логических групп).

Таким образом, при организации логических групп (а также отдельных пользователей) администратор ЦГКК должен согласовывать свои действия с

администраторами тех ФПСУ-IP, через которые будут работать пользователи данной Криптосети.

Для того, чтобы создать логическую группу необходимо:

1. Выбрать Криптосеть в левой половине рабочего окна;
2. Выбрать подпункт «Создать группу» пункта «Действия» меню «Операции», либо аналогичный пункт контекстного меню Криптосети, либо воспользоваться соответствующей кнопкой на панели инструментов ЦГКК;

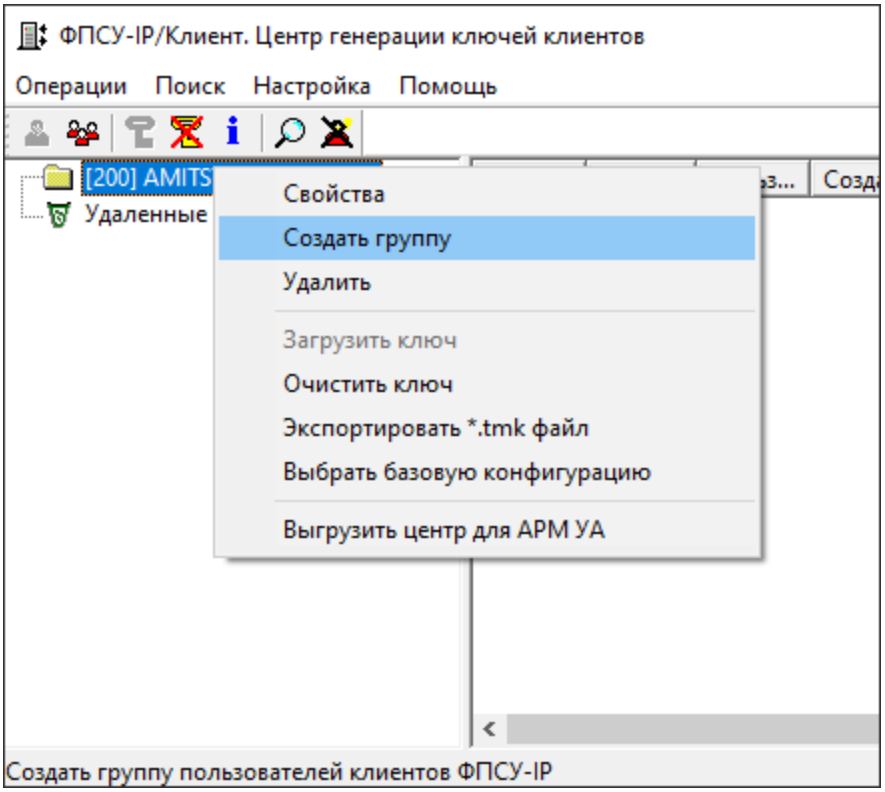

Рисунок 44 - Контекстное меню Криптосети

3. Установить переключатель в положение «с USB-токеном» для создания группы пользователей, работающих с ФПСУ-IP/Клиентом с применением устройства «VPN-Key», или «Мобильная (без USB-токена)» для создания группы пользователей, работающих без использования устройства «VPN-Key».
4. В открывшемся окне ввести номер и имя создаваемой группы.

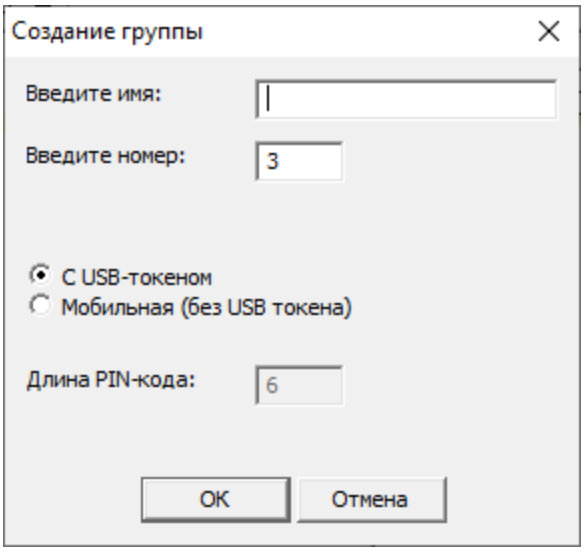

Рисунок 45 - Создание группы

После создания группы её имя появится в списке групп выбранной Криптосети.

Контекстное меню группы пользователей, работающих с ФПСУ-IP/Клиентом с применением устройства «VPN-Key», содержит следующие пункты:

- Свойства - информация о группе Криптосети включает в себя:
  - номер и имя группы;
  - состояние;
  - базовую конфигурацию.

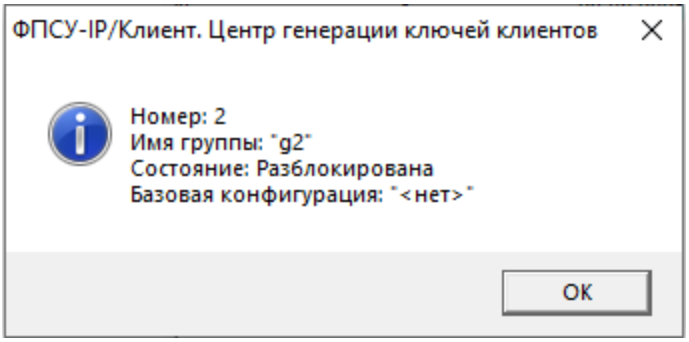

Рисунок 46 - Информация о группе Криптосети

- Создать пользователя - команда для создания нового пользователя в данной группе (см. пункт «Создание пользователя»).
- Переименовать - команда для изменения имени группы.
- Удалить - команда для удаления группы из Криптосети Клиентов. Доступно удаление только пустой группы.

- Установить базовую конфигурацию - команда для установки базовой конфигурации на данную группу (аналогично установке базовой конфигурации на Криптосеть Клиентов). При установке базовой конфигурации на Криптосеть Клиентов и на группу, при инициализации пользователя или выдаче QR-кода будет предложена базовая конфигурация группы.
- Заблокировать/Разблокировать команда блокировки и разблокировки группы.

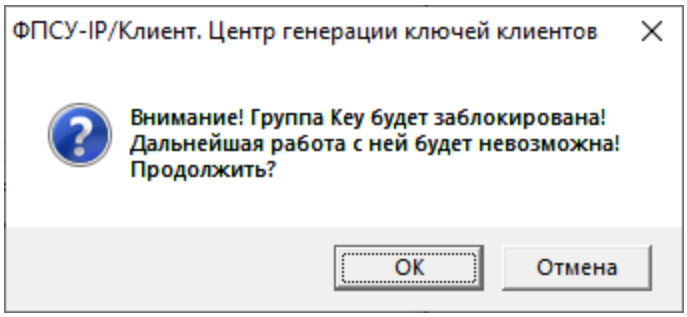

Рисунок 47 - Предупреждение о последствиях блокировки

- Изменить длину PIN-кода - по умолчанию длина PIN-кода для пользователей программно-аппаратных Клиентов составляет 6 цифр, что является минимальным значением. При необходимости длина PIN-кода может быть увеличена до 31 цифры.
- Изменить количество комплектов для смены ключей - команда для изменения количества бинарных файлов для распределения в них ключевой информации для изменения ключей, производимого раз в год.
- Выбрать базовую конфигурацию - команда для установки базовой конфигурации на данную группу (аналогично установке базовой конфигурации на Криптосеть Клиентов). При установке базовой конфигурации на Криптосеть Клиентов и на группу, при инициализации пользователя или выдаче QR-кода будет предложено воспользоваться настройками базовой конфигурации группы.
- Инициализировать пользователей - команда для последовательной инициализации всех пользователей данной группы (см. пункт «Инициализация VPN-профиля пользователя в VPN-Key»).
- Выгрузить группу для АРМ УА - операция создания списка активных пользователей из группы, который в дальнейшем можно загрузить в АРМ УА с целью автоматизации внесения информации о разрешении или запрете работы для ФПСУ-IP/Клиентов в конфигурации. Этот список представляет собой файл формата *.exc, содержащий следующие сведения:
  - общие сведения о файле экспорта (описание версия, кодировка, система);
  - информация о группе (наименование, ID, тип группы (не мобильная), признак наличия блокировки группы);

- информация о пользователях группы (наименование, ID, тип пользователя (не мобильный), признак наличия блокировки пользователя).

Контекстное меню группы пользователей, работающих с ФПСУ-IP/Клиентом без применения устройства «VPN-Key», содержит следующие пункты:

- Свойства - информация о группе Криптосети включает в себя:
  - номер и имя группы;
  - состояние;
  - базовую конфигурацию;
  - тип группы;
  - длину PIN кода и PIN кода для смены ключей.

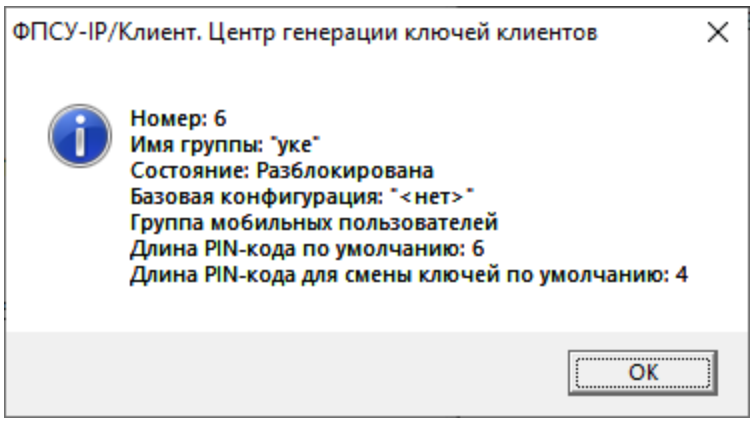

Рисунок 48 - Информация о группе Криптосети

- Создать пользователя - команда для создания нового пользователя в данной группе.
- Переименовать - команда для изменения имени группы.
- Удалить - команда для удаления группы из Криптосети Клиентов. Доступно удаление только пустой группы.
- Заблокировать/Разблокировать - команда блокировки и разблокировки группы.
- Изменить длину PIN-кода - по умолчанию длина PIN-кода для пользователей программных Клиентов составляет 6 цифр, что является минимальным значением. При необходимости длина PIN-кода может быть увеличена до 31 цифры.
- Изменить длину PIN-кода для смены ключей - по умолчанию PIN-код для изменения ключей, производимого раз в год, состоит из 4 цифр, что является минимальным значением. При необходимости длина PIN-кода может быть увеличена до 31 цифры.
- Изменить количество комплектов для смены ключей - команда для изменения количества бинарных файлов для распределения в них ключевой информации для изменения ключей, производимого раз в год.

- Выбрать базовую конфигурацию - команда для установки базовой конфигурации на данную группу (аналогично установке базовой конфигурации на Криптосеть Клиентов). При установке базовой конфигурации на Криптосеть Клиентов и на группу, при инициализации пользователя или выдаче QR-кода будет предложено воспользоваться настройками базовой конфигурации группы.
- Инициализировать пользователей - команда для инициализации пользователей группы с USB-токеном.
- Выгрузить группу для АРМ УА - операция создания списка активных пользователей из группы, который в дальнейшем можно загрузить в АРМ УА с целью автоматизации внесения информации о разрешении или запрете работы для ФПСУ-IP/Клиентов в конфигурации. Этот список представляет собой файл формата *.exc, содержащий следующие сведения:
  - общие сведения о файле экспорта (описание версия, кодировка, система);
  - информация о группе (наименование, ID, тип группы (мобильная), признак наличия блокировки группы);
  - информация о пользователях (наименование, ID, тип пользователя (мобильный), признак наличия блокировки пользователя).

Ненужные группы могут быть удалены из списка только в том случае, если в этих группах нет пользователей.

5. 8. Смена номера генерации ключевых данных

Номер генерации – числовой счетчик-идентификатор сгенерированных ЦГКК ключевых данных пользователя Криптосети ФПСУ-IP/Клиентов (изменяется от 1 до 256, по умолчанию равен 1). Записывается в VPN-профиль ФПСУ-IP/Клиента при инициализации VPN-Key или выдаче VPN-профиля в файл. Номер генерации, записанный в VPN-профиль ФПСУ-IP/Клиента, должен соответствовать тому, что указан на ФПСУ-IP, иначе ФПСУ-IP/Клиент не сможет соединиться с ФПСУ-IP.

Номер генерации ключевых данных может быть изменен администратором ЦГКК. После изменения номера генерации рекомендуется выдать ключевые данные для смены.

Для смены номера генерации выбрать пользователя, по нажатию правой клавиши мыши в контекстном меню выбрать команду «Сменить номер генерации».

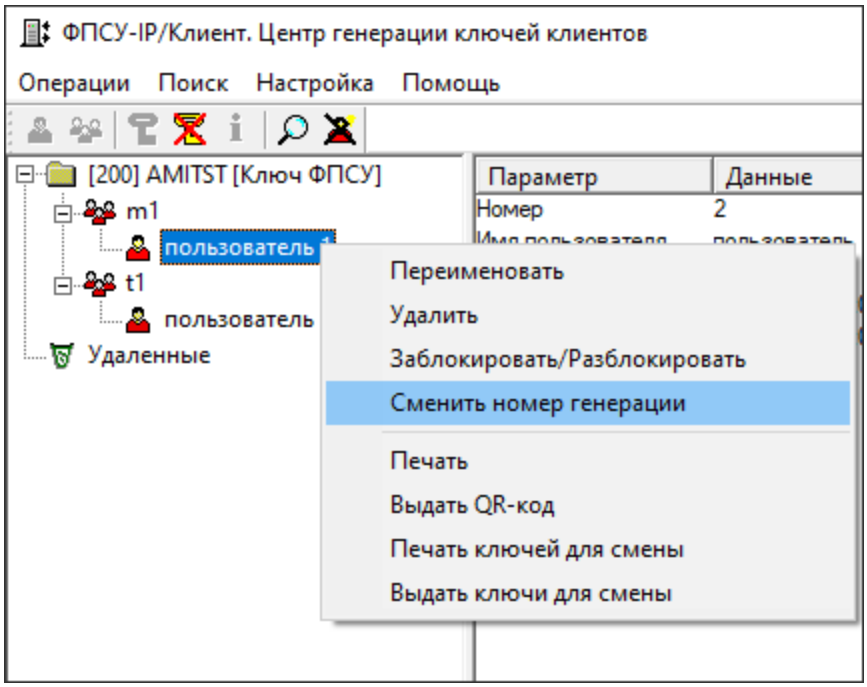

Рисунок 49 - Контекстное меню пользователя

Откроется окно, в котором следует ввести номер генерации ключевых данных. По нажатию кнопки «ОК» номер генерации будет изменен.

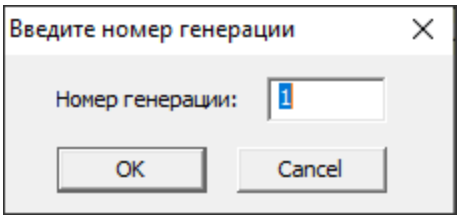

Рисунок 50 - Ввод номера генерации

5. 9. Изготовление VPN-ключей Клиентов и генерация QR-кодов

1. Для того, чтобы изготовить и записать ключ пользователя в устройство «VPN-Key», требуется:

- заранее зарегистрировать Криптосеть Клиента;
- заранее создать логическую группу пользователя;
- иметь доступ к общесистемному ключу Криптосети.

Для непосредственной регистрации пользователя, требуется:

- загрузить общесистемный ключ Криптосети Клиента в оперативную память;

- создать учетную запись пользователя (см. пункт «Создание пользователя»);
- проинициализировать пользователя.

2. Для того, чтобы сгенерировать криптографический ключ пользователя в виде бинарного файла:

- заранее зарегистрировать Криптосеть Клиента;
- заранее создать логическую группу пользователя;
- иметь доступ к общесистемному ключу Криптосети.

Для непосредственной регистрации пользователя, требуется:

- загрузить общесистемный ключ Криптосети Клиента в оперативную память;
- создать учетную запись пользователя (см. пункт «Создание пользователя»);
- сгенерировать и выдать ключевую информацию в виде бинарного файла или графического QR-кода.

5. 9. 1. Загрузка общесистемного ключа

Для изготовления ключевых носителей ФПСУ-IP/Клиентов необходимо загрузить общесистемный ключ той Криптосети Клиентов, в которой требуется создать пользователя.

При отсутствии загруженного общесистемного ключа Криптосети Клиентов инициализация устройств «VPN-Key» и выработка ключей для пользователей данной Криптосети Клиентов невозможны. Для загрузки общесистемного ключа необходимо:

1. В левой половине рабочего окна программы выбрать нужную Криптосеть Клиентов;
2. Выбрать в контекстном меню команду «Загрузить ключ» или воспользоваться соответствующей кнопкой панели инструментов;

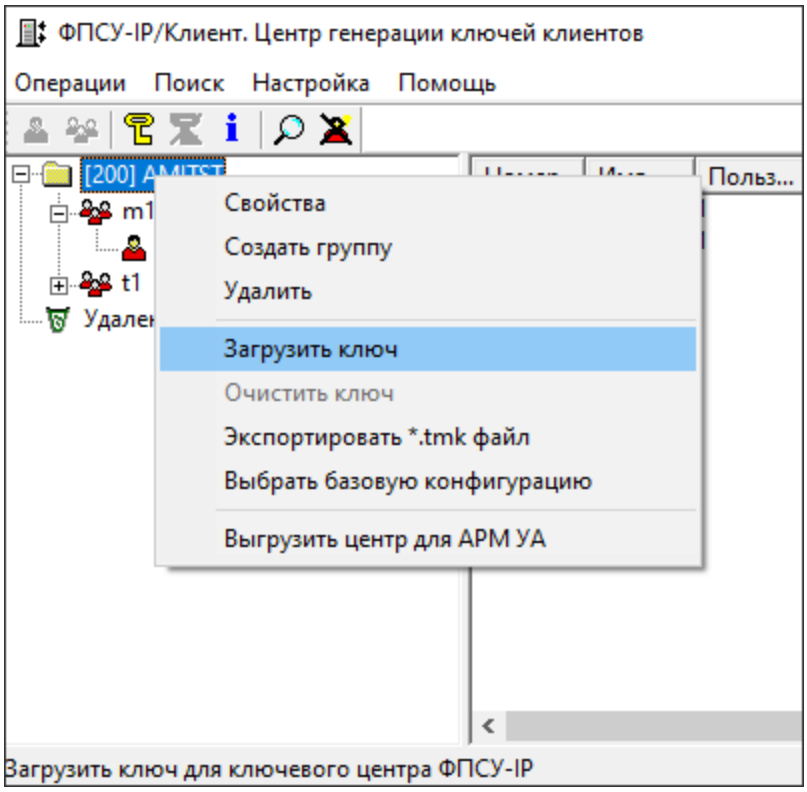

Рисунок 51 - Контекстное меню Криптосети

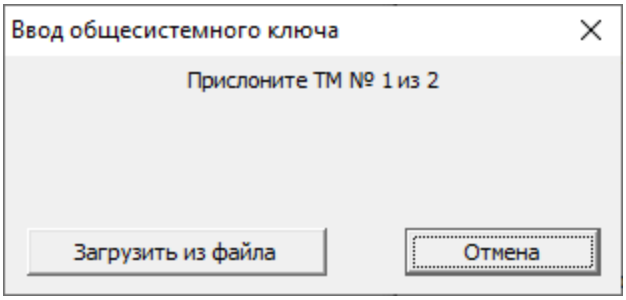

Рисунок 52 - Ввод общесистемного ключа

3. Прислонить по очереди (или подключить к USB-порту) все запрашиваемые ключевые носители. Если общесистемный ключ записывался в виде файла, необходимо нажать кнопку «Загрузить из файла» и последовательно загрузить все файлы, в которые были записаны части общесистемного ключа.
4. После загрузки ключа справа от описателя Криптосети появляется надпись [Ключ].

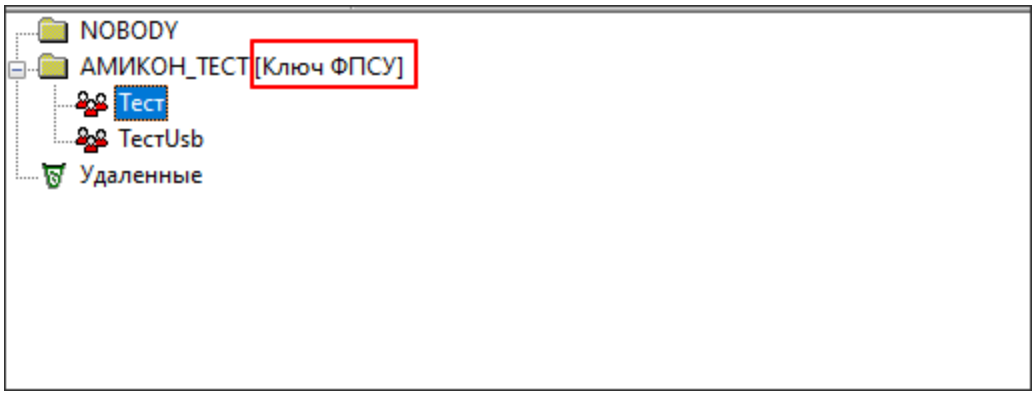

Рисунок 53 - Общесистемный ключ Криптосети загружен

5. 9. 2. Создание пользователя

Чтобы создать пользователя необходимо выполнить следующие действия:

1. В левой половине экрана выбрать нужную группу пользователей (вне какой-либо логической группы создать пользователя нельзя);
2. Выбрать подпункт «Создать пользователя» пункта «Действия» меню «Операции». Так же пользователь создается выбором пункта «Создать пользователя» в контекстном меню группы или нажатием одноименной кнопки на панели инструментов;

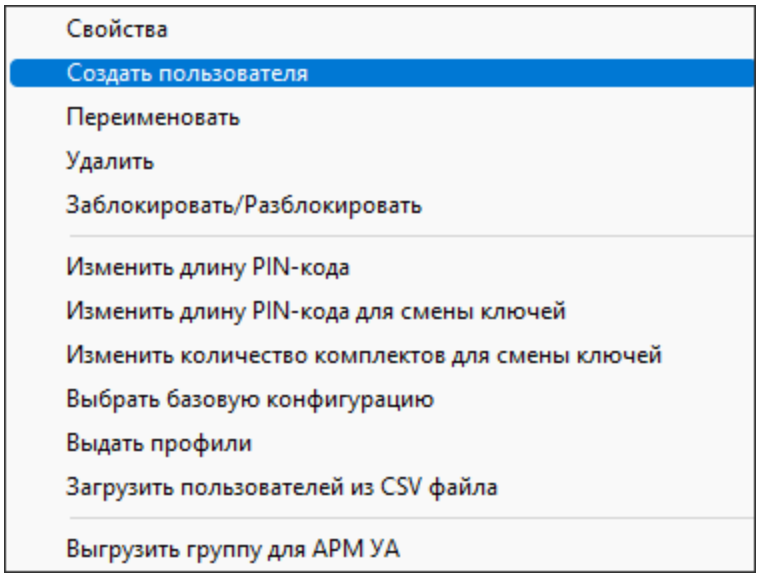

Рисунок 54 - Контекстное меню группы

3. Ввести номер и имя пользователя.

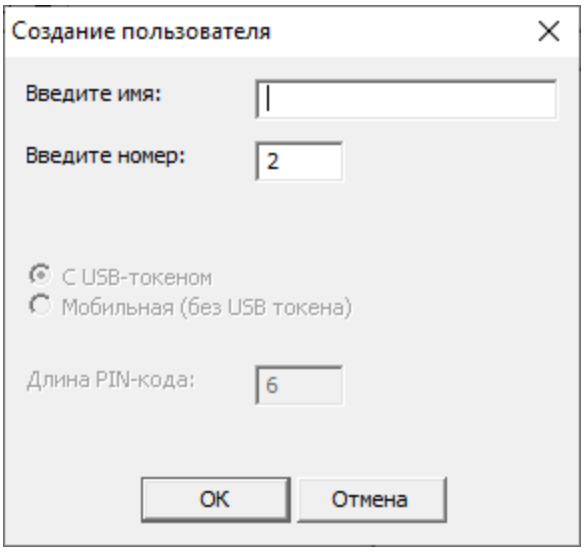

Рисунок 55 - Создание учетной записи пользователя

После создания пользователя его имя появится в списке.

Контекстное меню пользователя устройства «VPN-Key» включает команды:

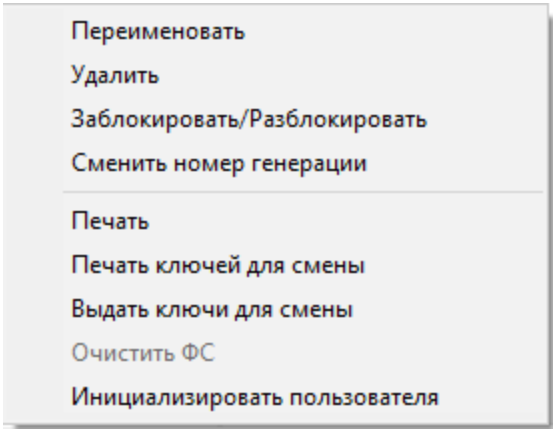

Рисунок 56 - Контекстное меню пользователя устройства VPN-Key

- Переименовать - сменить имя пользователя.
- Удалить - команда для удаления пользователя из Криптосети Клиентов. Следует обратить внимание на то, что удаление пользователя из Криптосети Клиентов при отсутствии «VPN-Key», в который он был ранее инициализирован, не приведёт к окончательному удалению пользователя из ЦГКК, равно как и к запрету взаимодействия данного «VPN-Key» с ФПСУ-IP.
- Заблокировать/разблокировать - команда для включения/выключения метки запрета инициализации пользователя в устройства «VPN-Key».

- Печать - команда для вывода на печать содержащейся в ЦГКК информации о пользователе.
- Печать ключей для смены - команда для вывода на печать ключевых данных пользователя для смены.
- Выдать ключ для смены - команда для вывода ключевых данных пользователя для смены ключевой информации в виде QR-кода и возможностью записи в файл *.bin.
- Очистить ФС - кнопка очистки файловой системы, форматирования. При форматировании вся хранящаяся на устройстве информация (данные о пользователях и настройки работы с хостами и ФПСУ-IP) будет уничтожена.
- Инициализировать пользователя - команда для записи данных пользователя в устройство «VPN-Key».

Контекстное меню пользователя группы, не использующей «VPN-Key», включает команды:

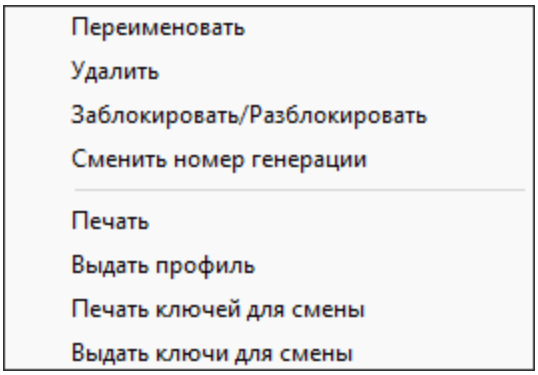

Рисунок 57 - Контекстное меню пользователя мобильной группы (без USB токена)

- Переименовать - сменить имя пользователя.
- Удалить - команда для удаления пользователя из Криптосети Клиентов.
- Заблокировать/разблокировать - команда для включения/выключения метки запрета выдачи QR-кодов.
- Печать - команда для вывода на печать содержащейся в ЦГКК информации о пользователе.
- Выдать профиль - команда для записи данных пользователя в виде QR-кода.
- Печать ключей для смены - команда для вывода на печать ключевых данных пользователя для смены.
- Выдать ключи для смены - команда для вывода ключевых данных пользователя для смены в виде QR-кода и возможностью записи в файл *.bin.

5. 9. 3. Добавление пользователей из CSV файла

При возникновении необходимости автоматической загрузки информации о пользователях предоставляется возможность создать файл формата *.csv, пример которого представлен на рисунке ниже, и загрузить внесенные в него сведения в ЦГКК.

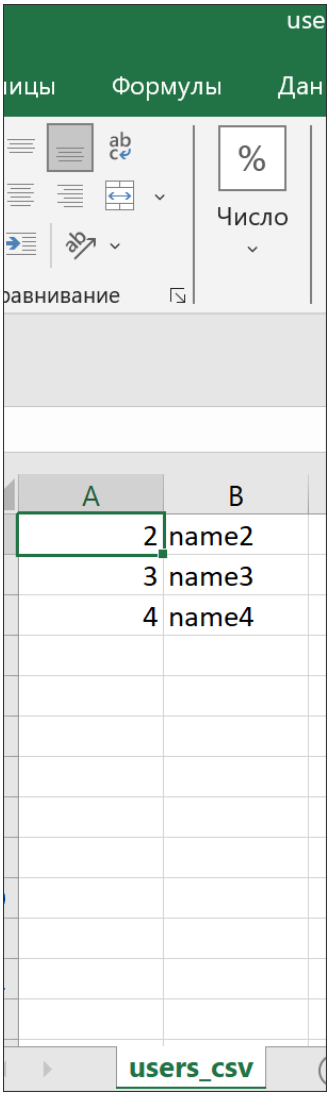

Рисунок 58 - Пример CSV файла для автоматической закрузки информации о пользователях

В файл вносятся номера и имена пользователей.

Чтобы добавить пользователей из файла со списком необходимо выполнить следующие действия:

1. В левой половине экрана выбрать нужную группу пользователей;
2. Выбрать подпункт «Добавить пользователей из CSV файла» пункта «Действия»

меню «Операции». Так же пользователь создается выбором пункта «Добавить пользователей из CSV файла» в контекстном меню группы.

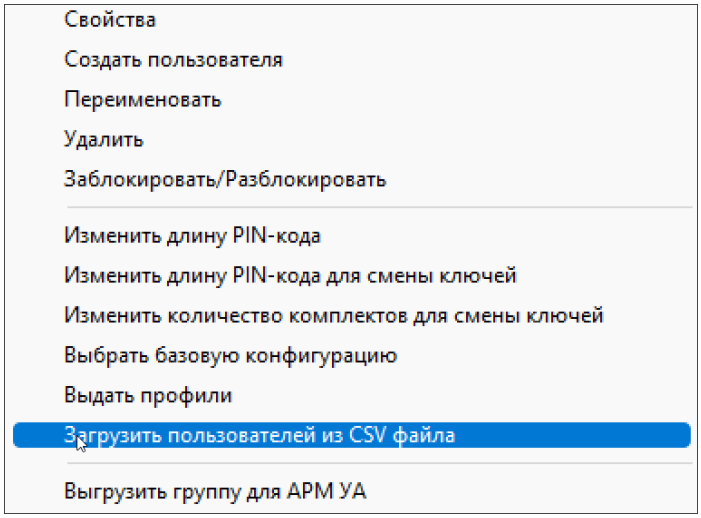

Рисунок 59 - Контекстное меню группы

На экран будет сообщение о необходимости выбора файла:

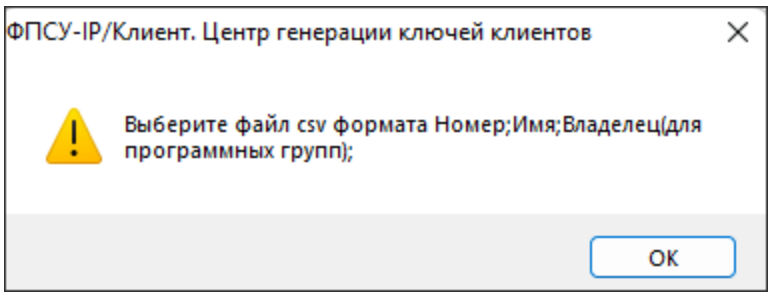

Рисунок 60 - Предложение выбора файла

Для продолжения следует нажать кнопку «ОК». В появившемся окне необходимо выбрать путь к нужному файлу, после чего в открывшемся окне создания инициализирующей последовательности для программного датчика случайных чисел потребуется перемещать указатель мыши без нажатия на клавиши в пределах окна.

После заполнения строки состояния, расположенной под текстом, датчик случайных чисел будет инициализирован.

На экран будет выведено сообщение о добавлении пользователей:

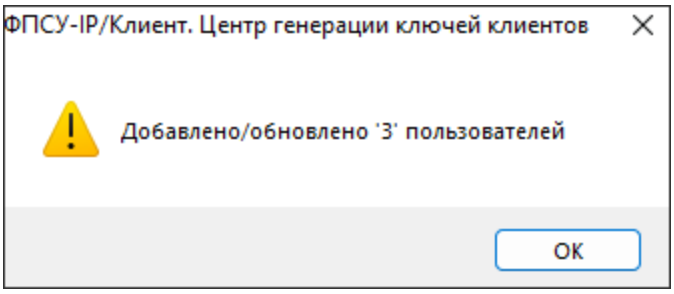

Рисунок 61 - Сообщение о добавлении ползователей

5. 9. 4. Инициализация VPN-профиля пользователя в VPN-Key

Инициализация пользователя группы с USB-токеном подразумевает генерацию для него ключевых данных, выбор конфигурации подключения к ФПСУ-IP, и запись перечисленных данных в устройство «VPN-Key».

Кроме этого, в устройство «VPN-Key» записывается специальное стартовое значение для ДСЧ, используемое встроенными модулями СКЗИ. Это значение требуется раз в 15 месяцев переписывать (выбором пункта «Инициализация ДСЧ VPN-Key» основного меню «Операции»).

В одном устройстве «VPN-Key» программой ЦГКК может быть последовательно инициализировано до семи пользователей (т.е. создано не более 7 VPN-профилей). Каждый дополнительный VPN-профиль должен принадлежать другой Криптосети Клиентов. Для инициализации пользователя и записи VPN-профиля необходимо:

1. Вставить «VPN-Key» в USB-порт. При этом в строке статуса появится надпись «VPN-KEY». Следует иметь в виду, что при работе с ЦГКК в определенный момент времени может быть подключено только одно устройство VPN-Key;
2. Выбрать пользователя, который инициализируется в устройство «VPN-Key»;
3. Нажать клавишу «Enter», или вызвать контекстное меню пользователя и выбрать пункт меню «Инициализировать пользователя». Для продолжения следует нажать кнопку «ОК» в появившемся системном окне.

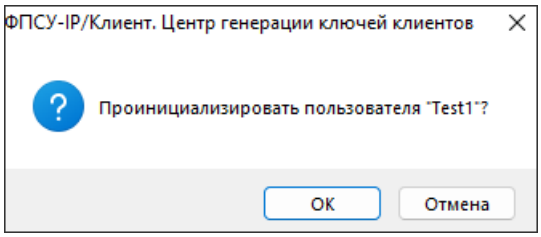

Рисунок 62 - Инициализация пользователя

4. При первом использовании устройства «VPN-Key» откроется окно ввода новых PIN-кодов, в котором необходимо заменить сгенерированные программой PIN-коды пользователя (имеющего права оператора) и администратора (обладающего правом менять рабочие параметры ФПСУ-IP/Клиента) на новые **цифровые** PIN-коды.

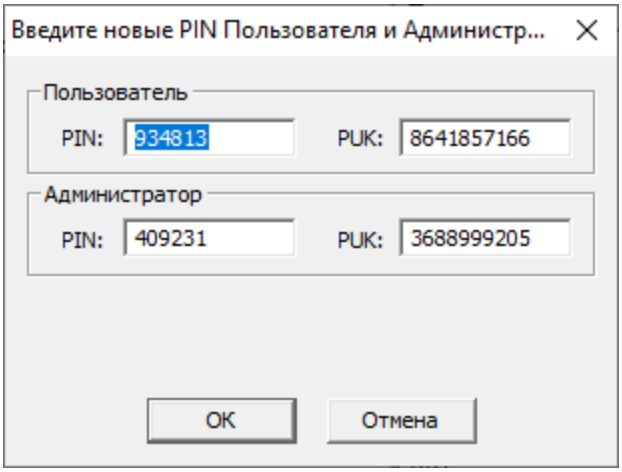

Рисунок 63 - Назначение кодов доступа

При повторном подключении устройства «VPN-Key» вначале откроется окно, в котором предлагается ввести существующие PIN-коды доступа к устройству «VPN-Key».

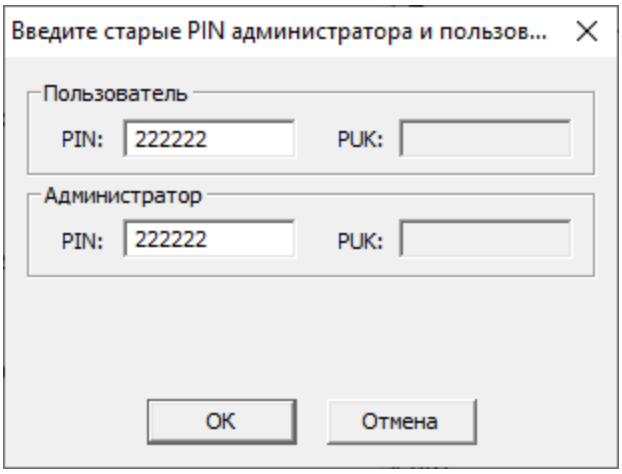

Рисунок 64 - Ввод существующих идентификационных кодов

В том случае, если в общих настройках не установлен флаг «Сохранять PIN при переинициализации пользователя» (см. пункт «Настройки ЦГКК»), после ввода старых PIN-кодов, откроется окно ввода новых идентификаторов, в котором необходимо подтвердить сгенерированные программой случайным образом идентификационные коды для пользователя (имеющего права оператора) и администратора (обладающего правом менять рабочие параметры ФПСУ-IP/Клиента) или ввести свои PIN-коды (Рисунок «Назначение кодов доступа»). Если флаг «Сохранять PIN при переинициализации пользователя» (см. пункт «Настройки ЦГКК») был установлен, система сохранит ранее заданные идентификационные коды.

5. По нажатию кнопки «ОК» будет выдано окно выбора конфигурации для пользователя инициализируемого устройства «VPN-Key», в котором предоставляется возможность выбрать одну из ранее созданных конфигураций или создать новую (см. пункт «Создание шаблона конфигурации VPN-профиля»). Можно пропустить этот пункт, и внести изменения в конфигурацию устройства позднее, с помощью PIN-кода администратора.
6. Критерием успешности процесса инициализации является служебное оповещение «Носитель ключей для пользователя %Username% проинициализирован».

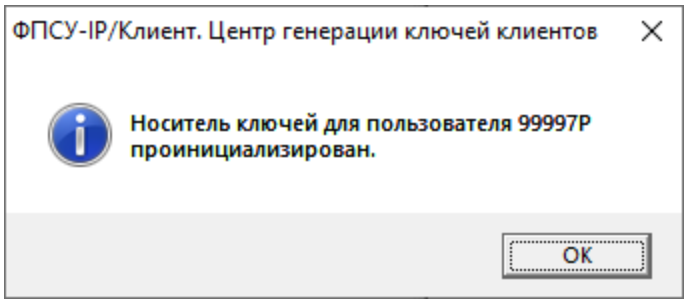

Рисунок 65 - Сообщение об успешной инициализации

При попытке удаления пользователя с предъявлением устройства «VPN-Key» VPN-профиль пользователя будет так же удален из устройства «VPN-Key».

При инициализации пользователя в устройство «VPN-Key» записываются:

• системные параметры пользователя — номер Криптосети, номер группы и номер пользователя;

• ключевые данные пользователя Криптосети Клиентов;

• номер серии общесистемного ключа;

• номер генерации ключевых данных;

• дата инициализации.

Номер серии общесистемного ключа Криптосети ЦГКК, с помощью которого инициализировали пользователя, можно посмотреть в поле «Серия ключа» при выборе пользователя в основном окне программы. Номер серии начинается с единицы; при повторной инициализации пользователя, номер серии, как правило, увеличивают на один.

Для удобства контроля номера серии большой группы пользователей, в основном окне программы можно отметить одним фоновым цветом иконки тех пользователей, которые имеют одинаковый номер серии (для этого необходимо в общих настройках программы ввести нужную серию ключа в поле «Выделять серию» - см. пункт «Настройки ЦГКК»).

Номер генерации ключевых данных пользователя можно посмотреть в поле «Генерация ключа». Он может быть изменен по команде контекстного меню «Сменить номер генерации» (см. пункт «Смена номера генерации ключевых данных»).

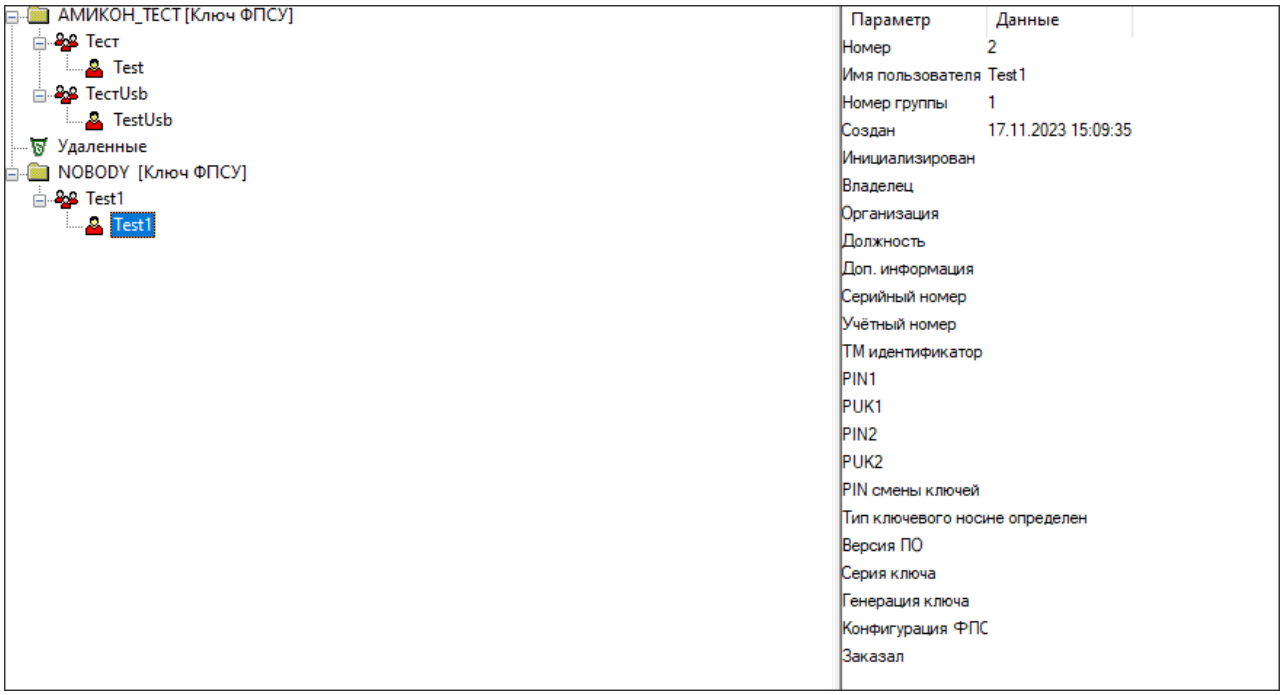

Рисунок 66 - Серия общесистемного ключа и номер генерации

5. 9. 5. Инициализация VPN-профиля пользователя в файл

Инициализация пользователя мобильной группы (без USB-токена) подразумевает генерацию для него ключевых данных, выбор конфигурации подключения к ФПСУ-IP, и выдачу перечисленных данных в виде QR-кода, а также запись перечисленных данных в бинарный файл.

Для формирования и записи VPN-профиля необходимо:

1. Выбрать пользователя, для которого формируется файл с ключевой информацией;
2. Выбрать подпункт «Выдать профил» пункта «Действия» меню «Операции» или аналогичный пункт из контекстного меню пользователя.

Программа выдаст запрос о формате записи ключей:

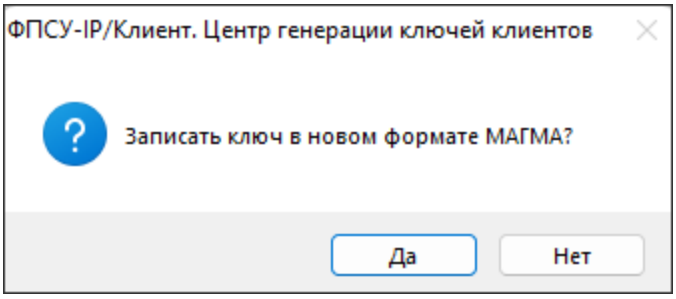

Рисунок 67 - Запрос записи ключа в новом формате

По нажатию кнопки «Да» ключ записывается в файл для протокола МАГМА и ФПСУ-IP/Клиент сможет работать с ФПСУ-IP только по протоколу МАГМА, по нажатию кнопки «Нет» - для протокола ГОСТ 28147-89.

3. После выбора формата записи ключа на экран будет выведено окно выбора конфигурации, в котором предоставляется возможность выбрать одну из ранее созданных конфигураций или создать новую (см. пункт «Создание шаблона конфигурации VPN-профиля»). Можно пропустить этот пункт, и внести изменения в конфигурацию устройства позднее, с помощью PIN-кода администратора.
4. Изменить сгенерированный программой случайным образом PIN-код доступа администратора (при работе с программным Клиентом любой пользователь обладает правами администратора) на **цифровой**.

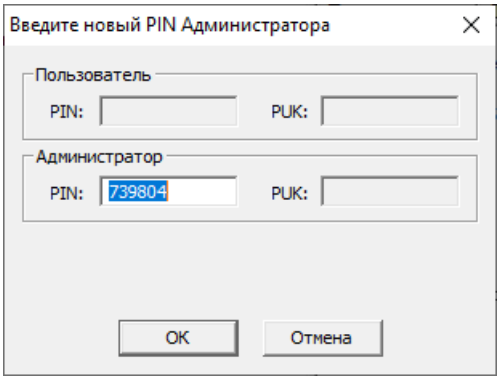

Рисунок 68 - Назначение кодов доступа

5. На экран будет выведено окно с графическим изображением ключевой информации в виде QR-кода.

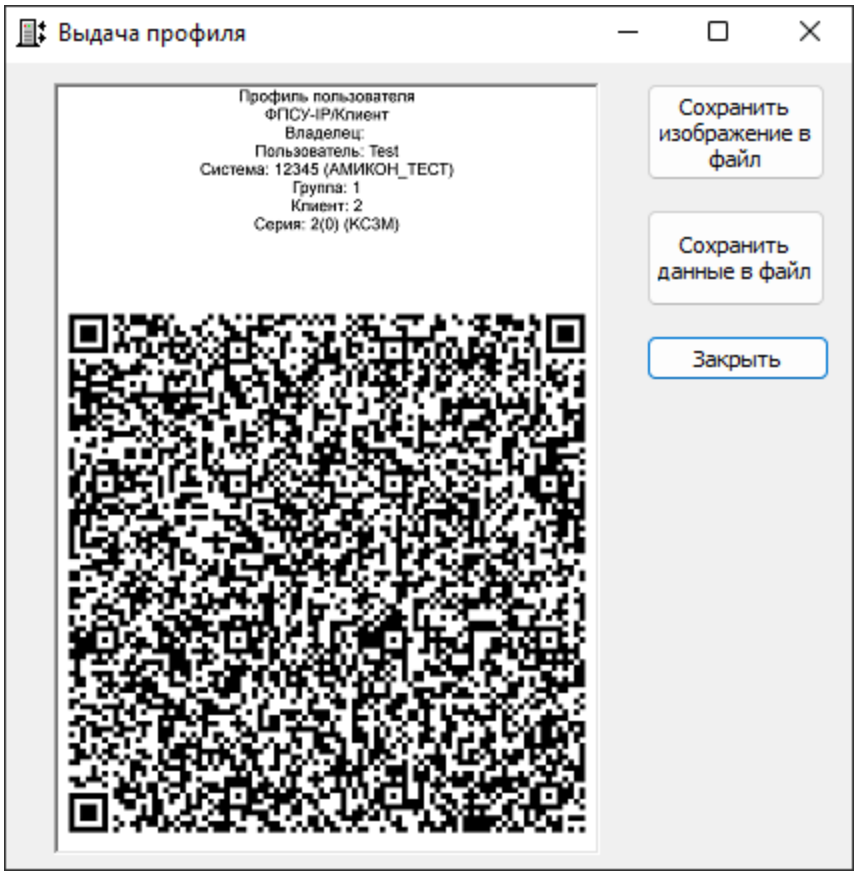

Рисунок 69 - Выдача QR-кода

Графический файл формата *.png для последующего вывода на экран ЦГКК формируется при нажатии на кнопку «Сохранить изображение в файл».

Также предоставляется возможность сохранить сгенерированный QR-код в виде файла формата *.bin (по нажатию на кнопку «Сохранить данные в файл»). В этом слу-чае файл необходимо передать доверенным образом на АРМ пользователя ФПСУ-IP/Клиент.

Критерием успешности процесса инициализации пользователя мобильной груп-пы (без USB-токена) является проставленная дата инициализации.

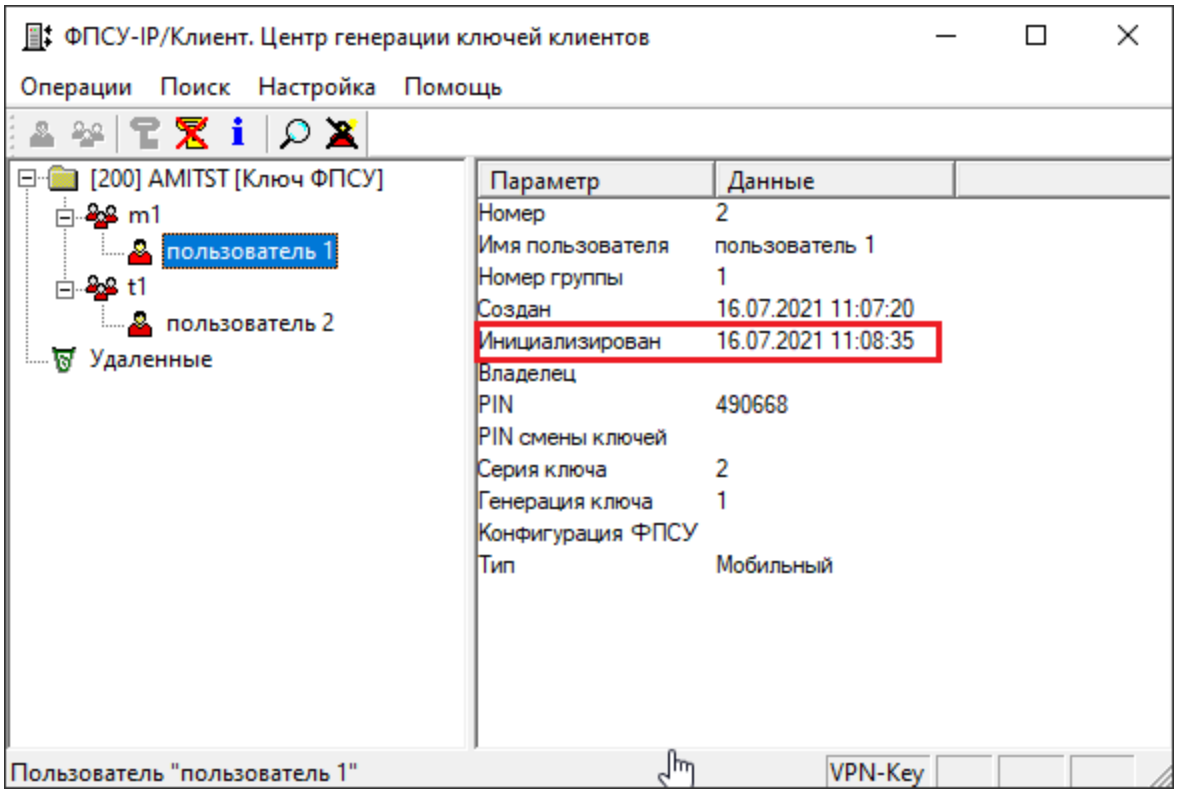

Рисунок 70 - Дата инициализации

При инициализации пользователя мобильной группы (без USB-токена) в QR-код записываются:

- системные параметры пользователя — номер Криптосети, номер группы и номер пользователя;
- ключевые данные пользователя Криптосети Клиентов;
- номер серии общесистемного ключа;
- номер генерации ключевых данных;
- дата инициализации.

Номер серии общесистемного ключа Криптосети ЦГКК, с помощью которого инициализировали пользователя, можно посмотреть в поле «Серия ключа» при выборе пользователя в основном окне программы. Номер серии начинается с единицы; при повторной инициализации пользователя, номер серии, как правило, увеличивают на один.

Для удобства контроля номера серии большой группы пользователей, в основном окне программы можно отметить одним фоновым цветом иконки тех пользователей, которые имеют одинаковый номер серии (для этого необходимо в общих настройках

программы ввести нужную серию ключа в поле «Выделять серию» - см. пункт «Настройки ЦГКК»).

Номер генерации ключевых данных пользователя можно просмотреть в поле «Генерация ключа». Может быть изменен по команде контекстного меню «Сменить номер генерации» (см. пункт «Смена номера генерации ключевых данных»).

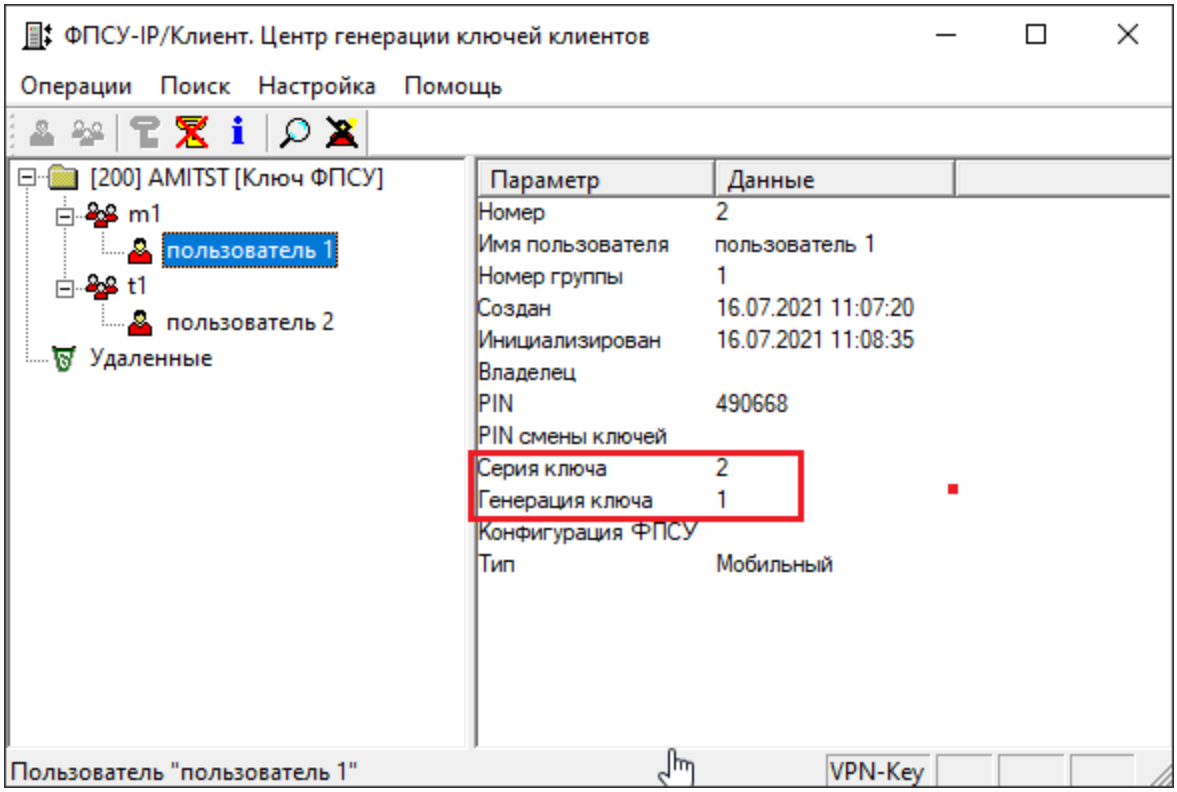

Рисунок 71 - Серия общесистемного ключа и номер генерации

5. 9. 6. Регистрация нескольких устройств VPN-Key

При инициализации пользователей из группы пользователей, работающих с ФПСУ-IP/Клиентом с применением устройства «VPN-Key», могут быть введены сведения об устройствах «VPN-Key» для учёта и дальнейшей инвентаризации устройств.

Для инициализации всех пользователей группы с USB-токеном выбрать группу и в контекстном меню команду «Инициализировать пользователей».

Для пользователей группы необходимо сразу настроить конфигурацию, выбрав её в списке конфигураций одноименной кнопкой («Выбрать»).

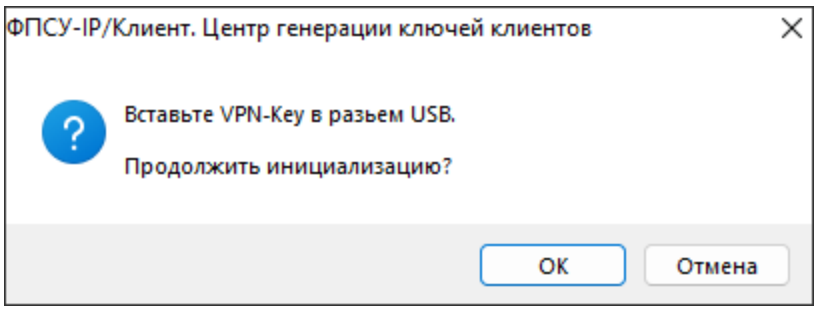

Рисунок 72 - Запрос на подключение VPN-Key

Для ввода регистрационных данных о каждом устройстве «VPN-Key» требуется поочерёдно вставлять «VPN-Key» в USB-порт, так как в определенный момент времени может быть подключено только одно устройство VPN-Key:

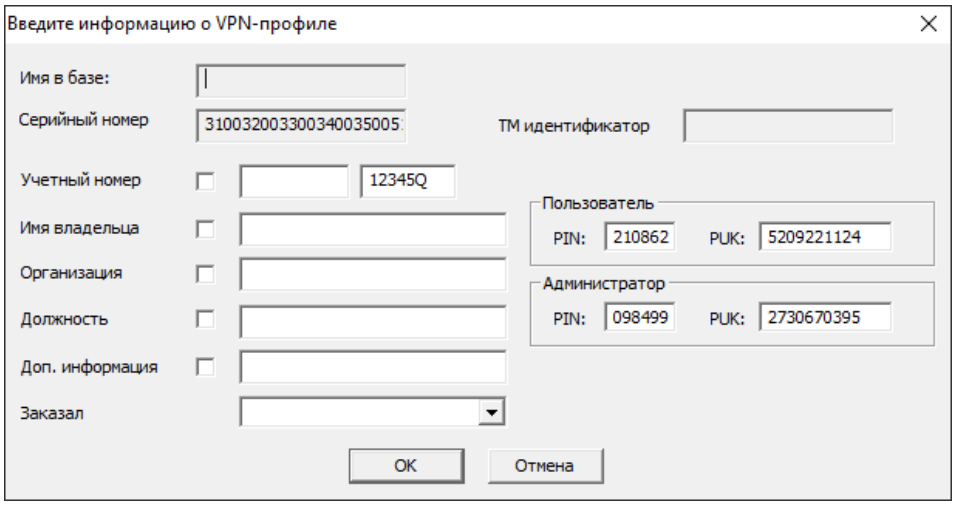

Рисунок 73 - Окно ввода сведений об устройстве VPN-Key

При повторной инициализации сведения об устройстве «VPN-Key» могут быть изменены.

5. 10. Выдача ключей для смены ключевой информации VPN-профиля

Срок действия ключевой информации отсчитывается с момента генерации ключевых данных и не должен превышать 15 месяцев. До истечения срока действия текущих ключевых данных требуется повторно сгенерировать и установить новые ключевые данные на местах использования СКЗИ.

Для смены ключевой информации VPN-профиля программного, программно-аппаратного Клиента или мобильного приложения «ФПСУ-IP/Клиент» на ЦГКК генерируются ключи, которые записываются в виде файла формата *.bin или графического

QR-кода.

Для того, чтобы выдать ключ для замены, необходимо:

1. Загрузить общесистемный ключ (см. пункт «Загрузка общесистемного ключа»)
2. Выбрать подпункт «Выдать ключи для смены» пункта «Действия» меню «Операции» для предварительно выбранного пользователя или воспользоваться аналогичным пунктом контекстного меню пользователя.

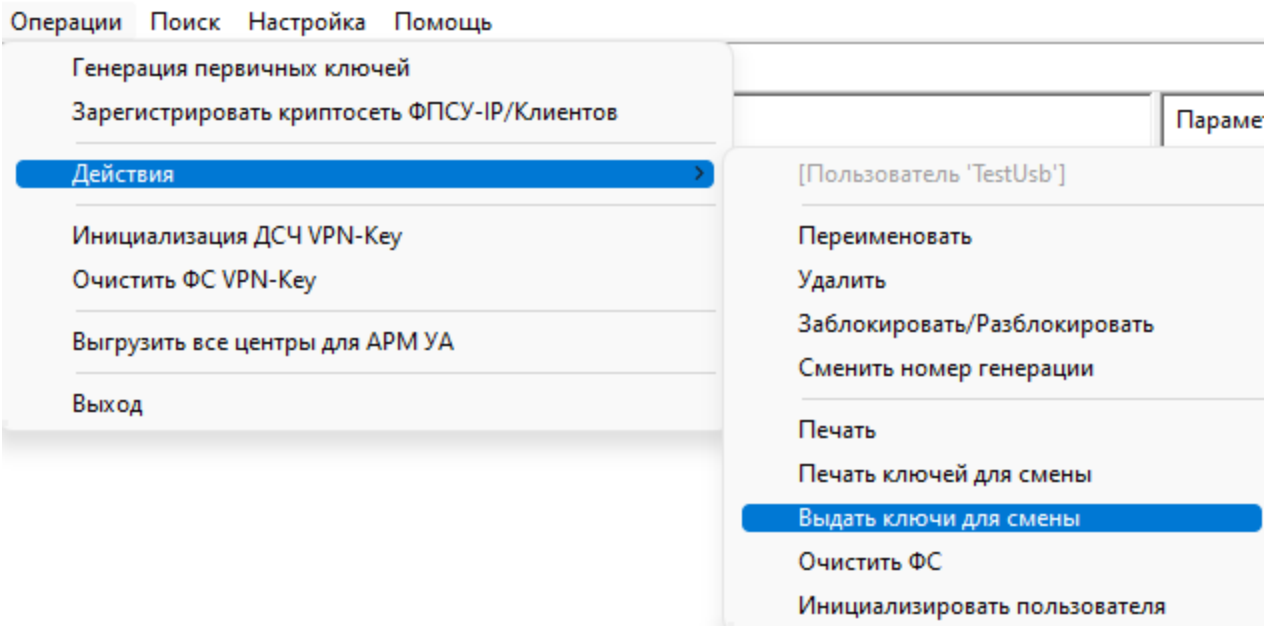

Рисунок 74 - Выбор пункта меню для выдачи ключа

3. Откроется окно запроса формата записи ключа. По нажатию кнопки «Да» ключ записывается в файл для протокола МАГМА и ФПСУ-IP/Клиент сможет работать с ФПСУ-IP только по протоколу МАГМА, по нажатию кнопки «Нет» - для протокола ГОСТ 28147-89.

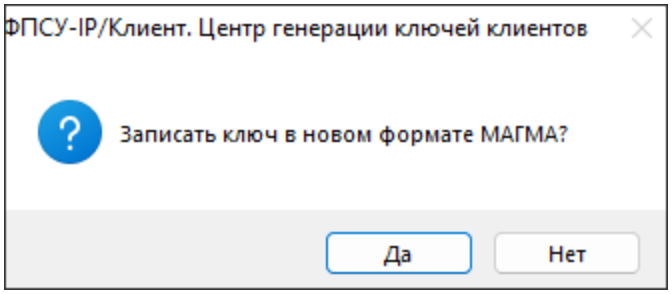

Рисунок 75 - Выбор криптографического протокола

По нажатию кнопки «Да» откроется окно, в котором предлагается ввести

транспортный PIN-код (транспортный ключ — это ключ, который используется для шифрования другого ключа при его передаче.).

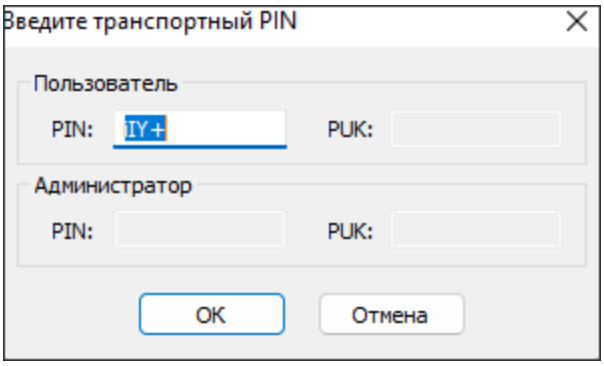

Рисунок 76 - Окно ввода транспортного PIN-кода

По умолчанию в поле ввода PIN-кода отображается сгенерированный программой случайным образом код.

4. По нажатию кнопки «ОК» на экран будет выведено окно с графическим изображением ключевой информации в виде QR-кода.

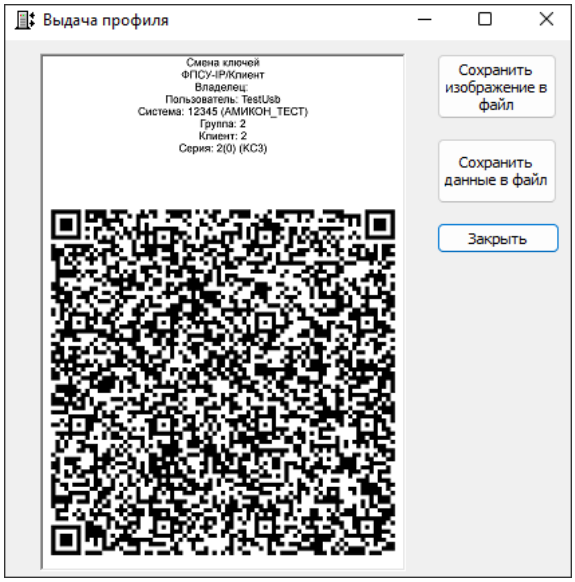

Рисунок 77 - Выдача QR-кода

При выдаче ключевой информации в файл записываются:

• системные параметры пользователя — номер Криптосети, номер группы и номер пользователя - не изменяются при выдаче;

• ключевые данные пользователя Криптосети Клиентов;
• номер серии общесистемного ключа - не изменяется при выдаче;
• номер генерации ключевых данных - не изменяется при выдаче.

Номер генерации ключевых данных пользователя может быть изменен по команде контекстного меню «Сменить номер генерации» (см. пункт «Смена номера генерации ключевых данных»).

5. 11. Выгрузка для АРМ УА

При необходимости предоставляется возможность выгрузить в файл основные параметры конфигурации криптосети или группы клиентов для последующей загрузки этого файла на АРМ УА. Файл содержит список активных пользователей криптосети или группы. В дальнейшем этот список можно загрузить в АРМ УА с целью автоматизации внесения информации о разрешении или запрете работы для групп клиентов в конфигурации (т.е. для пакетного изменения блокировок клиентов). Этот список представляет собой файл формата *.exc, содержащий следующие сведения:

- общие сведения о файле экспорта (описание версия, кодировка, система);
- информация о группе пользователей (наименование, ID, тип группы (мобильная или нет), признак наличия блокировки группы);
- информация о пользователях (наименование, ID, тип пользователя (мобильный или нет), признак наличия блокировки пользователя).

5. 11. 1. Выгрузка криптосети для АРМ УА

Для выгрузки в файл для АРМ УА основных параметров группы криптосети, необходимо выбрать криптосеть и в контекстном меню для нее нажать на «Выгрузить центр для АРМ УА»

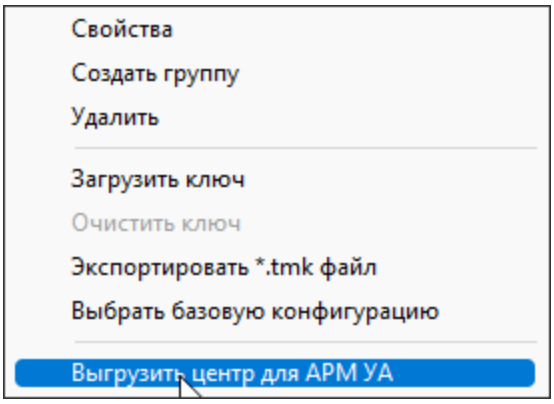

Рисунок 78 - Выбор пункта контекстного меню для выгрузки данных криптосети

Затем в открывшемся стандартном окне указать путь к формируемому файлу выгрузки и его наименование (по умолчанию файл именуется «System_sX.exc», где X - номер криптосети). По нажатию кнопки «Сохранить» будет сформирован файл формата *.exc.

5. 11. 2. Выгрузка группы для АРМ УА

Для выгрузки в файл для АРМ УА основных параметров группы клиентов, необходимо выбрать группу и в контекстном меню дл нее нажать на «Выгрузить группу для АРМ УА»

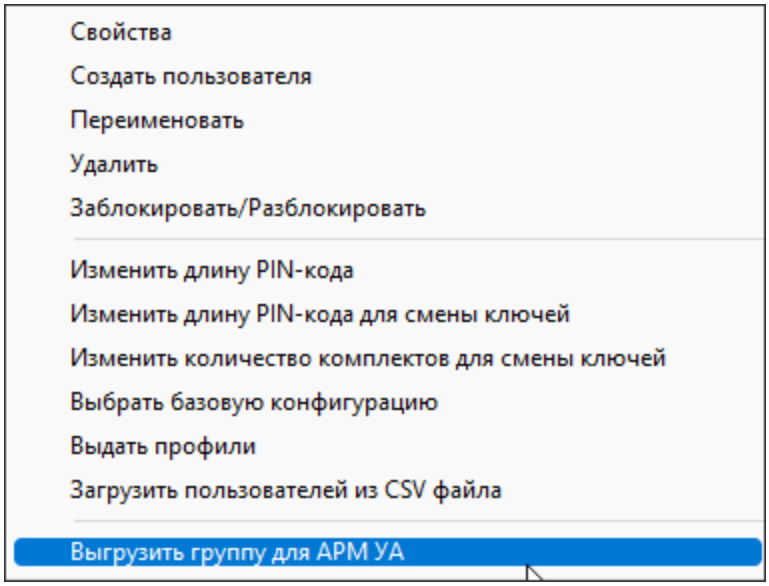

Рисунок 79 - Контекстное меню группы клиентов

Затем в открывшемся стандартном окне указать путь к формируемому файлу выгрузки и его наименование (по умолчанию файл именуется «Group_sXgY.exc», где X - номер криптосети, Y - номер группы). По нажатию кнопки «Сохранить» будет сформирован файл формата *.exc.

5. 12. Инициализация ПДСЧ VPN-Key

При необходимости переинициализировать программный датчик случайных чисел, реализованный в устройстве «VPN-Key», следует выбрать пункт «Инициализация ДСЧ VPN-Key» меню «Операции».

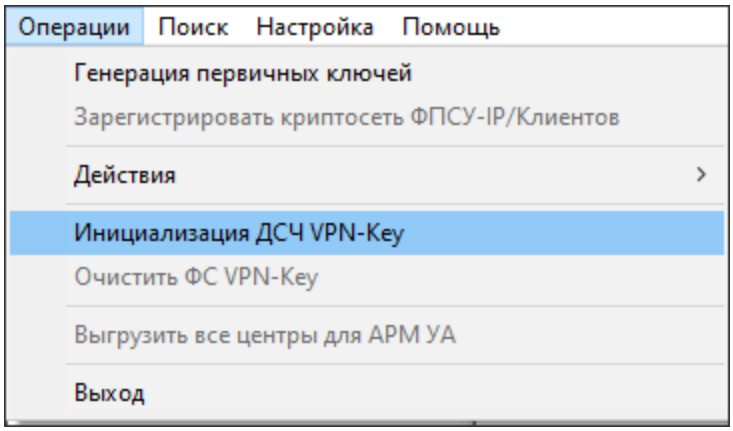

Рисунок 80 - Меню «Операции»

Произойдет вызов датчика случайных чисел, в котором требуется сформировать случайное число путем перемещения указателя мыши в пределах открывшегося окна.

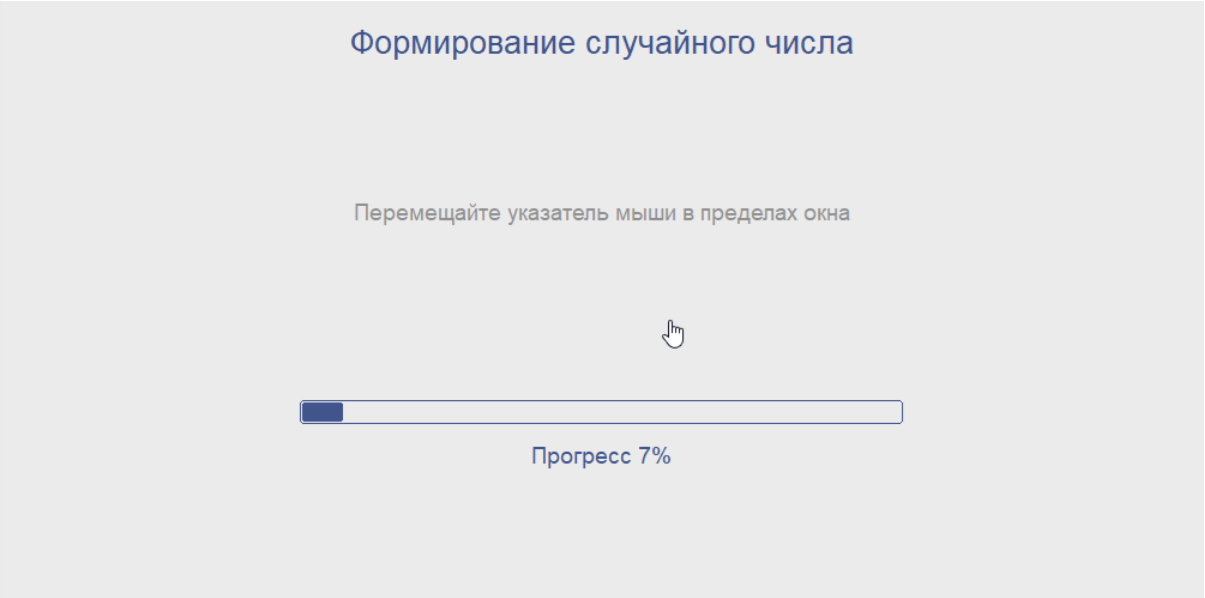

Рисунок 81 - Формирование случайного числа

По окончанию инициализации датчика случайных чисел система выдаст сообщение о том, что устройство «VPN-Key» успешно проинициализировано.

5. 13. Вывод информации о пользователе на печать

Информация по отдельному пользователю, созданному в ЦГКК, может быть выведена на печать посредством выполнения команды контекстного меню пользователя «Печать».

При этом выводится окно предпросмотра печати, с возможностью выбора принтера, информационных полей и параметров печати.

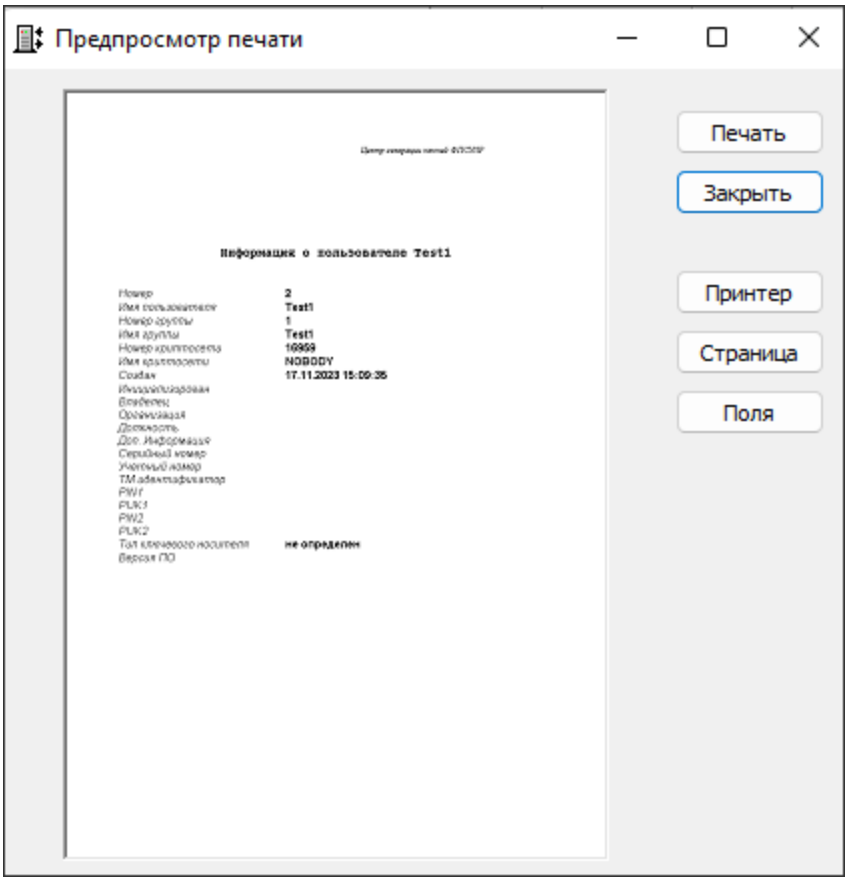

Рисунок 82 - Вывод информации о пользователе на печать

Выбрать выводимые на печать информационные поля можно, вызвав редактор нажатием на кнопку «Поля». Выбирается наличие/присутствие следующих элементов:

Номер	- номер пользователя, введённый при создании;
Имя пользователя	- имя пользователя, введённое при создании;
Номер группы	- номер группы, в которую включен пользователь;
Имя группы	- имя группы, в которую включен пользователь;
Номер криптосети	- номер Криптосети Клиентов, в которую включен пользователь;
Имя криптосети	- имя Криптосети Клиентов, в которую включен пользователь;
Создан	- дата создания пользователя в программе ЦГКК;
Инициализирован	- дата инициализации пользователя в устройство «VPN-Key»;

Владелец	- опционально, имя владельца устройства «VPN-Key», в который инициализирован данный пользователь;
Организация	- опционально, название организации, в которой работает владелец устройства «VPN-Key»;
Должность	- опционально, должность владельца устройства «VPN-Key»;
Доп. Информация	- опционально, поле для ввода произвольной информации;
Серийный номер	- серийный номер устройства «VPN-Key» выбранного пользователя;
Учетный номер	- опционально, учётный номер устройства «VPN-Key» пользователя;
ТМ идентификатор	- в данном поле указывается уникальный номер ТМ-идентификатора, который записывается в «VPN-Key»;
PIN1	- PIN-код пользователя (оператора) устройства «VPN-Key»;
PUK1	- PUK-код пользователя (оператора) устройства «VPN-Key»;
PIN2	- PIN-код администратора ключа «VPN-Key»;
PUK2	- PUK-код администратора ключа «VPN-Key»;
Тип ключевого носителя	- «VPN-KEY», если пользователь инициализирован, в противном случае «не определён»;
Версия ПО	- версия микрокода устройства «VPN-Key»;

Нажатие на кнопку «Страница» позволяет задать отступ полей страницы.

Нажатие на кнопку «Принтер» позволяет перейти к окну выбора принтера и параметров печати. Список принтеров берется из операционной системы.

5. 14. Обновление микрокода устройства VPN-Key

Программа ЦГКК предоставляет администратору возможность контроля версии внутреннего программного обеспечения устройства «VPN-Key» (микрокода) и файло-вой системы.

Обновления микрокода и файловой системы устройства «VPN-Key» — файлы с

расширением .FWU (обновление микрокода) и .FSU (обновление файловой системы), должны быть размещены в подкаталог UPDATES рабочего каталога программы ЦГКК.

При инициализации пользователя в устройство «VPN-Key», программа автома-тически производит опрос внутреннего программного обеспечения устройства, сравне-ние его версий с версиями имеющихся в подкаталоге UPDATES обновлений. Если в подкаталоге обнаруживаются более новые версии, программа предлагает администра-тору обновить микрокод и/или файловую систему перед дальнейшей инициализацией пользователя.

Для обновления микрокода и файловой системы устройства «VPN-Key» при инициализации пользователя и записи VPN-профиля необходимо:

1. Подключить «VPN-Key» к USB-порту, при этом в строке статуса должна появиться надпись «VPN-KEY»;
2. Выбрать пользователя, который инициализируется в устройство «VPN-Key»;
3. Вызвать контекстное меню пользователя и выбрать пункт меню «Очистить ФС» или в меню «Операции» выбрать пункт «Очистить ФС VPN-Key». Данные пункты меню будут доступны только в том случае, если обнаружены файлы обновлений с более новыми версиями программного обеспечения устройства «VPN-Key».

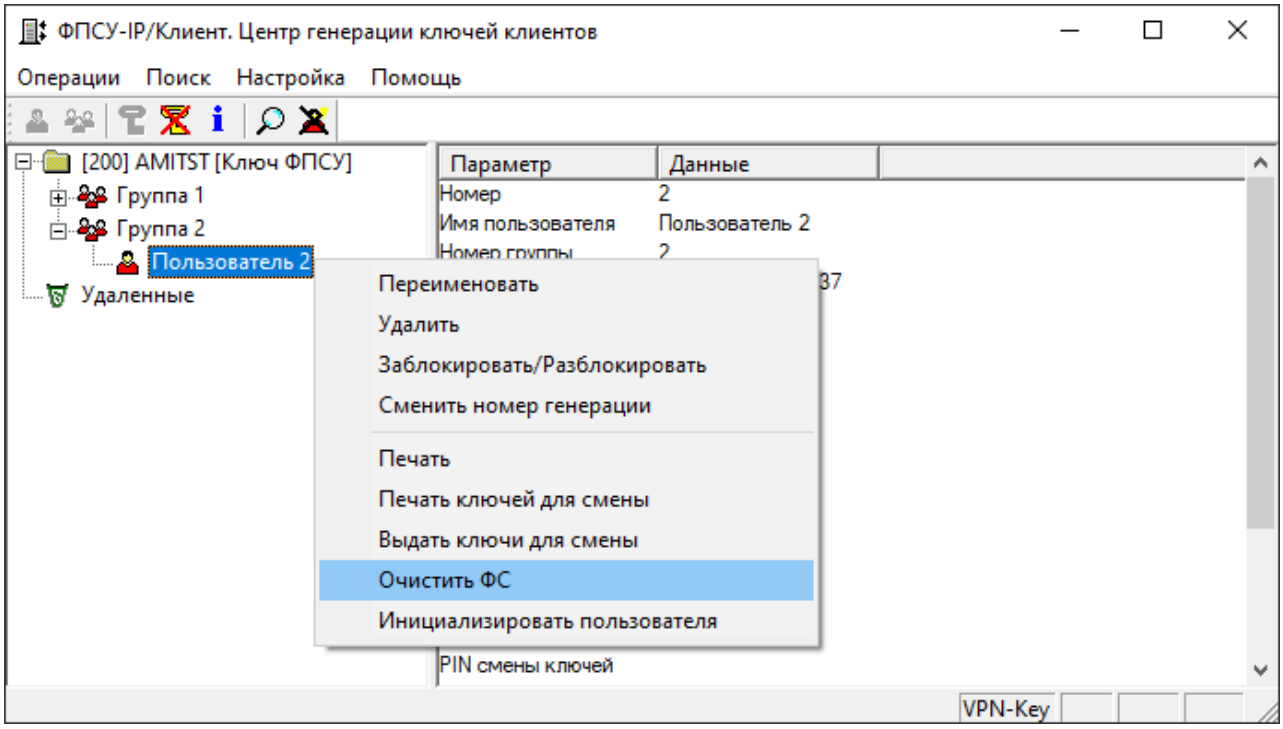

Рисунок 83 - Контекстное меню пользователя

На экран будет выведено окно о загрузке файловой системы «VPN-Key» и сообщение

об успешном обновлении, в котором требуется нажать кнопку «ОК».

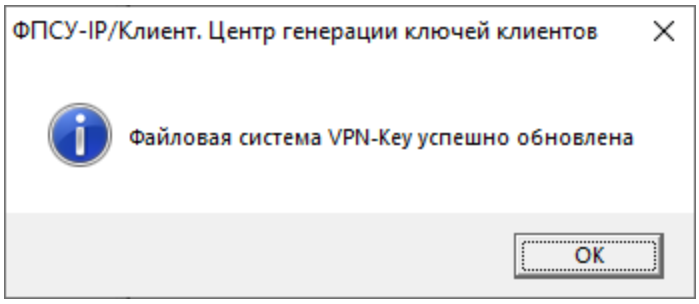

Рисунок 84 - Обновление файловой системы

4. Далее нажать клавишу «Enter», или вызвать контекстное меню пользователя и выбрать пункт меню «Инициализировать пользователя». На экран будет выведено окно с сообщением о найденной файловой системе с новой версией.

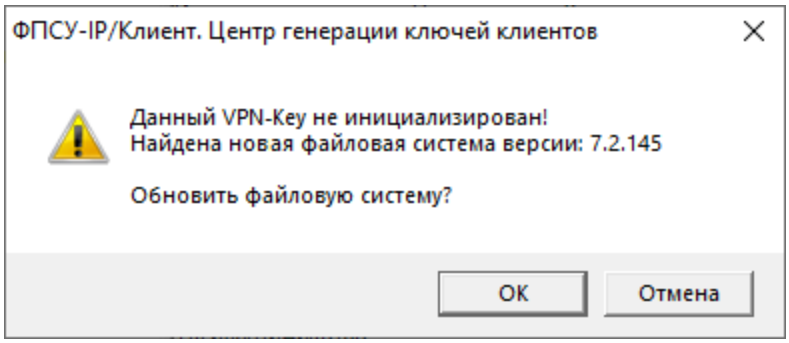

Рисунок 85 - Сообщение о новой версии файловой системы

Для обновления файловой системы до указанной версии нажать кнопку «ОК».

На экран будет снова выведено окно о загрузке файловой системы «VPN-Key» и сообщение об успешном обновлении, в котором требуется нажать кнопку «ОК».

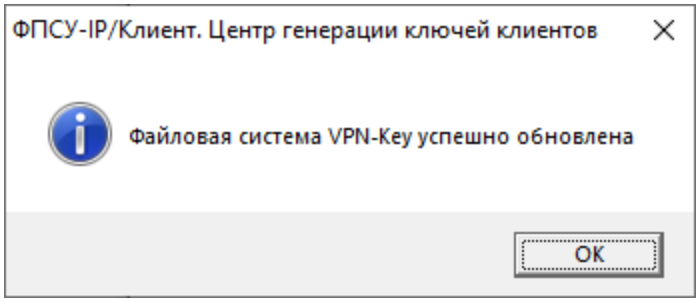

Рисунок 86 - Обновление файловой системы

5. Откроется окно для ввода регистрационных данных об устройстве «VPN-Key».

Данные сведения заполняются опционально. После заполнения нажать кнопку «ОК».

Данные сведения могут быть изменены при переинициализации пользователя.

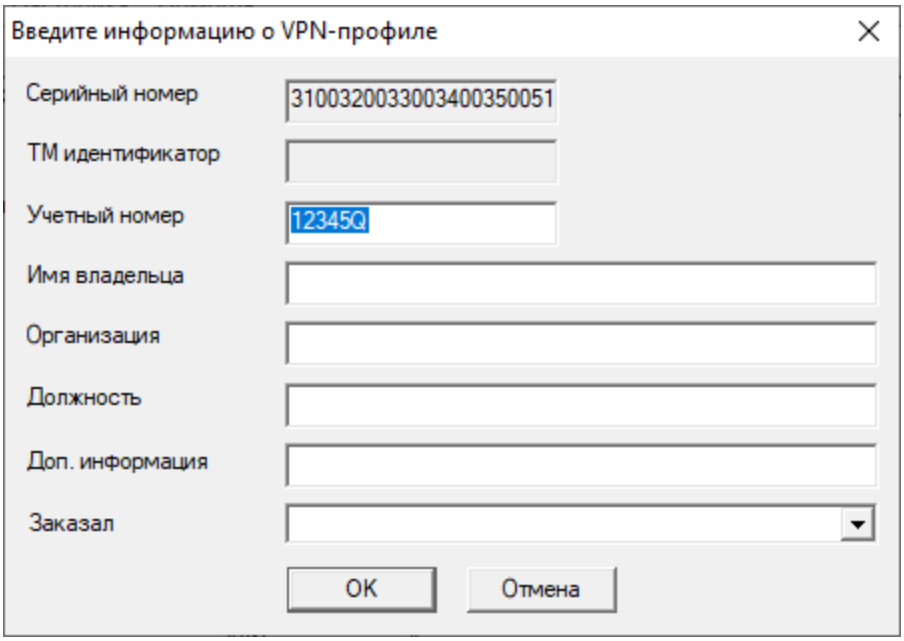

Рисунок 87 - Окно ввода сведений об устройстве VPN-Key

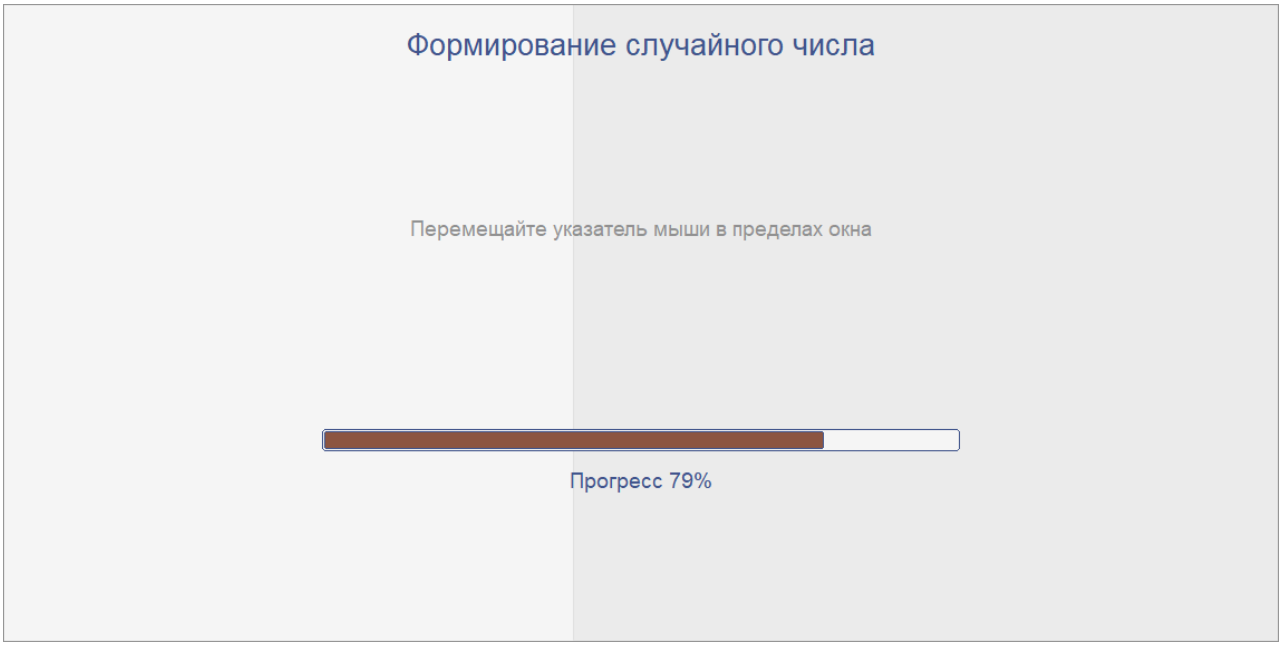

Рисунок 88 - Формирование случайного числа

7. Откроется окно ввода новых идентификаторов, в котором необходимо подтвердить сгенерированные программой случайным образом идентификационные коды для пользователя (имеющего права оператора) и администратора (обладающего правом менять рабочие параметры ФПСУ-IP/Клиента) или ввести свои PIN-коды.

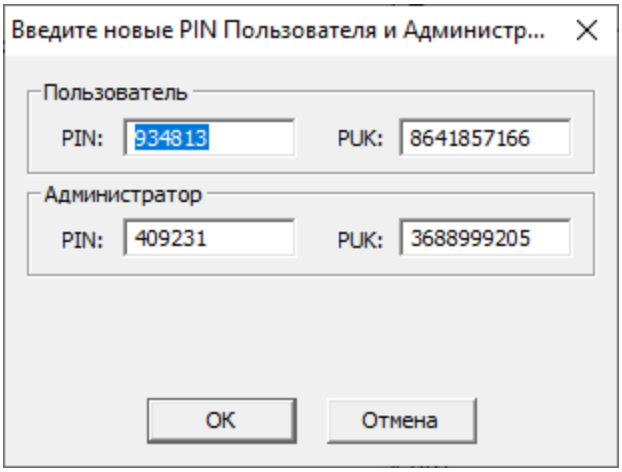

Рисунок 89 - Коды доступа

На экран будет выдан запрос на формат записи ключевых данных в устройство «VPN-Key».

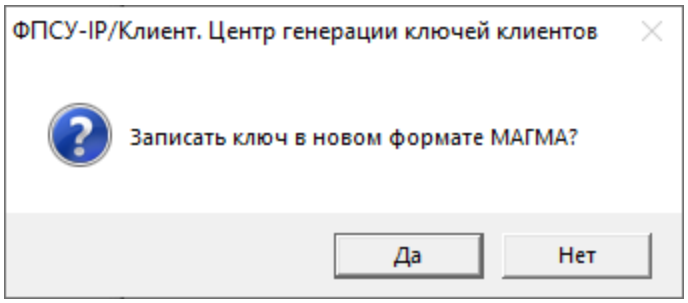

Рисунок 90 - Выбор формата записи ключей

По нажатию кнопки «Да» ключ записывается в «VPN-Key» с признаком поддержки алгоритмов шифрования в соответствии с ГОСТ 34.12–2015 (блочный шифр «Магма»), по нажатию кнопки «Нет» - с признаком поддержки алгоритмов шифрования в соответствии с ГОСТ 28147-89.

8. По нажатию кнопки «ОК» будет выдано окно выбора конфигурации для пользователя инициализируемого устройства «VPN-Key», в котором предоставляется возможность выбрать одну из ранее созданных конфигураций или создать новую (см. пункт «Создание шаблона конфигурации VPN-профиля»). Можно пропустить этот пункт, и внести изменения в конфигурацию устройства

позднее, с помощью PIN-кода администратора.

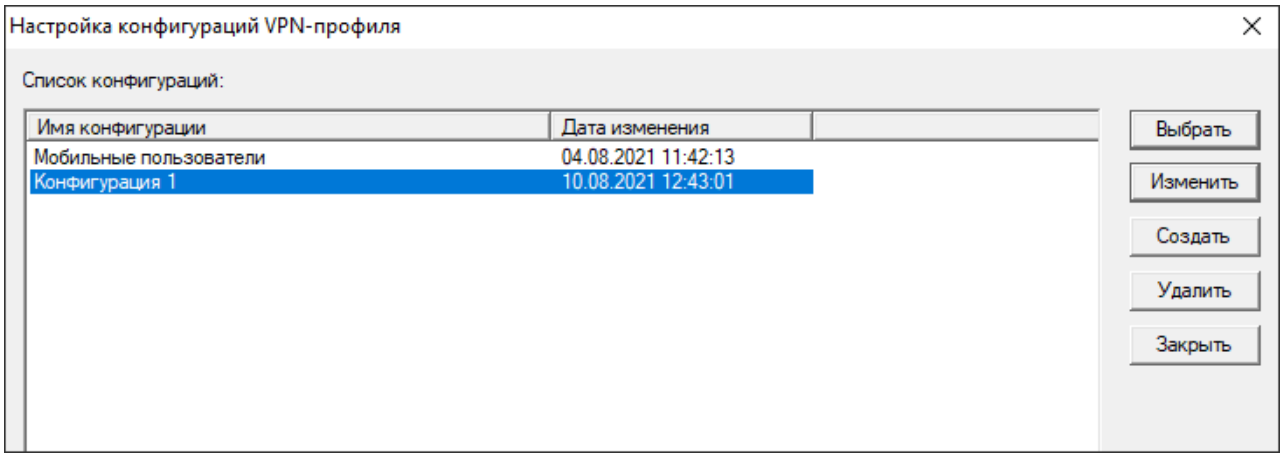

Рисунок 91 - Окно со списком конфигураций

На экран будет выдано окно с сообщением об успешной инициализации пользователя.

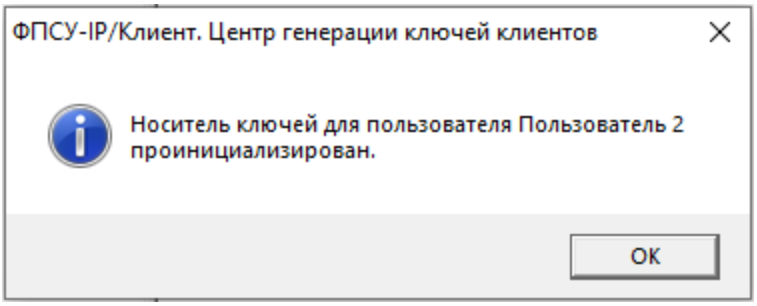

Рисунок 92 - Пользователь инициализирован

Информацию о версиях микрокода и файловой системы проинициализированного устройства «VPN-Key» можно по кнопке «Информация о VPN-Key», , панели инструментов.

5. 15. Подключение VPN-Key к ЦГКК и получение информации о VPN-Key

Информацию о версиях микрокода и файловой системы проинициализированного устройства «VPN-Key» можно по кнопке «Информация о VPN-Key», , панели инструментов. Эта кнопка становится активной только после подключения VPN-Key к USB-разъему ПК. При нажатии на кнопку отображается следующая информация:

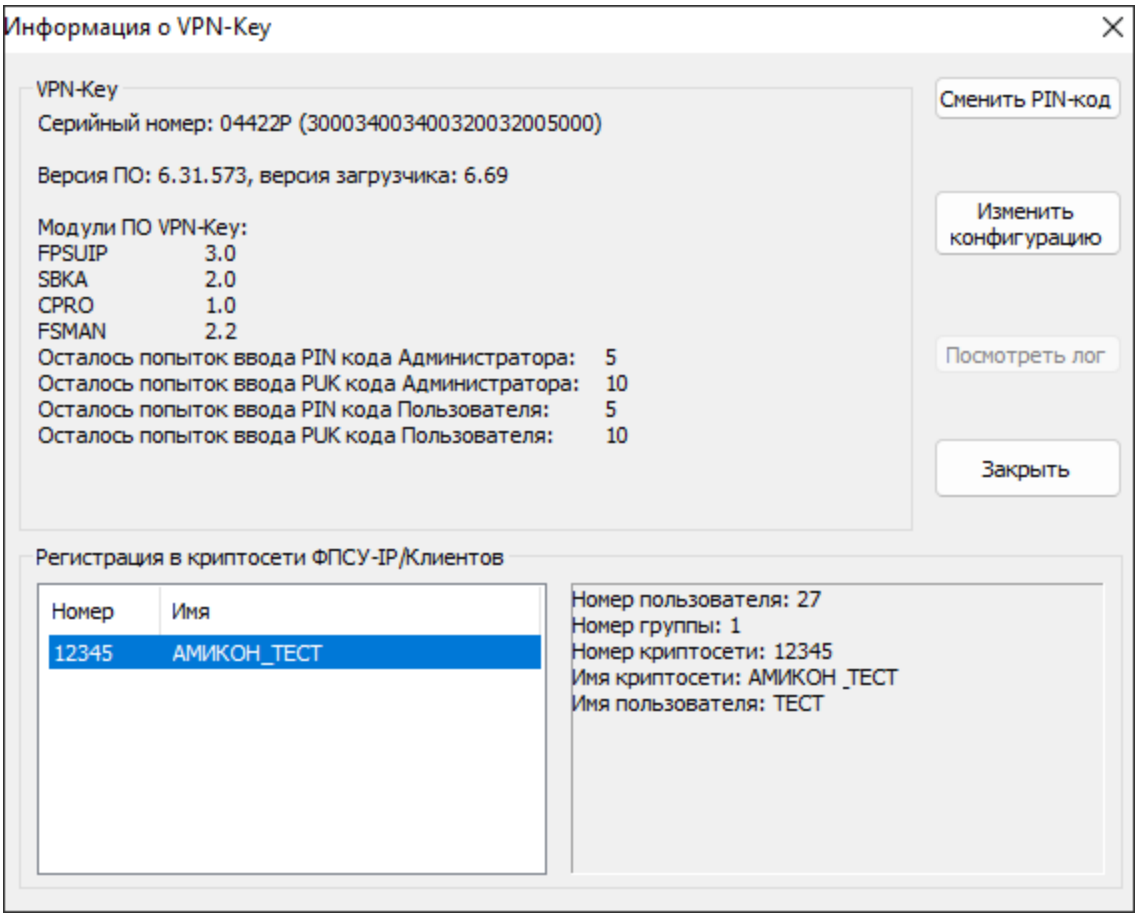

Рисунок 93 - Информация о VPN-Key

В открывшемся окне предоставляется возможность просмотреть информацию о серийном номере, версиях микрокода изагрузчика, модулях ПО подключенного устройства «VPN-Key» и количестве оставшихся попыток ввода PIN- и PUK-кодов Пользователя и Администратора. Кроме того, в данном окне отображается информация о криптосетях, в которых зарегистрирован подключенный VPN-Key (в том числе номер и имя пользователя, номер круппы, номер и наименование Криптосети). Так же по одноименным кнопкам в данном окне можно изменить PIN-код, конфигурацию и посмотреть журнал происходивших в работе VPN-Key событий.

5. 16. Горячие клавиши программы ЦГКК

Для удобства выполнения стандартных задач, в программе предусмотрен ряд «горячих» клавиш быстрого вызова необходимых команд.

Список горячих клавиш можно вывести на экран путем выбора пункта «Горячие клавиши» меню «Помощь».

Комбинации клавиш для вызова команд:

<Ctrl+A> — загрузка ключа КА;

<Ctrl+C>, <Ctrl+Ins> — копирование выделенного текста в буфер обмена;

<Ctrl+E> — перезагрузка в ФС;

<Ctrl+F> — вызов панели поиска пользователя;

<Ctrl+K> — запуск процедуры загрузки общесистемного ключа выбранной Криптосети Клиентов в оперативную память ПЭВМ;

<Ctrl+V>, <Shift+Ins> — вставка текста из буфера обмена;

<Ctrl+Enter> — ввод общесистемного ключа или инициализация пользователя;

<Ctrl+I > — информация о пользователе;

<Ctrl+L > — информация о пользователе КА;

<Del> — удаление пользователя/группы;

<Enter> — запуск процедуры инициализации пользователя, если курсор установлен на пользователе;

<F3> — найти далее с теми же условиями;

<Ins> — создание новой группы (если курсор установлен на Криптосети) или нового пользователя (если курсор установлен на группе);

<Tab> — переход в следующую панель;

<Shift+Tab> — переход в предыдущую панель.

5. 17. Просмотр сведений о программе

Для получения справочной информации о программе ЦГКК необходимо войти в основное меню и выбрать пункт «О программе» меню «Помощь».

На экран будет выдано информационное окно, отображающее:

- название программы и номер текущей версии (в приведенном на рисунке примере «модификация 7.0»);

- название организации-разработчика программы..

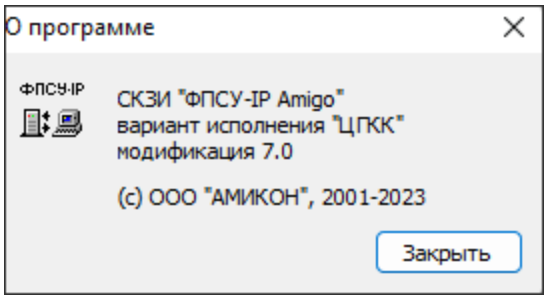

Рисунок 94 - Справочная информация о программе

6. Контроль целостности программы ЦГКК

Полная информация по использованию программы WinFPSUHash.exe для создания эталонных контрольных сумм и проведения проверки указанных файлов предоставлена в документе «Программа контроля целостности файлов. Руководство оператора», а также на сайте в разделе Проверка целостности файлов по контрольной сумме.

6. 1. Контроль целостности до установки

Контроль целостности инсталляционного модуля программы «Центр генерации ключей Клиентов» осуществляется на начальном этапе установки ЦГКК (до запуска файла CGKK_7_0.exe), и производится при помощи специальной программы WinFPSUHash.exe.

При проверке целостности ЦГКК программой WinFPSUHash.exe используется поставляемый вместе с ЦГКК файл install.hsh, содержащий эталонные контрольные данные, сравнение с которыми производится при проверке.

Контроль целостности осуществляется запуском программного модуля WinFPSUHash.exe из командной строки операционной системы Windows, из предварительно запущенной командной оболочки (например, cmd или PowerShell) или с помощью пункта «Выполнить» меню «Пуск», указывается полный путь к программному модулю с параметром проверки по файлу хэша и дополнительным параметром install.hsh. Программа WinFPSUHash.exe должна запускаться из того же каталога, в котором находится файл CGKK_7_0.exe.

```
C:\Users\zak.v.y.AMICON\Desktop>C:\Users\zak.v.y.AMICON\Desktop\7.0_Cert_2023\WinFPSUHash.exe -C install.hsh

Программа контроля целостности файлов. Версия 2.0, (C) ООО "АМИКОН", 2022

Проверка хэш-кода на "Amicon CGKK installer for Windows"
Файл: ".\CGKK_7_0.exe"
Алгоритм хэш-кода: ГОСТ Р 34.11-2012
Эталонный хэш-код:    6ADBE29CD084027A4CF0BE7B04FC549450181E7AAEF12DC3B5FC84C3709838D3
Рассчитанный хэш-код: 6ADBE29CD084027A4CF0BE7B04FC549450181E7AAEF12DC3B5FC84C3709838D3
Результат: Верно. Рассчитанный хэш-код совпадает с эталонным.

Отчет: "install.lst"
```

Рисунок 95 - Проверка целостности по файлу с хэша

После отработки программы результаты проверки будут выданы в текстовом виде на экран монитора.

При совпадении полученных данных с эталоном в окне проверки будет выведена строка-сообщение: «Хэш верен». Инсталляция возможна только в этом случае.

Если в результате работы программы контроля целостности появляется сообщение о

нарушении целостности файла CGKK_7_0.exe, рекомендуется прекратить установку ЦГКК.

6. 2. Первоначальный контроль целостности после установки

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

Контроль целостности осуществляется при помощи программы WinFPSUHash.exe, при этом используется поставляемые вместе с ЦГКК файлы KeyGen.hsh, AConfig.hsh, Grn.hsh, содержащие контрольные данные.

Для выполнения первоначального контроля целостности после установки следует:

- Открыть каталог Filehash в рабочем каталоге программы ЦГКК (при установке по умолчанию это каталог «%Program Files%\AMICON\Centre FPSU-IP»);
- Запускать программу проверки WinFPSUHash.exe из командной строки операционной системы Windows, указывая путь к программе с дополнительными параметрами KeyGen.hsh, AConfig.hsh, Grn.hsh.Запустить программу проверки WinFPSUHash.exe из командной строки операци-онной системы Windows, указывая каждый раз путь к программе с дополнительными параметрами KeyGen.hsh, AConfig.hsh, Grn.hsh.

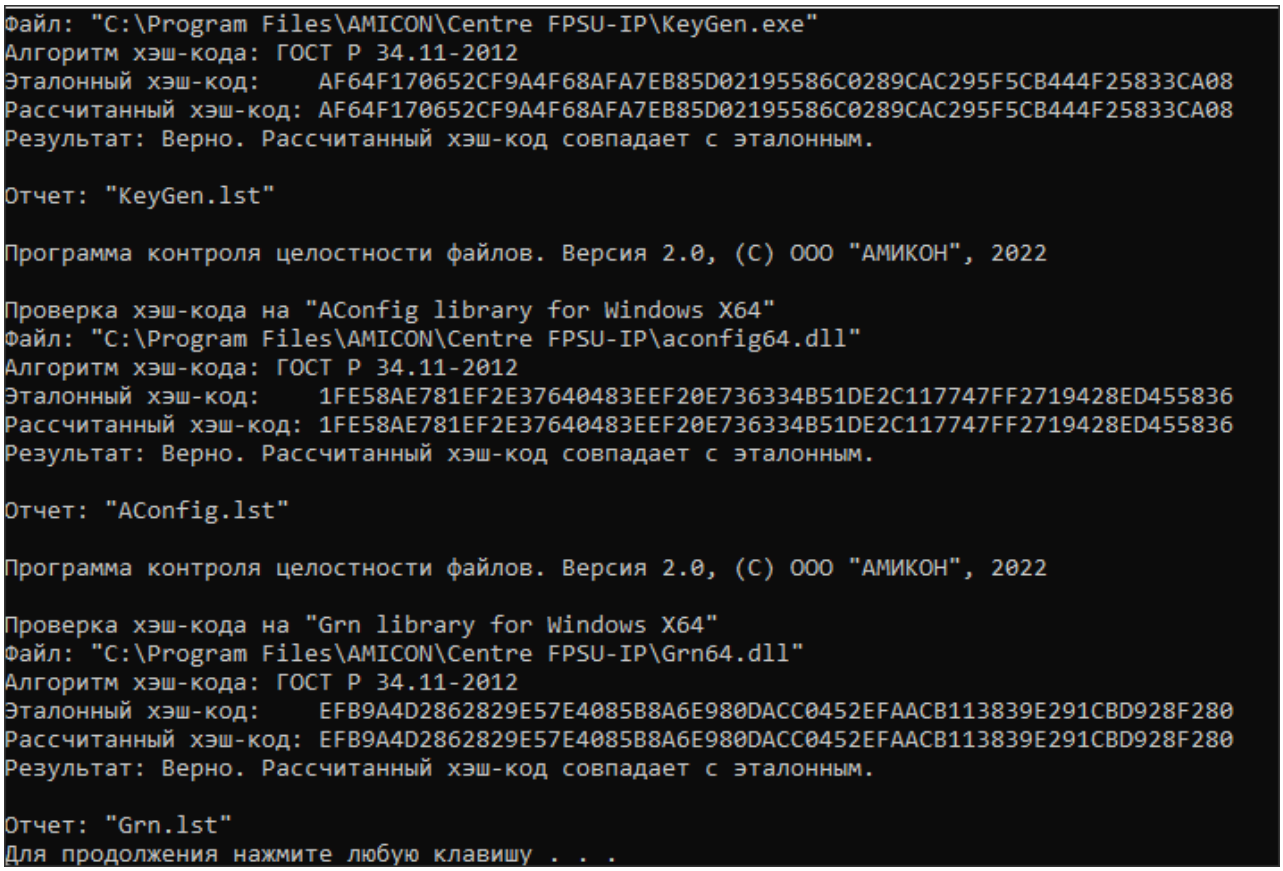

Рисунок 96 - Запуск программы проверки WinFPSUHash.exe

После отработки программы результаты проверки будут выданы в текстовом ви-де на экран монитора. Полученные контрольные суммы следует сравнить с эталонными контрольными суммами для используемой версии программы ЦГКК, указанными в формуляре.

При нарушении целостности программных модулей ЦГКК, необходимо повтор-но установить программу с инсталляционного носителя.

6. 3. Контроль целостности в процессе эксплуатации

Для использования ЦГКК как СКЗИ класса КС2, контроль целостности программы в процессе эксплуатации можно осуществлять средствами сертифицированного по Требованиям ФСБ АПМДЗ.

В остальных случаях, контроль целостности программы в процессе эксплуатации следует осуществлять программой WinFPSUHash.exe, запуская её с параметрами командной строки FPSUHash.hsh, KeyGen.hsh, AConfig.hsh, Grn.hsh или запуском файла CheckHashes.cmd.

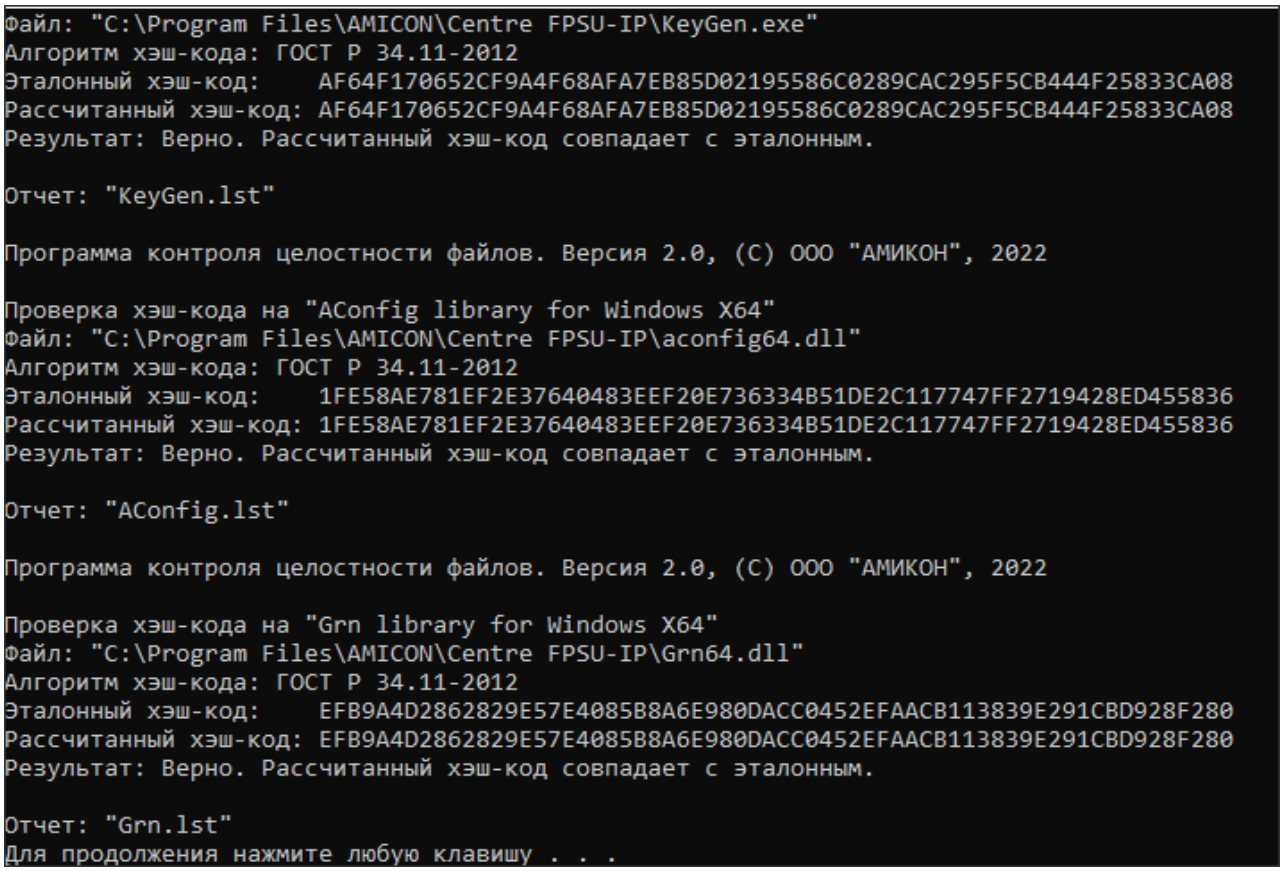

Рисунок 97 - Запуск файла CheckHashes.cmd

Контролю целостности подлежит программные модули программы ЦГКК, исполняемые файлы ОС, и исполняемые файлы сторонних программ, функционирующих совместно с программой ЦГКК.

После отработки программы результаты проверки будут выданы в текстовом виде на экран монитора. Полученные контрольные суммы следует сравнить с эталонными для используемой версии программы ЦГКК, исполняемых файлов ОС и сторонних программ.

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

Если в результате работы программы проверки появляется сообщение о нарушении целостности контролируемых файлов ОС и/или сторонних программ, работающих совместно с программой ЦГКК, дальнейшая эксплуатация ЦГКК не допускается. Следует проанализировать причину изменения контролируемых файлов, и затем, в случае необходимости, переустановить контролируемые файлы.

7. Удаление ЦГКК

Для удаления программного обеспечения ЦГКК с компьютера необходимо запустить файл «amivpn-uninst.exe», находящийся в каталоге программы, или выполнить удаление стандартным для Windows образом через последовательность команд «Панель управления» → «Установка и удаление программ», найдя приложение ««ПАК 'ФПСУ-IP/Клиент' 7.0 СКЗИ 'ФПСУ-IP/Клиент' Изделие Центр генерации ключей клиентов»» и нажав кнопку «Удалить».

Откроется окно, в котором отобразится путь к папке с установленным программным обеспечением.

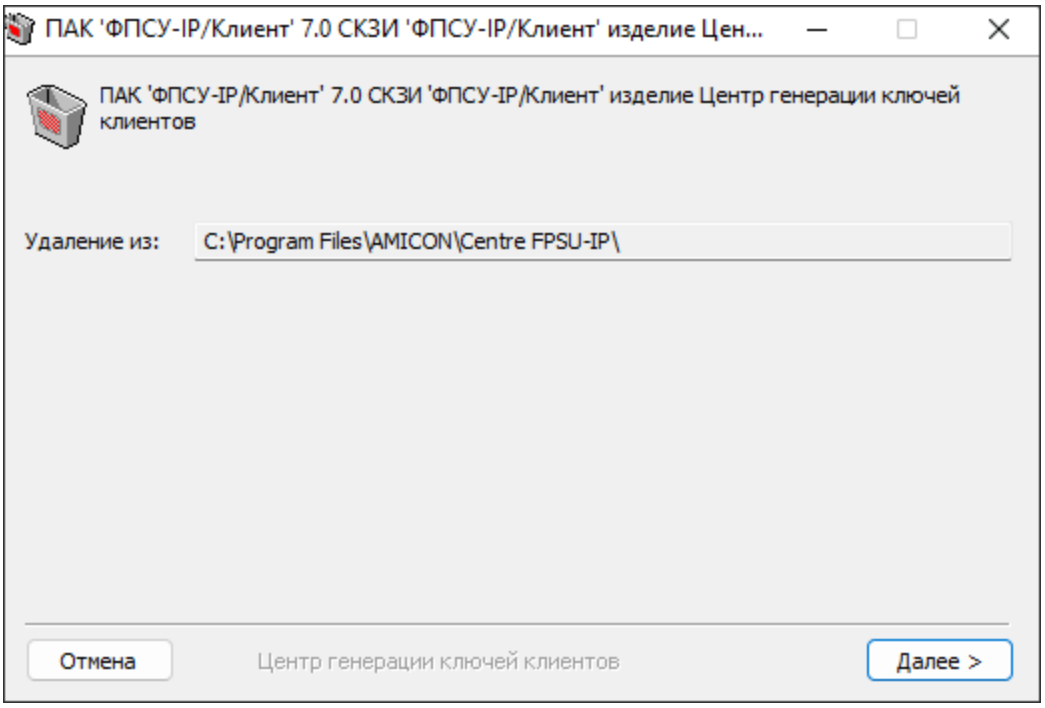

Рисунок 98 – Отображение папки для удаления ПО

После нажатия кнопки «Далее» откроется окно, в котором необходимо выбрать компоненты для деинсталляции и нажать кнопку «Удалить».

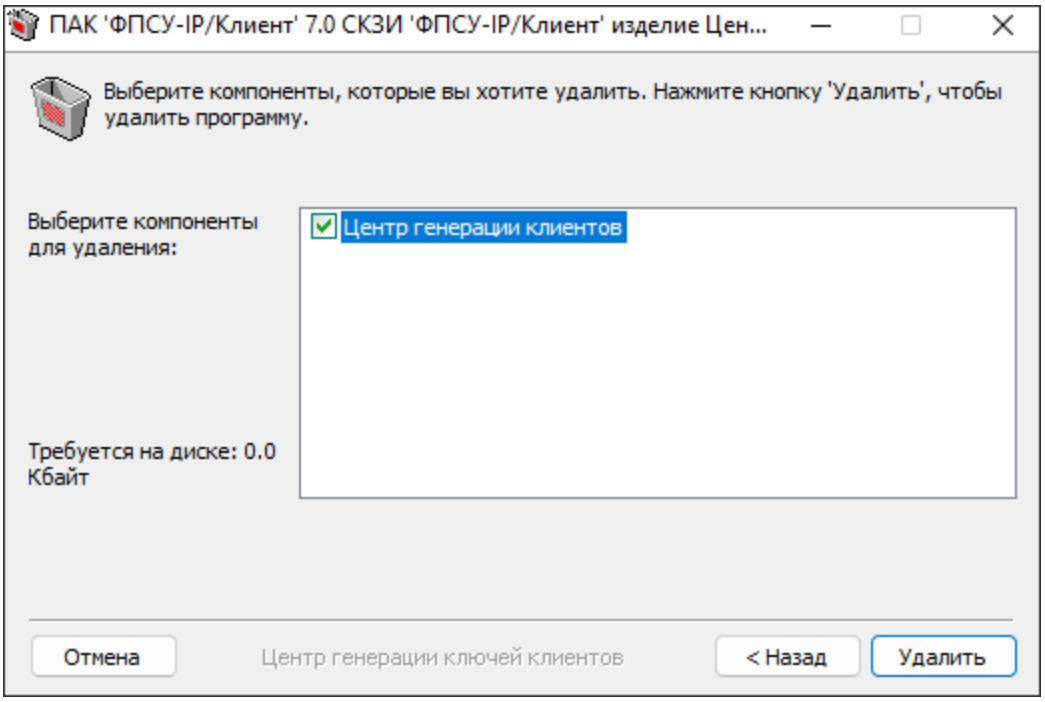

Рисунок 99 – Выбор компонент ПО для удаления

Будет выполнен переход в окно прогресса удаления программного обеспечения, по завершению которого состояние перейдет в статус «Готово». Для завершения удаления необходимо нажать кнопку «Закрыть»:

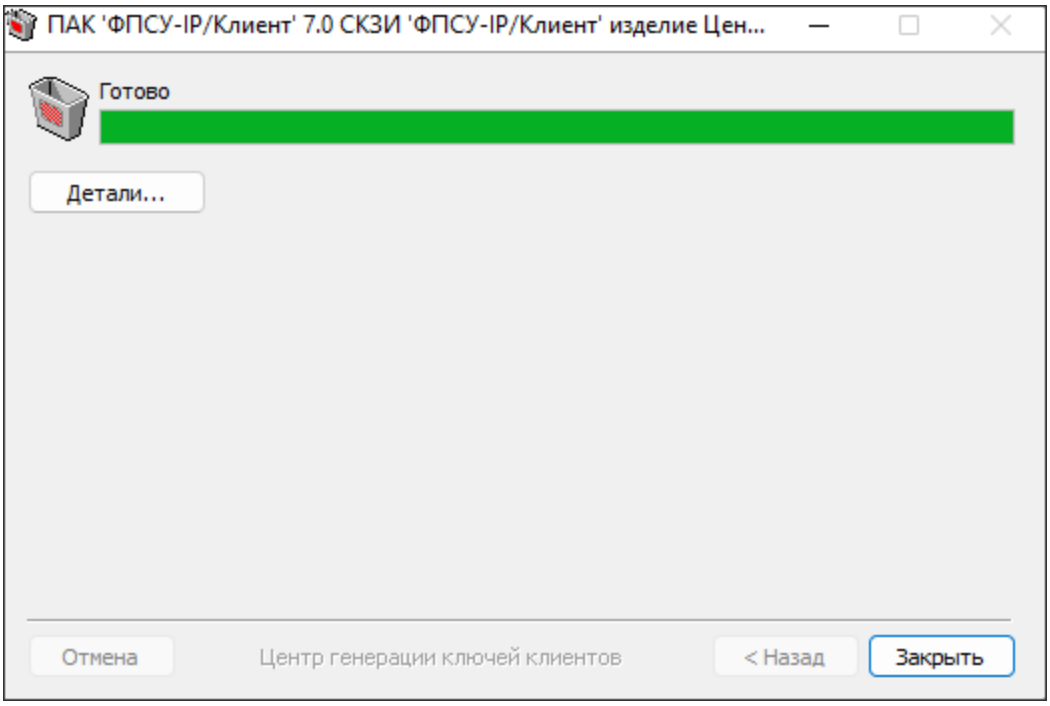

Рисунок 100 – Удаление ПО завершено

После завершения процесса деинсталляции рекомендуется выполнить перезагрузку ОС компьютера.