ООО «ВАЛИДАТА»

ПРОГРАММА «ВАЛИДАТА АРХИВАТОР L»
(ПРОГРАММА АРХИВАТОР)

РУКОВОДСТВО ПО УСТАНОВКЕ И НАСТРОЙКЕ

ВАМБ.00197-01 91 01

2023

Основные понятия и определения

Термин		**Определение**
БД	-	База данных
ПК	-	Программный комплекс
АРМ	-	Автоматизированное рабочее место
ОС	-	Операционная система
ПО	-	Программное обеспечение
СКЗИ	-	Средство криптографической защиты информации
TLS	-	Transport Layer Security – протокол защиты сетевого уровня
TCP	-	Transmission Control Protocol – один из основных сетевых протоколов передачи данных
DER	-	Distinguished Encoding Rules – бинарная кодировка, применяемая для кодирования сертификатов
VPN	-	Виртуальные частные сети

АННОТАЦИЯ

Настоящий документ содержит описание установки и настройки Программы Резервного копирования (далее – Программа) под управлением ОС Linux.

Программа предназначена для организации резервного копирования различных данных (файлы, каталоги, архивы, резервные копии БД) на сервере с ОС Linux. Программа автоматически выполняет настраиваемые процедуры создания резервных данных, пересылку их на резервный сервер (ОС Linux), а также обеспечивает защиту пересылаемых данных. Дополнительно в Программе реализован «TLS посредник» для создания защищенных прокси соединений, «TLS шлюз» для создания виртуальных частных сетей (VPN) и «TLS файл» для организации автоматического обмена подписанными файлами между сервером и его клиентами.

Предусмотрен кластерный режим работы.

Документ предназначен для администраторов в качестве руководства по установке и настройке.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Программа Резервного копирования предназначена для организации:

- резервного копирования различных данных (файлы, каталоги, архивы, резервные копии БД) на сервере с ОС Linux;
- защищенной пересылки данных через TLS посредник (прокси);
- защищенных сетевые взаимодействий между сервером и его клиентами с помощью TLS шлюза для организации виртуальных частных сетей (VPN);
- защищенного автоматического обмена файлами между сервером и его клиентами по TLS протоколу в подписанном виде.

Программа поддерживает кластерный режим работы.

1.2 Условие выполнения

1.2.1. Требования к установке

Если Программа не использует TLS и кластерный режим работы, то выполнять предварительные установки не нужно.

При использовании TLS перед установкой Программы необходимо выполнить установку следующего ПО:

- ПК «Валидата Клиент L» версия 6.

Если Программа устанавливается на кластер, то нужно дополнительно установить:

- Кластерное ПО Corosync.

Примеры установки этих программных пакетов для deb дистрибутива даны ниже.

1	sudo dpkg -i zpki-6.0.464.0-0.amd64.deb Подключить CD диск с ОС Linux и установить дополнительное необходимое ПО. sudo apt -f install –y	ПК «Валидата Клиент L» версия 6
2	sudo apt install pacemaker pcs –y	Кластерное ПО Corosync

1.2.2. Требования к сертификатам

При использовании протокола TLS нужно учитывать следующие требования к сертификатам.

1.2.2.1. Сертификат сервера

Сертификат TLS сервера должен содержать обязательный идентификатор (OID) в «расширенной области применения»: проверка подлинности TLS сервера (1.3.6.1.5.5.7.3.1).

Сертификат TLS сервера должен содержать доменное имя сервера в «альтернативном имени владельца» DNS: «доменное имя сервера» (например, TLS.server).

1.2.2.2. Сертификат клиента

Сертификат TLS клиента должен содержать обязательный идентификатор (OID) в «расширенной области применения»: проверка подлинности TLS клиента (1.3.6.1.5.5.7.3.2).

2 УСТАНОВКА ПРОГРАММЫ

2.1 Установка

Установка Программы Архиватора осуществляется на АРМ или сервер, работающие под управлением ОС Linux, из дистрибутива bucopvd.deb с помощью команды:

sudo dpkg -i bucopvd.deb

Все программы Резервного копирования устанавливаются в раздел «Утилиты» (Utility) операционной системы.

Для операционных систем (ОС) Linux (например, OpenSUSE) установка выполняется с помощью дистрибутива bucopvd-1.0.1-1.x86_64.rpm (версия 1.0.1-1 может изменяться):

sudo rpm -i ./bucopvd-1.0.1-1.x86_64.rpm

или

sudo zypper install ./bucopvd-1.0.1-1.x86_64.rpm

2.2 Отключение FIREWALL

Если под ОС Linux установлен FIREWALL то его работа мешает Архиватору создавать виртуальные частные сети (VPN) в режиме TLS шлюза. В этом случае FIREWALL нужно отключить. Например, под ОС Linux OpenSUSE он устанавливается по умолчанию.

Проверить наличие FIREWALL можно с помощью команды:

systemctl status firewalld

Убрать его из автозапуска можно так:

sudo systemctl disable firewalld

Для его остановки выполнить команду:

sudo systemctl stop firewalld

2.3 Состав установленного ПО

	/opt/validata/bucopvd	Каталог размещения ПО
1	./bin	Подкаталог с программами
	bucopvd	Сервис Архиватора, работающий в автоматическом режиме

	bucopvdcfg	Конфигурационная программа, работающая в интерактивном (ручном) режиме
	bucopvd_d	Сервисная утилита, которая необходима для решения проблемы загрузки ключа в кластерном режиме работы
	bucopvdmon	Интерактивная программа мониторинга, обеспечивающая запуск и остановку программы файлового шлюза
	bucopvdlic	Программа установки лицензии
2	./share	Подкаталог описаний для «десктопа»
	bucopvdcfg.desktop	Описание конфигурационной программы
	bucopvd.desktop	Описание сервиса
	bucopvdmon.desktop	Описание программы мониторинга
	bucopvdcfg_root.desktop ru.x509.bucopvdcfg.policy	Описание конфигурационной программы для запуска от имени Администратора (root)
	bucopvd_root.desktop ru.x509.bucopvd.policy	Описание сервиса для запуска от имени Администратора (root)
	bucopvdmon_root.desktop ru.x509.bucopvdmon.policy	Описание программы мониторинга для запуска от имени Администратора (root)
	bucopvdlic_root.desktop ru.x509.bucopvdlic.policy	Описание программы установки лицензии для запуска от имени Администратора (root)
3	./signal	Подкаталог управляющего сигнала
	system_add	Командная процедура создания сервиса
8	./signal/proceed	Подкаталог управляющего сигнала для продолжения работы в режиме кластера
	bucopvd.in	Управляющий сигнал сервиса
9	./signal/quit	Подкаталог управляющего сигнала принудительного завершения
	bucopvd_d.in	Управляющий сигнал для сервисной утилиты

10	./signal/stop	Подкаталог управляющего сигнала для остановки
	bucopvd_d.in	Управляющий сигнал для сервисной утилиты
	bucopvd.in	Управляющий сигнал для сервиса
11	./signal/suspend	Подкаталог управляющего сигнала остановки в режиме кластера
	bucopvd.in	Управляющий сигнал для сервиса

2.4 Дополнительные команды

1	sudo dpkg -r bucop	Деинсталляция Файлового шлюза
2	dpkg -l bucop dpkg -l | grep bucop	Посмотреть состояние установки

3 НАСТРОЙКА ПРОГРАММЫ

3.1 Конфигурационная программа

3.1.1. Запуск

Запуск конфигурационной программы осуществляется в главного меню ОС, в разделе «Утилиты», в строке «Конфигурация Архиватора». Для запуска от имени Администратора (root) необходимо выбрать «Конфиг. Архив. (Админ.)»

Запуск можно выполнить из терминального окна с помощью команды:

/opt/validata/bucopvd/bin/bucopvdcfg

На экран выдается следующее диалоговое окно.

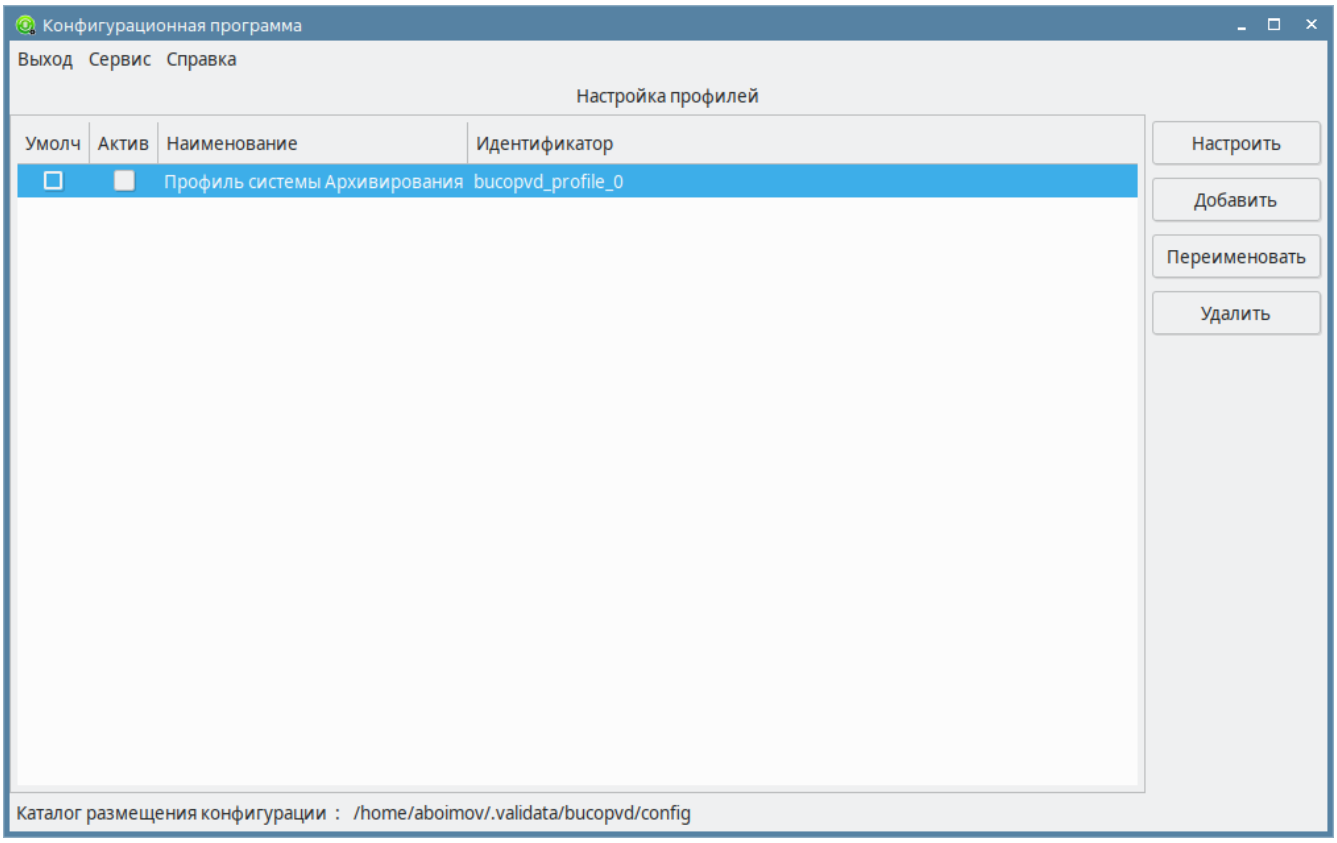

Рисунок 1. Главное окно конфигурационной программы

При первом запуске создается нулевой профиль с именем «Профиль системы Резервного копирования» с идентификатором «bucopvd_profile_0», который отмечен как запускаемый по умолчанию.

Данный диалог позволяет добавлять новые профили, удалять и переименовывать их. Но при переименовании нельзя изменять идентификатор.

При добавлении профиля нужно задать его наименование (это произвольная строка, которая несет только визуальную информацию) и идентификатор, который является именем XML файла со всеми конфигурационными параметрами. Идентификатор может содержать только латинские буквы в нижнем регистре, цифры и символ подчерка «_». Длина идентификатора не может превышать 64 символа.

В нижней строке окна отображается каталог конфигурации, который находится в HOME разделе пользователя, запустившего программу конфигурации.

~/.validata/bucopvd/config

Все настроенные конфигурационные профили будут доступны только для работы от имени этого пользователя.

Список профилей размещается в основном файле bucopvd_config.xml. Все профили лежат рядом в файлах «идентификатор».xml (например, bucopvd_profile_0.xml). При любом изменении содержимого профиля, предыдущая версия сохраняется в файле «идентификатор».xml~ (например, bucopvd_profile_0.xml~).

Идентификатор профиля нужен для запуска сервиса Программы, который выполняется следующим образом:

/opt/validata/bucopvd/bin/bucopvd <идентификато>

Например:

/opt/validata/bucop/bin/bucopvd bucopvd_profile_0

Если запустить сервис без параметра, то он будет работать с конфигурацией профиля, отмеченного по умолчанию, как будто он был запущен с параметром идентификатора, отмеченного по умолчанию.

Нельзя запустить два сервиса с одинаковым идентификатором профиля.

3.1.2. Главное меню программы

Главное меню программы позволяет выполнить следующие действия.

- Выйти из программы конфигурации.
- Настроить параметр (по умолчанию /usr/bin/kate), содержащий имя программы текстового редактора, который будет использоваться при просмотре текстовых файлов с протоколами работы программы.
- Выдать информацию о программе.

3.1.3. Настройка

Для настройки параметров профиля его нужно выбрать и нажать кнопку «Настроить».

3.1.3.1. Общие параметры

На экран будет выдан раздел «Общие»

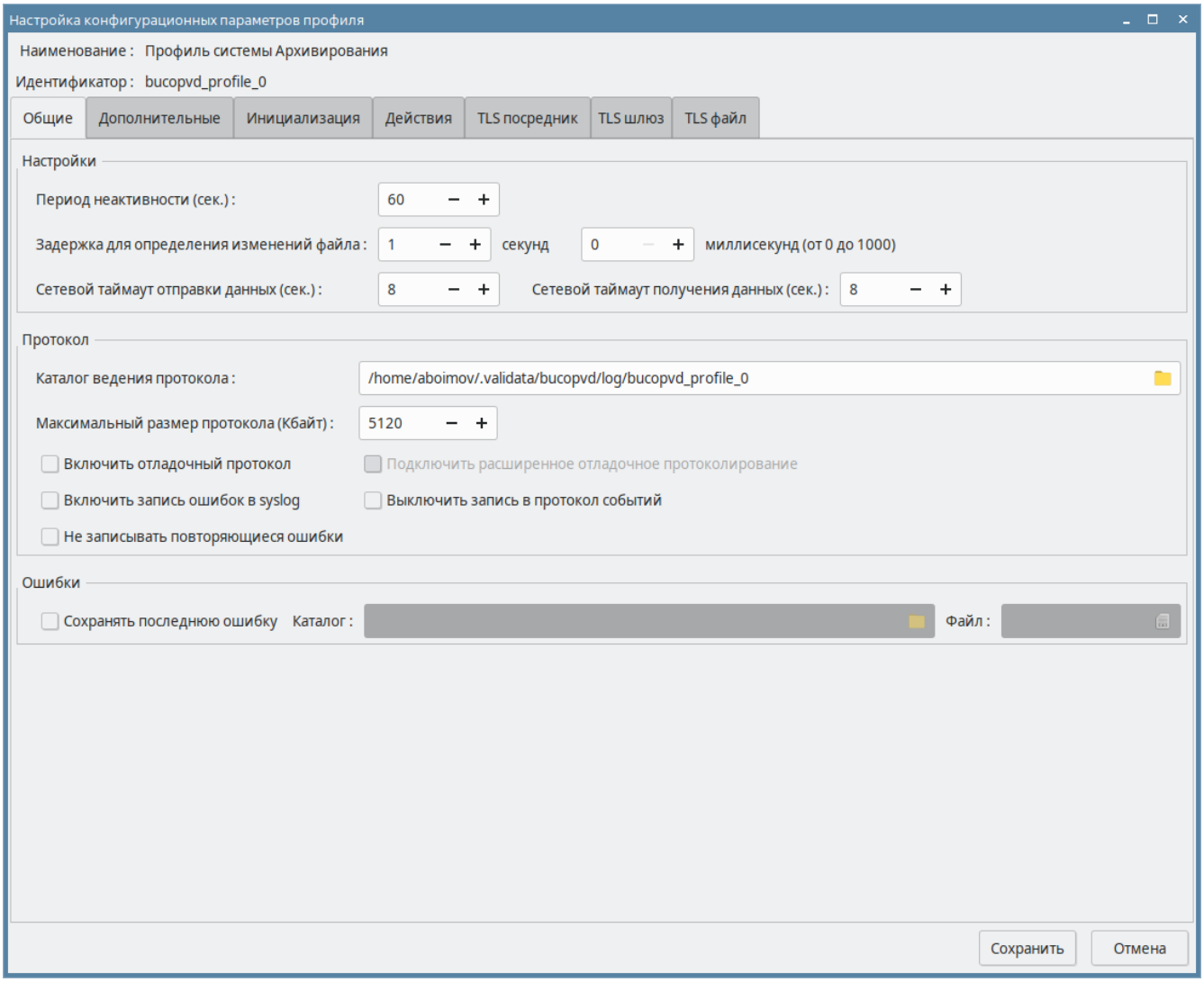

Рисунок 2. Настройка общих параметров

В разделе «Настройки» в параметре «Период неактивности (сек.)» устанавливается значение периода «засыпания» программы перед выполнением каждой проверкой инициализационных данных.

Параметр «Задержка для определения изменений файла» позволяет настроить период времени между двумя чтениями файла, чтобы определить наличие его изменений.

Параметры «Сетевой таймаут отправки данных (сек.)» и «Сетевой таймаут получения данных (сек.)» определяют время зависания при отправке и получении данных по сети.

В разделе «Протокол» в параметре «Каталог ведения протокола» устанавливается значение каталога, в котором будут размещаться файлы протокола работы сервиса программы.

Каталог ведения протокола задает место хранения файловых протоколов:

- bucopvd.log - протокол ошибок сервиса Программы;
- bucopvd_report.log - протокол событий сервиса Программы.

Максимальный размер протокола задет параметр в Кбайтах, после достижения которого файл протокола будет пересоздаваться. Предыдущий файл сохраняется с добавлением порядкового номера (например, bucopvd.log, bucopvd~1.log, bucopvd~2.log, …). Если этот параметр равен 0, то протокол будет записываться в один файл. Этот параметр распространяется на протокол ошибок и протоколы событий.

Параметры «Включить отладочный протокол» и «Подключить расширенное отладочное протоколирование» предназначены только для решения проблемы, когда даже разработчик ПО не может разобраться с возникающей ошибкой в работе Программы. Для штатной работы ПО эти параметры включать не рекомендуется. Если включен отладочный режим протоколирования, то дополнительно к штатным файлам протокола будет создаваться отладочные файлы протокола с именами: debug_bcp.log, debug_socket.log, debug_gw_send_socket.log, debug_gw_recv_socket.log, debug_gw_socket.log.

Параметр «Включить запись ошибок в syslog» позволяет организовать дополнительное протоколирование ошибок в системный протокол ОС Linux, который называется syslog. Эта запись не отменяет ведение штатного текстового протокола ошибок (bucopvd.log).

С помощью параметра «Выключить запись в протокол событий» можно отключить протокол событий (bucopvd_report.log).

Параметр «Не записывать повторяющиеся ошибки» позволяет не записывать в протокол ошибок (bucopvd.log) больше 3 повторяющихся ошибок за каждый час.

В разделе «Ошибки» можно указать каталог и имя файла, в который будет записана последняя ошибка Программы. Данная процедура позволяет отследить возникновении ошибки и выполнить ее обработку.

3.1.3.2. Дополнительные параметры

Для настройки дополнительных параметров выберите закладку «Дополнительные»

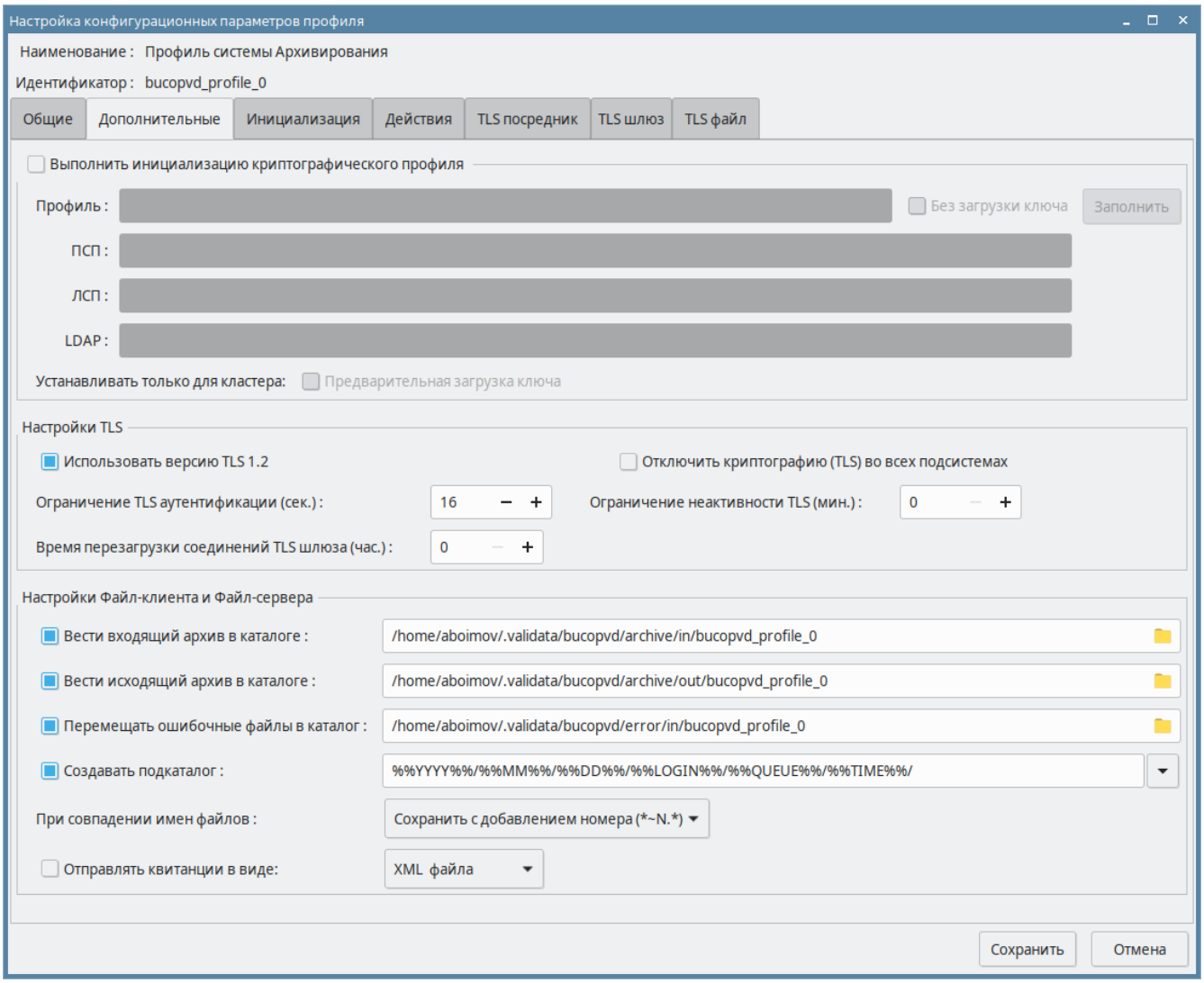

Рисунок 3. Настройка дополнительных параметров.

Для заполнения криптографического профиля (включая ПСП, ЛСП и LDAP) необходимо выбрать раздел «Выполнить инициализацию криптографического профиля» и нажать кнопку «Заполнить». На экран будет выдан диалог со списком криптографических профилей пользователя, запустившего программу конфигурации. Предварительно этот пользователь должен создать с помощью ПК «Валидата Клиент L» один или несколько криптографических профилей.

Если настройка криптографического профиля выполняется для TLS шлюза, то профили ПК «Валидата Клиент L» нужно создавать под учетной записью Администратора (root). Для этого установка Программы создает специальный пункт меню «Справочник Серт. (Админ.)», который обеспечивает запуск «Справочника сертификатов» от имени Администратора (root).

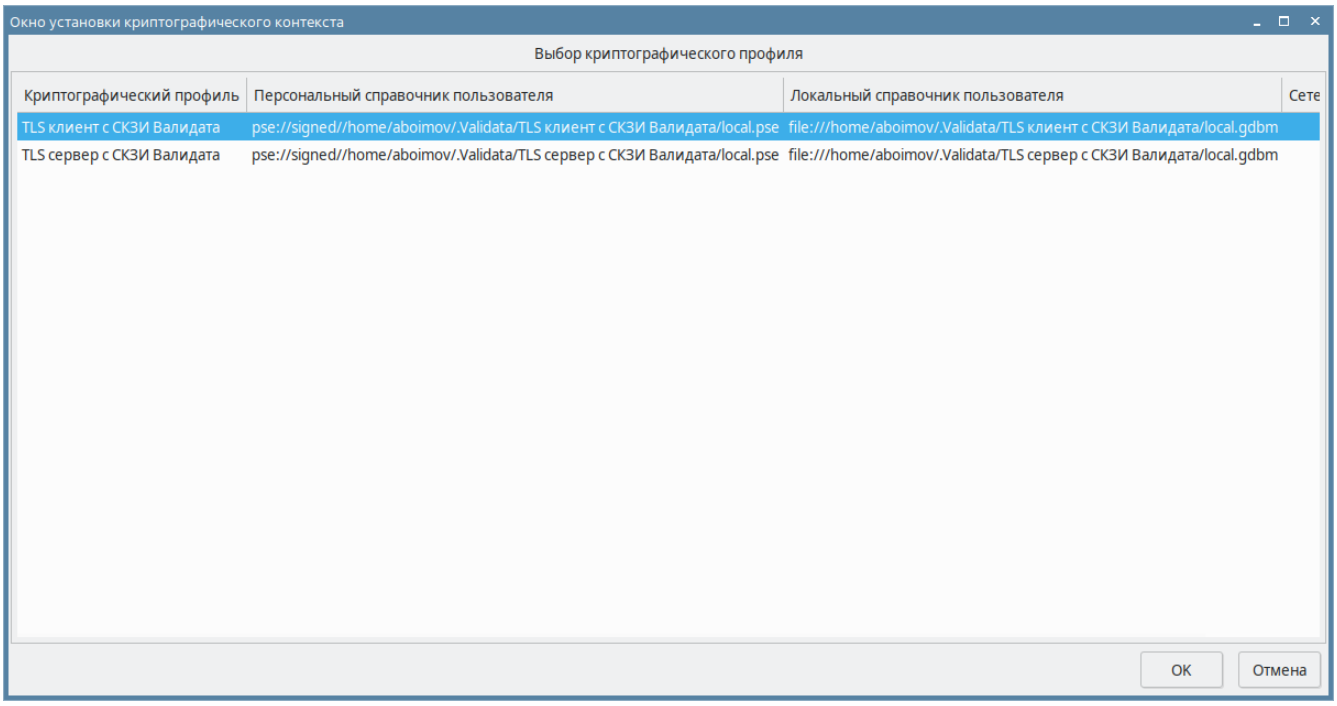

Рисунок 4. Выбор криптографического профиля

Выберете нужный криптографический профиль из списка и нажмите кнопку «ОК»

Опциональный параметр «Без загрузки ключа» обеспечивает загрузку криптографического профиля без загрузки ключа. Такой криптографический профиль может использоваться для анонимного режима работы клиента TLS прокси.

Если вы собираетесь использовать сервис Программы в кластерном режиме, то установите опциональный параметр «Предварительная загрузка ключа». В этом случае сервис после запуска загрузит ключ, но работать не будет. Для начала и завершения работы Файловый шлюз будет ожидать сигналов от Сервисной утилиты (bucopvd_d), которой должен управлять кластер (corosync).

Настройка криптографического профиля может выглядеть так, как это показано на следующей картинке.

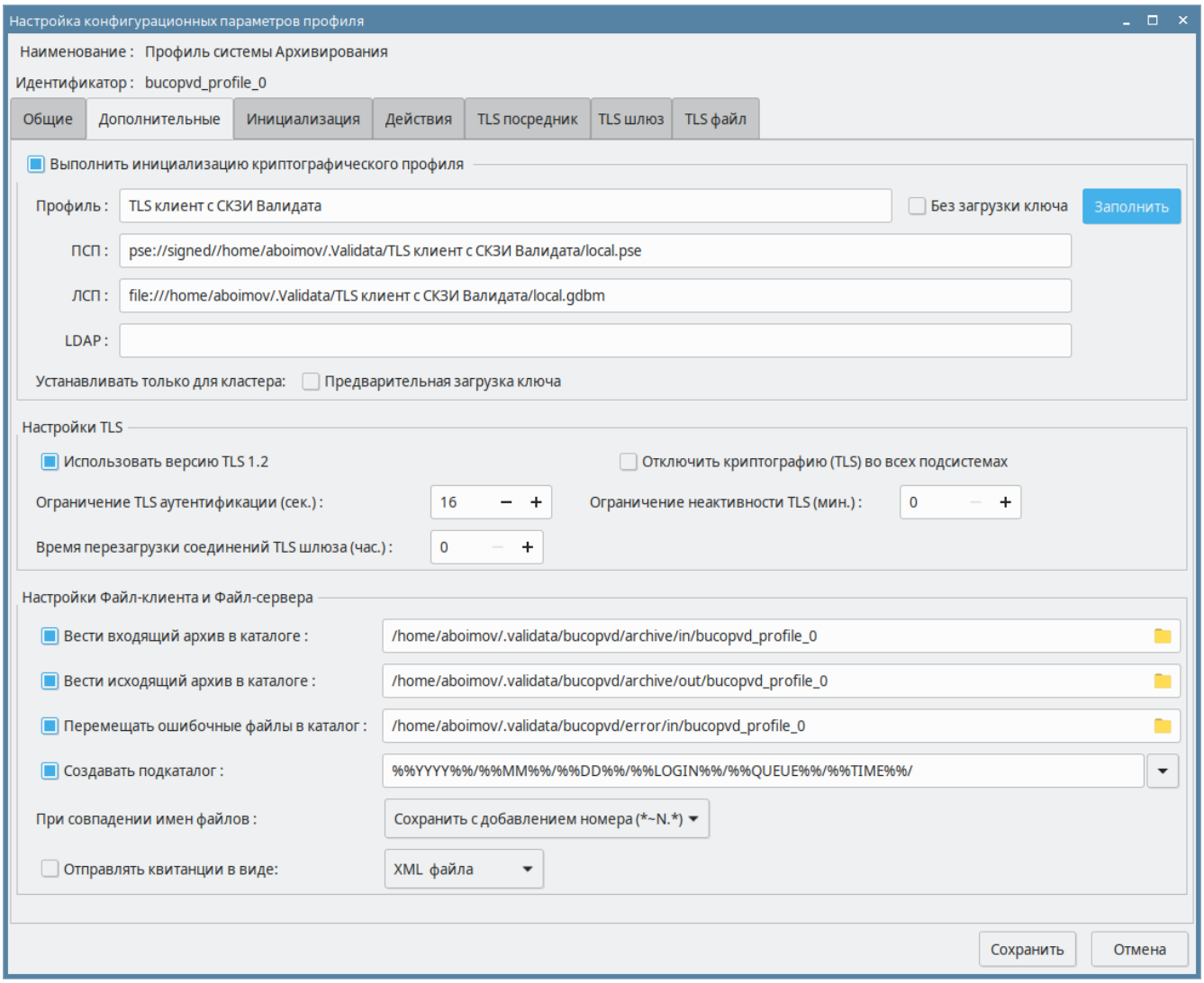

Рисунок 5. Настройка криптографического профиля.

Настройки раздела «Настройки TLS» позволяют задать следующий набор параметров.

Установка параметра «Отключить криптографию (TLS) во всех подсистемах» отключает загрузку криптографического профиля и всех криптографических функций данного профиля. Данный режим работы можно применять для тестирования работы Программы без криптографии и ключей.

Параметр «Использовать версию TLS 1.2» включает использование нового протокола TLS, который работает на новом криптографическом алгоритме («Кузнечик»).

Параметр «Ограничение TLS аутентификации (сек.)» обеспечивает установку времени ожидания выполнения аутентификации по протоколу TLS. Если за отведенное время аутентификация не будет завершено, то произойдет автоматический разрыв сетевого соединения. Установка 0 выключает применение этого параметра.

Установка времени в параметре «Ограничение неактивности TLS (мин.)» позволяет разрывать сетевые соединения, по которым не идет обмен данными, через указанное время. Установка 0 выключает применение этого параметра.

Параметр «Время перезагрузки соединений TLS шлюза (час.)» позволяет принудительно разрывать сетевые соединения через указанное время вне зависимости от трафика, проходящего через эти соединения. Установка 0 выключает применение этого параметра.

Раздел параметров «Настройки Файл-клиента и Файл-сервера» предназначен только для службы, работающей в режиме «TLS файл».

Данные параметры позволяют:

- вести архив всех входящих файлов в заданном каталоге;
- вести архив всех исходящих файлов в заданном каталоге;
- в случае возникновения ошибок по приему входящих файлов перемещать их в указанный каталог.

Параметр «Создавать подкаталог» предоставляет возможность структурировать размещение файлов в архивных каталогах и каталоге ошибок. Специальные символьные последовательности будут заменены следующим образом:

- %%YYYY%% - заменяется на текущий год (например, 2023);
- %%MM%% - заменяется на текущий месяц (например, 03);
- %%DD%% - заменяется на текущий день (например, 27);
- %%LOGIN%% - заменяется для сервера на логин клиента, с которым взаимодействует сервер, а для клиента заменяется на его локальный логин;
- %%QUEUE%% - заменяется на идентификатор используемой очереди;
- %%TIME%% - заменяется на текущее время в формате HHMMSS (например, 133657).

Если специальных символов нет, то замена не производится.

Настройка «При совпадении имен файлов» позволяет задать три режима:

- «Перезаписать файл»;
- «Сохранить с добавлением номера (*~N.*)»;
- «Выдать сообщение об ошибке».

Установленный опциональный параметр «Отправлять квитанцию в виде» будет заставлять «Файл-клиент» или «Файл-сервер» отправлять квитанцию о получении файла в виде XML или

текстовом виде. Квитанция содержит имя полученного файла, его размер, хэш-функцию и дату получения.

3.1.3.3. Инициализация программы

Перейдите в раздел «Инициализация»

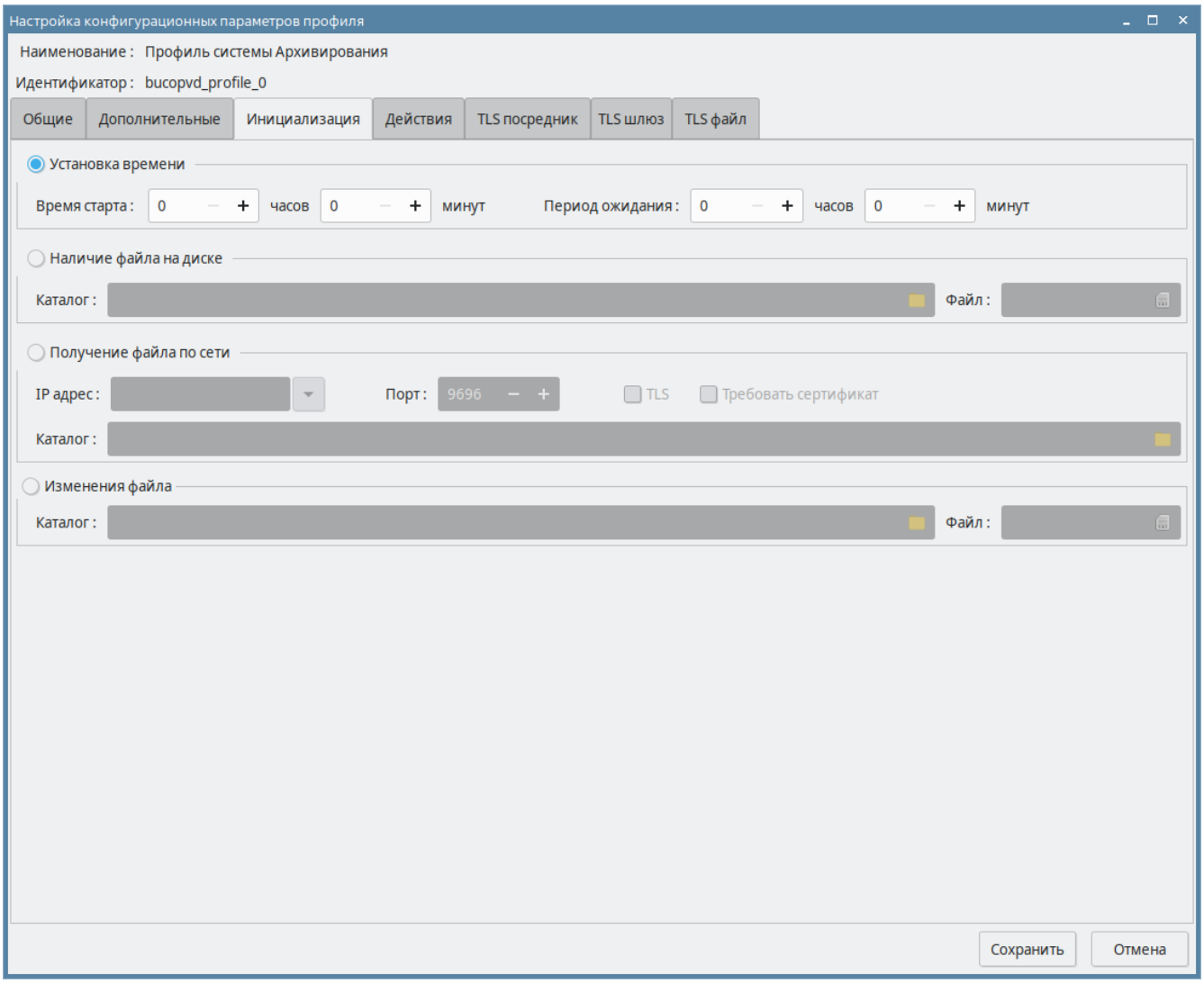

Рисунок 6. Общие настройки

Закладка «Инициализация» позволяет выбрать один из 4 режимов инициализации выполнения набора действий, которые задаются в следующей закладке «Действия».

В разделе «Установка времени» можно уставить время активации набора действий в периоде каждых суток.

Параметр «Время старта» обеспечивает выполнение действий каждый день в заданное время. Например, если установить 23 часа 30 минут, то сервис будет выполняться каждый день в 23.30.

«Период ожидания» позволяет установить периодичность выполнения набора действий в течении дня. Например, если установить 6 часов 0 минут, то сервис будет выполняться периодически через каждые 6 часов, начиная с времени, заданном в параметре «Время старта».

Если «Время старта» установить равным 0 часов 0 минут, то время старта будет считаться равным времени запуска сервис.

«Период ожидания» равный 0 часов 0 минут означает, что периодичность будет составлять сутки (24 часа)

Если установить «Время старта» равным 0 часов 0 минут и «Период ожидания» равный 0 часов 0 минут, действия сервиса будут выполнены один раз в момент запуска программы, а после выполнения программа завершится (будет выгружена из памяти ОС). Данный режим предусмотрен для однократного запуска программы.

Раздел «Наличие файла на диске» обеспечивает запуск набора действий, как только программа обнаружит заданный файл в заданном каталоге. При инициализации этот файл не удаляется. Если в наборе действий не задать удаление этого файла, то программа после периода неактивности «Период неактивности (сек.)» будет активировать набор действий каждый раз.

В разделе «Получение файла по сети» задаются сетевые параметры IP адреса и номера порта, на которое будет передан файл. Сохранение полученного файла будет выполнено в указанный каталог. Если установить параметр «TLS», то программа будет принимать файл только по протоколу TLS, для которого необходимо обязательно задать криптографический профиль. Установка параметра «Требовать сертификат» запрещает использовать клиенту анонимный режим TLS.

Раздел «Изменения файла» обеспечивает запуск набора действий, как только программа обнаружит, что заданный файл в заданном каталоге был изменен. Если файл находится в каталоге при запуске программы, то считается, что он был изменен.

3.1.3.4. Действия программы

Рассмотрим назначение параметров в раздел «Действия».

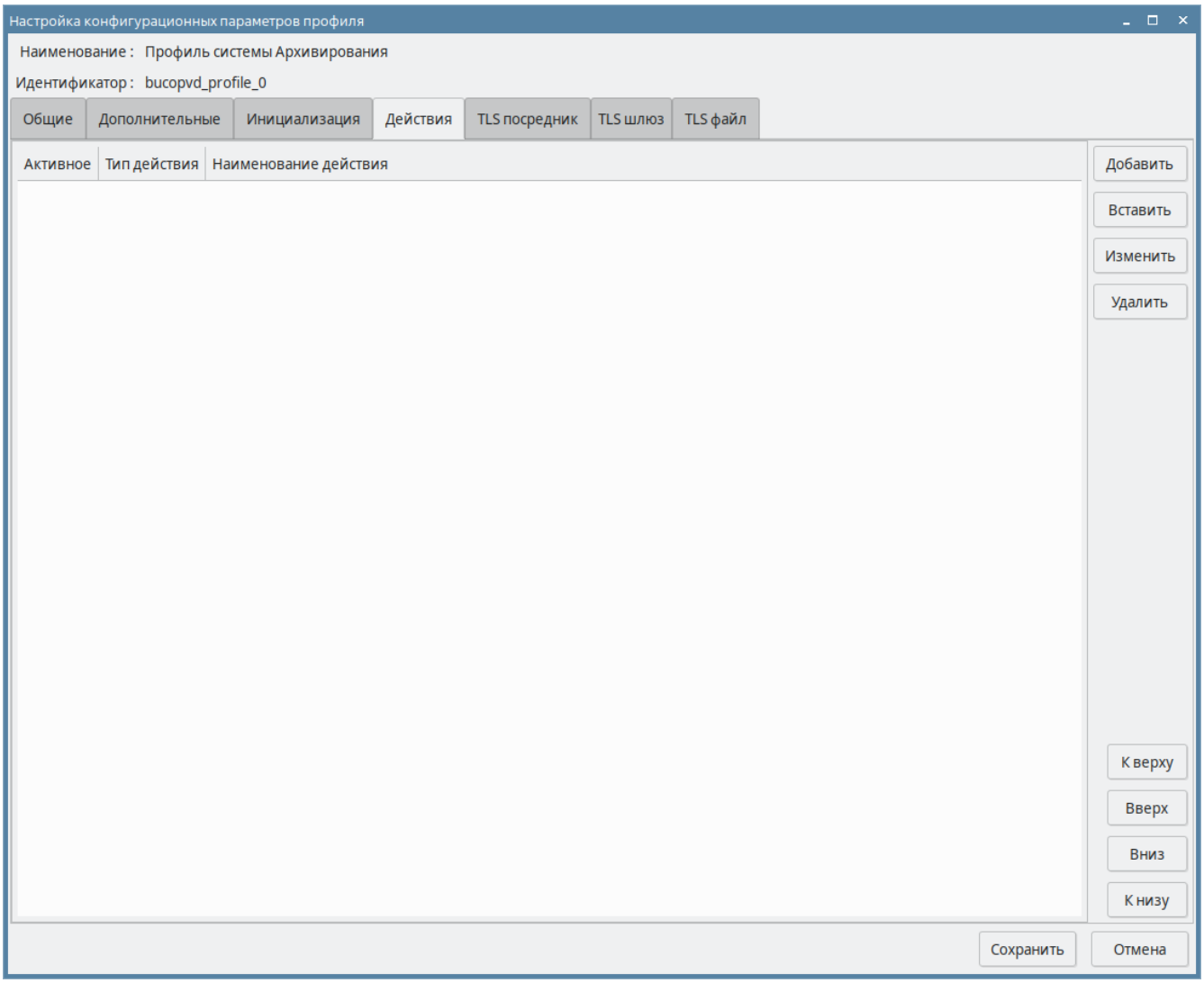

Рисунок 7. Настройка действий программы.

Закладка «Действия» обеспечивает задание списка действий, которые будут выполняться последовательно от первого до последнего, после применения одного из 4 режимов инициализации, заданных в закладке «Инициализация».

Кнопка «Добавить» позволяет добавить одно действие в конец списка.

Кнопка «Вставить» добавляет одно действие перед строкой, выделенной курсором.

Для изменения действия, выделенного курсором, предусмотрена кнопка «Изменить».

Удалить одно или несколько действий можно с помощью кнопки «Удалить». Данный список предусматривает множественное выделение курсором с помощью одновременного нажатия «мыши» и кнопки «Ctrl» («Shift»).

Кнопки «К верху», «Вверх», «Вниз» и «К низу» позволяют изменить последовательность в списке действий, перемещая выделенные курсором одно действие или несколько действий.

После нажатия на кнопку «Добавить» на экран выдается следующий диалог.

Рисунок 8. Добавление действия.

По умолчанию диалог предлагает добавить активное действие. Если убрать отметку параметра «Действие активно», то добавленное действие будет присутствовать в списке, но выполняться не будет.

Прежде всего нужно задать тип действия. Параметр «Тип действия» имеет 5 вариантов:

- «Консольная утилита»;
- «Отправка файла»;
- «Копирование файла»;
- «Запуск программы»;
- «Наличие файла».

Дополнительно нужно обязательно задать произвольное наименование этого действия, которое будет иметь только информационное значение.

После нажатия на кнопку «Настроить» выдается диалог заполнения параметров выбранного типа действий.

Тип действия «Консольная утилита».

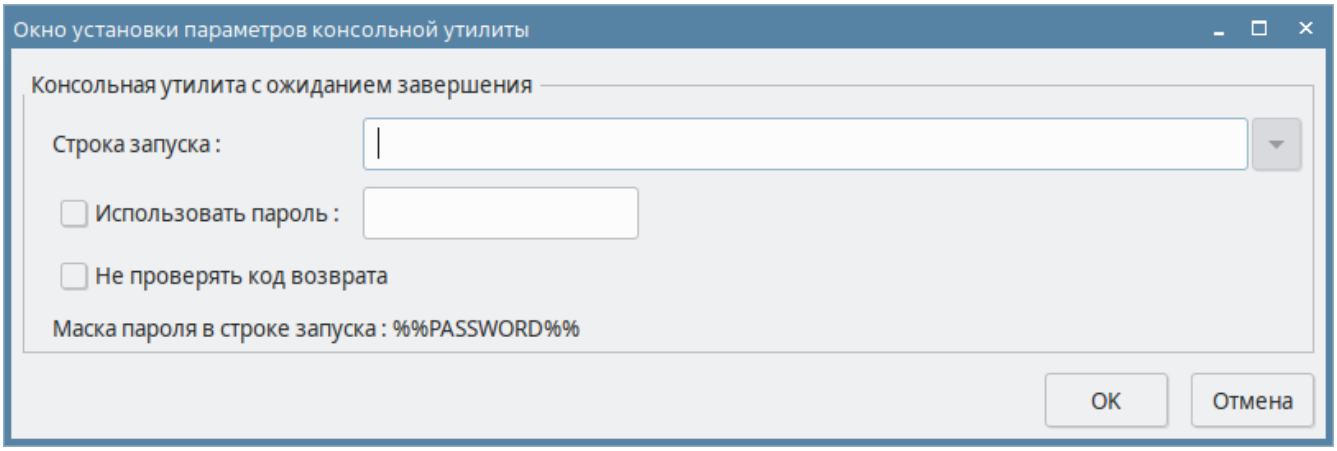

Рисунок 9. Консольная утилита.

В строке запуска задается исполняемая команда так, как эта команда записывается в консоли для выполнения. Например, для удаления файла можно задать такую команду (rm –f /home/username/file/text.txt).

Если в командной строке нужно передать пароль, то вместо него нужно указать специальное имя в верхнем регистре (%%PASSWORD%%). Включить параметр «Использовать пароль» и ввести пароль, который в диалоге будет отображаться символами «*».

При выполнении командной утилиты обычно при успешном выполнении возвращается нулевой код возврата и не нулевой при ошибке. По умолчанию Программа завершится с ошибкой, если получит не нулевой код возврата. Если включить параметр «Не проверять код возврата», то Программа будет его игнорировать.

Действие «Консольная утилита» будет ожидать завершения выполняемой команды.

Тип действия «Отправка файла».

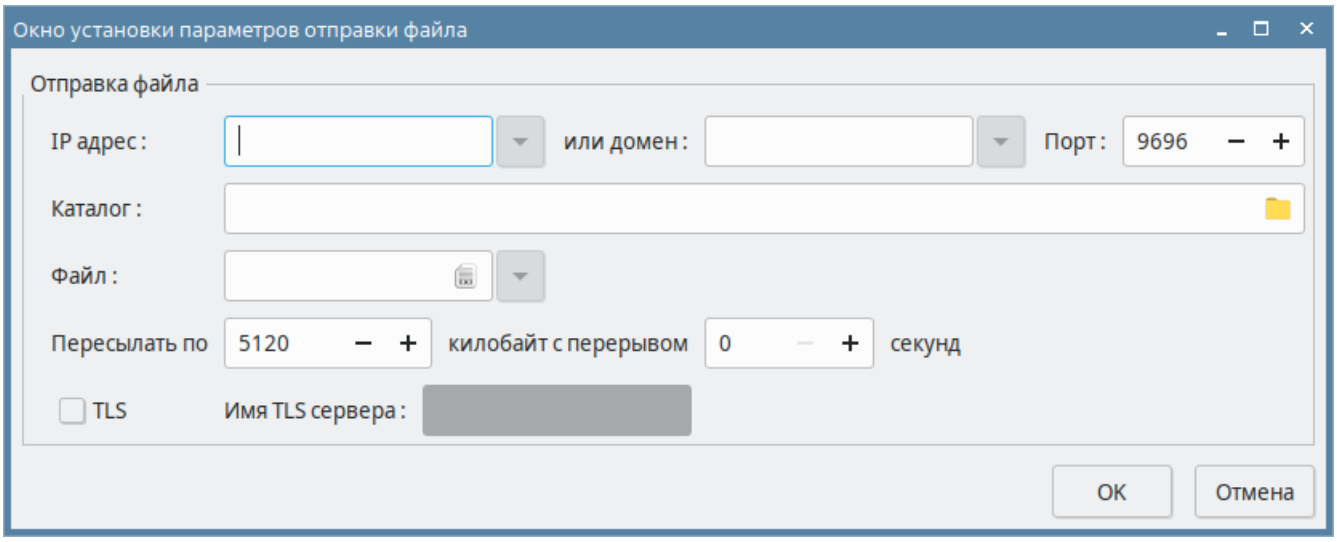

Рисунок 10. Отправка файла.

Отправка файла выполняется по сети на указанный IP адрес или на заданное доменное имя (поле «домен»). Номер порта нужно обязательно записать в поле «Порт».

Отправляемый файл задается в поле «Файл», а каталог его размещения в поле «Каталог». Для упрощения заполнения этих полей в конце строки ввода предусмотрена «иконка», нажатие на которую выдаст диалог заполнения каталога или файла.

Файл передается по сети блоками, заданными в килобайтах. Для уменьшения нагрузки на сеть предусмотрена возможность после передачи каждого блока делать перерыва, заданные в секундах.

Опция «TLS» позволяет выполнить передачу файла в защищенном виде на принимающий сервер. На принимающем сервере также должна быть включена опция «TLS». В поле «Имя TLS сервера» записывается доменное имя сервера из его сертификата (поле DNS).

Тип действия «Копирование файла».

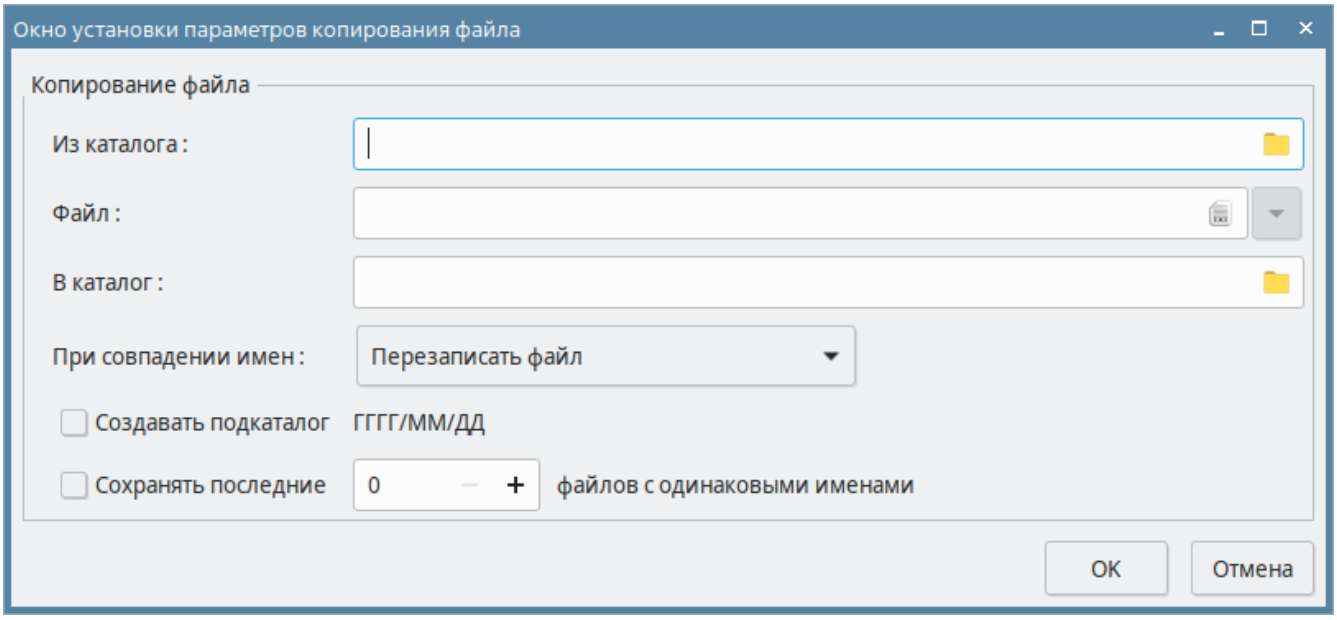

Рисунок 11. Копирование файла.

Копирование файла осуществляется из одного каталога в другой. Диалог предусматривает соответствующие поля их заполнения.

Если в каталоге назначения уже присутствует файл с таким названием, то возможны 3 варианта действий Программы:

- «Перезаписать файл»;
- «Сохранить с добавлением номера (*~N.*)»;
- «Выдать сообщение об ошибке».

Включение опции «Создавать подкаталог ГГГГ/ММ/ДД» позволяет копировать файл в подкаталог с текущей датой в момент его копирования.

Опция «Сохранять последние N файлов с одинаковыми именами» предоставляет возможность сохранять в одном каталоге не более N последних резервных копий. С оригинальным именем файла всегда будет последняя резервная копия. Все предыдущие имена файлов резервных копий получат порядковый номер в виде (*~n).

Тип действия «Запуск программы».

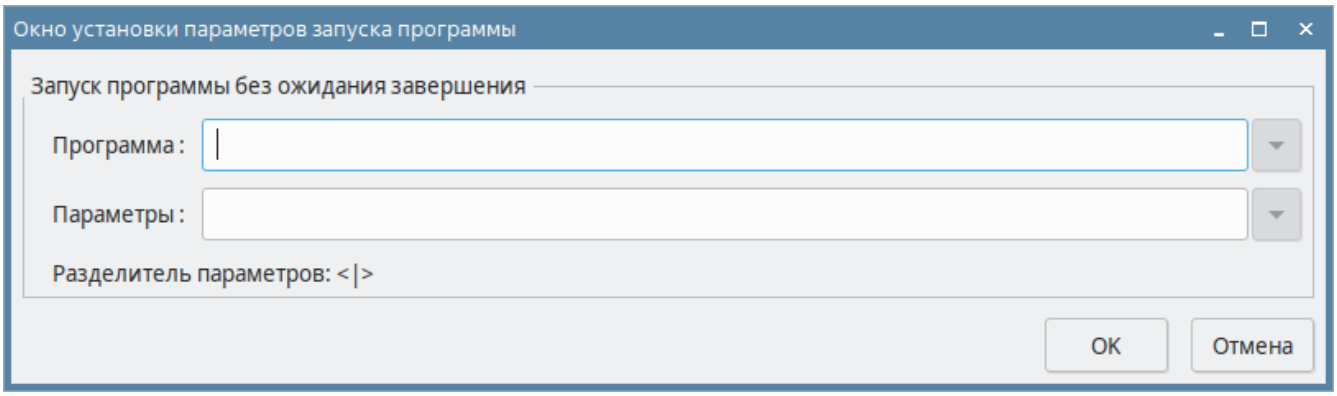

Рисунок 12. Запуск программы.

Данное действие дает возможность запуска внешней программы (например, gedit) с указанием передаваемых параметров. Если параметров несколько, то их необходимо разделить специальными тремя символами (<|>). Например, file1.txt<|> file2.txt<|> file3.txt.

Данное действие не ждет завершения запущенной программы.

Тип действия «Наличие файла».

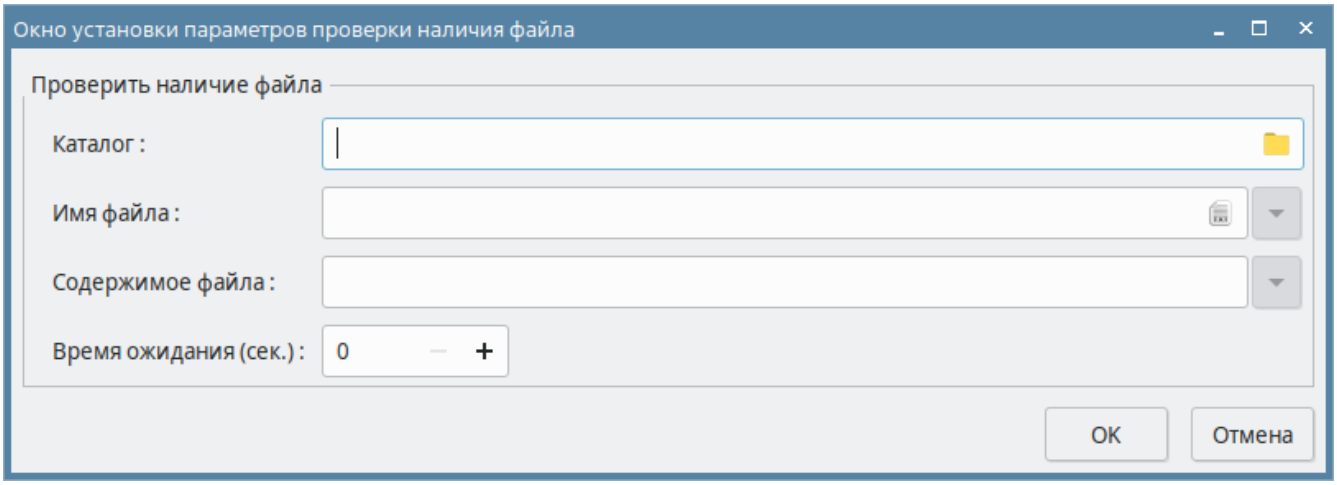

Рисунок 13. Наличие файла.

Данное действие проверяет наличие указанного фала в заданном каталоге. Наличие файла ожидается в течение времени, заданного в поле «Время ожидания (сек.)».

Поле «Содержимое файла» позволяет проверить наличие в файле заданной строки. Сравнение строк выполняется без учета регистра. Если его не заполнить, то будет проверяться только наличие файла в каталоге.

Заполненный список действий может выглядеть так, как это показано на следующей картинке.

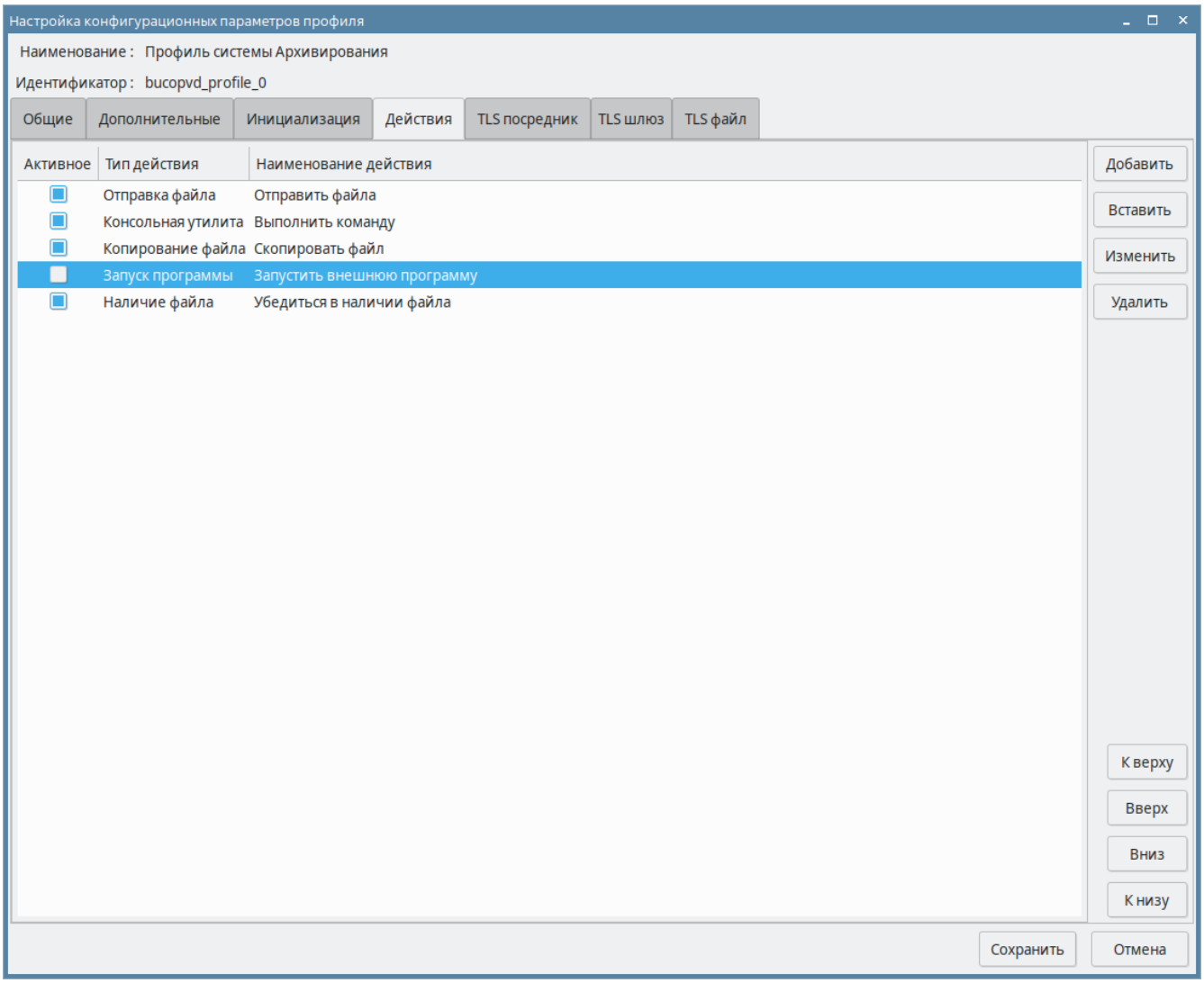

Рисунок 14. Список действий.

Столбец «Активное» позволяет включать и выключать действия с помощью «мыши». Выключенные действия могут присутствовать в списке, но не выполняться.

3.1.3.5. TLS ПОСРЕДНИК

Для настройки TLS посредника (прокси) нужно открыть закладку «TLS посредник».

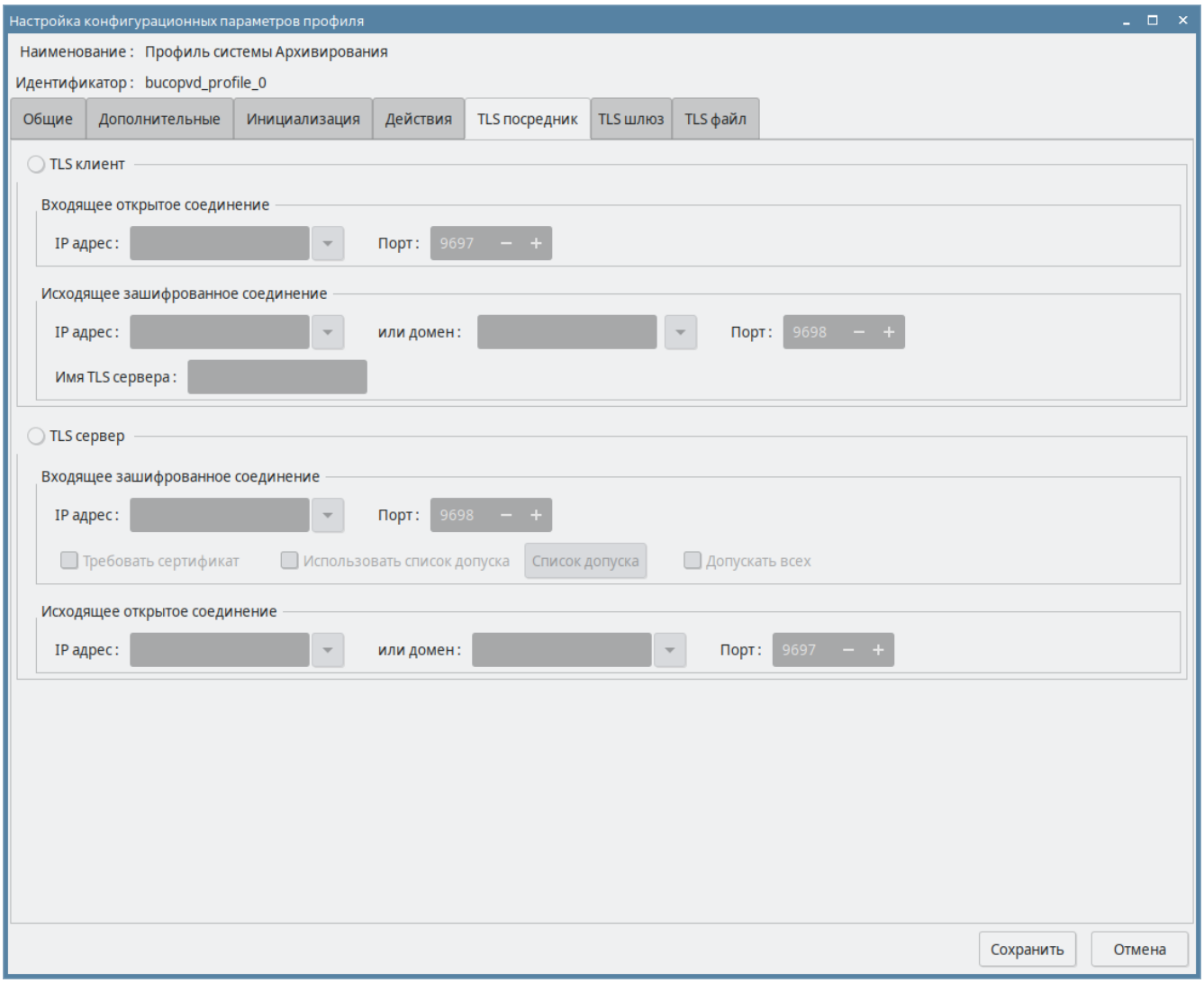

Рисунок 15. TLS посредник.

Данная закладка позволяет настроить как клиентскую часть TLS посредника (прокси), так и серверную часть. Установка клиентской части и серверной предусматривается на разных компьютерах.

Для настройки клиентской части нужно выбрать раздел «TLS клиент».

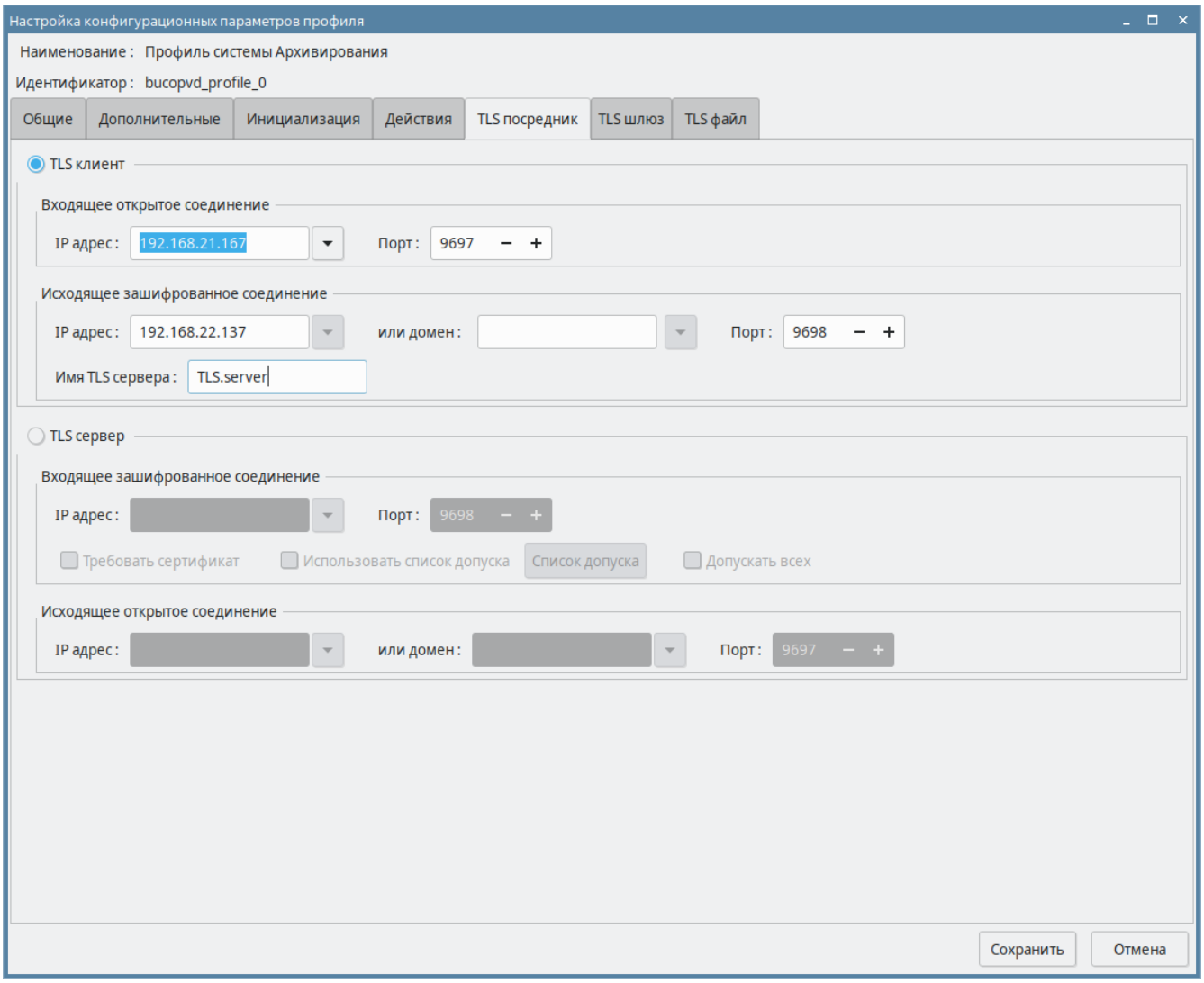

Рисунок 16. TLS клиент.

В разделе «Входящее открытое соединение» нужно задать IP адрес и номер порта, на котором клиентская часть будет ожидать открытое сетевое соединение от клиента по TCP протоколу.

В разделе «Исходящее зашифрованное соединение» задаются параметры серверной части TLS сервера: IP адрес или доменное имя, номер порта и имя TLS сервера (должно совпадать с полем DNS в сертификате сервера).

Настройка серверной части осуществляется аналогично на другом сервере.

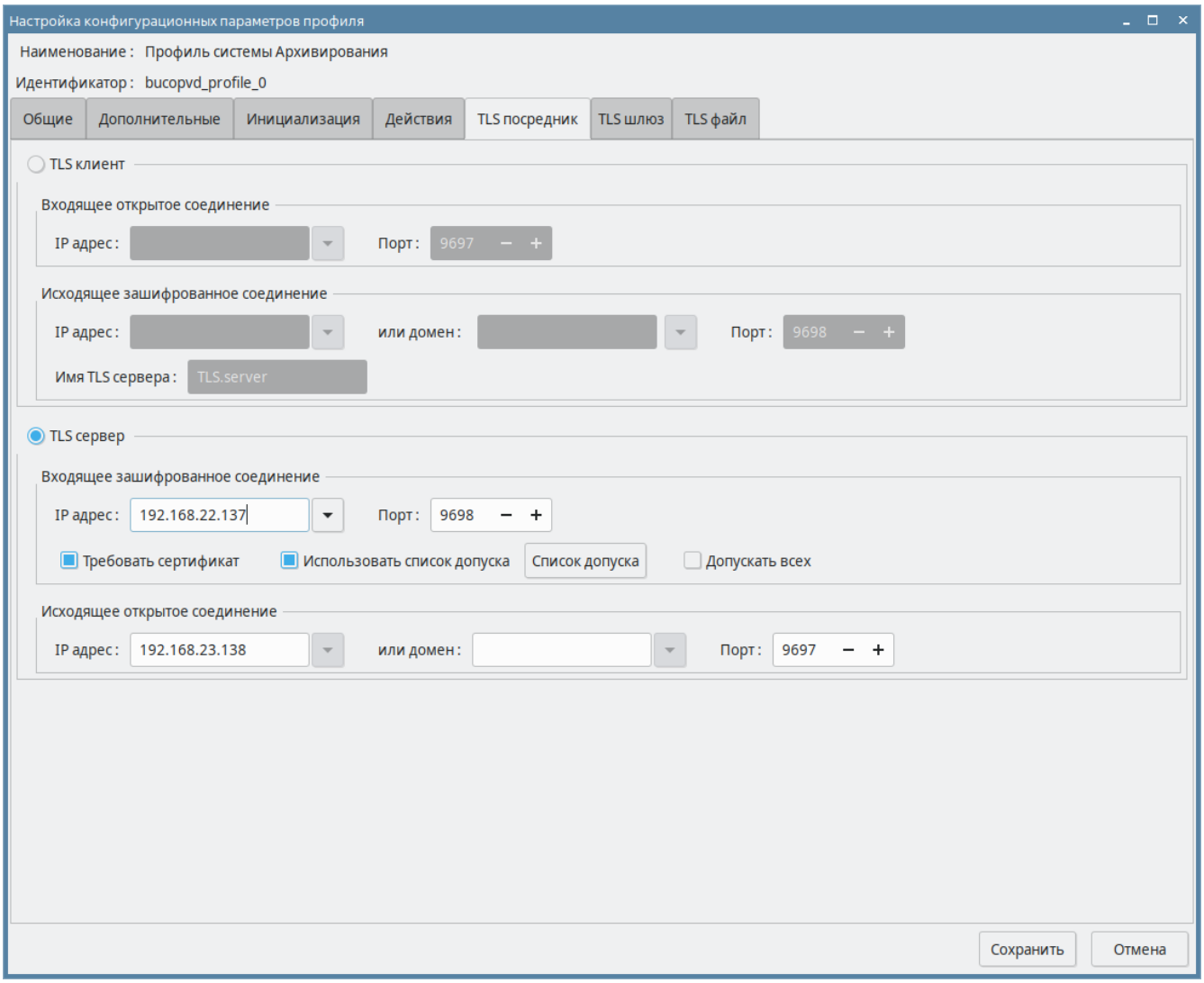

Рисунок 17. TLS сервер

В разделе «Входящее зашифрованное соединение» задаются IP адрес и номер порта, на котором TLS сервер будет ожидать входящее зашифрованное TLS соединение от TLS клиента. После его получения TLS сервер должен будет установить открытое TCP соединение с компьютером, имеющем IP адрес или доменное имя и номер порта, заданные в разделе «Исходящее открытое соединение».

Без установленного параметра «Требовать сертификат» TLS сервер будет принимать как соединения от клиентов с сертификатами, так и соединения от анонимных TLS клиентов. Если включить этот параметр («Требовать сертификат»), то TLS сервер будет принимать соединения только от клиентов с сертификатами.

Если необходимо ограничить список TLS клиентов с сертификатами, то можно установить параметр «Использовать список допуска». Кнопка «Список допуска» обеспечивает задание этого

списка. Включение опции «Допускать всех» позволяет иметь список допуска и принимать всех TLS клиентов с сертификатами.

После нажатия на кнопку «Список допуска» будет выдан следующий диалог.

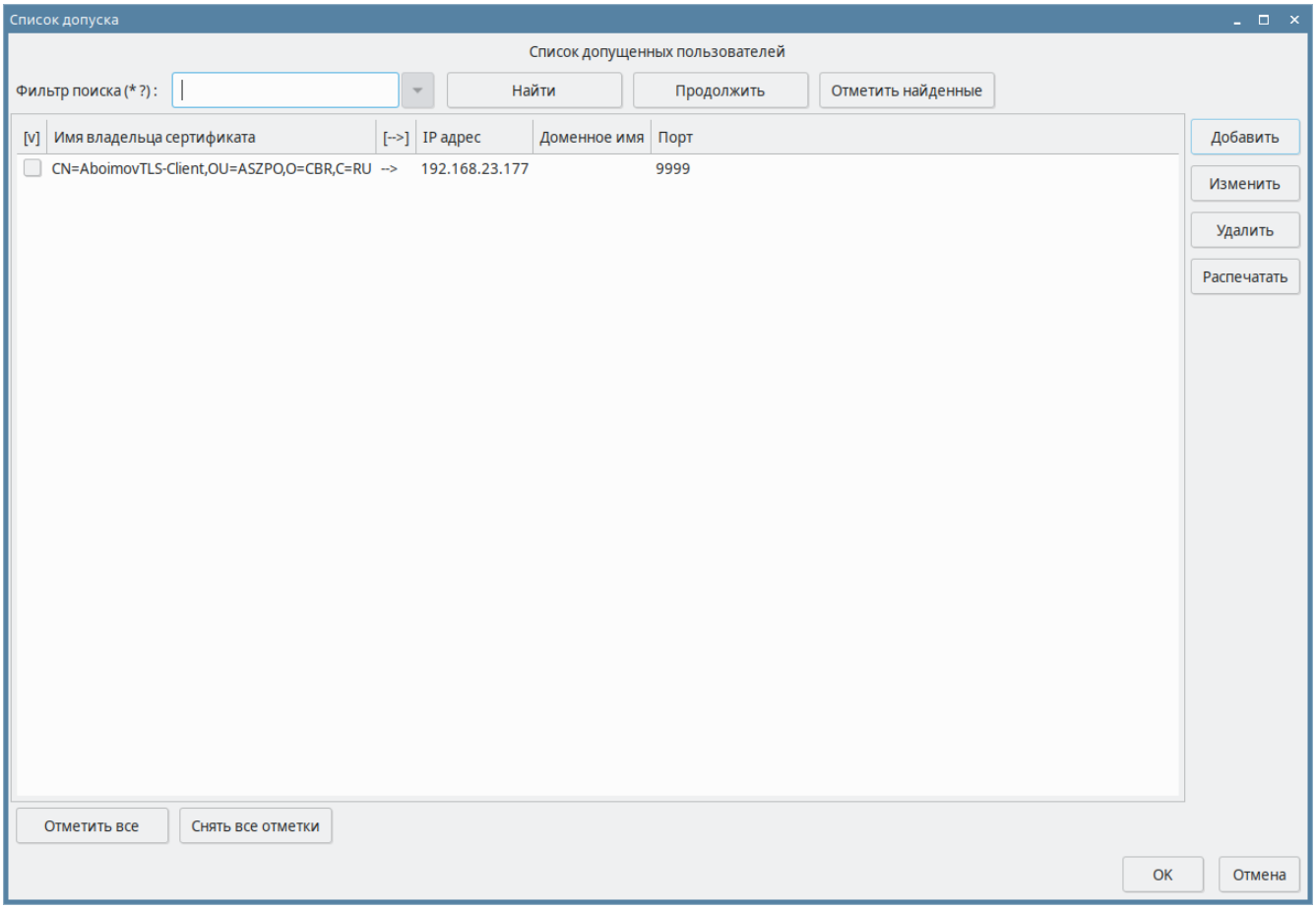

Рисунок 18. Список допущенных пользователей.

Данный диалог позволяет добавлять, удалять, изменять и распечатывать в текстовый файл список допущенных сертификатов.

По списку можно выполнять поиск допущенных пользователей по именам владельцев сертификатов. Для поиска можно задавать маску поиска, которая предусматривает специальные символы (символ «*» - для замены любой последовательности символов и символ «?» – для замены одного символа). Например, маска (CN=a*) найдет все имена сертификатов, начинающиеся на букву «а». Верхний или нижний регистр в этом поиске значения не имеет. Поиск осуществляется с помощью нажатия кнопки «Найти», а кнопка «Продолжить» предусмотрена для продолжения поиска.

Удалять из списка можно только строки, отмеченные «галочкой» в столбце [v]. Эти отметки можно делать «мышкой» или с помощью нажатия кнопок «Отметить все» или «Снять

все отметки». Дополнительно можно использовать кнопку «Отметить найденные» при заданной маске поиска.

Нажмем кнопку «Добавить».

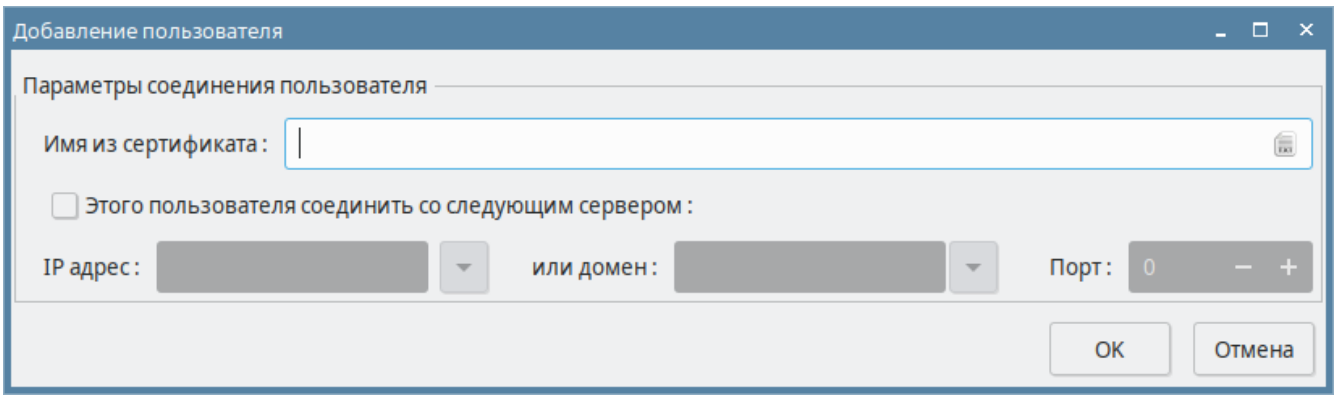

Рисунок 19. Добавление пользователя.

Поле «Имя из сертификата» нужно заполнить именем владельца сертификата. Для упрощения предусмотрена «иконка» файла в конце строки ввода, которая выдает диалог поиска файла. Если выбрать файл с сертификатом в DER кодировке, то эта строка будет заполнена автоматически.

В TLS сервере предусмотрен механизм динамической переадресации входящих TLS клиентов в зависимости от их имен. Для включения этого механизма нужно включить опцию «Этого пользователя соединить со следующим сервером» и указать его IP адрес или доменное имя (поле «домен») и номер порта TCP соединения.

3.1.3.6. TLS шлюз

TLS шлюз предназначен для создания виртуальных частных сетей (VPN) на основе шифрования по TLS протоколу на 3 сетевом уровне, когда IP пакеты от клиента к серверу передаются по зашифрованному TLS протоколу.

Настройка TLS шлюза должна выполняться только под Администратором (root), так как Linux позволяет работать на уровне IP пакетов только под управлением Администратора (root). Программа предусматривает запуск конфигурации в этом режиме с помощью меню «Конфигурация ПРК (Админ.)».

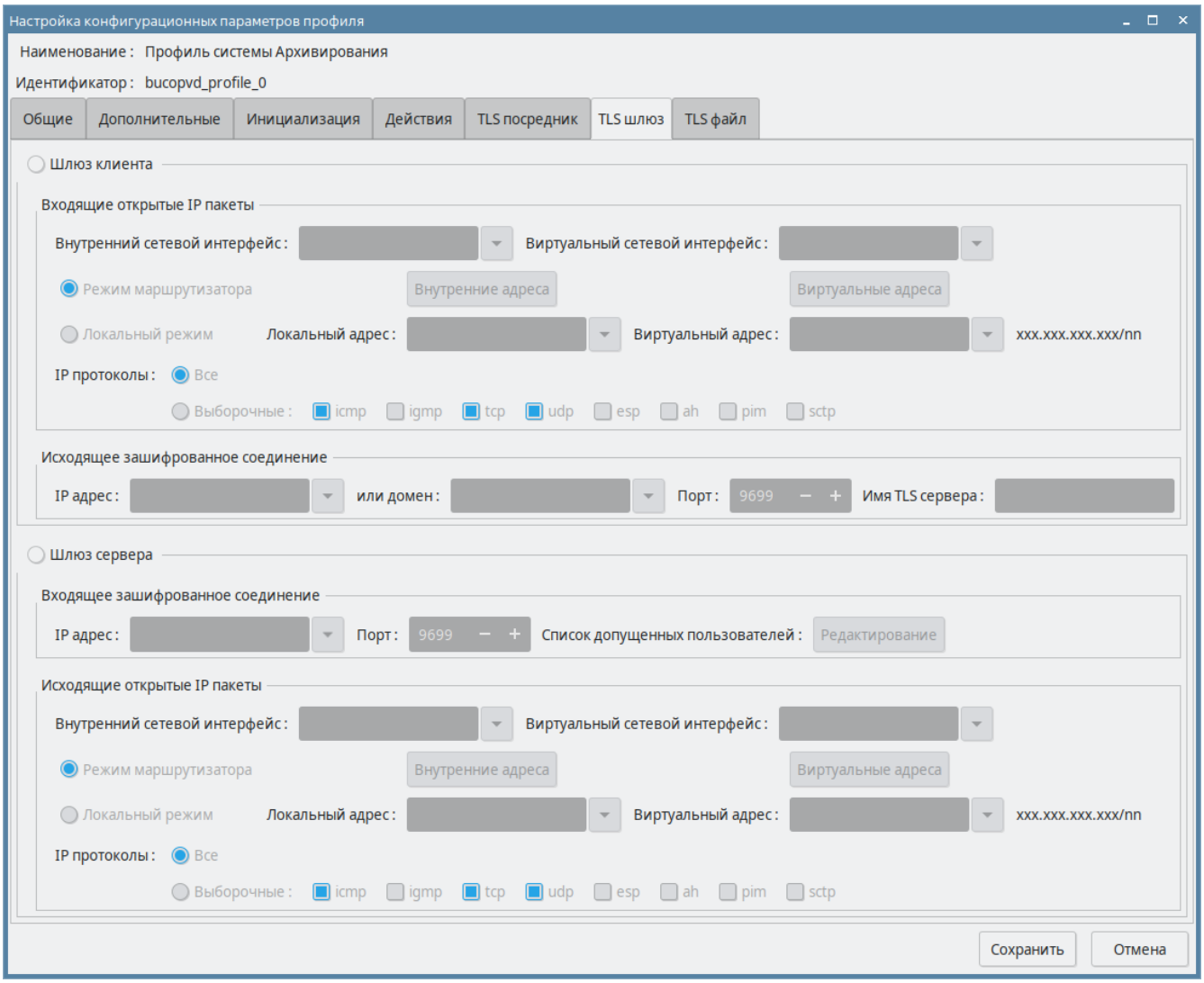

Рисунок 20. TLS шлюз.

Рассмотрим закладку настройки TLS шлюза. Она состоит из раздела настроек «Шлюза клиента» и раздела настроек «Шлюза сервера». Данные разделы предусматривают настройки на разных компьютерах (серверах).

TLS шлюз можно настроить для работы как в режиме маршрутизатора, так и локальном режиме работы. Совмещать на одном компьютере режим маршрутизатора и локальный режим нельзя.

TLS шлюз поддерживает передачу через VPN как всех IP протоколов, так и выборочных IP протоколов (ismp, igmp, tcp, udp, esp, ah, pim, sctp).

Параметр «IP протоколы» позволяет ограничить перечень пропускаемых через шлюз IP пакетов. Установка этого параметра в режим «Все» обеспечивает снятие всех ограничений, но если установить его в режим «Выборочные», то шлюз будет пропускать только IP пакеты только

тех протоколов, которые отмечены «галочкой». По умолчанию программа предлагает пропускать только ICMP, TCP и UDP.

Для настройки клиентской части шлюза в режиме маршрутизатора нужно включить раздел «Шлюз клиента» и выбрать параметр «Режим маршрутизатора».

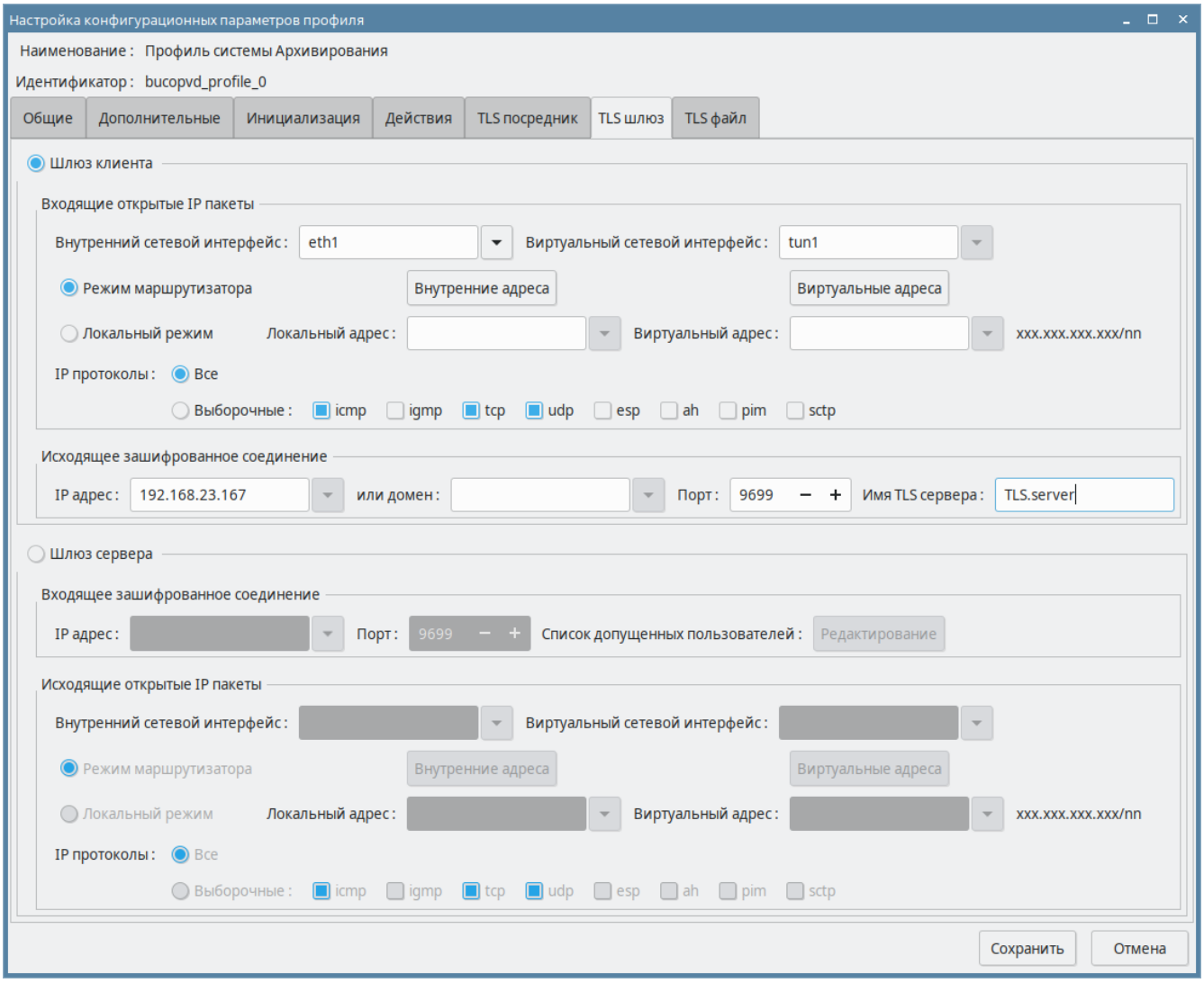

Рисунок 21. Шлюз клиента в режиме маршрутизатора.

Нужно обязательно задать «Внутренний сетевой интерфейс» (например, eth0), к которому подключается внутренняя защищаемая подсеть, и выбрать произвольное имя «Виртуального сетевой интерфейса» (например, tun1).

ВАЖНОЕ ПРИМЕЧАНИЕ! Имена виртуальных сетевых интерфейсов должны отличаться от виртуальных сетевых интерфейсов других клиентских шлюзов (например, tun2, tun3, …), подключающихся к одному серверному шлюзу, так как «Шлюз сервера» будет для каждого клиента создавать виртуальный сетевой интерфейс типа TUN. Если у двух клиентских

шлюзов будет одинаковое имя виртуального сетевого интерфейса (например, tun3), то серверный шлюз затрет предыдущий интерфейс при создании нового.

Задать список внутренних защищаемых адресов можно нажав на кнопку «Внутренние адреса».

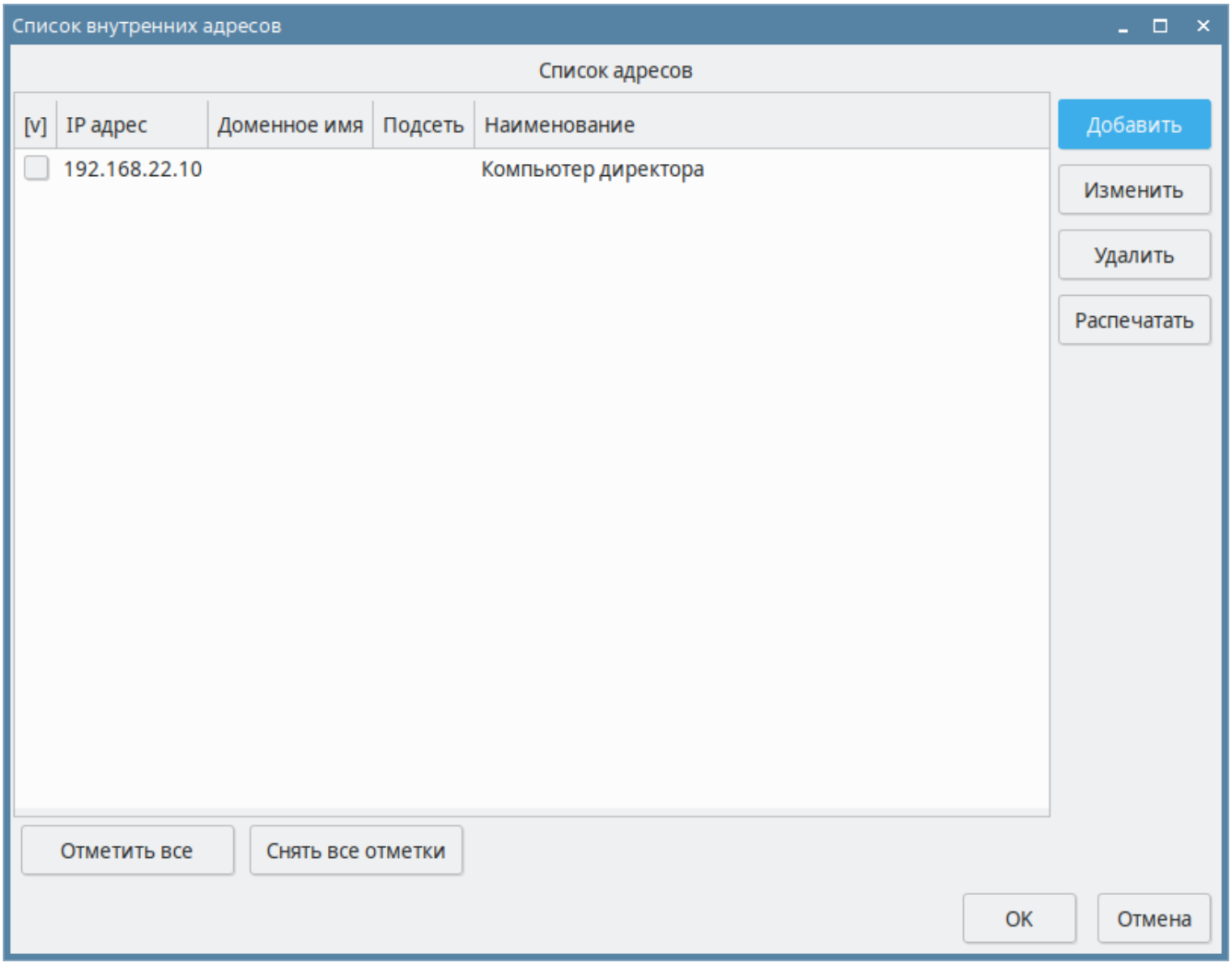

Рисунок 22. Список внутренних адресов.

Данный диалог позволяет добавлять, удалять, изменять и распечатывать в текстовый файл список внутренних адресов.

Удалять из списка можно только строки, отмеченные «галочкой» в столбце [v]. Эти отметки можно делать «мышкой» или с помощью нажатия кнопок «Отметить все» или «Снять все отметки».

После нажатия кнопки «Добавить» будет выдан следующий диалог.

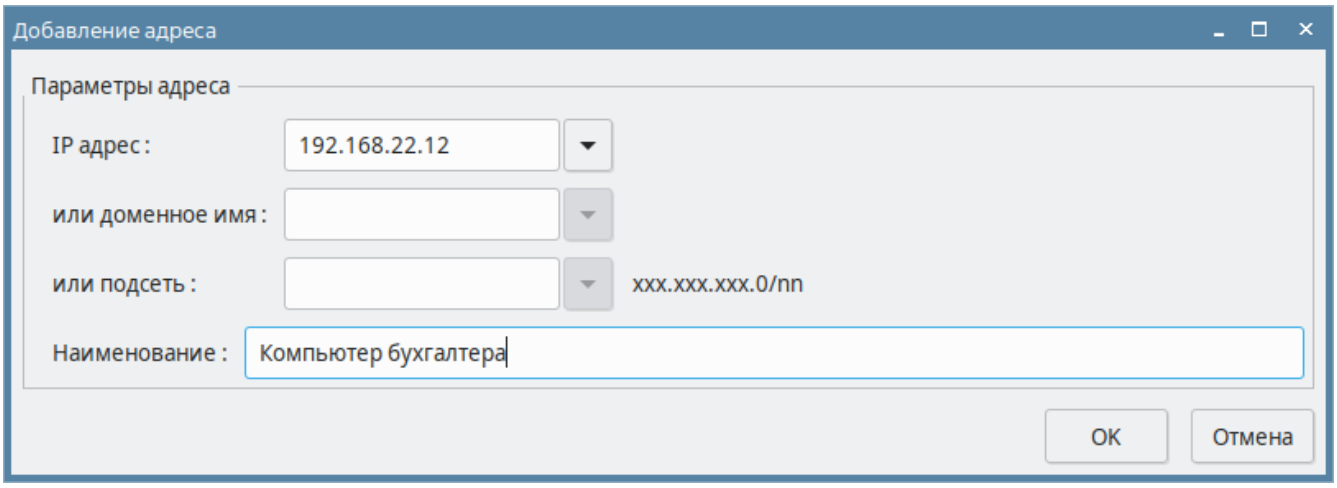

Рисунок 23. Добавление адреса.

Нужно задать или IP адрес компьютера или его доменное имя.

Возможно задание всей защищаемой подсети в формате xxx.xxx.0.0/16 (например, 192.168.22.0/24). В этом случае все компьютеры из этой подсети будут подключены к VPN.

«Список внутренних адресов» поддерживает как несколько адресов, так и несколько подсетей в одном списке.

«Наименование» добавляемого адреса имеет только информационное значение.

ВАЖНОЕ ПРИМЕЧАНИЕ! Если к одному серверному шлюзу подключаются несколько клиентских шлюзов, то их подсети не должны совпадать и пересекаться. Например, нельзя допускать, чтобы у двух клиентов были подсети 198.168.1.0/24, так как в этом случае серверный шлюз не будет знать какому клиенту отправить IP пакет с адресом получателя 198.168.1.3.

После завершения создания списка внутренних адресов нужно обязательно заполнить список виртуальных адресов. Для этого нажмите кнопку «Виртуальные адреса».

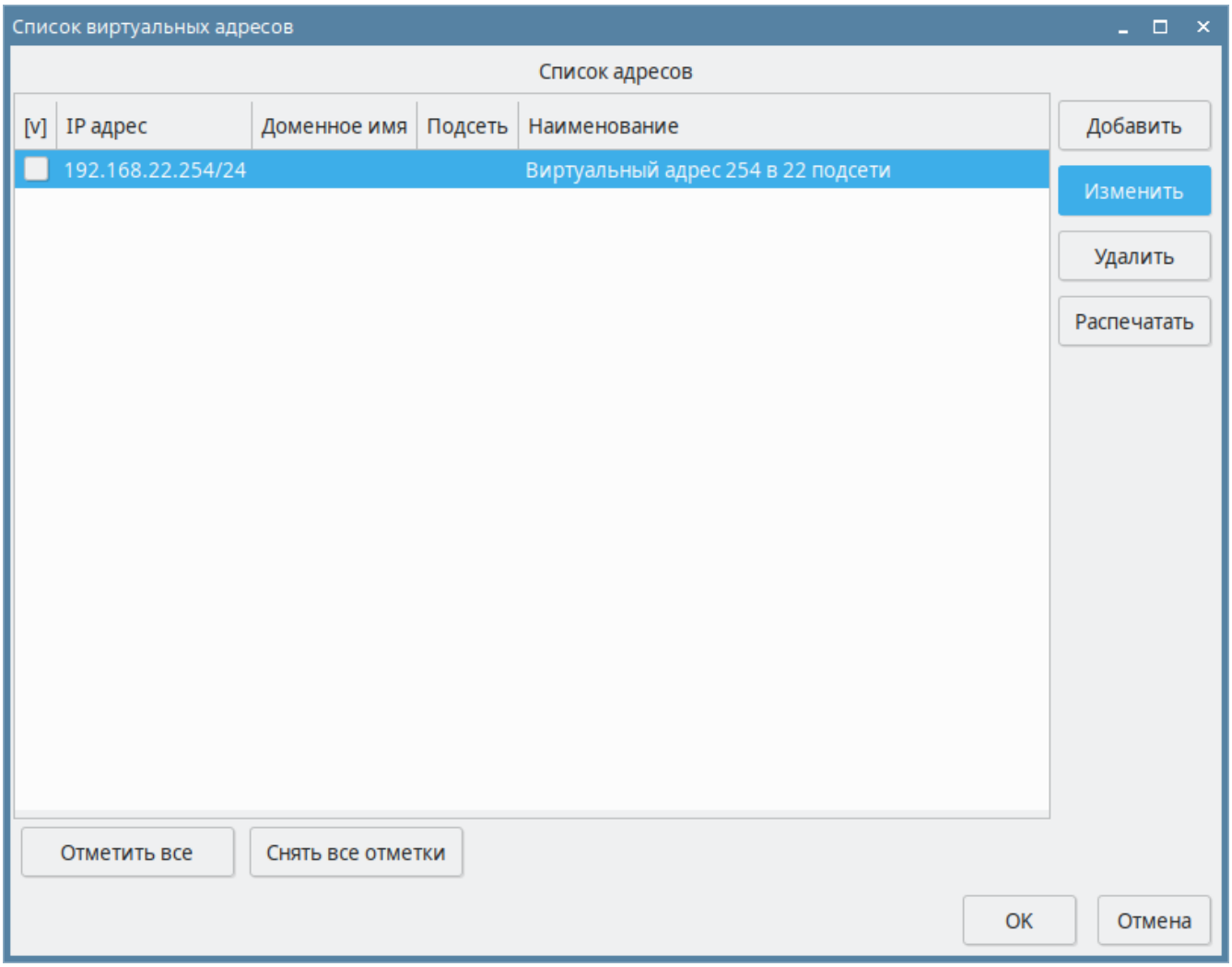

Рисунок 24. Список виртуальных адресов.

Данный диалог позволяет добавлять, удалять, изменять и распечатывать в текстовый файл список внутренних адресов.

Удалять из списка можно только строки, отмеченные «галочкой» в столбце [v]. Эти отметки можно делать «мышкой» или с помощью нажатия кнопок «Отметить все» или «Снять все отметки».

После нажатия кнопки «Добавить» будет выдан следующий диалог.

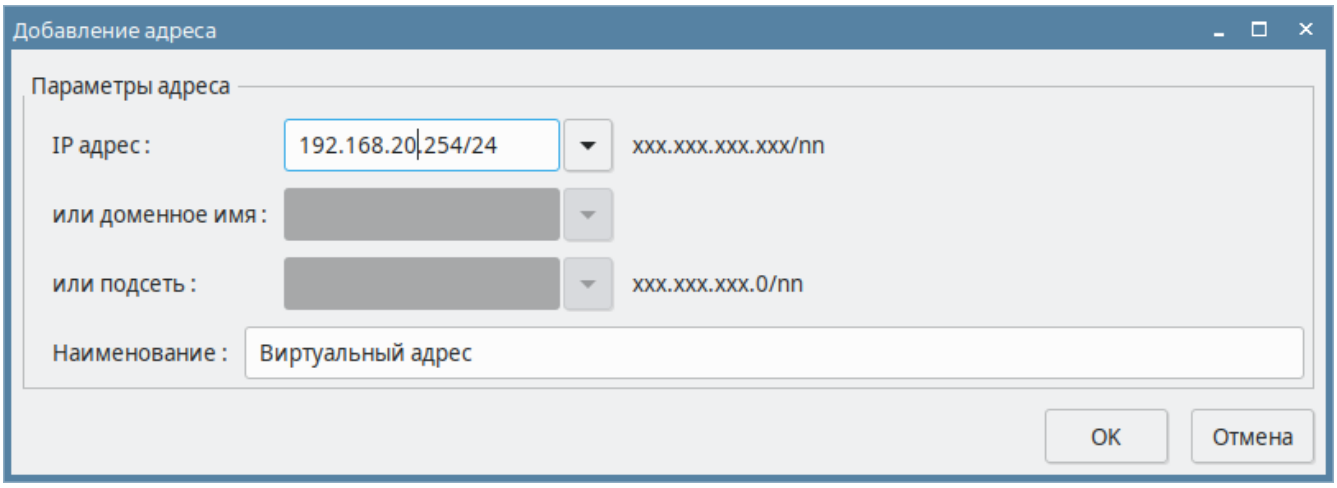

Рисунок 25. Добавление виртуального адреса.

В данном диалоге поля «доменное имя» и «подсеть» не доступны для заполнения.

В поле «IP адрес» нужно указать виртуальный (например, 254) адрес подсети, которая используется в «Списке внутренних адресов». Виртуальный адрес не должен совпадать ни с одним реальным внутренним адресом этой подсети, так как работа с ним будет не возможна.

«Наименование» добавляемого адреса имеет только информационное значение.

ВАЖНОЕ ПРИМЕЧАНИЕ! Если в списке внутренних адресов присутствуют несколько подсетей или адреса из нескольких подсетей, то нужно обязательно добавить в список виртуальных адресов строго по одному виртуальному адресу для каждой подсети. Например, если в список внутренних адресов состоит из:

192.168.22.10, 192.168.22.12, 192.168.23.5, 192.192.0.0/16,

то в списке виртуальных адресов должны присутствовать следующие адреса:

192.168.22.254/24, 192.168.23.254/24, 192.192.254.254/16

ВАЖНОЕ ПРИМЕЧАНИЕ! Все компьютеры, которые будут работать с VPN через «Клиентский шлюз», должны задать в качестве шлюза (маршрутизатора) реальный адрес внутреннего сетевого интерфейса (например, eth0) сервера «Клиентского шлюза».

В разделе «Исходящее зашифрованное соединение» задаются параметры серверной части TLS сервера: IP адрес или доменное имя, номер порта и имя TLS сервера (должно совпадать с полем DNS в сертификате сервера).

Для настройки клиентской части шлюза в локальном режиме нужно включить раздел «Шлюз клиента» и выбрать параметр «Локальный режим».

ВАЖНОЕ ПРИМЕЧАНИЕ! TLS шлюз не может одновременно работать как в локальном режиме, так и в режиме маршрутизатора.

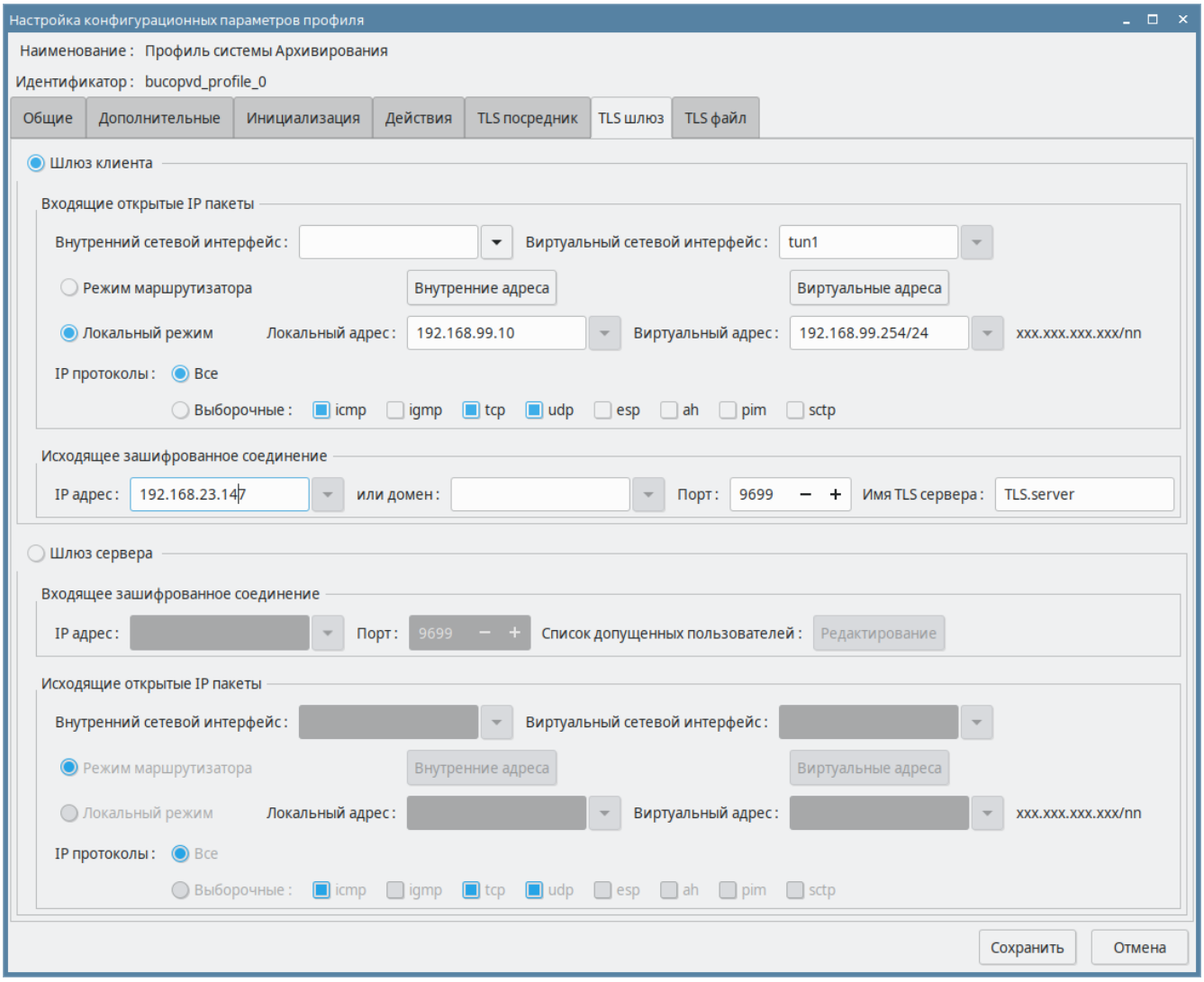

Рисунок 26. Локальный режим клиентского шлюза

Поле «Внутренний сетевой интерфейс» можно не заполнять.

Для «Виртуального сетевого интерфейса» нужно ввести произвольное короткое имя (например, tun1), которое не должно присутствовать у других клиентских шлюзов.

В локальном режиме необходимо заполнить только один локальный адрес и один виртуальный адрес, выбрав любую произвольную подсеть, которой нет в реальной сети. Например, если не существует реальной 99 подсети, то локальный адрес будет 198.168.99.10, а виртуальный адрес 198.168.99.254/24.

В разделе «Исходящее зашифрованное соединение» задаются параметры серверной части TLS сервера: IP адрес или доменное имя, номер порта и имя TLS сервера (должно совпадать с полем DNS в сертификате сервера).

Для настройки серверной части шлюза нужно включить раздел «Шлюз сервера».

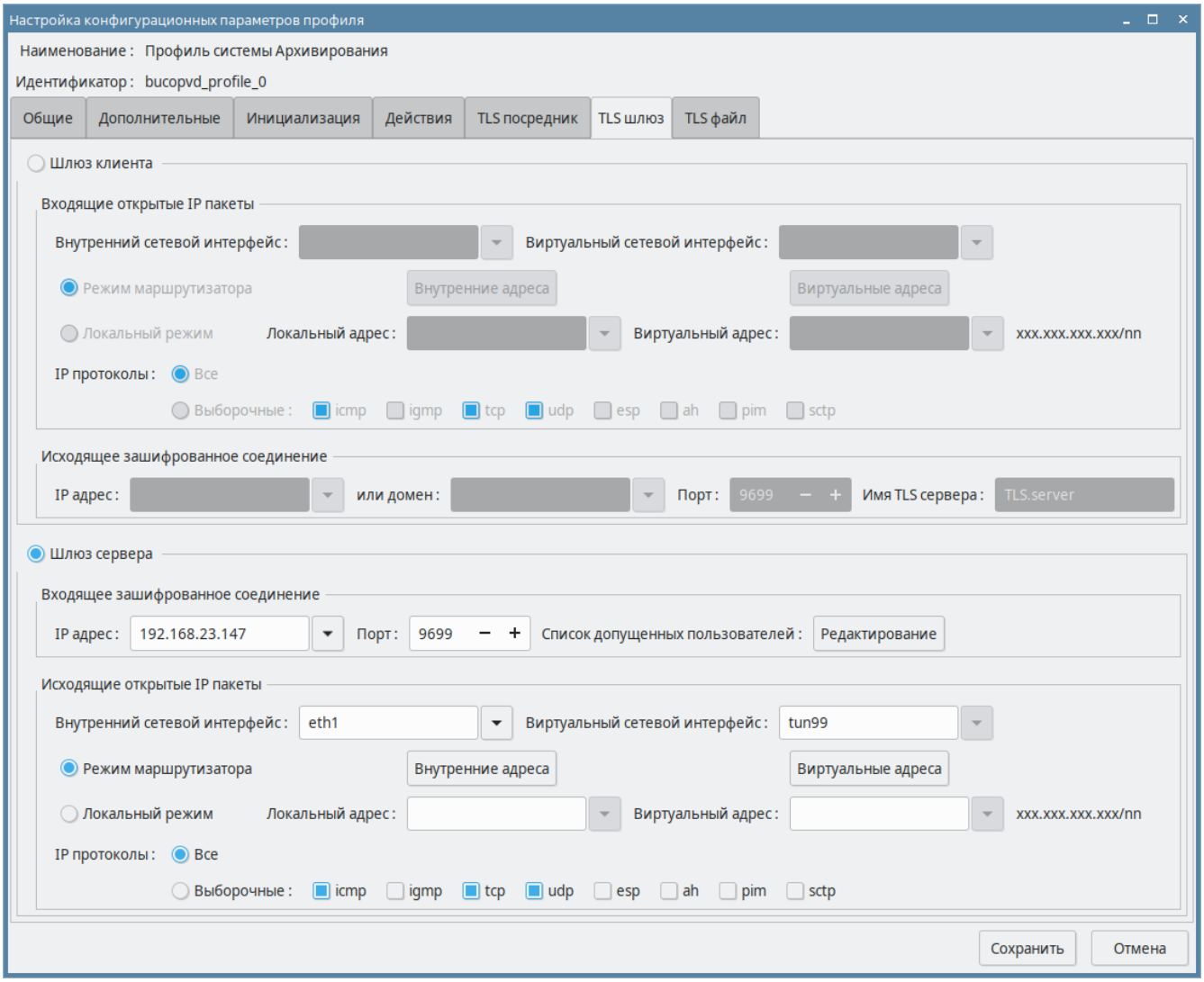

Рисунок 27. Шлюз сервера.

В разделе «Входящее зашифрованное соединение» задаются IP адрес и номер порта, на котором «Шлюз сервера» будет ожидать входящее зашифрованное TLS соединение от «Шлюзов клиента». Зашифрованные TLS соединение будут приниматься только от клиентов, имена сертификатов которых занесены в «Список допущенных пользователей».

Для формирования списка допущенных пользователей нужно нажать кнопку «Редактировать».

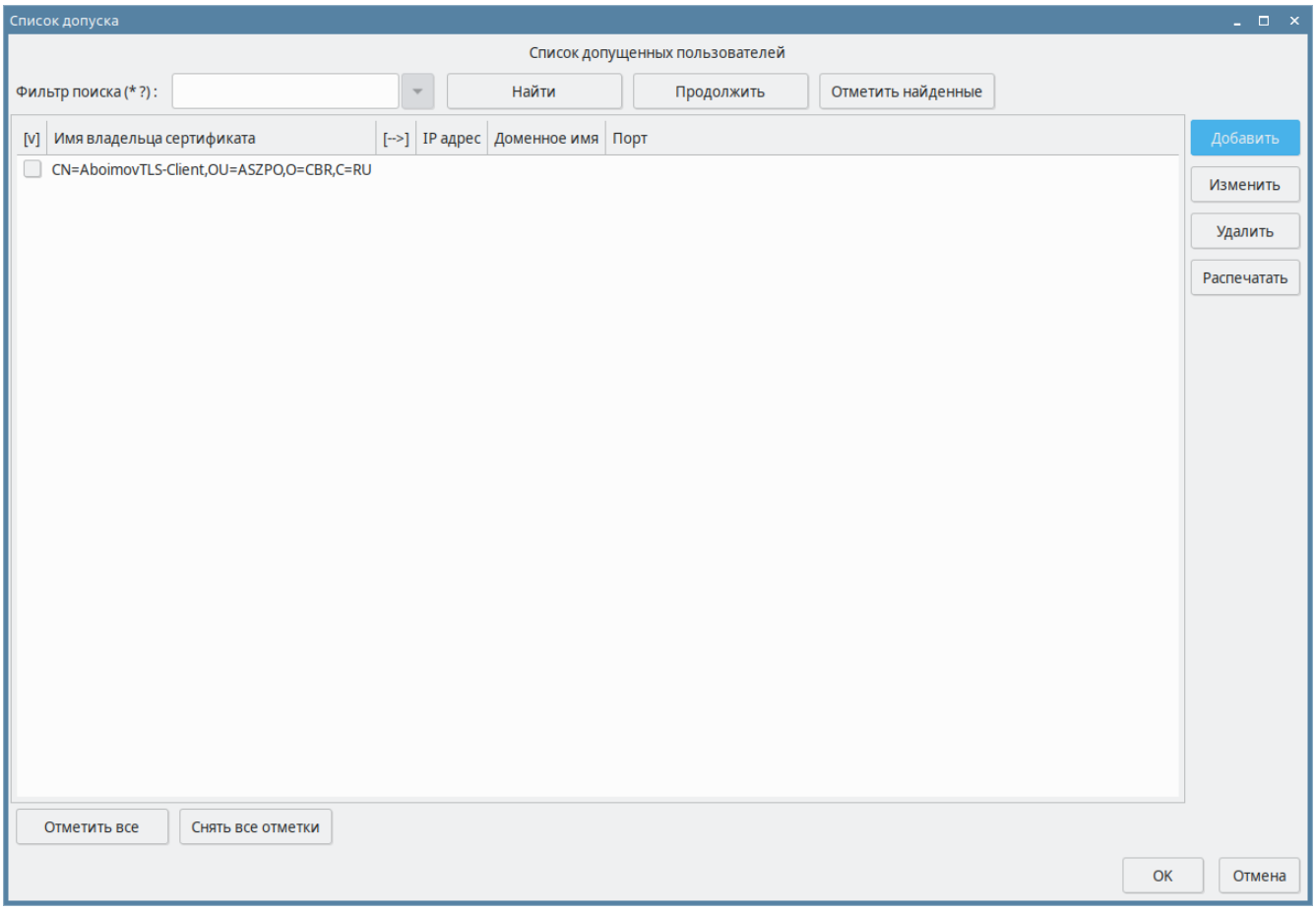

Рисунок 28. Список допуска.

Данный диалог позволяет добавлять, удалять, изменять и распечатывать в текстовый файл список допущенных сертификатов.

По списку можно выполнять поиск допущенных пользователей по именам владельцев сертификатов. Для поиска можно задавать маску поиска, которая предусматривает специальные символы (символ «*» - для замены любой последовательности символов и символ «?» – для замены одного символа). Например, маска (CN=a*) найдет все имена сертификатов, начинающиеся на букву «а». Верхний или нижний регистр в этом поиске значения не имеет. Поиск осуществляется с помощью нажатия кнопки «Найти», а кнопка «Продолжить» предусмотрена для продолжения поиска.

Удалять из списка можно только строки, отмеченные «галочкой» в столбце [v]. Эти отметки можно делать «мышкой» или с помощью нажатия кнопок «Отметить все» или «Снять все отметки». Дополнительно можно использовать кнопку «Отметить найденные» при заданной маске поиска.

Нажмем кнопку «Добавить».

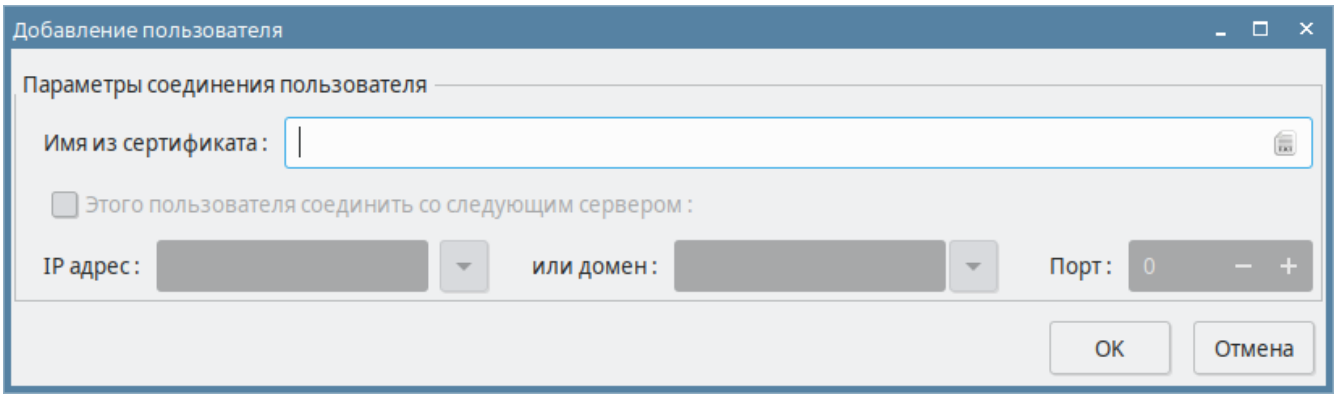

Рисунок 29. Добавление пользователя.

Поле «Имя из сертификата» нужно заполнить именем владельца сертификата. Для упрощения предусмотрена «иконка» файла в конце строки ввода, которая выдает диалог поиска файла. Если выбрать файл с сертификатом в DER кодировке, то эта строка будет заполнена автоматически.

Остальные поля в этом диалоге заблокированы.

Для настройки «Шлюза сервера» для работы в режиме маршрутизатора необходимо установить переключатель в «Режим маршрутизатора».

ВАЖНОЕ ПРИМЕЧАНИЕ! Списки «Внутренних адресов» и списки «Виртуальных адресов» формируются аналогично тому, как это было описано ранее для «Шлюза клиента».

Для настройки «Шлюза сервера» для работы в локальном режиме необходимо установить переключатель в «Локальный режим» и заполнить «Локальный адрес» и «виртуальный адрес» так, как это было ранее описано для «Шлюза клиента».

Поле «Внутренний сетевой интерфейс» заполнять не нужно, в поле «Виртуальный сетевой интерфейс» нужно обязательно записать короткое произвольное имя (например, tun99). Так будет называться дополнительный сетевой интерфейс на каждом «Шлюзе клиента», который будет подключен к этому серверному шлюзу.

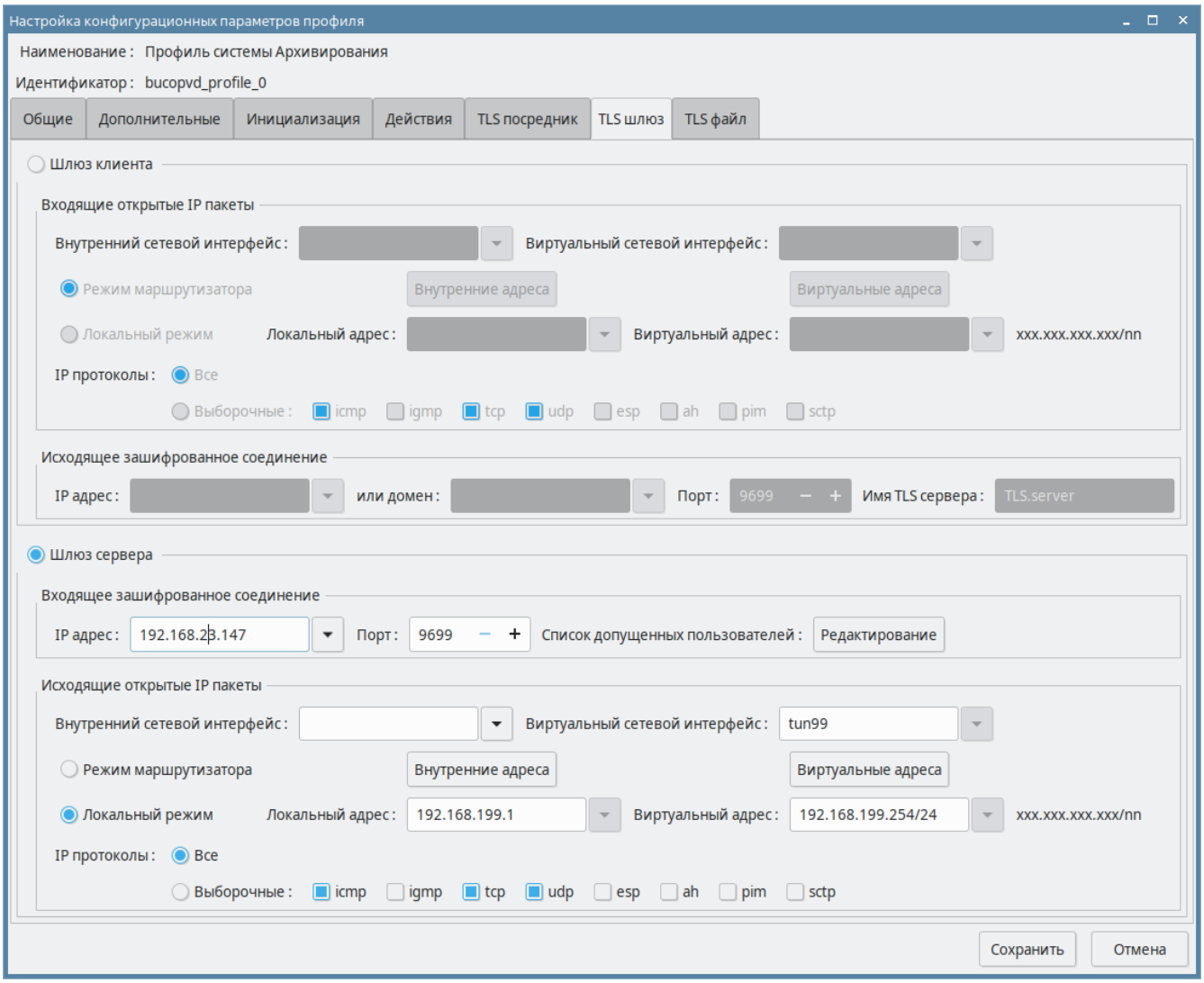

Рисунок 30. Шлюз сервера в локальном режиме.

ВАЖНОЕ ПРИМЕЧАНИЕ! Все компьютеры, которые будут работать с VPN через «Серверный шлюз», должны задать в качестве шлюза (маршрутизатора) реальный адрес внутреннего сетевого интерфейса (например, eth0) сервера «Серверного шлюза».

3.1.3.7. TLS ФАЙЛ

«TLS файл» предназначен для создания системы автоматического обмена файлами между сервером (Файл-сервер) и его клиентами (Файл-клиент) по протоколу TLS в подписанном виде.

ВАЖНОЕ ПРИМЕЧАНИЕ! «TLS файл» не передает файлы нулевой длины и файлы с расширением «.tmp».

Настройка как Файл-сервера, так и Файл-клиента выполняется на закладке «TLS файл».

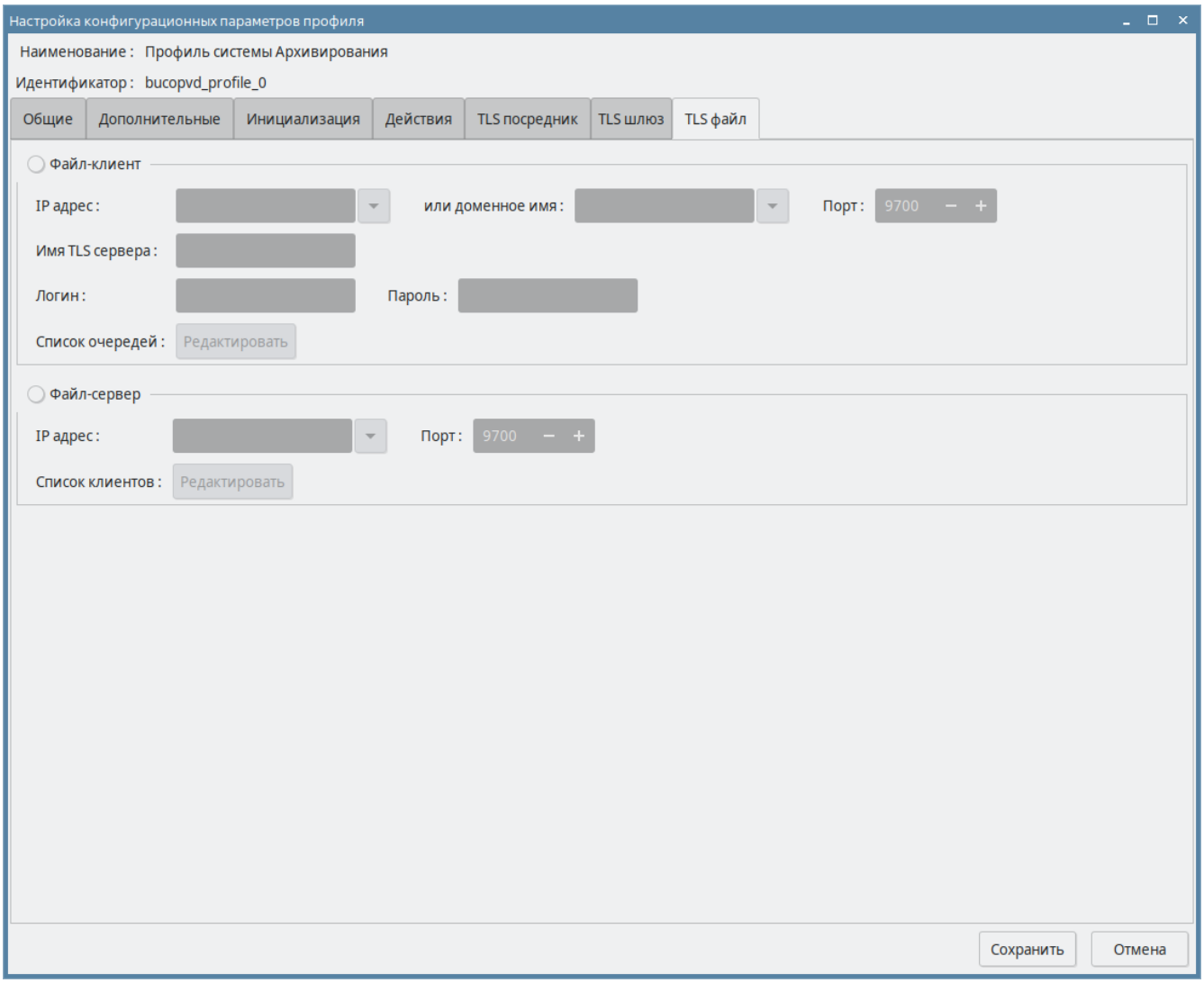

Рисунок 31. Настройки TLS файла.

Если настраивается программа у клиента, то нужно выбрать раздел «Файл-клиент».

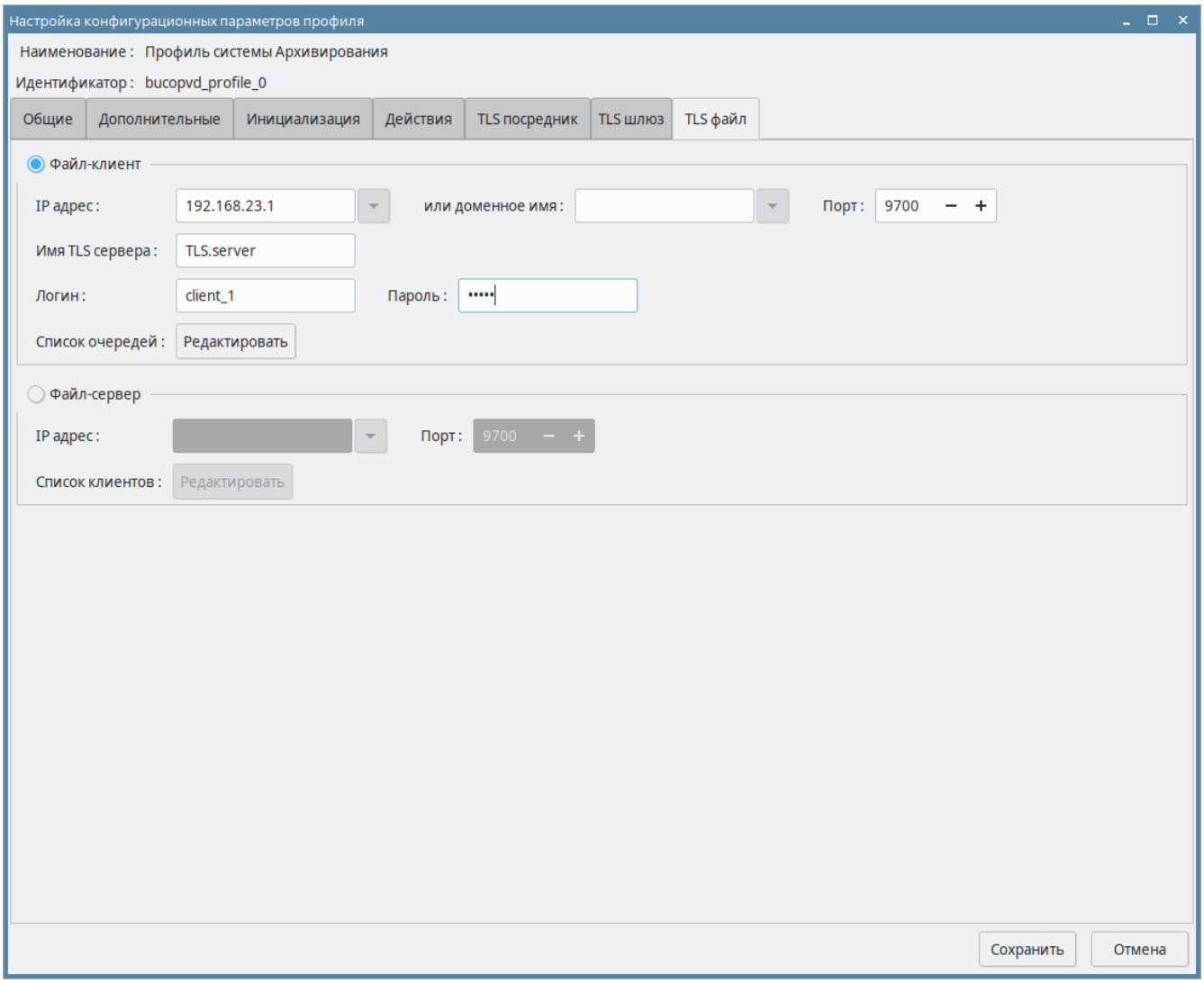

Рисунок 32. Настройка Файл-клиента.

Укажите «IP адрес» сервера (на котором установлена программа «Файл-сервер») или его доменное имя, а также укажите порт ожидания соединения.

В поле «Имя TLS сервера» нужно обязательно задать имя, которое совпадает с полем DNS в сертификате сервера.

Идентификатор «Логин» также является обязательным. Он представляет собой произвольную последовательность до 64 символов в нижнем регистре латинского алфавита с цифрами и символом подчерка «_». Пробелы не допускаются.

Параметр «Пароль» является необязательным. Но если он задается, то он должен совпадать с паролем этого пользователя на «Файл-сервере». Данный пароль может служить дополнительным усиление TLS аутентификации.

Список очередей является обязательным параметром для заполнения. Нажмите кнопку «Редактировать».

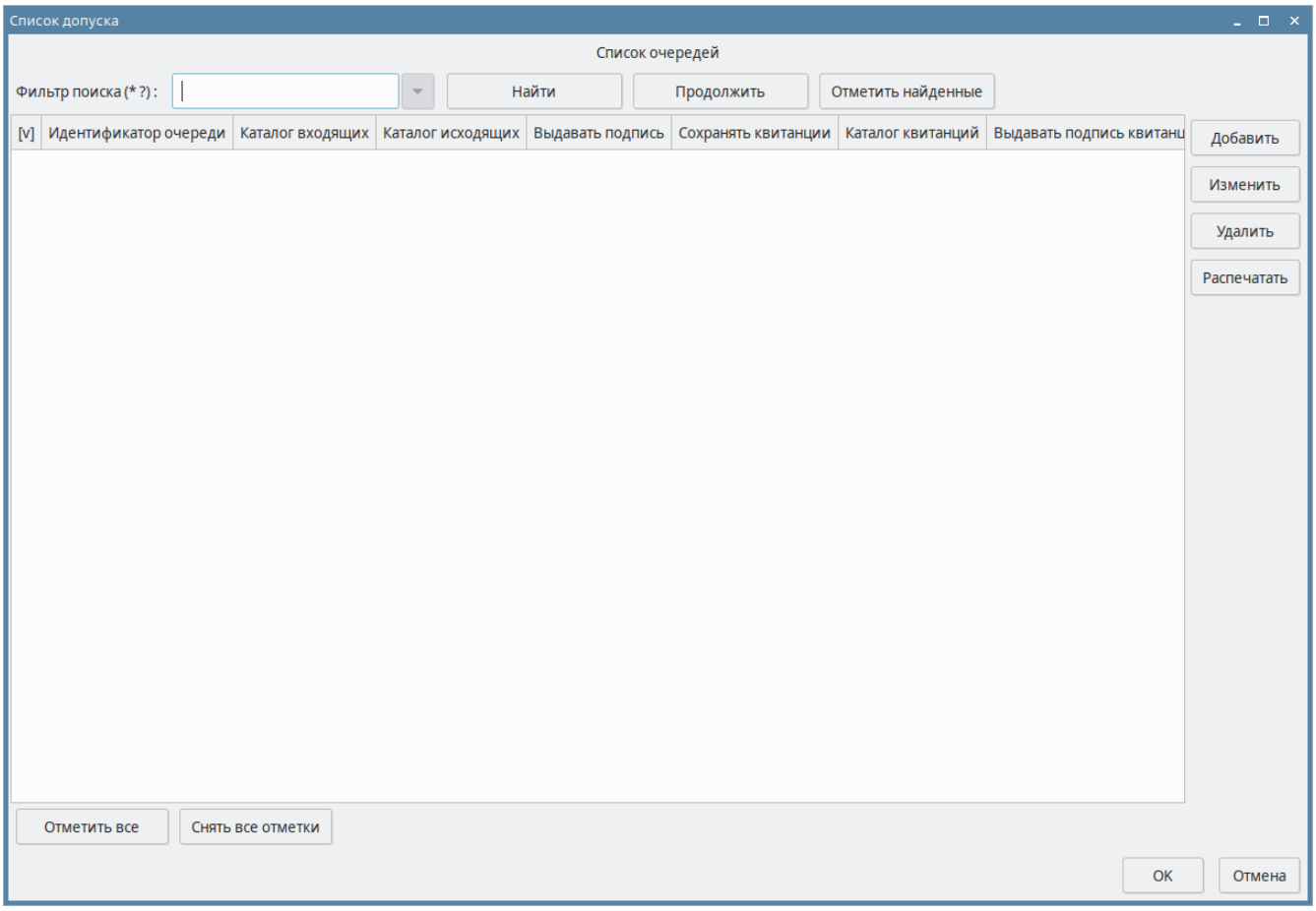

Рисунок 33. Список очередей клиента.

Данный диалог позволяет добавлять, изменять и удалять очереди в списке.

Для удаления записей необходимо выбрать их в специальной колонке [v] с помощью «мышки» или кнопки «Отметить все». Кнопка «Снять все отметки» отменяет все отметки в колонке [v].

Кнопка «Распечатать» обеспечивает распечатку списка очередей в текстовом виде.

Добавление очередей выполняется с помощью кнопки «Добавить».

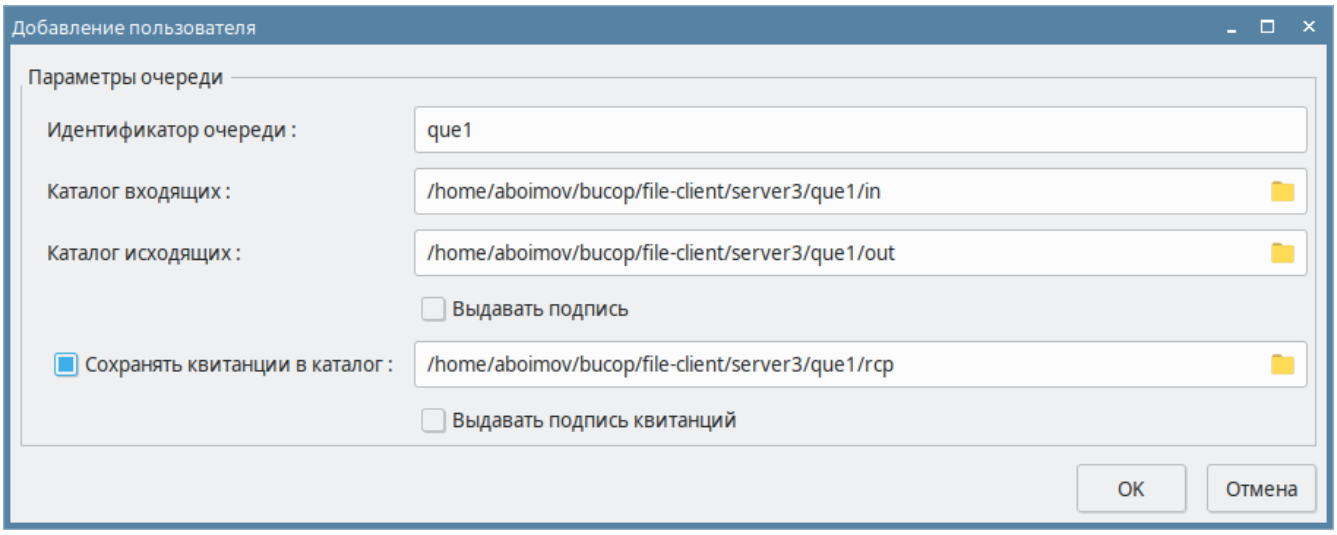

Рисунок 34. Добавление очереди.

«Идентификатор очереди» является обязательным для заполнения. Он представляет собой произвольную последовательность до 64 символов в нижнем регистре латинского алфавита с цифрами и символом подчерка «_». Пробелы не допускаются.

Дополнительно к идентификатору очереди нужно обязательно задать каталог для сохранения входящих файлов и каталог исходящих файлов, из которого программа будет отправлять файлы на сервер. После успешной отправки файлы удаляются из этого каталога.

Важное примечание: Все идентификаторы очередей клиента, должны совпадать с идентификаторами очередей этого клиента, заданными на сервере. Если на сервере список очередей для этого клиента будет не соответствовать списку очередей клиента, то сетевое соединение с этим клиентом будет разорвано.

Параметр «Выдавать подпись» обеспечивает сохранение во входящем каталоге не только файлов (например, file.txt), но и его подпись в виде файла в DER кодировке (например, file.txt.p7d). расширение «.p7d» добавляется автоматически.

Если нужно еще сохранять полученные квитанции на отправленные файлы, то можно включить опцию «Сохранять квитанции в каталог» и указать каталог для сохранения квитанций. Квитанции сохраняются в виде фалов с названием, совпадающим с отправленным файлом, к которому добавляется расширение «.rcp» (например, file.txt.rcp).

Параметр «Выдавать подпись квитанций» обеспечивает сохранение в каталоге не только квитанций (например, file.txt.rcp), но и их подписей в виде файла в DER кодировке (например, file.txt.rcp.p7d). расширение «.p7d» добавляется автоматически.

Для настройки программы на сервере выберите раздел «Файл-сервер».

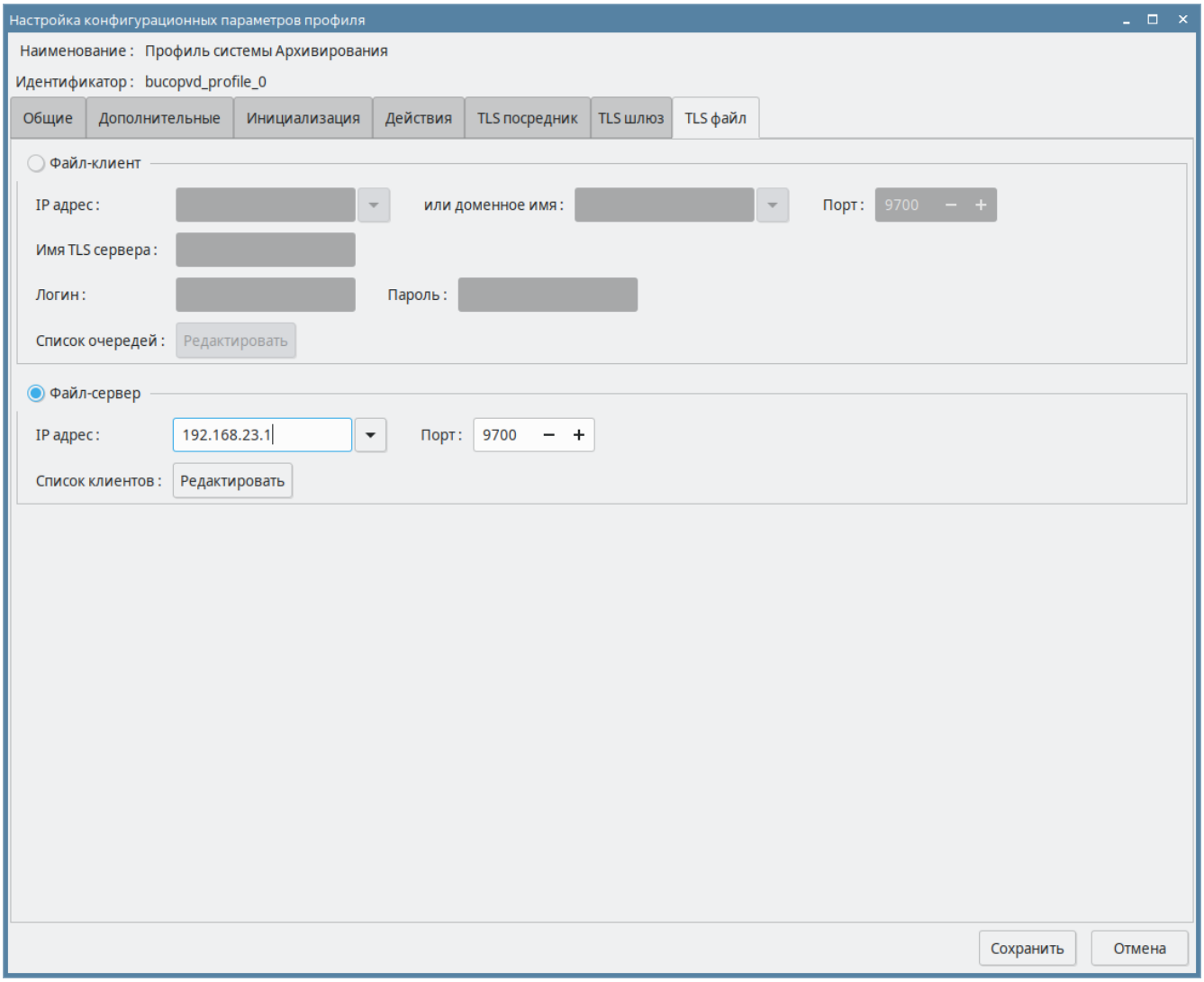

Рисунок 35. Настройка Файл-клиента.

«IP адрес» и «Порт» задает адрес и порт, на которых «Файл-сервер» будет принимать входящие сетевые соединения от «Файл-клиентов».

Для создания, просмотра и редактирования списка клиентов, которым разрешено подключиться к «Файл-серверу» предусмотрен параметр «Список клиентов» с кнопкой «Редактировать».

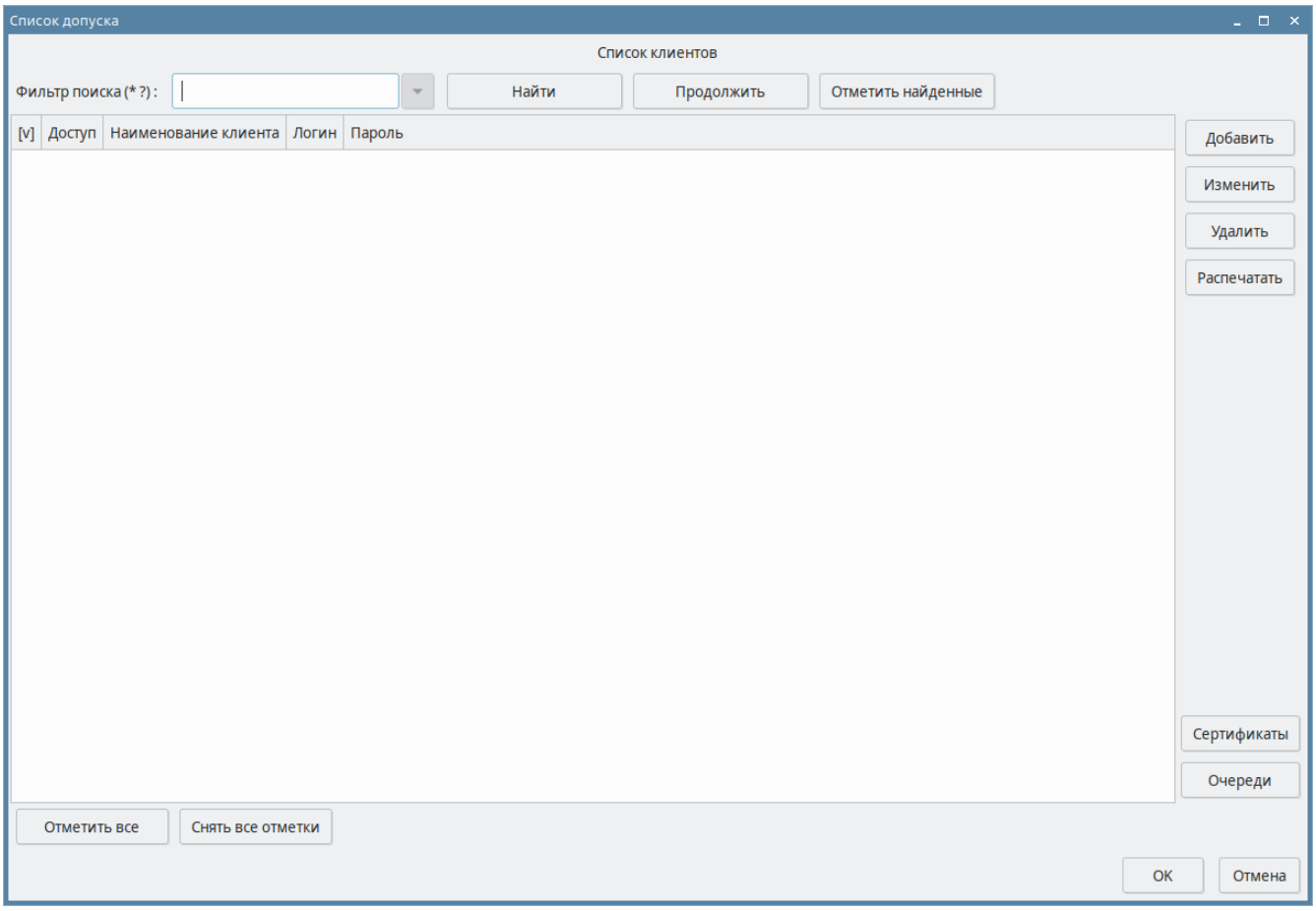

Рисунок 36. Список клиентов.

Данный диалог позволяет добавлять, изменять и удалять клиентов в списке.

Для удаления записей необходимо выбрать их в специальной колонке [v] с помощью «мышки» или кнопки «Отметить все». Кнопка «Снять все отметки» отменяет все отметки в колонке [v].

Кнопка «Распечатать» обеспечивает распечатку списка клиентов в текстовом виде.

Добавление клиента выполняется с помощью кнопки «Добавить».

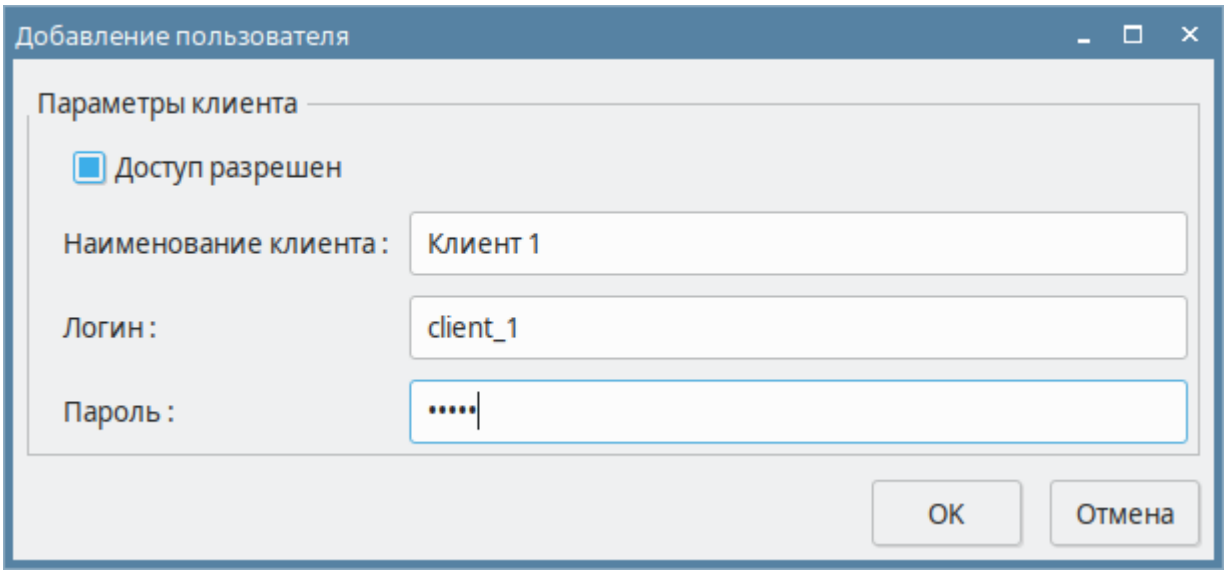

Рисунок 37. Добавление клиента.

Параметр «Доступ разрешен» по умолчанию установлен. Если его выключить, то запись клиента будет добавлена в список, но этот клиент («Файл-клиент») подключиться к «Файл-серверу» не сможет.

«Наименование клиента» может заполняться произвольно, так как несет только информацию для удобства идентификации клиента. Данное поля обязательное для заполнения.

Значение поля «Логин» является обязательным и должно точно соответствовать значению поля «Логин» у «Файл-клиента». При наличии расхождений работа этого клиента будет невозможна.

Заполнение поля «Пароль» не является обязательным. Если это поле пустое, то клиент сможет подключаться к серверу без проверки пароля. Если задать значение пароля, то клиент сможет подсоединиться к серверу только после проверки точного совпадения пароля.

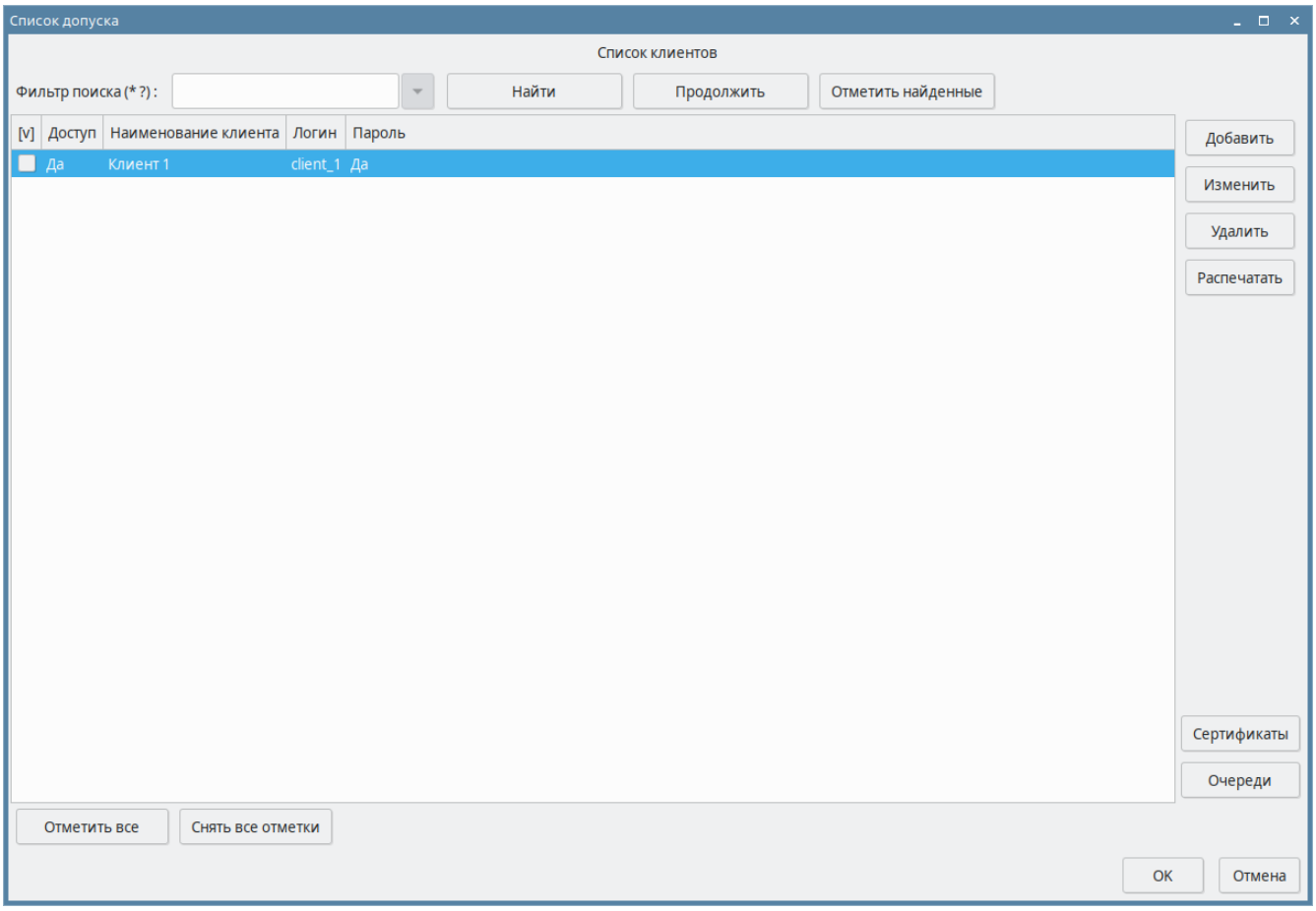

Рисунок 38. Список допущенных клиентов.

После добавления записи клиента нужно обязательно указать список имен сертификатов этого клиента, а также создать список очередей, соответствующих очередям этого клиента.

Для указания списка имен сертификатов необходимо выбрать курсором запись клиента и нажать кнопку «Сертификаты».

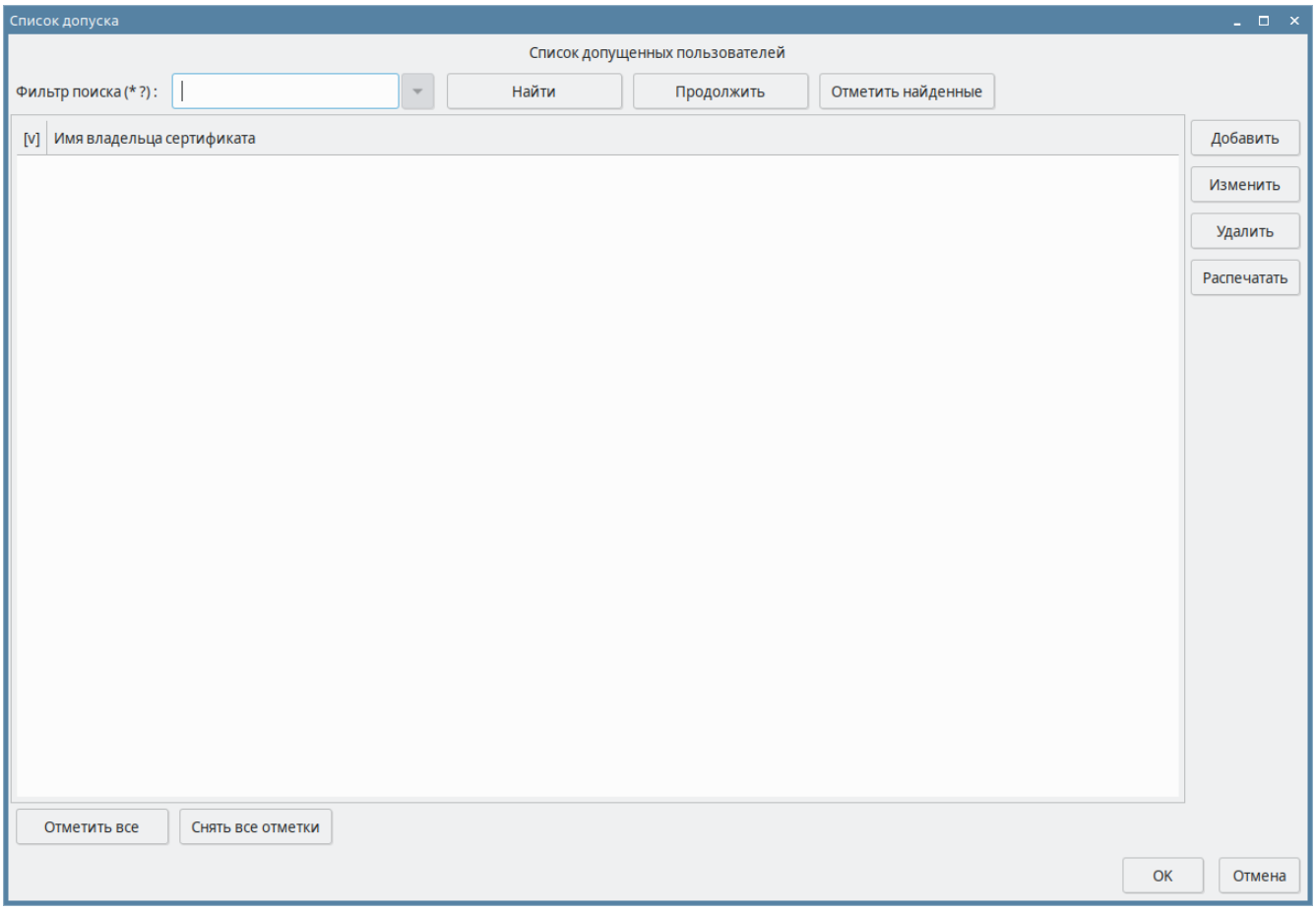

Рисунок 39. Список сертификатов.

Данный диалог позволяет вести список имен владельцев сертификатов путем их добавления, изменения и удаления.

Для удаления записей необходимо выбрать их в специальной колонке [v] с помощью «мышки» или кнопки «Отметить все». Кнопка «Снять все отметки» отменяет все отметки в колонке [v].

Кнопка «Распечатать» обеспечивает распечатку списка имен сертификатов в текстовом виде.

Добавление имени сертификата выполняется с помощью кнопки «Добавить».

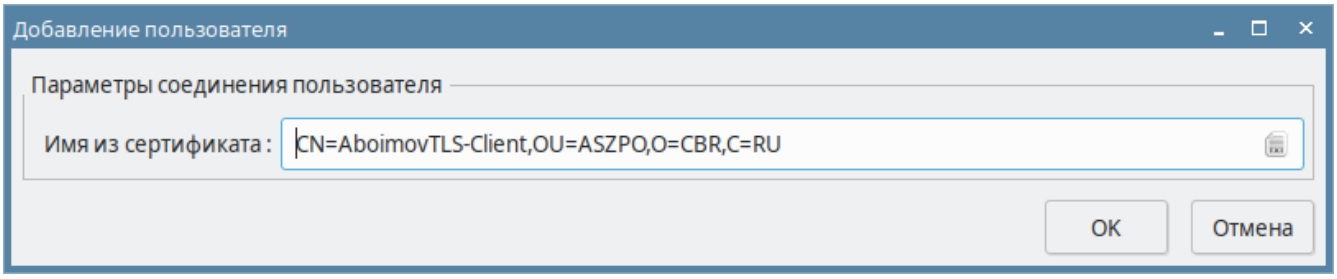

Рисунок 40. Добавление имени владельца сертификата.

Имя владельца из сертификата клиента можно ввести вручную или получить из файла с сертификатом в DER кодировке. Если нажать на иконку файла в конце ввода строки, то будет выдан стандартный диалог выбора файла. Имя владельца автоматически будет размещено в стоке ввода.

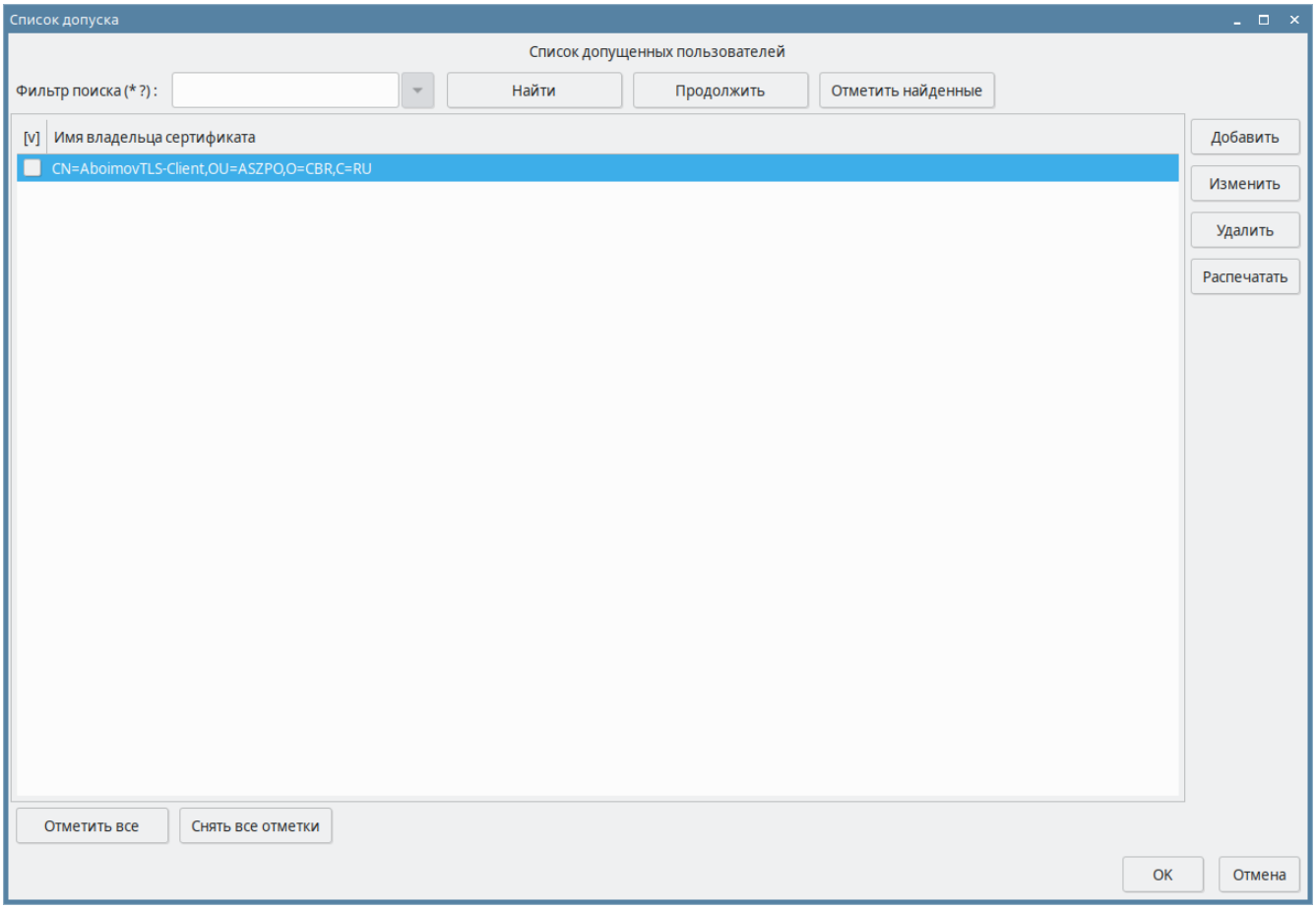

Рисунок 41. Список сертификатов клиента.

Для задания списка очередей необходимо выбрать курсором запись клиента и нажать кнопку «Очереди» (Рисунок 36. Список клиентов.).

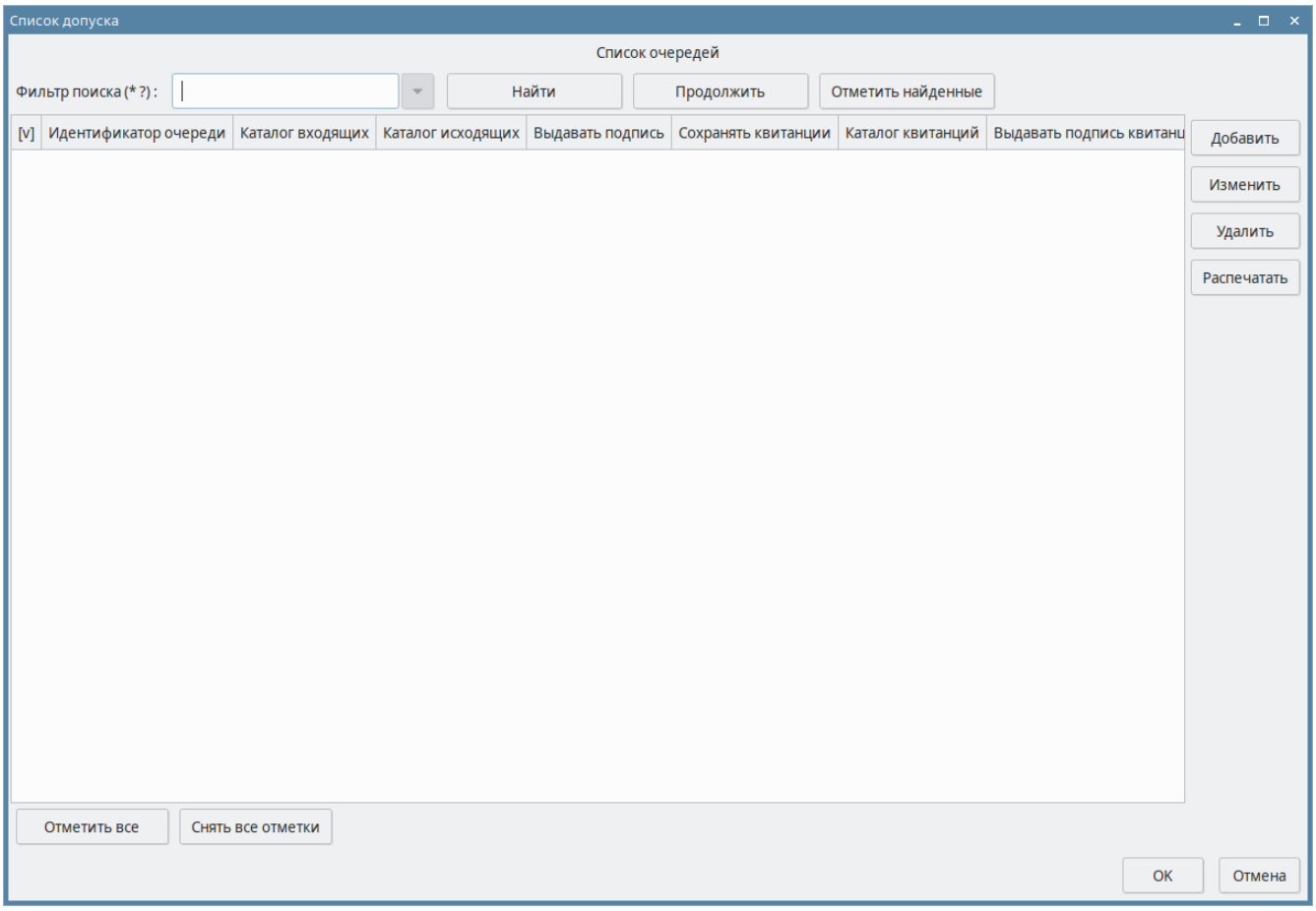

Рисунок 42. Список очередей.

Данный диалог позволяет добавлять, изменять и удалять очереди в списке.

Для удаления записей необходимо выбрать их в специальной колонке [v] с помощью «мышки» или кнопки «Отметить все». Кнопка «Снять все отметки» отменяет все отметки в колонке [v].

Кнопка «Распечатать» обеспечивает распечатку списка очередей в текстовом виде.

Добавление очередей выполняется с помощью кнопки «Добавить».

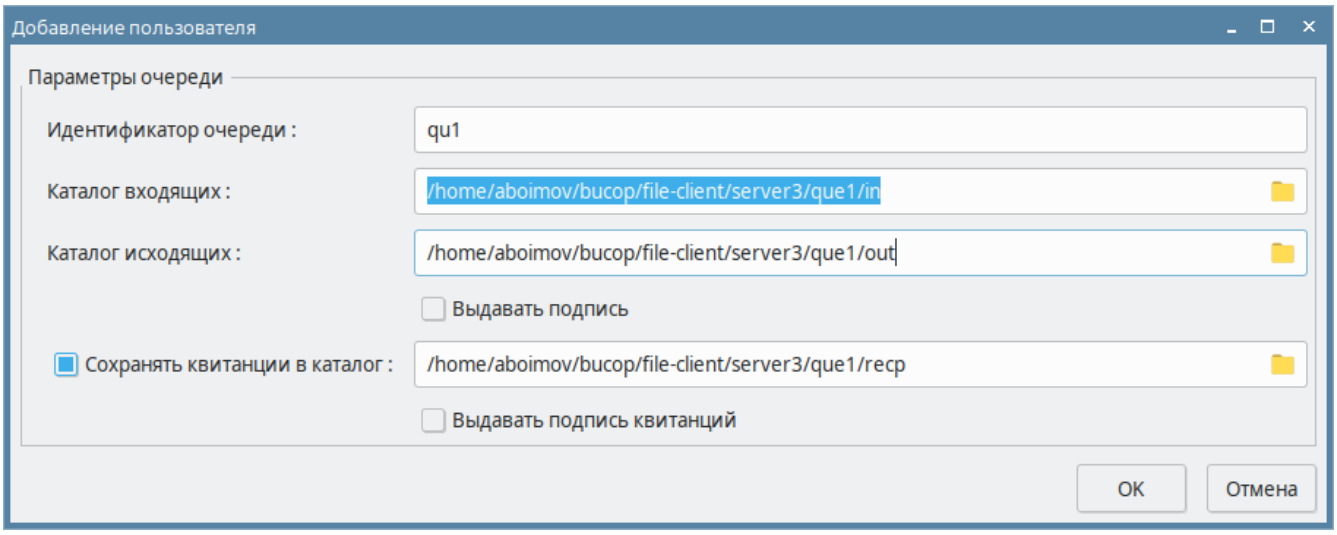

Рисунок 43. Добавление очереди.

«Идентификатор очереди» является обязательным для заполнения. Он представляет собой произвольную последовательность до 64 символов в нижнем регистре латинского алфавита с цифрами и символом подчерка «_». Пробелы не допускаются.

Дополнительно к идентификатору очереди нужно обязательно задать каталог для сохранения входящих файлов и каталог исходящих файлов, из которого программа будет отправлять файлы на сервер. После успешной отправки файлы удаляются из этого каталога.

Важное примечание: Все идентификаторы очередей клиента, должны совпадать с идентификаторами очередей этого клиента, заданными на сервере. Если на сервере список очередей для этого клиента будет не соответствовать списку очередей клиента, то сетевое соединение с этим клиентом будет разорвано.

Параметр «Выдавать подпись» обеспечивает сохранение во входящем каталоге не только файлов (например, file.txt), но и его подпись в виде файла в DER кодировке (например, file.txt.p7d). расширение «.p7d» добавляется автоматически.

Если нужно еще сохранять полученные квитанции на отправленные файлы, то можно включить опцию «Сохранять квитанции в каталог» и указать каталог для сохранения квитанций. Квитанции сохраняются в виде фалов с названием, совпадающим с отправленным файлом, к которому добавляется расширение «.rcp» (например, file.txt.rcp).

Параметр «Выдавать подпись квитанций» обеспечивает сохранение в каталоге не только квитанций (например, file.txt.rcp), но и их подписей в виде файла в DER кодировке (например, file.txt.rcp.p7d). расширение «.p7d» добавляется автоматически.

3.2 Протокол

Протокол ошибок конфигурационной программы ведется в текстовом файле «bucopvdcfg.log», который располагается в каталоге HOME/.validata/bucopvd/log (например, /home/aboimov/.validata/bucopvd/log).

3.3 Настройка сервиса

Для создания сервиса необходимо разместить в специальном каталоге ОС Linux текстового файла с определенными параметрами.

Каталог: /etc/sytemd/system

Файл: <service_name>.service (например, bucopvd_0.service), где <service_name> - это имя сервиса.

Пример доступных команд для сервиса bucop_0

	systemctl status bucopvd_0	Посмотреть состояние сервиса
	sudo systemctl enable bucopvd_0	Разрешить автоматический запуск сервиса после загрузки/перезагрузки ОС
	sudo systemctl start bucopvd_0	Запустить сервис
	sudo systemctl stop bucopvd_0	Остановить сервис
	sudo systemctl disable bucopvd_0	Отменить автоматический запуск сервиса после загрузки/перезагрузки ОС
	sudo systemctl daemon-reload	Перегрузить systemctl

Для удобства создания сервиса в комплект установки входит командная процедура:

/opt/validata/bucopvd/signal/systemd_add

Для создания сервиса service_name с профилем id_profile используйте команду:

sudo /opt/validata/bucopvd/signal/systemd_add service_name id_profile program_name $HOME $(whoami) "$(groups)"

Сервис будет создан в каталоге /etc/systemd/system с именем service_name.service для выполнения программы program_name (bucopvd или bucopvd_d) с параметром id_profile

3.3.1. Пример сервиса с автоматической загрузкой ключа

Если возможно обеспечить автоматическую загрузку ключа без интерактивных (ручных) операций по установке ключевого носителя или ввода PIN кода во время загрузки, то можно создать сервис непосредственно для программы (bucopvd) с профилем (bucopvd_profile_0) следующим образом:

sudo /opt/validata/bucopvd/signal/systemd_add bucopvd_0 bucopvd_profile_0 bucopvd $HOME $(whoami) "$(groups)"

После выполнения команды:

sudo systemctl enable bucopvd_0

Сервис Программы будет автоматически запускаться после загрузки/перезагрузки ОС.

3.3.2. Пример сервиса с предварительной загрузкой ключа

Если невозможно обеспечить автоматическую загрузку ключа без интерактивных (ручных) операций по установке ключевого носителя или ввода PIN кода во время загрузки, то можно создать сервис для вспомогательной утилиты (bucopvd_d) с профилем (bucopvd_profile_0) следующим образом:

sudo /opt/validata/bucopvd/signal/systemd_add service_name bucopvd_profile_0 bucopvd_d $HOME $(whoami) "$(groups)"

Установить параметр «Предварительная загрузка ключа» в профиле bucopvd_profile_0 с помощью Конфигурационной программы (bucopvdcfg).

Этот сервис нельзя ставить в автозапуск, так как после загрузки ОС необходимо запустить Программу с помощью программы Мониторинга или из командной строки:

/opt/validata/bucopvd/bin/bucopvd bucopvd_profile_0

Загрузить ключ в «ручном» режиме.

В дальнейшем следующие команды могут заставлять Программу начинать работу и останавливать его работу без выгрузки ключа.

sudo systemctl start bucopvd_d_0

sudo systemctl stop bucopvd_d_0

Данный вариант создан для работы Программы на сервере в режиме кластера.

3.4 Настройка кластера

Установка кластерного ПО на каждом узле (сервере) кластера:

sudo apt install pacemaker pcs

На каждом узле (сервере) следует произвести запуск необходимых служб кластера:

sudo systemctl start corosync

sudo systemctl start pacemaker

Оба сервера должны «видеть» друг друга по имени, для этого должен быть настроен DNS или в файле: /etc/hosts

Нельзя использовать адрес 127.0.0.1. Должны разрешаться только реальные адреса, например, записать в /etc/hosts следующие строки:

192.168.22.137 node-1

192.168.22.138 node-2

На каждом сервере удалить возможно сохранившуюся предыдущую конфигурацию кластера:

sudo pcs cluster destroy

На каждом сервере установить одинаковый пароль пользователю hacluster:

sudo passwd hacluster

Установить аутентификацию локальных компьютеров (возможно, эту команду не нужно выполнять если не нужен TLS)

sudo pcs host auth al-node-1 al-node-2 -u hacluster

Создать кластер с помощью команды (my_cluster – это произвольное имя созданного кластера)

sudo pcs cluster setup my_cluster al-node-1 al-node-2

Запустить кластер на всех узлах (серверах):

sudo pcs cluster start --all

Важное замечание: Отключить поддержку stonith (без этого ничего не работает). Это нужно делать на запущенном кластере до установки ресурсов.

sudo pcs property set stonith-enabled=false

Отключаем кворум, так как у нас 2 узла:

sudo pcs property set no-quorum-policy=ignore

Настройка автоматического включения кластера на всех узлах (серверах) при загрузке:

sudo pcs cluster enable --all

Проверка состояния кластера:

sudo pcs status

sudo pcs status cluster

Остановить кластер на всех узлах (серверах):

sudo pcs cluster stop --all

Настройка автоматического выключения кластера на всех узлах (серверах) при загрузке:

sudo pcs cluster disable –all

После создания кластера нужно приступать к созданию ресурсов кластера. Рассмотрим два варианта создания ресурса запуска сервиса Программы.

3.4.1. Кластер с автоматической загрузкой ключа

Если возможно обеспечить автоматическую загрузку ключа без интерактивных (ручных) операций по установке ключевого носителя или ввода PIN кода во время загрузки, то можно создать кластерный ресурс (res_bucopvd_0 – это произвольное имя ресурса) непосредственно для сервиса Программы (bucopvd_0) следующим образом:

sudo pcs resource create res_bucopvd_0 systemd:bucopvd_0

Сделать его активным, поставив в автозапуск:

sudo pcs resource enable res_bucopvd_0

Посмотреть статус ресурса:

sudo pcs resource status

3.4.2. Кластер с предварительной загрузкой ключа

Если невозможно обеспечить автоматическую загрузку ключа без интерактивных (ручных) операций по установке ключевого носителя или ввода PIN кода во время загрузки, то

можно создать кластерный ресурс (res_bucopvd_d_0) для сервиса вспомогательной утилиты (bucopvd_d_0) следующим образом:

sudo pcs resource create res_bucopvd_d_0 systemd:bucop_d_0

Кластер с таким ресурсом нельзя ставить в автозапуск, то есть делать активным (enable), так как после запуска ОС нужно будет запустить сервис Программы в «ручном режиме» с загрузкой ключа. После этого можно стартовать кластер тоже «вручную»:

sudo pcs cluster start –all

Останавливать кластер нужно будет тоже «вручную»:

sudo pcs cluster stop –all

4 ЛИЦЕНЗИРОВАНИЕ

4.1 Программа установки лицензии

Запуск программы установки лицензии выполняется от имени Администратора (root) через главное меню приложений путем выбора закладки «Лицензия Архив.(Админ.)». После этого нужно будет ввести пароль Администратора (root).

На экран выдается главное меню программы установки лицензий.

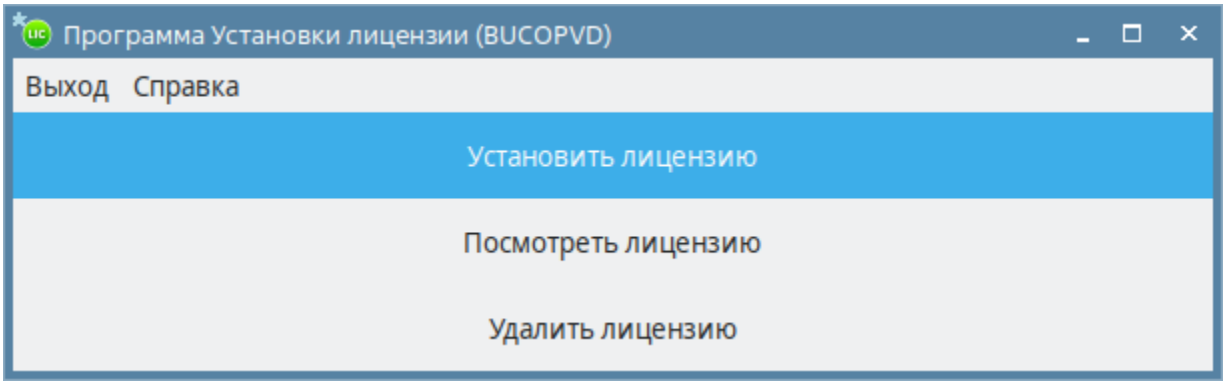

Рисунок 44. Главное меню программы установки лицензий.

Выберите пункт меню «Установить лицензию».

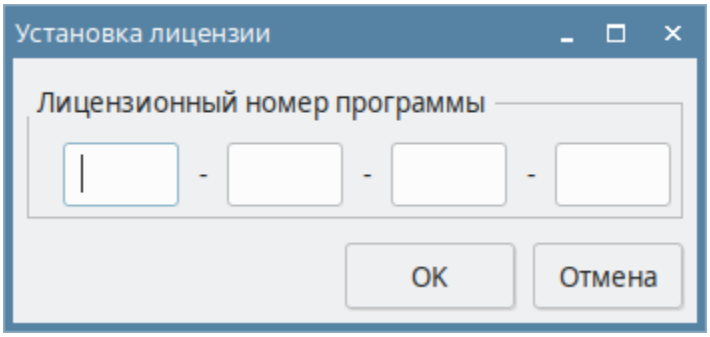

Рисунок 45. Ввод лицензионного номера.

После ввода лицензионного номера (например, 12345-12345-12345-12345) будет выполнена его проверка и установка.

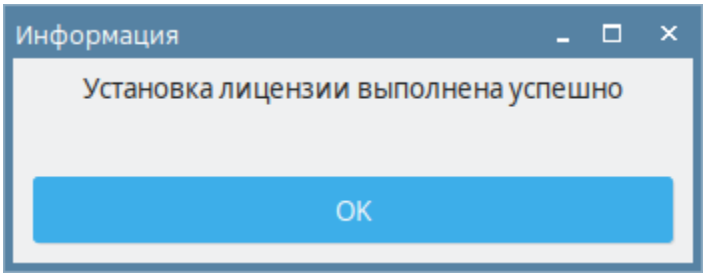

Рисунок 46. Успешная установка лицензии.

После успешной установки лицензии в «Конфигурационной программе» или «Программе мониторинга» можно будет выбрать пункт меню («Справка»-«О программе») и посмотреть лицензионный номер этой программы.

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					