ООО «АМИКОН»

Программный и программно-аппаратный комплекс ФПСУ-IP/Клиент для Windows v.7.0 BETA

Руководство пользователя

РОФ.ПЕРС.109-01

Количество листов 109

2023

Аннотация

Документ предназначен для пользователей ФПСУ-IP/Клиента для Windows, сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением комплексов ФПСУ-IP. В документе содержатся общие сведения о средстве криптографической защиты информации «ФПСУ-IP/Клиент для Windows», приведен перечень необходимых организационно-технических мер и дано описание последовательности действий при установке, настройке параметров функционирования в процессе эксплуатации и в аварийных ситуациях.

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

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

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

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

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

On-line документация по продукции ООО "АМИКОН": https://wiki.amicon.ru/

Электронная почта: info@amicon.ru

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

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

Содержание

1. Список используемых сокращений и определений

PIN-код администратора VPN-профиля	цифровой код, требующийся для работы ФПСУ-IP/Клиента с этим VPN-профилем и для системной настройки VPN-профиля;
устройство VPN-Key/RKL, RKL-токен	электронный идентификатор на базе устройства «VPN-Key» для «ФПСУ-IP/Клиент» с RKL функциональностью. Предназначен для удаленной установки на АРМ пользователя ФПСУ-IP/Клиент лицензии на использование Программного Клиента и VPN-профилей пользователей Программного Клиента.
VPN	Virtual Private Network, виртуальная частная сеть передачи данных, создаваемая поверх существующей общедоступной или частной сети передачи данных;
VPN-Key	программно-аппаратное устройство «VPN-Key/Client» с установленным микрокодом из состава СКЗИ «ФПСУ-IP/Client», являющееся ключевым носителем и реализующее алгоритмы криптографических преобразований и выработки случайных последовательностей;
VPN-туннель	виртуальный канал связи, защищенный криптографическими методами (двусторонней аутентификацией и шифрованием передаваемых данных);
АРМ пользователя ФПСУ-IP/Клиент, АРМ Клиента	автоматизированное рабочее место, ПЭВМ или мобильное устройство на которое установлено СКЗИ «ФПСУ-IP/Клиент», изделие «Программный клиент для Windows» или «Аппаратный клиент для Windows», с введенной ключевой информацией или подключенным устройством «VPN-Key/Client»;
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	устройство, предназначенное для записи и хранения данных, на котором размещена ключевая информация;
Криптосеть	Криптосеть ФПСУ-IP/Клиентов, совокупность ФПСУ-IP/Клиентов, использующих ключи, выработанные в ЦГКК на основе единого общесистемного ключа; каждая Криптосеть имеет собственное имя и

	уникальный номер, присвоенные производителем;
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;
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;
Программный Клиент	Изделие «Программный клиент для Windows» из состава СКЗИ «ФПСУ-IP/Клиент», используется для создания VPN-туннеля без применения устройства «VPN-Key/Client»;
Программно-аппаратный Клиент	Изделие «Аппаратный клиент для Windows» из состава СКЗИ «ФПСУ-IP/Клиент», используется для создания VPN-туннеля с применением устройства «VPN-Key/Client»;
Пользователь	пользователь Криптосети,
ПЭВМ	персональная электронная вычислительная машина, персональный компьютер;
СКЗИ	средство криптографической защиты информации;
ФПСУ-IP	Изделие «Криптомаршрутизатор» из состава СКЗИ «ФПСУ-IP»;
ФПСУ-IP/Клиент	общее название для изделий «Программный клиент для Windows» и «Аппаратный клиент для Windows» из состава СКЗИ «ФПСУ-IP/Клиент»;
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую;
ЦГКК	Изделие Центр генерации ключей клиентов из состава СКЗИ «ФПСУ-IP/Клиент»;

2. Общие сведения о ФПСУ-IP/Клиенте

В настоящем руководстве описывается работа программного и программно-аппаратного ФПСУ-IP/Клиента версии 7.0.19 beta для рабочих станций под управлением ОС Windows. ВНИМАНИЕ! Программное обеспечение находится в статусе Beta.

ФПСУ-IP/Клиент является средством защиты информационных обменов отдельных рабочих станций от несанкционированного доступа. ФПСУ-IP/Клиент предназначен для построения защищенных каналов связи между рабочей станцией и ФПСУ-IP, кроме того, ФПСУ-IP/Клиент может выполнять функции локального межсетевого экрана, принимая и передавая сетевые пакеты в соответствии с задаваемыми правилами фильтрации.

Механизм защиты канала связи заключается в том, что поверх существующей общедоступной или частной сети передачи данных создается VPN-туннель между ФПСУ-IP/Клиентом и ФПСУ-IP, по которому IP-пакеты передаются в зашифрованном виде (шифрование передаваемой информации выполняется в соответствии с ГОСТ 28147-89), что обеспечивает целостность и конфиденциальность передаваемой информации. ФПСУ-IP/Клиентом поддерживается алгоритм МАГМА ГОСТ Р 34.12-2015 для шифрования трафика при установленном соединении с ФПСУ-IP, если ФПСУ-IP поддерживает этот алгоритм.

В VPN-туннеле производятся обязательные взаимные процедуры идентификации и аутентификации ФПСУ-IP/Клиента и ФПСУ-IP, как при установлении защищенного соединения, так и в процессе передачи данных через VPN-туннель.

Для построения VPN-туннеля используется UDP-протокол. ФПСУ-IP принимает соединения Клиентов на 87 порт UDP. ФПСУ-IP/Клиент при соединении с ФПСУ-IP выбирает порт источника динамически, выше 1024.

Аутентификация взаимодействующих ФПСУ-IP/Клиента и ФПСУ-IP, а так же шифрование передаваемой в VPN-туннеле информации производятся с использованием ключей клиентов Криптосети, вырабатываемых при помощи программы ЦГКК. ЦГКК вырабатывает общесистемный ключ Криптосети клиентов, который может храниться в распределенном виде на нескольких носителях. На основе общесистемного ключа ЦГКК вырабатывает индивидуальные ключи клиентов, записываемые на ключевые носители и передаваемые на рабочие места клиентов.

ФПСУ-IP/Клиент после установки может быть использован как программно-аппаратный, так и как программный Клиент.

На ПЗУ или в устройстве VPN-Key хранятся VPN-профили, содержащие информацию об IP-адресе ФПСУ-IP, с которым ФПСУ-IP/Клиент устанавливает VPN-туннель, IP-адресах находящихся за ФПСУ-IP рабочих станций, к которым пользователь ФПСУ-IP/Клиента сможет получить защищенный доступ; уникальных системных номерах и имени, закрепленных за данным пользователем ФПСУ-IP/Клиента администратором ЦГКК.

При попытке установить соединение с ФПСУ-IP, у пользователя запрашивается PIN-код. Опционально, администратором ФПСУ-IP может быть подключена дополнительная авторизация у Raduis-сервера по логину и паролю.

При использовании устройства VPN-Key, вся необходимая для организации и защиты межсетевых соединений информация хранится в этом устройстве, и пользователь может соединяться с ФПСУ-IP с любого компьютера сети, на который установлено программное обеспечение ФПСУ-IP/Клиента. К одному компьютеру с установленным ПО ФПСУ-IP/Клиент может быть подключено до восьми устройств VPN-Key. В процессе работы пользователь имеет возможность переключаться на тот или иной VPN-Key.

ФПСУ-IP/Клиент по указанию пользователя может производить сжатие передаваемой через VPN-туннель информации, что может быть эффективно для низкоскоростных соединений.

Для защиты от несанкционированного доступа со стороны сети Интернет и блокирования нежелательных сетевых пакетов, ФПСУ-IP/Клиент при соединении с ФПСУ-IP может производить фильтрацию сторонних по отношению к VPN-туннелю пакетов данных. Часть фильтров на прием и/или передачу устанавливает администратор ФПСУ-IP при регистрации ФПСУ-IP/Клиента, администратор ФПСУ-IP/Клиента может установить дополнительные ограничения.

Фильтрация исходящих и входящих пакетов данных по задаваемым пользователем условиям может производиться ФПСУ-IP/Клиентом и в периоды отсутствия связи с ФПСУ-IP.

Во время существования VPN-туннеля с ФПСУ-IP, ФПСУ-IP/Клиент осуществляет автоматический сбор регистрационной информации о приеме и передаче пакетов на всех сетевых интерфейсах рабочей станции пользователя.

Общая схема применения ФПСУ-IP/Клиента совместно с ФПСУ-IP для организации защищенного доступа рабочих станций в защищаемую сеть приведена на рисунке ниже:

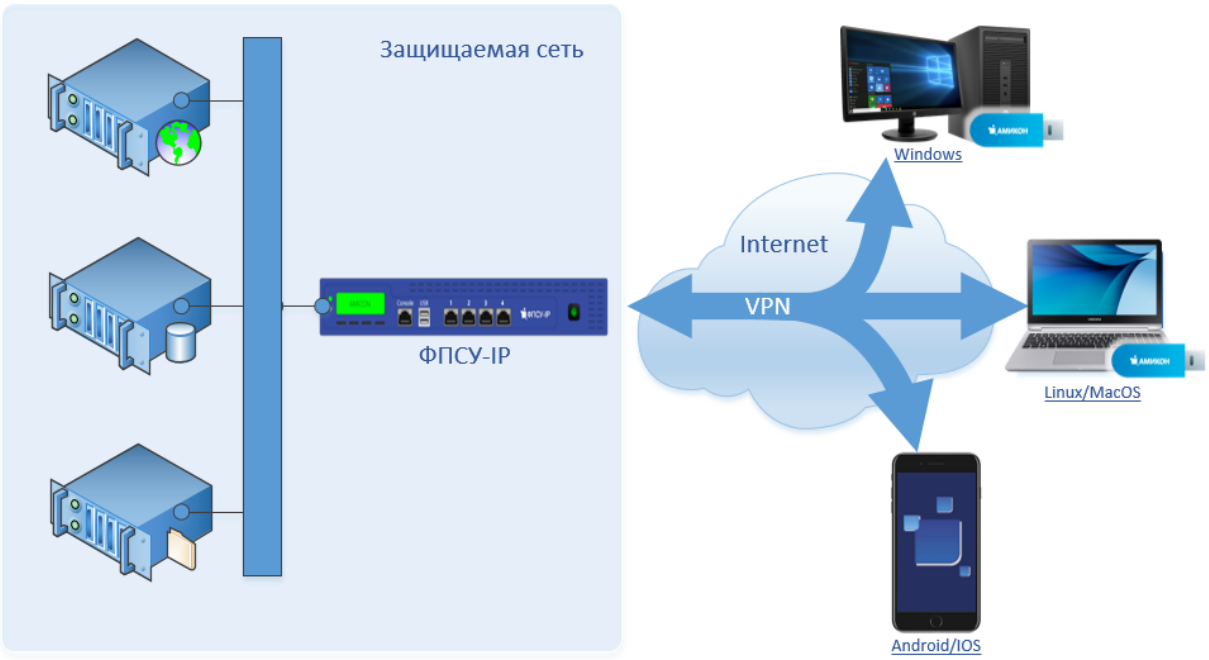


Рисунок 1 - Общая схема применения ФПСУ-IP/Клиента

3. Установка программного обеспечения

3.1. Системные требования

Для установки программного обеспечения компьютер должен отвечать следующим программным и аппаратным требованиям:

- операционная система:
  - 32-разрядная Windows Server 2008/7/8/8.1/10 X86;
  - 64-разрядная Windows Server 2008/Server 2008 R2/7/8/8.1/10/11/Server 2016/Server 2019/Server 2022;
- необходимое оборудование:
  - контроллер универсальной последовательной шины (для подключения с использованием программно-аппаратного Клиента);
  - сетевой адаптер;
  - монитор;
  - средства ввода (клавиатура, манипулятор типа "мышь" etc).

Для работы с программно-аппаратным Клиентом дополнительно необходимо устройство VPN-Key и персональные коды доступа к нему (PIN и PUK).

Рисунок 2 - Устройство VPN-Key

Для работы с Программным Клиентом помимо носителя с дистрибутивом программного обеспечения необходимы лицензия (серийный номер) и ключевая информация в виде VPN-профиля, переданная с ЦГКК доверенным образом (подробнее см. пункт Начало работы с Программным Клиентом)

3.2. Контроль целостности инсталляционного пакета

Перед установкой программного обеспечения ФПСУ-IP/Клиента на рабочую станцию требуется произвести контроль целостности дистрибутива. Проверка производится вычислением программой «WinFPSUHash.exe» хэш-функции на файл с дистрибутивом и сравнением полученного результата с контрольными данными.

Программа контроля целостности файлов «WinFPSUHash.exe» и файл с контрольными суммами INSTALL.HSH входит в комплект поставки ФПСУ-IP/Клиента.

Для выполнения проверки необходимо:

1. Убедиться, что в одном каталоге находятся:
   - установочный файл «AmiVPN_7_0_19b1_for_Windows.exe»;
   - программа контроля целостности файлов «WinFPSUHash.exe»;
   - файл с контрольной суммой установочного файла «INSTALL.HSH»;
   - пакетный файл «filehash.cmd», запускающий WinFPSUHash.exe в режиме проверки по файлу с контрольной суммой INSTALL.HSH;
2. Запустить«filehash.cmd».

Результат выполнения проверки будет выведен на экран, а также сохранен в текущий каталог в файл листинга «install.lst». Файл листинга содержит текст в кириллической кодировке и может быть открыт любым текстовым редактором.

При совпадении полученных данных с эталоном в окне проверки будет выведена строка-сообщение: «Хеш верен». Выведенные контрольные суммы дополнительно следует сверить с эталонными контрольными суммами, находящимися в паспорте или формуляре на изделие. Инсталляция программного обеспечения ФПСУ-IP/Клиента возможна только в случае сообщения «Хеш верен» и совпадения рассчитанных хешей с эталонными контрольными суммами.

Если программа проверки выдаст ошибку при выполнении контроля целостности, следует прекратить установку и обратиться к поставщику данного ФПСУ-IP/Клиента.

3.3. Процедура инсталляции

ФПСУ-IP/Клиент после установки может быть использован как Программно-аппаратный (при подключении устройства VPN-Key), так и как Программный Клиент (при установке лицензии на ПО и VPN-профиля).

Перед установкой следует в обязательном порядке выполнить контроль целостности программного обеспечения (см. предыдущий раздел).

Все скриншоты и примеры в данном документе приводятся для ОС Windows 10. При установке и использовании ПО в иных операционных системах во внешнем виде интерфейса, расположении иконок и пунктов меню могут наблюдаться отличия от приведенных скриншотов.

Для установки ПО ФПСУ-IP/Клиента на рабочую станцию необходимо выполнить следующие действия:

1. Убедиться в том, что устанавливаемое программное обеспечение предназначено именно для той операционной системы, под управлением которой работает компьютер, и запустить программу инсталляции «AmiVPN_7_0_19b1_for_Windows.exe».

В качестве первого этапа инсталляции будет предложено выбрать язык установки.

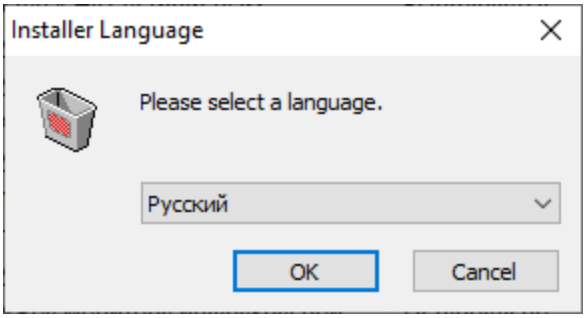


Рисунок 3 – Окно выбора языка

2. После выбора языка программа установки выдаст на экран лицензионное соглашение между пользователем ФПСУ-IP/Клиента и ООО «АМИКОН». Для продолжения установки необходимо прочитать лицензионное соглашение и нажать кнопку «Принимаю» для согласия с условиями лицензионного соглашения, или отказаться от инсталляции при помощи кнопки «Отмена».

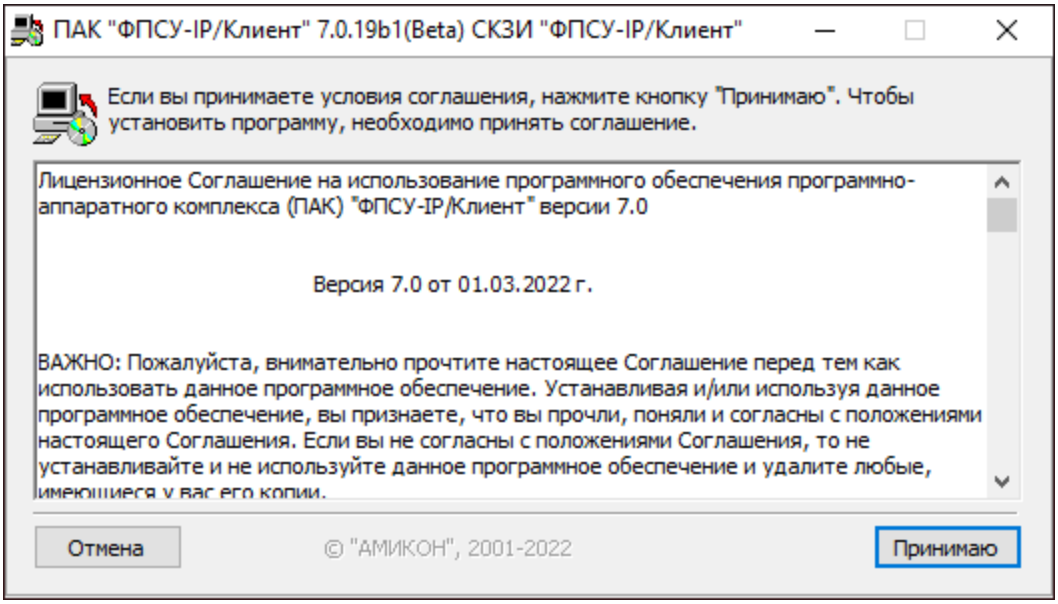


Рисунок 4 - Лицензионное соглашение

3. После принятия условий лицензионного соглашения необходимо выбрать установочные опции программного обеспечения ФПСУ-IP/Клиента.

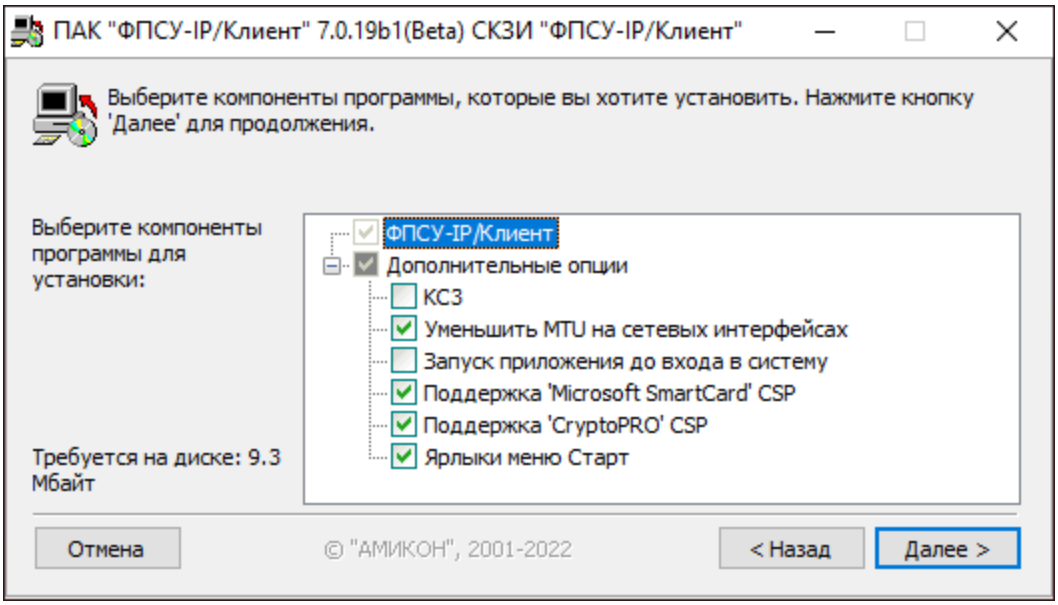


Рисунок 5 - Опции установки

- установка флага «КС3» запускает установку ФПСУ-IP/Клиента с дополнительными программными модулями для обеспечения уровня криптозащиты КС3;
- установка флага «Уменьшить MTU на сетевых интерфейсах» изменяет максимальный размер пакета при передаче в IP-сеть (англ. Maximum Transmission Unit, MTU) для всех установленных на рабочей станции сетевых адаптеров на 1400 байт. Не влияет на максимальный размер пакета, используемый протоколами

доступа в WAN-сеть (такие как PPP или PPPoE, используемые при модемных соединениях);

- установка флага «Запуск приложения до входа в систему» позволяет ФПСУ-IP/Клиент подключаться к ФПСУ-IP до авторизации пользователя в операционной системе;
- опции «Поддержка «Microsoft SmartCard» CSP» и «Поддержка «CryptoPro» CSP» реализованы для микрокода версии 5.30.303 и выше и означают возможность хранения в устройстве VPN-Key данных указанных криптопровайдеров;
- установка флага «Ярлыки меню Старт» создает в пусковом меню ОС ярлык «IP-Клиент» с ссылкой на устанавливаемое приложение.

ПО ФПСУ-IP/Клиент устанавливается как служба Windows с названием «Amicon FPSU-IP/Client service», запуск службы происходит при старте операционной системы в автоматическом режиме.

В левой нижней части окна отображается количество свободного дискового пространства, необходимое для установки отмеченных компонентов. Для продолжения установки необходимо нажать кнопку «Далее».

4. В следующем окне необходимо выбрать каталог на диске компьютера, в который инсталлируется ПО ФПСУ-IP/Клиента. По умолчанию программа будет установлена в «Program Files\AMICON\Client FPSU-IP», для выбора другого каталога необходимо воспользоваться кнопкой «Обзор».

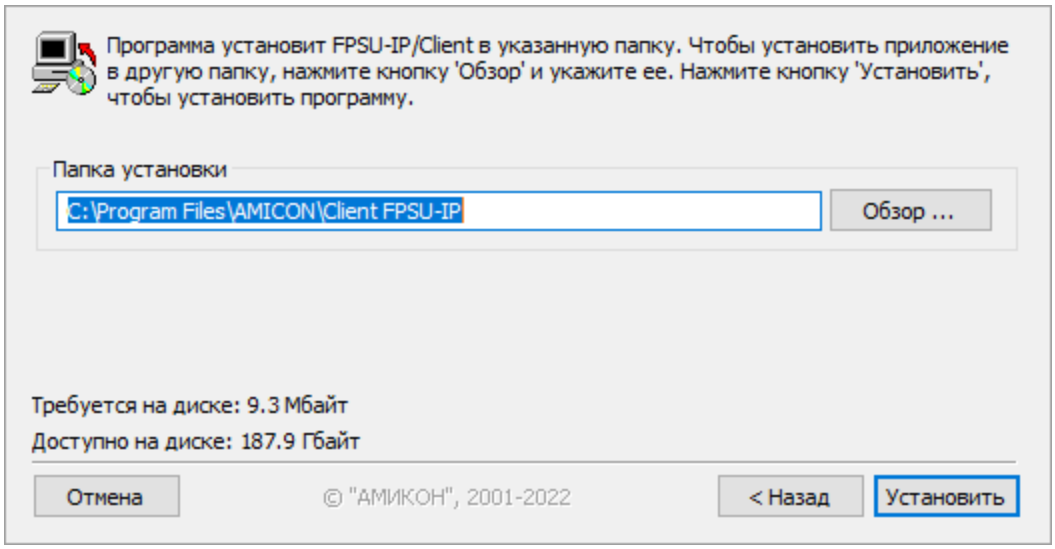


Рисунок 6 - Выбор каталога

В левой нижней части рабочего окна программы установки отображается требуемое количество свободного дискового пространства и доступное место на выбранном логическом диске. Для продолжения установки следует нажать кнопку «Установить».

5. В случае успешной установки программы на экран будет выдано сообщение о завершении работы инсталлятора - строка состояния установки приложения перейдет в статус «Готово». В журнале установки (по умолчанию это файл «Install.log» в рабочей папке программы) можно ознакомиться с отчетом, содержащем подробное описание процесса инсталляции. Для продолжения нажмите кнопку «Далее >».

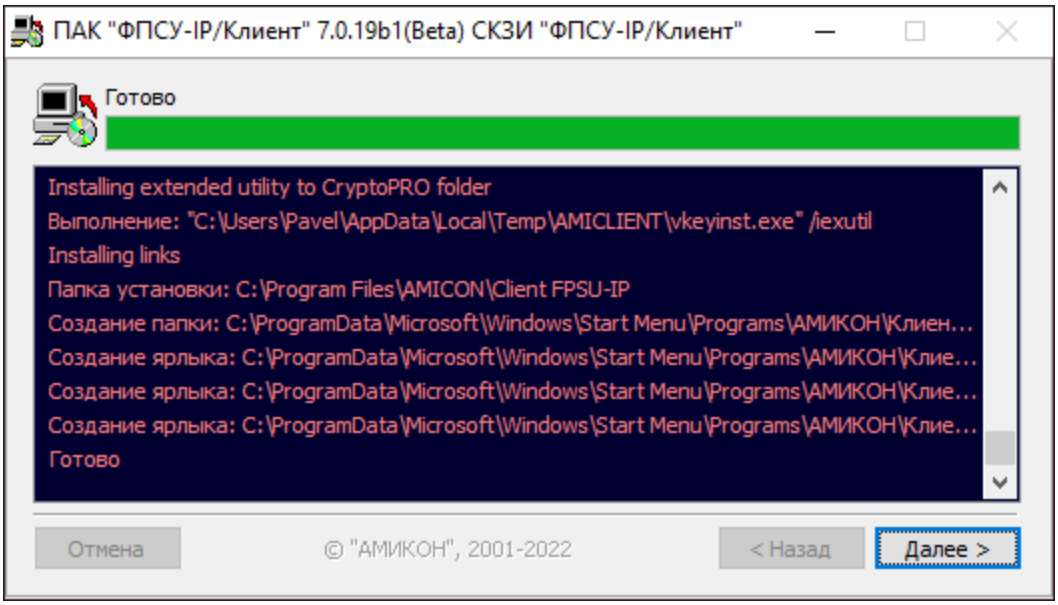


Рисунок 7 - Завершение установки ПО ФПСУ-IP/Клиент

6. Откроется окно успешного завершения установки. Для продолжения необходимо нажать кнопку «Закрыть»:

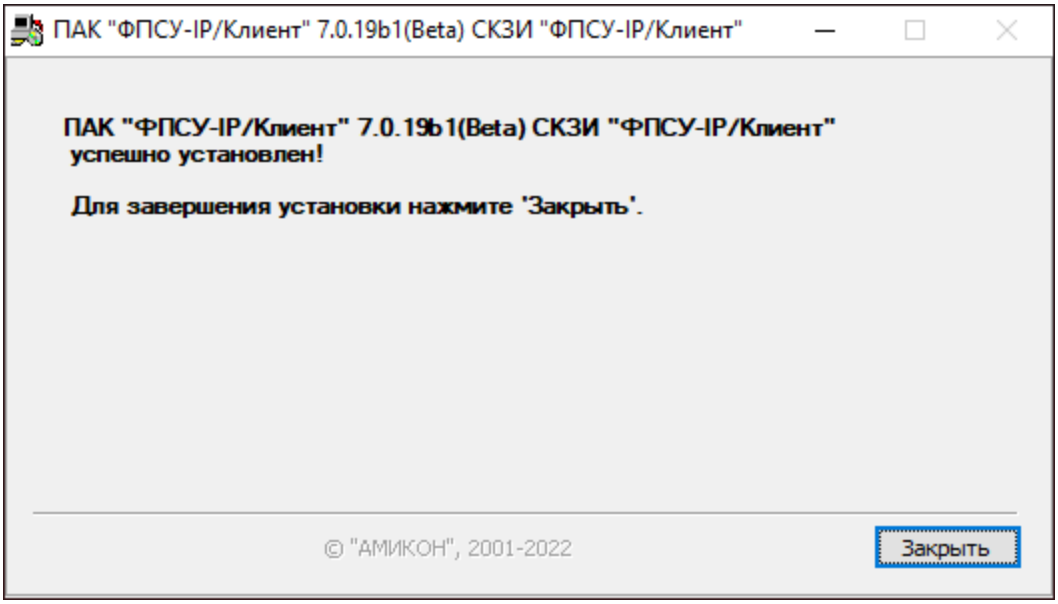


Рисунок 8 - Экран с сообщением об успешной установке

После будет выдано служебное оповещение, что изменения вступят в силу после перезагрузки компьютера. Рекомендуется произвести перезагрузку операционной системы компьютера, нажав кнопку «Да»:

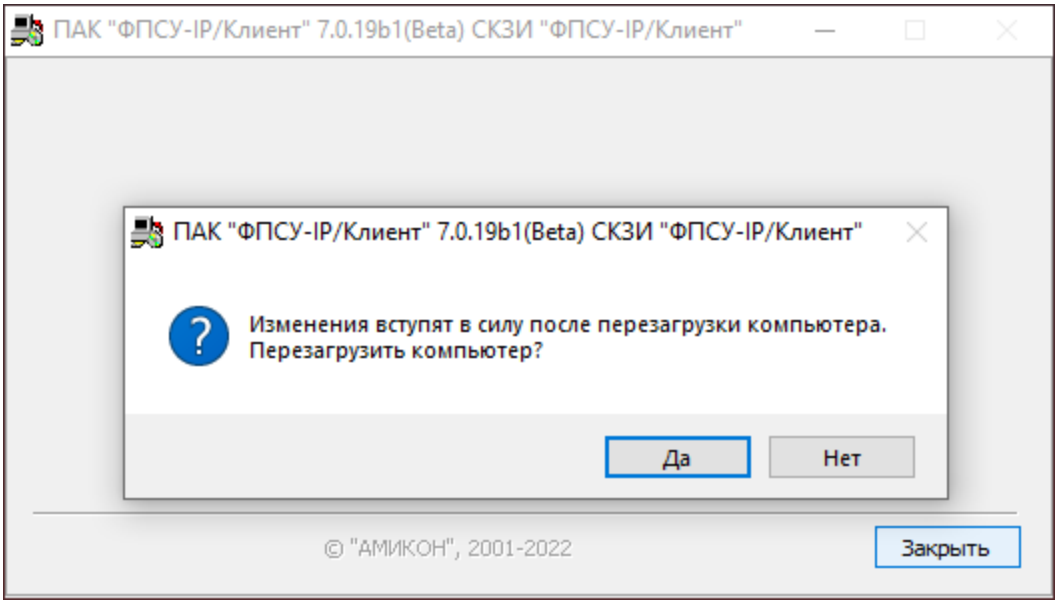


Рисунок 9 - Экран с сообщением об успешной установке

Когда установка программного обеспечения ФПСУ-IP/Клиента успешно завершится, на панели задач Windows в области уведомлений появится значок  . Через контекстное меню этого значка пользователю предоставляется доступ к настройкам и основным командам программы.

4. Запуск и основное меню ФПСУ-IP/Клиента

Программное обеспечение ФПСУ-IP/Клиента загружается автоматически, при старте операционной системы Windows (до регистрации и входа пользователя в операционной системе).

После регистрации и входа пользователя в области уведомлений на панели задач Windows отображается его значок:  .

При установке по умолчанию программное обеспечение ФПСУ-IP/Клиента находится в папке «SYSTEMDISK:\Program Files\AMICON\Client FPSU-IP». Возможен старт ПО ФПСУ-IP/Клиент вручную запуском исполняемого файла «ip-client.exe», находящегося в папке программного обеспечения.

Для вызова меню необходимо нажать правой клавишей мыши на значке программы. На экран будет выдано меню ФПСУ-IP/Клиента, содержащее следующие команды:

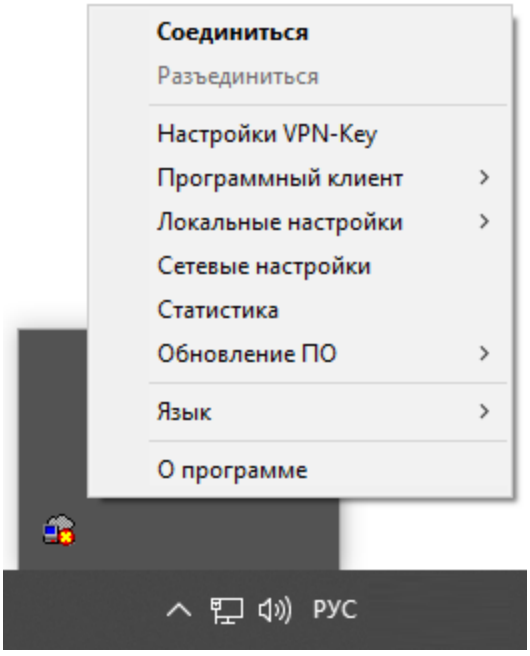


Рисунок 10 – Меню ФПСУ-IP/Клиента

- «Соединиться» - пункт для установления VPN-туннеля с ФПСУ-IP;
- «Разъединиться» - пункт для разрыва VPN-туннеля с ФПСУ-IP;
- «Настройки VPN-Key» - пункт для установки параметров работы программно-аппаратного ФПСУ-IP/Клиента в VPN-туннеле с ФПСУ-IP с использованием устройства VPN-Key;
- «Программный клиент» - пункт для установки параметров работы ФПСУ-IP/Клиента в VPN-туннеле с ФПСУ-IP с применением VPN-профилей

программных клиентов, без использования устройства VPN-Key;

- «Локальные настройки» - пункт для настройки локального межсетевого экрана ФПСУ-IP/Клиента и настроек безопасности, в частности настроек КС3;
- «Сетевые настройки» - пункт для настройки режима соединения ФПСУ-IP/Клиента с ФПСУ-IP через прокси-сервер SOCKS 5;
- «Статистика» - пункт для просмотра регистрационной информации о переданных данных при работе в VPN-туннеле с ФПСУ-IP;
- «Обновление ПО» - пункт для запроса с ФПСУ-IP обновленных версий программного обеспечения ФПСУ-IP/Клиента;
- «Язык» - пункт меню для выбора языка интерфейса, русского или английского;
- «О программе» - пункт для получения справочной информации.

5. Программно-аппаратный Клиент

5.1. Начало работы с программно-аппаратным Клиентом

Для начала работы с программно-аппаратным Клиентом требуется выполнить первичное подключение устройства VPN-Key к рабочей станции. Для этого необходимо выполнить следующие действия:

1. Подключить к USB-порту компьютера устройство VPN-Key. Для корректной работы с устройством VPN-Key в операционной системе должен присутствовать драйвер для устройства чтения смарт-карт (USB smart card reader), usbccid.sys. В случае его отсутствия в операционной системе драйвер устанавливается в процессе инсталляции программного обеспечения ФПСУ-IP/Клиент.

Если это первое подключение устройства VPN-Key к данному USB-порту рабочей станции, то операционной системе потребуется некоторое время для поиска драйвера устройства VPN-Key.

2. Проверить, закончилась ли установка драйвера успешно, можно через меню диспетчера устройств компьютера. При подключенном VPN-Key в диспетчере должен присутствовать объект «Устройство чтения смарт-карт».

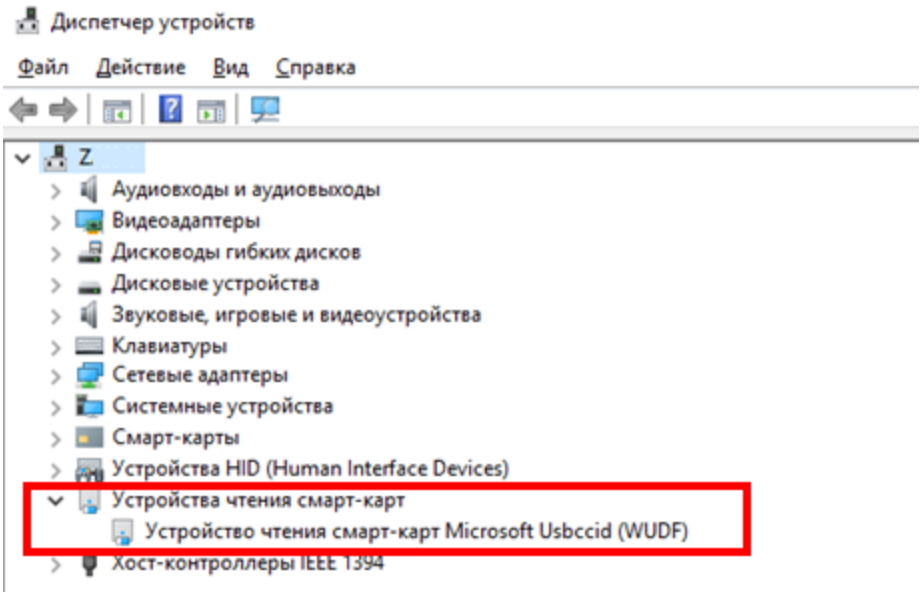


Рисунок 11 - К ПЭВМ подключено устройство VPN-Key

3. Если устройство VPN-Key успешно определилось операционной системой, на экране появится окно регистрации пользователя ФПСУ-IP/Клиент. Регистрация необходима для установления соединения ФПСУ-IP/Клиента с ФПСУ-IP и для настройки параметров работы.

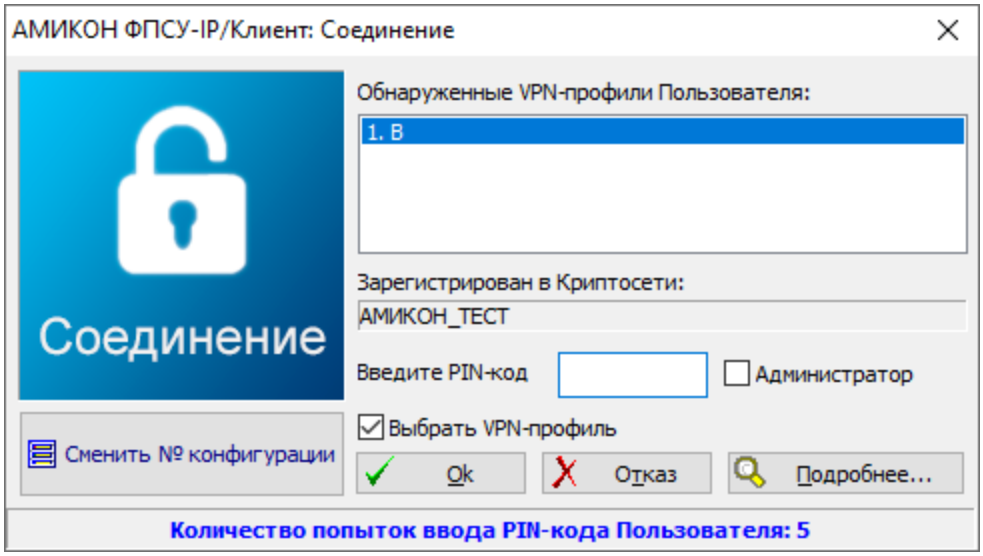


Рисунок 12 - Регистрация пользователя VPN-Key

Появление окна регистрации пользователя является показателем успешной установки программного обеспечения ФПСУ-IP/Клиента и драйверов в операционную систему рабочей станции.

5.2. Соединение программно-аппаратного Клиента с ФПСУ-IP

Основным назначением ФПСУ-IP/Клиента является организация соединения с ФПСУ-IP для безопасного доступа к защищенным ФПСУ-IP локальным сетям, рабочим станциям и серверам.

Для установления соединения с ФПСУ-IP необходимо выполнить следующие действия:

1. Подключить к USB-порту компьютера устройство VPN-Key.
2. В контекстном меню выбрать пункт «Соединиться» или дважды щелкнуть по иконке программы на панели задач.

На экран будет выдаваться сообщение о начале регистрации пользователя, отображающее данные VPN-профиля, авторизовавшегося в ФПСУ-IP/Клиенте последним.

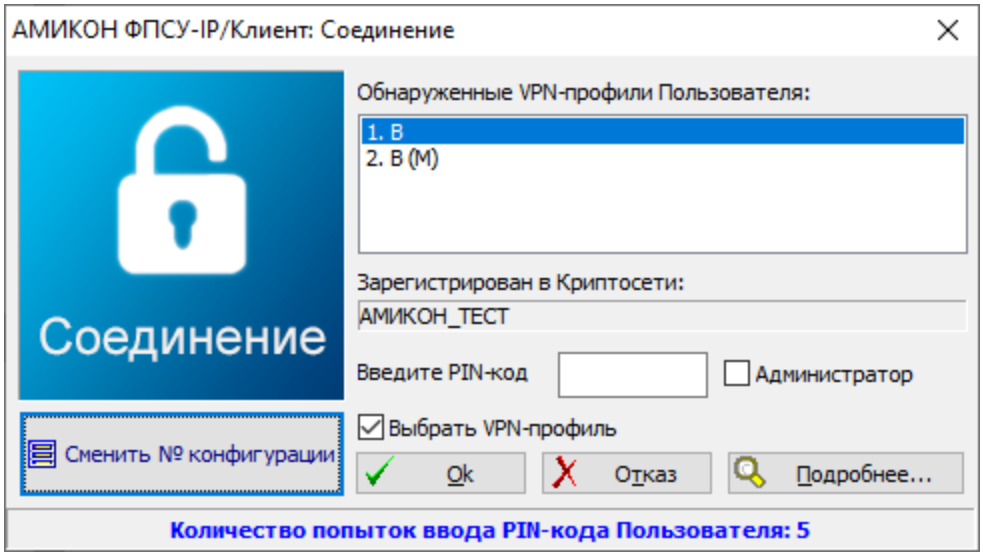


Рисунок 13 - Окно регистрации пользователя в ФПСУ-IP/Клиенте

В том случае, если последняя авторизация производилась для VPN-профиля пользователя программного Клиента, флаг «Администратор» в окне регистрации будет отсутствовать (раздел «Соединение Программного Клиента с ФПСУ-IP»).

При выборе опции «Выбрать VPN-профиль» появятся дополнительные возможности в окне интерфейса, позволяющие выбрать:

- настраиваемый VPN-Key из списка физически подключенных к данной машине устройств;
- редактируемую конфигурацию выбранного VPN-Key - нажатием кнопки «Сменить № конфигурации» и выбором нужной из выпадающего списка.

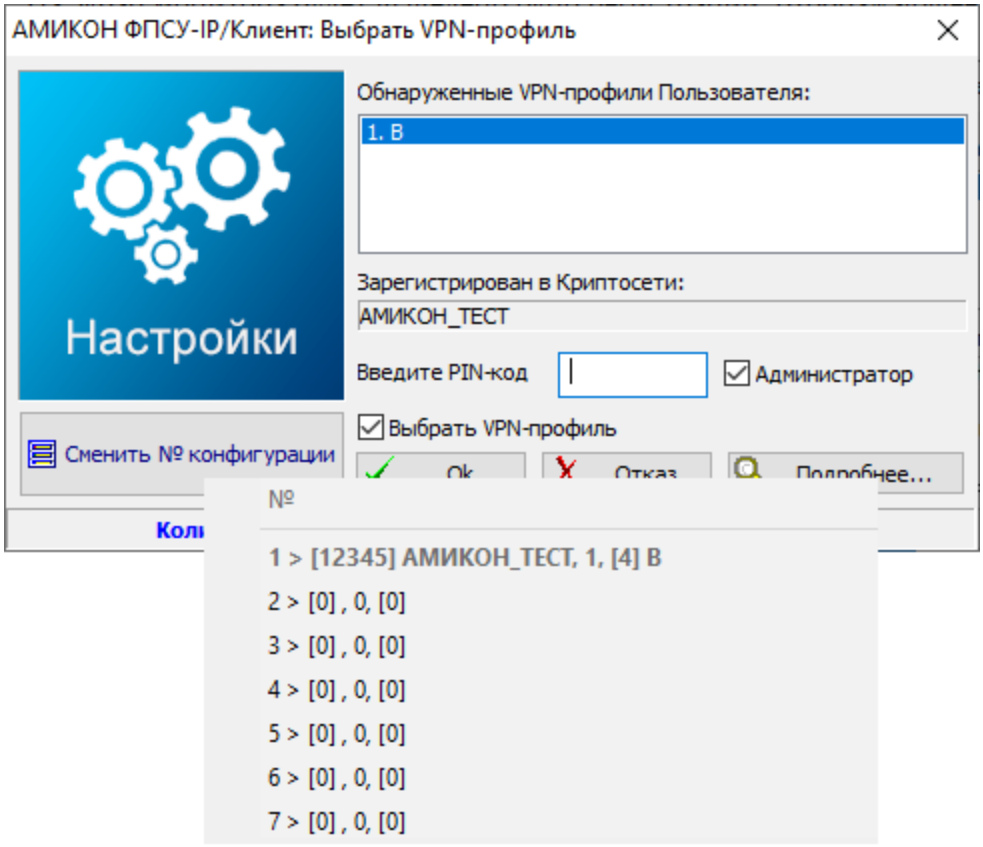


Рисунок 14 - Выбор VPN-профиля

Если при настройке VPN-Key был установлен режим автосоединения (см. раздел «Регистрация администратора в программно-аппаратном Клиенте), ФПСУ-IP/Клиент автоматически попытается идентифицировать пользователя и начать сеанс связи с ФПСУ-IP, в противном случае необходимо воспользоваться командой меню «Соединиться» или выбрать знак программы двойным нажатием левой клавиши.

Если настройки VPN-Key содержат установку запоминания PIN-кода пользователя, то в режиме автосоединения идентификация пользователя производиться не будет, а ФПСУ-IP/Клиент начнет производить попытки соединения с ФПСУ-IP.

3. Ввести в соответствующее диалоговое поле окна регистрации четырехзначный PIN-код пользователя или администратора устройства VPN-Key. В отношении задачи установления соединения с ФПСУ-IP, нет разницы, был введен PIN-код пользователя или администратора.
4. Если вводимые персональные коды верны и количество попыток их ввода не превышено, ФПСУ-IP/Клиент считает идентификацию пользователя завершенной и пытается установить VPN-туннель с ФПСУ-IP. При этом на экран выдается информационное окно, отображающее процесс установления соединения.

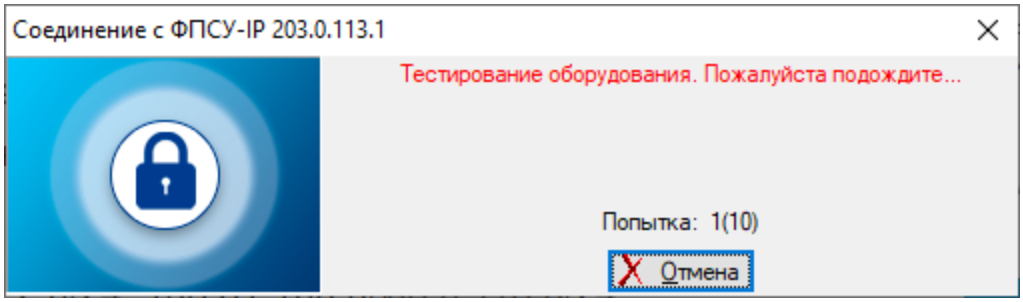


Рисунок 15 - Соединение с ФПСУ-IP

Если попытки соединиться с ФПСУ-IP окажутся неудачными, на экран будет выведено одно из диагностических сообщений, которые приведены в таблице («Сообщения об ошибках при соединении с ФПСУ-IP») вместе с комментариями.

5. Если VPN-туннель с ФПСУ-IP установлен, на экран может быть выдано окно опциональной авторизации через Radius-сервер. Необходимость авторизации через Raduis-сервер устанавливается администратором ФПСУ-IP.

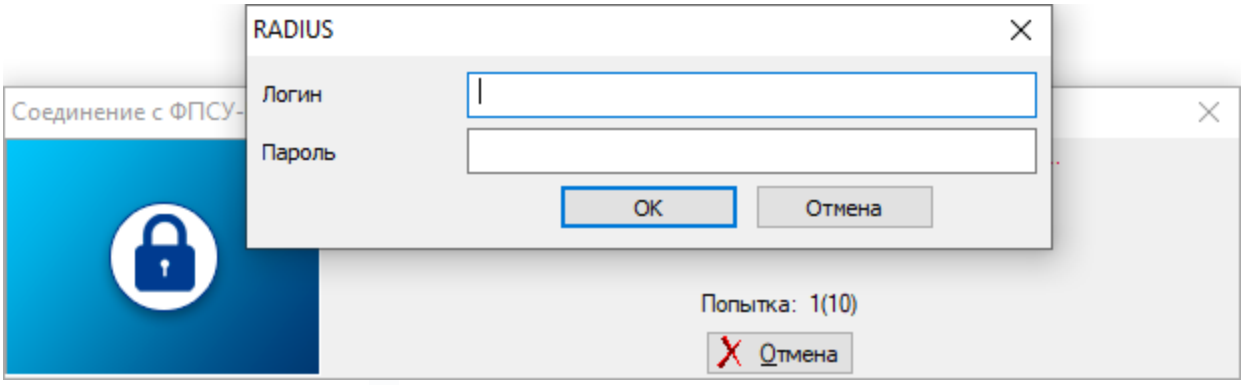


Рисунок 16 - Опциональная авторизация по RADIUS

В случае появления окна Raduis-авторизации, необходимо указать в появившемся окне учетные данные пользователя и пароль (или комбинацию паролей, в зависимости от настроек Raduis-сервера). Учетные данные и пароль должны быть получены от администратора Raduis-сервера.

6. Если VPN-туннель с ФПСУ-IP установлен и доступ пользователю разрешается, окно «Соединение» закроется, а значок программы ФПСУ-IP/Клиент внизу экрана изменит свой вид  .

Соединение ФПСУ-IP/Клиента с ФПСУ-IP в ОС Windows может быть осуществлено вручную посредством выполнения команды:

«"DRIVE:\Program Files\Amicon\Client FPSU-IP\ip-client.exe" connect» из командной строки (в том числе и удаленно).

Аналогично возможно вручную выполнить разрыв установленного с ФПСУ-IP VPN-туннеля командой: «"DRIVE:\Program Files\Amicon\Client FPSU-IP\ip-client.exe" disconnect».

Для окончания сеанса связи и завершения работы VPN-туннеля с ФПСУ-IP необходимо воспользоваться командой «Разъединиться» контекстного меню ФПСУ-IP/Клиента или физически отключить от рабочей станции VPN-Key.

5.3. Доступные пользователю настройки программно-аппаратного Клиента

Для просмотра пользователем настроек ФПСУ-IP/Клиента необходимо выполнить следующие действия:

1. Подключить VPN-Key к USB-порту компьютера;
2. Вызвать контекстное меню программы и выбрать команду «Настройки VPN-Key»;

На экран монитора будет выдано окно регистрации, отображающее данные VPN-профиля, загруженные из устройства VPN-Key.

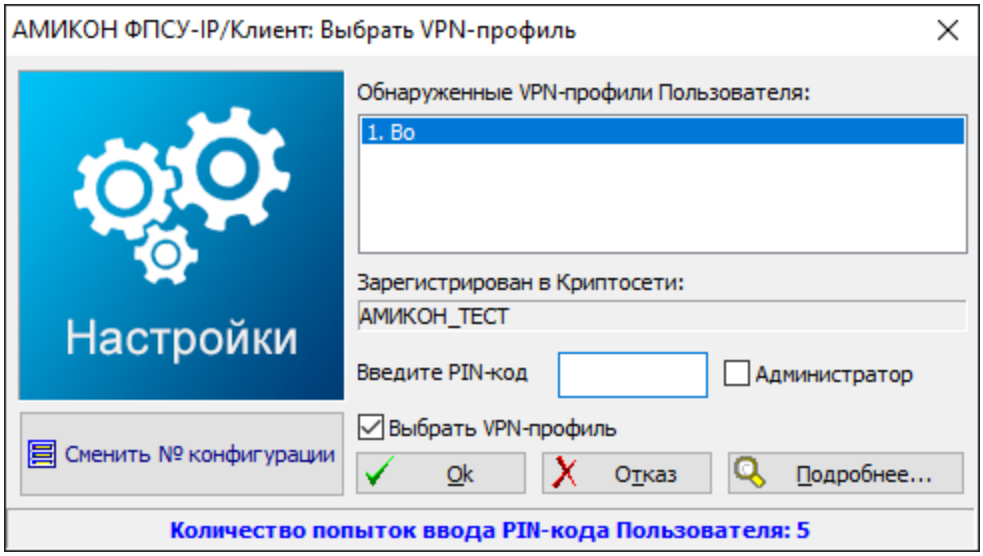


Рисунок 17 - Окно регистрации

3. Ввести PIN-код пользователя.

Если введенный PIN-код не соответствует данным, заложенным в подключенном VPN-Key, он будет запрошен снова. По истечении установленного количества неудачных попыток система начнет запрашивать десятизначный PUK-код пользователя.

Если попытки ввести PUK-код также не увенчаются успехом, предъявленный VPN-Key будет заблокирован и дальнейшая работа с текущей конфигурацией (на любом компьютере) окажется невозможной. Если вводимые персональные коды верны и количество попыток их ввода не превышено, регистрация пользователя считается

завершенной.

После корректного ввода пароля откроется окно просмотра настроек с возможностью изменения PIN-кода пользователя и некоторыми дополнительными функциями.

5.3.1. Просмотр настроек подключения к ФПСУ-IP

Для просмотра описания ФПСУ-IP в левой части окна настроек необходимо выбрать строку «ФПСУ-IP».

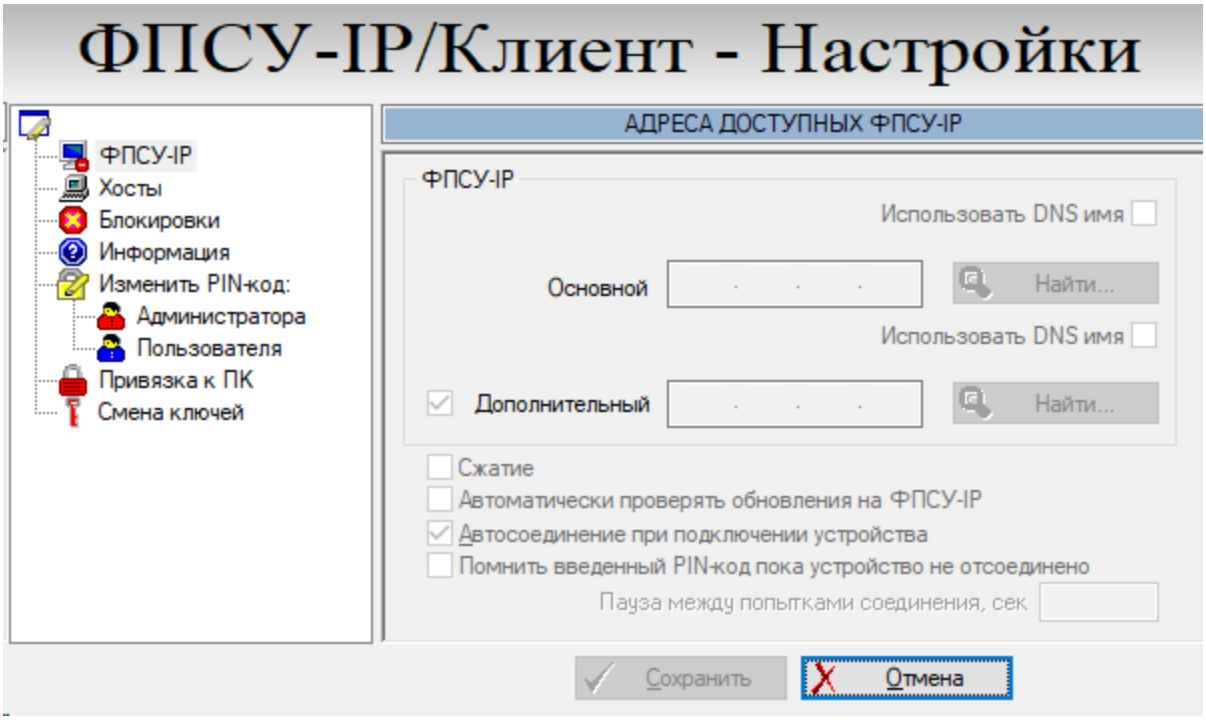


Рисунок 18 - Настройки работы ФПСУ-IP/Клиента с ФПСУ-IP

В поле «Основной» в правой части окна отображается основной IP-адрес ФПСУ-IP, через который осуществляется доступ ФПСУ-IP/Клиента к защищенным хостам. При наличии дополнительного ФПСУ-IP его адрес отображается в соответствующем поле.

Если флаг «Сжатие» установлен, при соединении с ФПСУ-IP происходит сжатие трафика, отправляемого в туннель. Следует иметь в виду, что включение опции "Сжатие" приводит к увеличению загрузки процессора.

Если флаг «Автоматически проверять обновления» установлен, то при каждом соединении с ФПСУ-IP (основным или дополнительным) ФПСУ-IP/Клиент будет запрашивать у него наличие новых версий программного обеспечения ФПСУ-IP/Клиент.

Если флаг «Автосоединение при подключении VPN-Key» установлен, то при

подключении VPN-Key в USB-порт рабочей станции с установленным ПО «ФПСУ-IP/Клиент», автоматически будет произведена попытка соединения с ФПСУ-IP. Так же при установленном флаге будет произведена попытка соединения с ФПСУ-IP при старте ПО ФПСУ-IP/Клиент вручную, или после перезагрузки операционной системы (при наличии подключенного к рабочей станции VPN-Key).

При установленном флаге «Помнить введенный PIN-код пока VPN-Key не отсоединен» один раз введенный PIN-код пользователя VPN-Key будет запомнен, и при дальнейших попытках установления VPN-туннеля с ФПСУ-IP не будет выводится запрос его повторного ввода. PIN код сохраняется и при перезагрузках, вплоть до физического отсоединения устройства VPN-Key от USB порта рабочей станции. Запомненный PIN-код действует только для попыток установления соединения с ФПСУ-IP, и не будет подставляться при попытках пользователя изменить конфигурацию VPN-Key.

При введенном в поле «Пауза между попытками соединения, сек» значении попытки соединения с ФПСУ-IP будут повторяться с заданным интервалом. Если поле не заполнено, при команде на установление соединения ФПСУ-IP/Клиент сделает 10 попыток соединения сначала с основным ФПСУ-IP, затем с 10 попыток - с дополнительным. После чего, в случае неудачи, выдаст сообщение об отказе и прекратит попытки установления VPN-туннеля. Если в поле опции указано какое-то значение, после отказа в соединении от основного и дополнительного ФПСУ-IP, ФПСУ-IP/Клиент через указанное время вновь попытается установить связь. В этом случае ФПСУ-IP/Клиент будет пытаться установить VPN-туннель с ФПСУ до тех пор, пока не получит ответ.

5.3.2. Доступные через ФПСУ-IP рабочие станции

Для отображения настроек работы с сетевыми ресурсами, доступными через туннель с ФПСУ-IP, в левой части окна настроек необходимо выделить строку «Хосты».

Если VPN-профиль содержит IP-адреса рабочих станций, с которыми ФПСУ-IP/Клиент может работать через VPN-туннель, они будут отображаться в списке справа.

Список IP-адресов может быть также получен от ФПСУ-IP, где он формируется администратором ФПСУ-IP. Для его просмотра после установки VPN-туннеля с ФПСУ-IP необходимо нажать кнопку «Список хостов, полученных от ФПСУ».

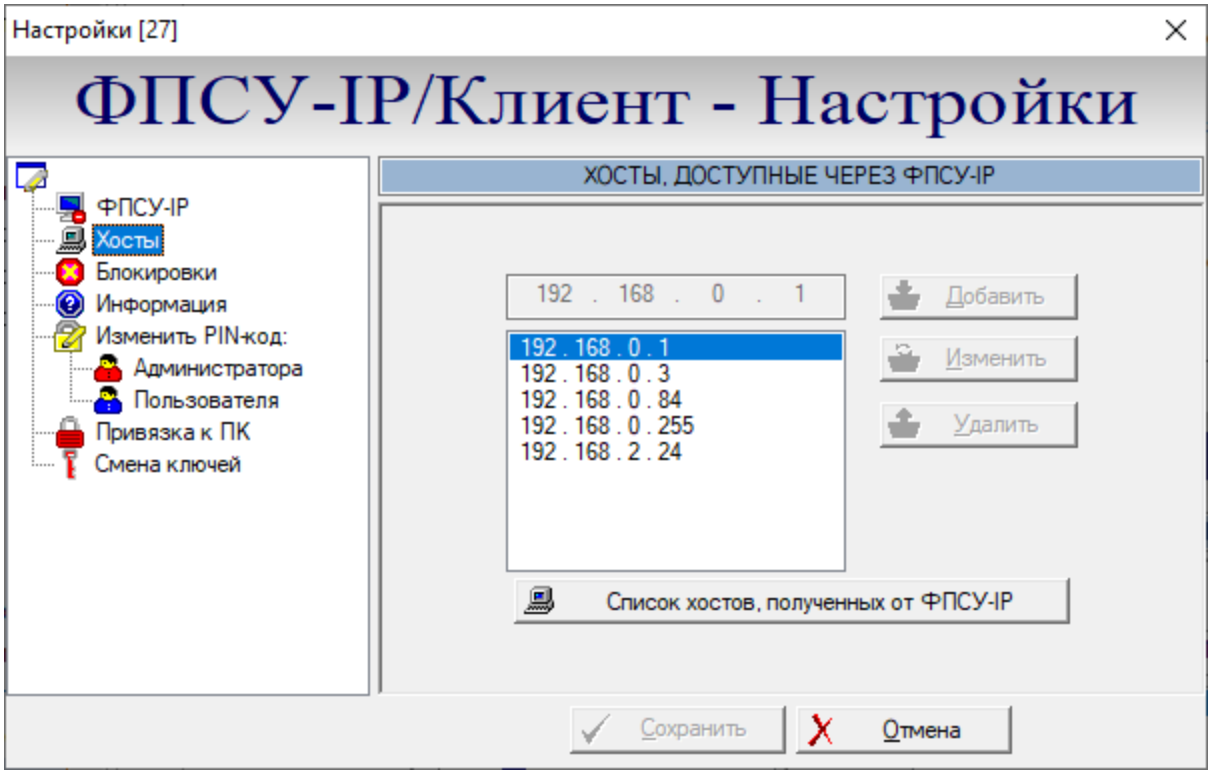


Рисунок 19 – Доступные хосты

ФПСУ-IP/Клиент сможет работать через VPN-туннель с ФПСУ-IP только с теми рабочими станциями и серверами, чьи IP-адреса явно указаны либо в конфигурации VPN-профиля, либо в конфигурации данного пользователя Криптосети Клиентов в настройках ФПСУ-IP.

Для выхода из окна настройки можно воспользоваться кнопкой «Отмена».

5.3.3. Блокировки пакетов при установленном VPN-туннеле с ФПСУ-IP

Во время существования VPN-туннеля с ФПСУ-IP, ФПСУ-IP/Клиент может обмениваться данными с другими рабочими станциями сети в обычном открытом режиме. Администраторы ФПСУ-IP и ФПСУ-IP/Клиента могут ограничивать сетевое взаимодействие компьютера пользователя во время установленного соединения с ФПСУ-IP. В интерфейсе ФПСУ-IP/Клиента такие ограничения называются «блокировками» и доступны через меню настройки VPN-Key.

Пользователь может только просматривать текущие блокировки.

В левой части окна необходимо выбрать строку «Блокировки», после чего справа появится информация о правилах фильтрации входящих и исходящих пакетов данных на время существования VPN-туннелей с ФПСУ-IP.

Во время установки VPN-туннеля с ФПСУ-IP правила фильтрации, возможно, будут принудительно дополнены в соответствии с указаниями администратора ФПСУ-IP - в этом случае во время соединения около соответствующего поля будет отображаться знак запрета («кирпич»). Эти правила имеют более высокий приоритет, чем настройки VPN-профиля.

Кроме того, во время существования VPN-туннеля могут работать ограничения на прием и передачу пакетов, установленные администратором.

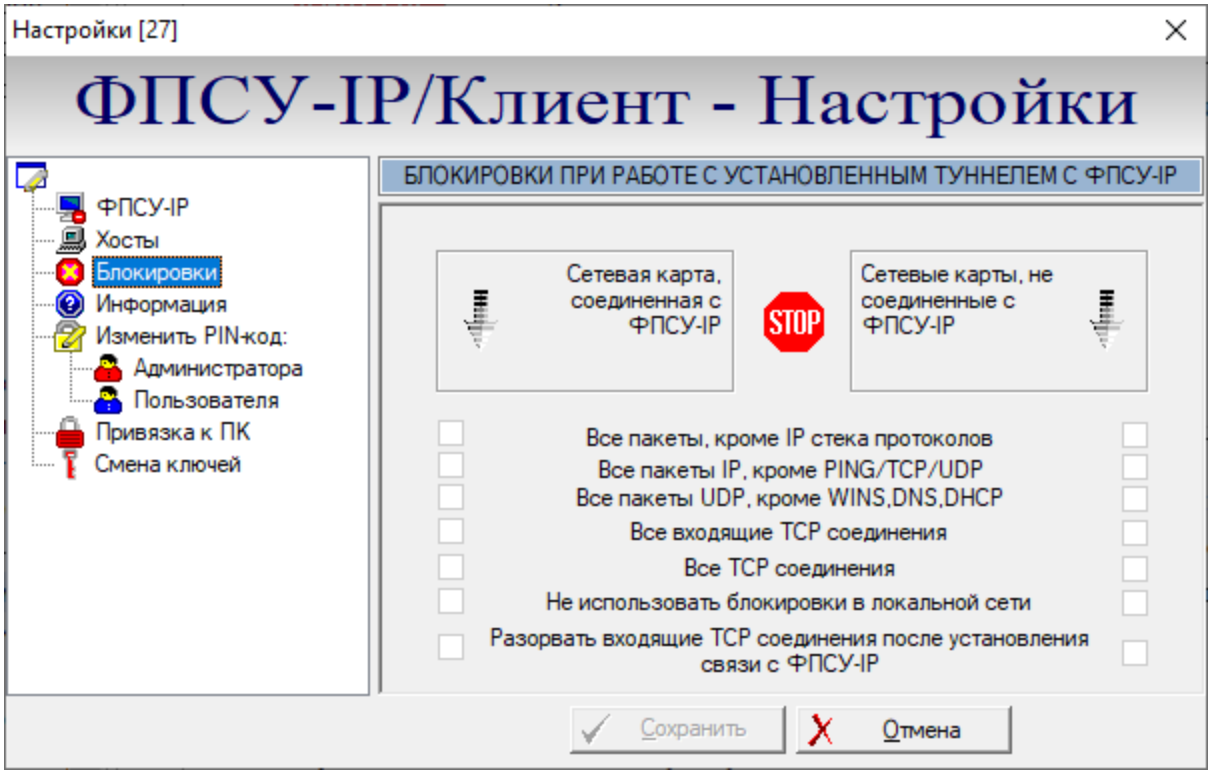


Рисунок 20 - Настройка блокировок сетевых пакетов

Правила блокировки межсетевого экрана состоят из следующих полей:

- Все пакеты, кроме IP стека протоколов — блокируются пакеты, не принадлежащие к стеку протоколов TCP\IP (например, блокируются протоколы PPP и PPPoE);
- Все пакеты IP, кроме PING/TCP/UDP — блокируются все пакеты стека протоколов TCP/IP, кроме эхо-запросов (ping) и транспортных протоколов TCP и UDP;
- Все пакеты UDP, кроме WINS, DNS, DHCP — блокируются все UDP пакеты, кроме WINS, DNS, DHCP;
- Все входящие TCP соединения — блокируются все IP пакеты с TCP трафиком, если инициатором соединения является другой хост;
- Все TCP соединения — блокируются все TCP соединения;
- Не использовать блокировки в локальной сети — не использовать все указанные выше блокировки, если рабочая станция ФПСУ-IP/Клиента взаимодействует с

хостами своей собственной подсети;

- Разорвать входящие TCP соединения после установки связи с ФПСУ — после установления соединения с ФПСУ-IP принудительно завершить все TCP соединения, инициатором которых является другой хост.

5.3.4. Получение сведений о VPN-Key и VPN-профиле

Для ознакомления с параметрами VPN-профиля в подключенном устройстве VPN-Key необходимо выбрать строку «Информация». При этом справа появится информационное окно, отображающее номера текущих версий внутреннего программного обеспечения устройства VPN-Key, ключевой системы VPN-профиля, системные идентификаторы VPN-профиля и допустимое количество последовательных попыток ввода персональных идентификаторов.

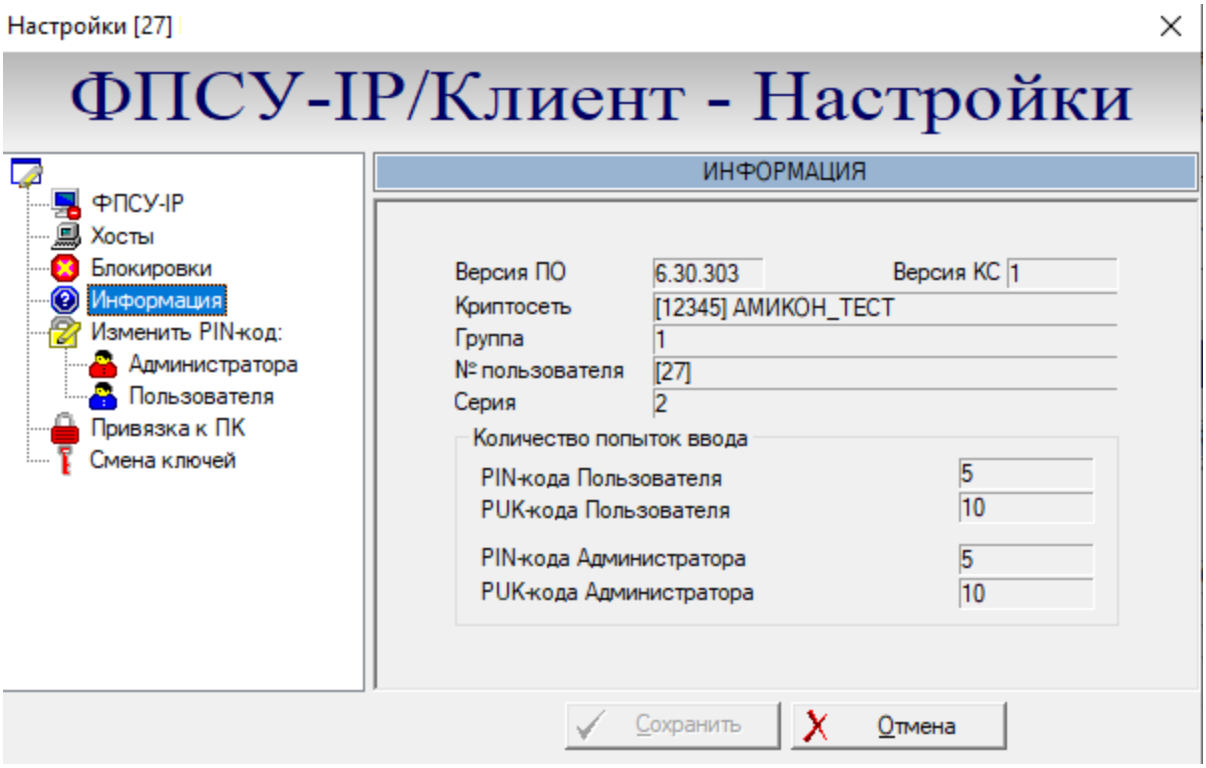


Рисунок 21 - Информация об устройстве VPN-Key

5.3.5. Изменение PIN-кода пользователя

Персональные идентификаторы пользователя обеспечивают дополнительный уровень безопасности (например, в случае утери контроля над устройством VPN-Key) и включают в себя:

- четырехзначный PIN-код (Personal Identity Number) пользователя;
- десятизначный PUK-код (Personal Unblocked Key) пользователя;
- четырехзначный PIN-код администратора;
- десятизначный PUK-код администратора.

Персональные идентификационные коды запрашиваются системой при попытках доступа ФПСУ-IP/Клиент к ФПСУ-IP.

Для того чтобы изменить PIN-код пользователя, хранящийся в устройстве VPN-Key, в левой части окна необходимо выбрать строку «Изменить PIN-код: Пользователя». В открывшемся окне следует ввести новый PIN-код и нажать командную кнопку «Изменить». PIN-код пользователя будет заменен на введенный новый.

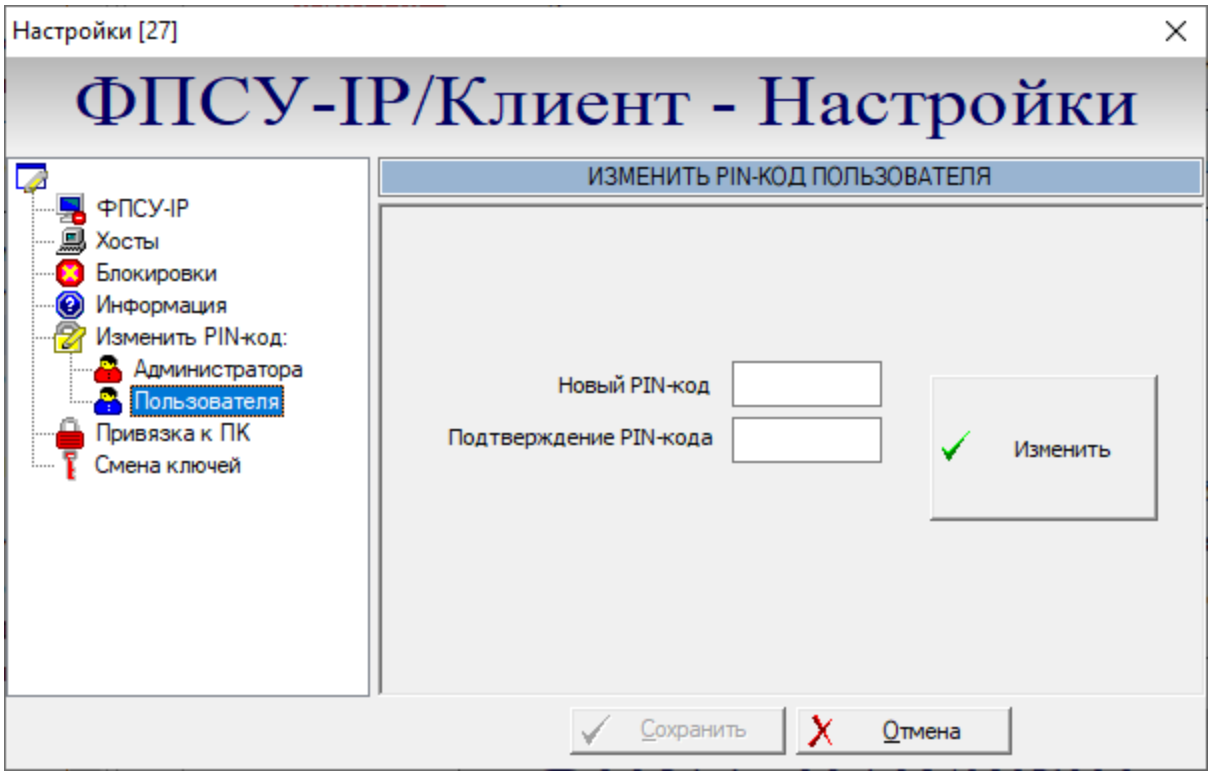


Рисунок 22 - Изменение персональных идентификаторов

5.4. Администрирование программно-аппаратного Клиента

В VPN-Key может быть записано до семи VPN-профилей, каждый из которых содержит в себе:

- уникальные системные идентификаторы ФПСУ-IP/Клиента;
- персональные ключи доступа (аутентификационные данные);
- настройки для формирования VPN-туннеля с ФПСУ-IP:

- IP-адрес ФПСУ-IP;
- IP-адреса рабочих станций, доступных ФПСУ-IP/Клиенту через этот ФПСУ-IP;
- обусловленные политикой безопасности ограничения на прием и передачу пакетов во время работы через VPN-туннель.

Персональные идентификаторы (PIN-коды пользователя и администратора) записываются для VPN-Key, т.е. для всех VPN-профилей, размещенных на устройстве, предусмотрен один PIN-код пользователя и один - администратора.

Эта информация записывается в конфигурацию VPN-Key либо при его изготовлении, либо пользователем с правами администратора VPN-Key после установки ФПСУ-IP/Клиент на ПЭВМ. В процессе эксплуатации пользователь с правами администратора может изменить указанные параметры, а также установить новые персональные идентификаторы пользователя и/или администратора.

Управление ФПСУ-IP/Клиентом на рабочем месте осуществляется через контекстное меню, вызываемое нажатием правой клавиши мыши на значке программы в области уведомлений панели задач Windows.

5.4.1. Регистрация администратора в программно-аппаратном Клиенте

Для того, чтобы получить полный доступ к настройкам устройства VPN-Key и хранящихся в нём VPN-профилям следует подтвердить полномочия администратора VPN-Key. Для этого необходимо выполнить следующие действия:

1. Подключить VPN-Key к USB-порту компьютера.
2. Вызвать контекстное меню программы и выбрать команду «Настройки VPN-Key».

На экран монитора будет выведено окно регистрации, отображающее данные VPN-профиля, авторизовавшегося в ФПСУ-IP/Клиенте последним.

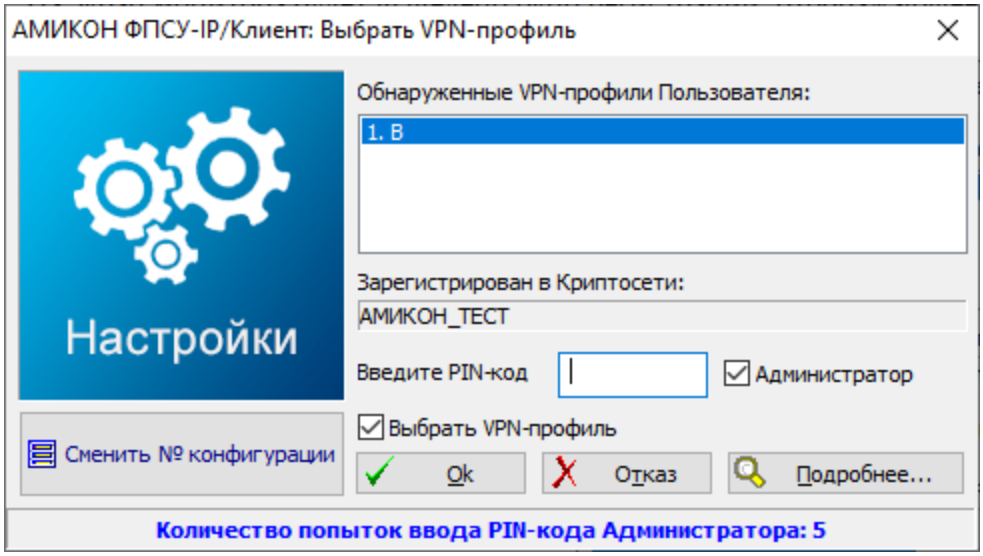


Рисунок 23 - Регистрация в ФПСУ-IP/Клиент

При установке флага «Выбрать VPN-профиль» в верхней части окна отобразится список физически подключенных к данной машине устройств VPN-Key (для каждого устройства будет отображаться VPN-профиль, активировавшийся на данном устройстве последним). Для того, чтобы выбрать другой VPN-профиль из записанных на подключенном устройстве VPN-Key, необходимо выбрать запись из списка, нажать кнопку «Сменить № конфигурации» и выбрать нужный VPN-профиль из выпадающего списка.

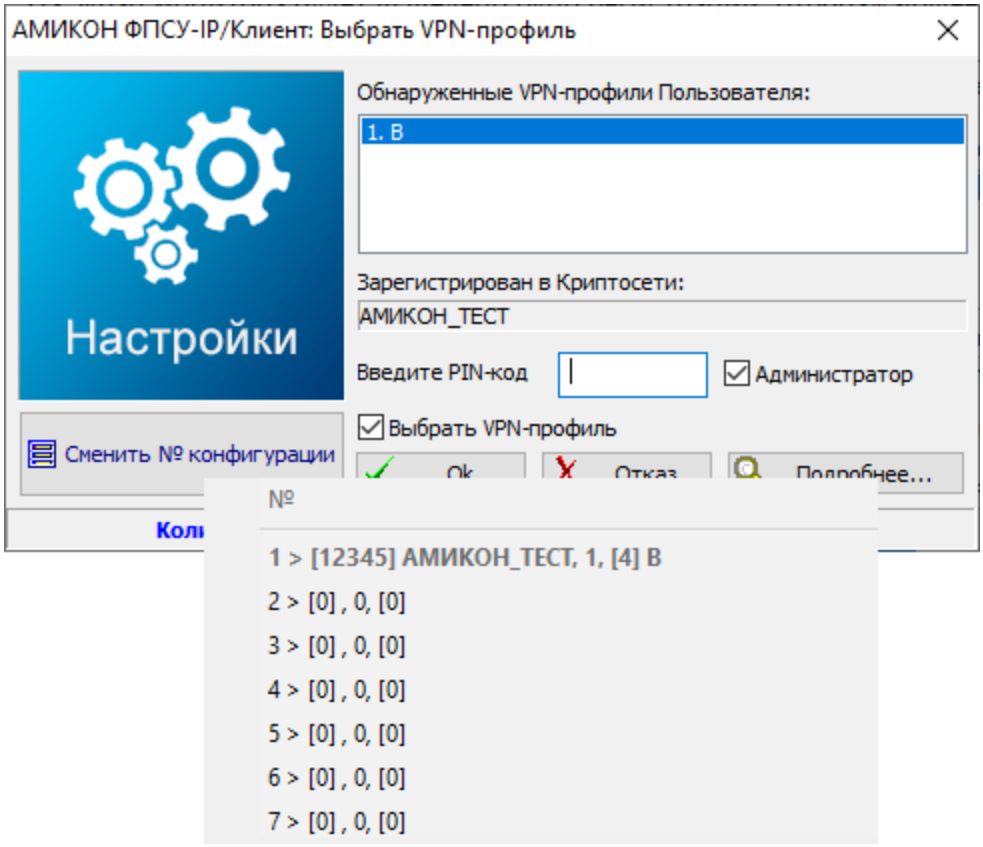


Рисунок 24 - Выбор VPN-профиля

3. Выбрать необходимую запись в поле «Обнаруженные устройства пользователя».
4. В окне регистрации установить флаг в поле «Администратор», ввести PIN-код администратора и нажать кнопку «Ok».

Если введенный код не соответствует данным, заложенным в подключенном VPN-Key, он будет запрошен снова. По истечении установленного количества неудачных попыток система начнет запрашивать десятизначный PUK-код администратора.

Если попытки ввести PUK-код также не увенчаются успехом, предъявленный VPN-Key будет заблокирован и дальнейшая работа с текущим VPN-профилем (на любом компьютере) окажется невозможной. Если вводимые персональные коды верны и количество попыток их ввода не превышено, регистрация пользователя считается завершенной.

Если регистрация администратора завершена успешно, на экран монитора будет выведено окно настроек. Левая часть окна содержит список доступных параметров VPN-профиля, а правая отображает значения установок текущего параметра.

5.4.2. Настройка параметров ФПСУ-IP/Клиента

Управление программно-аппаратным комплексом "ФПСУ-IP/Клиент" на рабочем месте осуществляется через контекстное меню, вызываемое нажатием правой клавиши мыши на значке программы в области уведомлений панели задач.

В данном разделе описывается настройка параметров для программно-аппаратного ФПСУ-IP/Клиента.

5.4.2.1. Настройка подключения к ФПСУ-IP

Для просмотра или редактирования настроек параметров к ФПСУ-IP, в левой части окна настроек необходимо выбрать строку «ФПСУ-IP».

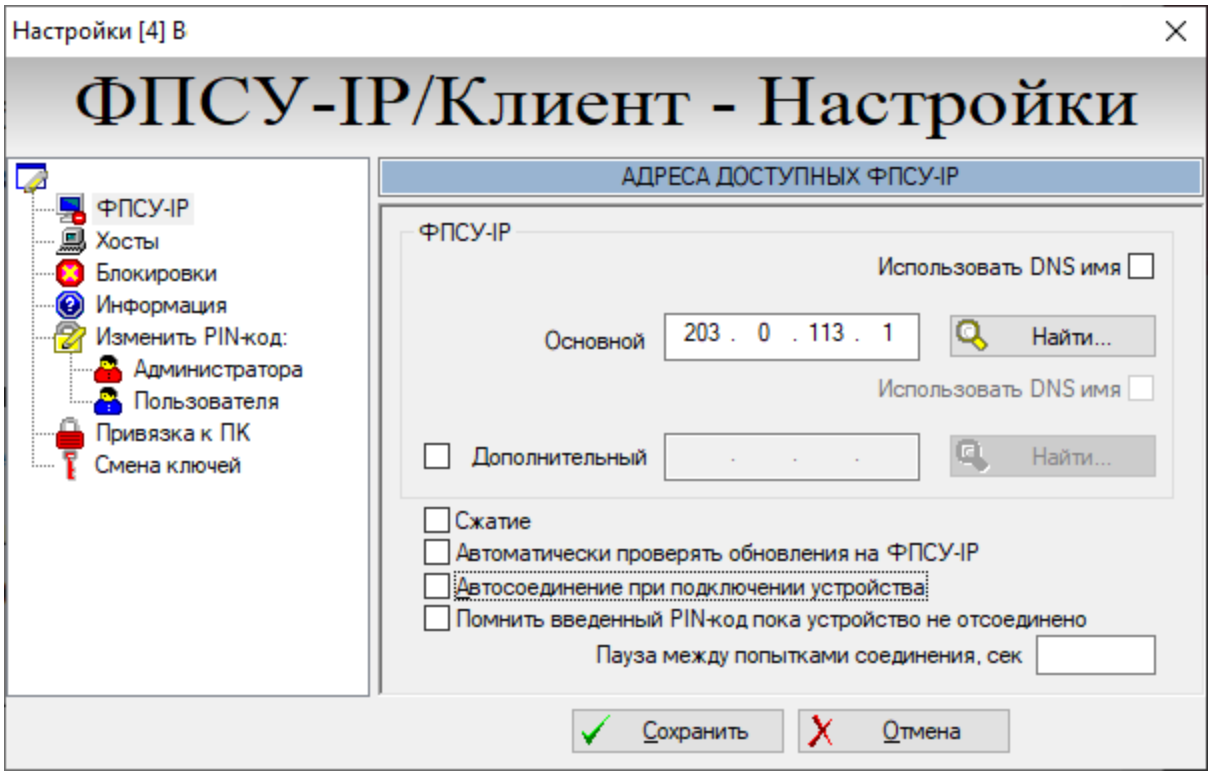


Рисунок 25 - Настройки работы Клиента с ФПСУ-IP

В поле «Основной» в правой части окна необходимо ввести IP-адрес ФПСУ-IP, через который будет осуществляться доступ ФПСУ-IP/Клиента к защищенным рабочим станциям и серверам.

Если сетевым службам компьютера доступны средства разрешения Интернет-имен (есть поддержка службы DNS), по нажатию кнопки «Найти» можно запросить IP-адрес ФПСУ-IP с известным именем у обслуживающего DNS сервера. Вместо указания IP-адреса

ФПСУ-IP можно сохранить в настройках DNS-имя, установив опцию «Использовать DNS-имя». В этом случае перед установлением соединения ФПСУ-IP/Клиента с ФПСУ-IP будет каждый раз выполняться DNS-запрос на получение IP-адреса ФПСУ-IP у обслуживающего рабочую станцию DNS-сервера.

Если в локальной сети имеется еще один ФПСУ-IP, который может предоставить доступ ФПСУ-IP/Клиенту в случае отсутствия связи с основным ФПСУ-IP, необходимо установить флаг в поле «Дополнительный» и указать его IP-адрес в окне справа (либо воспользоваться кнопкой «Найти», как описано выше).

Если канал связи с ФПСУ-IP обеспечивает скорости передачи данных не выше 5 Мбит/с, рекомендуется указать ФПСУ-IP/Клиент на необходимость сжатия данных перед передачей их в VPN-туннель (для чего следует установить флаг «Сжатие»). При более высоких скоростях соединения эта опция неэффективна для повышения скорости передачи данных, но может быть применена в целях экономии сетевого трафика.

Для установки режима автоматической проверки обновлений необходимо установить флаг «Автоматически проверять обновления» – в этом случае при каждом соединении с ФПСУ-IP (основным или дополнительным) ФПСУ-IP/Клиент будет запрашивать у него наличие новых версий программного обеспечения ФПСУ-IP/Клиента (раздел «Обновление ПО ФПСУ-IP/Клиента с ФПСУ-IP»).

Если установить флаг «Автосоединение при подключении устройства», то при выборе VPN-профиля автоматически будет произведена попытка соединения с ФПСУ-IP.

Установленный флаг «Помнить введенный PIN-код пока устройство не отсоединено» указывает программе запомнить введенный один раз PIN код доступа к VPN-профиля, и при дальнейших попытках установления VPN-туннеля с ФПСУ-IP не будет требовать его повторного ввода. PIN код сохраняется и при перезагрузках. Запомненный PIN-код действует только для попыток установления соединения с ФПСУ-IP, и не будет подставляться при попытках пользователя изменить конфигурацию VPN-профиля.

Опция «Пауза между попытками соединения, сек» предназначена для задания временного интервала, с которым будут повторяться попытки соединения с ФПСУ-IP. Если опция не выставлена (окно пусто), при команде на установление соединения ФПСУ-IP/Клиент сделает 10 попыток соединения сначала с основным ФПСУ-IP, затем 10 попыток - с дополнительным. После чего, в случае неудачи, выдаст сообщение об отказе и прекратит попытки установления VPN-туннеля. Если в поле опции указано какое-то значение, после отказа в соединении от основного и дополнительного ФПСУ-IP, ФПСУ-IP/Клиент через указанное время вновь попытается установить связь. В этом случае ФПСУ-IP/Клиент будет пытаться установить VPN-туннель с ФПСУ до тех пор, пока не получит от ФПСУ-IP ответа.

Произведенные установки сохраняются при помощи кнопки «Сохранить». Для

выхода из окна настройки без сохранения нужно воспользоваться кнопкой «Отмена».

Все действия, необходимые для настройки подключения к ФПСУ-IP при работе с программным Клиентом, аналогичны действиям для программно-аппаратного Клиента.

5.4.2.2. Настройка доступных через ФПСУ-IP рабочих станций

Для отображения настроек работы с сетевыми ресурсами, доступными через туннель с ФПСУ-IP, в левой части окна настроек необходимо выделить строку «Хосты».

Если VPN-профиль содержит IP-адреса рабочих станций, с которыми ФПСУ-IP/Клиент может работать через VPN-туннель, они будут отображаться в списке справа. Для введения новых IP-адресов необходимо воспользоваться полем ввода над списком и кнопкой «Добавить».

Список IP-адресов может быть также получен от ФПСУ-IP, где он формируется администратором ФПСУ-IP. Для его просмотра после установки VPN-туннеля с ФПСУ-IP необходимо нажать кнопку «Список хостов, полученных от ФПСУ». Ранее добавленные в VPN-профиль адреса можно отредактировать или удалить из списка при помощи кнопок «Изменить» или «Удалить».

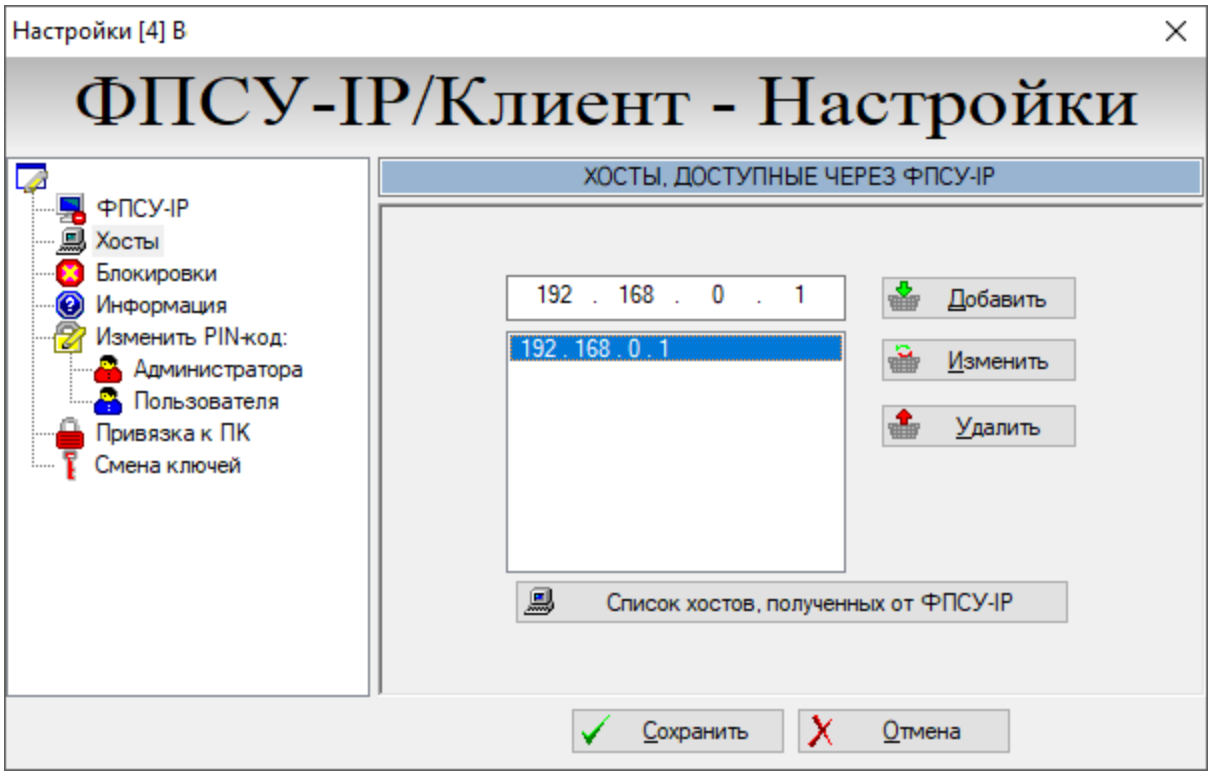


Рисунок 26- Настройка доступных ФПСУ-IP/Клиенту через VPN-туннель с ФПСУ-IP хостов

ФПСУ-IP/Клиент сможет работать через VPN-туннель с ФПСУ-IP только с теми рабочими станциями и серверами, чьи IP-адреса явно указаны либо в конфигурации VPN-профиля, либо в конфигурации данного пользователя Криптосети Клиентов в настройках ФПСУ-IP.

Произведенные настройки сохраняются при помощи соответствующей кнопки. Для выхода из окна настройки без сохранения можно воспользоваться кнопкой «Отмена».

Все действия, необходимые для настройки доступных через ФПСУ-IP рабочих станций при работе с программным Клиентом, аналогичны действиям для программно-аппаратного Клиента.

5.4.2.3. Блокировки пакетов при установленном VPN-туннеле с ФПСУ-IP

Во время существования VPN-туннеля с ФПСУ-IP, ФПСУ-IP/Клиент может обмениваться данными с другими рабочими станциями сети в обычном открытом режиме. Администраторы ФПСУ-IP и ФПСУ-IP/Клиента могут ограничивать сетевое взаимодействие компьютера пользователя во время установленного соединения с ФПСУ-IP. В интерфейсе ФПСУ-IP/Клиента такие ограничения называются «блокировками» и доступны для изменения через меню настройки VPN-Key или VPN-профиля.

В левой части окна необходимо выбрать строку «Блокировки», после чего справа появится список блокировок, позволяющий установить правила фильтрации входящих и исходящих пакетов данных на время существования VPN-туннелей с ФПСУ-IP.

В группе переключателей нужно отметить те соединения, которые будут запрещены во время сеансов с ФПСУ-IP. Ограничения на прием и передачу пакетов могут быть установлены как для сетевого адаптера, связанного с ФПСУ-IP, так и для других сетевых адаптеров ФПСУ-IP/Клиент.

Во время установки VPN-туннеля с ФПСУ-IP правила фильтрации, возможно, будут принудительно дополнены в соответствии с указаниями администратора ФПСУ-IP - в этом случае во время соединения около соответствующего поля будет отображаться знак запрета (знак «въезд запрещен»). Эти правила имеют более высокий приоритет, чем настройки устройства VPN-Key.

Кроме того, во время существования VPN-туннеля могут работать ограничения на прием и передачу пакетов, установленные локальным межсетевым экраном Клиента (см. раздел «Настройка локального межсетевого экрана ФПСУ-IP/Клиента».

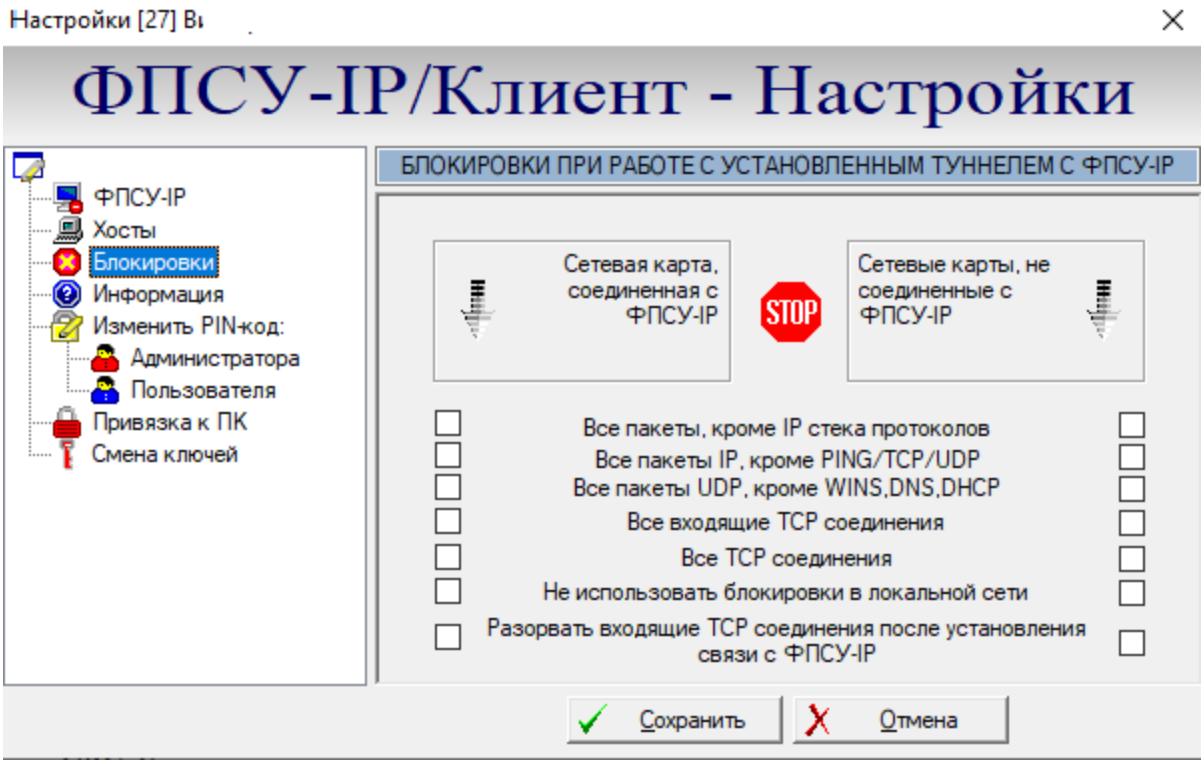


Рисунок 27 - Настройка блокировок сетевых пакетов

Правила блокировки межсетевого экрана состоят из следующих полей:

- Все пакеты кроме IP стека протоколов — блокируются пакеты, не принадлежащие к стеку протоколов TCP/IP (например, блокируются протоколы PPP и PPPoE);
- Все пакеты IP, кроме PING/TCP/UDP — блокируются все пакеты стека протоколов TCP/IP, кроме эхо-запросов (ping) и транспортных протоколов TCP и UDP;
- Все пакеты UDP, кроме WINS, DNS, DHCP — блокируются все UDP пакеты, кроме WINS, DNS, DHCP;
- Все входящие TCP соединения — блокируются все IP пакеты с TCP трафиком, если инициатором соединения является другой хост;
- Все TCP соединения — блокируются все TCP соединения;
- Не использовать блокировки в локальной сети — не использовать все указанные выше блокировки, если рабочая станция Клиента взаимодействует с хостами своей собственной подсети;
- Разорвать входящие TCP соединения после установки связи с ФПСУ — после установления соединения с ФПСУ-IP принудительно завершить все TCP-соединения, инициатором которых является другой хост.

Все действия, необходимые для настройки блокировок пакетов при установленном VPN-туннеле при работе с программным Клиентом, аналогичны действиям для программно-аппаратного Клиента.

5.4.2.4. Получение сведений о VPN-Key и VPN-профиле

Для ознакомления с параметрами подключенного VPN-Key или VPN-профиля необходимо выбрать строку «Информация». При этом справа появится информационное окно, отображающее текущую версию программного обеспечения микрокода устройства VPN-Key, параметры ключевой системы, системные идентификаторы и допустимое количество последовательных попыток ввода персональных идентификаторов.

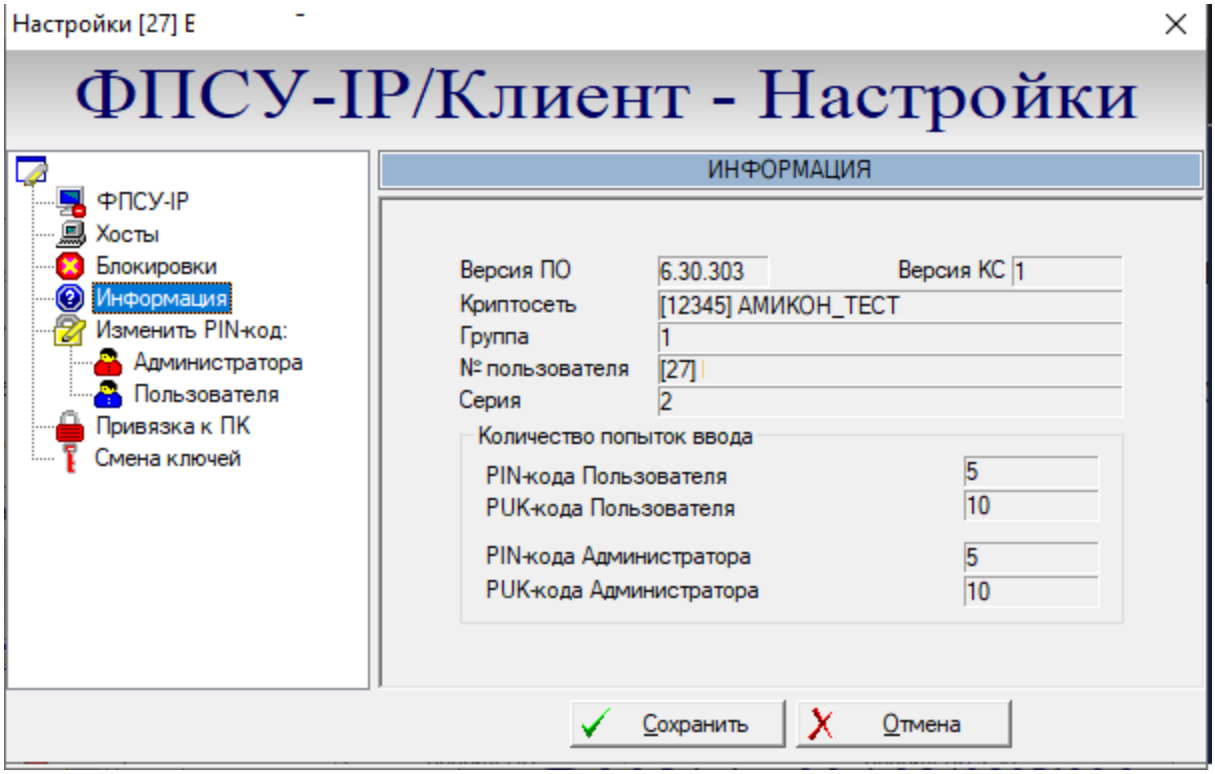


Рисунок 28 - Информация о VPN-Key

Все действия, необходимые для получения сведений о VPN-профиле при работе с программным Клиентом, аналогичны действиям при получении сведений о VPN-Key для программно-аппаратного Клиента. Также следует учитывать, что при работе с программным Клиентом пользователь обладает правами администратора по умолчанию, соответственно количество попыток ввода персонального идентификатора будет отображено только для PIN-кода Администратора.

5.4.2.5. Изменение PIN-кода администратора и пользователя

Персональные идентификаторы пользователя обеспечивают дополнительный уровень безопасности (например, в случае утери контроля над устройством VPN-Key) и включают в себя:

- четырехзначный PIN-код (Personal Identity Number) пользователя устройства VPN-Key;
- десятизначный PUK-код (Personal Unblocked Key) пользователя устройства VPN-Key;
- четырехзначный PIN-код администратора устройства VPN-Key;
- десятизначный PUK-код администратора устройства VPN-Key.

Персональные идентификационные коды текущей конфигурации пользователя запрашиваются системой при попытках соединения ФПСУ-IP/Клиент с ФПСУ-IP, а коды администратора – при попытках редактирования текущей конфигурации находящихся в устройстве VPN-Key VPN-профилей.

Для того чтобы изменить PIN-код администратора в левой части окна необходимо выбрать строку «Изменить PIN-код: Администратора». В поле появившегося окна следует ввести новый PIN-код и нажать кнопку «Изменить». PIN-код администратора будет заменен на введенный новый.

Для того чтобы изменить PIN-код пользователя, необходимо выбрать курсором строку «Изменить PIN-код: Пользователя» и действовать аналогично описанной выше процедуре.

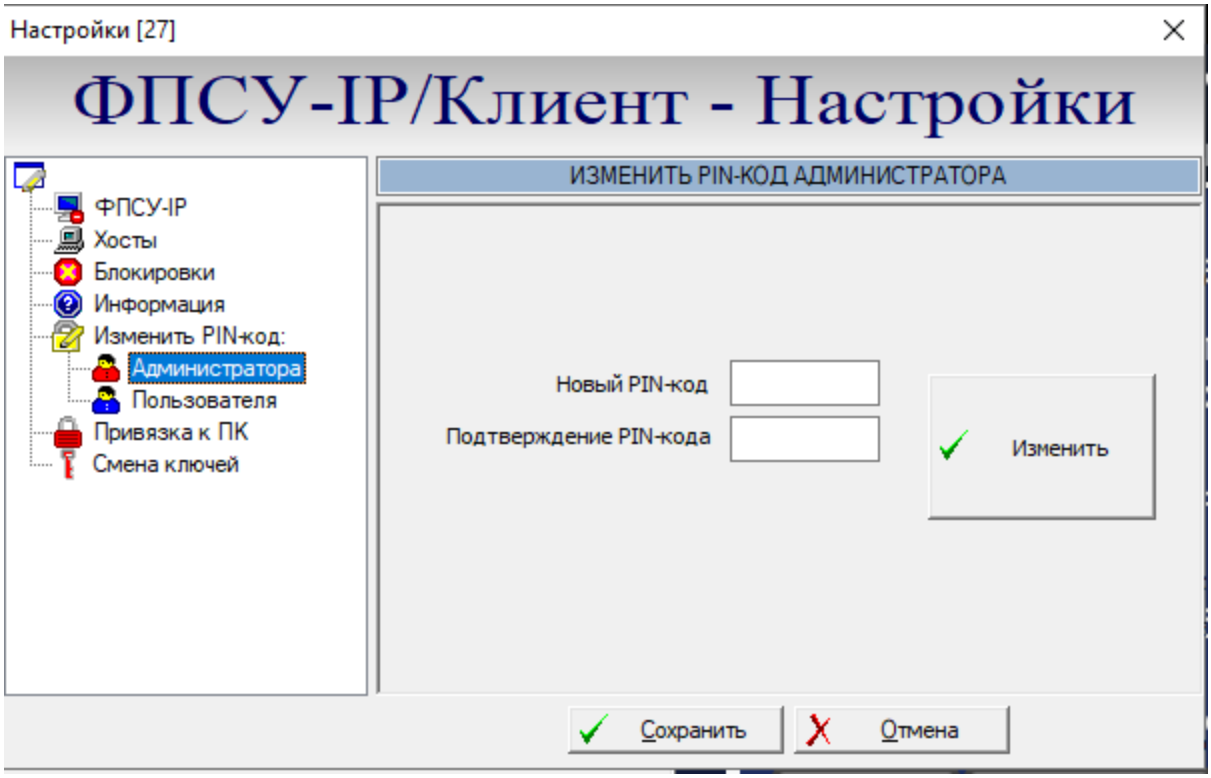


Рисунок 29 - Изменение персональных идентификаторов VPN-Key

5.4.2.6. Привязка VPN-Key к ПК

Если необходимо привязать VPN-Key к определенному рабочему месту, то в левой части окна необходимо выбрать пункт «Привязка к ПК». В правой части окна настроек появится функционал для привязки.

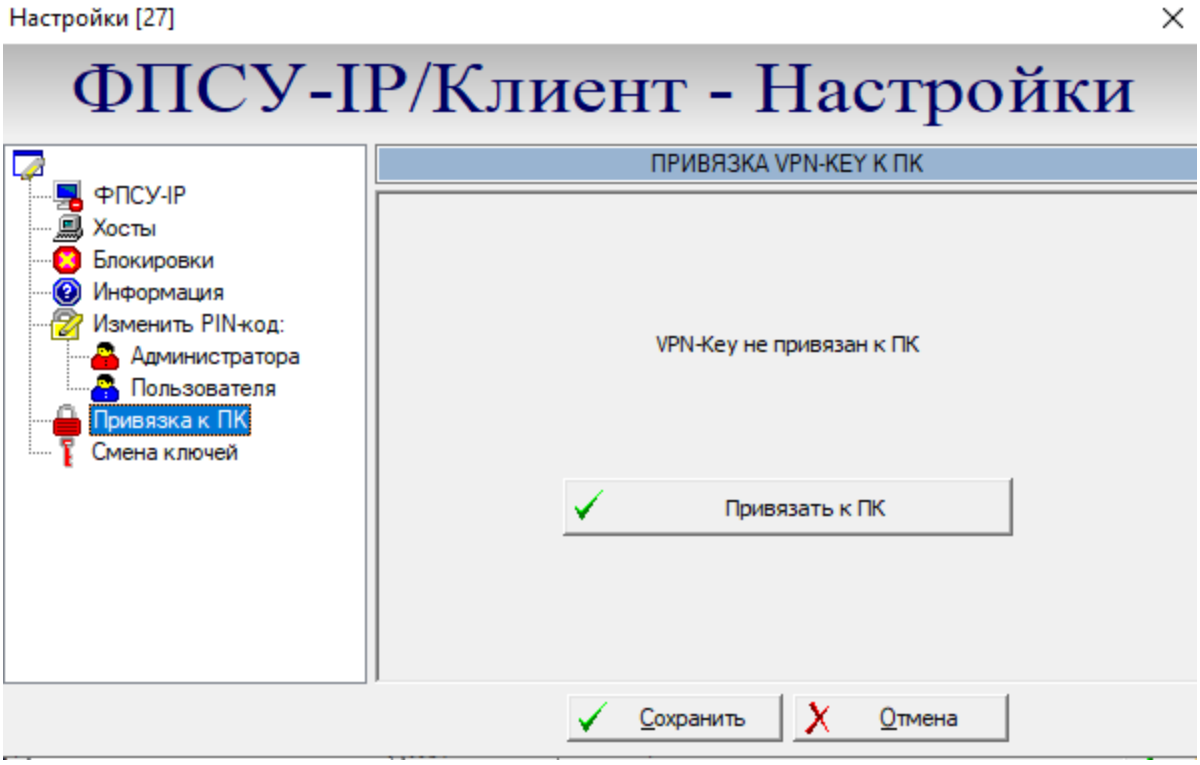


Рисунок 30 – Привязка к ПК

Привязка устройства VPN-Key к персональному компьютеру осуществляется по ряду параметров, в том числе учитывается:

- серийный номер ОС (только для Windows),
- серийный номер материнской платы,
- серийный номер системного диска.

Для того, чтобы пользователь текущего VPN-ключа мог работать только на одном АРМ пользователя ФПСУ-IP/Клиент, необходимо нажать кнопку «Привязать к ПК». Окно примет вид, представленный на рисунке ниже.

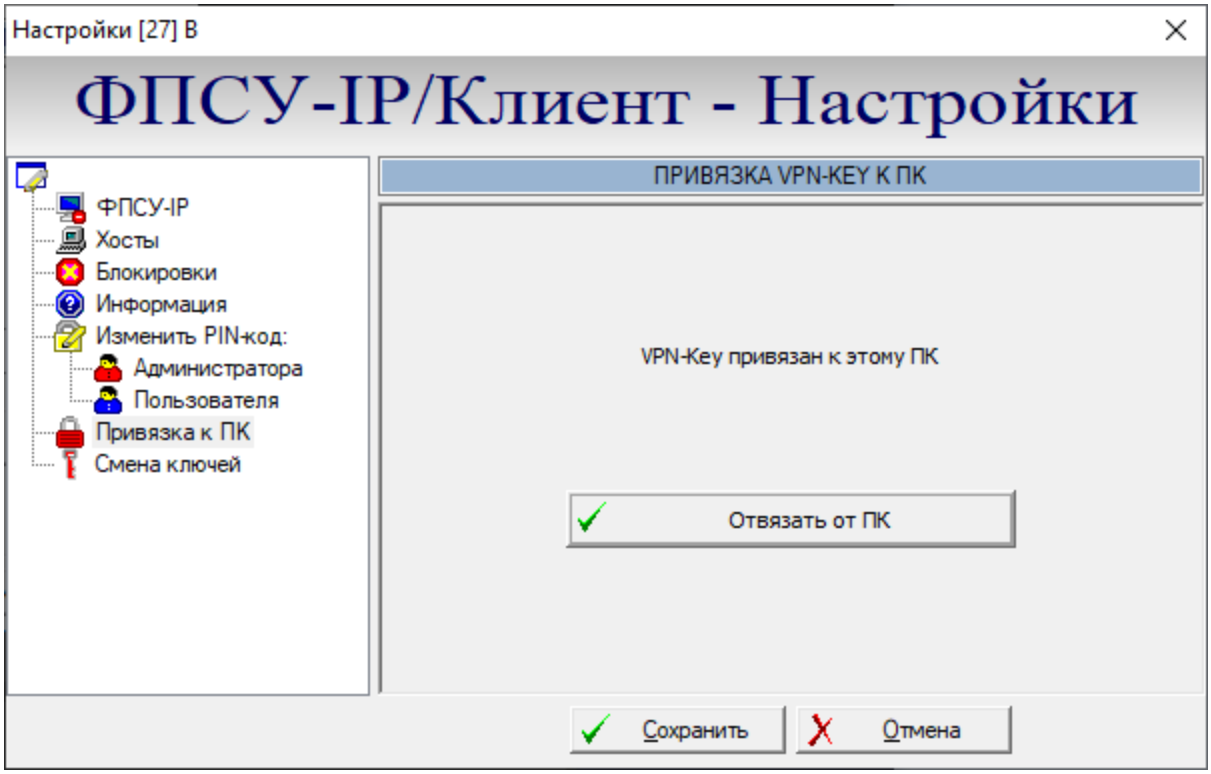


Рисунок 31 – VPN-Key привязан к ПК

Для того, чтобы VPN-Key можно было использовать на любом компьютере, в окне настроек ФПСУ-IP/Клиент необходимо нажать «Отвязать от ПК».

5.4.2.7. Смена серии ключей

Ключевые данные необходимо изменять не реже чем в 15 месяцев. Смена ключей через интерфейс Клиента возможна только для устройств VPN-Key с версией микрокода 6.30+ и 7.0+. В остальных случаях ключевые данные необходимо менять на ЦГКК. Для смены ключевых данных в интерфейсе Клиента требуется зайти в настройки устройства VPN-Key с полным доступом.

Для смены ключей в левой части окна необходимо выбрать пункт «Смена ключей». В правой части окна настроек появится интерфейс управления сменой ключевых данных.

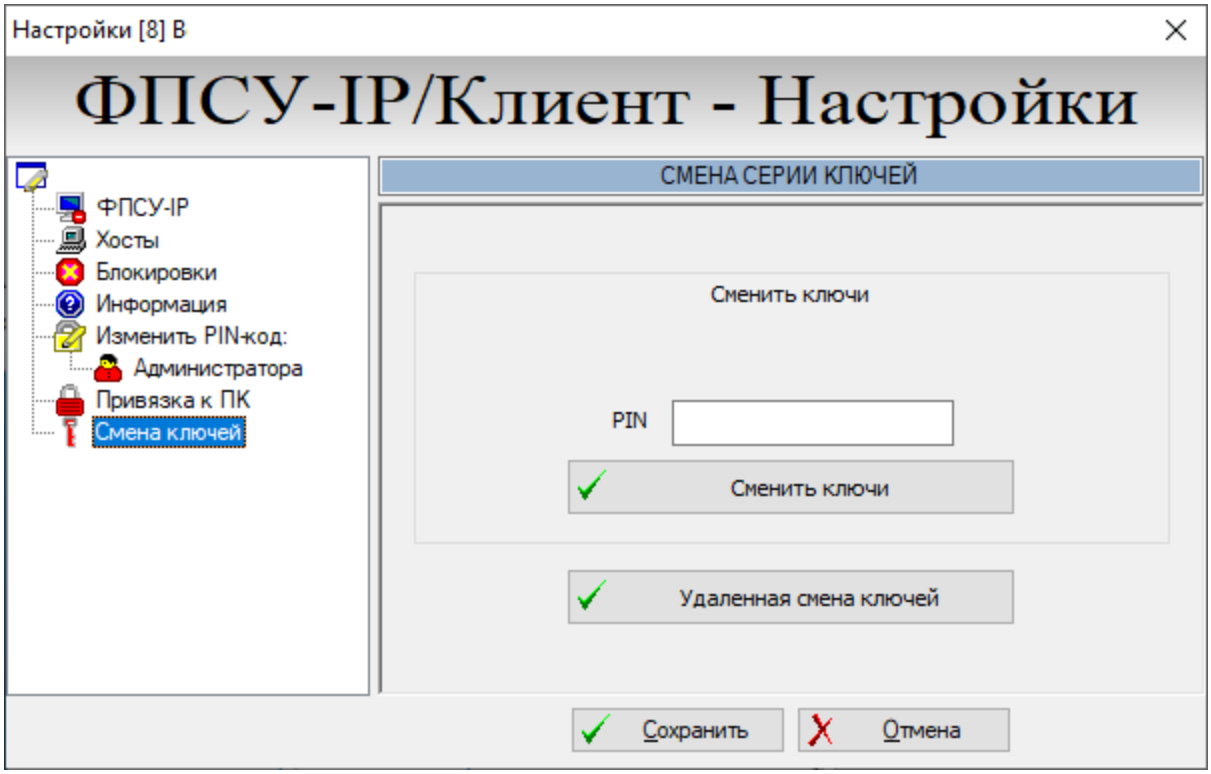


Рисунок 32 – Смена ключей

Для изменения ключевой информации необходимо ввести транспортный PIN-код для смены ключей VPN-профиля и нажать кнопку «Сменить ключи».

В открывшемся стандартном окне выбора файлов следует выбрать файл, выданный ЦГКК для смены ключей и нажать кнопку «Открыть».

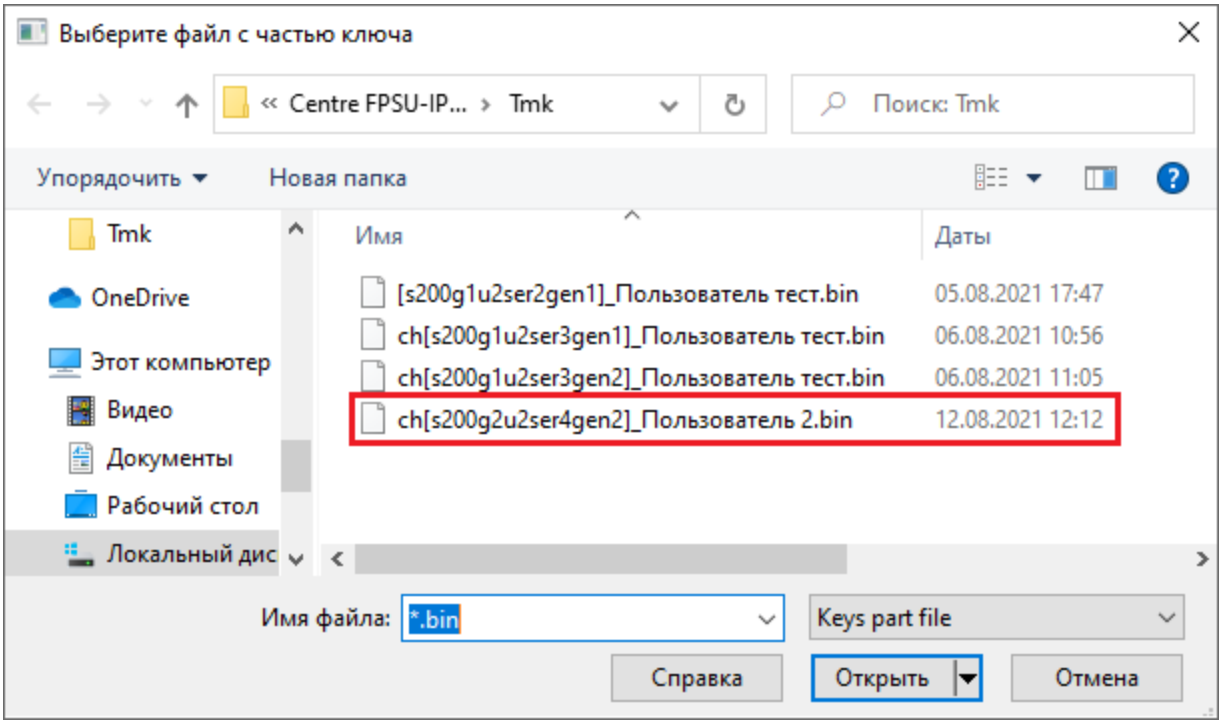


Рисунок 33 – Выбор файла для смены ключей

На экран будет выдано сообщение об успешной смене ключей:

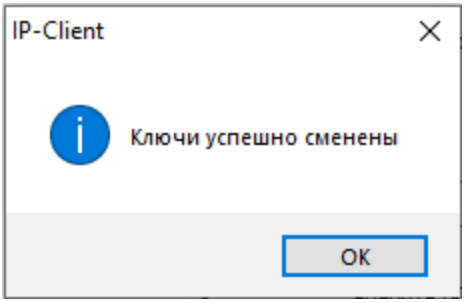


Рисунок 34 – Сообщение о смене ключей

Внесенные изменения необходимо подтвердить путем нажатия одноименной кнопки.

В случае введения неверного PIN-кода, после попытки выбора ключевой информации система выдаст следующее сообщение:

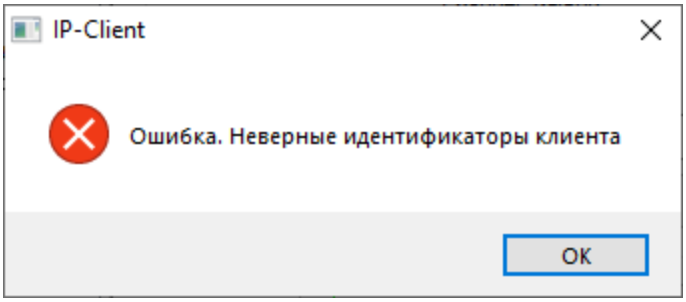


Рисунок 35 – Сообщение о неверном PIN-коде

5.4.2.8. Смена серии ключей через ФПСУ-RKL

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.

Смена ключей через интерфейс Клиента возможна только для устройств VPN-Key с версией микрокода 6.30+ и 7.0+. В остальных случаях ключевые данные необходимо менять на ЦГКК.

ФПСУ-RKL позволяет удобным и безопасным способом удаленно обновить ключевую информацию VPN-профиля на рабочих местах с установленным ФПСУ-IP/Клиентом.

Смена ключей возможна только в том случае, когда администратор ФПСУ-RKL разрешил данному пользователю сменить ключи удаленно через RKL.

Смена ключей через ФПСУ-RKL выполняется автоматически после установления соединения Клиента с ФПСУ-IP. Если администратор ФПСУ-IP установил новую серию ключей на ФПСУ-IP, на подключившемся клиенте прозрачно для пользователя Клиента будет выполнена процедура смены ключа.

Тем не менее, пользователь Клиента может вручную запросить смену ключа через ФПСУ-RKL. Для смены ключевых данных в интерфейсе Клиента требуется зайти в настройки устройства VPN-Key с полным доступом.

Для смены ключей с помощью ФПСУ-RKL в левой части окна настроек Клиента необходимо выбрать пункт «Смена ключей». В правой части окна настроек появится интерфейс управления сменой ключевых данных. Нажмите кнопку «Удаленная смена ключей» для перехода в окно создания запроса смены ключей к ФПСУ-RKL.

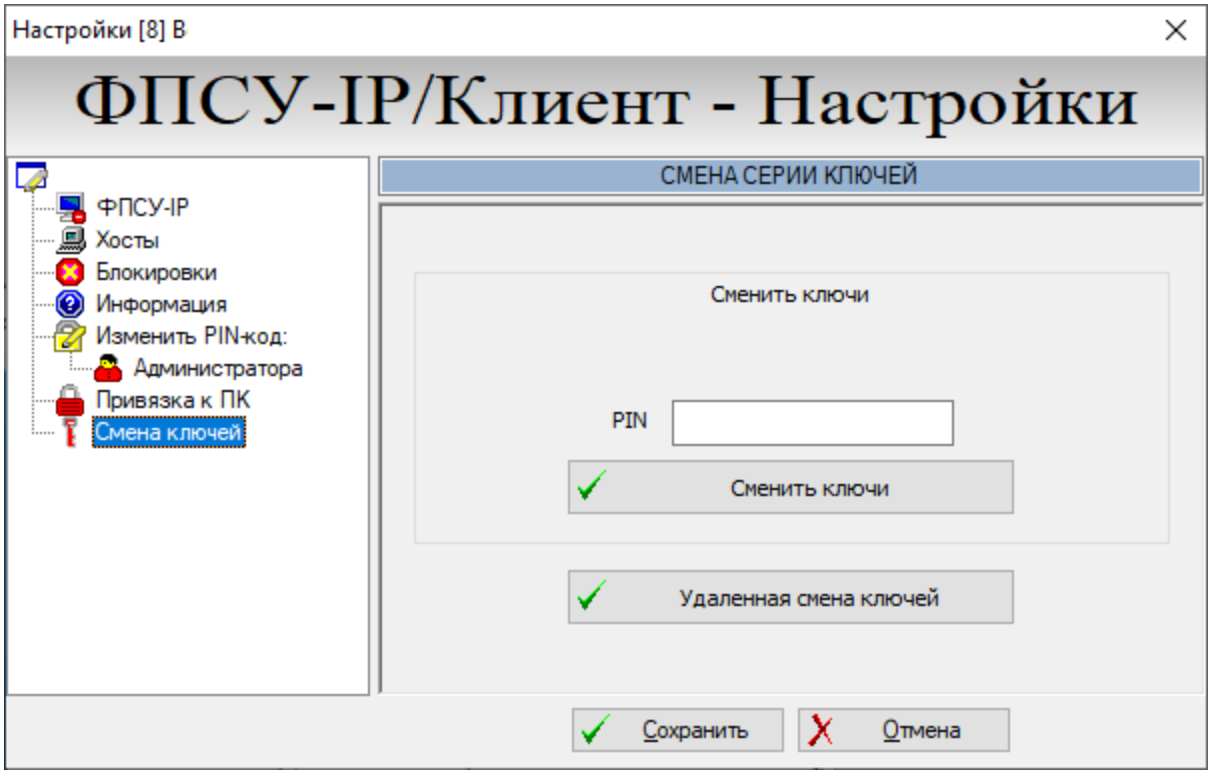


Рисунок 36 – Вкладка смены ключей

В открывшемся окне следует указать полученную от администратора безопасности информацию для запроса: IP-адрес ФПСУ-RKL, порт запроса. Из выпадающего поля выбора укажите сетевой адаптер, ведущий к указанному выше IP-адресу. Для отправления запроса нажмите клавишу «ОК»:

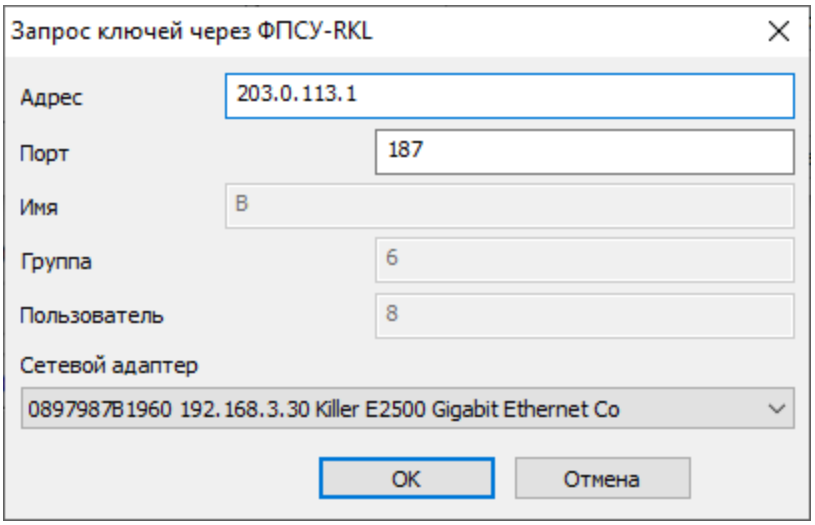


Рисунок 37 – Окно запроса к ФПСУ-RKL

В случае получения на ФПСУ-RKL и одобрения со стороны ФПСУ-RKL запроса, клиенту будут выданы новые ключи.

5.4.3. Обновление микрокода VPN-Key по запросу пользователя

Микрокод устройства VPN-Key может быть обновлён администратором VPN-Key вручную, при наличии *.FWU файла с обновлением микрокода.

Файл *.FWU должен быть получен доверенным способом от разработчика или организатора Криптосети Клиентов. На файл с обновленной версией микрокода должны быть рассчитаны контрольные суммы программой контроля целостности файлов FPSUHASH и сравнены с предоставленными разработчиком эталонными контрольными суммами.

Для обновления микрокода в окне регистрации пользователя (см. Рисунок «Регистрация пользователя VPN-Key») необходимо нажать кнопку «Подробнее».

Кнопка «Получить» открывшегося окна служит для формирования e-mail запроса к разработчику на обновление микрокода. При нажатии кнопки «Получить» с помощью настроенного в системе почтового клиента по умолчанию будет сформировано почтовое сообщение на адрес updates@amicon.ru с запросом обновления микрокода. Следует учитывать, что в случае отсутствия настройки e-mail клиента в операционной системе по умолчанию, то сообщение не будет сформировано.

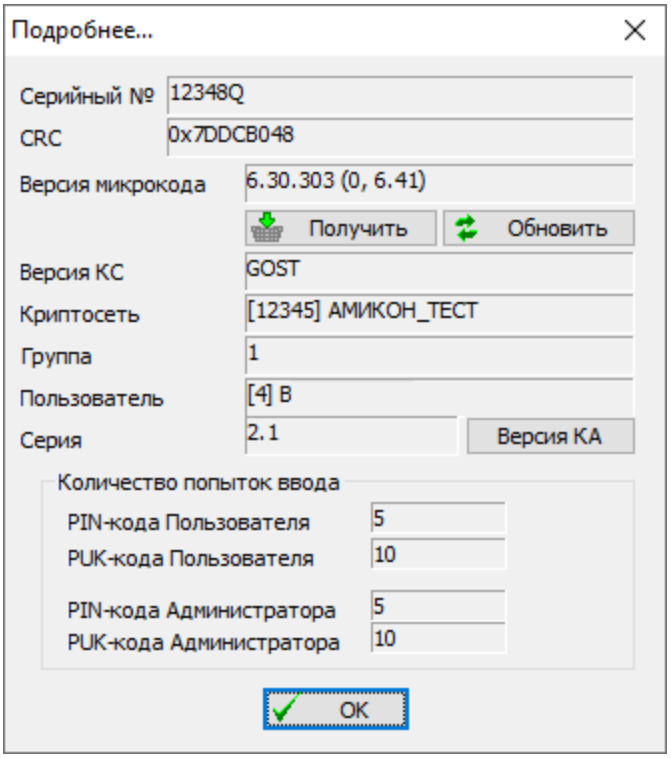


Рисунок 38 - Управление обновлениями микрокода

Файл с обновлением микрокода будет выслан в ответ на сообщение на адрес

отправителя электронного письма.

Микрокод представляет из себя файл с расширением *.FWU, прикладываемый к ответу на e-mail запрос. необходимо рассчитать контрольные суммы при помощи входящего в состав программного обеспечения Клиента программного модуля контроля целостности файлов FPSUHASH, и сверить с эталонными контрольными суммами в формуляре на СКЗИ.

Кнопка «Обновить» открывшегося окна служит для указания *.FWU файла и запуска процедуры обновления микрокода устройства VPN-Key. После нажатия кнопки «Обновить», откроется системное окно выбора файла, где необходимо указать месторасположение полученного *.FWU файла, содержащего обновление микрокода.

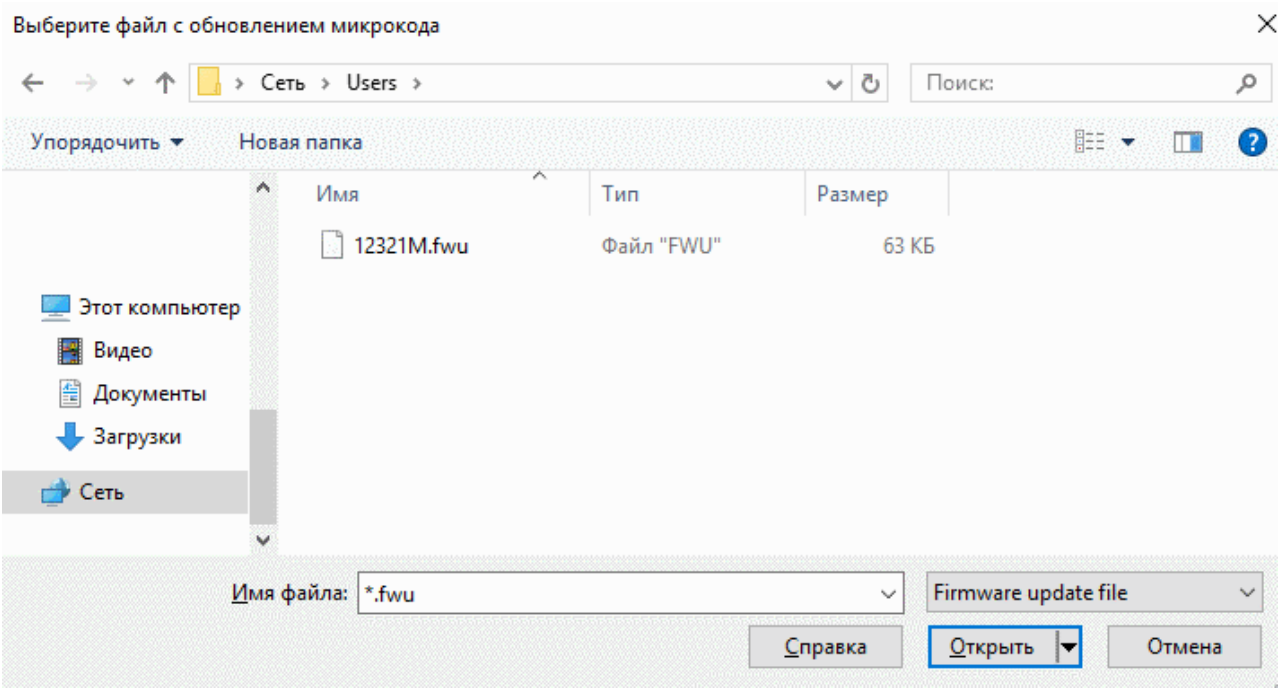


Рисунок 39 - Выбор .FWU файла

После указания и подтверждения выбора *.FWU файла следует дождаться сообщения об успешном завершении процедуры обновления внутреннего программного обеспечения устройства VPN-Key.

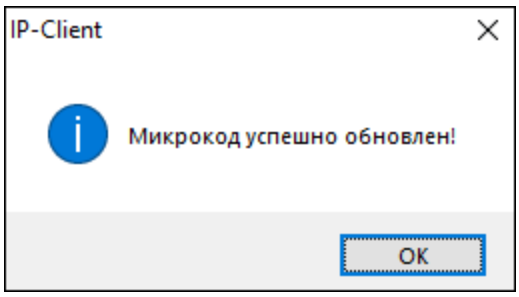


Рисунок 40 - Микрокод успешно обновлён

После получения сообщения следует отсоединить устройство VPN-Key от компьютера и перед дальнейшей эксплуатацией подключить заново.

5.5. Дополнительная информация о VPN-Key и VPN-профиле

При необходимости можно просмотреть дополнительную информацию о подключенном VPN-Key и хранящемся в нем VPN-профиле. Обозначенные сведения отображаются в дополнительном окне, открывающемся из окна соединения с ФПСУ-IP или окна настроек устройства VPN-Key:

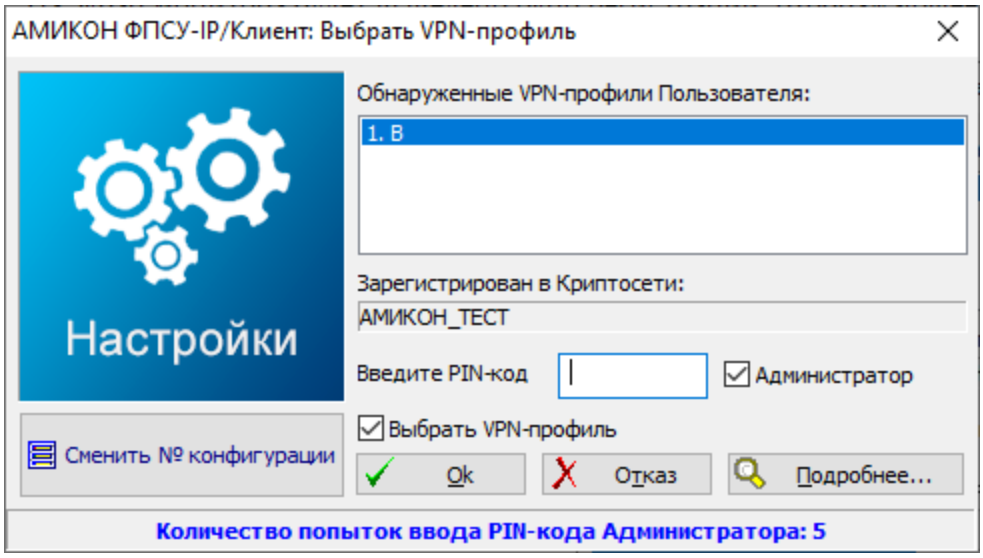


Рисунок 41 - Регистрация в ФПСУ-IP/Клиент

Для получения дополнительной информации о подключенном VPN-Key необходимо нажать кнопку «Подробнее».

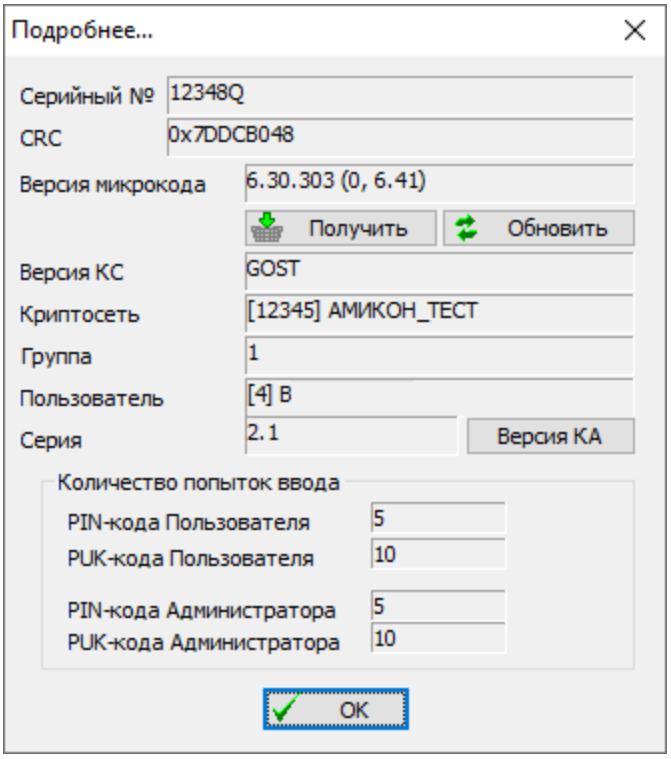


Рисунок 42 - Сведения об устройстве VPN-Key

На экране откроется окно, в котором отобразится:

- серийный номер устройства VPN-Key;
- контрольная сумма микрокода устройства VPN-Key в поле «CRC»;
- номера текущих версий программного обеспечения VPN-Key и ключевой системы;
- кнопки обновления микрокода «Обновить» и «Получить» (см. пункт «Обновление микрокода по запросу пользователя»);
- системные идентификаторы VPN-профиля, находящемся в устройстве VPN-Key;
- допустимое количество последовательных попыток ввода PIN-кодов устройства VPN-Key.

6. Программный Клиент

При использовании программного Клиента аутентификация пользователя на ФПСУ-IP при установлении соединения производится с применением VPN-профиля, выдаваемого Центром генерации ключей клиентов (ЦГКК).

Кроме VPN-профиля, Программному клиенту для работы с ФПСУ-IP требуется установленная лицензия на программное обеспечение.

Управление программой «ФПСУ-IP/Клиент» на рабочем месте осуществляется через контекстное меню, вызываемое нажатием правой клавиши мыши на значке программы в области уведомлений панели задач:  .

6.1. Начало работы с Программным Клиентом

Перед штатным использованием Программного Клиента необходимо выполнить предварительную настройку: добавить лицензию на использование программы и указать используемый VPN-профиль.

Предварительная настройка может быть выполнена администратором устройства VPN-Key/RKL («RLK-токена»), подробнее см. пункт «Добавление лицензии и VPN-профиля с помощью RKL-токена».

6.1.1. Добавление лицензии

Лицензия на использование программного обеспечения ФПСУ-IP/Клиента (файл формата *.bsn) передается в комплекте поставки программного обеспечения или получается с Сервера лицензирования. На одном рабочем месте пользователя ФПСУ-IP/Клиент используется одна лицензия. Без указания лицензии соединение с ФПСУ-IP будет невозможно выполнить. С одной лицензии можно установить только одно защищенное соединение с ФПСУ-IP - если установить одну и ту же лицензию на два рабочих места, одновременно соединиться с ФПСУ-IP будет возможно только с одного из этих двух рабочих мест.

Лицензию можно указать через локальный файл, или запросить с Сервера Лицензирования (подробнее см. пункт «Добавление лицензии с Сервера лицензирования»).

Для того, чтобы ввести лицензию через локальный файл, необходимо в основном меню ФПСУ-IP/Клиента, открывающемся по нажатию на значок программы правой

клавишей мыши, выбрать подпункт «Лицензия» пункта меню «Программный клиент» и нажать «Ввести лицензию».

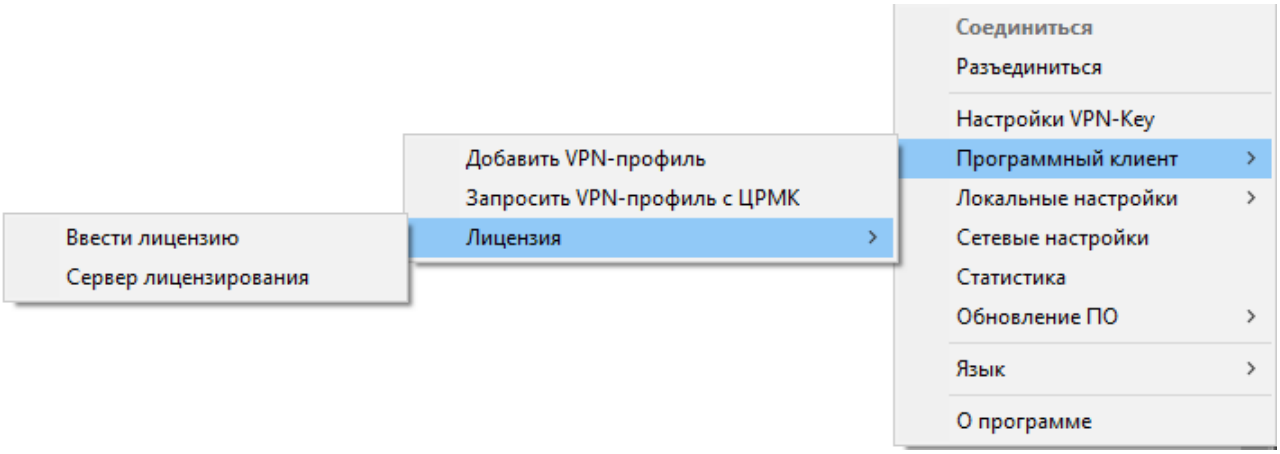


Рисунок 43 - Команда ввода лицензии

В открывшемся системном окне выбора файлов необходимо указать местоположение файла лицензии на данный экземпляр программного обеспечения(файл с расширением *.bsn, должен быть получен от поставщика программного обеспечения или администратора безопасности) и нажать «Открыть». Система выдаст подтверждение того, что лицензия (серийный номер) был добавлен:

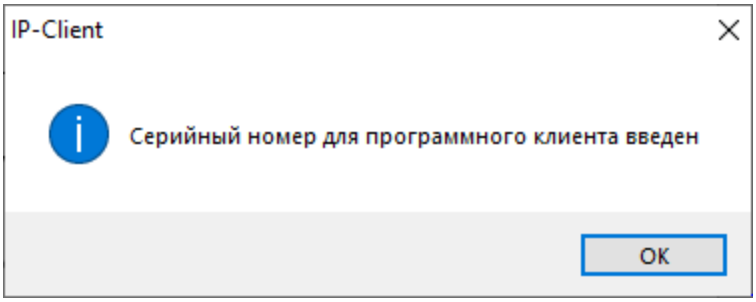


Рисунок 44 - Сообщение о добавлении серийного номера

При необходимости можно просмотреть более подробные сведения о введенной ранее лицензии (серийном номере). Для того, чтобы просмотреть эту информацию, необходимо выбрать в основном меню подпункт «Лицензия» пункта меню «Программный клиент» и нажать на наименовании лицензии. На экран будет выведена информация о лицензии (серийном номере).

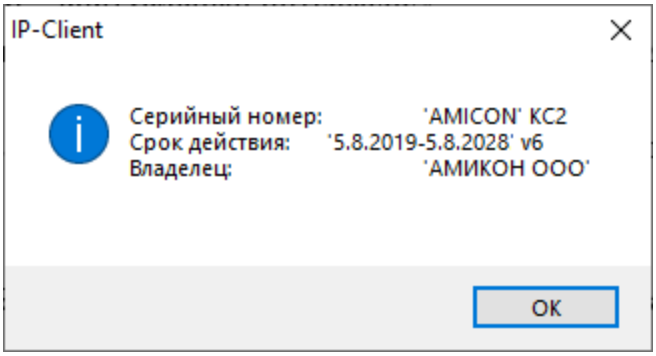


Рисунок 45 - Сведения о серийном номере

6.1.2. Добавление VPN-профиля

VPN-профиль передается от администратора ЦГКК на рабочую станцию пользователя в виде файла с расширением .bin. Кроме этого, предоставляется возможность запросить VPN-профиль через сеть из Центра распределения мобильных ключей (подробнее см. пункт «Добавление VPN-профиля с ЦРМК»). Для того, чтобы добавить из локального файла новый VPN-профиль в Программного Клиента и установить его ключи, необходимо выбрать подпункт «Добавить VPN-профиль» пункта меню «Программный клиент».

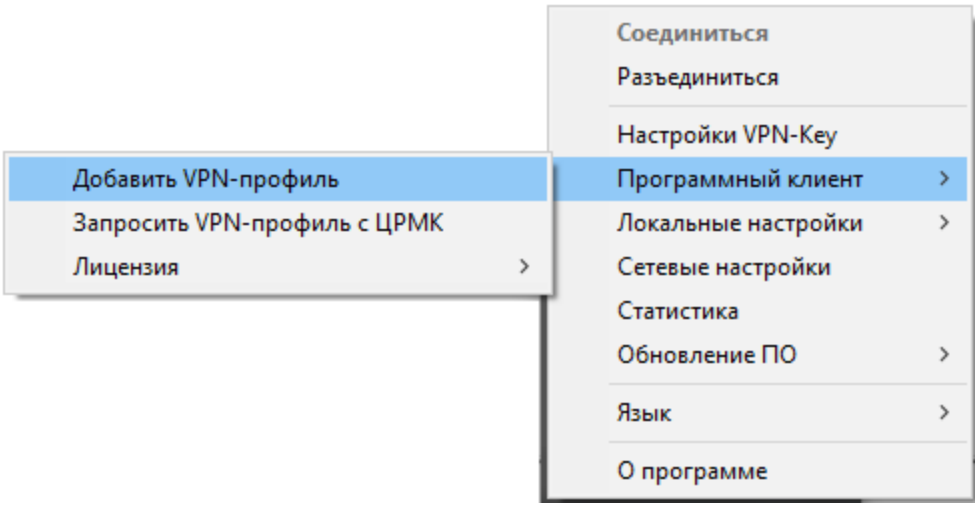


Рисунок 46 - Добавление ключа

В открывшемся окне укажите местонахождение полученного от администратора ЦГКК файла формата *.bin и нажмите кнопку «Открыть».

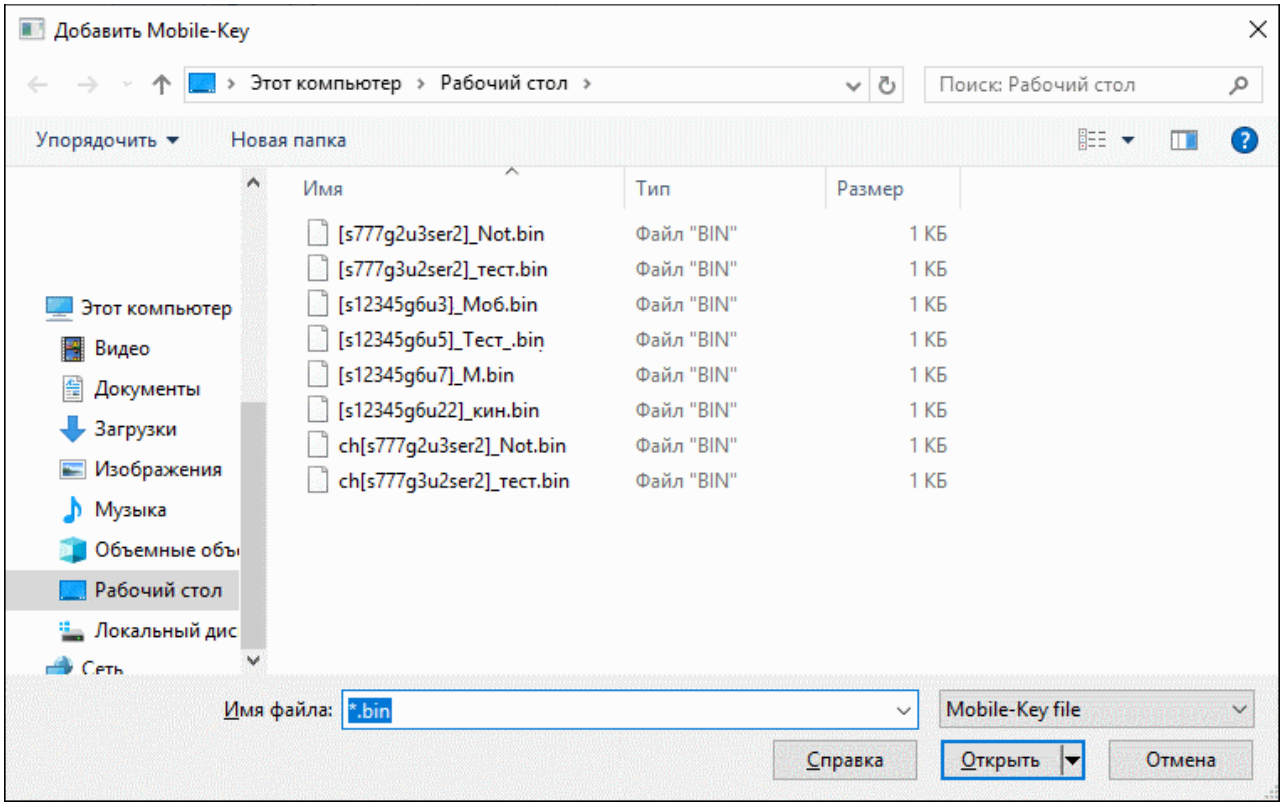


Рисунок 47 - Добавление ключа

Программа выдаст сообщение об успешном добавлении VPN-профиля в Программного Клиента.

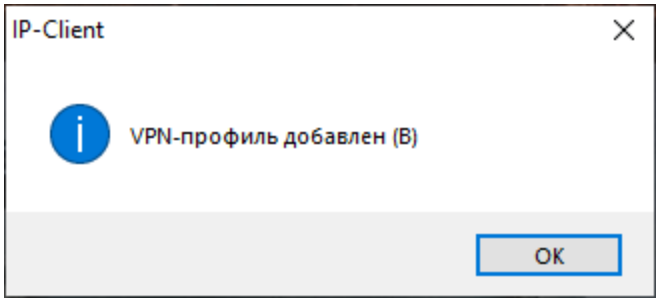


Рисунок 48 - Сообщение об успешном создании VPN-профиля

В случае, если в качестве профиля указан файл неподходящего формата или файл с искаженным содержанием, будет выдано сообщение об ошибке добавления VPN-профиля. Повторите процедуру, указав корректный файл VPN-профиля.

6.1.3. Добавление лицензии и VPN-профиля с помощью RKL-токена

Лицензия и VPN-профиль на рабочее место пользователя могут быть добавлены другим пользователем (администратором безопасности, сервисным инженером, инженером

технической поддержки и т. д.) с помощью специального устройства VPN-Key/RKL (RKL-токена).

Для выполнения задачи пользователь RKL-токена должен подключить RKL-токен к АРМ Программного Клиента, авторизоваться в Программном Клиенте с помощью PIN-кода RKL-токена и выполнить ряд запросов к ФПСУ-IP, настроенному на работу с данным RKL-токеном (ФПСУ-RKL). Параметры подключения RKL-токена к ФПСУ-RKL могут быть заданы заранее на ЦГКК администратором безопасности, а так же могут быть изменены администратором RKL-токена (подробнее см. раздел «Администрирование программно-аппаратного Клиента»).

ФПСУ-RKL выдает VPN-профили в ответ на программный запрос Клиента с подключенным RKL-токеном, и так же является посредником, защищающим взаимодействие Программного Клиента и выдающего лицензии Сервера лицензирования. Общая схема применения RKL-токена для установки лицензии и VPN-профиля на АРМ Программного Клиента приводится ниже.

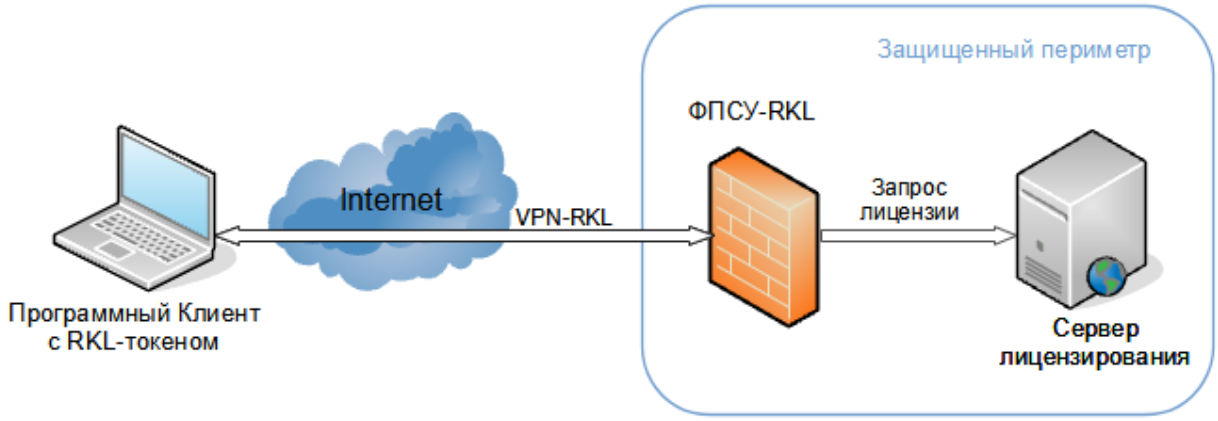


Рисунок 49 - Соединение с ФПСУ-RKL с помощью RLK-токена

Для добавления лицензии и VPN-профиля на АРМ пользователя ФПСУ-IP/Клиента владельцу RKL-токена необходимо выполнить следующие действия:

1. Подключить RKL-токен к USB-порту рабочей станции и выполнить команду контекстного меню «Соединиться».

На экран будет выдано стандартное окно установления соединения с ФПСУ-IP:

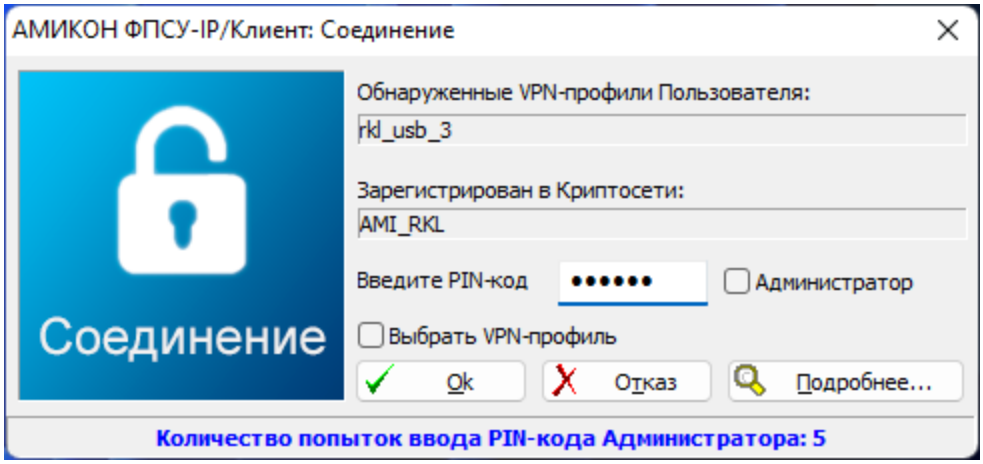


Рисунок 50 - Соединение с ФПСУ-RKL с помощью RLK-токена

Необходимо проверить, что для организации соединения выбран находящийся в RKL-токене VPN-профиль, принадлежащий специальной RKL-криптосети. Проверка выполняется по именам, указанных в полях «Обнаруженные VPN-профили Пользователя» и «Зарегистрирован в Криптосети:». Эти имена должны совпадать с назначенными администратору RKL-токена именами.

После проверки введите пользовательский PIN-код доступа к RKL-токену и подтвердите установление соединения, нажав кнопку «Ok».

ВНИМАНИЕ! После установления соединения RKL-токена с ФПСУ-RKL, любая прочая сетевая активность рабочей станции ограничивается, Программному Клиенту и остальным программам операционной системы сетевые пакеты разрешено передавать только в адрес ФПСУ-RKL!

2. После успешного установления соединения с ФПСУ-RKL на экран будет выведено служебное окно с вопросом, требуется ли запросить лицензию на программу:

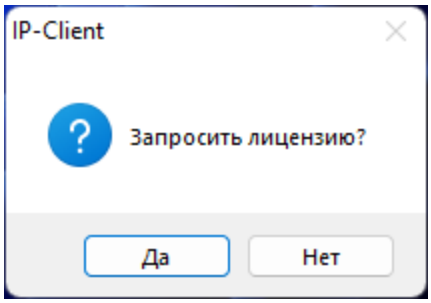


Рисунок 51 - Окно запроса лицензии

Если лицензия на Программного Клиента была ранее установлена, можно в данном окне нажать «Нет» и перейти к шагу запроса VPN-профиля (5-й шаг процедуры).

Если лицензия на Программного Клиента не была ранее установлена на рабочее

место, нажмите «Да» для формирования запроса на лицензию у Сервера лицензирования через ФПСУ-RKL.

3. Программа выведет окно указания логина и пароля пользователя для авторизации на Сервере Лицензирования:

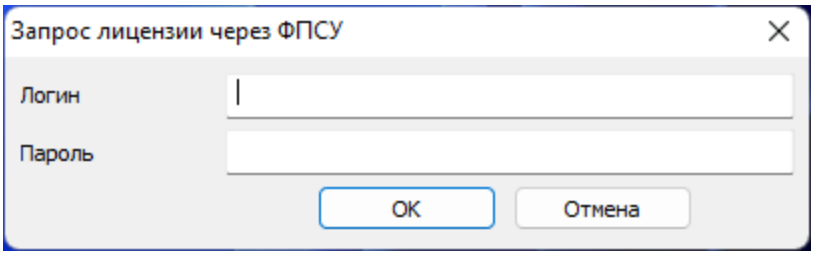


Рисунок 52 - Опциональная авторизация на Сервере Лицензирования

Ввод запрашиваемого «Логина» и «Пароля» опционален и зависит от настроек Сервера Лицензирования. Если администратором безопасности указано что необходимо вводить логин и пароль для запроса лицензии, их следует ввести. Если Сервер Лицензирования выдает лицензии без дополнительной авторизации по логину и паролю, следует оставить поля пустыми и подтвердить запрос, нажав «ОК».

4. В случае успешного запроса и получения лицензии программой будет выведено служебное окно:

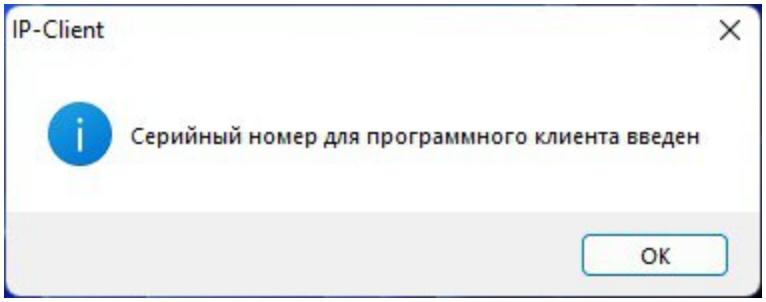


Рисунок 53 - Опциональная авторизация на Сервере Лицензирования

Для продолжения нажмите «ОК».

5. Программа перейдет к следующему обязательному шагу - запросу VPN-профиля у ФПСУ-RKL. На экран будет выведено окно формирования запроса:

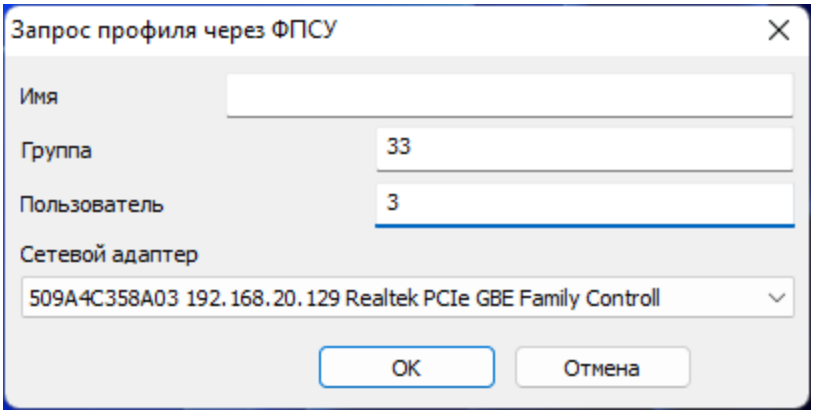


Рисунок 54 - Запрос профиля

В окне запроса VPN-профиля следует указать передаваемые на ФПСУ-RKL параметры запроса:

«Имя» - опциональное поле. Необходимость и параметры заполнения следует уточнять у администратора безопасности. По умолчанию - не заполняется;

«Группа» - в этом поле указывается номер группы, для пользователя которой запрашивается VPN-профиль;

«Пользователь» - в этом поле указывается номер пользователя, которому выдается VPN-профиль.

Номера группы и пользователя следует уточнять у администратора ФПСУ-RKL и ЦГКК.

Диалог выбора сетевого адаптера выводит MAC- и IP-адреса сетевого адаптера, который ведет к ФПСУ-RKL и носит справочный характер. Не рекомендуется менять указанный по умолчанию сетевой адаптер.

После заполнения полей подтвердите отправление запроса, нажав кнопку «ОК».

6. После успешного выполнения запроса и получения VPN-профиля для Программного Клиента, на экран будет выдано RKL-окно с сообщением "VPN-профиль добавлен":

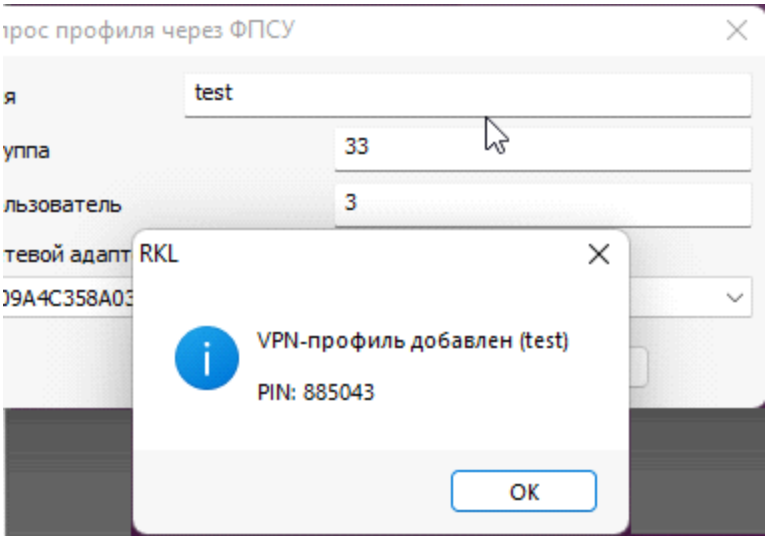


Рисунок 55 - Запрос VPN-профиля выполнен успешно

6.2. Соединение Программного Клиента с ФПСУ-IP

Основным назначением ФПСУ-IP/Клиента является организация соединения с ФПСУ-IP для безопасного доступа к защищенным ФПСУ-IP рабочим станциям. Для установления соединения с ФПСУ-IP, на АРМ Программного Клиента требуется предварительно установить лицензию на использование программы и VPN-профиль пользователя. В отсутствие лицензии или VPN-профиля Программный Клиент не сможет соединиться с ФПСУ-IP.

Для установления соединения с ФПСУ-IP необходимо выполнить следующие действия:

1. Открыть контекстное меню ФПСУ-IP/Клиента;
2. Выбрать пункт «Соединиться».

На экран будет выдаваться сообщение о начале регистрации пользователя, отображающее список добавленных VPN-профилей. Следует учитывать, что буквой «М» в данном окне будут помечены VPN-профили программного Клиента:

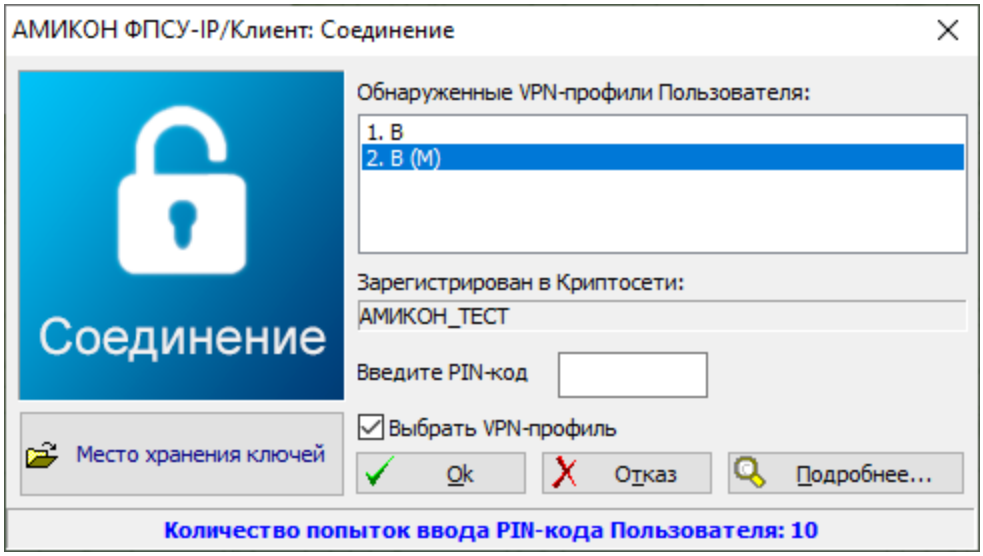


Рисунок 56 - Окно регистрации пользователя ФПСУ-IP/Клиента

По умолчанию окно регистрации открывается в статусе расширенных настроек (флаг «Выбрать VPN-профиль» установлен). При снятии указанного флага окно регистрации в дальнейшем будет открываться с данными VPN-профиля, авторизовавшегося в ФПСУ-IP/Клиенте последним;

3. Выбрать необходимый VPN-профиль.

Следует иметь в виду, что при установке в качестве места хранения ключей жесткого диска компьютера, жесткий диск становится носителем ключевой информации. Для того, чтобы избежать возникновения подобной ситуации, в качестве места хранения ключевой информации следует использовать съемный носитель.

В случае хранения ключевой информации на съемном носителе подключить его к USB-порту компьютера;

4. Ввести в соответствующее диалоговое поле окна регистрации PIN-код и нажать «ОК».

Если настройки VPN-профиля пользователя содержат установку запоминания PIN-кода, то идентификация пользователя производиться не будет, а ФПСУ-IP/Клиент начнет производить попытки соединения с ФПСУ-IP;

5. Если вводимые персональные коды верны и количество попыток их ввода не превышено, ФПСУ-IP/Клиент считает идентификацию пользователя завершенной и пытается установить VPN-туннель с ФПСУ-IP. При этом на экран выдается информационное окно, отображающее процесс установления соединения.

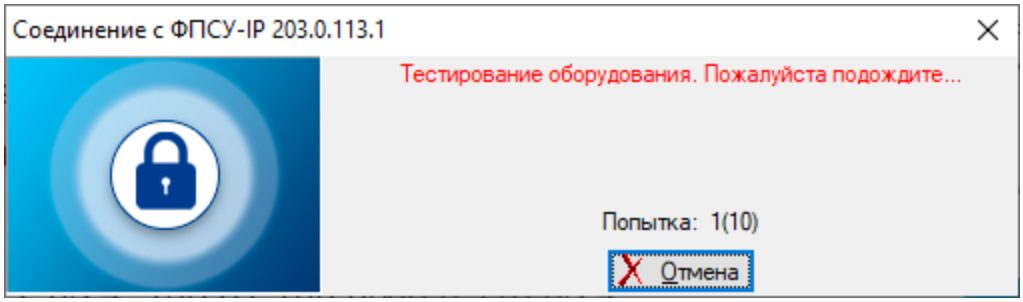


Рисунок 57 - Соединение с ФПСУ-IP

Если попытки соединиться с ФПСУ-IP окажутся неудачными, на экран будет выведено одно из диагностических сообщений, которые приведены в таблице («Сообщения об ошибках при соединении с ФПСУ-IP») вместе с комментариями;

6. Если VPN-туннель с ФПСУ-IP установлен, на экран может быть выдано окно опциональной авторизации через Radius-сервер. Необходимость авторизации через Raduis-сервер устанавливается администратором ФПСУ-IP.

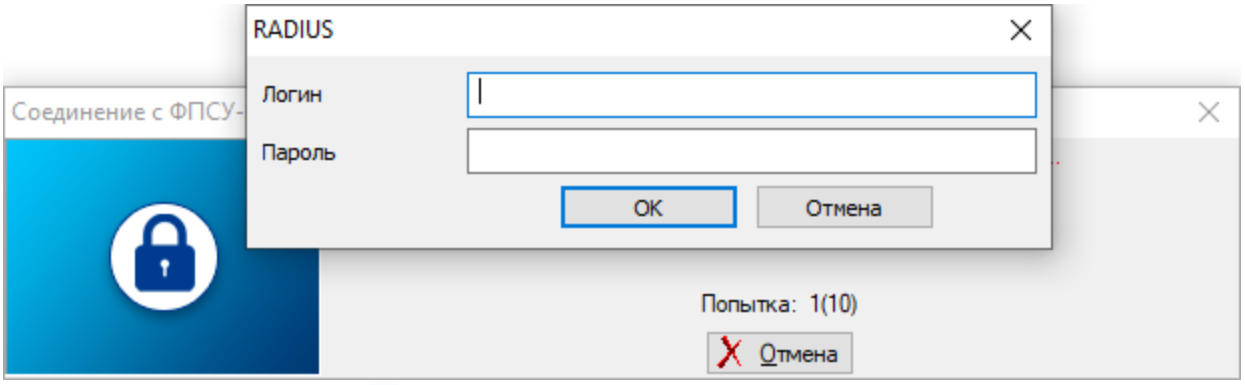


Рисунок 58 - Опциональная авторизация по RADIUS

В случае появления окна Raduis-авторизации, необходимо указать в появившемся окне учетные данные пользователя и пароль (или комбинацию паролей, в зависимости от настроек Raduis-сервера). Учетные данные и пароль должны быть получены от администратора Raduis-сервера;

7. Если доступ пользователю разрешается, окно «Соединение» закроется, а значок программы ФПСУ-IP/Клиент внизу экрана изменит свой вид  . После установления соединения с ФПСУ-IP АРМ Клиента может взаимодействовать с рабочими станциями и серверами защищенной сети.

Соединение «ФПСУ-IP/Клиента» с ФПСУ-IP может быть осуществлено из командной строки с помощью команды:

««DRIVE:\Program Files\Amicon\Client FPSU-IP\ip-client.exe» connect» из командной

строки (в том числе и удаленно).

Аналогично возможно вручную выполнить разрыв установленного с ФПСУ-IP VPN-туннеля командой: ««DRIVE:\Program Files\Amicon\Client FPSU-IP\ip-client.exe» disconnect».

Для окончания сеанса связи и завершения работы VPN-туннеля с ФПСУ-IP необходимо воспользоваться командой «Разъединиться» контекстного меню ФПСУ-IP/Клиента.

6.3. Настройки Программного Клиента

6.3.1. Добавление лицензии с Сервера лицензирования

Если в сети организации установлен и задействован Сервер Лицензирования ФПСУ-IP/Клиентов, то лицензию для Программного Клиента можно запросить с него, исключая необходимость вручную передавать файл с лицензией на рабочее место с установленным Программным Клиентом.

Для запроса лицензии с сервера следует в основном меню ФПСУ-IP/Клиента, открывающемся по нажатию на значок программы правой клавишей мыши, выбрать выбрать подпункт «Лицензия» пункта основного меню «Программный клиент» и нажать «Сервер лицензирования».

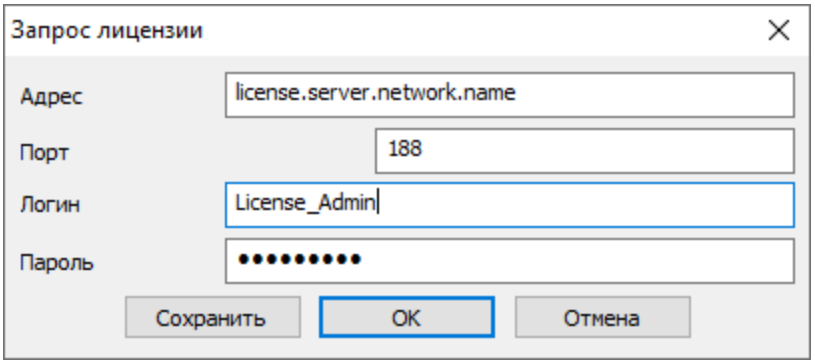


Рисунок 59 - Запрос лицензии с сервера лицензирования

В открывшемся окне следует заполнить все поля. Адрес и порт сервера лицензирования, логин и пароль запрашивающего лицензию пользователя следует уточнять у администратора безопасности сети. Введенные данные можно сохранить в Программном Клиенте для последующих запросов, нажав клавишу «Сохранить».

После заполнения полей подтвердите запрос к серверу, нажав клавишу «ОК». ФПСУ-IP/Клиент выполнит запрос к Серверу лицензирования. Если на Сервере лицензирования администратором безопасности разрешена выдача лицензии для указанного логина и

пароля, то лицензия на Программный Клиент будет загружена по сети и установлена в ФПСУ-IP/Клиент.

6.3.2. Удаление лицензии

При необходимости замены лицензии она может быть удалена из Программного Клиента. ВНИМАНИЕ! После удаления лицензии для VPN-профилей программного клиента будут доступны только настройки. Создание VPN-туннелей с использованием сформированных ранее VPN-профилей программного Клиента в отсутствии лицензии невозможно.

Для удаления лицензии необходимо выбрать подпункт «Лицензия» пункта основного меню «Программный клиент» и нажать «Удалить лицензию».

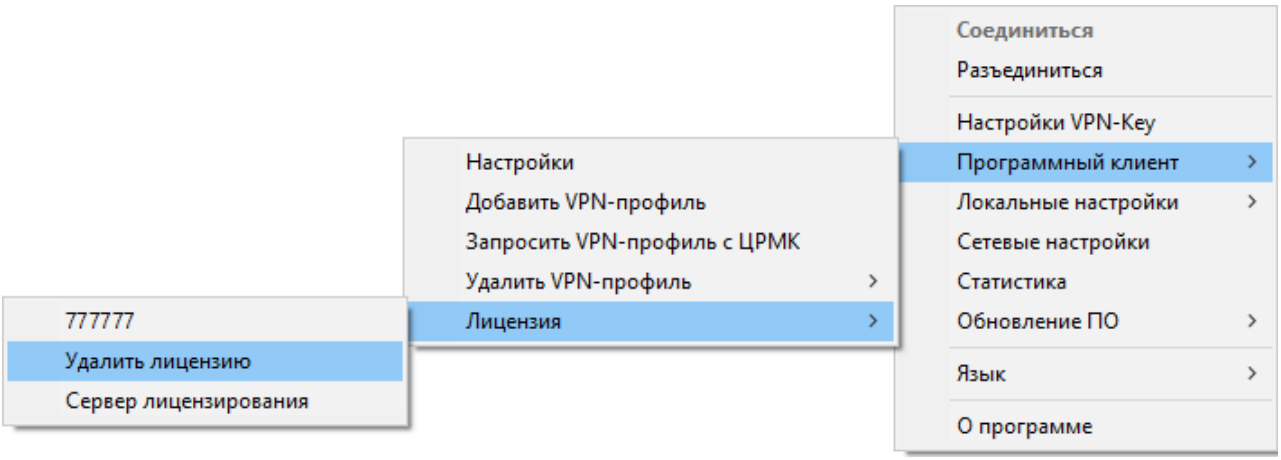


Рисунок 60 - Удаление лицензии

После выполнения команды «Удалить лицензию» программа уточнит необходимость удаления лицензии для Программного Клиента.

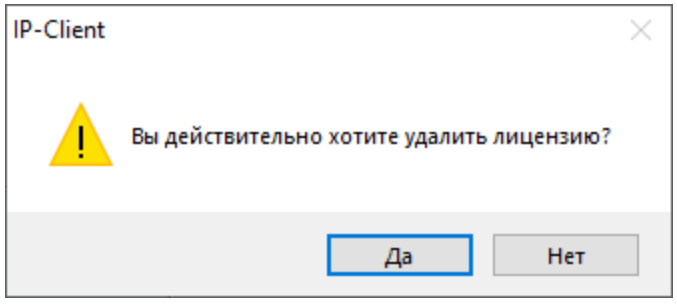


Рисунок 61 - Подтверждение необходимости удаления лицензии

После нажатия кнопки «Да» лицензия будет удалена

6.3.3. Добавление VPN-профиля с ЦРМК

Помимо передачи VPN-профиля от администратора ЦГКК на рабочую станцию пользователя в виде файла с расширением .bin, существует способ получения VPN-профиля через сеть, с помощью запроса к специальному сетевому сервису Центру распределения мобильных ключей (ЦРМК).

Запрос профиля с ЦРМК возможен только в том, когда администратор ЦРМК разрешил данному пользователю получать VPN-профиль по сети и выдал пользователю необходимую для выполнения запроса информацию.

Для создания запроса к ЦРМК на получение VPN-профиля по сети, необходимо выбрать подпункт «Запросить VPN-профиль с ЦРМК» пункта меню «Программный клиент»:

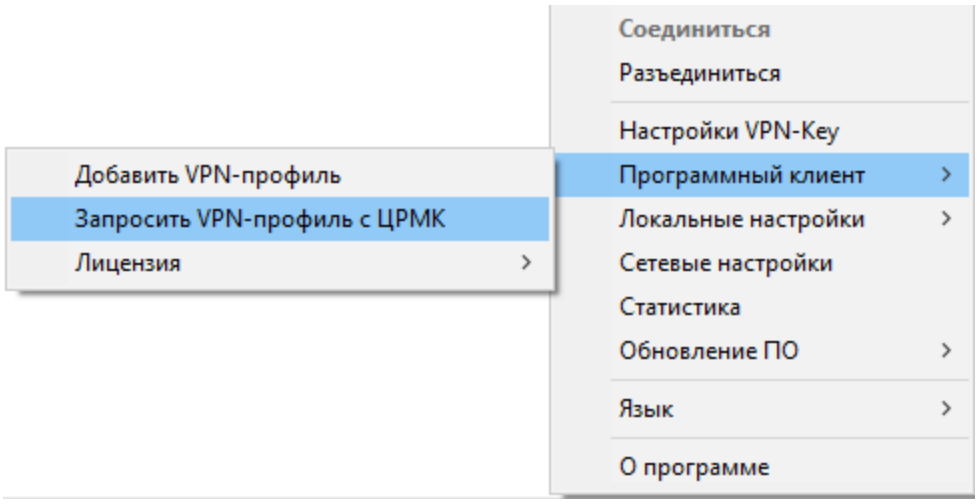


Рисунок 62 - Добавление ключа

Появится окно подготовки запроса к ЦРМК. В нём следует заполнить все поля. Информацию для заполнения полей следует получить у администратора ЦРМК или администратора безопасности. Указываются:

Сервер - IP адрес сетевого сервиса ЦРМК;

Порт - порт сетевого сервиса ЦРМК;

Логин - специальное имя пользователя для запроса VPN-профиля;

ID - служебный идентификатор запроса;

Пароль запроса - пароль, привязанный к логину и ID запроса, подтверждающий запрос.

Все эти данные можно заполнить из специального графического файла-памятки с QR-кодом, выдаваемым администратором ЦРМК. Программа может считать данные

находящегося в графическом файле QR-кода и заполнить все поля запроса. Файл с QR-кодом указывается по команде "Заполнить из QR-кода":

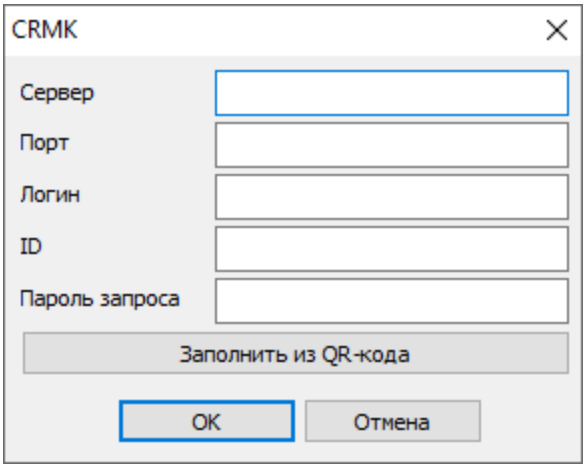


Рисунок 63 - Добавление ключа

После заполнения полей, для отправления запроса на ЦРМК нажмите кнопку «ОК». Если все параметры указаны верно и ЦРМК доступен, в ответ на запрос будет выслан VPN-профиль, программа автоматически его установит.

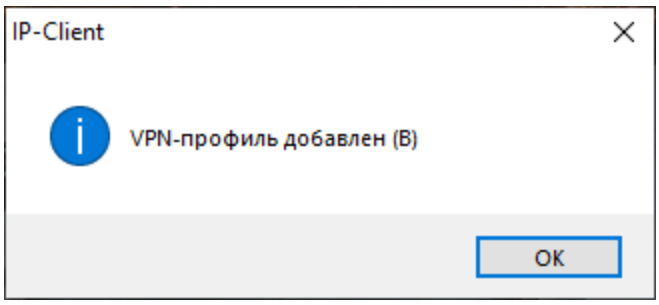


Рисунок 64 - VPN-профиль получен и установлен

6.3.4. Особенности хранения VPN-профилей

Изначально VPN-профили прописываются в папку программного обеспечения (по умолчанию «SYSTEMDISK:\Program Files\AMICON\Client FPSU-IP\Reginfo»). PIN-код к VPN-профилю является ключом доступа к настройкам VPN-профилю.

Следует иметь в виду, что при установке в качестве места хранения ключей жесткого диска компьютера, жесткий диск становится носителем ключевой информации. Для того, чтобы избежать возникновения подобной ситуации, в качестве места хранения ключевой информации следует использовать съемный носитель (Соединение Программного Клиента с ФПСУ-IP). При этом на жестком диске в папке программного обеспечения сохраняется VPN-профиль без ключа, а сам ключ записывается на съемный носитель.

Чтобы использовать съемный диск в качестве носителя следует:

- подключить съемный носитель к USB-порту компьютера;
- установить в окне регистрации ФПСУ-IP/Клиента флаг «Выбрать VPN-профиль»;
- нажать кнопку «Место хранения ключей» и выбрать путь ко внешнему носителю.

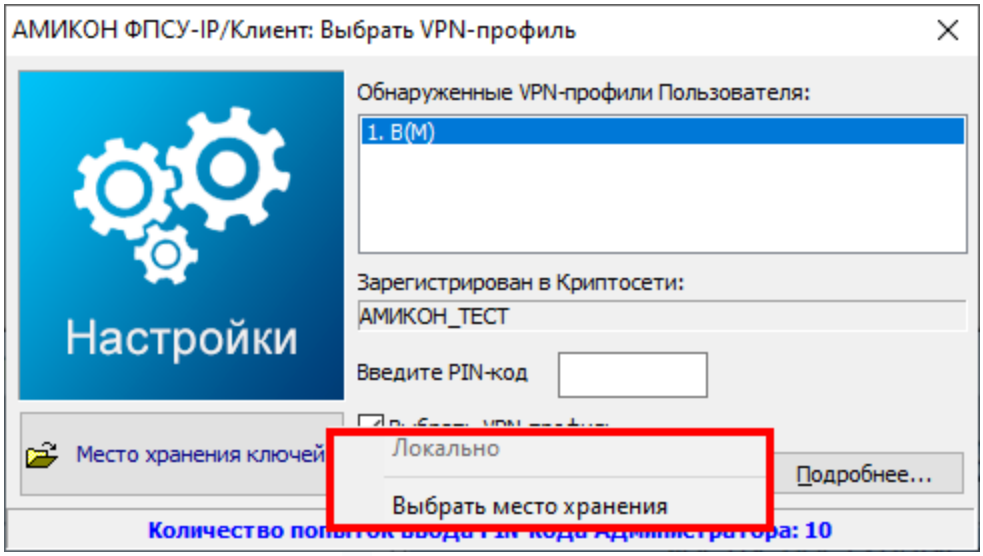


Рисунок 65 - Расширенные настройки

Следует иметь в виду, что, в случае хранения ключевой информации на съемном носителе, для соединения с ФПСУ-IP обязательно подключение этого носителя к USB-порту компьютера.

6.3.5. Удаление VPN-профиля

При необходимости VPN-профиль может быть удален. Для того, чтобы удалить VPN-профиль, необходимо выбрать подпункт «Удалить VPN-профиль» пункта основного меню «Программный клиент», после чего отметить необходимую запись.

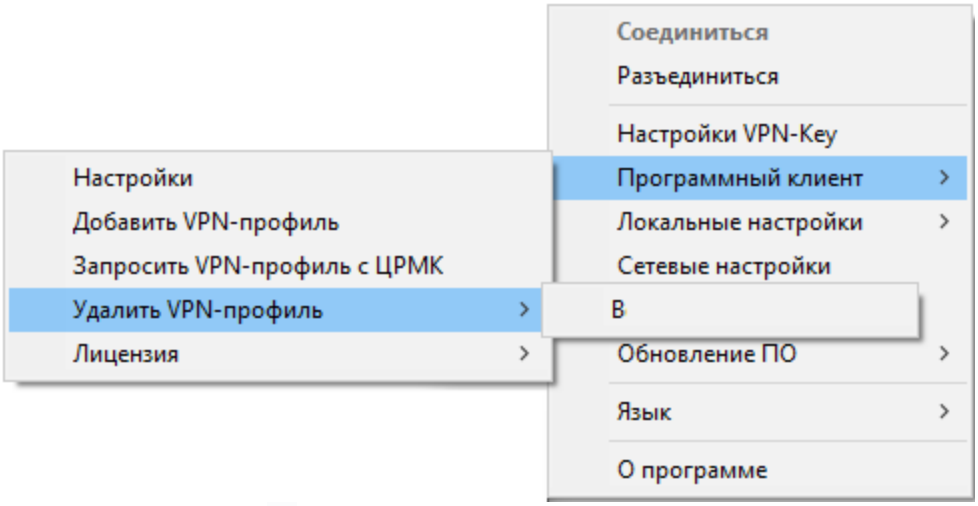


Рисунок 66 - Выбор VPN-профиля для удаления

Система выдаст запрос на подтверждение необходимости удаления VPN-профиля:

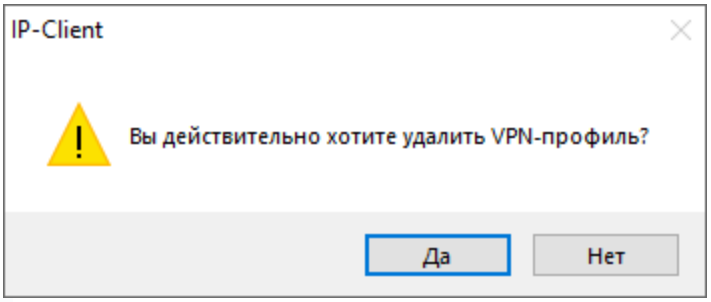


Рисунок 67 - Подтверждение необходимости удаления VPN-профиля

После нажатия кнопки «Да» VPN-профиль будет удален из Программного Клиента.

6.3.6. Настройка параметров VPN-профиля

Управление «ФПСУ-IP/Клиентом» и хранящимися в нём VPN-профилями осуществляется через контекстное меню, вызываемое нажатием правой клавиши мыши на значке программы в области уведомлений панели задач.

Следует учитывать то, что при работе с Программным Клиентом получивший PIN-код доступа к VPN-профилю пользователь обладает правами администратора и программы и VPN-профиля.

После добавления первого VPN-профиля в пункте основного меню «Программный клиент» становится доступным пункт «Настройки».

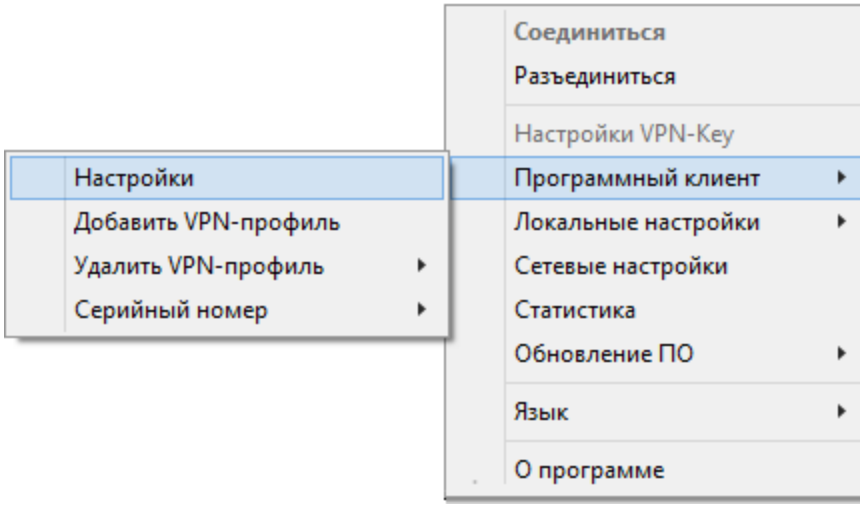


Рисунок 68 - Настройки программного Клиента

После выбора подпункта «Настройки» на экран монитора будет выведено окно регистрации. По умолчанию окно регистрации открывается в статусе расширенных настроек (флаг «Выбрать VPN-профиль» установлен). При снятии указанного флага окно регистрации в дальнейшем будет открываться с данными VPN-профиля, авторизовавшегося в ФПСУ-IP/Клиенте последним.

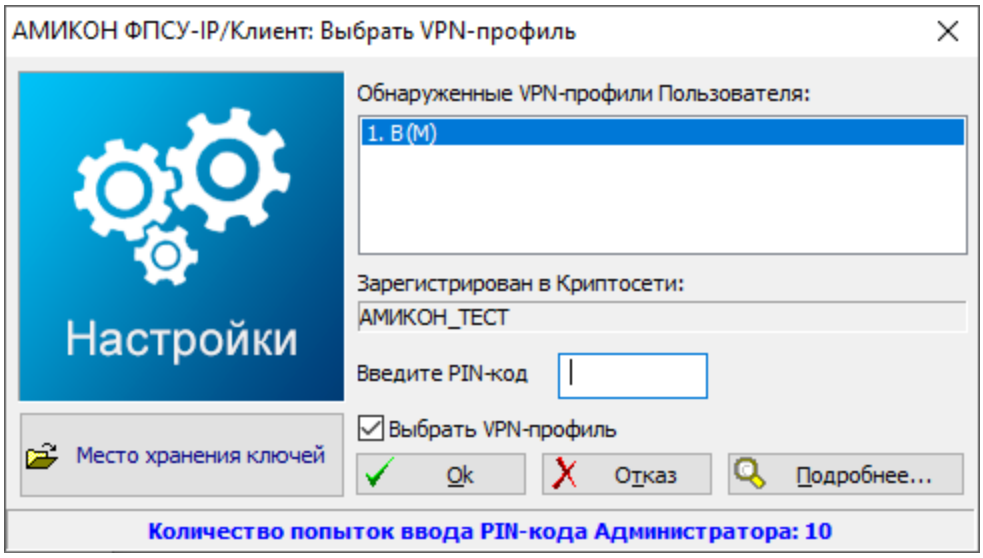


Рисунок 69 - Авторизация для редактирования VPN-профиля

В окне регистрации пользователя необходимо выбрать VPN-профиль и ввести PIN-код доступа к VPN-профилю. В случае хранения ключевой информации на съемном носителе (подробнее см. пункт Особенности хранения VPN-профилей) необходимо подключить его к USB-порту компьютера.

Если введенный код не соответствует данным, заложенным в ключевой информации, он будет запрошен снова. Количество попыток ввода PIN-кода администратора VPN-

профиля ограничено десятью попытками, после чего VPN-профиль будет заблокирован.

Если регистрация администратора завершена успешно, на экран монитора будет выведено окно настроек. Левая часть окна содержит список доступных параметров VPN-профиля, а правая отображает значения установок текущего параметра.

6.3.6.1. Настройка подключения к ФПСУ-IP

Для просмотра или редактирования настроек параметров подключения клиента к ФПСУ-IP, в левой части окна настроек необходимо выбрать строку «ФПСУ-IP».

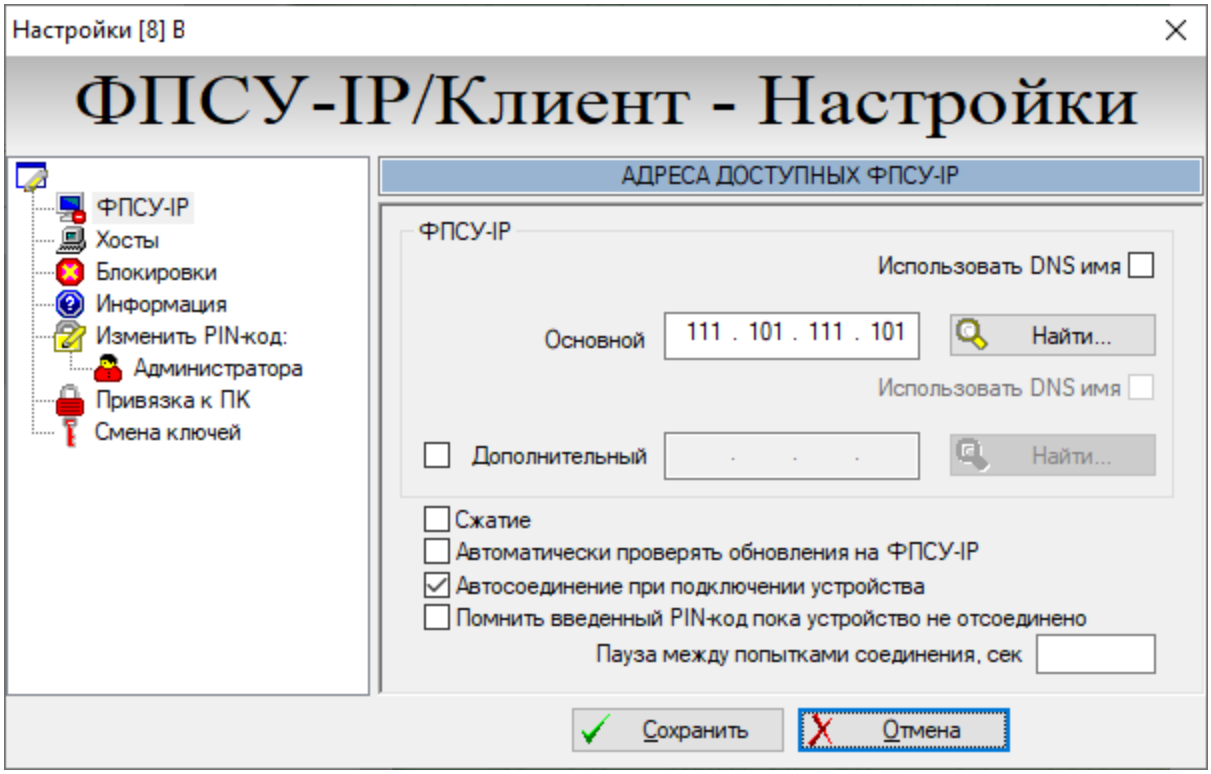


Рисунок 70 - Настройки работы Клиента с ФПСУ-IP

В поле «Основной» в правой части окна необходимо ввести IP-адрес ФПСУ-IP, через который будет осуществляться доступ ФПСУ-IP/Клиента к защищенным рабочим станциям и серверам.

Если сетевым службам компьютера доступны средства разрешения Интернет-имен (есть поддержка службы DNS), по нажатию кнопки «Найти» можно запросить IP-адрес ФПСУ-IP с известным именем у обслуживающего DNS сервера. Вместо указания IP-адреса ФПСУ-IP можно сохранить в настройках DNS-имя, установив опцию «Использовать DNS-имя». В этом случае перед установлением соединения ФПСУ-IP/Клиента с ФПСУ-IP будет каждый раз выполняться DNS-запрос на получение IP-адреса ФПСУ-IP у обслуживающего рабочую станцию DNS-сервера.

Если в локальной сети имеется еще один ФПСУ-IP, который может предоставить доступ ФПСУ-IP/Клиенту в случае отсутствия связи с основным ФПСУ-IP, необходимо установить флаг в поле «Дополнительный» и указать его IP-адрес в окне справа (либо воспользоваться кнопкой «Найти», как описано выше).

Если канал связи с ФПСУ-IP обеспечивает скорости передачи данных не выше 5 Мбит/с, рекомендуется указать ФПСУ-IP/Клиент на необходимость сжатия данных перед передачей их в VPN-туннель (для чего следует установить флаг «Сжатие»). При более высоких скоростях соединения эта опция неэффективна для повышения скорости передачи данных, но может быть применена в целях экономии сетевого трафика.

Для установки режима автоматической проверки обновлений необходимо установить флаг «Автоматически проверять обновления» – в этом случае при каждом соединении с ФПСУ-IP (основным или дополнительным) ФПСУ-IP/Клиент будет запрашивать у него наличие новых версий программного обеспечения ФПСУ-IP/Клиента (раздел «Обновление ПО ФПСУ-IP/Клиента с ФПСУ-IP»).

Если установить флаг «Автосоединение при подключении устройства», то при запуске программного обеспечения ФПСУ-IP/Клиента с хотя бы одним установленным VPN-профилем, автоматически будет произведена попытка соединения с ФПСУ-IP.

Установленный флаг «Помнить введенный PIN-код пока устройство не отсоединено» указывает программе запомнить введенный один раз PIN код доступа к VPN-профилю, и при дальнейших попытках установления VPN-туннеля с ФПСУ-IP программа не будет требовать его повторного ввода. PIN код сохраняется и при перезагрузках. Запомненный PIN-код действует только для попыток установления соединения с ФПСУ-IP, и не будет подставляться при попытках пользователя изменить конфигурацию VPN-профиля.

Опция «Пауза между попытками соединения, сек» предназначена для задания временного интервала, с которым будут повторяться попытки соединения с ФПСУ-IP. Если опция не выставлена (окно пусто), при команде на установление соединения ФПСУ-IP/Клиент сделает 10 попыток соединения сначала с основным ФПСУ-IP, затем 10 попыток - с дополнительным. После чего, в случае неудачи, выдаст сообщение об отказе и прекратит попытки установления VPN-туннеля. Если в поле опции указано какое-то значение, после отказа в соединении от основного и дополнительного ФПСУ-IP, ФПСУ-IP/Клиент через указанное время вновь попытается установить связь. В этом случае ФПСУ-IP/Клиент будет пытаться установить VPN-туннель с ФПСУ до тех пор, пока не получит от ФПСУ-IP ответа.

Произведенные установки сохраняются при помощи кнопки «Сохранить». Для выхода из окна настройки без сохранения нужно воспользоваться кнопкой «Отмена».

6.3.6.2. Доступные через ФПСУ-IP рабочие станции

После установления соединения с ФПСУ-IP, АРМ Клиента может устанавливать сетевые соединения с рабочими станциями и серверами защищенной сети. Доступ к сетевым ресурсам настраивается и на ФПСУ-IP и в Клиенте. Настройки на ФПСУ-IP имеют приоритет и могут запрещать доступ к сетевым ресурсам, указанным в программном обеспечении Клиента.

Для отображения настроек работы АРМ Клиента с доступными через туннель с ФПСУ-IP сетевыми ресурсами, в левой части окна настроек необходимо выделить строку «Хосты».

Если VPN-профиль содержит IP-адреса рабочих станций, с которыми ФПСУ-IP/Клиент может работать через VPN-туннель, они будут отображаться в списке справа. Для разрешения взаимодействия клиента с новыми IP-адресами необходимо воспользоваться полем ввода над списком и кнопкой «Добавить».

Список IP-адресов может быть также получен от ФПСУ-IP, где он формируется администратором ФПСУ-IP. Для его просмотра после установки VPN-туннеля с ФПСУ-IP необходимо нажать кнопку «Список хостов, полученных от ФПСУ». Ранее добавленные в VPN-профиль адреса можно отредактировать или удалить из списка при помощи кнопок «Изменить» или «Удалить».

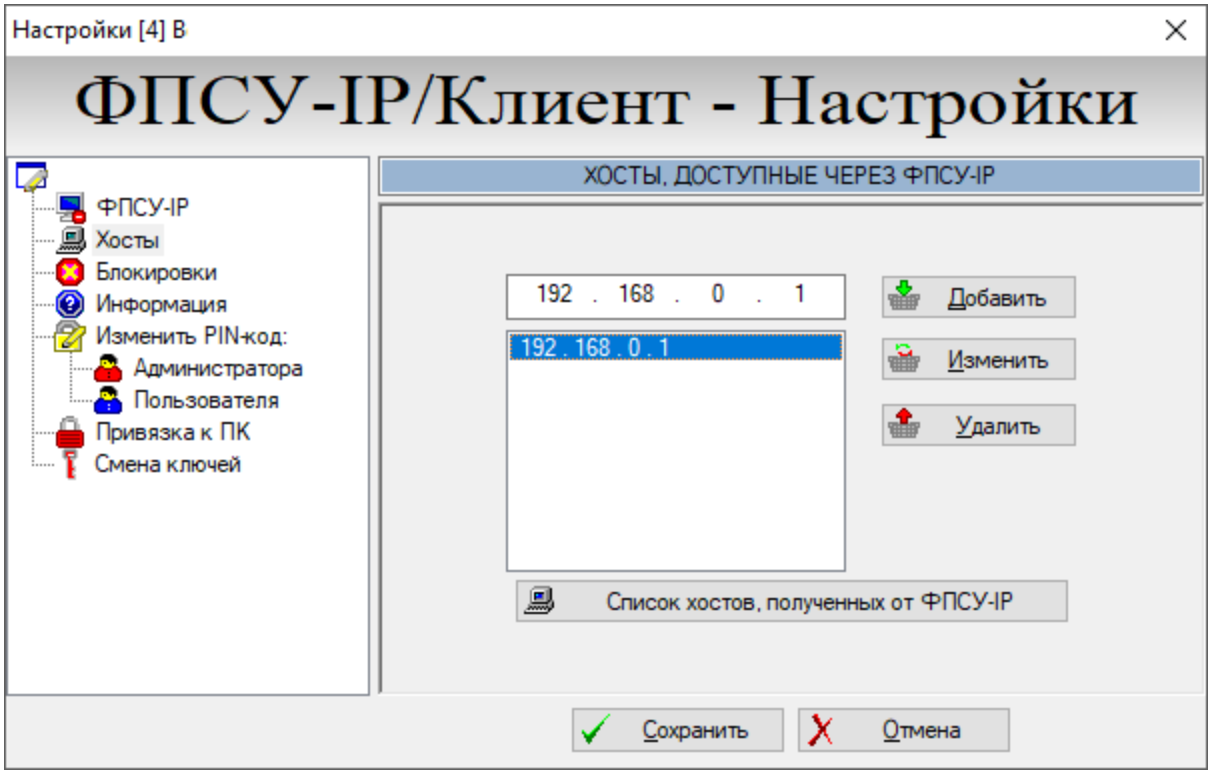


Рисунок 71- Настройка доступных ФПСУ-IP/Клиенту через VPN-туннель с ФПСУ-IP хостов

ФПСУ-IP/Клиент сможет работать через VPN-туннель с ФПСУ-IP только с теми рабочими станциями и серверами, чьи IP-адреса явно указаны либо в конфигурации VPN-профиля, либо в конфигурации данного пользователя Криптосети Клиентов в настройках ФПСУ-IP.

Произведенные настройки сохраняются при помощи соответствующей кнопки. Для выхода из окна настройки без сохранения можно воспользоваться кнопкой «Отмена».

6.3.6.3. Блокировка пакетов при установленном VPN-туннеле с ФПСУ-IP

Во время существования VPN-туннеля с ФПСУ-IP, ФПСУ-IP/Клиент может обмениваться данными с другими рабочими станциями сети в обычном открытом режиме. Администраторы ФПСУ-IP и ФПСУ-IP/Клиента могут ограничивать сетевое взаимодействие компьютера пользователя во время установленного соединения с ФПСУ-IP. В интерфейсе ФПСУ-IP/Клиента такие ограничения называются «блокировками» и доступны для изменения через меню настройки VPN-профиля.

В левой части окна необходимо выбрать строку «Блокировки», после чего справа появится список блокировок, позволяющий установить правила фильтрации входящих и исходящих пакетов данных на время существования VPN-туннелей с ФПСУ-IP.

В группе переключателей нужно отметить те соединения, которые будут запрещены во время сеансов с ФПСУ-IP. Ограничения на прием и передачу пакетов могут быть установлены как для сетевого адаптера, связанного с ФПСУ-IP, так и для других сетевых адаптеров ФПСУ-IP/Клиент.

Во время установки VPN-туннеля с ФПСУ-IP правила фильтрации, возможно, будут принудительно дополнены в соответствии с указаниями администратора ФПСУ-IP - в этом случае во время соединения около соответствующего поля будет отображаться знак запрета (знак «въезд запрещен»). Эти правила имеют более высокий приоритет, чем настройки VPN-профиля.

Кроме того, во время существования VPN-туннеля могут работать ограничения на прием и передачу пакетов, установленные пользователем (см. раздел «Сетевые настройки (SOCKS 5)»).

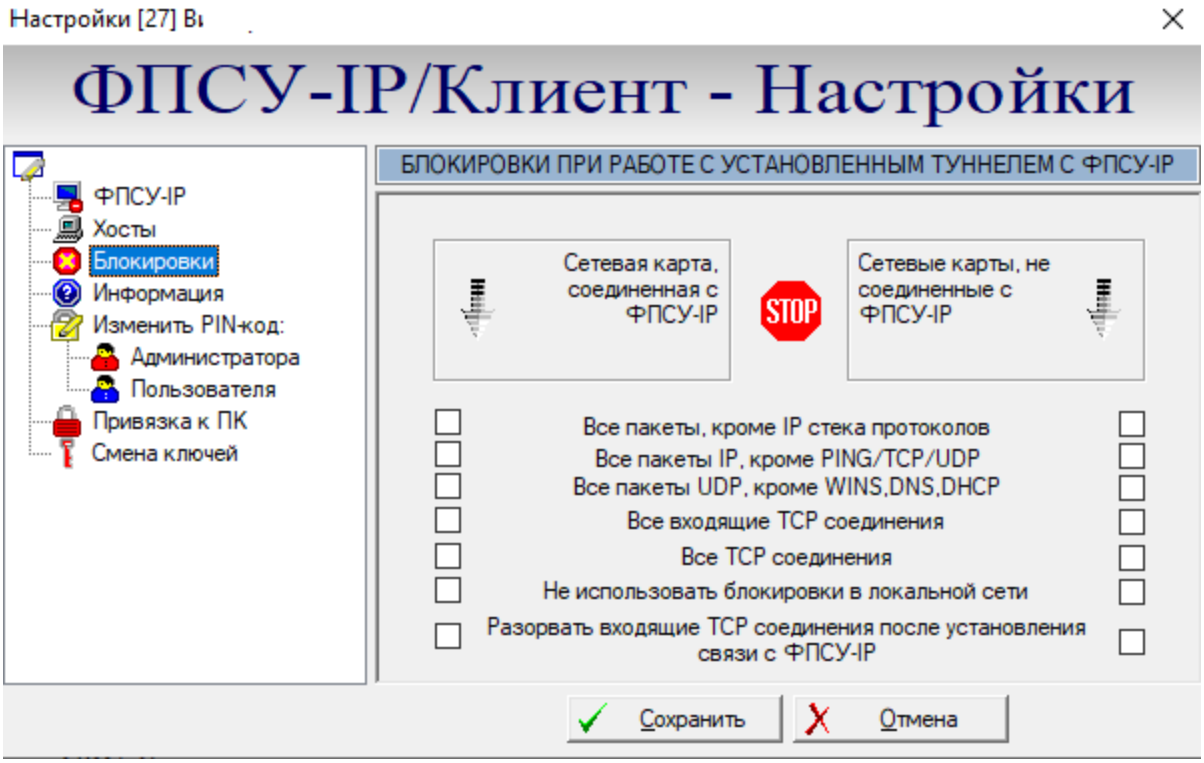


Рисунок 72 - Настройка блокировок сетевых пакетов

Правила блокировки межсетевого экрана состоят из следующих полей:

- Все пакеты кроме IP стека протоколов — блокируются пакеты, не принадлежащие к стеку протоколов TCP/IP (например, блокируются протоколы PPP и PPPoE);
- Все пакеты IP, кроме PING/TCP/UDP — блокируются все пакеты стека протоколов TCP/IP, кроме эхо-запросов (ping) и транспортных протоколов TCP и UDP;
- Все пакеты UDP, кроме WINS, DNS, DHCP — блокируются все UDP пакеты, кроме

WINS, DNS, DHCP;

- Все входящие TCP соединения — блокируются все IP пакеты с TCP трафиком, если инициатором соединения является другой хост;
- Все TCP соединения — блокируются все TCP соединения;
- Не использовать блокировки в локальной сети — не использовать все указанные выше блокировки, если рабочая станция Клиента взаимодействует с хостами своей собственной подсети;
- Разорвать входящие TCP соединения после установки связи с ФПСУ — после установления соединения с ФПСУ-IP принудительно завершить все TCP-соединения, инициатором которых является другой хост.

6.3.6.4. Получение сведений о VPN-профиле

Для ознакомления с параметрами VPN-профиля необходимо выбрать строку «Информация» окна настроек ФПСУ-IP/Клиента. При этом справа появится информационное окно, отображающее параметры ключевой системы, системные идентификаторы VPN-профиля (номер и имя Криптосети, номер Группы, номер и имя пользователя, серия ключевых данных пользователя), допустимое количество последовательных попыток ввода PIN-кода доступа к VPN-профилю.

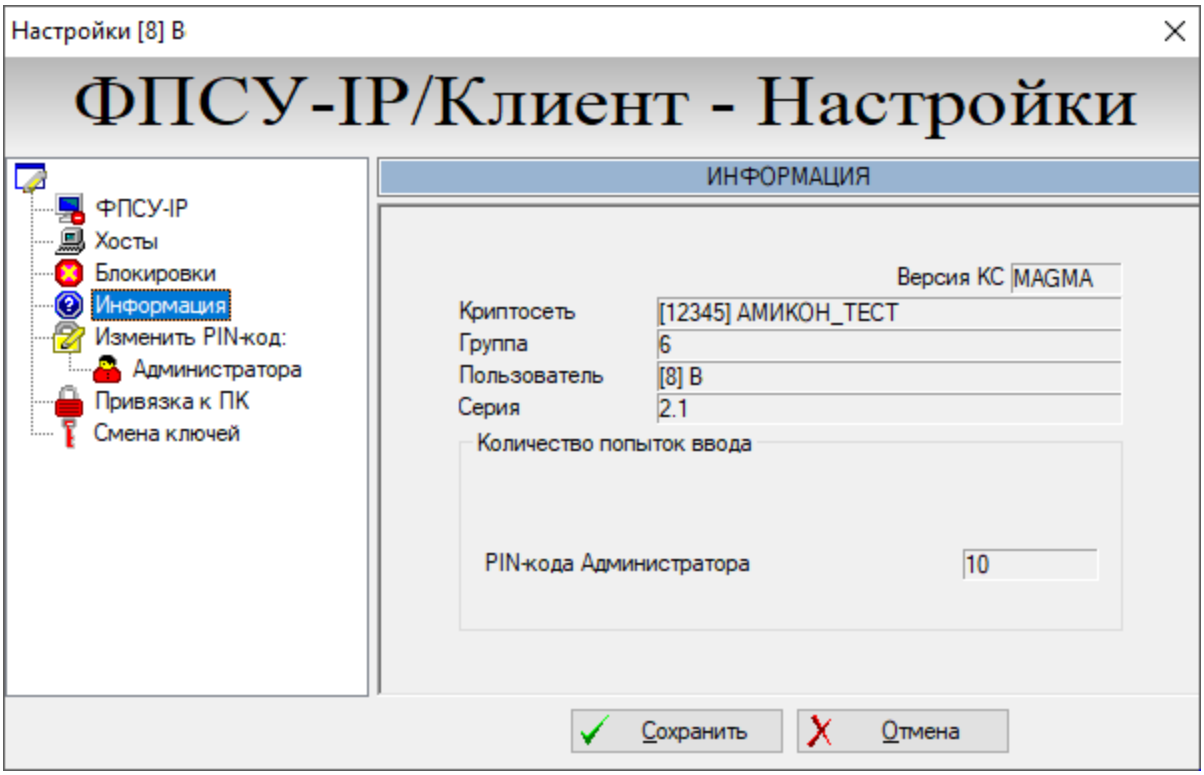


Рисунок 73 - Информация о VPN-профиле

Следует учитывать, что при работе с Программным Клиентом пользователь обладает

правами администратора, поэтому количество попыток ввода персонального идентификатора отображается только для PIN-кода Администратора.

6.3.6.5. Изменение PIN-кода доступа к VPN-профилю

Персональным идентификатором доступа к VPN-профилю является десятизначный PIN-код администратора.

Персональный идентификационный код VPN-профиля запрашивается программой при попытках соединения ФПСУ-IP/Клиент с ФПСУ-IP, и при попытках редактирования текущей конфигурации VPN-профиля.

Следует учитывать, что при работе с Программным Клиентом пользователь с PIN-кодом доступа к VPN-профилю обладает правами администратора по умолчанию, соответственно изменение персонального идентификатора предусмотрено только для PIN-кода Администратора.

Для того чтобы изменить PIN-код администратора, в левой части окна необходимо выбрать строку «Изменить PIN-код: Администратора». В поле появившегося окна следует ввести новый PIN-код и нажать кнопку «Изменить». PIN-код администратора будет заменен на введенный новый.

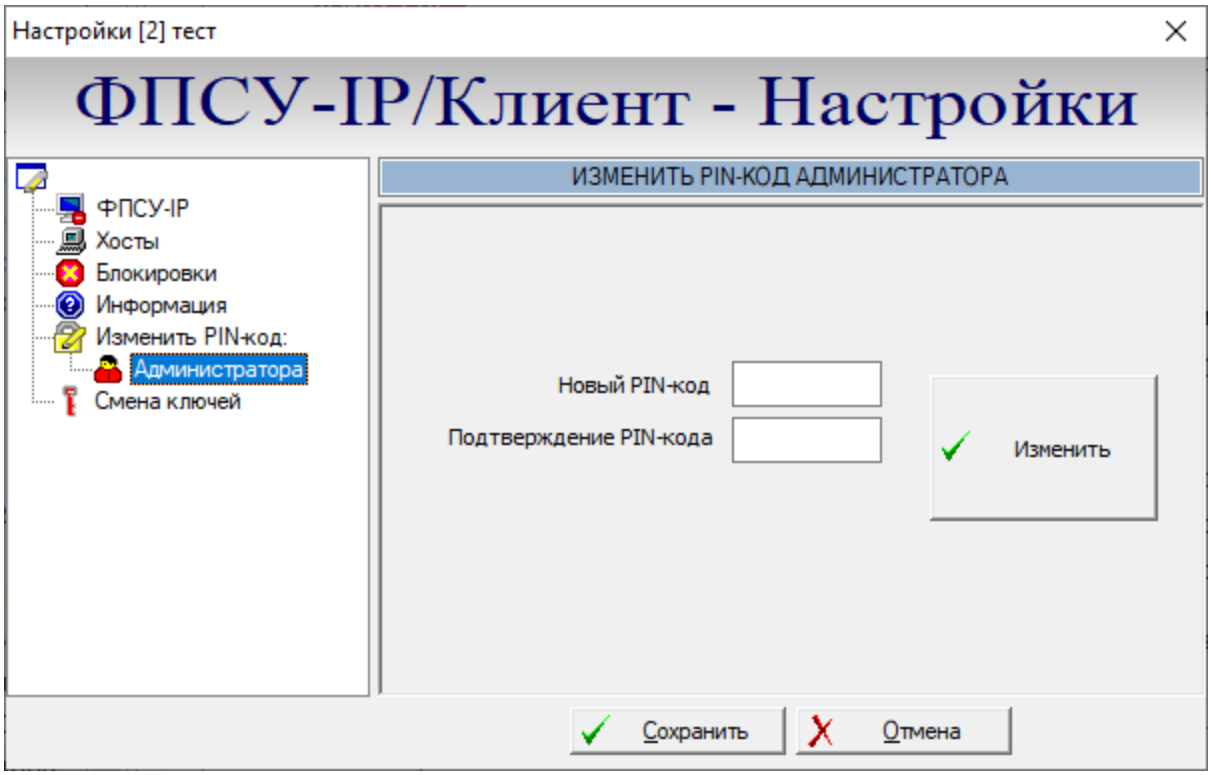


Рисунок 74 - Изменение PIN-кода доступа к VPN-профилю Программного Клиента

6.3.6.6. Привязка VPN-профиля к ПК

В качестве дополнительной меры защиты от копирования VPN-профиля, можно привязать находящийся на АРМ Клиента VPN-профиль к рабочему месту. Для этого в левой части окна настроек ФПСУ-IP/Клиента необходимо выбрать пункт «Привязка к ПК» (персональному компьютеру).

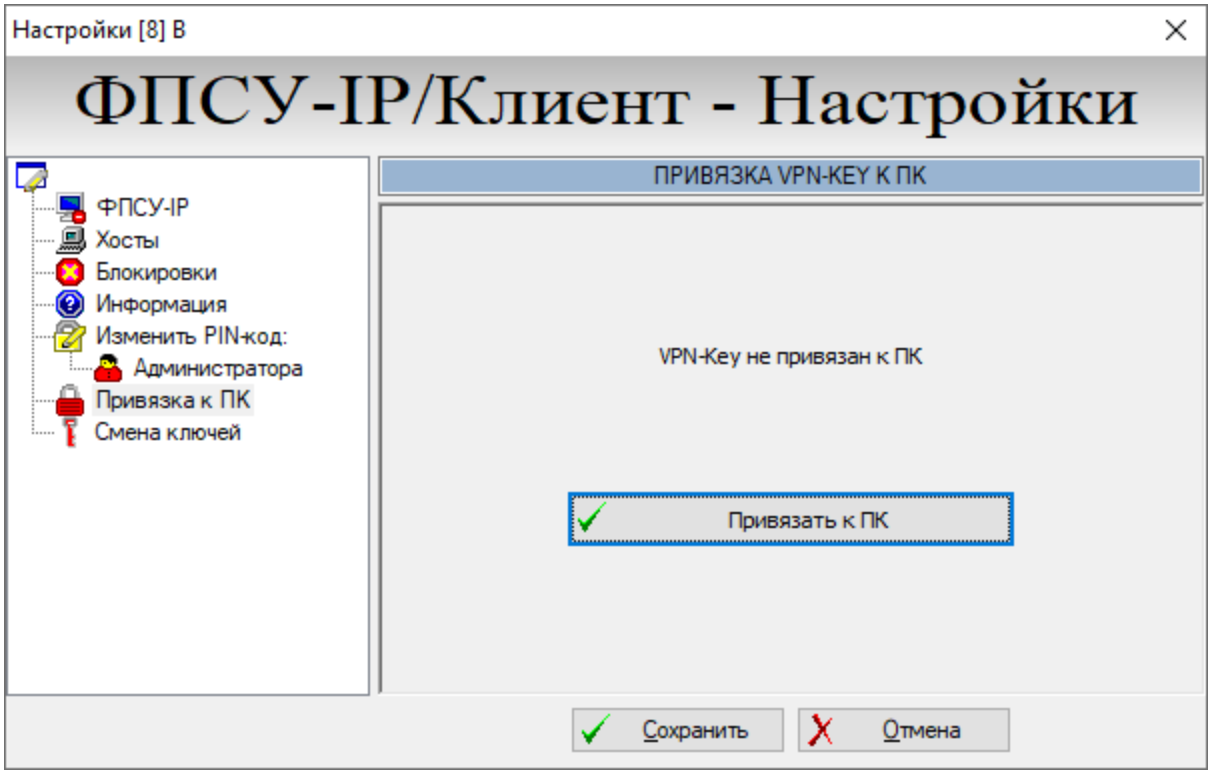


Рисунок 75 – Привязка VPN-профиля к ПК

Привязка к персональному компьютеру осуществляется по ряду параметров, в том числе учитывается:

- серийный номер ОС;
- серийный номер материнской платы;
- серийный номер системного диска.

Для того, чтобы привязать загруженный в АРМ Клиента VPN-профиль, нажмите кнопку «Привязать к ПК». Окно примет вид, представленный на рисунке ниже, статус привязки сменится на текст "VPN-Key привязан к этому ПК":

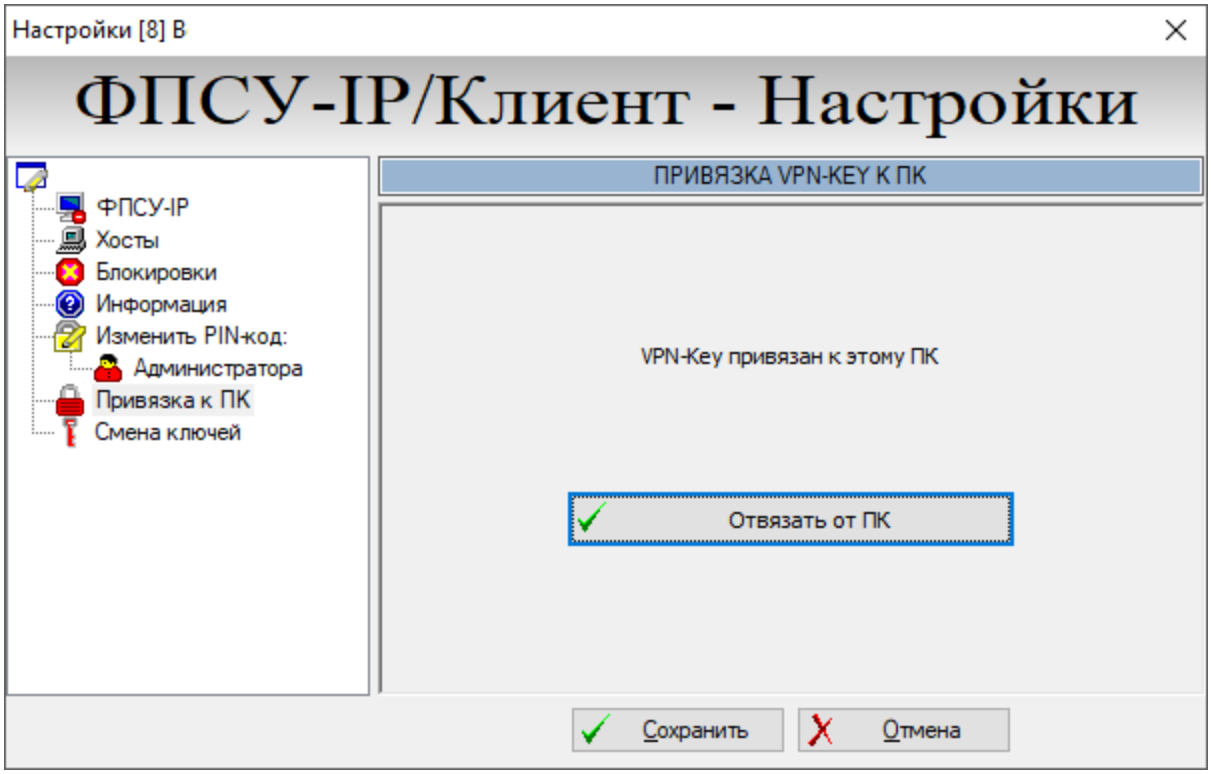


Рисунок 76 – VPN-профиль привязан к ПК

Для отмены привязки VPN-профиля в окне настроек ФПСУ-IP/Клиент необходимо нажать «Отвязать от ПК».

6.3.6.7. Смена серии ключей 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.

Ключи VPN-профиля пользователя могут быть обновлены администратором ЦГКК на АРМ ЦГКК, а могут быть доверенным образом в виде файла переданы на АРМ Клиента. Данные в файле находятся в зашифрованном на транспортном PIN-коде виде.

Для смены ключей в левой части окна необходимо выбрать пункт «Смена ключей». В правой части окна настроек появится интерфейс управления сменой ключевых данных.

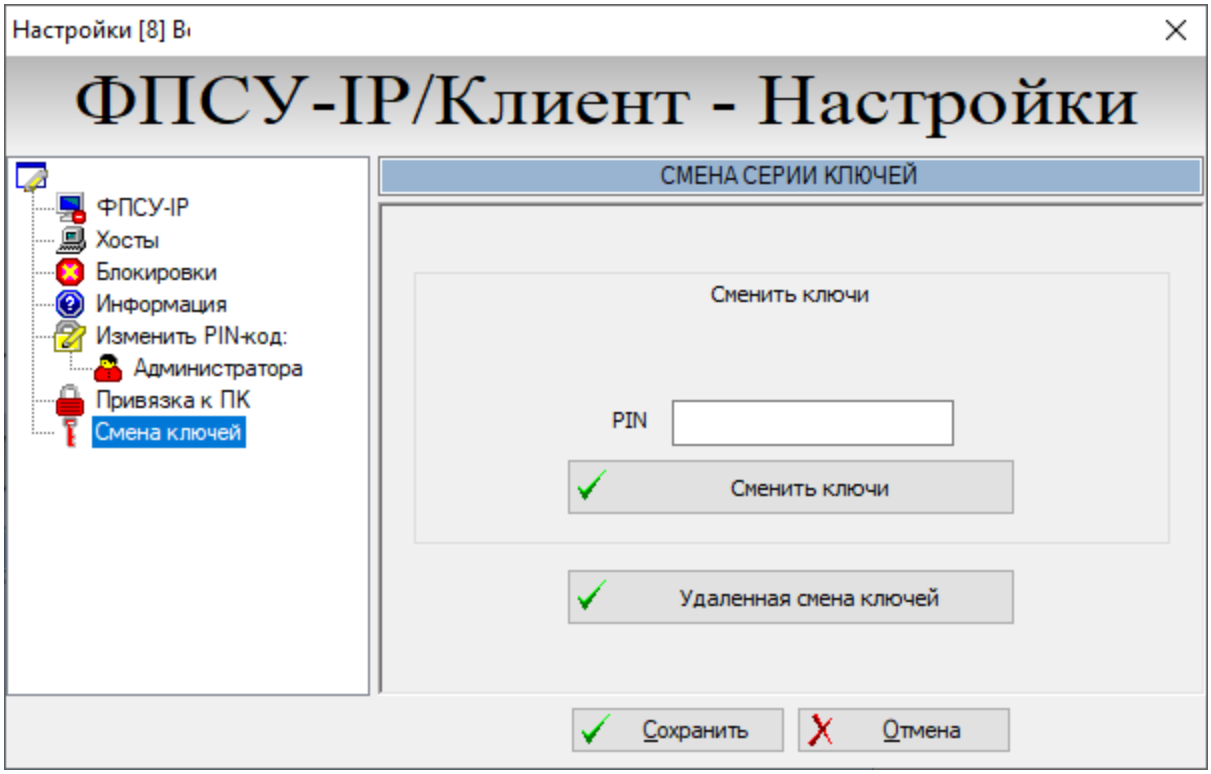


Рисунок 77 – Смена ключей

Для изменения ключевой информации VPN-профиля необходимо в поле «PIN» окна «Смена серии ключей» ввести полученный от администратора ЦГКК транспортный PIN-код и нажать кнопку «Сменить ключи».

В открывшемся стандартном окне операционной системы выбора файлов следует выбрать файл с расширением «.BIN», выданный ЦГКК для смены ключей и нажать кнопку «Открыть».

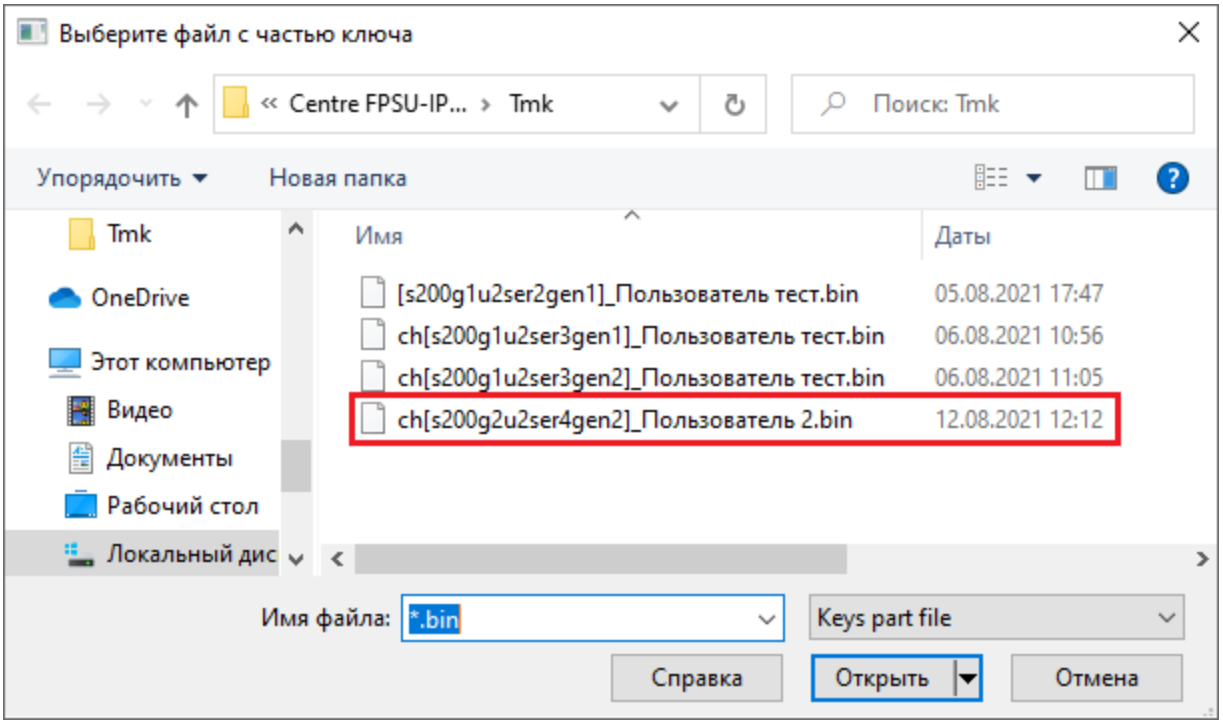


Рисунок 78 – Выбор файла для смены ключей

На экран будет выдано сообщение об успешной смене ключей:

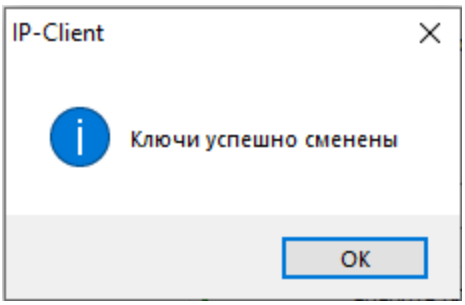


Рисунок 79 – Сообщение о смене ключей

В случае введения неверного PIN-кода, после попытки выбора ключевой информации система выдаст следующее сообщение:

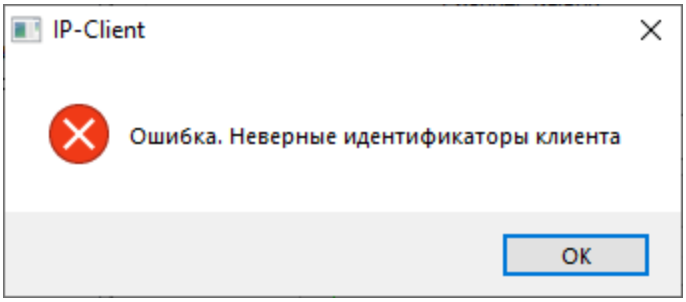


Рисунок 80 – Сообщение о неверном PIN-коде

6.3.6.8. Смена серии ключей через ФПСУ-RKL

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.

ФПСУ-RKL позволяет удобным и безопасным способом удаленно обновить ключевую информацию VPN-профиля на рабочих местах с установленным ФПСУ-IP/Клиентом.

Смена ключей возможна только в том случае, когда администратор ФПСУ-RKL разрешил данному пользователю сменить ключи удаленно через RKL.

Смена ключей через ФПСУ-RKL выполняется автоматически после установления соединения Клиента с ФПСУ-IP. Если администратор ФПСУ-IP установил новую серию ключей на ФПСУ-IP, на подключившемся клиенте прозрачно для пользователя Клиента будет выполнена процедура смены ключа. Тем не менее, пользователь Клиента может вручную запросить смену ключа через ФПСУ-RKL.

Для смены ключей с помощью ФПСУ-RKL в левой части окна настроек Клиента необходимо выбрать пункт «Смена ключей». В правой части окна настроек появится интерфейс управления сменой ключевых данных. Нажмите кнопку «Удаленная смена ключей» для перехода в окно создания запроса смены ключей к ФПСУ-RKL.

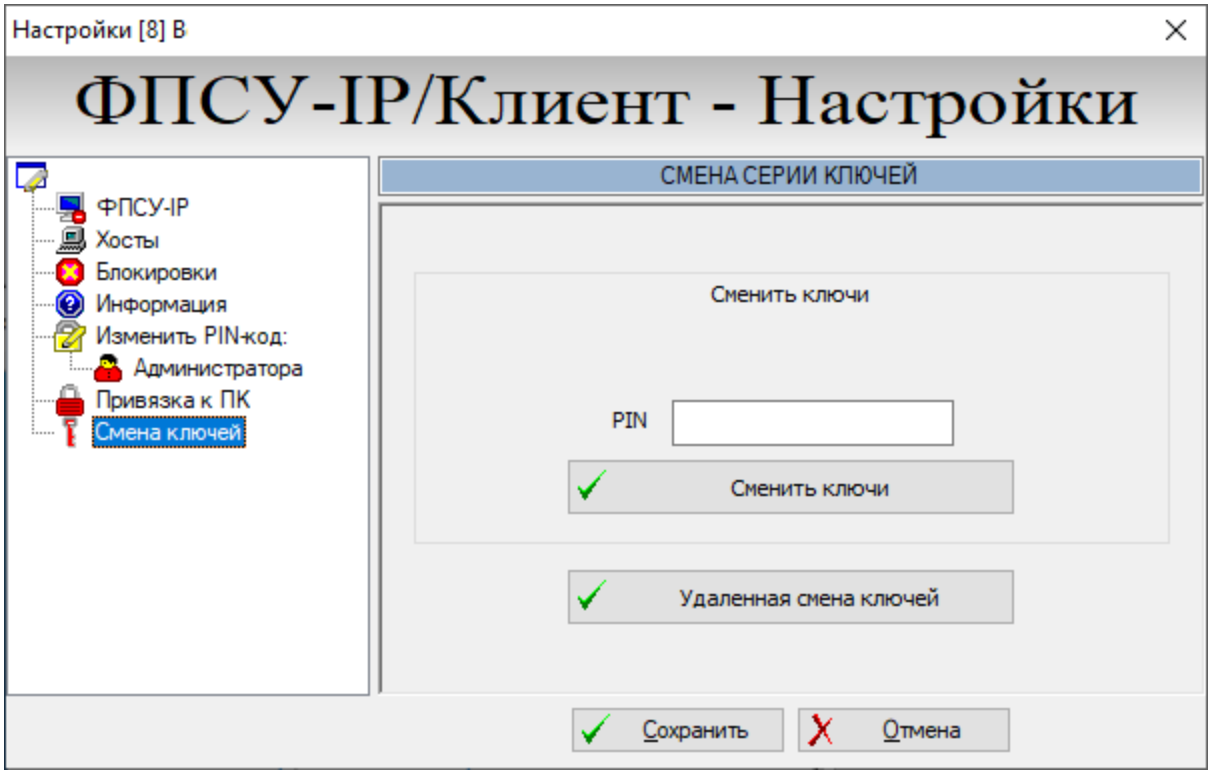


Рисунок 81 – Вкладка смены ключей

В открывшемся окне следует указать полученную от администратора безопасности информацию для запроса: IP-адрес ФПСУ-RKL, порт запроса. Из выпадающего поля выбора укажите сетевой адаптер, ведущий к указанному выше IP-адресу. Для отправления запроса нажмите клавишу «ОК»:

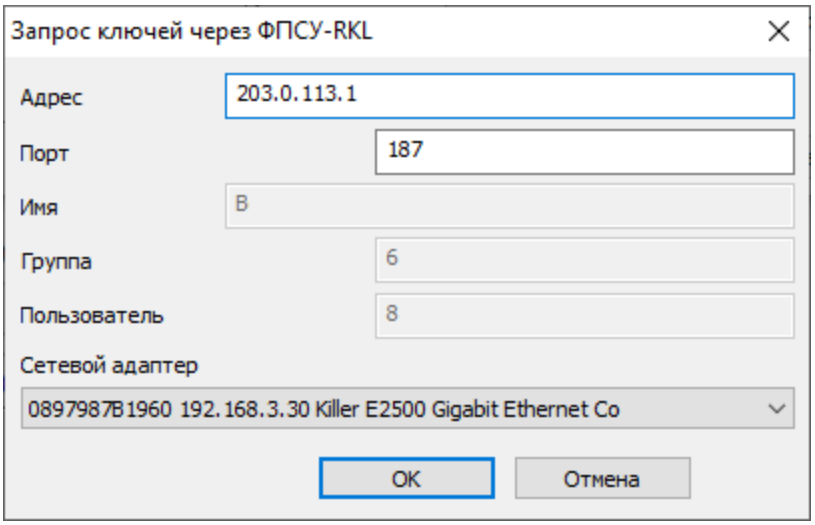


Рисунок 82 – Окно запроса к ФПСУ-RKL

В случае получения на ФПСУ-RKL и одобрения со стороны ФПСУ-RKL запроса, клиенту будут выданы новые ключи.

6.4. Дополнительная информация о VPN-профиле

При необходимости можно просмотреть справочную информацию о VPN-профиле. Сведения отображаются в дополнительном окне, открывающемся из окна установки соединения с ФПСУ-IP или окна входа в настройки VPN-профиля (разделы «Соединение Программного Клиента с ФПСУ-IP» и «Настройка параметров VPN-профиля».

Для получения дополнительной информации о VPN-профиле необходимо нажать кнопку «Подробнее». В открывшемся окне отобразится:

- лицензия, выданная программе (в поле «Серийный №»);
- номер текущей версий программного обеспечения ключевой системы;
- системные идентификаторы VPN-профиля (номера Криптосети, Группы и Пользователя, а так же серия ключевых данных);
- допустимое количество последовательных попыток ввода PIN-кода.

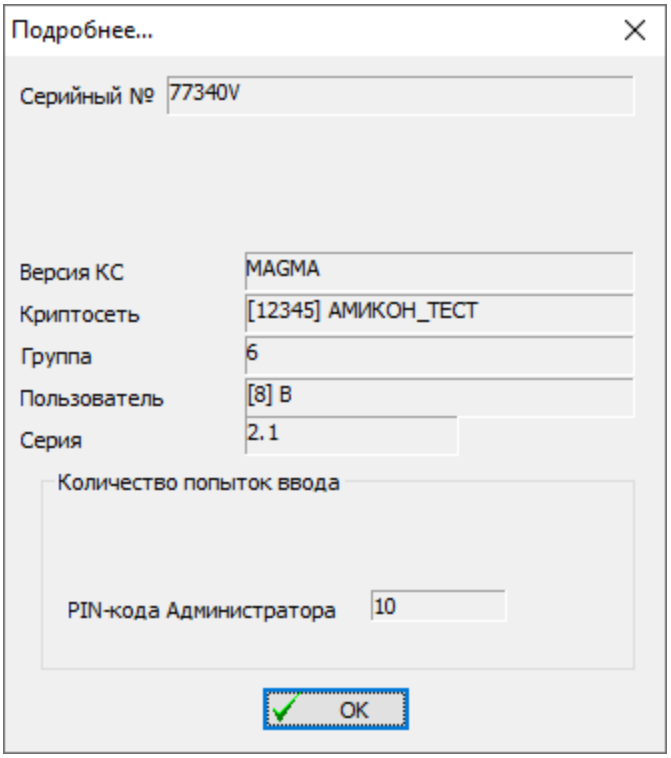


Рисунок 83 - Сведения о VPN-профиле

7. Дополнительные опциональные настройки ФПСУ-IP/Клиента

7.1. Настройка локального межсетевого экрана ФПСУ-IP/Клиента

Функционал локального межсетевого экран присутствует и в программном, и в программно-аппаратном варианте ФПСУ-IP/Клиента.

Локальный межсетевой экран ФПСУ-IP/Клиента анализирует поступающие на интерфейсы исходящие и входящие пакеты данных и проверяет их заголовки на соответствие правилам фильтрации. Пакеты, не прошедшие процедуру фильтрации, сбрасываются.

Правила фильтрации локального межсетевого экрана ФПСУ-IP/Клиент не применяются к пакетам, которые направлены в VPN-туннель к ФПСУ-IP.

Данные настройки не требуют регистрации пользователя и могут быть выполнены любым пользователем ОС. В качестве критериев фильтрации пользователь может задавать: IP-адреса взаимодействующих с ФПСУ-IP/Клиент рабочих станций, используемые IP-протоколы, разрешенное направление передачи данных.

Локальный межсетевой экран пользователя работает по принципу «все, что не разрешено - запрещено». Во время работы в межсетевых VPN-туннелях (в момент связи с ФПСУ-IP) локальный межсетевой экран по указанию пользователя может быть отключен.

Пользователь может установить пароль на работу с правилами фильтрации, который будет запрашиваться программой при попытке установки или редактирования существующих установок и правил фильтрации.

Для того чтобы просмотреть установленные правила фильтрации или настроить локальный межсетевой экран пользователя ФПСУ-IP/Клиент, необходимо открыть меню программы и выбрать строку «Локальные настройки».

На экран монитора будет выдано диалоговое окно настроек межсетевого экрана.

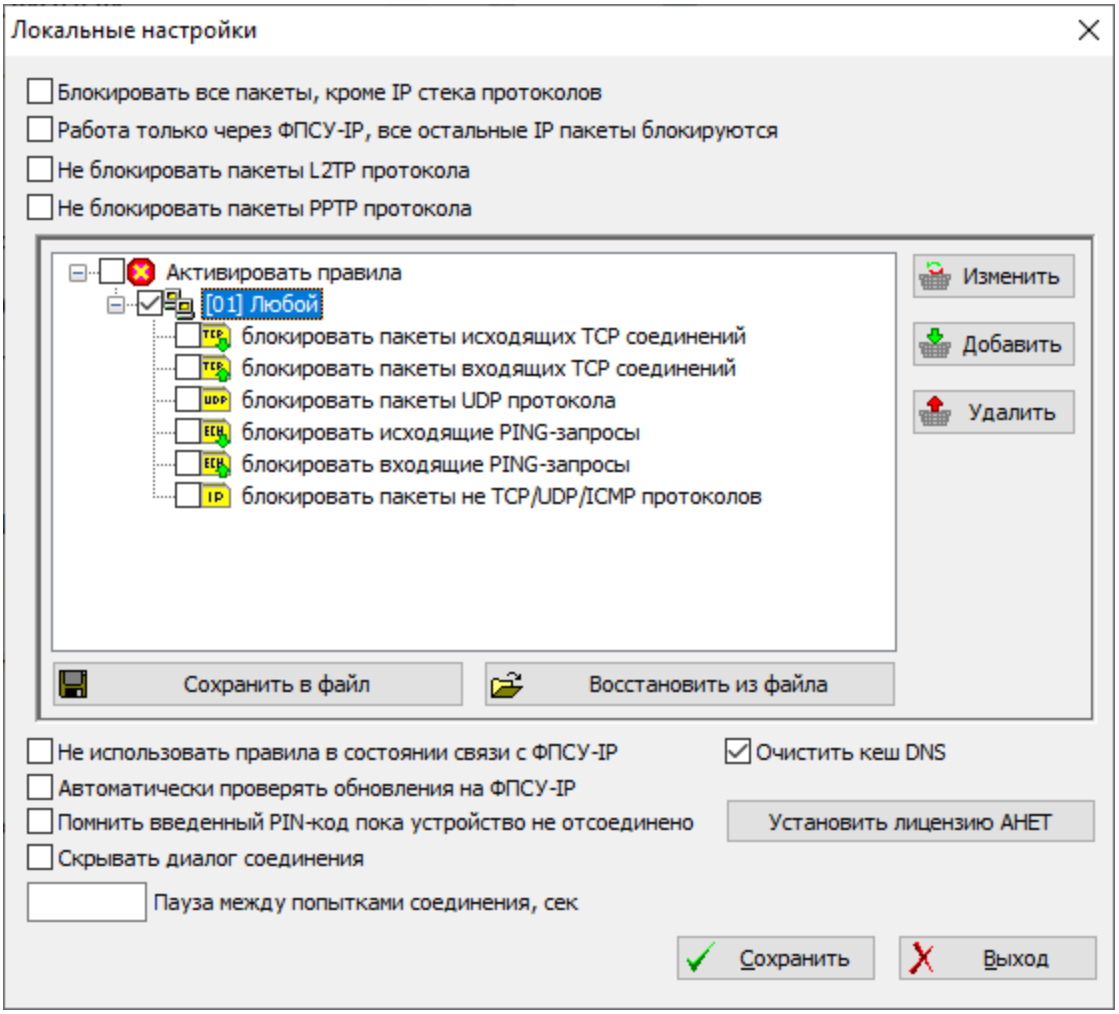


Рисунок 84 - Настройка локального межсетевого экрана ФПСУ-IP/Клиента

В верхней части окна отображаются переключатели общих настроек локального межсетевого экрана, а центральная часть окна содержит раскрывающийся список установленных правил фильтрации.

Максимальное количество записей в списке - 512.

Каждая строка правил описывает взаимодействие рабочей станции пользователя с каким-либо хостом или подсетью или любым неописанным ранее хостом и может содержать краткий комментарий - справочную информацию по текущему правилу. Каждое правило может быть активным (отмеченным флагом в начале строки) или неактивным (это означает, что правило описано, но не задействовано).

Если соединения с одним и тем же хостом (группой хостов) описываются несколькими правилами фильтрации, работать будет то правило, которое встречается в списке первым. При введении новых правил ФПСУ-IP/Клиент производит их автосортировку: записи для хостов помещаются в начало списка, затем идут записи для

подсетей с уменьшением маски, и в конце списка располагается запись типа «любой хост».

Правила локального межсетевого экрана могут быть сохранены в отдельный файл правил (кнопка «Сохранить») для последующего восстановления (кнопка «Загрузить») или переноса шаблонных правил на другие рабочие станции с установленным ПО ФПСУ-IP/Клиент.

7.1.1. Установка общих параметров межсетевого экрана

В окне локальных настроек межсетевого экрана ФПСУ-IP/Клиент присутствует ряд общих параметров его работы. Для установки общих параметров работы локального межсетевого экрана пользователя необходимо установить или снять следующие флаги рядом с названием параметра (см. рисунок в пункте «Настройка локального межсетевого экрана ФПСУ-IP/Клиента»):

- «Блокировать все пакеты, кроме IP-стека протоколов» – установленный флаг означает, что при приеме и передаче все пакеты, не соответствующие формату пакетов стека TCP/IP, будут сброшены.
- «Работа только через ФПСУ - IP, остальные IP-пакеты блокируются» – установленный флаг означает, что, при отсутствии соединения между ФПСУ-IP/Клиент и ФПСУ-IP, рабочая станция с установленным программным обеспечением ФПСУ-IP/Клиент будет блокировать передачу в сеть всех IP пакетов, кроме служебных в адрес ФПСУ-IP. После установления соединения между ФПСУ-IP/Клиент и ФПСУ-IP блокировка передачи пакетов в сеть с помощью этой опции не осуществляется.
- «Не блокировать пакеты L2TP протокола» – установленный флаг добавляет в межсетевом экране приоритетное разрешающее исключение для пакетов L2TP протокола, вне зависимости от всех других блокирующих опций.
- «Не блокировать пакеты PPTP протокола» – установленный флаг добавляет в межсетевом экране приоритетное разрешающее исключение для пакетов PPTP протокола, вне зависимости от всех других блокирующих опций.
- «Не использовать в состоянии связи с ФПСУ-IP» - флаг, позволяющий отменять работу локального межсетевого экрана (игнорировать установленные правила фильтрации) в состоянии связи с ФПСУ-IP.
- «Автоматически проверять обновления на ФПСУ-IP» - флаг проверки новых версий программного обеспечения ФПСУ-IP/Клиент (подробнее см. раздел «Обновление ПО ФПСУ-IP/Клиента с ФПСУ-IP»).
- «Помнить введенный PIN-код, пока устройство не отсоединено» - установленный флаг позволяет запомнить введенный один раз PIN код, и при дальнейших

попытках установления VPN-туннеля с ФПСУ-IP не будет требовать его повторного ввода. PIN код сохраняется и при перезагрузках. Запомненный PIN-код действует только для попыток установления соединения с ФПСУ-IP, и не будет подставляться при попытках пользователя изменить конфигурацию VPN-профиля.

- «Скрывать диалог соединения» - скрывать всплывающее окно, отображающее ход и ошибки подключения ФПСУ-IP/Клиента к принимающему ФПСУ-IP. Рекомендуется устанавливать на локальных станциях, дисплей которых может быть доступен для обзора посторонним людям (например, в банкоматах).
- «Пауза между попытками соединения, сек» - дублирование аналогичной опции в «Программный клиент», предназначена для задания временного интервала, с которым будут повторяться попытки соединения с ФПСУ-IP (подробнее см. раздел «Настройка подключения к ФПСУ-IP».
- «Очистить кэш DNS» - установленный флаг позволяет очистить локальный кэш DNS рабочей станции. Опцию можно пробовать включать при проблемах установления соединений с защищенными ФПСУ-IP серверами, доступ к которым организован через систему имен а не напрямую через IP-адресацию.

7.1.2. Настройка правил фильтрации

Командные кнопки «Изменить», «Добавить», «Удалить» используются для создания и управления набором правил фильтрации.

Для создания нового правила фильтрации необходимо нажать на кнопку «Добавить». На экран будет выведено диалоговое окно редактирования.

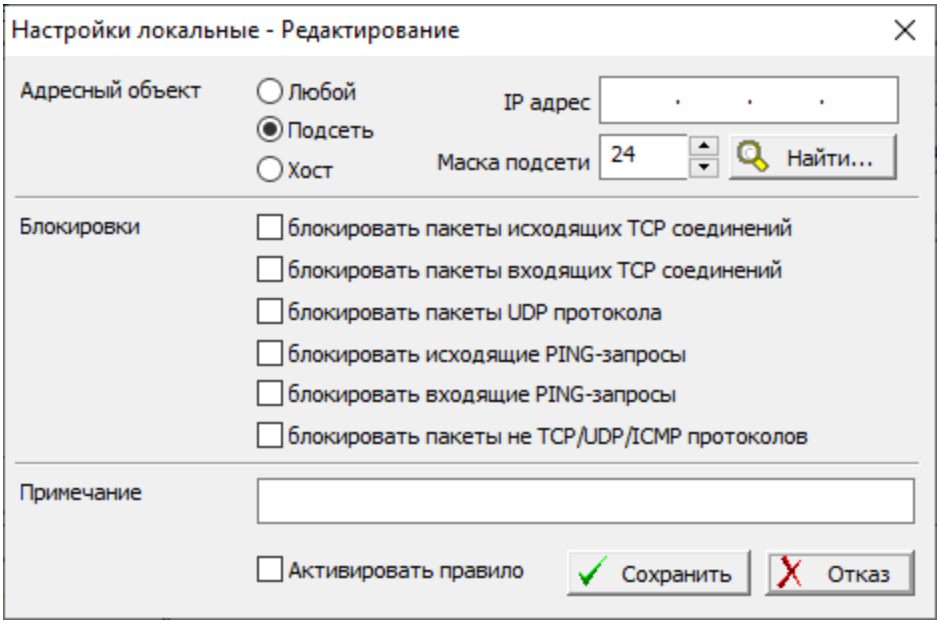


Рисунок 85 - Создание правила фильтрации

Переключатель в поле «Адресный объект» необходимо установить в нужное положение для выбора типа адреса, взаимодействие с которым описывается. Для хоста нужно указать его IP-адрес, для подсети - IP-адрес и маску (число значащих разрядов).

Если сетевым службам компьютера доступны какие-либо средства разрешения Интернет-имен, по нажатию кнопки «Найти» можно запросить IP-адрес рабочей станции с известным именем у соответствующего сервера.

Запись типа «Любой» создается для регламентации взаимодействия ФПСУ-IP/Клиент с явно не описанными хостами.

В группе флагов «Блокировки» нужно указать типы соединений с описываемым адресом, которые будут запрещены при сетевом взаимодействии.

В поле «Примечание» можно ввести, если это необходимо, справочную информацию по текущему правилу – она будет отображаться вместе с правилом в окне локальных настроек.

Для включения правила необходимо установить флаг «Активировать правило». Если правило необходимо временно отключить - флаг необходимо снять.

После нажатия кнопки «Сохранить» установленное правило будет отображаться в списке окна локальных настроек.

Чтобы отредактировать какое-либо правило фильтрации, также необходимо нажать командную кнопку «Разрешить редактирование» в нижнем левом углу окна «Локальные настройки» (если пароль на редактирование устанавливался, нужно ввести его по запросу

программы).

Для изменения какой-либо записи нужно выбрать ее в списке и открыть окно редактирования двойным нажатием левой клавиши мыши (или нажатием кнопки «Изменить»). После внесения всех необходимых изменений необходимо нажать кнопку «Сохранить» в правой нижней части окна.

Чтобы удалить какое-либо существующее правило фильтрации, нужно выбрать его в списке и нажать кнопку «Удалить» в правой нижней части окна локальных настроек.

7.2. Настройка КС3

При работе с ФПСУ-IP/Клиентом предоставляется возможность включения и отключения защиты класса КС3 (в том случае, если при установке эта опция была включена соответственно описанию в разделе «Процедура инсталляции». Если при инсталляции опция не была выбрана, для использования КС3 требуется переинсталлировать ФПСУ-IP/Клиента с включенным флагом КС3 на экране выбора опций инсталляции). Для настроек работы с КС3 необходимо выбрать подпункт «Настройки КС3» подпункта «Настройки безопасности» пункта основного меню «Локальные настройки».

В качестве первого шага необходимо установить пароль на создание и изменение создания межсетевого экрана с использованием средств криптографической защиты класса КС3. Для этого после выбора подпункта «Настройки КС3» будет выдано окно ввода пароля.

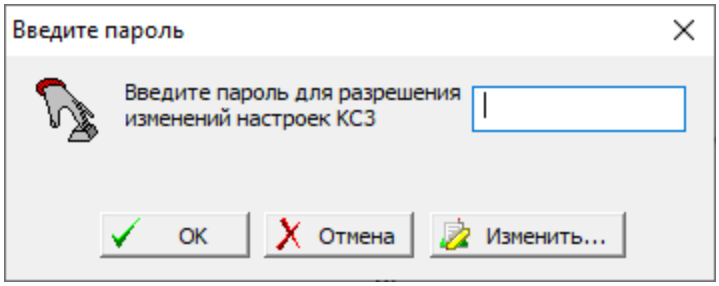


Рисунок 86 - Ввод пароля для настройки межсетевого экрана

Если пароль устанавливается впервые или уже был установлен, необходимо ввести его и нажать «OK».

Чтобы изменить пароль на редактирование настроек КС3 необходимо установить действующий пароль и нажать кнопку «Изменить». На экране появится диалоговое окно ввода, в котором следует ввести новый пароль и его подтверждение. Для сохранения изменений следует нажать «OK».

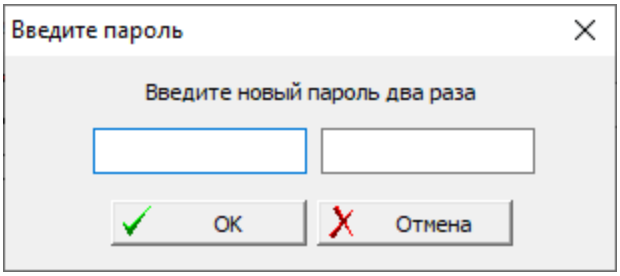


Рисунок 87 - Установка (изменение) пароля для настройки КСЗ

После ввода (или изменения) пароля откроется окно «Настройки КСЗ (замкнутая среда)».

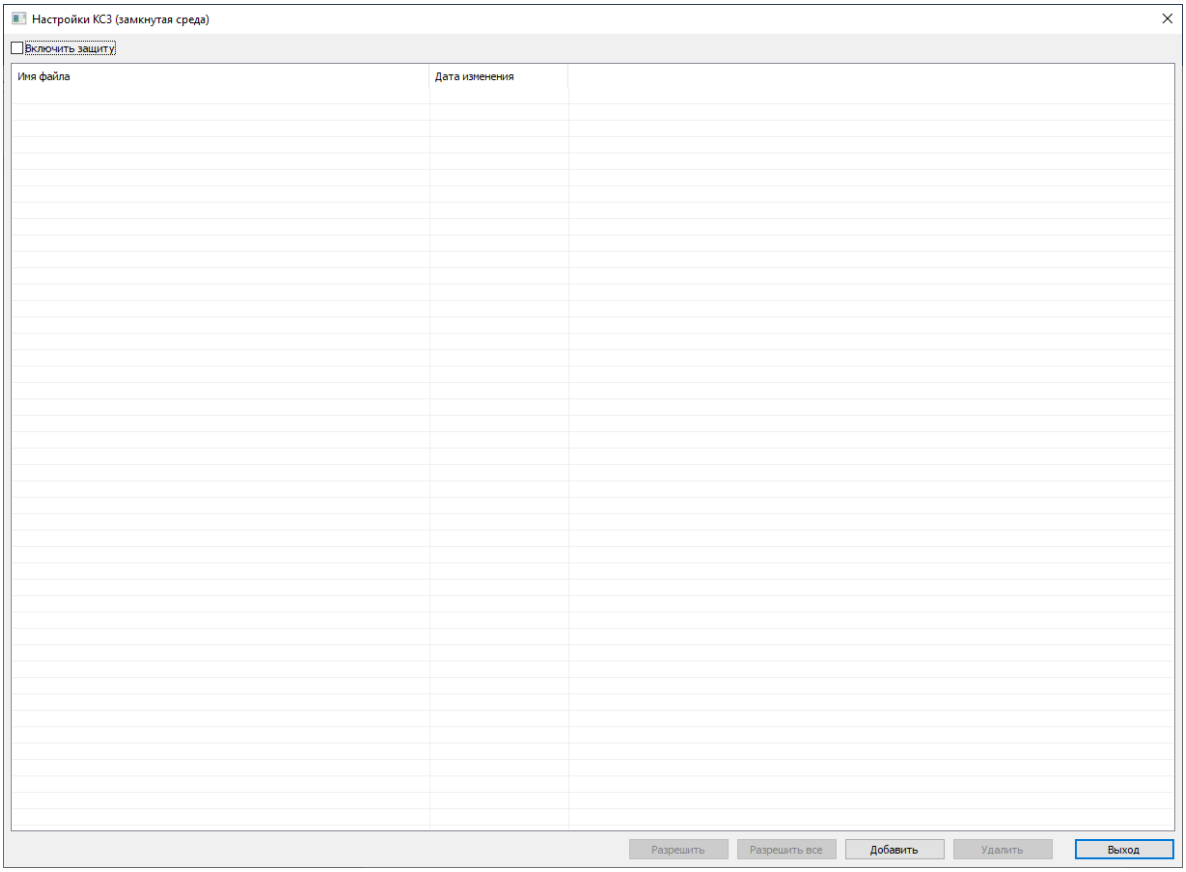


Рисунок 88 - Окно установки настроек КСЗ

В окне настроек КСЗ предоставляется возможность создать список запрещенных к исполнению файлов.

Для добавления файла в список необходимо нажать кнопку добавить и в открывшемся окне выбрать файл, исполнение которого будет запрещено. Файл появится в списке в окне настроек КСЗ.

В дальнейшем список можно редактировать несколькими способами:

- путем разрешения определенных файлов из него, для чего следует выбрать нужные файлы (если необходимо разрешить исполнение нескольких файлов из списка, следует выбирать их нажатием левой клавиши мыши с одновременным удержанием клавиши «Ctrl»);
- разрешения к исполнению всех файлов (по нажатию кнопки «Разрешить все»);
- путем удаления выбранных файлов с жесткого диска компьютера. В последнем случае система выдаст запрос на подтверждение действия.

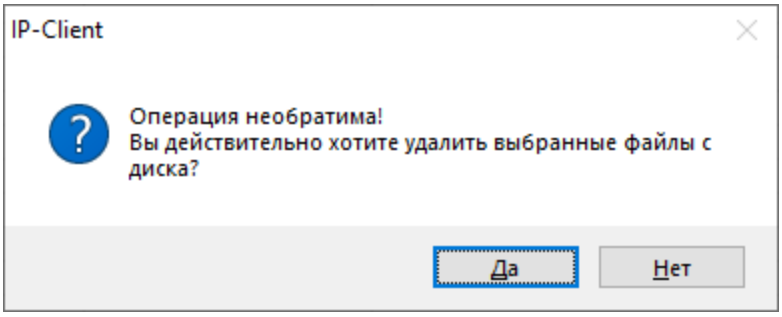


Рисунок 89 - Предупреждение о необратимости операции удаления

Следует учитывать, что файлы из списка будут исполняться вплоть до непосредственного включения защиты класса КС3.

Для включения защиты класса КС3 необходимо установить в верхней части окна флаг «Включить защиту». Система выдаст предупреждение о запрете исполнения файлов после включения защиты:

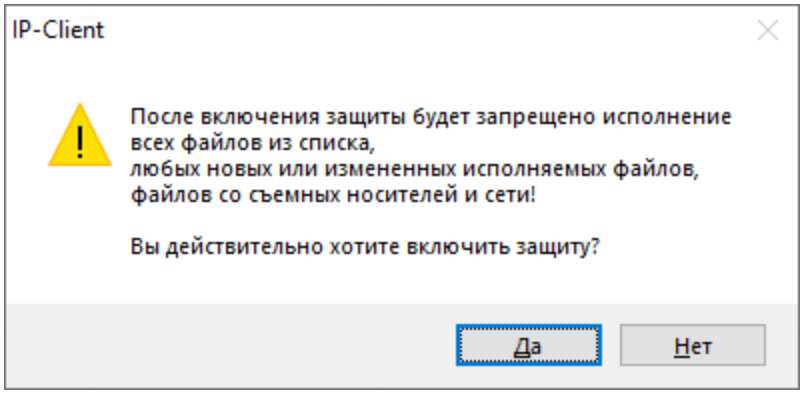


Рисунок 90 - Запрос необходимости включения защиты КС3

После нажатия на кнопку «Да» будет запрещен запуск всех исполняемых файлов из списка, любых новых или измененных исполняемых файлов, файлов со съемных носителей и из сети. Все файлы, которые будут запрещены к исполнению в процессе работы ФПСУ-IP/Клиента, будут отображаться в этом списке. Редактирование списка также доступно при включенной защите класса КС3.

Для отключения защиты необходимо снять флаг «Включить защиту», после чего

файлы из списка, новые или измененные исполняемые файлы, файлы со съемных носителей и из сети будут вновь разрешены к исполнению.

7.3. Сетевые настройки (SOCKS 5)

ФПСУ-IP/Клиент может устанавливать соединения с ФПСУ-IP через прокси-сервер (proxy), использующий протокол SOCKS 5. Общая схема взаимодействия ФПСУ-IP/Клиента, прокси-сервера и ФПСУ-IP изображена на рисунке ниже.

Рисунок 91 - Схема работы ФПСУ-IP/Клиента через Proxy-сервер SOCKS 5

Для соединения с ФПСУ-IP через прокси-сервер используется команда «Сетевые настройки» основного меню.

При включении опции «Использовать SOCKS 5», ФПСУ-IP/Клиент получает возможность работать с указанным по IP-адресу прокси-сервером на выбранном порту. Соединение использует UDP протокол для связи с прокси-сервером и внешним ФПСУ-IP. Каждое SOCKS-соединение проходит стадию аутентификации, если она требуется. ФПСУ-IP/Клиент поддерживает метод аутентификации на прокси-сервере с использованием имени пользователя (логина) и пароля по спецификации протокола SOCKS 5.

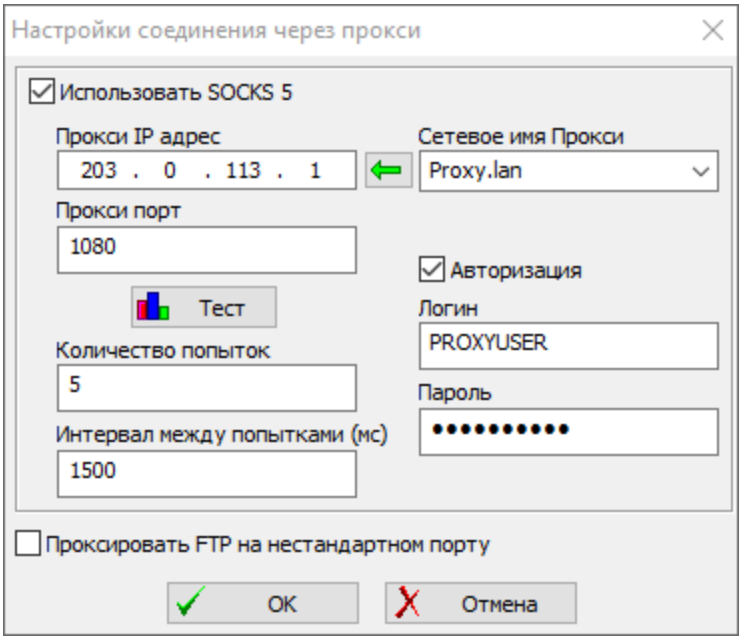


Рисунок 92 - Настройка работы через прокси сервер SOCKS 5

Для работы через прокси-сервер нужно указать:

- IP-адрес прокси-сервера SOCKS 5 (возможно заполнение данного поля по известному DNS-имени прокси-сервера);
- порт прокси-сервера, принимающий входящие соединения;
- имя пользователя и пароль, если на сервере требуется авторизация;
- количество попыток соединения с прокси-сервером и интервал между попытками.

Для проверки работоспособности текущих настроек необходимо нажать кнопку «Тест».

В этом же окне можно установить настройку для безопасности соединения по FTP - протоколу прикладного уровня для обмена файлами по транспортному протоколу TCP/IP. При установленном флаге «Проксировать FTP на нестандартном порту» (обязательным условием также является установка в настройках ФПСУ-IP возможности выдачи NAT адреса ФПСУ-IP/Клиенту) обмен данными по FTP будет происходить не только по стандартному порту (порт 21), но и по любому другому. В том случае, если NAT адрес ФПСУ-IP Клиенту не выдается, проксирование FTP производиться не будет.

7.4. Обновление ПО ФПСУ-IP/Клиента с ФПСУ-IP

Во время сеансов сетевого соединения с ФПСУ-IP, пользователь может получать от него и устанавливать на компьютер новые версии программного обеспечения ФПСУ-IP/Клиента.

Подсистема обновления программного обеспечения функционирует следующим образом:

1. На ФПСУ-IP устанавливаются обновления программного обеспечения для ФПСУ-IP/Клиента.
2. ФПСУ-IP/Клиент посылает ФПСУ-IP, с которым установлена связь, запрос обновления ПО (по запросу пользователя или автоматически). Если администратор ФПСУ-IP разрешил данному ФПСУ-IP/Клиенту скачивать новую версию, соответствующие программные файлы поступают на АРМ ФПСУ-IP/Клиента по межсетевому VPN-туннелю и записываются на внутренний носитель данных.
3. Пользователь устанавливает полученное от ФПСУ-IP обновление ПО (он должен принадлежать к группе администраторов операционной системы, имеющих права на установку программного обеспечения).

7.4.1. Обновление ПО по запросу пользователя

Для обновления ПО по запросу пользователя необходимо:

1. Установить межсетевой VPN-туннель с ФПСУ-IP («Соединение Программного Клиента с ФПСУ-IP»).
2. Войти в меню ПО и выбрать команду «Обновление ПО > Скачать обновление». ФПСУ-IP/Клиент проверит наличие обновлений, и в случае их обнаружения загрузит на АРМ, о чем будет выдано соответствующее сообщение.
3. Когда файл с обновлением ПО будет загружен, выполнить команду «Обновление ПО > Установить обновление». Откроется окно менеджера загруженных обновлений, которое будет пустым, если обновлений не было найдено или они еще не загружены.
4. Выбрав требуемое обновление, нажатием кнопки «Установить» обновить ПО ФПСУ-IP/Клиента.

Процесс установки обновлений производится аналогично установке ПО, описанной в разделе «Установка программного обеспечения».

7.4.2. Автоматический запрос обновлений

Для установки режима автоматического запроса обновлений ПО необходимо войти в меню ФПСУ-IP/Клиента и выбрать команду «Программный клиент». После регистрации с правами администратора (см. раздел «Регистрация администратора в программно-

аппаратном Клиенте») нужно выбрать в списке настроек строку «ФПСУ-IP».

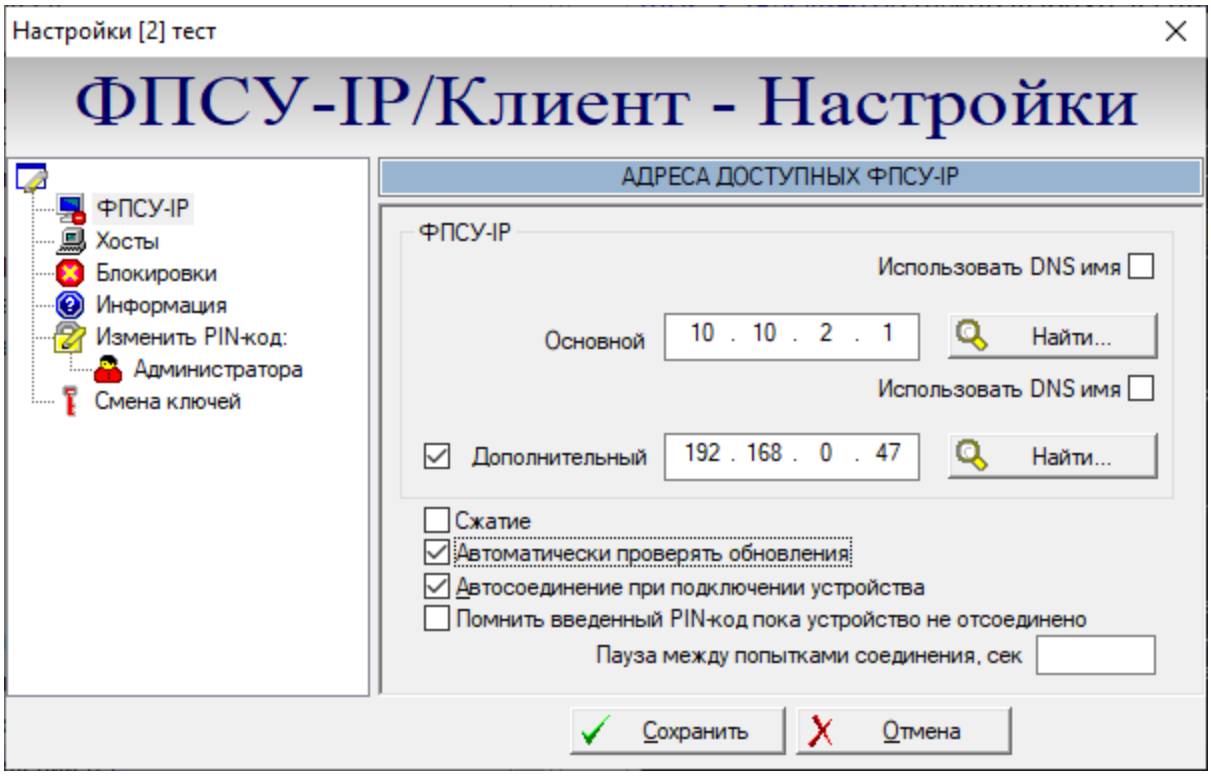


Рисунок 93 - Включение автоматического обновления

Для автоматизации запросов обновлений необходимо установить флаг «Автоматически проверять обновления» и нажать кнопку «Сохранить».

После того, как автоматический режим проверки обновлений ПО будет установлен, «ФПСУ-IP/Клиент» каждый раз после установки VPN-туннеля с основным или дополнительным ФПСУ-IP будет запрашивать соответствующие файлы.

8. Контроль целостности программного обеспечения

Во время эксплуатации контроль целостности установленного и используемого программного обеспечения ФПСУ-IP/Клиента производится вычислением поставляемой вместе с ФПСУ-IP/Клиент программой контроля целостности файлов WinFPSUHash.exe версии 2.0 (название приведено для дистрибутивов ОС семейства Windows) хэш-функции от установленных файлов и сравнением полученных данных с эталонными контрольными суммами.

Исполняемый файл программы «WinFPSUHash.exe» и контрольные суммы (они находятся в файлах AmiFlt.hsh, FPSUHash.hsh, IPClnt.hsh) хранятся в подкаталоге \Filehash каталога, куда было установлено программное обеспечение «ФПСУ-IP/Клиента» (по умолчанию это каталог C:\Program Files\Amicon\Client FPSU-IP) — в дальнейшем подкаталог проверки.

Контролю целостности подлежат следующие файлы из состава «ФПСУ-IP/Клиента»:

- сама утилита WinFPSUHash.exe;
- главное приложение, ip-client.exe, после установки по умолчанию находящееся в каталоге %ProgramFiles%\AMICON\Client FPSU-IP\;
- драйвер сетевого уровня, AmiIMFlt.sys, AmiNdisFlt.sys (в зависимости от ОС), находящийся в каталоге %SystemRoot%\SYSTEM32\DRIVERS\.

Для выполнения автоматизированной проверки перечисленных файлов с помощью утилиты WinFPSUHash.exe необходимо запустить на исполнение пакетный файл CheckHashes.cmd, хранящийся в подкаталоге проверки.

При совпадении полученных данных с эталоном будет выведено сообщение «Хеш верен». Результат выполнения проверки по каждому файлу будет выведен на экран, а также сохранен в подкаталог проверки в файлы листинга AmiFlt.lst, FPSUHash.lst, IPClnt.lst. Файлы листинга содержат текст в кириллической кодировке и могут быть открыты любым текстовым редактором.

В случае возникновения ошибки в процессе контроля целостности программного обеспечения следует прекратить дальнейшую работу с «ФПСУ-IP/Клиентом». Рекомендуется выполнить повторную инсталляцию ПО «ФПСУ-IP/Клиента» и обратиться к администратору.

9. Получение справочной информации

9.1. Информация о программе

Для получения справочной информации о функционирующем ФПСУ-IP/Клиент необходимо вызвать контекстное меню и выбрать команду «О программе». На экран будет выдано информационное окно, отображающее:

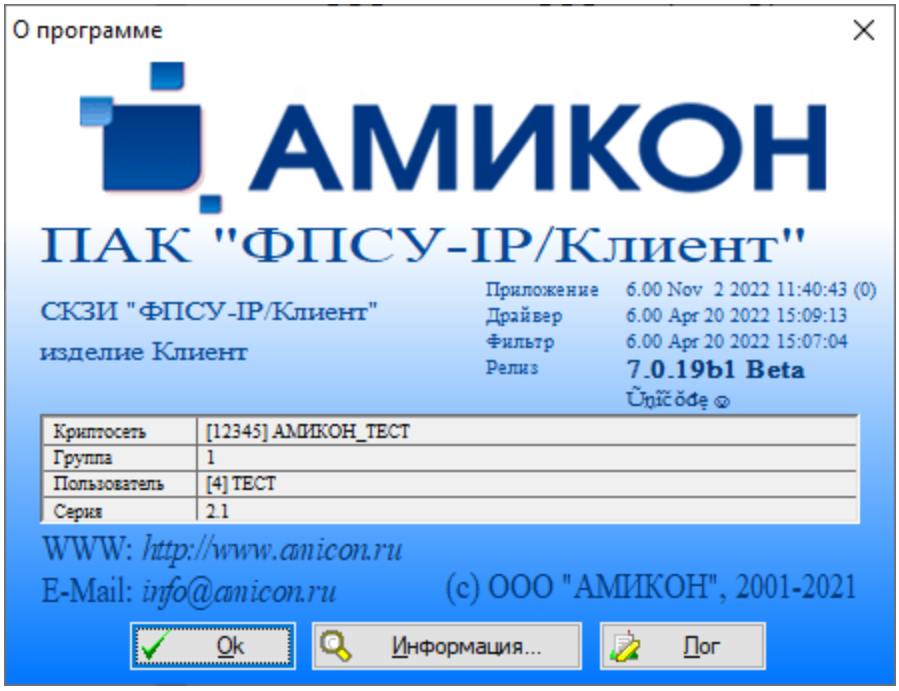


Рисунок 94 - Справочная информация о программе

- имя Разработчика ПО («АМИКОН») и контактные данные в Интернет;
- название программы (ФПСУ-IP/Клиент) и номер текущей версии (в приведенном на рисунке примере «Релиз – 7.019b»), а также номера версий и даты компиляций отдельных компонентов ПО («Приложение», «Драйвер», «Фильтр»);
- системные идентификаторы VPN-профиля пользователя Криптосети (уникальный номер Криптосети организации, которой принадлежит данный пользователь ФПСУ-IP/Клиент, уникальный номер логической группы, к которой пользователь прикреплен, и его уникальный персональный номер в этой группе, а также серии ключевых данных) - при работе с программно-аппаратным Клиентом данные сведения отображаются, если устройство VPN-Key подключено в данный момент.

9.2. Информация о сетевых адаптерах

Для получения сведений о сетевых адаптерах компьютера необходимо нажать кнопку «Информация». В верхней части открывшегося окна содержится название установленного на данном компьютере пакета обновлений операционной системы и далее в таблице:

- тип сетевого адаптера;
- аппаратный MAC адрес сетевого адаптера;
- IP-адрес;
- маска подсети;
- IP-адрес шлюза по умолчанию;
- MTU, выставленное на данном сетевом адаптере;
- название сетевого адаптера.

Для изменения MTU на сетевых адаптерах рабочей станции, необходимо ввести рекомендованное администратором сети передачи данных значение, выбрать сетевой адаптер и нажать кнопку «Изменить MTU». Для вступления изменений в силу требуется перезагрузка системы.

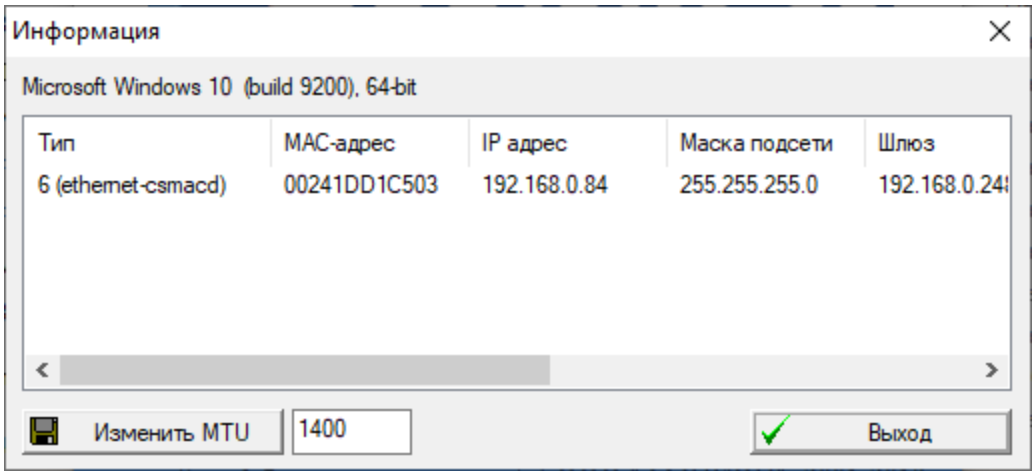
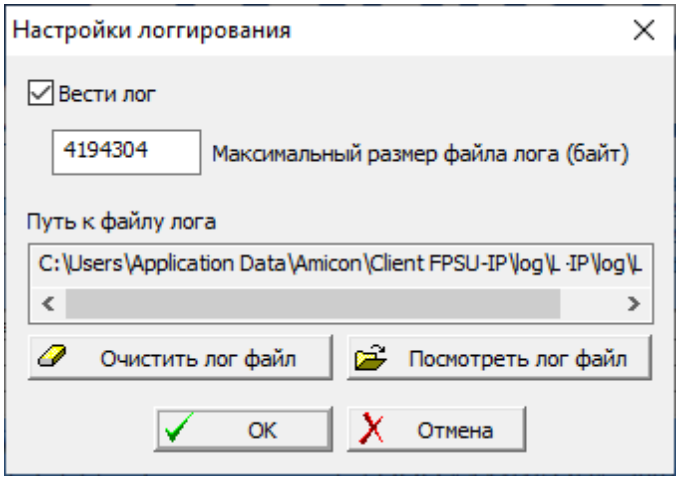


Рисунок 95 - Сведения о сетевых адаптерах

9.3. Настройка журнала событий

ФПСУ-IP/Клиент включает в себя возможность ведение журнала (лога) о происходящих в работе ФПСУ-IP/Клиента событиях — установлении связи с ФПСУ-IP, запуск и остановка работы ПО, открываемых окнах и запускаемых модулях программы, и т.д. По умолчанию журналирование включено. Данную опцию можно включить, установив флаг «Вести лог» в окне «Настройки логирования», открывающемся при нажатии в окне «О программе» кнопки «Лог».



96 - Настройки журналирования

В открывшемся окне также можно указать максимальный размер файла журнала, место хранения. Кнопки «Очистить лог файл» и «Посмотреть лог файл» предназначены для очистки собранной программой информации и просмотра накопленных данных соответственно.

9.4. Просмотр статистики

ФПСУ-IP/Клиент производит автоматический сбор регистрационной информации о принимаемых и передаваемых данных во время его работы в VPN-туннеле с ФПСУ-IP. Подсчет данных производится для всех сетевых адаптеров компьютера.

Для просмотра регистрационных данных, собранных за время существования VPN-туннелей с ФПСУ-IP, необходимо выбрать команду меню «Статистика», после чего на экране появится информационное окно. Для удобства работы размеры окна и его полей можно изменять, растаскиванием границ с помощью мыши.

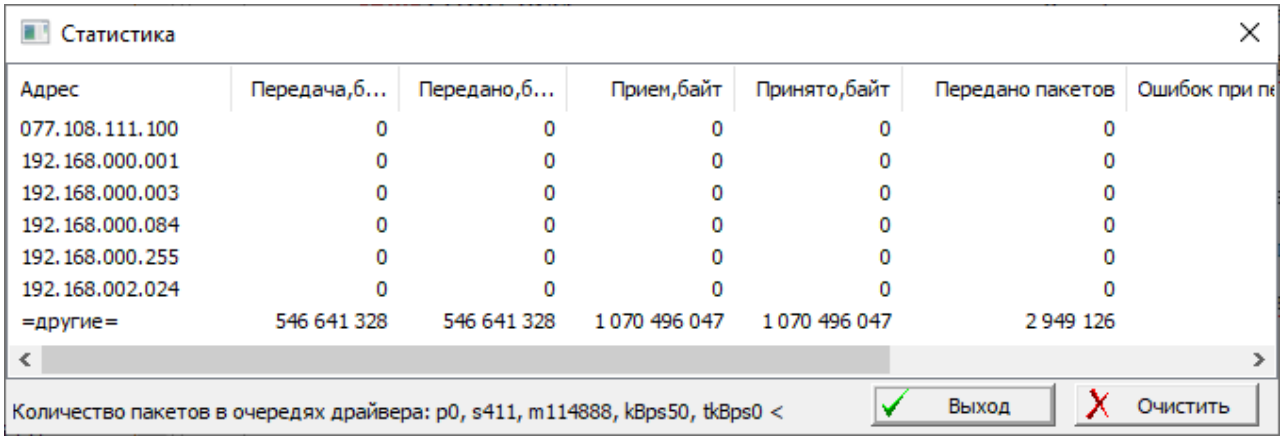


Рисунок 97 - Статистика работы ФПСУ-IP/Клиента в VPN-туннеле

Окно просмотра регистрационной информации построено в виде таблицы, в строках которой для зарегистрированных и незарегистрированных на АРМ ФПСУ-IP/Клиента IP-адресов хостов отображаются следующие данные (отсчет данных ведется с момента включения компьютера или сброса счетчиков вручную пользователем):

Передача, байт	количество байт данных, переданных ФПСУ-IP/Клиенту операционной системой для отправки по данному IP-адресу (адресам);
Передано, байт	количество байт данных, отправленных после соответствующей обработки по данному IP-адресу (адресам);
Прием, байт	количество байт, принятых из сети от данного IP-адреса (адресов);
Принято, байт	количество байт, принятых ФПСУ-IP/Клиент от данного IP-адреса (адресов) и переданных им прикладным программам. Для ФПСУ-IP и защищаемых им серверов этот параметр будет отличаться от предыдущего, поскольку принимаемые из VPN-туннеля данные освобождаются от служебной информации, расшифровываются и, возможно, декомпрессируются;
Передано пакетов	количество пакетов, переданных «ФПСУ-IP/Клиент» в сеть по данному IP-адресу (адресам);
Ошибок при передаче	количество ошибок при передаче пакетов;
Принято пакетов	количество пакетов, принятых ФПСУ-IP/Клиент из сети от данного IP-адреса (адресов);
Ошибок при приеме	количество ошибок при приеме пакетов.

Если слева от IP-адреса отображается буква «d» – это означает, что пакет поступил из VPN-туннеля с ФПСУ-IP, но его IP-адрес в конфигурации не прописан.

Счетчики данных можно сбросить (обнулить) при помощи соответствующей кнопки в нижней части окна. Это удобно, например, при проведении отладочных работ или контрольных замеров. Кроме того, счетчики сбрасываются автоматически при выключении компьютера.

В контекстной строке окна, «Количество пакетов в очередях драйвера:» содержится дополнительная информация о работе межсетевого экрана ФПСУ-IP/Клиент, со следующими информационными параметрами:

- «p» - количество пакетов в очередях драйвера, ждущих отправки в сеть или приема из сети. В штатном режиме работы p должно быть 0, то есть все пакеты были приняты или отправлены;
- «s» - количество TCP сессий в списке у межсетевого экрана;
- «m» - занятая межсетевым экраном оперативная память, в байтах.

9.5. Отображение в списках служб и в реестре

Для того, чтобы найти текстовое название службы в списке служб Windows, необходимо открыть список служб (ввести в меню «Пуск» операционной системы Windows слово «Службы»). «Amicon FPSU-IP/Client service» - отображаемое в интерфейсе служб Windows текстовое название службы.

«IP-Client» - системное короткое имя службы в редакторе реестра (Компьютер\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IP-Client).

10. Сообщения об ошибках при соединении с ФПСУ-IP

При ошибках соединения ФПСУ-IP/Клиент с ФПСУ-IP могут быть выданы указанные в таблице сообщения:

Диагностика ошибок при соединениях с ФПСУ-IP	
Сообщение	**Комментарий**
«Неподдерживаемый криптопротокол»	ФПСУ-IP/Клиент и ФПСУ-IP поддерживают разные версии протокола или набора шифров. Необходимо обратиться к администратору безопасности.
«Не сошлись имитовставки при обмене с устройством»	Необходимо обновить микрокод устройства VPN-Key. Обратитесь к администратору безопасности.
«Драйвер ФПСУ-IP клиента не может получить доступ к сетевому адаптеру»	Необходимо обновить программное обеспечение ФПСУ-IP/Клиента.
«ФПСУ-IP недоступен по неизвестной причине. Проверьте настройки межсетевого экрана и IP-адрес ФПСУ-IP»	Необходимо обратиться к администратору ФПСУ-IP.
«На ФПСУ-IP отключена совместимость с вашей версией клиента, необходимо обновить»	Необходимо обновить ПО ФПСУ-IP/Клиент.
«Превышен лимит одновременно работающих 'программных' клиентов»	Закончились свободные лицензии на одновременное подключение к ФПСУ-IP. Необходимо обратиться к администратору ФПСУ-IP.
«Не указаны идентификационные данные RADIUS»	На ФПСУ-IP задействована дополнительная авторизация через RADIUS-сервер. Пользователь ФПСУ-IP/Клиента не указал учетные данные для авторизации.

Диагностика ошибок при соединениях с ФПСУ-IP	
Сообщение	**Комментарий**
«Отказ аутентификации от RADIUS сервера»	На ФПСУ-IP задействована дополнительная авторизация через RADIUS-сервер. RADUIS-сервер отказал в авторизации с указанными пользователем ФПСУ-IP/Клиента учетными данными. Обратитесь к администратору ФПСУ-IP.
«Нет ответа от RADIUS сервера»	На ФПСУ-IP задействована дополнительная авторизация через RADIUS-сервер. RADIUS-сервер не отвечает. Следует обратиться к администратору ФПСУ-IP.
«Не совпадают RKL роли»	Устройство VPN-Key не поддерживает удаленную загрузку ключевых данных или на ФПСУ-IP не установлена подсистема удаленной загрузки ключевых данных. Следует обратиться к администратору ФПСУ-IP.
«Отказ сетевой подсистемы»	Ошибка в сетевом адаптере/драйвере сетевого адаптера рабочей станции ФПСУ-IP/Клиента, необходимо обратиться к системному администратору.
«Широковещательный адрес запрещен»	Ошибка в настройках сетевого адаптера: адрес ФПСУ-IP трактуется как широковещательный. Необходимо обратиться к администратору сети.
«Сокет закрыт»	Ошибка в сетевом адаптере/драйвере сетевого адаптера рабочей станции ФПСУ-IP/Клиент, необходимо обратиться к системному администратору.
«Удаленный хост недоступен»	Данные не доходят до ФПСУ-IP по причине отсутствия маршрута. Необходимо обратиться к администратору сети.
«Соединение отвергнуто удаленным хостом»	Удаленная рабочая станция (ФПСУ-IP) сбрасывает соединение по одной из следующих причин: хост не является ФПСУ-IP, перезагрузка ПО, внезапный сбой сетевого приложения, неполадки сетевых интерфейсов. Следует проверить, корректно ли указан IP адрес ФПСУ, после чего повторить попытку соединения и/или обратиться к администратору ФПСУ-IP.

Диагностика ошибок при соединениях с ФПСУ-IP	
Сообщение	**Комментарий**
«ФПСУ отвергает авторизацию по неизвестной причине -- Возможно ваши ключевые данные не соответствуют установленным на ФПСУ.»	Необходимо обратиться к администратору ФПСУ-IP.
«Ошибка приема winsock»	Ошибочно сконфигурировано, либо не сконфигурировано сетевое оборудование рабочей станции. Скорее всего не указан или указан неверно основной шлюз (Gateway) в настройках соединения по локальной сети. Необходимо обратиться к администратору локальной сети.
«Неправильный номер системы»	От ФПСУ-IP получен пакет для пользователя другой Криптосети. Необходимо обратиться к администратору ФПСУ-IP.
«Неправильный номер группы»	В полученных данных номер группы не соответствует номеру группы пользователя Криптосети. Необходимо обратиться к администратору ФПСУ-IP.
«Неправильный номер клиента»	Полученные данные предназначены пользователю Криптосети с другим номером. Необходимо обратиться к администратору ФПСУ-IP.
«Неверен идентификатор туннеля»	Ошибка аутентификации. Необходимо обратиться к администратору ФПСУ-IP.
«ФПСУ отвергает код системы распределения»	Общесистемный ключ Криптосети Клиентов данного пользователя не установлен на ФПСУ-IP.
«ФПСУ отвергает доступ в запрошенную сеть»	Общесистемный ключ Криптосети Клиентов данного пользователя не установлен на ФПСУ-IP.
«ФПСУ отвергает доступ в запрошенную группу»	Группа Криптосети, в которую входит пользователь, не зарегистрирована на ФПСУ-IP

Диагностика ошибок при соединениях с ФПСУ-IP	
Сообщение	**Комментарий**
«ФПСУ отвергает доступ клиенту»	Администратор ФПСУ-IP не зарегистрировал пользователя Криптосети с данным номером или не активировал/установил разрешения на его работу.
«Нет памяти для инициализации»	Недостаточно оперативной памяти. Необходимо закрыть лишние прикладные программы и перезагрузить компьютер. При повторном появлении сообщения рекомендуется установить на компьютер дополнительную оперативную память.
«Нет адаптеров. Попробовать исправить и продолжить соединение?»	На компьютере отсутствуют сетевые адаптеры или они некорректно установлены. Необходимо обратиться к администратору локальной сети
«Размер не соответствует типу пакета»	Несовместимая версия ПО ФПСУ-IP. Необходимо обратиться к производителю.
«Запрошено действие в несоответствующем состоянии фильтра»	Ошибка системы. Необходимо обратиться к производителю.
«Пакет игнорируется в текущем состоянии»	Время между отсылкой исходящих пакетов ФПСУ-IP/Клиентом меньше, чем время доставки ответных пакетов от ФПСУ-IP. Необходимо увеличить значение параметра HKey_LOCAL_MACHINE\SOFTWARE\Amicon\ClientFP SU-IP \CLIENTSENDTIMER в реестре WINDOWS (максимально до 20000 миллисекунд). Следует обратить внимание, что значение вводится в шестнадцатеричном виде.
«Исчерпано число попыток соединения!»	ФПСУ-IP/Клиент не получил ответа от ФПСУ-IP за отведенное время. Это может быть связано с неполадками или перегрузками в сети, а также с неполадками на ФПСУ-IP. Необходимо повторить попытку соединения, отправить ФПСУ-IP ICMP-запрос (Ping). Можно обратиться к администраторам сети и ФПСУ-IP.

Диагностика ошибок при соединениях с ФПСУ-IP	
Сообщение	**Комментарий**
«Запрет. Время работы ещё не наступило»	Заданный в группах доступа период работы пользователя Криптосети на ФПСУ-IP ещё не начался. Необходимо обратиться к администратору ФПСУ-IP.
«Запрет. Время работы истекло»	Закончился заданный в группах доступа период работы пользователя Криптосети на ФПСУ-IP. Необходимо обратиться к администратору ФПСУ-IP.

11. Удаление ФПСУ-IP/Клиента

Перед удалением ФПСУ-IP/Клиента, использовавшегося в качестве Программного Клиента, в обязательном порядке следует удалить все загруженные профили и лицензию (см. п.п. Удаление VPN-профиля и Удаление лицензии).

Для удаления программного обеспечения ФПСУ-IP/Клиент 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 «ФПСУ-IP/Клиент» и нажав кнопку «Удалить».

В качестве первого этапа деинсталляции будет предложено выбрать язык, соответствующий установленному.

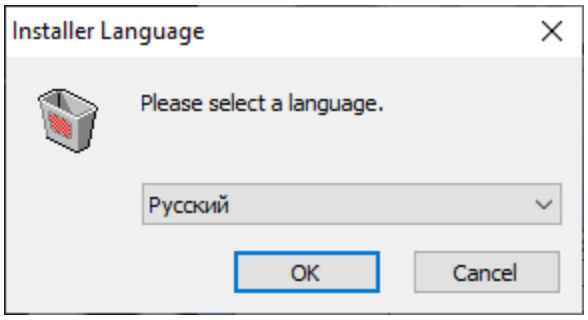


Рисунок 98 – Окно выбора языка

После выбора языка необходимо нажать кнопку «ОК». Откроется окно, в котором отобразится путь к папке с установленным программным обеспечением.

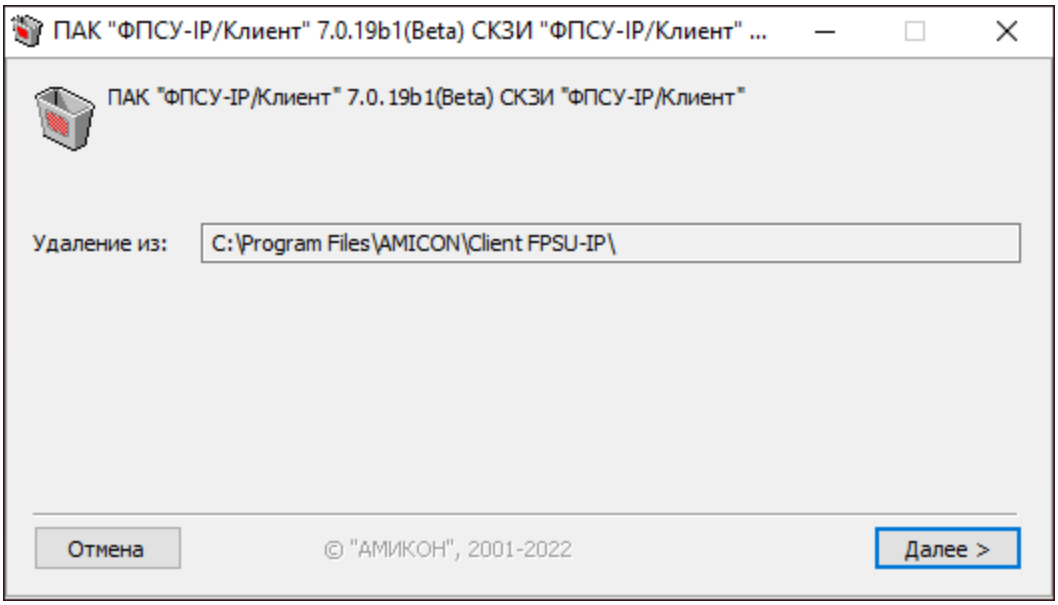


Рисунок 99 – Отображение папки для удаления ПО

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

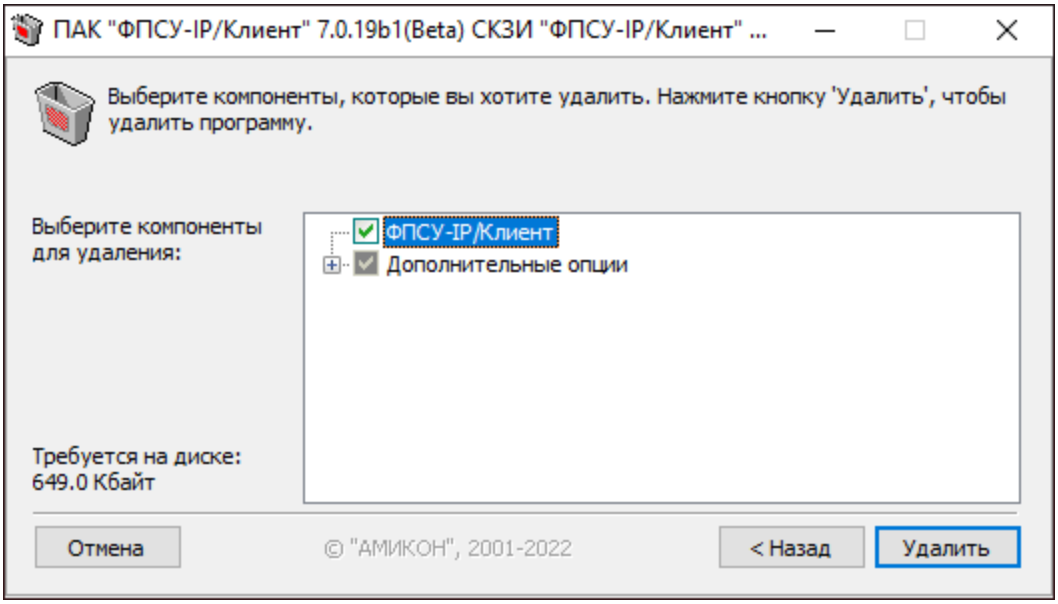


Рисунок 100 – Выбор компонент ПО для удаления

Будет выполнен переход в окно прогресса удаления программного обеспечения, по завершению которого состояние перейдет в статус «Готово». Нажмите кнопку «Далее >» для продолжения

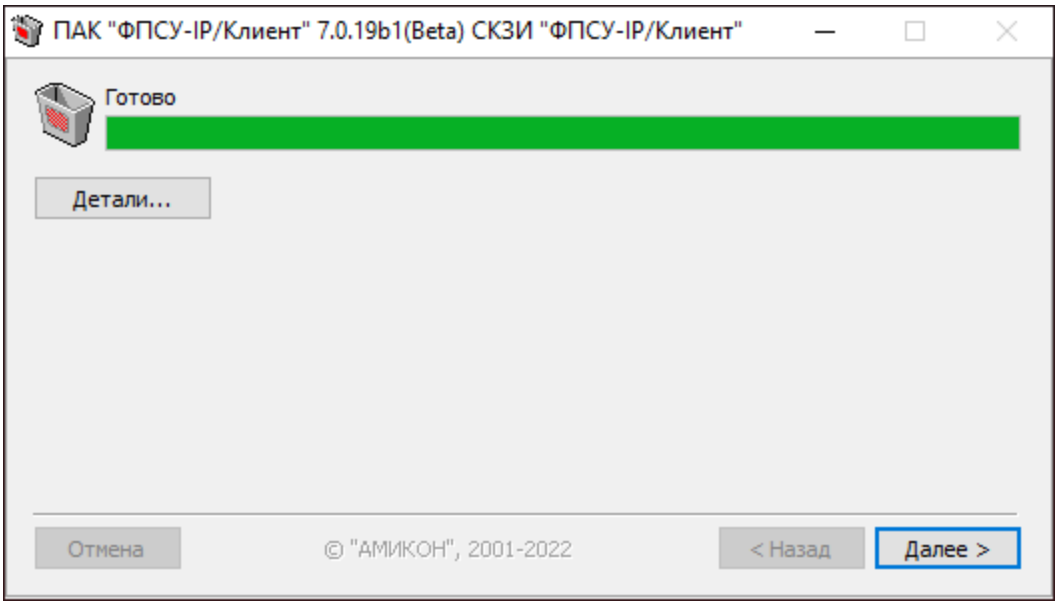


Рисунок 101 – Прогресс удаления ПО

Откроется окно успешного завершения деинсталляции. Для продолжения необходимо нажать кнопку «Закрыть»:

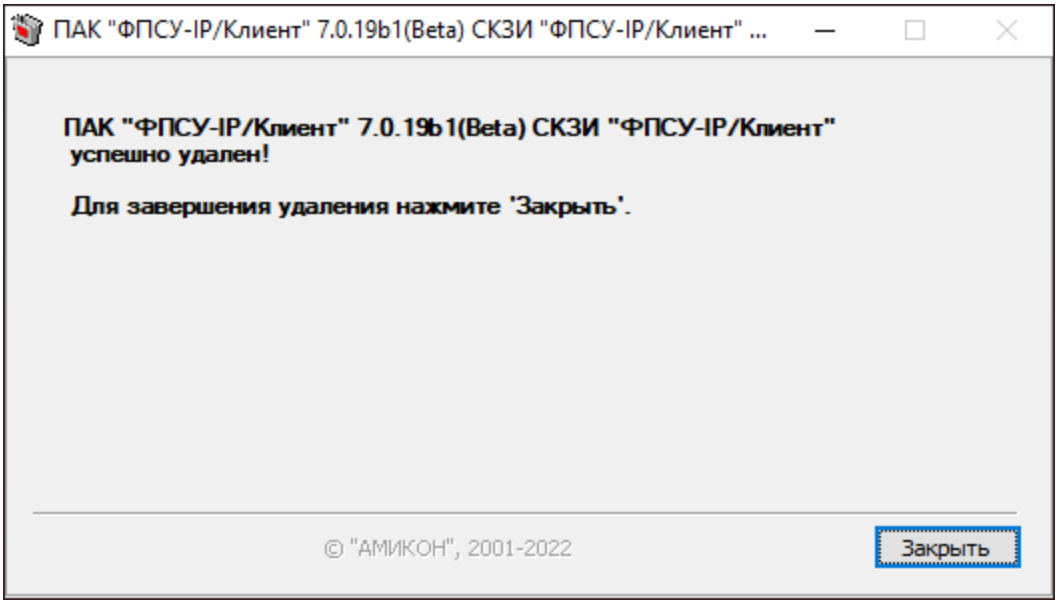


Рисунок 102 – Удаление ПО завершено

После завершения процесса деинсталляции рекомендуется выполнить перезагрузку ОС компьютера.