УТВЕРЖДАЮ
Директор
ОДО «ВИРУСБЛОКАДА»
_____ Г.К. Резников
«15» октября 2025 г.

ПРОГРАММНЫЙ КОМПЛЕКС ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ ДЛЯ ФУНКЦИОНИРОВАНИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS NT 10.0 И UNIX

Руководство пользователя

ЛИСТ УТВЕРЖДЕНИЯ

BY.ИАДВ.12010-03 101 01-ЛУ

Заместитель директора
_____ Ю.Г. Резников
«15» октября 2025 г.

Начальник отдела
разработки НТД
_____ А.В. Заговалко
«15» октября 2025 г.

Нормоконтролер
_____ М.А. Шилкина
«15» октября 2025 г.

2025

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата
249	15.10.2025	239		

2		15.10.2025
№ изм.	Подп.	Дата

УТВЕРЖДЕН
BY.ИАДВ.12010-03 101 01-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ ДЛЯ ФУНКЦИОНИРОВАНИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS NT 10.0 И UNIX

Руководство пользователя

BY.ИАДВ.12010-03 101 01

Листов 183

2025

№ изм.	Подп.	Дата

АННОТАЦИЯ

Настоящий документ содержит руководство пользователя программного комплекса защиты от вредоносного программного обеспечения, несанкционированного доступа и межсетевого экранирования для функционирования в операционных системах семейства Windows NT 10.0 и Unix (далее – программный комплекс ШХУНА), BY.ИАДВ.12010-01, который осуществляет защиту информации, распространение и (или) предоставление которой ограничено, в том числе персональных данных, от несанкционированного доступа и вредоносного программного обеспечения, контроль и фильтрация проходящего через программный комплекс защиты сетевого трафика в соответствии с заданными правилами.

Настоящий документ разработан в соответствии с требованиями СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности», компонент гарантии AGD_OPE.1 «Руководство пользователя», уровень гарантии оценки 4 (УГО 4).

Знак соответствия означает, что программный комплекс ШХУНА соответствует требованиям технического регламента Республики Беларусь ТР 2013/027/BY.

Разработчиком программного комплекса является предприятие ОДО «ВИРУСБЛОКАДА».

СОДЕРЖАНИЕ

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе применяют следующие обозначения и сокращения:

ВПО – вредоносное программное обеспечение;

ГТБ – гарантийное требование безопасности;

ЛВС – локальная вычислительная сеть;

ЛКМ – левая кнопка манипулятора типа «мышь»;

ОЗУ – оперативное запоминающее устройство;

ОС – операционная система;

ПО – программное обеспечение;

ПЭВМ – персональная электронно-вычислительная машина;

СВТ – средство вычислительной техники;

СЗИ – средство защиты информации;

СУБД – система управления базами данных;

УГО – уровень гарантии оценки;

ФТБ – функциональное требование безопасности;

ЦУ – модуль «Центр управления» программного комплекса ШХУНА.

2. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программный комплекс ШХУНА осуществляет защиту информации, распространение и (или) предоставление которой ограничено, в том числе персональных данных, от несанкционированного доступа и ВПО, контроль и фильтрация проходящего через программный комплекс сетевого трафика в соответствии с заданными правилами.

В состав программного комплекса ШХУНА входят следующие функциональные модули:

1) модуль управления доступом;
2) модуль контроля данных;
3) модуль межсетевого экранирования;
4) модуль удаления;
5) модуль контроля неизменности;
6) модуль графического интерфейса;
7) модуль «Агент удаленного администрирования»;
8) модуль «Центр управления»;
9) модуль взаимодействия.

Программный комплекс ШХУНА обеспечивает:

1) удаление информации, не требующейся для дальнейшего использования, в том числе следов ее обработки путем циклического затирания файла случайными данными и удалением его из файловой системы;
2) защиту средств вычислительной техники от ВПО за счет анализа файловых объектов (по требованию или в режиме реального времени) по сигнатурным базам, удаление и блокирование подозрительных объектов (файлов) с генерацией соответствующего события;
3) защиту от несанкционированного доступа к информации, контроль доступа к информации (к файлам на СВТ) осуществляется за счет компонента Монитор модуля контроля данных;
4) межсетевое экранирование (фильтрация данных, трансляция сетевых адресов) и защита настроек межсетевого экрана (в соответствии с требованиями СТБ 34.101.73-2017 п.7.3);

5) удаление временных файлов в ручном и автоматическом режимах (модуль удаления осуществляет поиск временных файлов и последующее их удаление путем циклического затирания файла случайными данными с последующим удалением его из файловой системы);
6) контроль неизменности конфигурации СВТ и установленного на нем ПО;
7) ведение аудита действий пользователя при работе с информацией, функционирования прикладного и системного ПО с возможностью просмотра и редактирования списка объектов и устройств в электронных журналах только администратором безопасности;
8) контроль неизменности файлов комплекса с реализацией функции восстановления из единого ЦУ в случае выявленного нарушения;
9) контроль настроек, запуска, обновления всех компонент комплекса, исключая необходимость каких-либо действий на СВТ пользователей, по инсталляции и настройке, кроме разрешения нештатных ситуаций (действия по инсталляции, настройке, контролю настроек, запуску и обновлению комплекса выполняет администратор);
10) контроль и управление перечнем программных процессов, функционирующих на СВТ для каждого пользователя;
11) контроль и управление перечнем установленного программного обеспечения на СВТ для каждого пользователя (программы и компоненты deb и rpm-пакеты);
12) ограничение доступа пользователей к настройкам комплекса (данные настройки должны защищаться компонентом, запрещающим доступ на запись к ним; графический интерфейс должен быть защищен паролем);
13) постоянный автоматический, либо по запросу анализ обрабатываемой информации на наличие вредоносных программ в соответствии с заданными администратором условиями;
14) непрерывный контроль за действиями пользователя при работе с информацией (доступ, запись, чтение, копирование информации, вывод на печать и т.д.), состояния защиты системы для своевременного обнаружения нарушений политики безопасности системы и действий вредоносных

программ с возможностью уведомления администратора при возникновении критических ситуаций;

15) фильтрацию проходящих через программный комплекс ШХУНА сетевых пакетов (IPv4 / IPv6) в соответствии с заданными правилами (сетевые адреса получателя и отправителя, используемый протокол передачи данных, порт) и принятие на основе интерпретируемых правил следующих решений: не пропустить данные, пропустить данные, занести информацию в журнал аудита, уведомить пользователя/администратора;
16) регистрацию запуска клиентской части и управление работой комплекса путем формирования событий о запуске/остановке комплекса на СВТ;
17) выставление приоритета на потребление ресурсов ОС при выполнении фоновых заданий комплекса;
18) объединение защищаемых объектов (СВТ) в группы и подгруппы для применения к ним отдельных политик и заданий;
19) контроль работы комплекса, состояния защищаемых объектов и отображение их состояния;
20) осуществление централизованного автоматического/принудительного обновления модулей программного комплекса ШХУНА;
21) уведомление администратора о критических событиях, возникающих при работе комплекса (с возможностью выбора уровня подробности протоколирования), о регистрации события, ведении, хранении и статистической обработке отчетов о результатах работы комплекса (указанные функции должны выполняться как с отдельными защищаемыми объектами, так и с группой таких объектов одновременно);
22) ограничение просмотра и редактирования списка защищаемых объектов и устройств только администратором;
23) назначение заданий по управлению клиентской частью ПО (задания могут быть как периодические, так и разовые);
24) хранение в журнале аудита событий безопасности и результатов заданий администратора;

25) ограничение возможности определения периферийных устройств, контроль и ограничение доступа (доступ, запись, чтение), к следующим видам устройств:
    а) USB-устройства (flash-накопители, внешние жесткие диски, цифровые камеры и аудиоплееры, карманные компьютеры, локальные и сетевые принтеры);
    б) контроллеры беспроводных сетей (Wi-Fi, Bluetooth, IrDA);
    в) сетевые карты и модемы, дисководы, CD и DVD-приводы, накопители на жестких магнитных дисках;
    г) внешние порты LPT, COM и IEEE 1394 и другие устройства, имеющие в ОС символическое имя.

Область применения программного комплекса ШХУНА – защита СВТ от ВПО, несанкционированного доступа и межсетевого экранирования.

3. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Программный комплекс ШХУНА устанавливается на СВТ, совместимые с набором команд x86-64 с поддержкой инструкций SSE2, и требует наличия аппаратного обеспечения с характеристиками не менее чем:

1) 2 ГГц тактовой частоты процессора;
2) 4 ГБ оперативной памяти;
3) 2 ГБ свободного пространства накопителя.

Для корректного функционирования ЦУ необходимо аппаратное обеспечение с характеристиками не менее чем:

1) 2 ГГц тактовой частоты процессора;
2) 8 ГБ оперативной памяти;
3) 100 ГБ для установки базы данных ЦУ;
4) сетевая карта пропускной способностью не менее 1 Гб/с.

Для централизованного управления необходимо наличие ЛВС пропускной способностью не менее 1 Гб/с.

Программный комплекс ШХУНА устанавливается и корректно функционирует в среде ОС семейства Windows NT 10.0, включая Windows 11, CentOS 7, Debian 9 и Astra Linux Special Edition (РУСБ.10015-37).

4. ВЫПОЛНЕНИЕ ПРОГРАММЫ И СООБЩЕНИЯ ОПЕРАТОРУ

4.1. Подготовка к установке

Для установки программного комплекса ШХУНА необходимо обладать правами суперпользователя в ОС Linux и/или правами локального администратора в ОС Windows.

4.1.1. Клиентская часть программного комплекса ШХУНА. ОС Windows

Для удаленной установки клиентской части программного комплекса ШХУНА на ОС Windows с использованием механизма сканирования сети ЦУ необходимо:

1) разрешить входящие ICMP-запросы в брандмауэре Windows. Для этого запустить командную строку (`cmd.exe`) с правами администратора и выполнить команду:
   ```
   netsh advfirewall firewall add rule name="ICMP Allow incoming V4
   echo request"protocol=icmpv4:8,any dir=in action=allow;
   ```
   (будьте особенно внимательны к пробелам и символам пунктуации);
2) убедиться в том, что сетевой ресурс администратора **admin$** доступен на чтение/запись по сети. При необходимости, разрешить соответствующий доступ в оснастке **Управление компьютером** (`compmgmt.msc`);
3) добавить ключ реестра ОС `HKLM\Software\Microsoft\Windows\ \CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy` типа `REG_DWORD` и со значением равным `1`.

После добавления данного ключа реестра необходимо перезагрузить СВТ.

4.1.2. Клиентская часть программного комплекса ШХУНА. ОС Linux

Перед установкой клиентской части программного комплекса ШХУНА необходимо получить права суперпользователя ОС.

Для этого можно воспользоваться командой: `sudo -s` для пользователя, входящего в группу администраторов ОС (рис. 1).

```
user@astra:~$ sudo -s
[sudo] пароль для user:
root@astra:/home/user#
```

Рис. 1 – Получение прав суперпользователя на Astra Linux

В случае удаленной установки необходимо разрешить удаленный доступ к системе для суперпользователя. Для этого необходимо:

1) открыть файл `/etc/sshd/openssh_server.config`;
2) заменить строку `PermitRootLogin no` на `PermitRootLogin yes`.

4.1.3. ЦУ. ОС Windows

Перед установкой ЦУ предварительно необходимо установить и настроить СУБД, которые могут быть следующими: PostgreSQL или Microsoft SQL Server (MS SQL).

4.1.3.1. Установка СУБД MS SQL (вариант для автономного окружения)

Загрузите установочный файл СУБД с официального сайта и запустите файл на исполнение (на ПЭВМ, имеющей доступ в интернет). Выберите тип установки **Скачать носитель** (рис. 2).

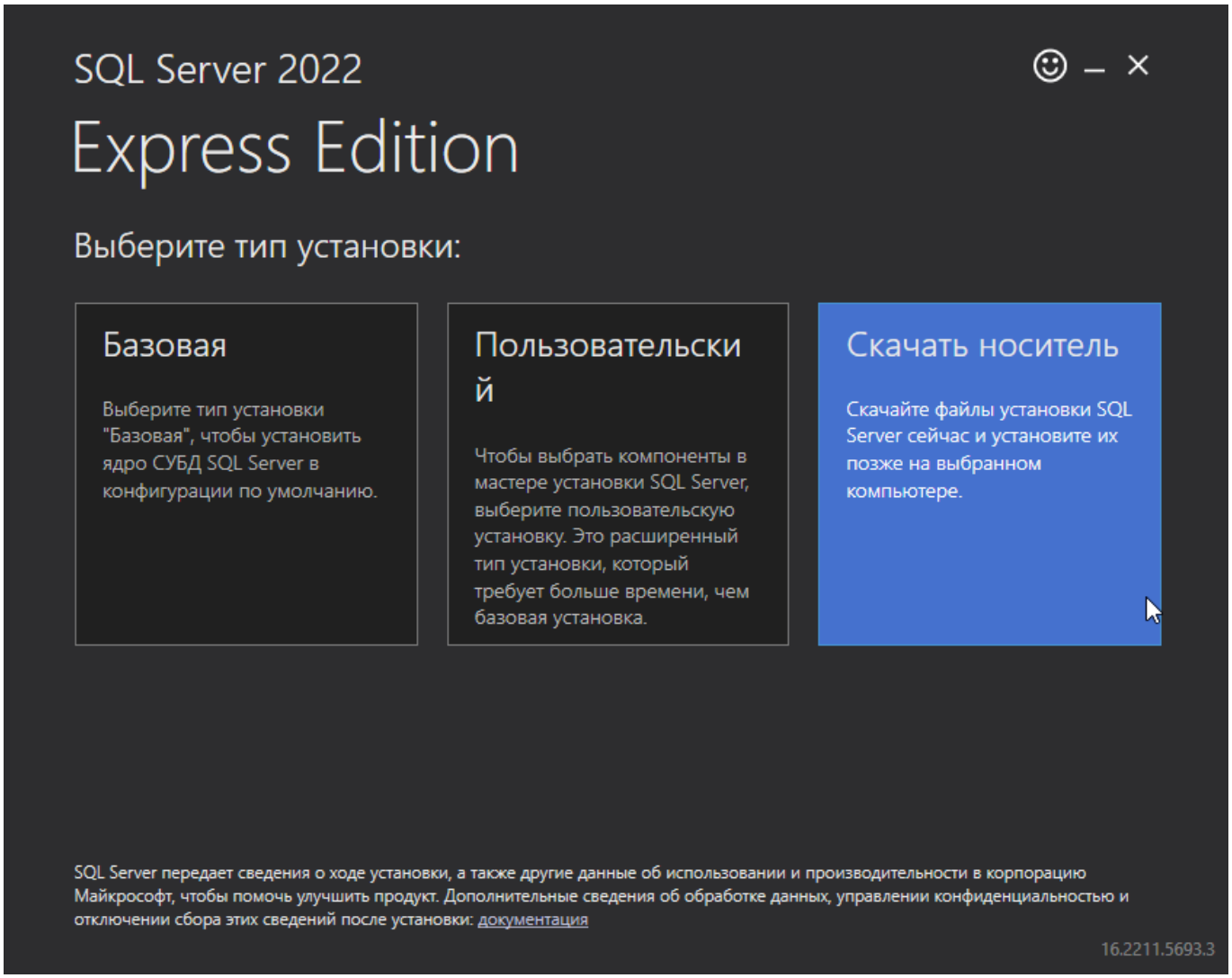


Рис. 2 – Установка MS SQL. Получение файлов установки

Выберите пакет для скачивания и укажите директорию для загрузки (рекомендуется оставить выбор директории по умолчанию). Нажмите кнопку **Скачать** для начала загрузки (рис. 3).

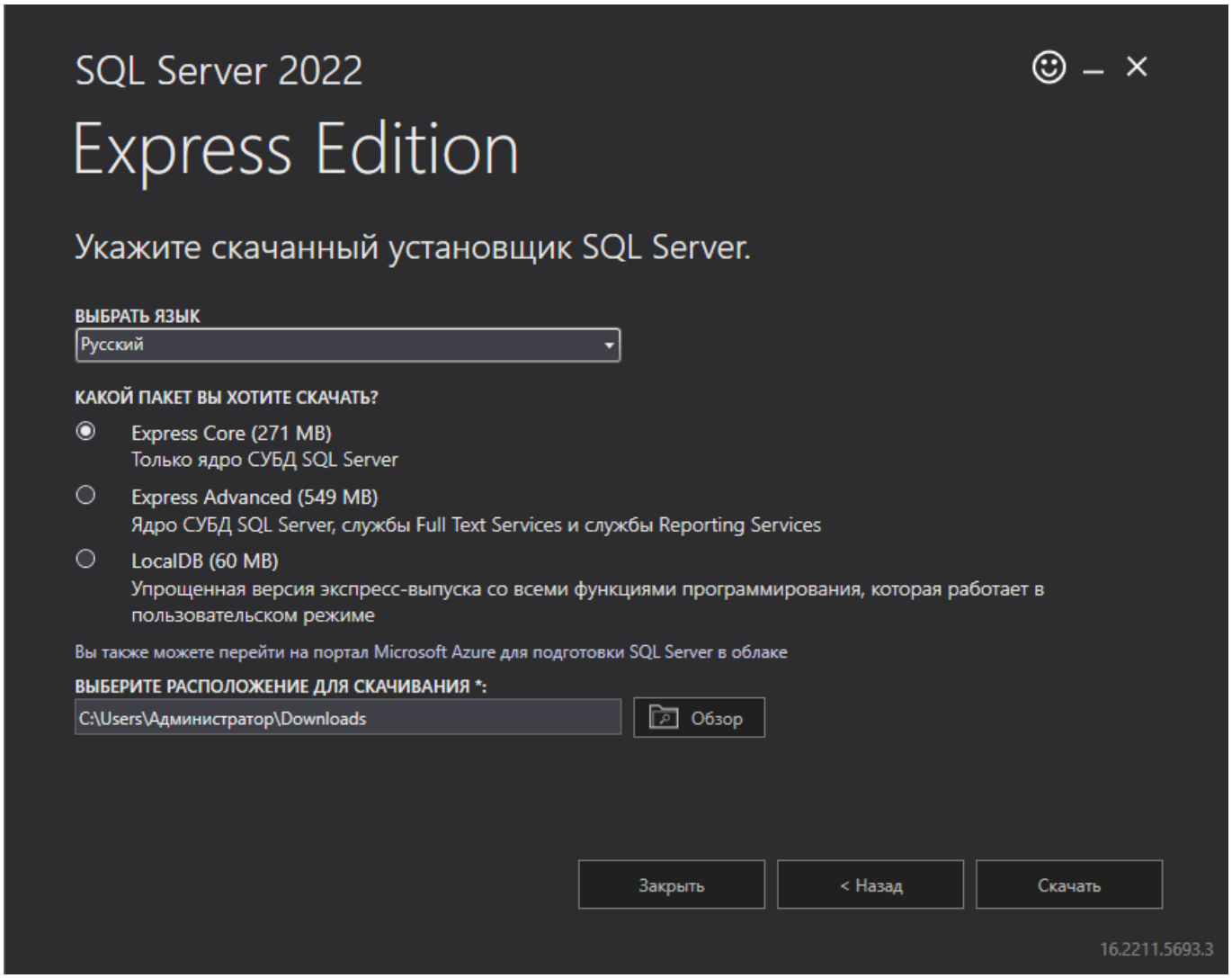


Рис. 3 – Установка MS SQL. Выбор варианта установки

Скопируйте полученные файлы (как правило, это msi-пакет) на ПЭВМ, где будет производиться установка СУБД. Запустите файл установщика на исполнение и выберите директорию для извлечения файлов.

Дождитесь запуска «Центра установки SQL Server». Выберите пункт «Новая установка изолированного экземпляра SQL Server или добавление компонентов к существующей установке» (рис. 4).

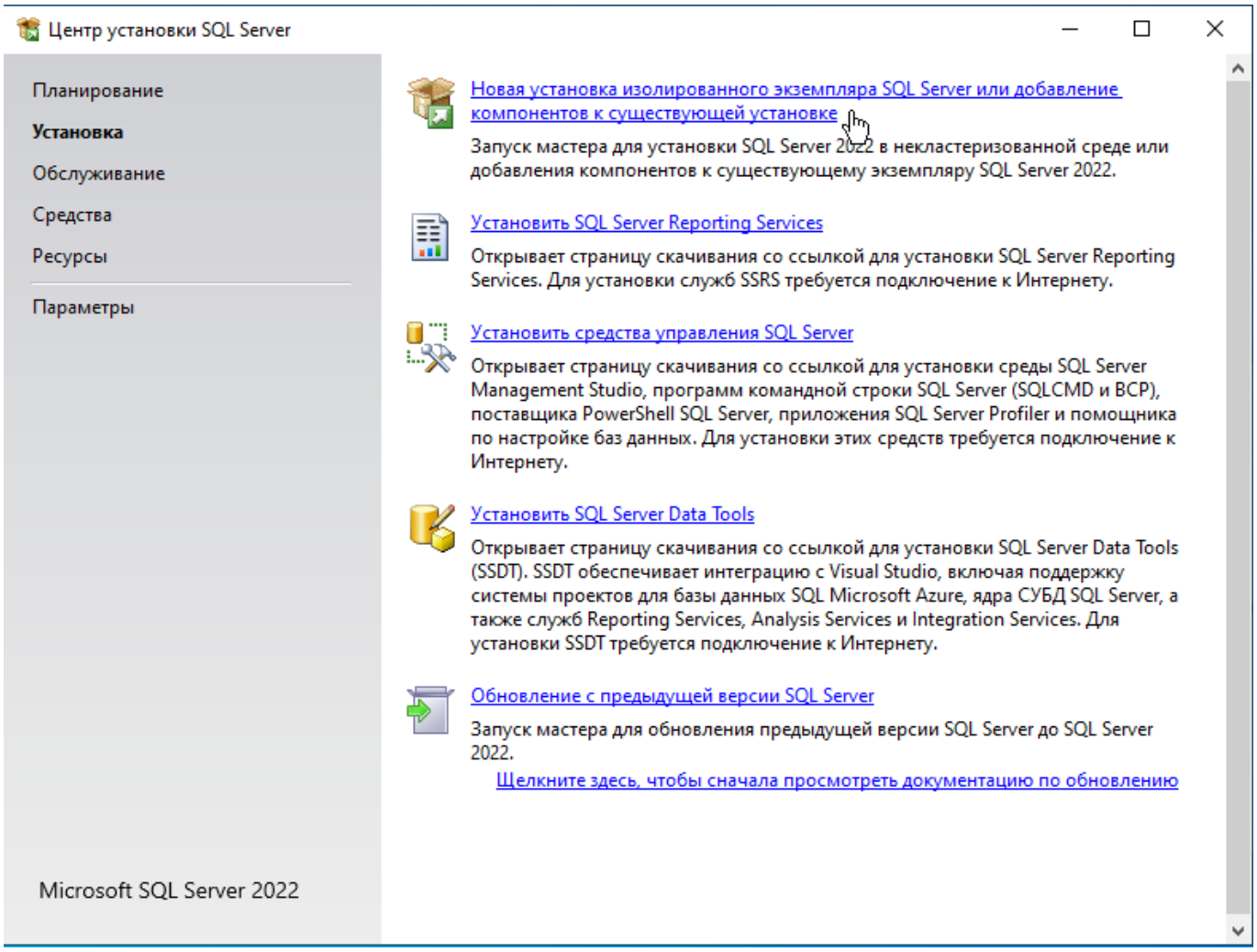


Рис. 4 – Установка MS SQL. Центр установки SQL Server

Примите условия лицензии, выбрав пункт «Я принимаю условия лицензии», и нажмите кнопку **Далее**.

В мастере установки на этапе «Правила установки» дождитесь выявления потенциальных проблем, и, при их наличии, устраните. После устранения или отсутствия проблем нажмите кнопку **Далее** (рис. 5).

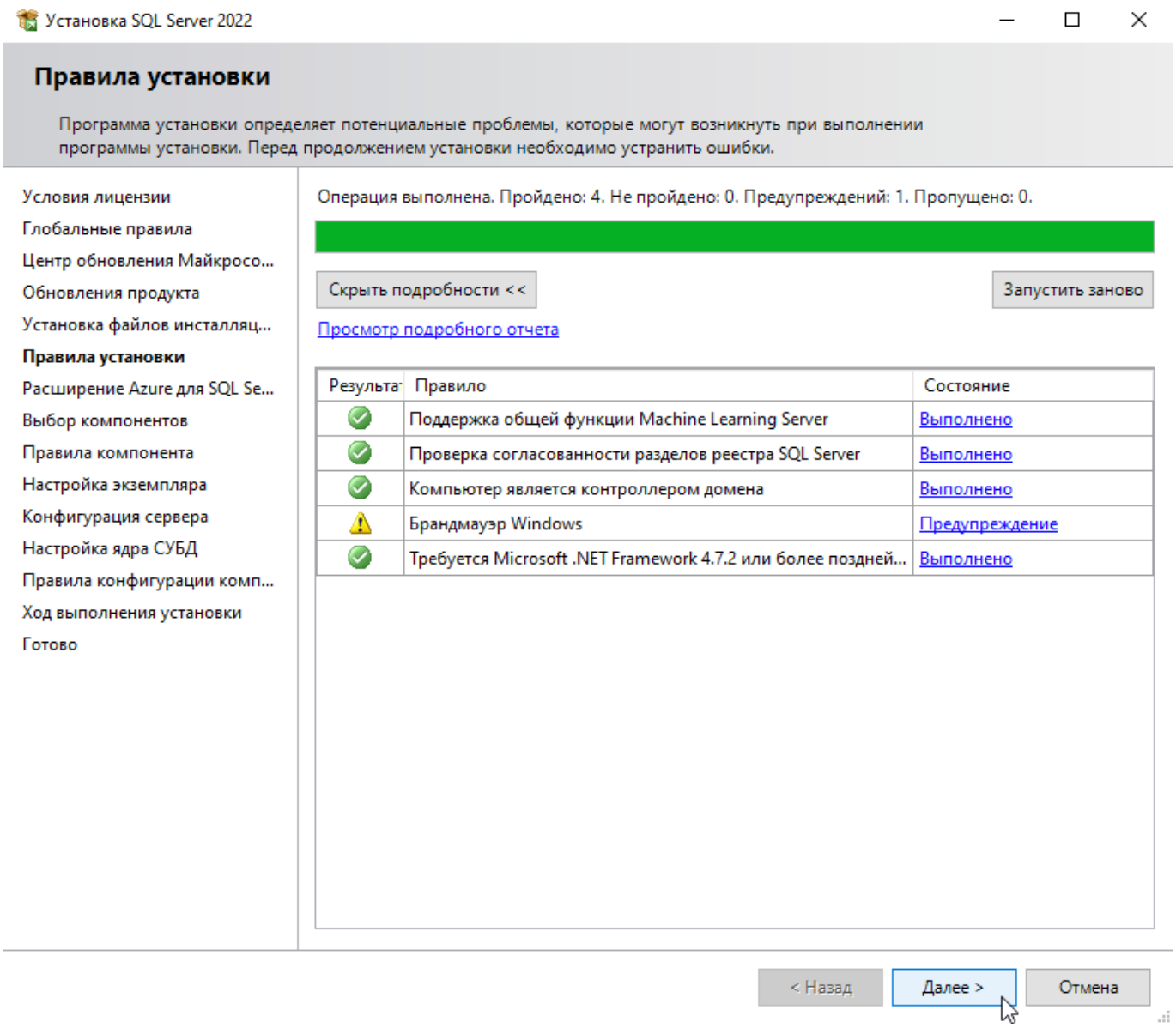


Рис. 5 – Установка MS SQL. Этап «Правила установки»

На этапе «Расширение Azure для SQL Server» отмените выбор «Расширение Azure для SQL Server» и нажмите кнопку **Далее**.

На этапе «Выбор компонентов» выберите компоненты Express и директорию для установки (рекомендуется оставить по умолчанию).

На этапе «Настройка экземпляра» оставьте выбор по умолчанию и нажмите кнопку **Далее**.

На этапе «Конфигурация сервера» оставьте выбор по умолчанию и нажмите кнопку **Далее**.

На этапе «Настройка ядра СУБД» выберите «Смешанный режим (аутентификация SQL Server и Windows)» и введите пароль в строках «Введите пароль» и «Подтвердить пароль» (пароль будет использоваться при установке ЦУ), нажмите кнопку **Далее** (рис. 6).

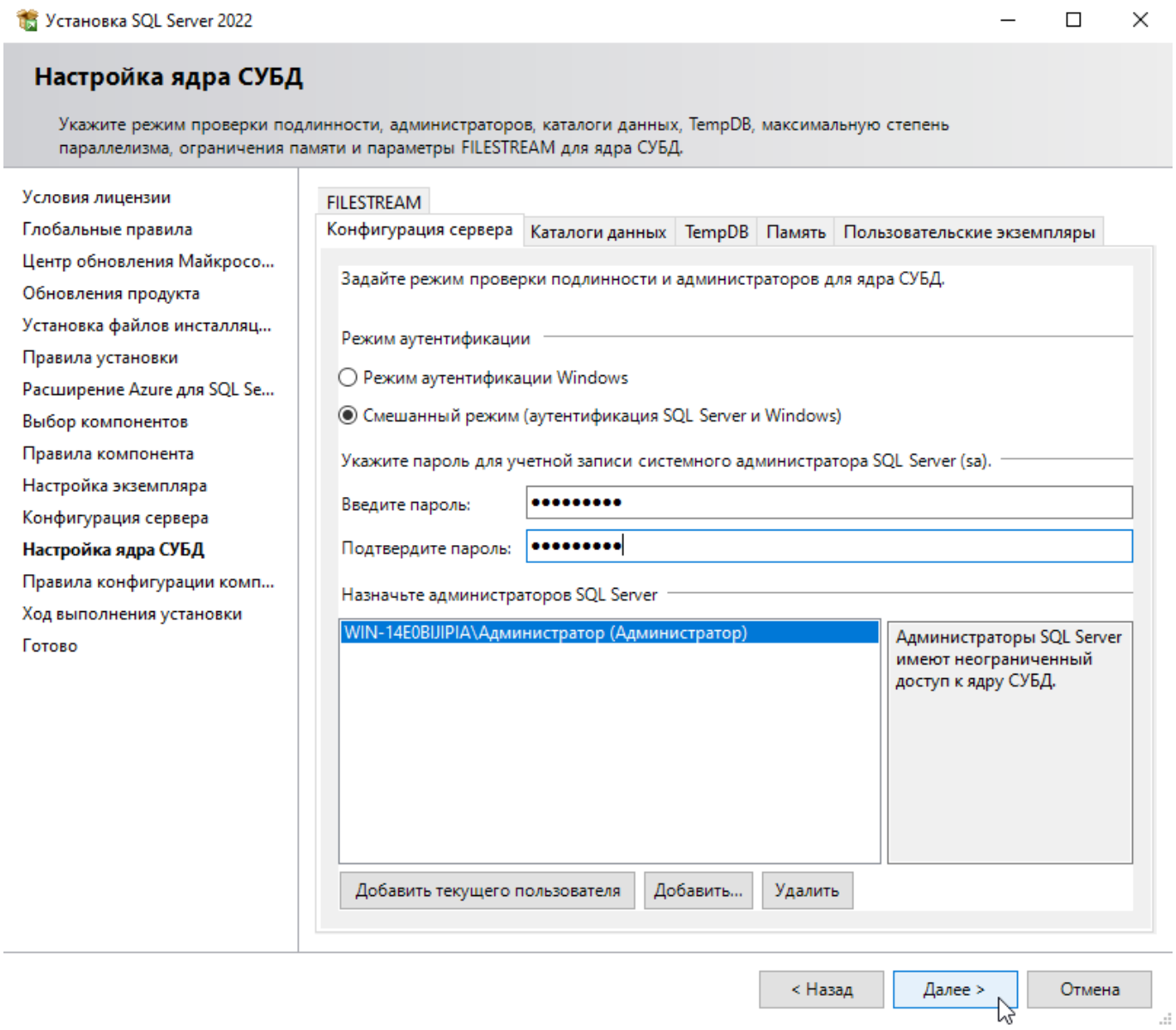


Рис. 6 – Установка MS SQL. Этап «Настройка ядра СУБД»

Дождитесь завершения установки и нажмите кнопку **Закрыть** (рис. 7).

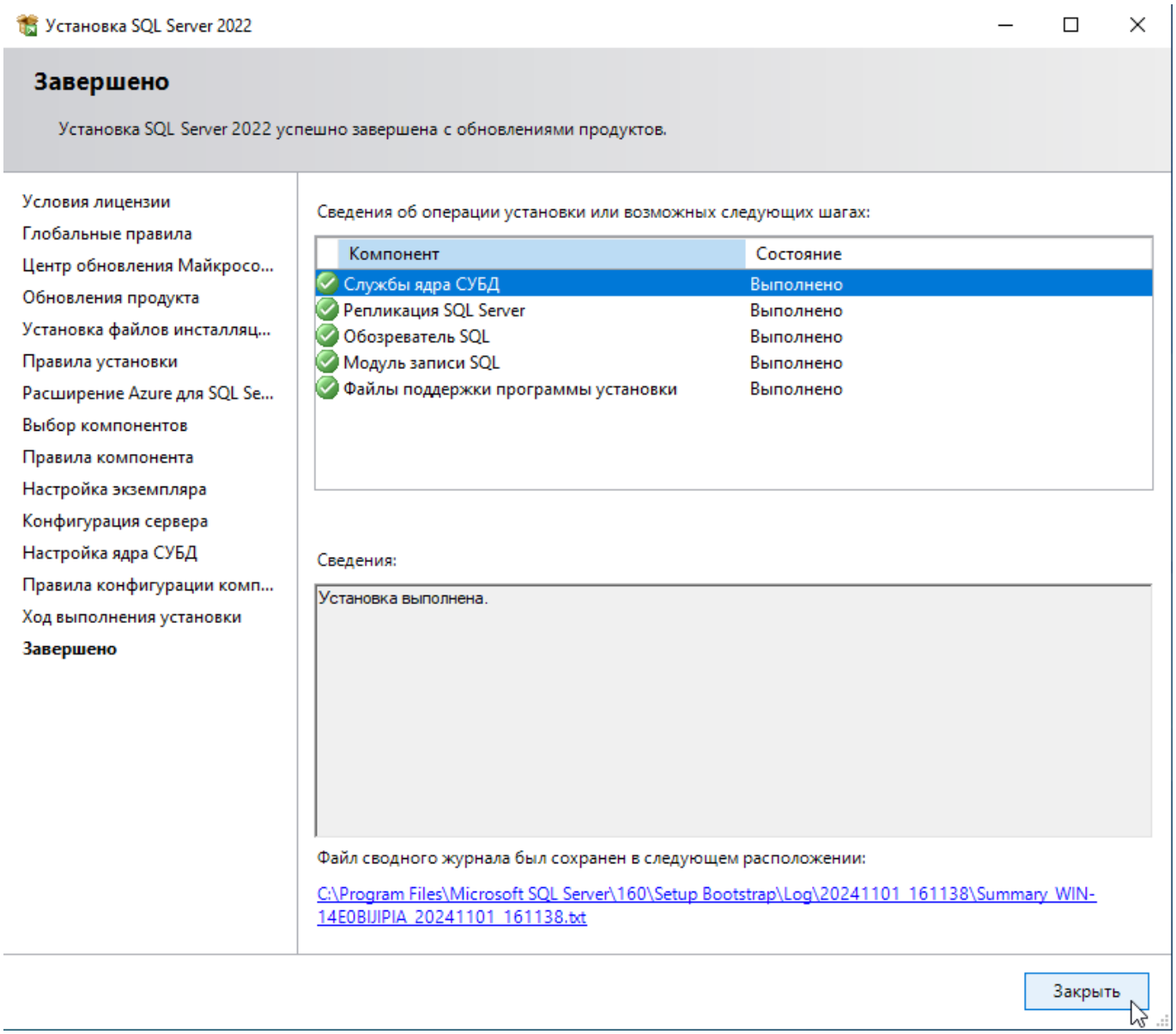


Рис. 7 – Установка MS SQL. Завершение установки

4.1.3.2. Установка СУБД PostgreSQL (вариант для автономного окружения)

Установка СУБД PostgreSQL осуществляется тривиальным способом и описывается следующими шагами:

1) получение установочных файлов PostgreSQL;
2) выбор директории для установки;
3) выбор компонентов для установки;
4) выбор директории для хранения базы данных;

5) задание пароля к базе данных;
6) задание порта;
7) выбор языка.

Во время установки рекомендуется оставить параметры по умолчанию.

4.1.4. ЦУ. ОС Linux

Перед установкой ЦУ необходимо установить и настроить СУБД. Выбранными вариантами могут быть PostgreSQL, MySQL или Microsoft SQL Server. Шаги установки будут отличаться в зависимости от выбранного дистрибутива ОС Linux. Для более детальных инструкций, выходящих за пределы данного руководства пользователя, обращайтесь в техническую поддержку ОДО «ВИРУСБЛОКАДА».

4.2. Установка продукта

Для установки программного комплекса ШХУНА используются инсталляционные пакеты:

1) `goleta_windows.msi` – локальная клиентская часть программного комплекса ШХУНА для ОС Windows;
2) `goleta_linux.run` – локальная клиентская часть программного комплекса ШХУНА для ОС Linux;
3) `goleta_cc_windows.msi` – ЦУ для ОС Windows;
4) `goleta_cc_linux.run` – ЦУ для ОС Linux.

Для удаленного варианта установки локальной клиентской части программного комплекса ШХУНА требуется иметь уже установленный ЦУ.

4.2.1. Клиентская часть программного комплекса ШХУНА. ОС Windows

4.2.1.1. Удаленная установка с помощью ЦУ

Удаленная установка клиентской части программного комплекса ШХУНА с предустановленного ЦУ на целевые компьютеры производится администратором через графический веб-интерфейс ЦУ (см. п. 4.6.13.1).

4.2.1.2. Локальная установка

После получения прав локального администратора необходимо запустить исполняемый файл `goleta_windows.msi`, входящий в комплект поставки программного комплекса ШХУНА для запуска установки клиентской части программного комплекса ШХУНА.

Процесс установки имеет интуитивно понятный графический интерфейс и не требует особого описания. При возникающих сложностях обращайтесь в техническую поддержку ОДО «ВИРУСБЛОКАДА».

4.2.2. Клиентская часть программного комплекса ШХУНА. ОС Linux

4.2.2.1. Удаленная установка с помощью ЦУ

Удаленная установка клиентов программного комплекса ШХУНА с предустановленного ЦУ на целевые компьютеры производится администратором через графический веб-интерфейс ЦУ (см. 4.6.13.1).

4.2.2.2. Локальная установка

После получения прав суперпользователя необходимо запустить исполняемый файл `goleta_linux.run`, входящий в комплект поставки программного комплекса ШХУНА для запуска установки клиентской части программного комплекса ШХУНА.

В процессе установки в консоль будут выводиться уведомления различного уровня нотификации:

1) `INF` – информационные сообщения;
2) `WARN` – предупреждения мастера установки;
3) `ERR` – ошибки установки.

Установка продукта производится в директорию `/opt/vba`.

После завершения установки служба программного комплекса ШХУНА регистрируется в `systemd` для автоматического запуска при старте системы.

Контроль над работой программного комплекса ШХУНА можно осуществлять

по журналам программного комплекса ШХУНА (доступны в графическом интерфейсе пользователя программного комплекса ШХУНА).

4.2.3. ЦУ. ОС Windows

Запустите на исполнение установочный файл ЦУ (рис. 8). Нажмите кнопку **Далее** для перехода к следующему шагу установки.

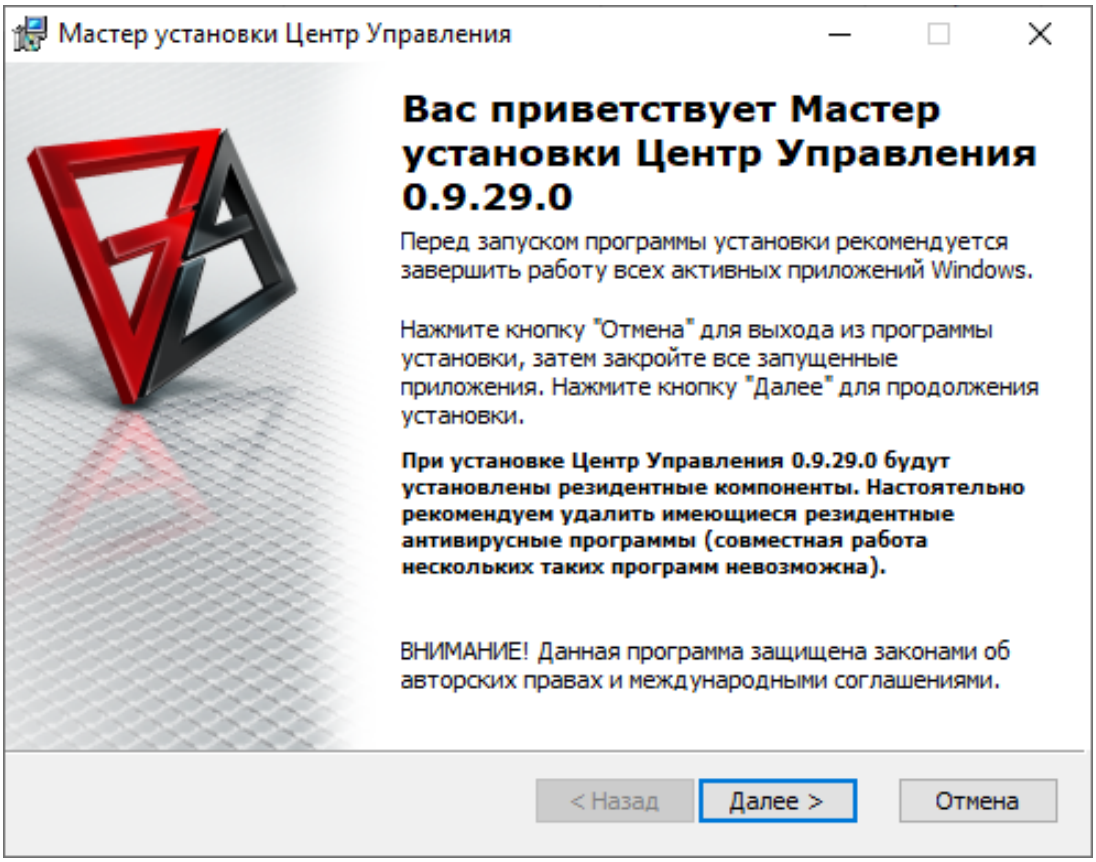


Рис. 8 – ЦУ. Мастер установки. ОС Windows

Укажите настройки SQL-сервера и базы данных, с которой будет работать приложение.

Для MSSQL настройки будут следующими:

- Провайдер сервера SQL: MSSQL;
- Имя сервера SQL: local;
- Имя пользователя: **sa**;
- Пароль пользователя: пароль, указанный при установке MSSQL;
- Имя базы данных: **vbaccdb**.

В случае PostgreSQL (рис. 9):

– Провайдер сервера SQL: PostgreSQL;
– Имя сервера SQL: localhost;
– Имя пользователя: **postgres**;
– Пароль пользователя: пароль, указанный при установке PostgreSQL;
– Имя базы данных: **vbaccdb**.

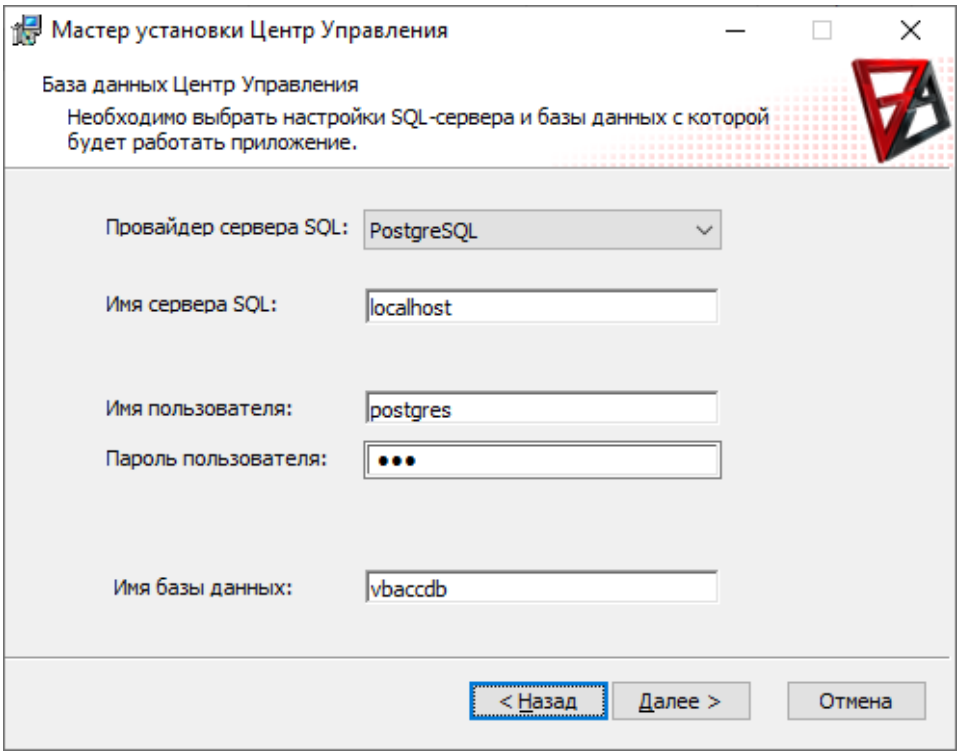


Рис. 9 – ЦУ. Мастер установки.
Выбор СУБД. PostgreSQL. ОС Windows

Затем нажмите кнопку **Далее**. Для запуска установки нажмите кнопку **Установить**.

Дождитесь окончания установки. Для завершения установки нажмите кнопку **Готово**.

4.2.4. ЦУ. ОС Linux

Перейдите в директорию с установщиком ЦУ (`goleta_cc_linux.run`) и выполните последовательно следующие команды:

`sudo chmod a+x ./goleta_cc_linux.run` либо

```
sudo chmod 777 ./goleta_cc_linux.run
```

```
sudo ./goleta_cc_linux.run install либо
sudo ./goleta_cc_linux.run
```

После запуска мастера установки управление установкой осуществляется следующим образом. Для редактирования параметров по умолчанию нужно сначала нажать клавиши управления курсором «←/→», иначе предлагаемые значения по умолчанию исчезнут.

Для удаления данных используется клавиша «Backspace», для перемещения по значениям параметров – клавиши управления курсором «←/→». Клавиша «Del» прерывает всю установку.

Директорией установки ЦУ предполагается путь «/opt/vbacc», СУБД по выбору (перемещение на пункт выбора СУБД осуществляется с помощью клавиш управления курсором «←/→»), в качестве имени экземпляра базы данных – значение **«localhost»**, имя базы данных – **«vbaccdb»**, имя для входа – **«sa»**, пароль к ней – **«1234qwer!»**.

Для первого входа в графический интерфейс ЦУ в адресной строке браузера используйте значение **«localhost»**, а в качестве данных авторизации: **«admin/1234qwer!»** (роль Администратор) и **«observer/asdf4321$»** (роль Наблюдатель).

4.3. Исполнение клиентской части программного комплекса ШХУНА

4.3.1. Активация продукта

После установки продукта необходимо обновить информацию о лицензии, предоставив регистрационный ключ. Для этого необходимо запустить продукт (ярлык программного комплекса ШХУНА доступен в меню окружения рабочего стола) и обновить регистрационный ключ с помощью кнопки в интерфейсе **Диспетчера** (рис. 12).

Примечание. Интерфейс графической части программного комплекса ШХУНА может иметь некоторые отличия (в зависимости от версии продукта и целевой ОС). Например, интерфейс раздела **Диспетчер** в ОС Windows может представлять собой окно, отрисованное средствами Microsoft GDI+ (рис. 10). Также

необходимо отметить различие в системных диалоговых окнах выбора (например, при выборе файлов – см. рис. 11), форматах задания путей к файлам и директориям, допустимых символах и т.д.

Для удобства пользователя функции, которые предоставляют модули программного комплекса ШХУНА, сгруппированы согласно UX/UI, выработанными на основании типичных задач, встречающихся во время эксплуатации комплекса, а не согласно их принадлежности модулям программного комплекса ШХУНА.

Соответствие разделов представленного графического интерфейса клиентской части модулям программного комплекса ШХУНА в ОС Windows:

1) **Диспетчер** – модуль взаимодействия;
2) **Проактивная защита** – модуль управления доступом;
3) **Антивирусный сканер** – модуль контроля данных;
4) **Монитор** – модуль контроля данных;
5) **Управление доступом** – модуль управления доступом;
6) **Межсетевой экран** – модуль межсетевого экранирования;
7) **Карантин** – модуль контроля данных;
8) **Целостность** – модуль неизменности;
9) **Модуль удаления** – модуль удаления.

Соответствие разделов представленного графического интерфейса клиентской части модулям программного комплекса ШХУНА в ОС Linux:

1) **Диспетчер** – модуль взаимодействия (в части выдачи общей информации о комплексе, выбора лицензии, настройках авторизации, предоставления настроек для ЦУ, обновления продукта и учета действий оператора графического интерфейса);
2) **Планировщик** – модуль взаимодействия (в версии графического интерфейса клиентской части программного комплекса ШХУНА для ОС Windows может находиться в разделе **Диспетчер** – вкладка **Планировщик**);
3) **Проактивная защита** – модуль управления доступом (в части защищаемых объектов и аудита);
4) **Пользователи** – модуль управления доступом (в части фильтрации действий пользователя);

5) **Антивирусный сканер** – модуль контроля данных;
6) **Монитор** – модуль контроля данных;
7) **Устройства** – модуль управления доступом;
8) **Принтеры** – модуль управления доступом (в части управления принтерами);
9) **Межсетевой экран** – модуль межсетевого экранирования;
10) **Карантин** – модуль контроля данных;
11) **Целостность** – модуль неизменности;
12) **Шредер** – модуль удаления.

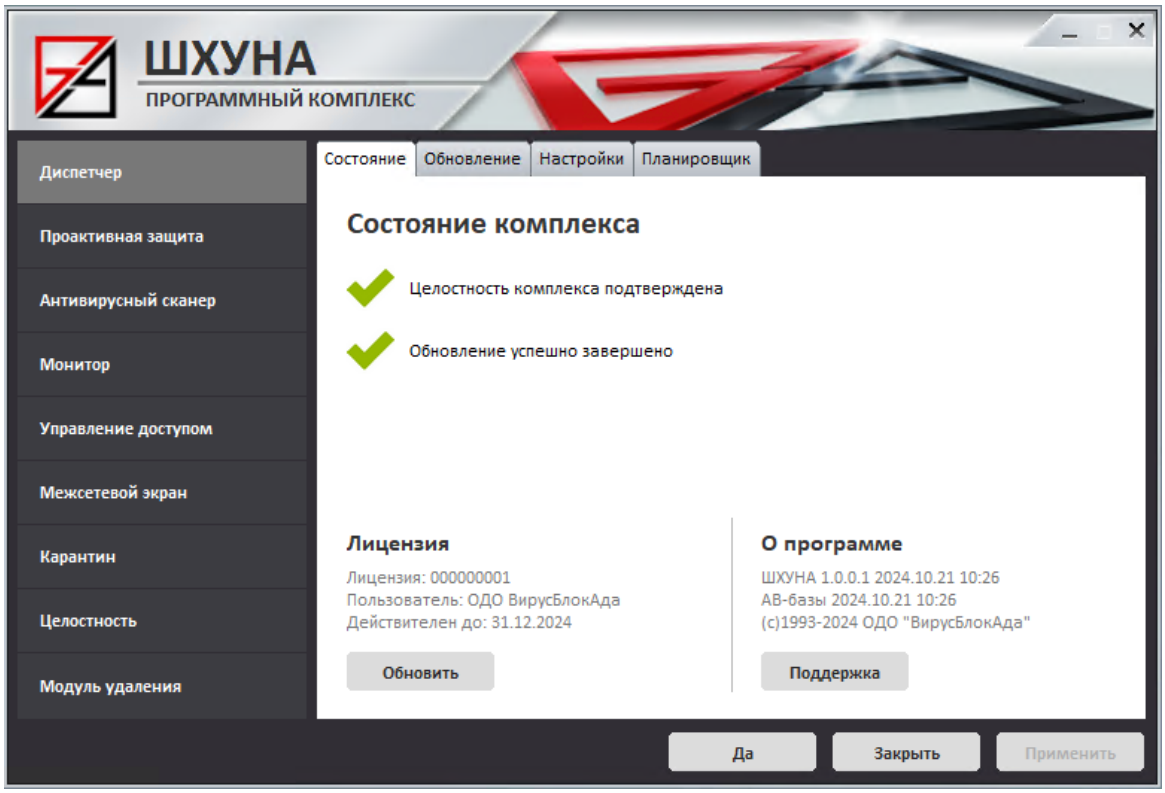


Рис. 10 – Интерфейс клиентской части программного комплекса ШХУНА. ОС Windows

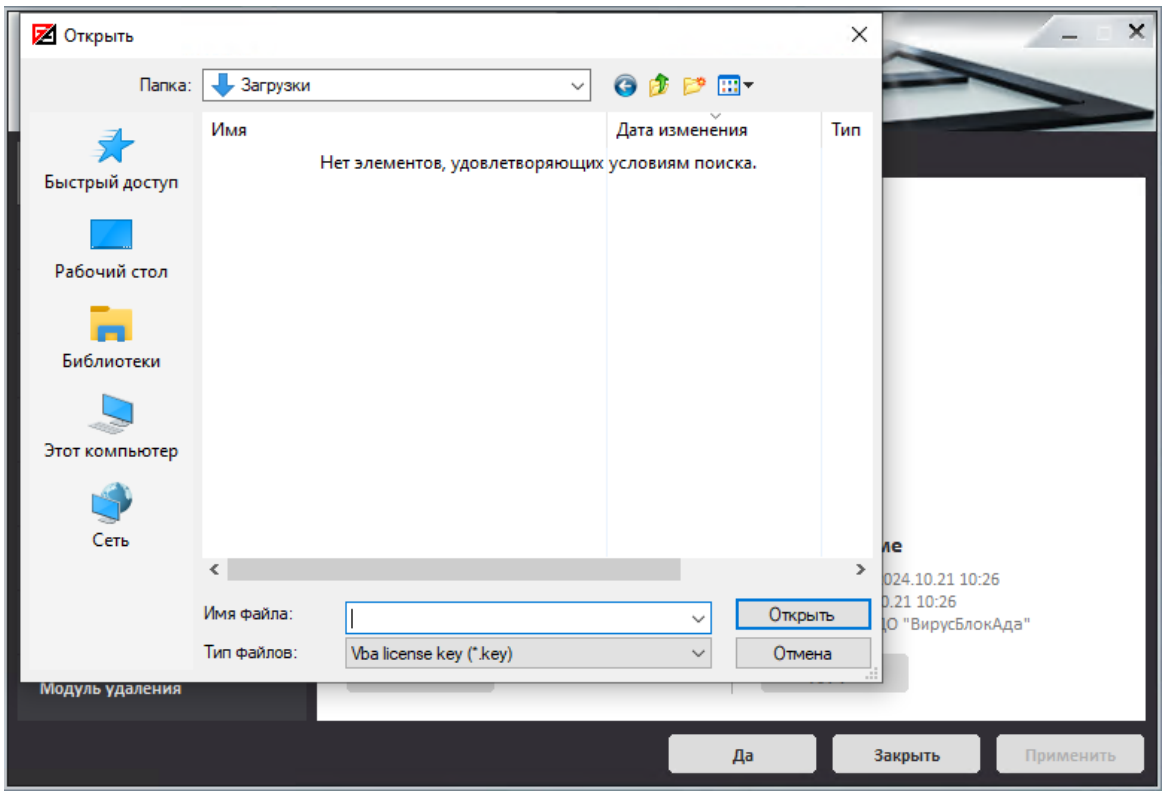


Рис. 11 – Обновление файла лицензии программного комплекса ШХУНА. ОС Windows

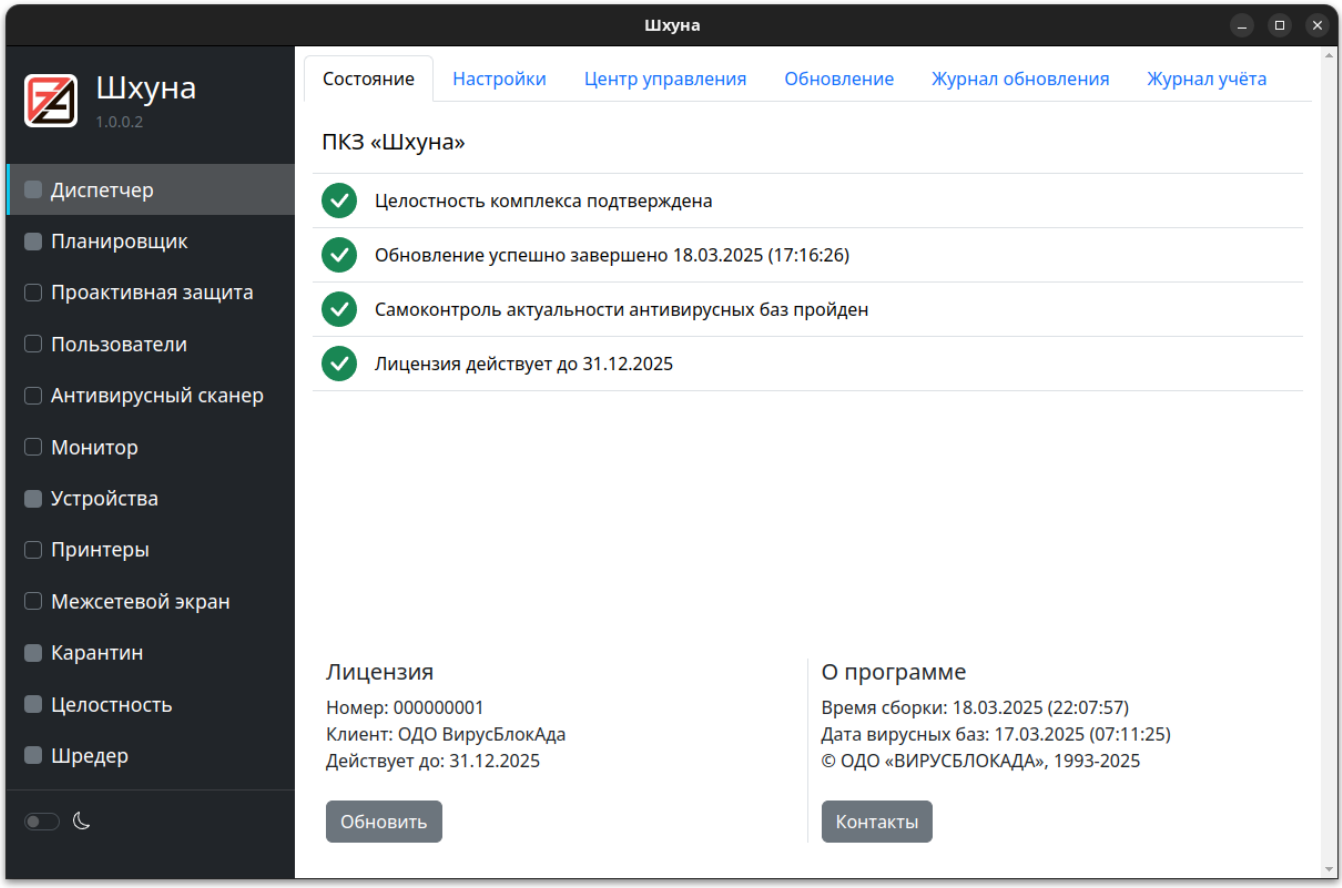


Рис. 12 – Интерфейс клиентской части программного комплекса ШХУНА. ОС Linux

Окно выбора лицензии показано на (рис. 13).

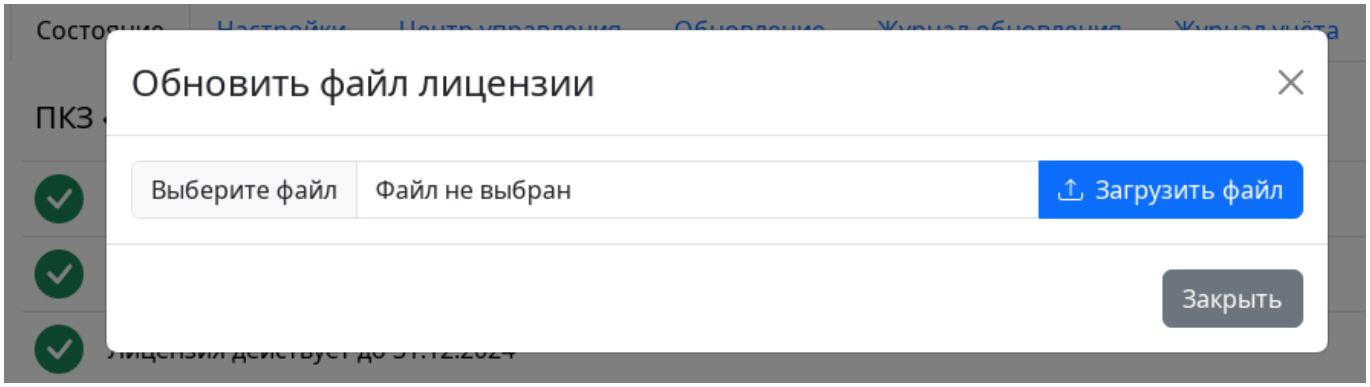


Рис. 13 – Обновление файла лицензии программного комплекса ШХУНА. ОС Linux

После выбора файла лицензии программный комплекс ШХУНА перейдет в полнофункциональный режим, о чем будет свидетельствовать соответствующая надпись в разделе **Диспетчер** (рис. 14, рис. 15).

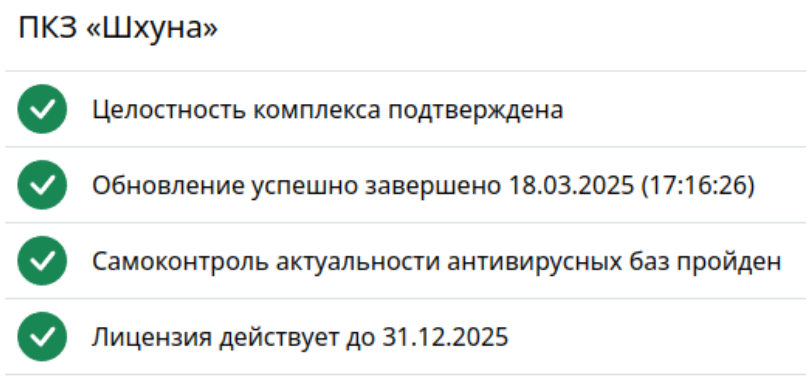


Рис. 14 – Диспетчер. Полнофункциональный режим

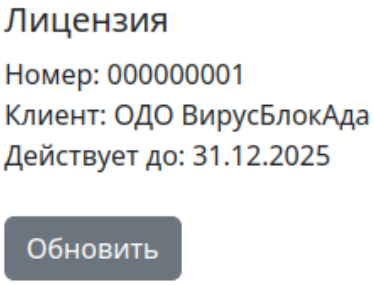


Рис. 15 – Диспетчер. Информация о лицензии

4.4. Работа клиентской части программного комплекса ШХУНА

Интерфейс клиентской части программного комплекса ШХУНА представляет собой универсальное графическое оконное приложение, которое позволяет получать доступ к элементам клиентской части программного комплекса ШХУНА, а также изменять его настройки.

4.4.1. Раздел Диспетчер

Раздел **Диспетчер** клиентской части программного комплекса ШХУНА включает следующие вкладки:

1) **Состояние**;
2) **Настройки**;
3) **Центр управления**;
4) **Обновление**;
5) **Журнал обновления**;
6) **Журнал учета**.

Вкладка **Состояние** (рис. 16) содержит информацию о регистрационном ключе, состоянии программного комплекса ШХУНА, дате и статусе его обновления.

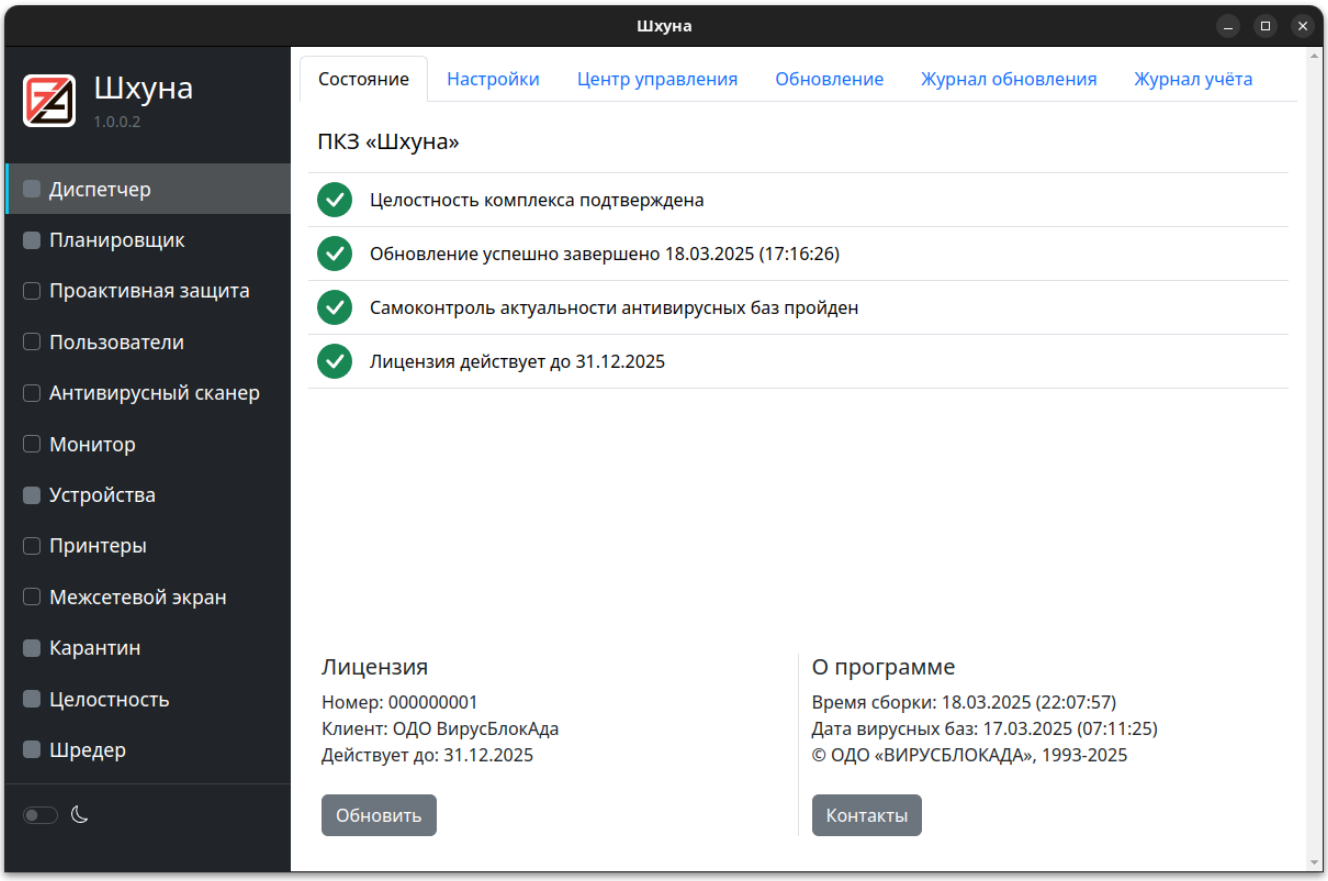


Рис. 16 – Диспетчер. Состояние

На вкладке находятся кнопки обновления регистрационного ключа (рис. 17) и получения контактной информации ОДО «ВИРУСБЛОКАДА» (рис. 18).

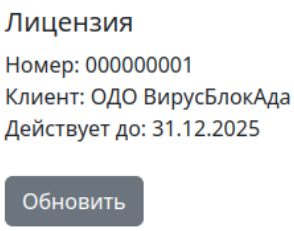


Рис. 17 – Диспетчер. Состояние. Лицензия

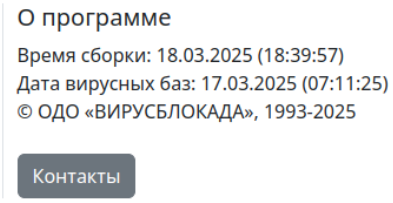


Рис. 18 – Диспетчер. Состояние. О программе

Для того, чтобы определить результат выполнения самоконтроля актуальности антивирусных баз, содержащих набор признаков известного ВПО, в клиентской части программного комплекса ШХУНА для ОС Linux предназначается информационная секция **Самоконтроль актуальности антивирусных баз пройден** (рис. 19), если результат положительный, или **Рекомендуется обновить ваши антивирусные базы** (рис. 20), в противном случае.

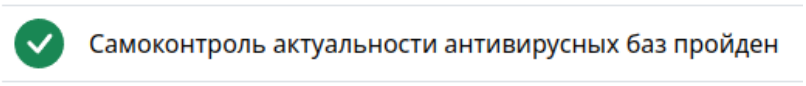


Рис. 19 – Самоконтроль актуальности антивирусных баз пройден

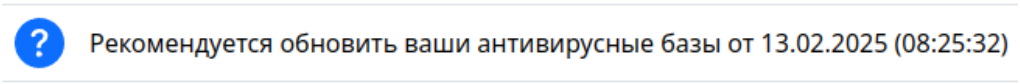


Рис. 20 – Рекомендация по обновлению антивирусных баз в ОС Linux

В клиентской части программного комплекса ШХУНА для ОС Windows результат выполнения самоконтроля актуальности антивирусных баз может отслеживаться визуально с помощью соответствующего уведомления (рис. 21). Если результат выполнения самоконтроля – положительный, то уведомление не отображается.

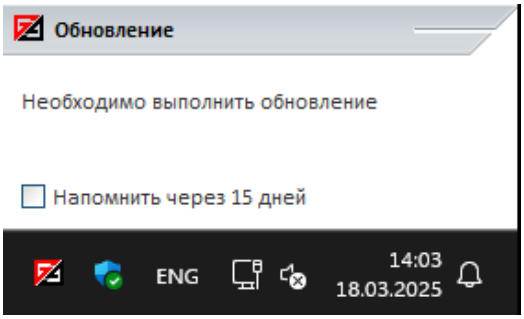


Рис. 21 – Рекомендация по обновлению антивирусных баз в ОС Windows

Примечание. Для непосредственного обновления антивирусных баз до актуального состояния *в автоматическом режиме* предназначена задача **Обновить антивирусные базы**, выполняемая по конфигурируемому расписанию. Регулярное выполнение задачи настраивается в разделе **Планировщик** (см. п. 4.4.2) графического интерфейса клиентской части программного комплекса ШХУНА, или в ЦУ – с помощью выдачи задачи **Настроить планировщик** (см. п. 4.6.2.19).

Вкладка **Настройки** (рис. 22) предназначена для выбора языка интерфейса и включения парольного доступа к интерфейсу программного комплекса ШХУНА.

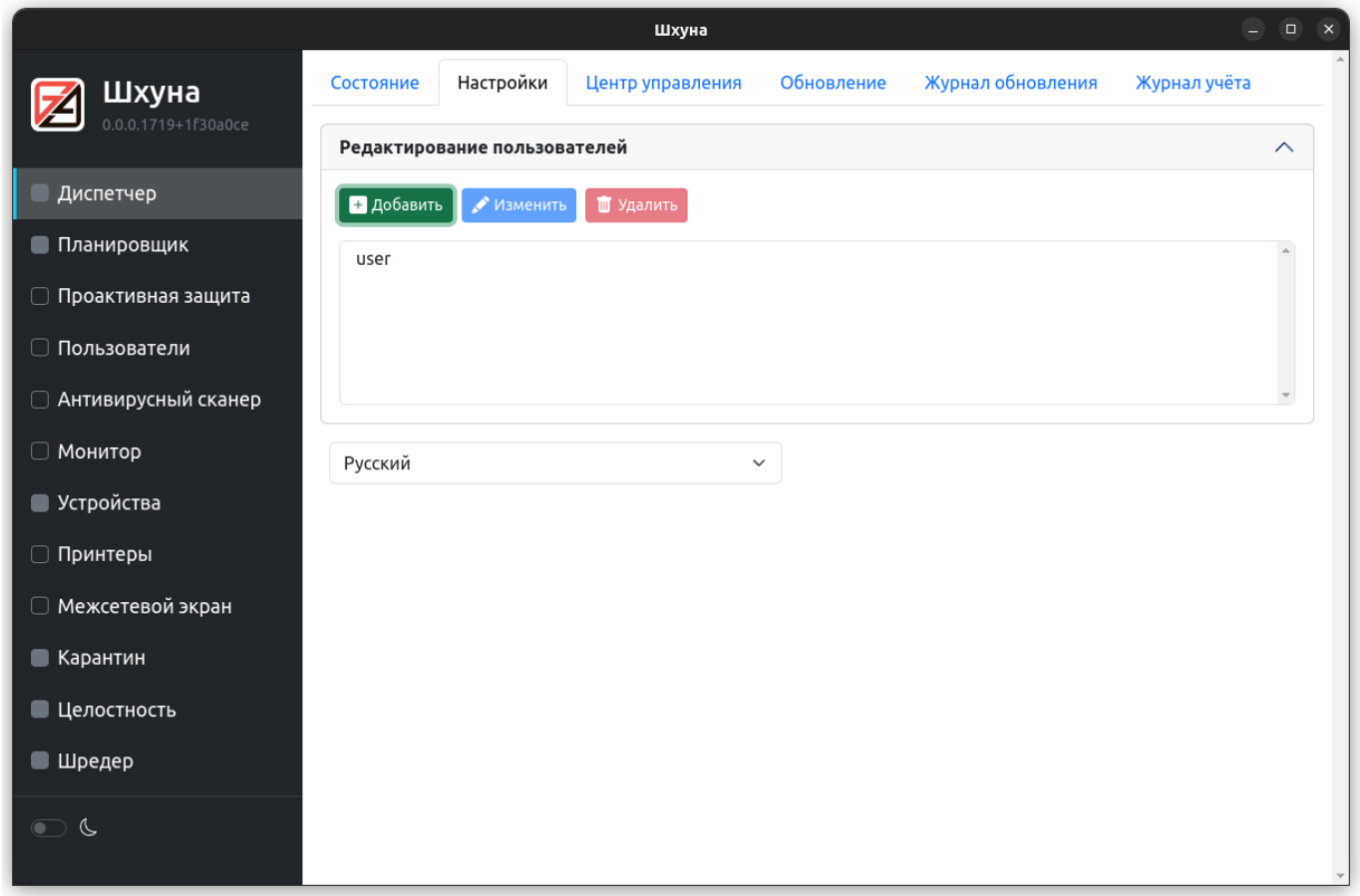


Рис. 22 – Диспетчер. Настройки

Для доступа в интерфейс может быть создано несколько учетных записей с различными парами **имя пользователя : пароль**. После задания имени пользователя и пароля при каждой попытке открытия окна программного комплекса ШХУНА будет демонстрироваться окно запроса имени пользователя и пароля (рис. 23).

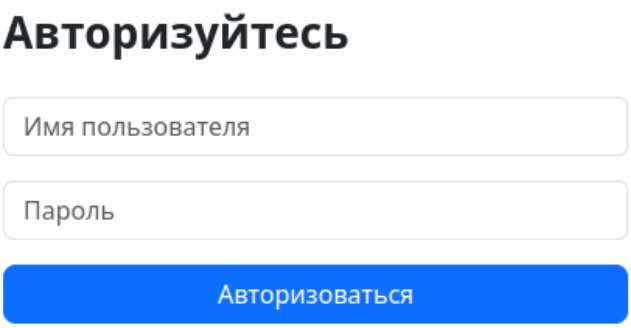


Рис. 23 – Авторизация

В случае ввода неверной комбинации имени пользователя и пароля пользователю будет продемонстрировано уведомление (рис. 24). В случае использования ЦУ соответствующее событие будет отображено на странице **События**.

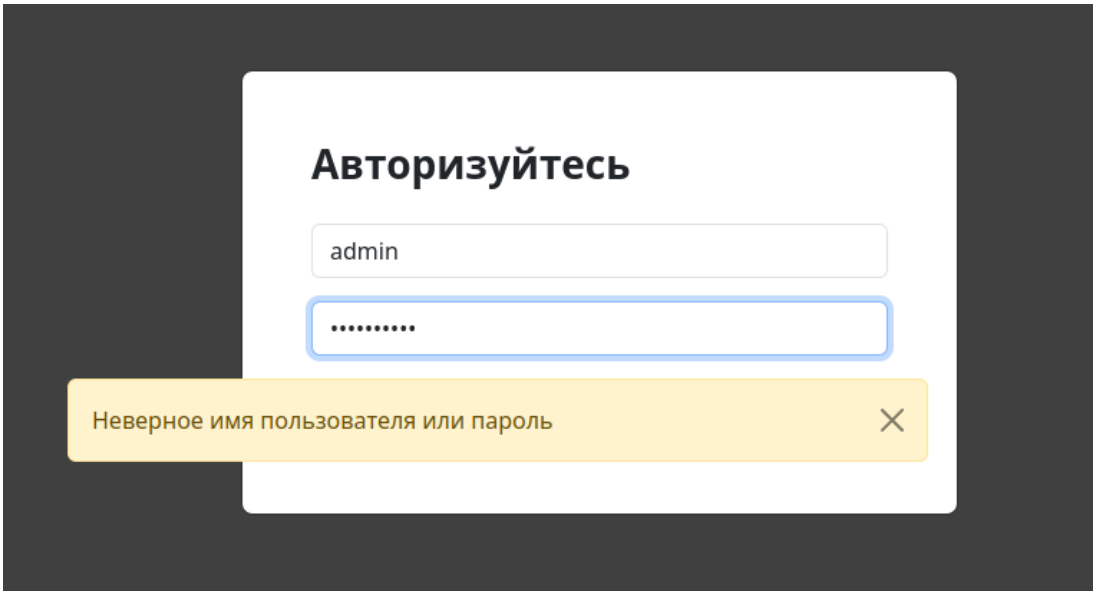


Рис. 24 – Авторизация. Неверный логин или пароль

Вкладка **Центр Управления** (рис. 25) предназначена для ручного подключения клиентской части программного комплекса ШХУНА к ЦУ.

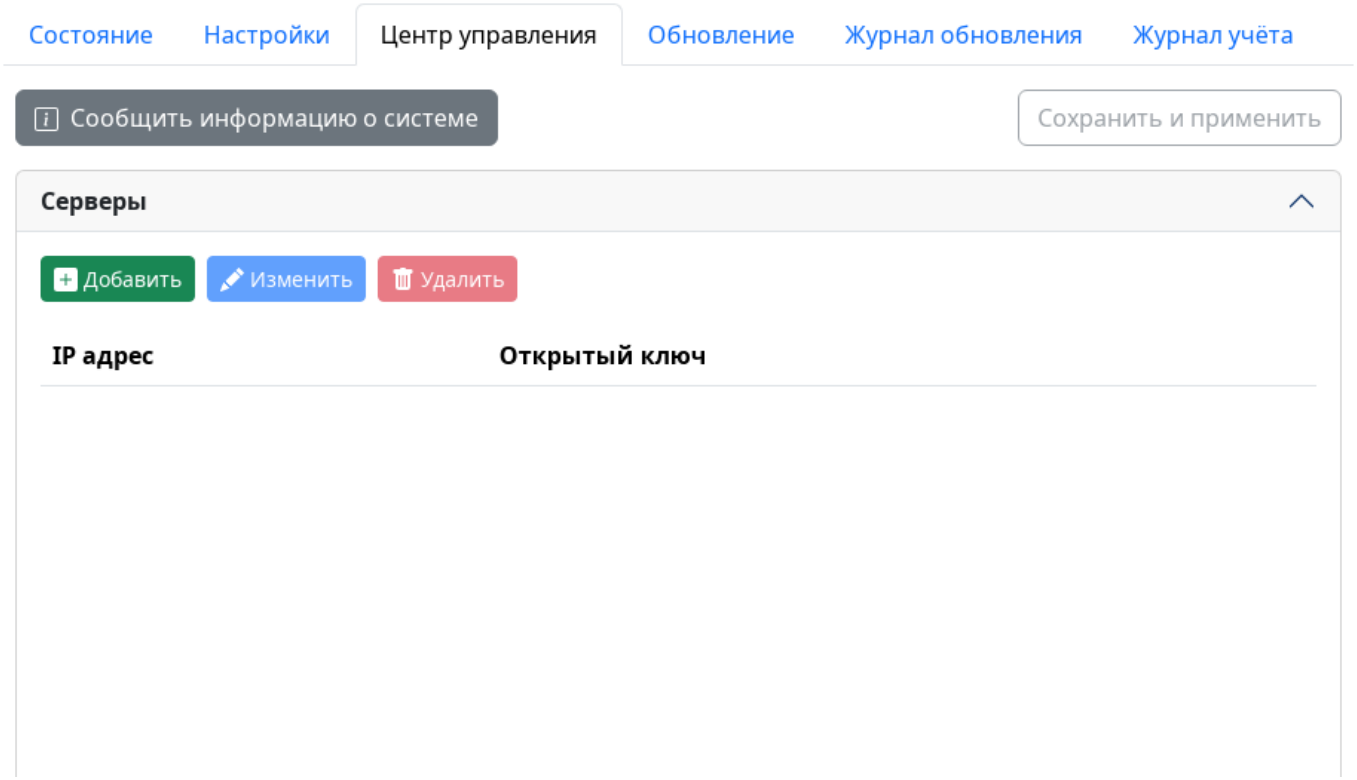


Рис. 25 – Диспетчер. Центр управления

На данной вкладке расположена группа элементов **Серверы**, состоящая из списка пар **IP-адрес: Открытый ключ** и кнопок: **Добавить**, **Изменить**, **Удалить**, а также кнопок **Сообщить информацию о системе**, **Сохранить и применить**.

Для ручного подключения клиентской части программного комплекса ШХУНА к ЦУ необходимо нажать кнопку **Добавить** в группе элементов **Серверы**. После нажатия на кнопку будет продемонстрировано диалоговое окно добавления сервера ЦУ в список (рис. 26).

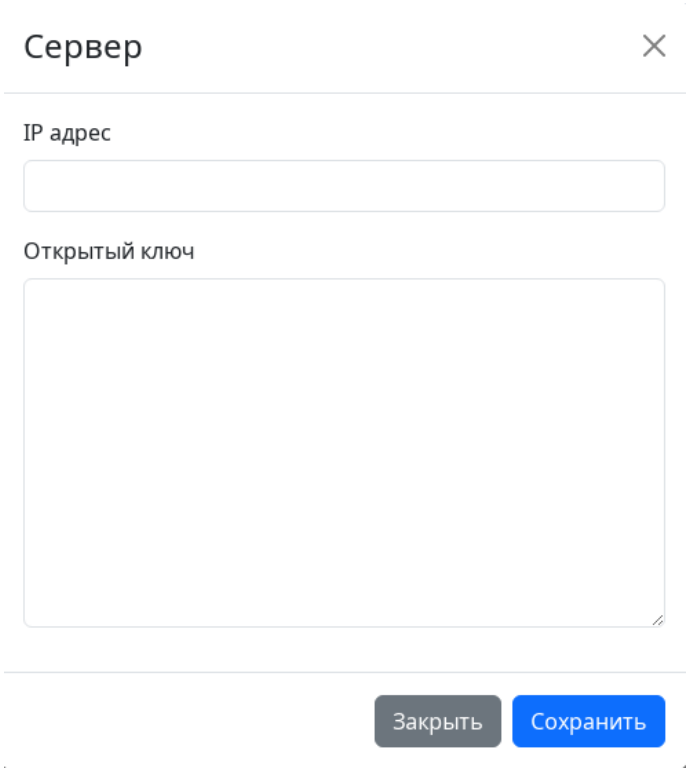


Рис. 26 – Диспетчер. Центр управления. Окно добавления сервера

В данном окне обязательны для заполнения следующие поля: **IP-адрес** сервера, где установлен ЦУ, и **Открытый ключ** для подписи отправляемых пакетов. Текстовое значение для поля **Открытый ключ** представлено в ЦУ под именем **Публичный ключ для подписи пакетов** (см. п. 4.6.14.1).

После добавления информации о сервере необходимо нажать кнопку **Сохранить и применить**. Кнопка **Сообщить информацию о системе** отправляет пакет с информацией о системе ЦУ.

Вкладка **Обновление** (рис. 27) предназначена для задания настроек обновления модулей программного комплекса ШХУНА и антивирусных баз. На вкладке находится:

1) кнопка **Запустить** (рис. 28) – запускает обновление комплекса и/или антивирусных баз;
2) кнопка **Сохранить и применить** – сохраняет настройки изменения;
3) группа элементов **Путь обновления**, состоящая из кнопок **Добавить**, **Изменить**, **Удалить**, **Вверх**, **Вниз** и списка ресурсов обновления;
4) ресурс обновления – строка URL, ведущая на FTP или HTTP-ресурс.

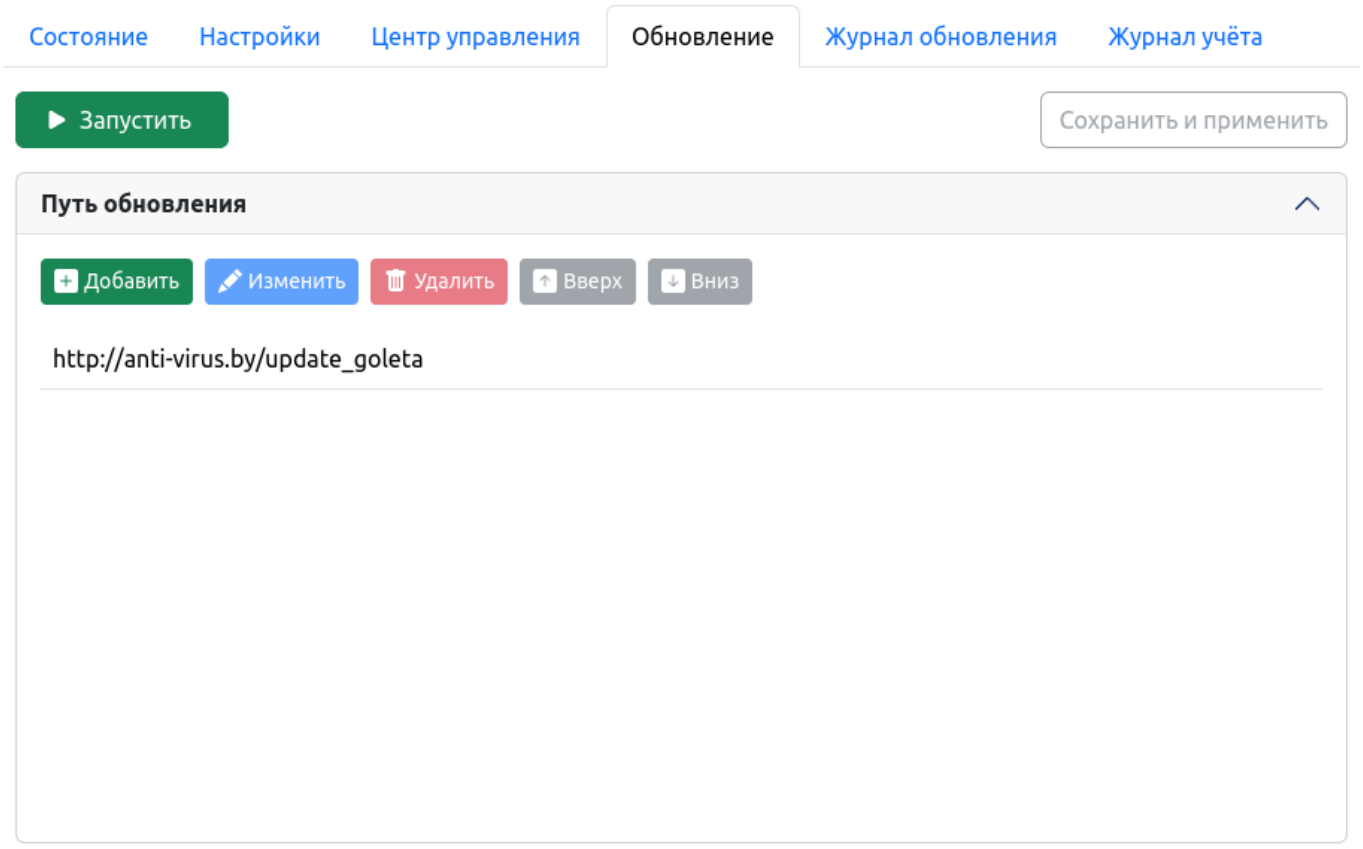


Рис. 27 – Диспетчер. Обновление

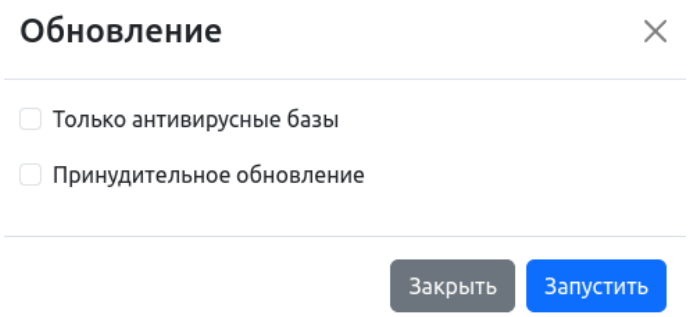


Рис. 28 – Диспетчер. Обновление. Параметры запуска

Для добавления ресурса обновления необходимо нажать кнопку **Добавить**. После нажатия будет продемонстрировано диалоговое окно добавления ресурса (рис. 29)

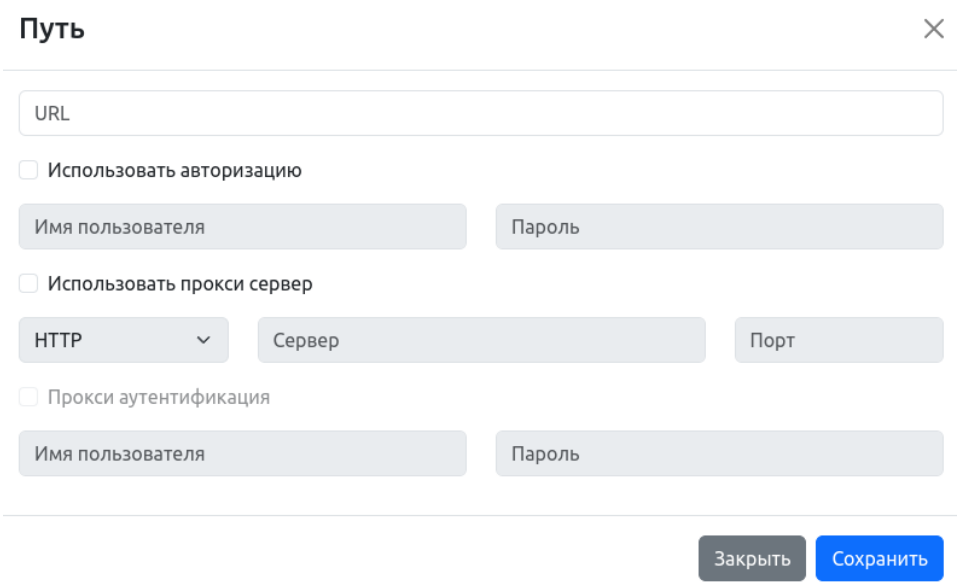


Рис. 29 – Диспетчер. Обновление. Путь к ресурсу обновления

При добавлении ресурса необходимо указать его URL. При необходимости есть возможность настроить авторизацию и прокси-сервер (HTTP/HTTPS), используемый для загрузки файлов.

Попытки загрузки файлов обновлений происходят согласно порядку, в котором они объявлены в списке ресурсов, который возможно изменить с помощью кнопок **Вверх** и **Вниз**.

На вкладках **Журнал обновления** (рис. 30) и **Журнал учета** (рис. 31) отображаются события, связанные с обновлением комплекса и авторизацией пользователей в интерфейсе программного комплекса ШХУНА.

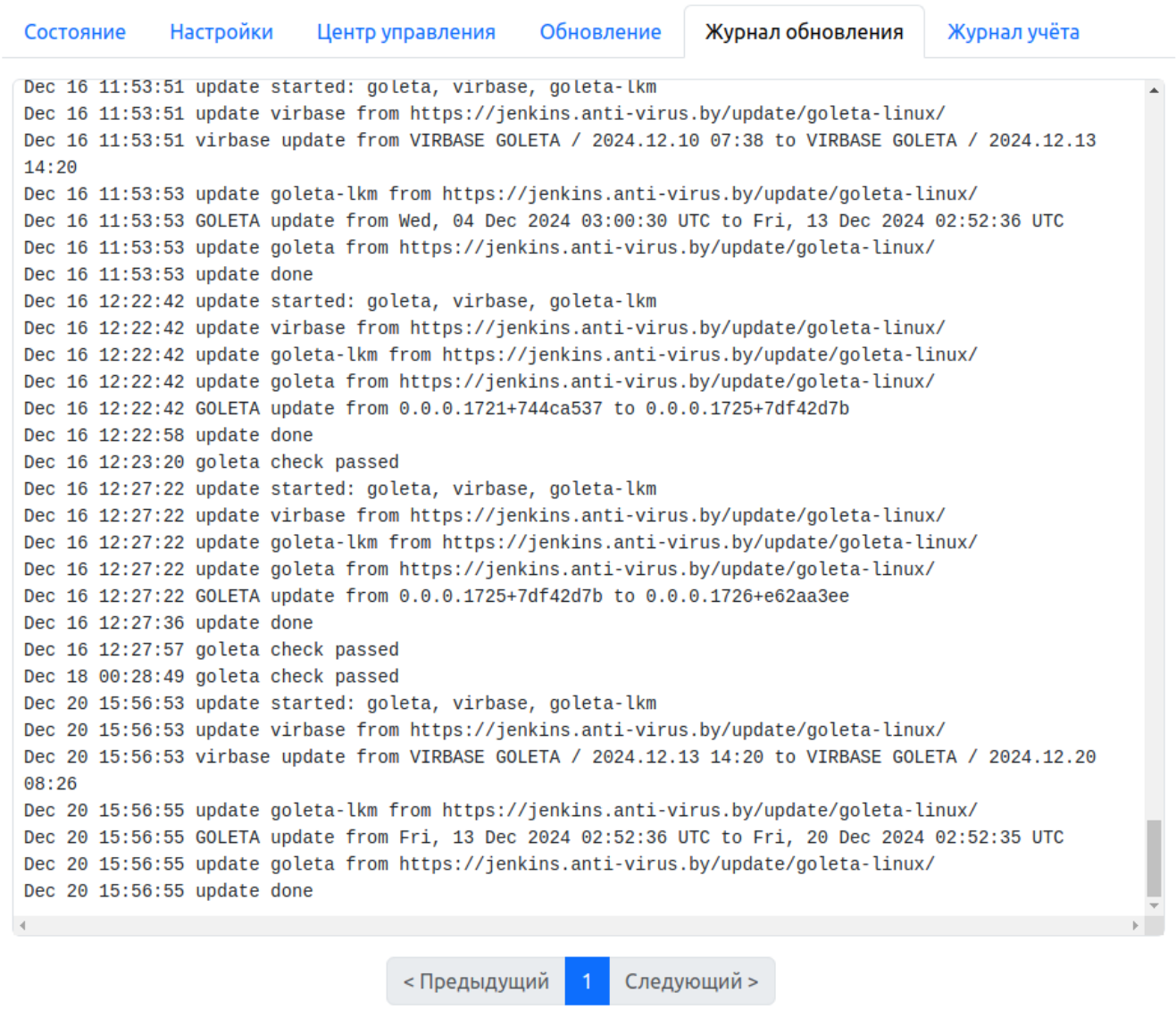


Рис. 30 – Диспетчер. Журнал обновления

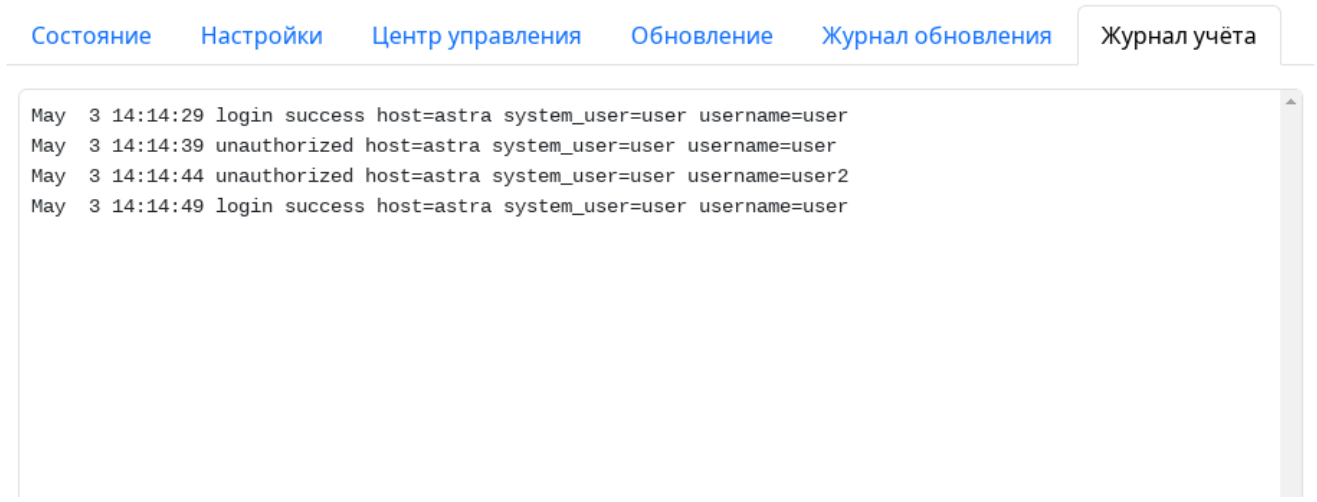


Рис. 31 – Диспетчер. Журнал учета

4.4.2. Раздел Планировщик

Раздел **Планировщик** предназначен для настройки выполнения программного комплекса ШХУНА задач по расписанию.

На вкладке **Планировщик** (рис. 32) расположены группа элементов **Таблица выдачи заданий**, состоящая из списка задач, кнопок **Добавить**, **Изменить** и **Удалить**, и кнопка **Сохранить и применить**.

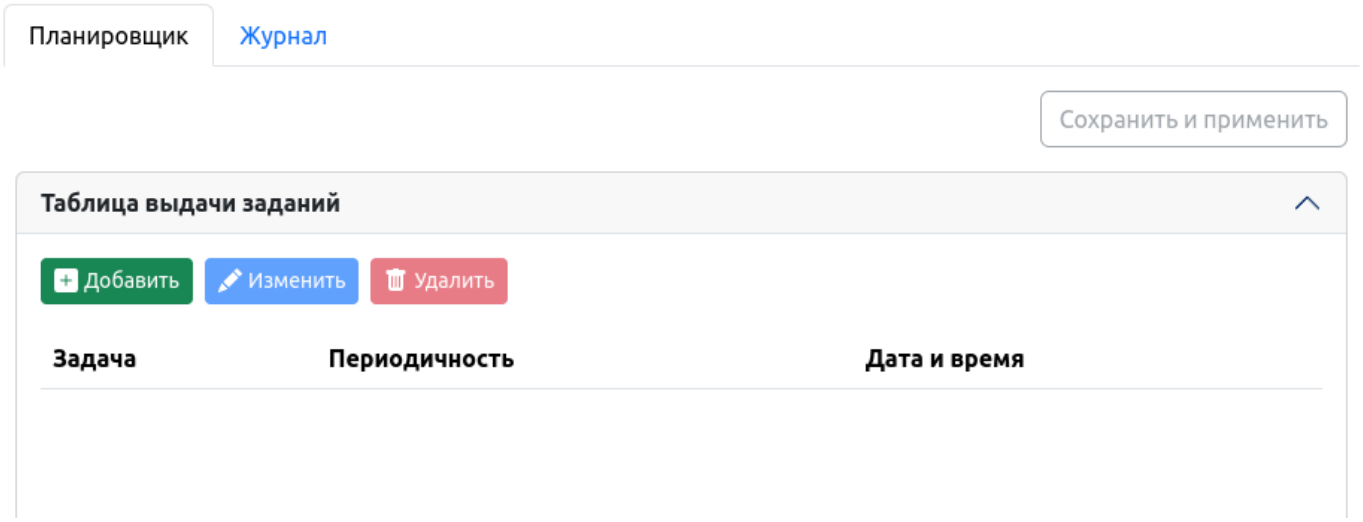


Рис. 32 – Планировщик. Таблица выдачи заданий

Нажатие кнопки **Добавить** показывает диалоговое окно добавления задачи и выбора настроек запуска (рис. 33).

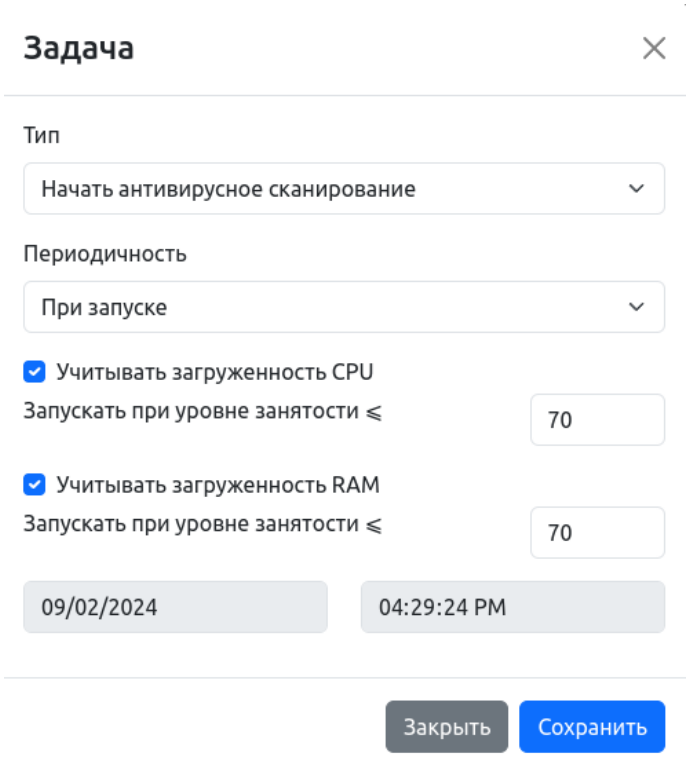


Рис. 33 – Планировщик. Добавление задачи

Перечень задач, доступных для добавления в расписание, изображен на рис. 34.

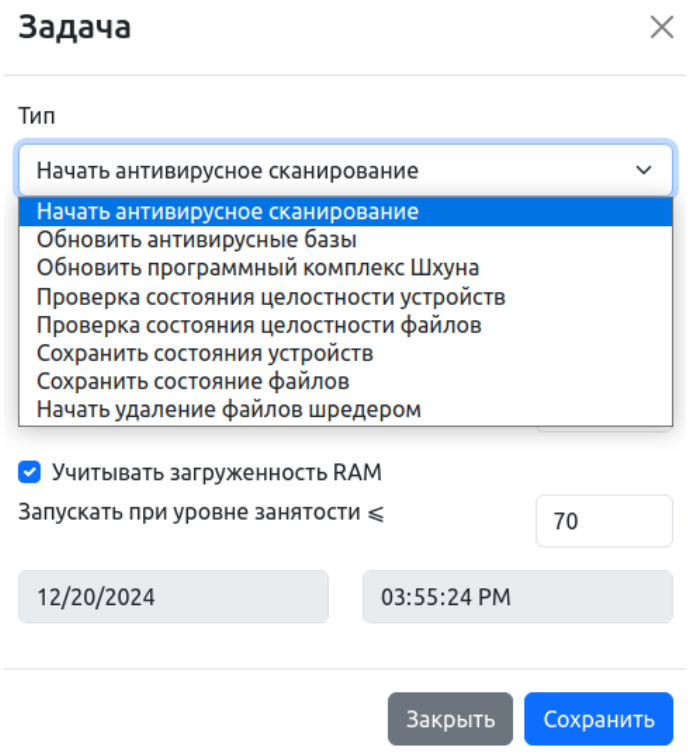


Рис. 34 – Планировщик.Тип задачи

Возможные типы периодичности показаны на рис. 35.

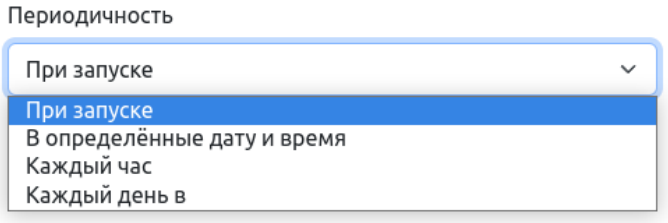


Рис. 35 – Планировщик. Периодичность задачи

При запуске задач возможен учет загруженности СВТ (CPU, RAM) с установленным программного комплекса ШХУНА. **Учитывать загруженность CPU** и **Учитывать загруженность RAM** включают соответствующие опции **Планировщика**. В текстовом поле **Запускать при уровне занятости** настраиваются максимальные значения загруженности, при которых будет запущена задача.

На вкладке **Журнал** (рис. 36) отображаются события, сгенерированные при запуске задач **Планировщика**.

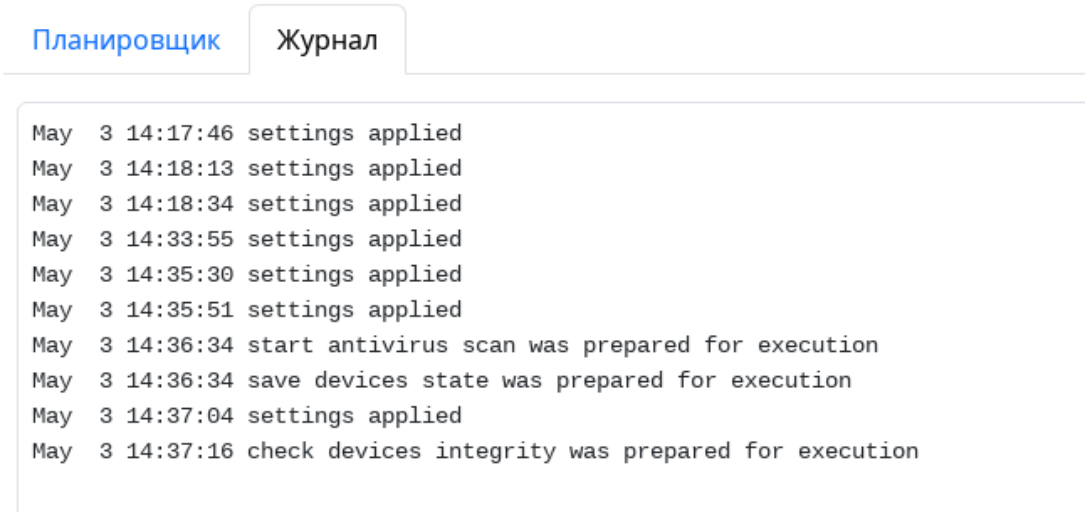


Рис. 36 – Планировщик. Журнал

4.4.3. Раздел Проактивная защита

Раздел **Проактивная защита** включает следующие вкладки:

1) **Защищаемые объекты**;
2) **Аудит**;
3) **Журнал**;
4) **События журнала**.

Вкладка **Защищаемые объекты** (рис. 37) предназначена для задания глобальных

правил Проактивной защиты программного комплекса ШХУНА. Глобальные правила распространяются на всех пользователей ОС СВТ. Правила по умолчанию выключены.

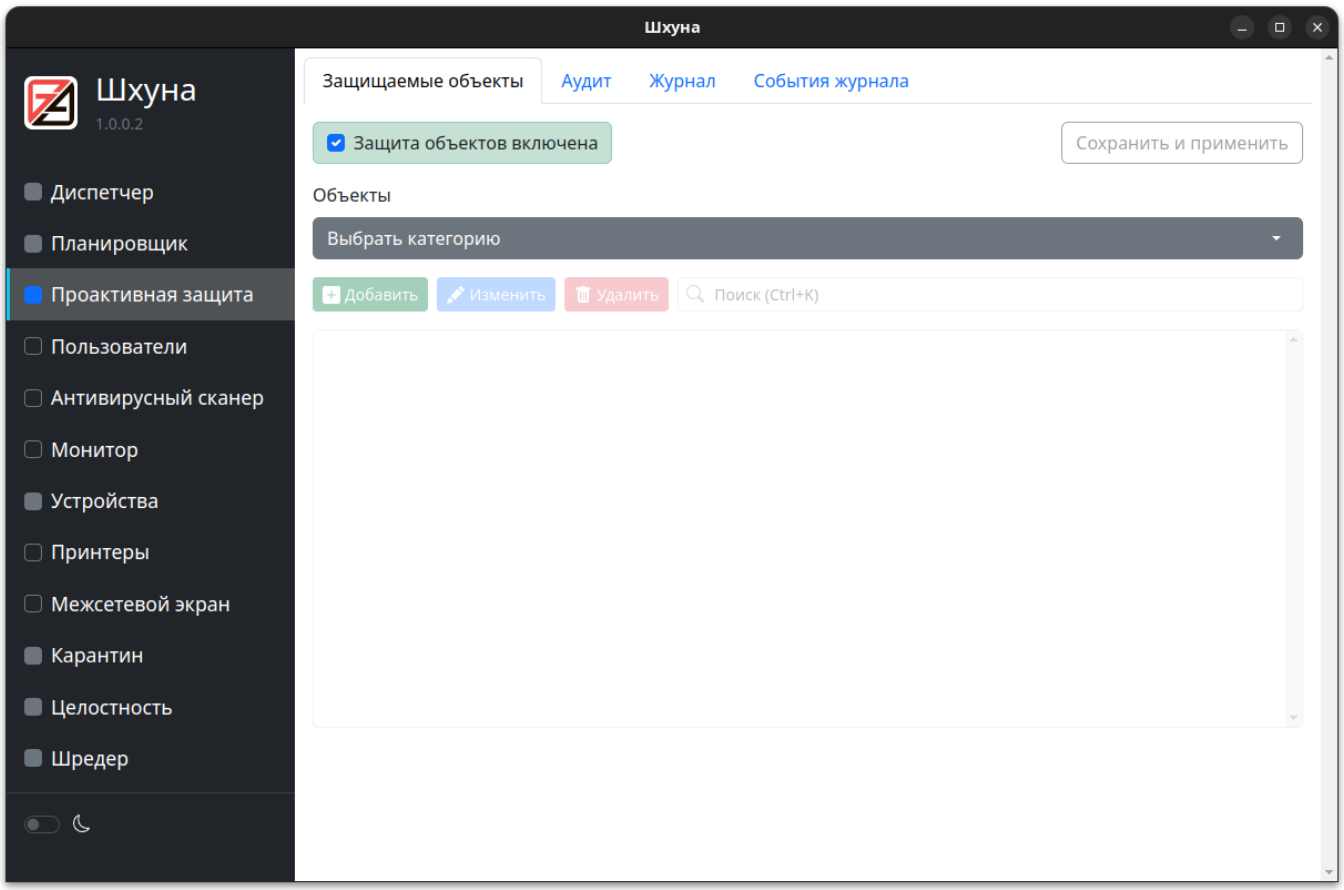


Рис. 37 – Проактивная защита. Защищаемые объекты

На вкладке расположено меню выбора типа объекта глобальных правил, список объектов одного типа, кнопки **Добавить**, **Удалить** и **Применить**.

Глобальные правила **Проактивной защиты** могут содержать следующие элементы (рис. 38):

1) **Защищенные директории** – директории, доступ к которым должен быть запрещен для всех пользователей СВТ;
2) **Защищенные файлы** – файлы, открытие которых на чтение/запись должно быть запрещено для всех пользователей СВТ;
3) **Директории (только чтение)** – директории, запись в которые должна быть запрещена для всех пользователей СВТ;

4) **Файлы (только чтение)** – файлы, открытие которых на запись должно быть запрещено для всех пользователей СВТ;
5) **Исключенные директории** – поддиректории защищаемых директорий, к которым должен быть предоставлен доступ всем пользователям СВТ;
6) **Исключенные файлы** – файлы в защищенных директориях, к которым должен быть предоставлен доступ всем пользователям СВТ.

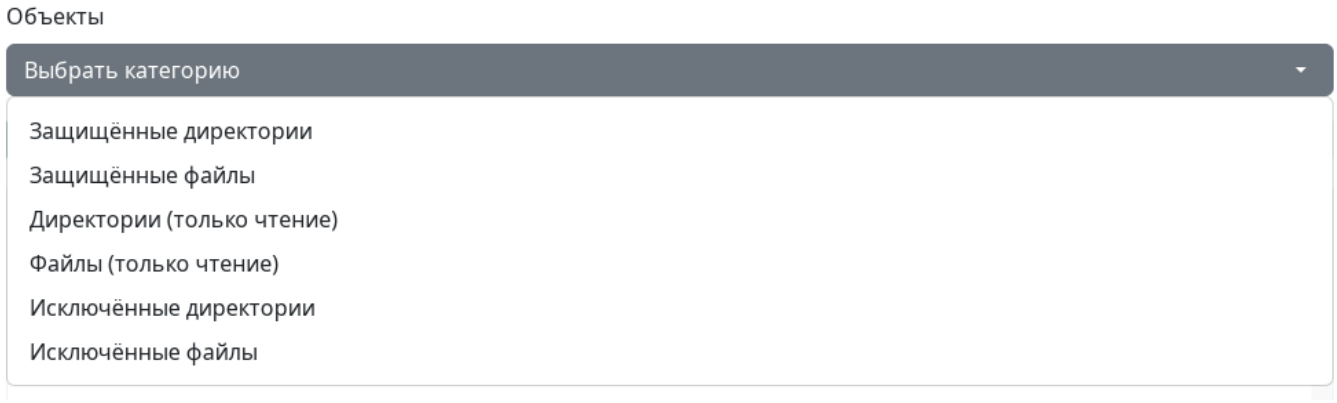


Рис. 38 – Проактивная защита. Категории защищаемых объектов

Вкладка **Аудит** (рис. 39) предназначена для настройки записи событий о чтении, записи и запуске файлов в соответствующий журнал.

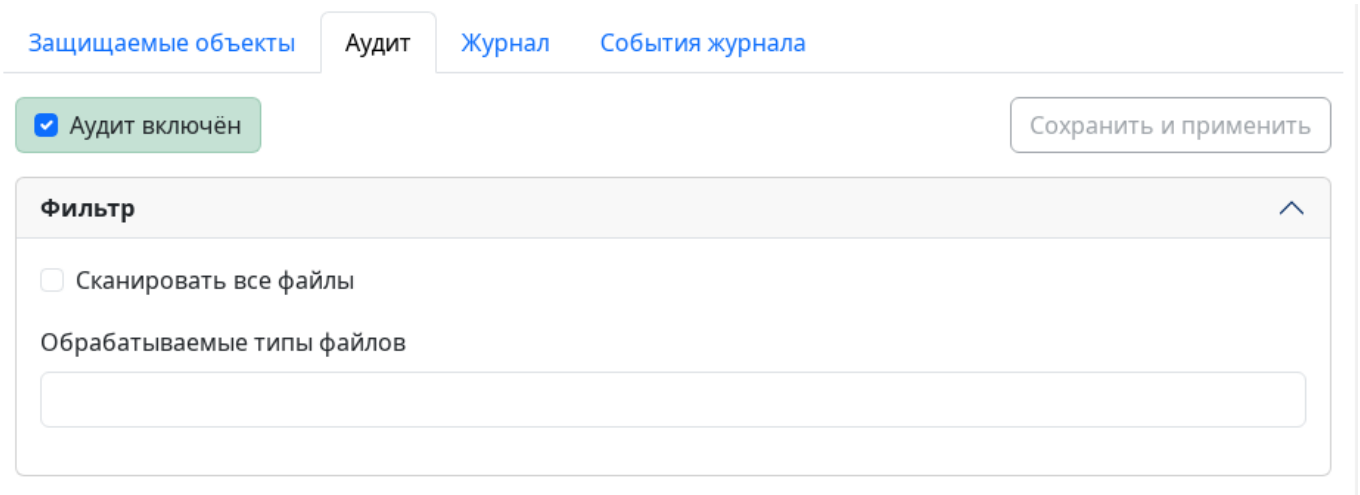


Рис. 39 – Проактивная защита. Аудит

Аудит назначается глобально (для всех пользователей) для конкретных типов (расширений) файлов.

Пункт выбора **Сканировать все файлы** включает аудит для всех файлов, открываемых на чтение/запись в ОС.

Расширения файлов задаются в виде списка, разделенного символом точка («.»).

Пример списка типов файлов для аудита: **DOCX.DOC.XLSX.XLS**

В данном случае в журнал аудита попадут события открытия и записи в файлы с расширениями **DOCX**, **DOC**, **XLSX** и **XLS**.

На вкладке **Журнал** (рис. 40) отображаются события, сгенерированные модулем **Проактивной защиты**.

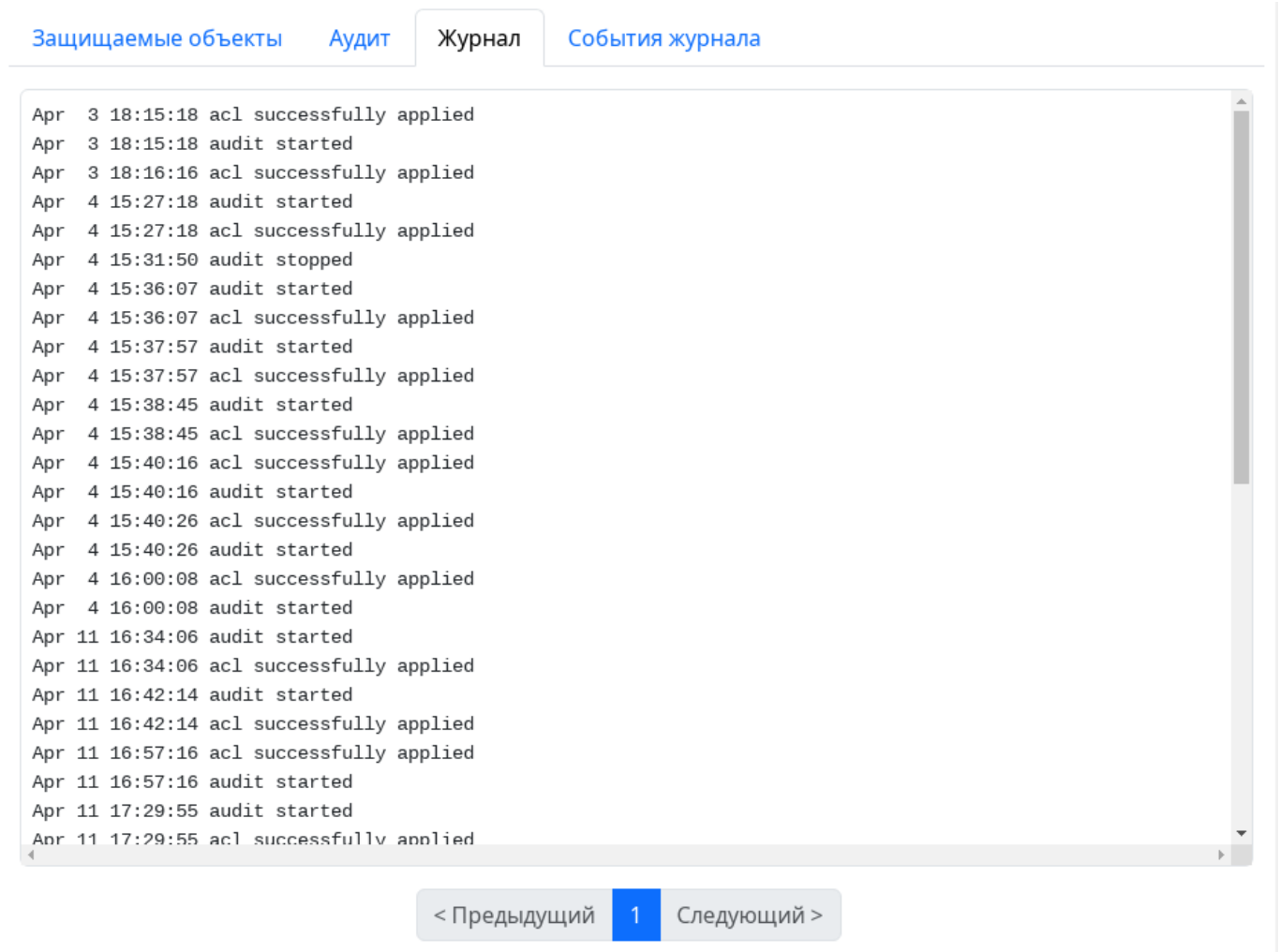


Рис. 40 – Проактивная защита. Журнал

Вкладка **События журнала** (рис. 41) используется для настройки того, где будет записано то или иное событие.

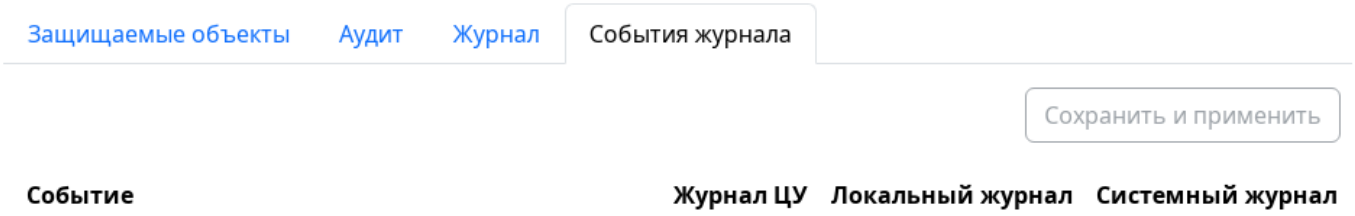


Рис. 41 – Проактивная защита. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.4. Раздел Пользователи

В разделе **Пользователи** производится настройка фильтрации действий (дискреционный контроль доступа) пользователей СВТ.

На вкладке **Пользователи** (рис. 42) указываются правила фильтрации действий пользователей, предназначенные для работы в контексте конкретной учетной записи ОС, установленной на СВТ. Правила по умолчанию выключены.

Примечание. Фильтрация действий работает для пользователей с uid ≥ 1000 (данная функция не работает для суперпользователя и системных пользователей). Для дополнительного ограничения возможностей доступа у пользователей рекомендуется дополнительно использовать утилиту `sudo` и не разрешать постоянную работу пользователей с административными правами в системе.

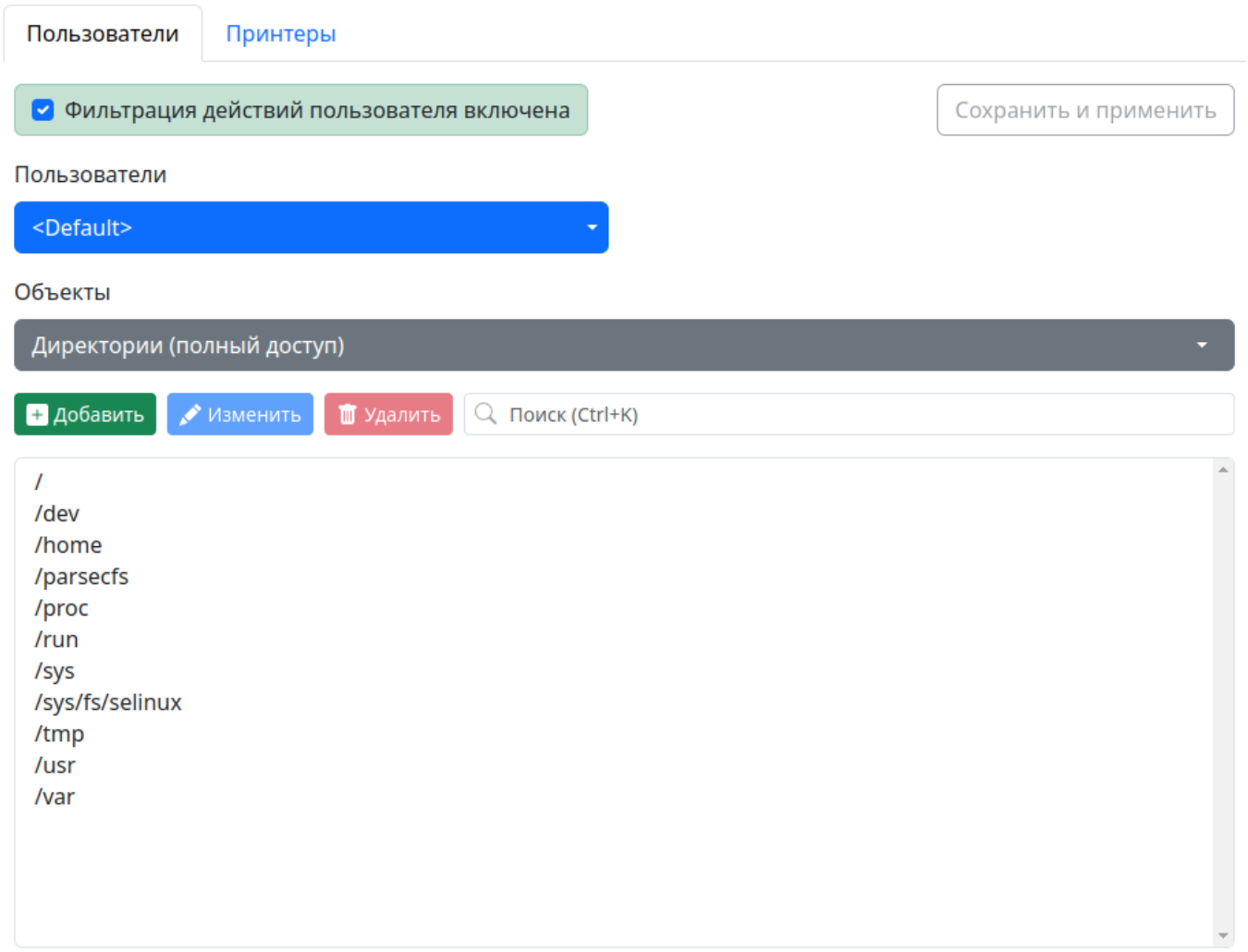


Рис. 42 – Пользователи

На вкладке отображается включение/выключение фильтрации действий пользователя, кнопка **Сохранить и применить**, выпадающее меню со списком пользователей, для которых существуют правила фильтрации, кнопки **Добавить**, **Изменить**, **Удалить**, поле поиска по списку объектов и список объектов одного типа.

Доступные объекты для добавления в список правил фильтрации действий пользователей (рис. 43):

1) **Директории (полный доступ)** – директории, к которым пользователь должен иметь доступ на чтение/запись;
2) **Директории (только чтение)** – директории, к которым пользователь должен иметь доступ только на чтение;

3) **Файлы (полный доступ)** – файлы, к которым пользователь должен иметь доступ на чтение/запись;
4) **Файлы (только чтение)** – файлы, к которым пользователь должен иметь доступ на чтение;
5) **Разрешенные приложения** – список приложений (исполняемых файлов), которые может запускать пользователь в рамках замкнутой программной среды.

Рис. 43 – Пользователи. Категории защищаемых объектов

При включении механизмов фильтрации по умолчанию начинают действовать правила из списка для пользователя **<Default>**. В данном списке указан набор правил, гарантирующий полнофункциональную работу ОС (без ограничений).

Для создания списка для конкретного пользователя необходимо выбрать его из списка доступных пользователей и нажать кнопку **Создать** (рис. 44, рис. 45). Список получается из ОС автоматически, в него попадают пользователи с uid ≥ 1000 при повторном переходе в раздел **Пользователи**.

Рис. 44 – Пользователи. Список пользователей

Рис. 45 – Пользователи. Список пользователей.
Создать настройки (список защищаемых объектов)

После создания списков объектов для пользователя в него будет добавлено содержимое списка **Default**. Для более точной настройки рекомендуем администратору руководствоваться текущим законодательством и опытом эксплуатации конкретной информационной системы.

На вкладке **Принтеры** (рис. 46) отображается кнопка **Сохранить и применить** и группа элементов для разрешения конкретного принтера конкретному пользователю. Данная вкладка получает список принтеров из сервера печати CUPS и позволяет ограничивать пользователю доступ к устройству печати.

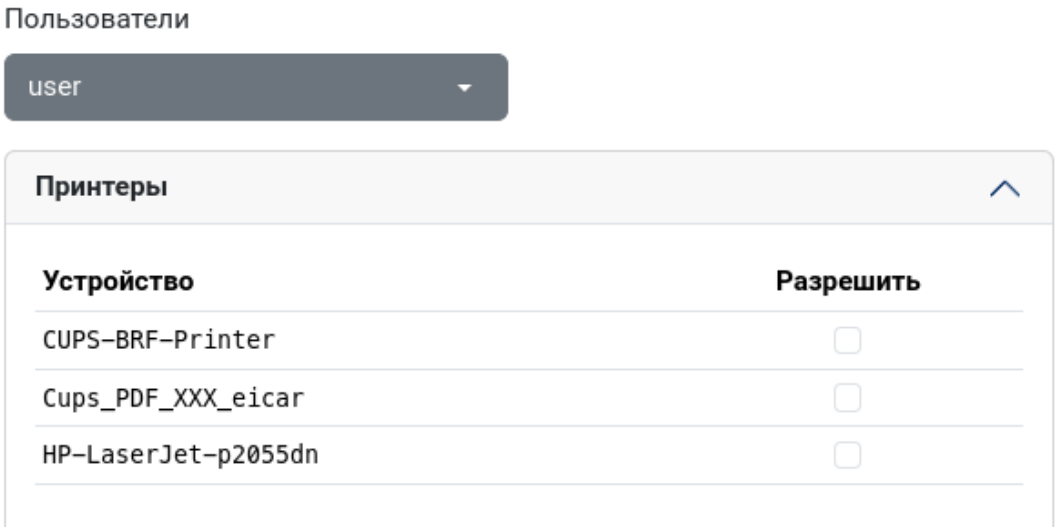


Рис. 46 – Пользователи. Принтеры

4.4.5. Раздел Антивирусный сканер

В состав программного комплекса ШХУНА входит антивирусное ядро и модули, позволяющие осуществить сканирование файлов на наличие вредоносных программ по требованию и в режиме реального времени.

Раздел **Антивирусный сканер** пользовательского интерфейса программного

комплекса ШХУНА предназначен для настройки антивирусного сканирование по требованию.

На вкладке **Сканирование** (рис. 47) расположены кнопка запуска сканирования, группа элементов **Параметры**, состоящая из пункта выбора включения/выключения **Полного сканирования** и группы элементов **Объекты для сканирования**, в которую входят кнопки **Добавить**, **Изменить**, **Удалить**, и списка объектов для сканирования и группы элементов **Сообщения**, в которой отображается имя проверяемого в данный момент времени файла и статус сканирования. Кнопка **Подробнее** раскрывает элемент списка с проверенными файлами и их статусом.

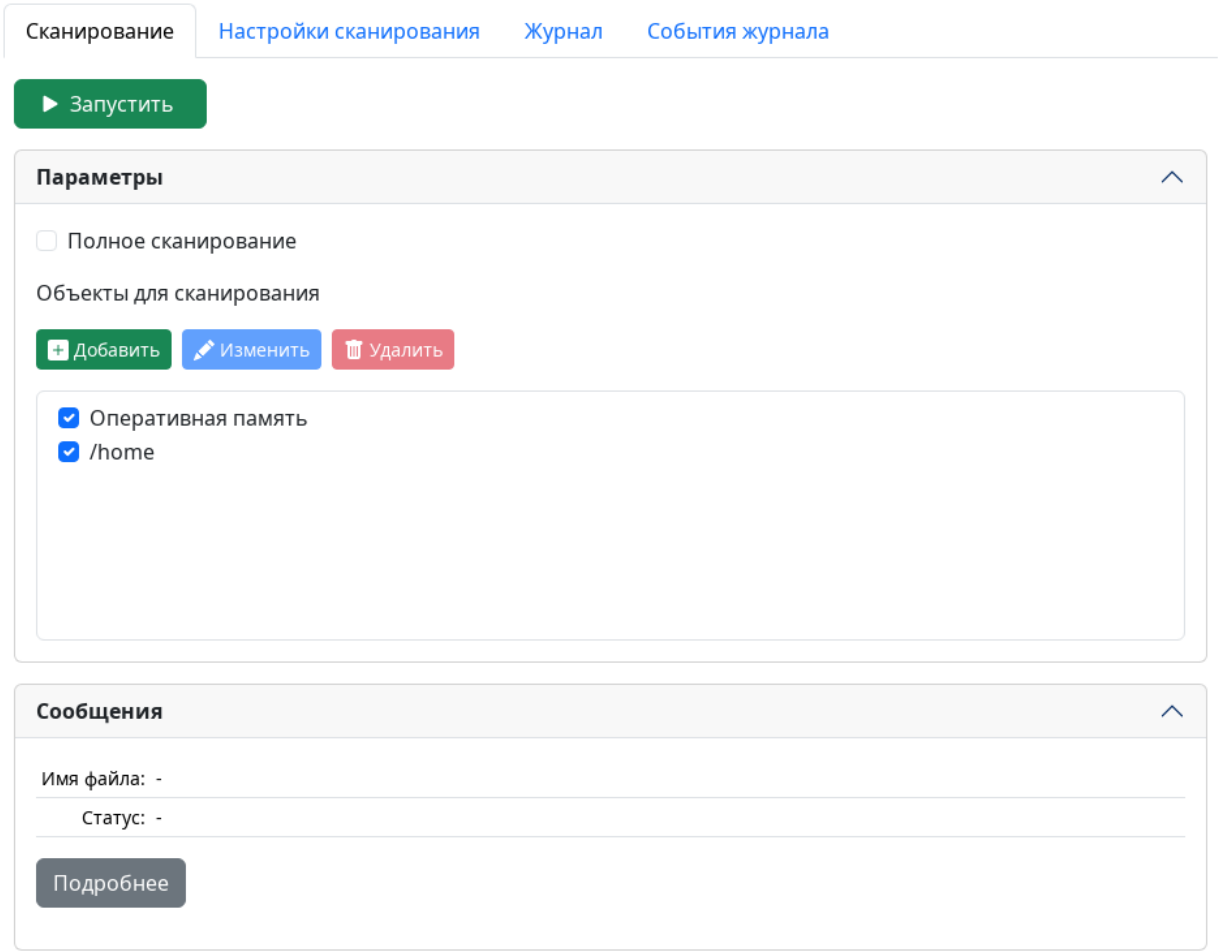


Рис. 47 – Антивирусный сканер. Сканирование

На вкладке **Настройки сканирования** (рис. 48) расположены кнопка **Сохранить и применить** и группы элементов **Фильтр** и **Действия**.

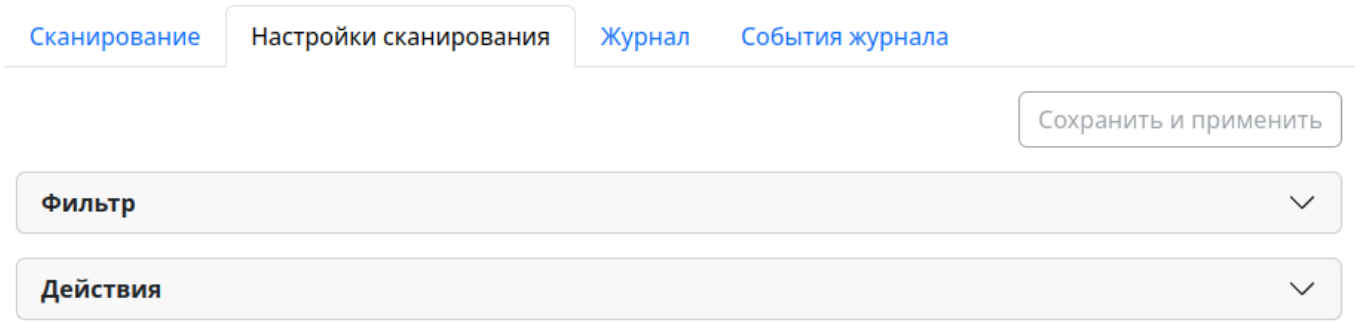


Рис. 48 – Антивирусный сканер. Настройки сканирования

В группу элементов **Фильтр** (рис. 49) входят следующие параметры:

1) **Сканировать все файлы** – устанавливает режим, при котором **Антивирусный сканер** проверяет на наличие ВПО все файлы в объектах сканирования;
2) текстовое поле **Исключаемые расширения** позволяет задать расширения файлов, которые должны быть исключены из проверки. Список расширений разделяется символом точка «.». Пример: **TXT.DB.NIL.INI**;
3) **Пропускать файлы больше** – устанавливает режим, при котором **Антивирусный сканер** исключит из проверки файлы, размер которых превышает указанный в соответствующем текстовом поле;
4) текстовое поле с размером ограничения размера проверяемых файлов в мегабайтах;
5) **Обнаружить потенциально опасные** – устанавливает дополнительный режим, при котором **Антивирусный сканер** перестанет игнорировать потенциально опасные программы;
6) **Сканировать почту** – включает режим проверки содержимого файлов почтовых программ (EML, PST, Mailbox, и т.д.) на наличие вредоносных программ;
7) **Сканировать архивы** – устанавливает режим, при котором **Антивирусный сканер** обрабатывает содержимое архивов;
8) **Пропускать архивы больше** – устанавливает режим, при котором **Антивирусный сканер** исключит из проверки архивы, размер которых превышает указанный в соответствующем текстовом поле;

9) текстовое поле с размером ограничения размера проверяемых архивов в мегабайтах;
10) **Обнаруживать установщики вредоносных программ** – устанавливает режим, при котором **Антивирусный сканер** обрабатывает самораспаковывающиеся архивы (SFX).

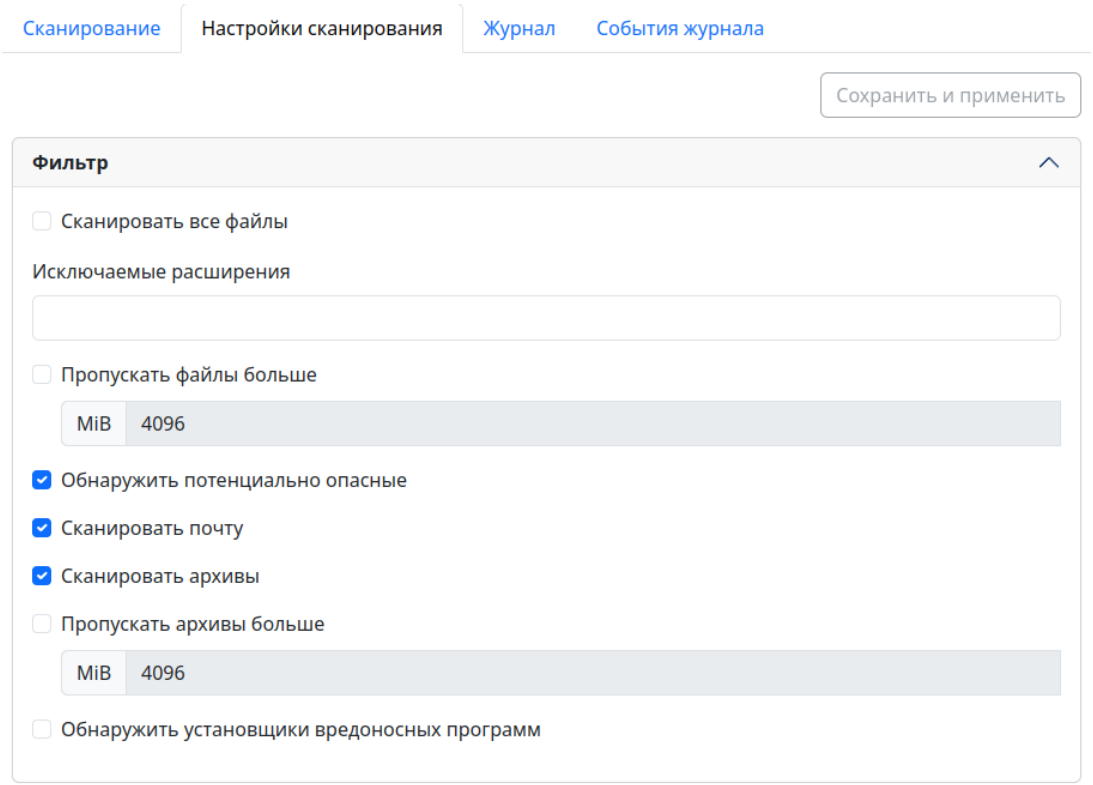


Рис. 49 – Антивирусный сканер. Настройки сканирования. Фильтр

В группу элементов **Действия** (рис. 50) входят следующие параметры:

1) элемент настройки действий для зараженных файлов, состоящий из действий **Лечить**, **Удалить** и возможности **Сохранить в карантин**;
2) элемент настройки действий для подозрительных файлов, состоящий из действий **Удалить** и возможности **Сохранить в карантин**;
3) для настройки последовательности действий администратору необходимо включить элементы действий над соответствующими файлами, выстроить их приоритет перетягиванием и нажать на кнопку **Сохранить и применить**.

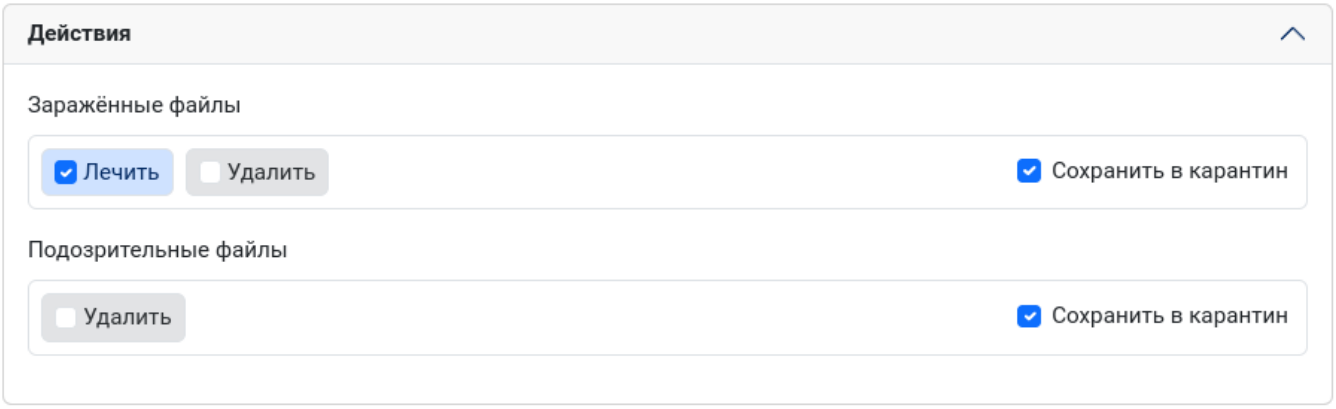


Рис. 50 – Антивирусный сканер. Настройки сканирования. Действия

Действие **Лечить** – изменяет файл, удаляя из него измененные ВПО части, либо удаляет файл, если он целиком представляет собой ВПО.

Действие **Удалить** – удаляет файл, содержащий ВПО (в этом случае изменение файла не будет произведено даже при наличии возможности).

Пункт выбора **Сохранить в карантин** – обеспечивает возможность сохранения копии инфицированного или подозрительного файла в компоненте **Карантин** модуля контроля данных программного комплекса ШХУНА.

На вкладке **Журнал** отображаются события, сгенерированные модулем **Антивирусного сканера**.

Вкладка **События журнала** (рис. 51) используется для настройки того, где будет записано то или иное событие.

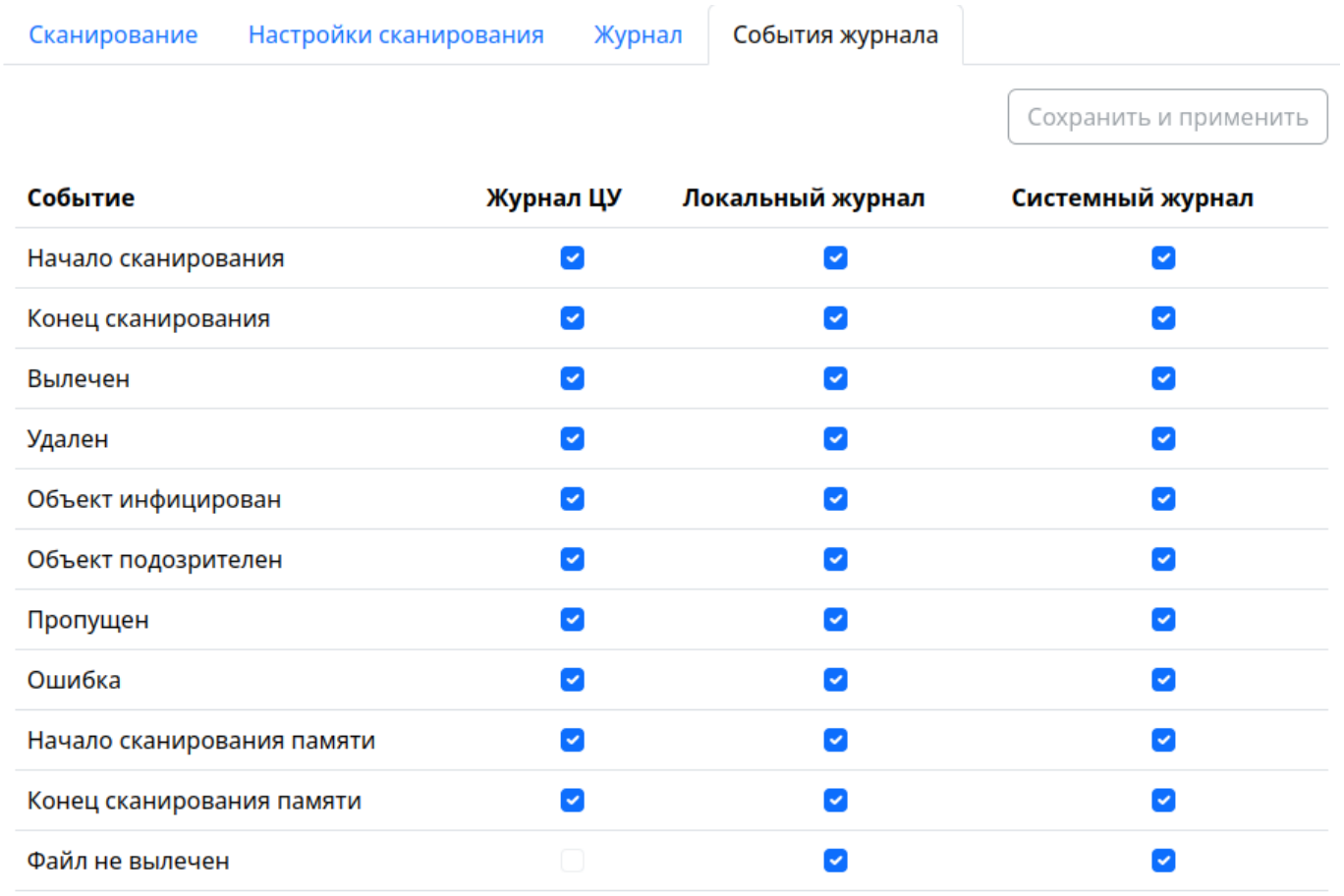


Рис. 51 – Антивирусный сканер. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.6. Раздел Монитор

Раздел **Монитор** пользовательского интерфейса программного комплекса ШХУНА предназначен для настройки антивирусного сканирования в режиме реального времени.

Проверка файлов осуществляется для локальных файловых систем (проверка в

точках монтирования общих сетевых папок или файловых систем типа FUSE может быть завершена с ошибкой). Проверка файлов производится при попытке открытия на чтение/запись (копирование файла с сетевого ресурса такой операцией не является).

Вкладка **Настройки** раздела **Монитор** (рис. 52) состоит из следующих управляющих элементов:

1) пункта выбора **Монитор включен** – отражает статус работы монитора. При включении/отключении данной формы выбора будет сгенерировано соответствующее событие;
2) группы элементов **Фильтр** (рис. 53);
3) группы элементов **Действия** (рис. 56).

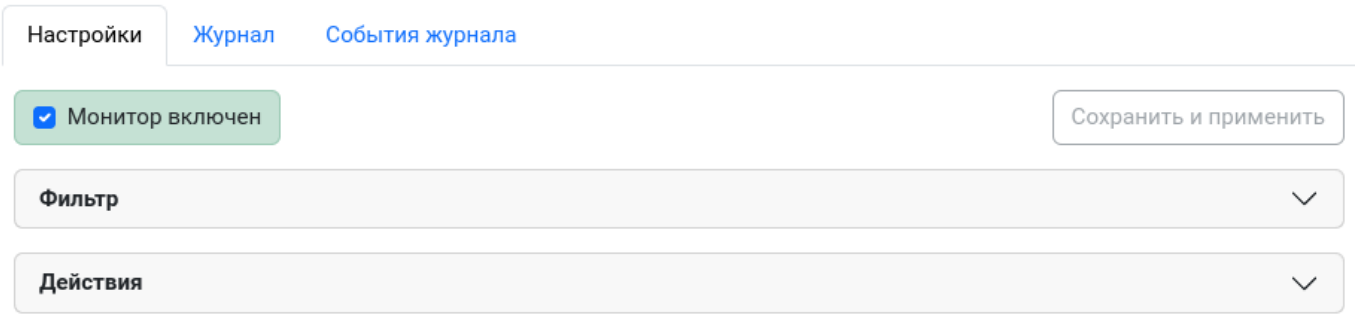


Рис. 52 – Монитор. Настройки

В группу элементов **Фильтр** входят следующие параметры:

1) **Проверять все файлы** – включает режим работы модуля Монитор программного комплекса ШХУНА, при котором на проверку будут отправлены все файлы, к которым осуществляется доступ пользователей (данная опция может сильно повлиять на потребление ресурсов СВТ, следует использовать с осторожностью).
2) **Проверять файлы с правами на исполнение** – включает режим работы компонента **Монитор** программного комплекса ШХУНА, при котором будут отправлены на проверку файлы с установленным флагом исполнения (**+x**);
3) **Проверять файлы с исполняемым форматом** – включает режим работы компонента **Монитор** программного комплекса ШХУНА, при котором будут отправлены на проверку файлы, формат которых исполняемый в

ОС Linux (ELF). Проверка принадлежности к исполняемому формату осуществляется по структуре файла;

4) поле ввода **Проверять файлы с расширениями** – содержит перечень расширений файлов, которые будут проверяться на наличие ВПО при попытке доступа к ним. По умолчанию в настройках указаны следующие расширения файлов:

   `COM.EXE.DLL.DRV.SYS.OV?.VXD.SCR.CPL.OCX.BPL.AX.PIF.LNK.DO*.XL*.HLP.RTF.WI?.WZ?.MSI.MSC.HT*.VB*.JS.JSE.ASP*.CGI.PHP*.?HTML.BAT.CMD.EML.NWS.MSG.XML.MSO.WPS.PPT.PUB.JPG.JPEG.ANI.INF.SWF.PDF`;

5) поле ввода **Исключить расширения** содержит перечень расширений файлов, которые не будут проверяться на наличие ВПО при попытке доступа к ним. При необходимости сброса настроек к настройкам по умолчанию предусмотрена соответствующая кнопка справа от поля ввода;

6) группа элементов **Исключить каталоги** позволяет исключить определенные пользователем директории из обработки **Монитором**. В группу элементов входят:
   - кнопки **Добавить**, **Удалить**, **Изменить** для элементов списка;
   - поле отображения списка исключенных из проверки директорий.

Примечания:

1. Символ «.» является символом–разделителем перечня расширений файлов.

2. Символы «?» и «*» в данном перечне означают один любой символ и неограниченное число любых символов соответственно.

3. При необходимости сброса настроек к настройкам по умолчанию предусмотрена соответствующая кнопка справа от поля ввода.

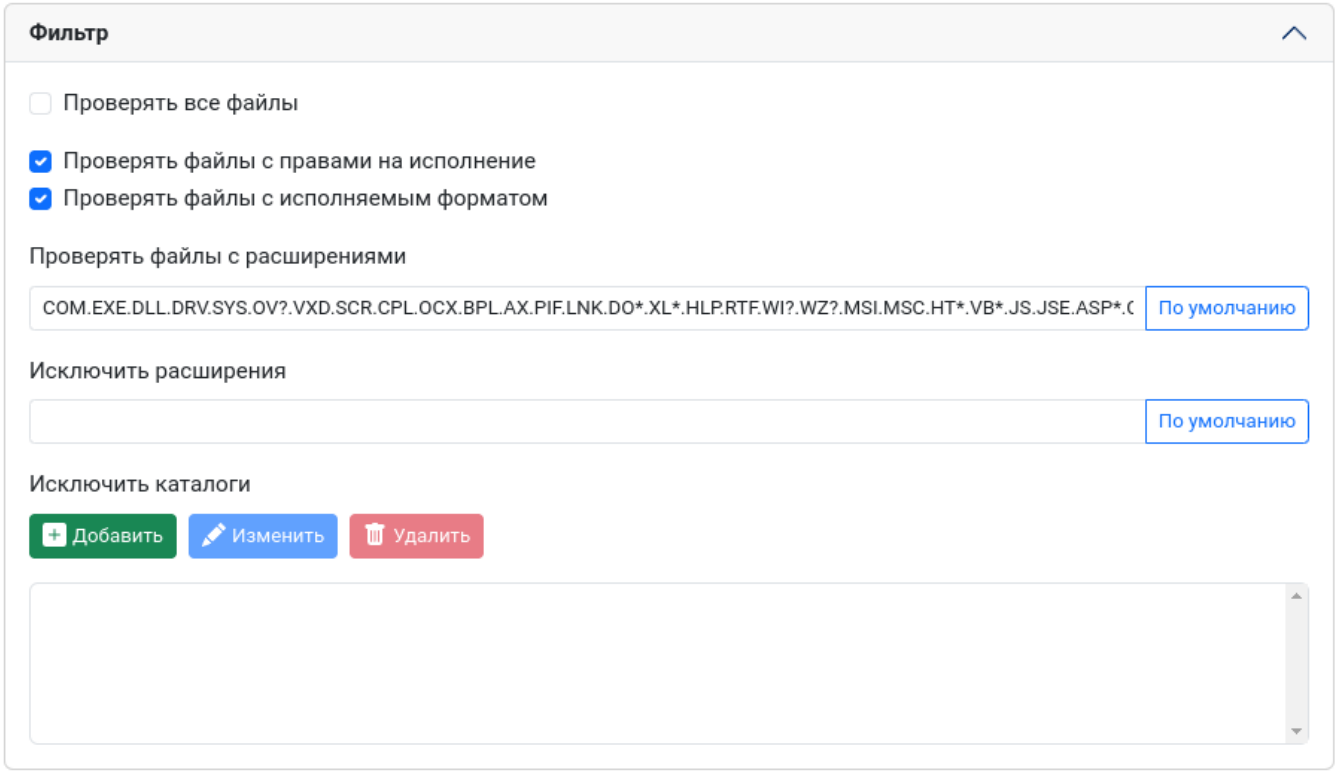


Рис. 53 – Монитор. Настройки. Фильтр

Кнопка **Добавить** вызывает диалоговое окно ввода пути к директории, которую необходимо исключить из обработки **Монитора** (рис. 54).

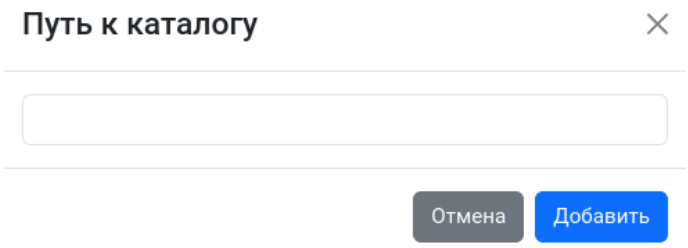


Рис. 54 – Монитор. Настройки. Фильтр. Добавить каталог

Выделив существующий путь в списке **Исключить каталоги** (рис. 55) можно воспользоваться кнопками **Изменить** для внесения изменений в путь к директории, которую необходимо исключить из обработки **Монитором**.

Рис. 55 – Монитор. Настройки. Фильтр. Исключить каталоги

Для удаления выбранной директории из списка **Исключить каталоги Монитора** необходимо нажать на кнопку **Удалить**.

В группу элементов **Действия** (рис. 56) входят следующие параметры:

1) элемент настройки действий для зараженных файлов, состоящий из элементов **Лечить**, **Удалить**, **Блокировать** и возможности **Сохранить в карантин**;
2) элемент настройки действий для подозрительных файлов, состоящий из элементов **Удалить** и возможности **Сохранить в карантин**.

Действие **Блокировать** – блокирует попытки доступа к файлу.

Действие **Лечить** – изменяет файл, удаляя из него измененные ВПО части, либо удаляет файл, если он целиком представляет собой ВПО.

Действие **Удалить** – удаляет файл, содержащий ВПО (в этом случае изменение файла не будет произведено даже при наличии возможности).

Пункт выбора **Сохранить в карантин** – обеспечивает сохранение копии инфицированного или подозрительного файла в компоненте **Карантин** модуля контроля данных программного комплекса ШХУНА.

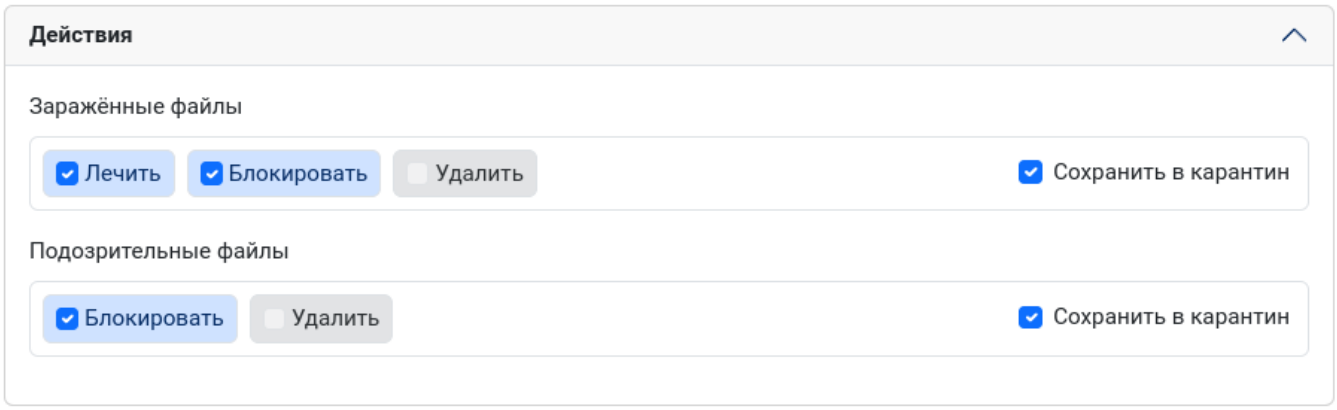


Рис. 56 – Монитор. Настройки. Действия

Для настройки последовательности действий администратору необходимо включить элементы действий над соответствующими файлами, выстроить их приоритет слева на право, перетягиванием и нажать на кнопку **Сохранить и применить** в верхней части настроек.

На вкладке **Журнал** отображаются события, сгенерированные модулем антивирусного сканера, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 57) используется для настройки, где будет записано то или иное событие.

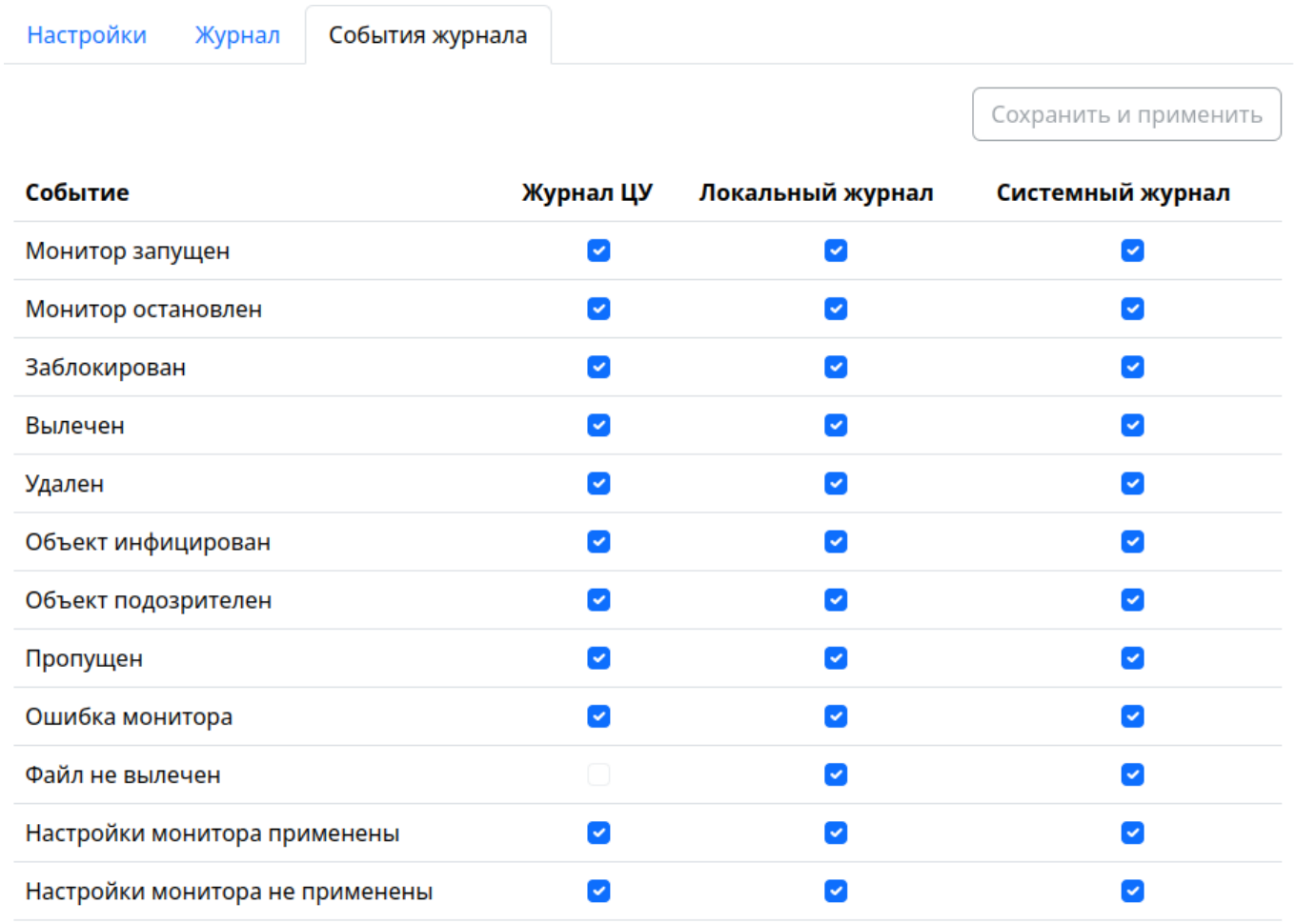


Рис. 57 – Монитор. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.7. Раздел Устройства

Раздел **Устройства** (рис. 58) является интерфейсом настройки модуля **Управление доступом**, который реализует контроль подключения устройств к СВТ.

Примечание. Необходимо учитывать, что модуль контроля доступа работает

согласно принципу «Все, что не разрешено явно – запрещено» (запрет по умолчанию). Включение функций модуля и применение настроек без их контроля может привести к нарушению работоспособности ОС СВТ.

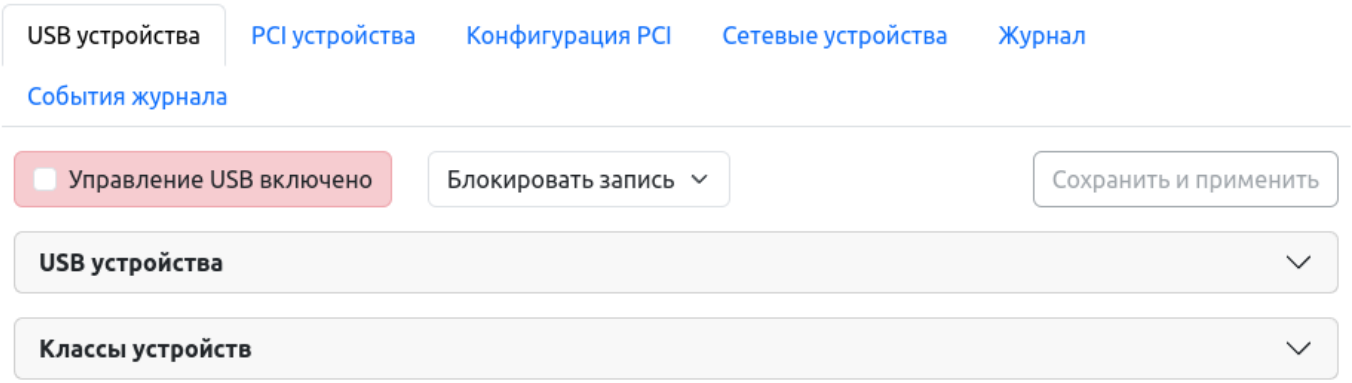


Рис. 58 – Устройства. Управление устройствами

На вкладке **USB устройства** осуществляется настройка контроля подключения USB-устройств к СВТ. Данная вкладка состоит из:

1) пункта выбора **Управление USB включено** – контролирует статус работы модуля;
2) выпадающего списка с набором действий по умолчанию для USB Mass Storage – доступные варианты для выбора: **Пропустить** (Разрешить), **Блокировать** (Запретить), **Блокировать запись** (Запретить запись) (рис. 59);
3) кнопки **Сохранить и применить**;
4) группы элементов **USB устройства** (рис. 60);
5) группы элементов **Классы устройства** (рис. 61).

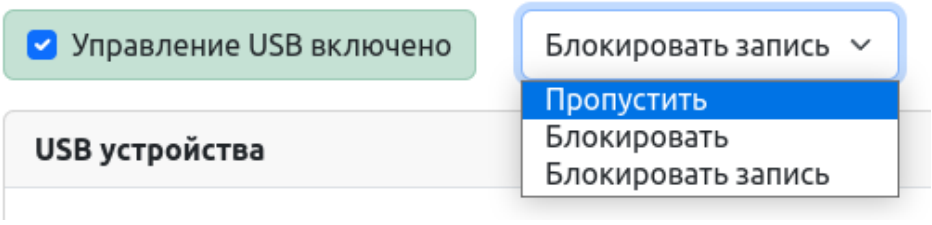


Рис. 59 – Устройства. USB-устройства. Действия по умолчанию

Группа элементов **USB-устройства** (рис. 60) представляет собой таблицу соответствий **Устройство-Действие**. В качестве элемента **Устройство** выступает серийный номер подключенного USB-устройства.

Действием может быть один из элементов выпадающего списка:

1) **Согласно классу устройства** – игнорирует серийный номер устройства, осуществляет работу по правилам, заданным в группе элементов **Классы устройств**;
2) **Разрешить** (Пропустить) – разрешает доступ к конкретному устройству по его серийному номеру;
3) **Блокировать** (Запретить) – блокирует доступ к конкретному устройству по его серийному номеру;
4) **Блокировать запись** (Запретить запись) – блокирует доступ к конкретному устройству для записи по его серийному номеру.

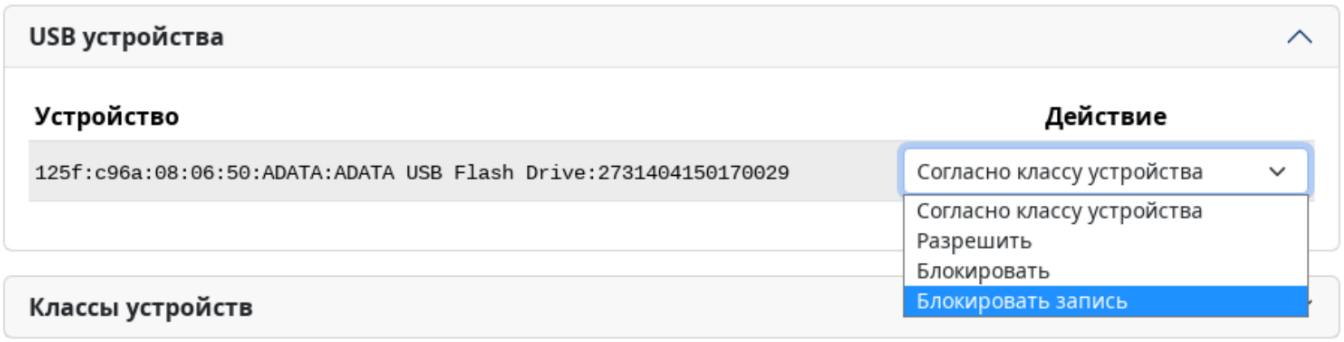


Рис. 60 – Устройства. USB-устройства. Действия

Группа элементов **Классы устройств** (рис. 61) представляет собой таблицу соответствий названия класса USB-устройств и формы выбора, разрешающего доступ к данному классу.

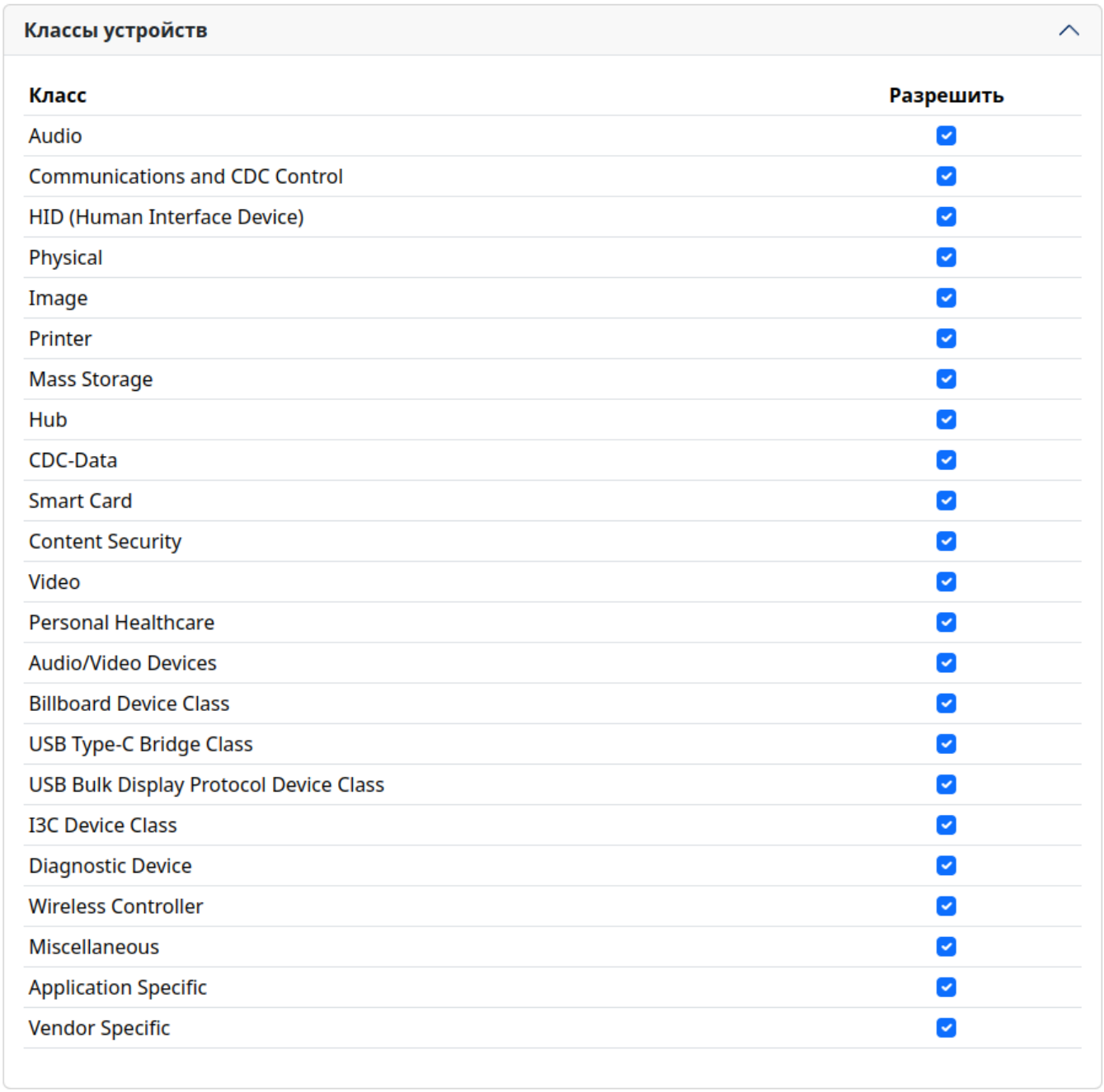


Рис. 61 – Устройства. USB-устройства. Классы

Модуль контроля доступа, настраиваемый с помощью раздела **Устройства**, работает согласно алгоритму, схематично изображенному на рис. 62.

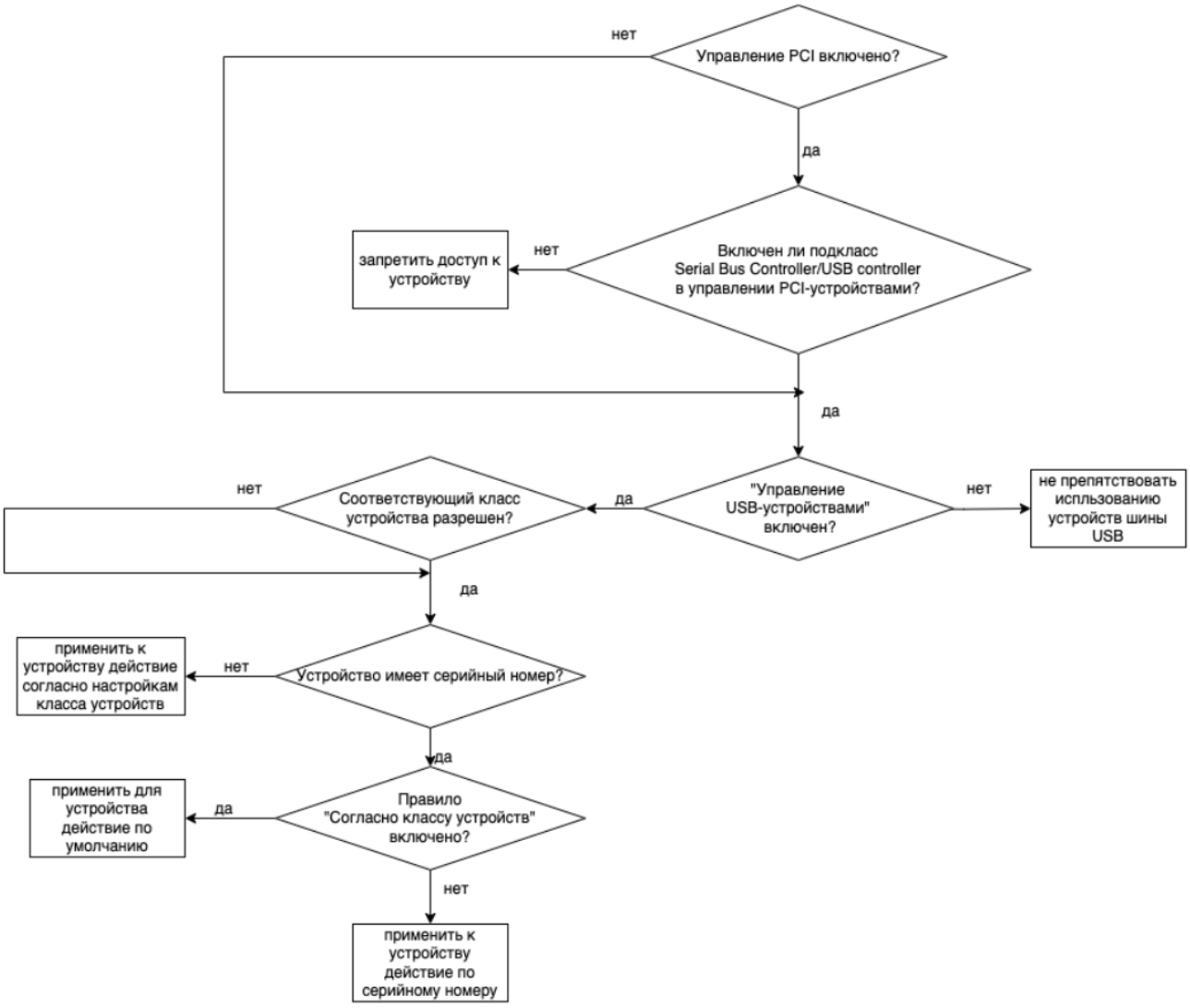


Рис. 62 – Устройства. Алгоритм контроля доступа к устройствам

На вкладке **PCI-устройства** (рис. 63) отображаются PCI-устройства, подключенные к СВТ в момент открытия вкладки.

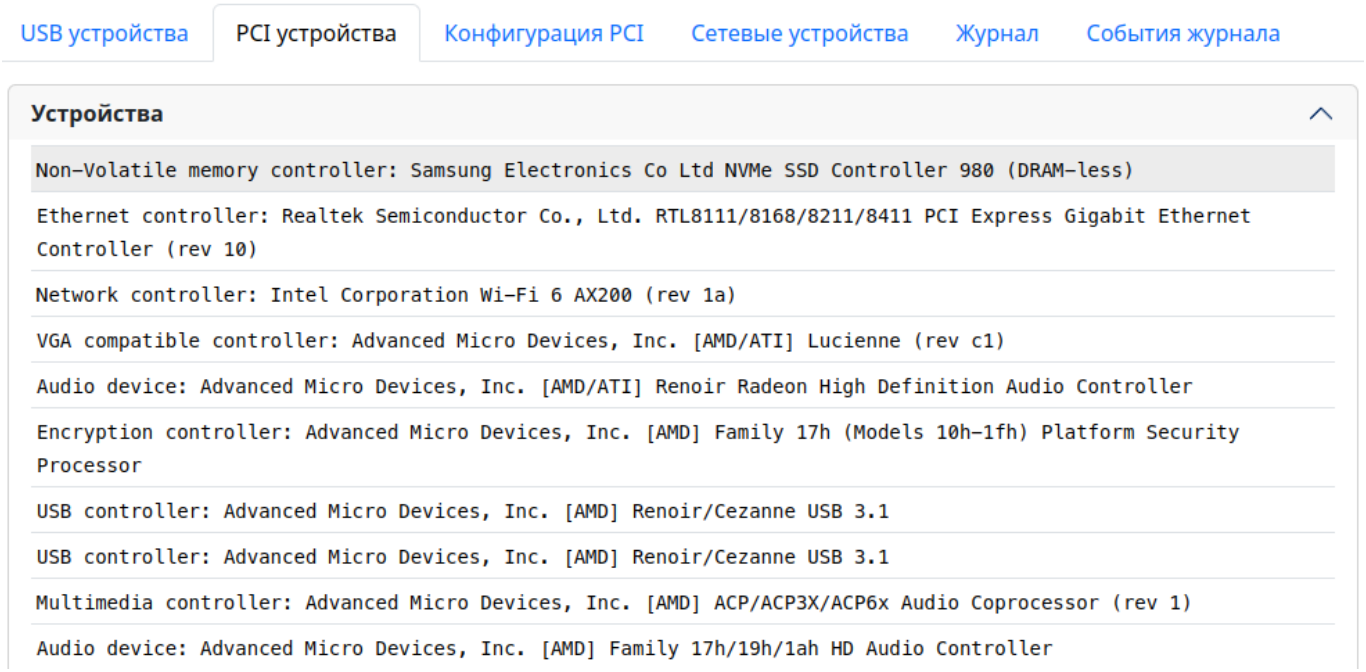


Рис. 63 – Устройства. PCI-устройства

Вкладка **Конфигурация PCI** (рис. 64) состоит из:

1) пункта выбора **Управление PCI включено** – контролирует работу модуля **Управления доступом** к устройствам шины PCI;
2) пункта выбора **Разрешить вне списка** – разрешает использование устройств классов, не входящих в список;
3) кнопки **Сохранить и применить** – применяются настройки изменений;
4) группы элементов **Классы устройств** (рис. 65) – состоит из списка классов PCI, их подклассов и правил подключения этих устройств (рис. 66).

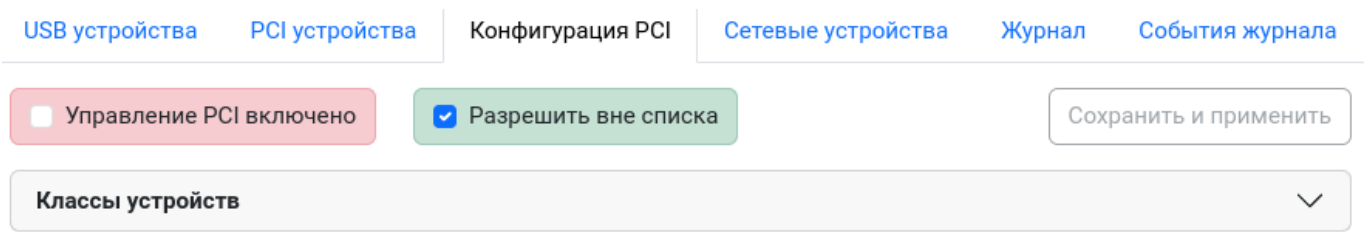


Рис. 64 – Устройства. Конфигурация PCI

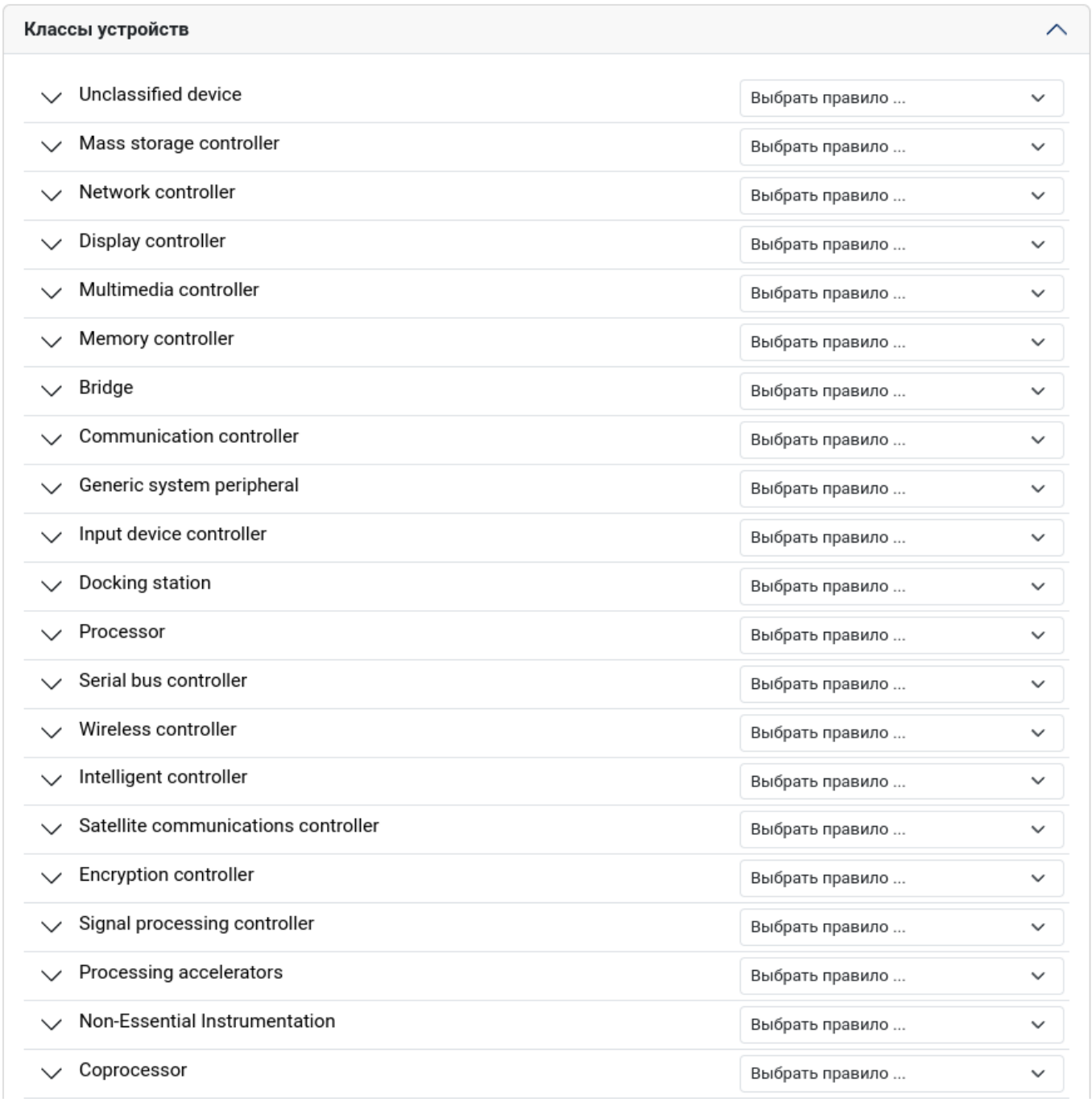


Рис. 65 – Устройства. Конфигурация PCI. Классы

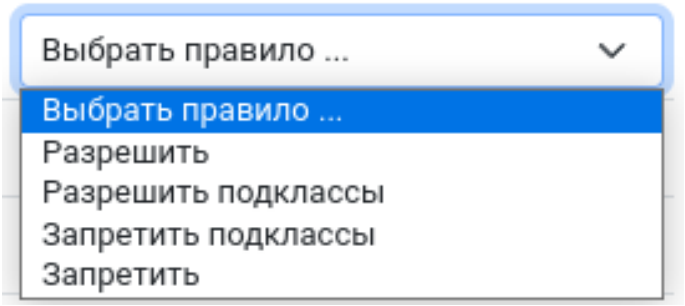


Рис. 66 – Устройства. Конфигурация PCI. Правила

Для работы с классами PCI устройствами необходимо:

1) выбрать соответствующий класс устройств;
2) раскрыть список правил и выбрать один из вариантов: **Разрешить**, **Разрешить подклассы**, **Запретить подклассы**, **Запретить** (рис. 67).

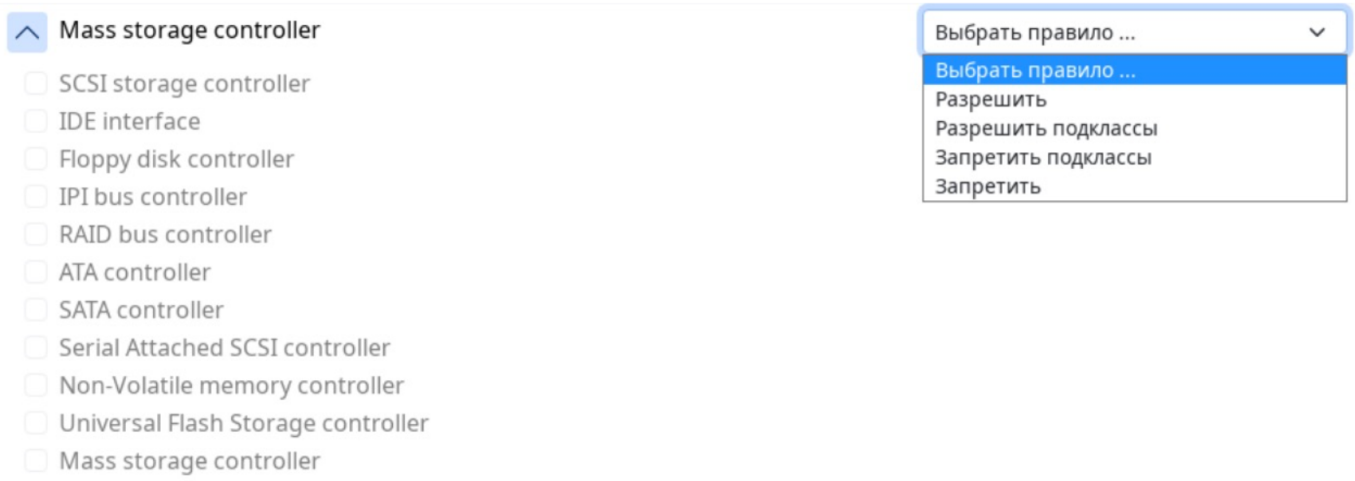


Рис. 67 – Устройства. Конфигурация PCI. Пример правила

Правила **Разрешить подклассы** и **Запретить подклассы** делают доступным выбор подклассов соответствующего класса PCI-устройств (рис. 68).

П р и м е ч а н и е . Данный раздел следует использовать с крайней осторожностью. Отключение некоторых классов PCI-устройств может нарушить работоспособность СВТ.

Рис. 68 – Устройства. Конфигурация PCI. Пример правила. Выбор подкласса

На вкладке **Сетевые устройства** (рис. 69) расположены:

1) пункт выбора **Управление сетевыми устройствами** – контролирует работу модуля контроля доступа к сетевым устройствам;
2) кнопка **Сохранить и применить** – для сохранения и применения измененных настроек;
3) группа элементов **Сетевые устройства** (рис. 70) – для настройки правил доступа к сетевым устройствам. В данную группу входит: список сетевых устройств и правила управления доступом к каждому из устройств списка.

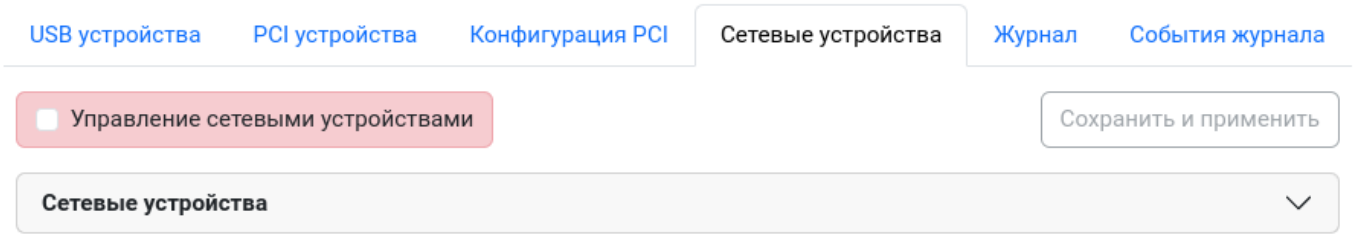


Рис. 69 – Устройства. Сетевые устройства

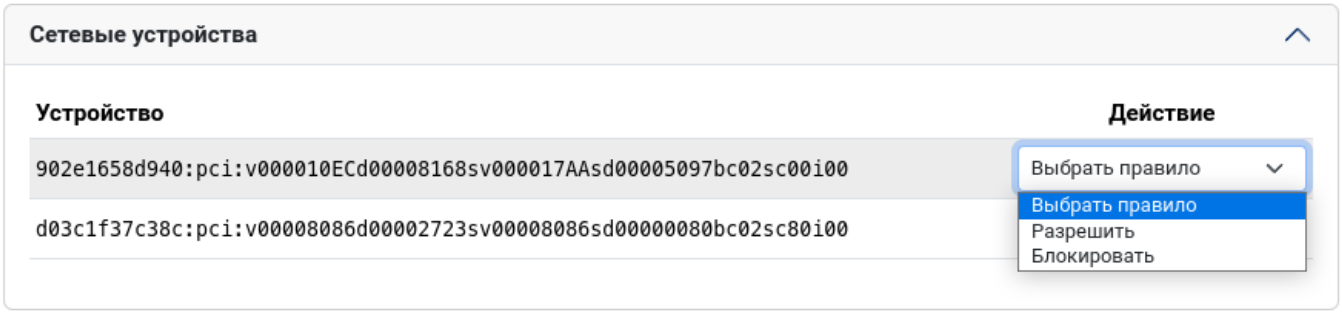


Рис. 70 – Устройства. Сетевые устройства. Действия

После включения формы выбора **Управление сетевыми устройствами** модуль контроля доступа программного комплекса ШХУНА по умолчанию запретит все сетевые устройства СВТ. Для разрешения работы сетевого устройства необходимо выбрать правило **Разрешить** в списке правил группы элементов **Сетевые устройства**.

На вкладке **Журнал** отображаются события, сгенерированные модулем управления доступом, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 71) используется для настройки того, где будет записано то или иное событие.

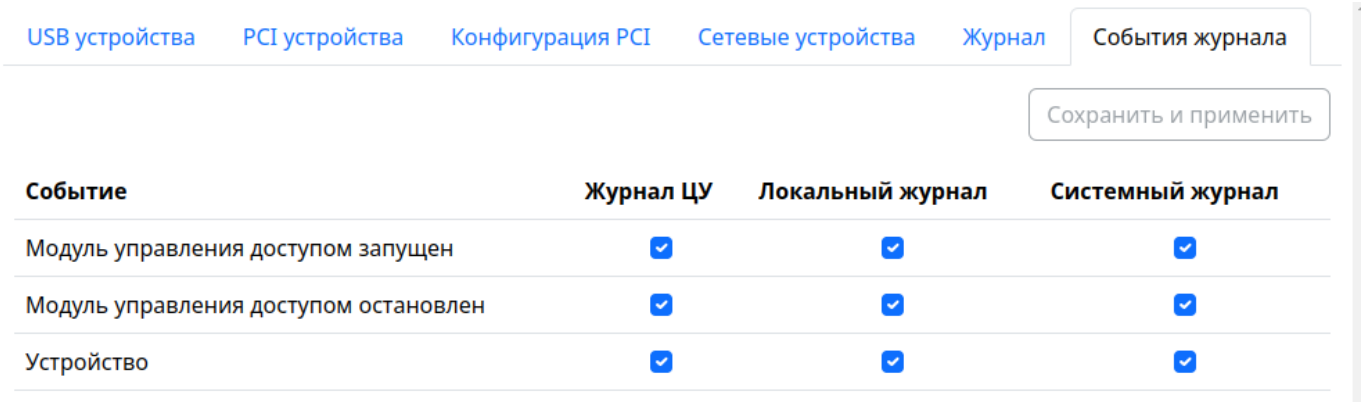


Рис. 71 – Устройства. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо

сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.8. Раздел Принтеры

Раздел **Принтеры** предназначен для управления доступом к принтерам на базе сервера печати CUPS.

На вкладке **Принтеры** (рис. 72) расположены:

1) пункт выбора **Контроль принтеров включен** – контролирует работу модуля управления доступом по работе с принтерами;
2) кнопка **Сохранить и применить** – для сохранения и применения измененных настроек;
3) группа элементов **Принтеры** (рис. 73), для настройки правил доступа к принтерам. В данную группу входит список подключенных к СВТ принтеров, форма выбора **Разрешить всем** и группа пользователей, которым разрешено использование принтера (соответствует настройке вкладки **Принтеры** раздела **Пользователи**).

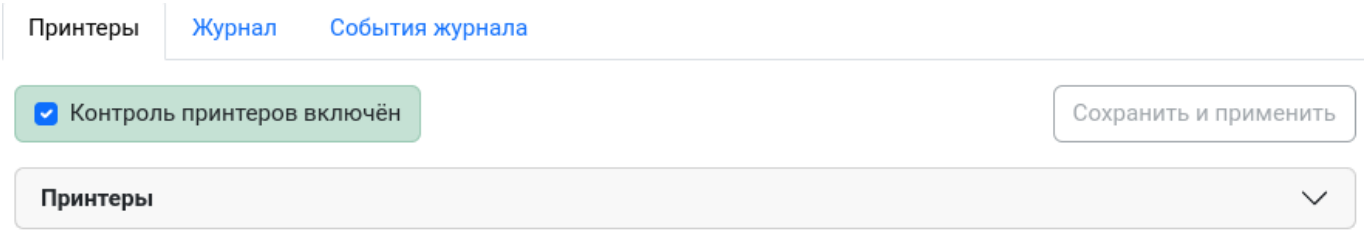


Рис. 72 – Устройства. Принтеры

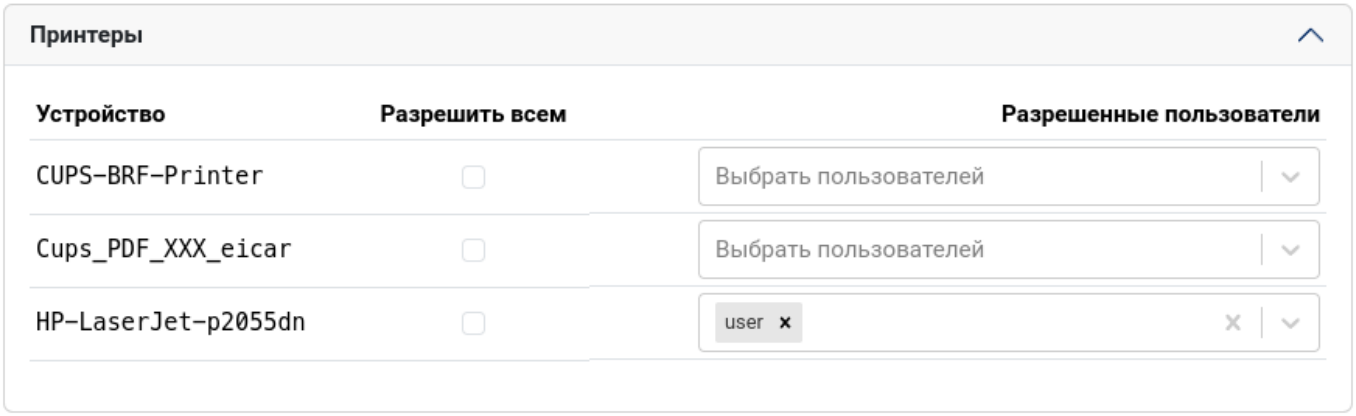


Рис. 73 – Устройства. Принтеры. Группа элементов

Форма выбора **Разрешить всем** – разрешает использование данного принтера всем пользователям СВТ.

На вкладке **Журнал** отображаются события, сгенерированные модулем управления доступом, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 74) используется для настройки того, где будет записано то или иное событие.

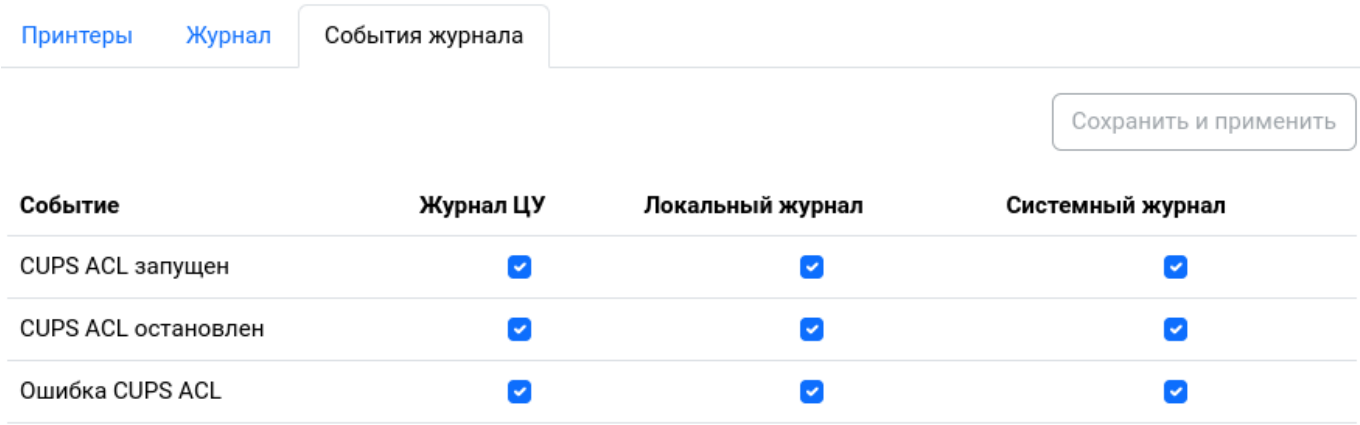


Рис. 74 – Устройства. Принтеры. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо

сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.9. Раздел Межсетевой экран

Раздел **Межсетевой экран** позволяет задавать настройки пакетного фильтра, входящего в состав программного комплекса ШХУНА.

На вкладке **Общие** (рис. 75) расположены следующие элементы:

1) пункт выбора **Межсетевой экран включен** – контролирует работу модуля межсетевого экранирования;
2) кнопка **Сохранить и применить** – для сохранения и применения измененных настроек;
3) поле со списком **Тип сети** (рис. 76) – позволяет выбрать один из предварительно настроенных профилей работы межсетевого экрана. Возможные для настройки профили:
   - **Открытая сеть** – фильтрация пакетов отключена, если не заданы запрещающие правила IPv4/IPv6 (в этом случае работают только запрещающие правила, остальной трафик проходит через пакетный фильтр без обработки);
   - **Закрытая сеть** – фильтрация пакетов включена, работают только разрешающие правила IPv4/IPv6;
   - **Частная сеть** – фильтрация пакетов включена, в пакетный фильтр добавлены разрешающие правила для работы NETBIOS и SMB. Данный режим предназначен для упрощения настройки межсетевого экрана в рабочей группе ОС Windows;
   - **Доменная сеть** – фильтрация пакетов включена, в пакетный фильтр добавлены разрешающие правила для работы DNS, KERBEROS, LDAP, NETBIOS и SMB. Данный режим предназначен для упрощения настройки межсетевого экрана в доменах Active Directory.

Примечания:

1. В запрещающих профилях настроек не блокируется связь с ЦУ (удаленный порт `tcp/17001` для отправки событий, локальный порт `tcp/17002` для приема событий).

2. На правила межсетевого экрана действуют глобальные настройки отслеживания соединений (`conntrack`) ОС Linux. При создании и применении правил необходимо учитывать, что в большинстве дистрибутивов время отслеживания соединений установлено равным 30 секундам. Это означает, что при создании запрещающего правила, под которое попадают активные сетевые соединения, правило применится через 30 секунд после завершения активных соединений.

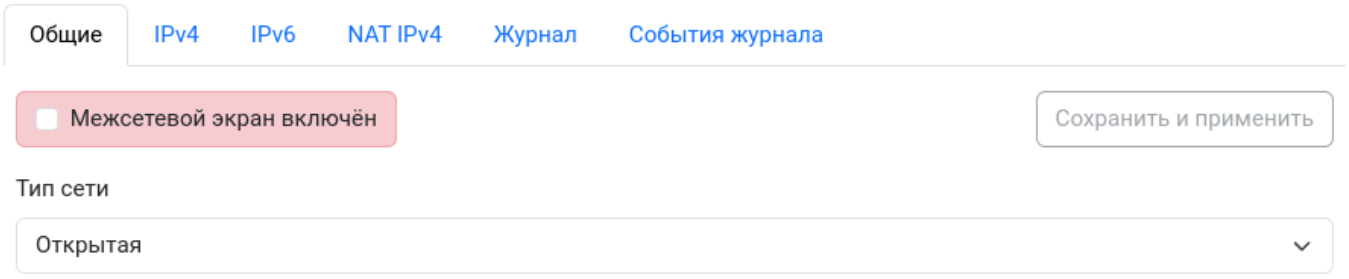


Рис. 75 – Межсетевой экран. Общие

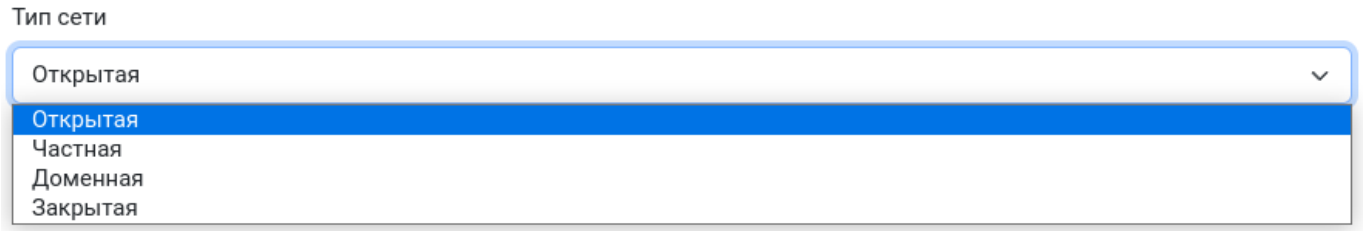


Рис. 76 – Межсетевой экран. Общие. Тип сети

На вкладке **IPv4** (рис. 77) отображаются следующие элементы:

1) кнопка **Сохранить и применить** – для сохранения и применения измененных настроек;
2) группа элементов **Правила** (рис. 78) – состоит из раскрывающегося списка, кнопок **Добавить**, **Изменить**, **Удалить**, **Вверх**, **Вниз** для управления правилами фильтрации пакетов, а также списка добавленных правил в виде таблицы.

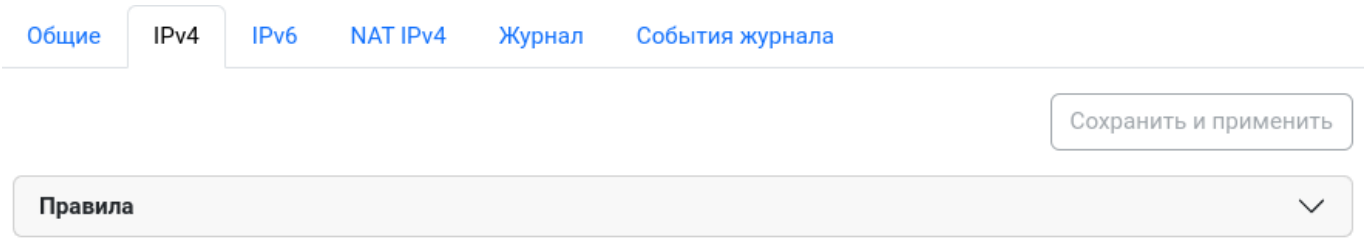


Рис. 77 – Межсетевой экран. IPv4

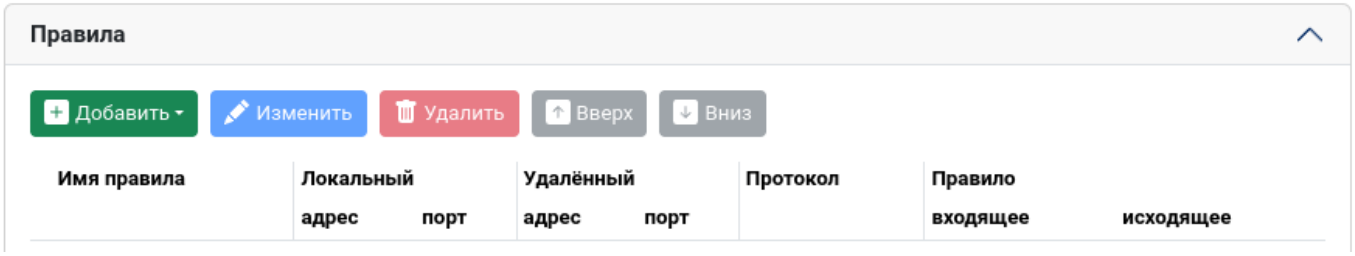


Рис. 78 – Межсетевой экран. IPv4. Правила

При нажатии на кнопку раскрывающегося списка **Добавить** появится возможность выбора типа создаваемого правила (рис. 79). Для создания доступны:

1) правило фильтрации TCP/UDP;
2) транспортное правило.

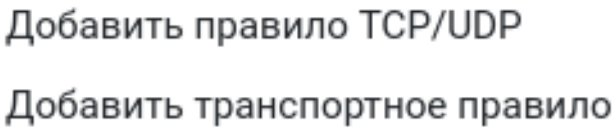


Рис. 79 – Межсетевой экран. IPv4. Добавить правило

При нажатии кнопки **Добавить правило TCP/UDP** отобразится диалоговое окно, изображенное на рис. 80. Правило фильтрации пакетов TCP/UDP состоит из следующих параметров:

1) Имя правила: строка для идентификации правила в интерфейсе вкладки IP версии 4;
2) Локальный адрес в виде IP и порта;
3) Удаленный адрес в виде IP и порта;
4) Протокол (TCP, UDP);

5) Действие для входящего правила: **Запретить**, **Разрешить** (рис. 81);
6) Действие для исходящего правила: **Запретить**, **Разрешить** (рис. 82).

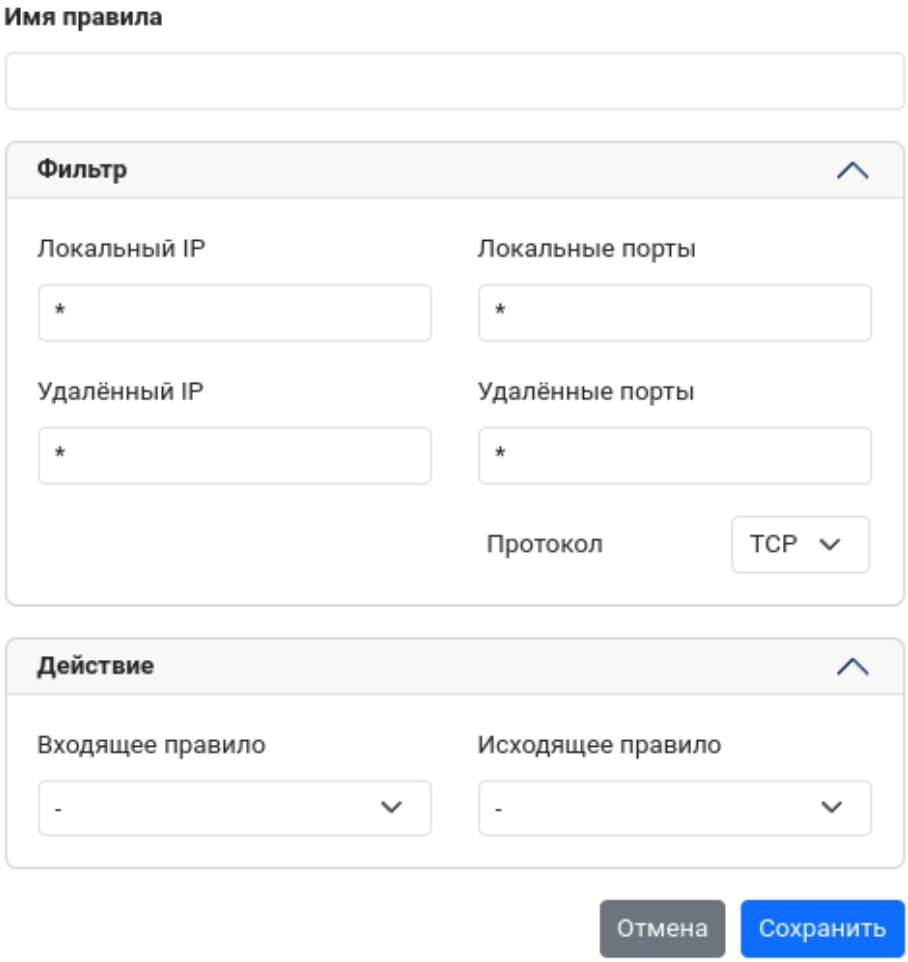


Рис. 80 – Межсетевой экран. IPv4. Окно добавления правила TCP/UDP

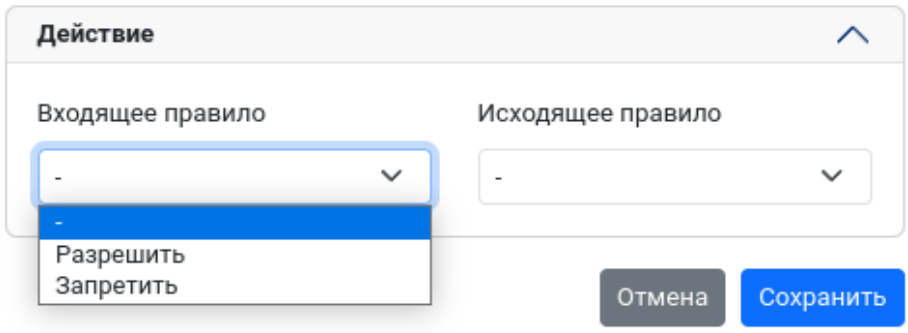


Рис. 81 – Межсетевой экран. IPv4. Окно добавления правила TCP/UDP. Действие для входящего правила

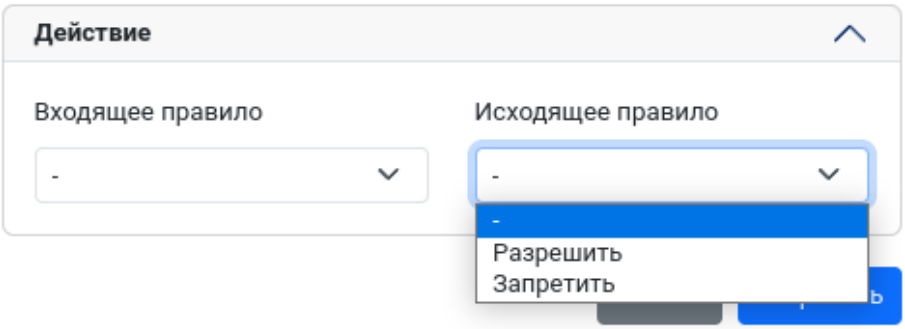


Рис. 82 – Межсетевой экран. IPv4. Окно добавления правила TCP/UDP. Действие для исходящего правила

IP-адрес задается четырьмя десятичными числами в диапазоне от 0 до 255, разделенными точками. Диалоговое окно настройки правил поддерживает несколько способов задания адресов IPv4:

1) конкретный адрес (например: 10.144.90.11);
2) диапазон в любом из четырех байт (например: 10.130-144.90.11-50);
3) регулярное выражение (если значение в каком-нибудь байте охватывает весь диапазон (т.е. от 0 до 255), то можно вместо промежутка 0-255 написать «*»); например, регулярное выражение «*.*.*.*» равнозначно одному символу «*».

Порт задается в виде десятичного числа с диапазоном значений от 0 до 65535. Способы задания портов:

1) конкретный порт (например: 80);
2) список портов (например: 25, 80);
3) диапазон портов (например: 1024-65535);
4) регулярное выражение – весь диапазон портов («*»).

Входящие правила регулируют прием пакетов, исходящие правила – их отправку. При нажатии кнопки **Добавить транспортное правило** отобразится диалоговое окно, изображенное на рис. 83.

Рис. 83 – Межсетевой экран. IPv4. Добавить транспортное правило

Диалоговое окно добавления транспортного правила межсетевого экрана программного комплекса ШХУНА состоит из:

1) текстового поля **Имя правила**, предназначенного для идентификации правила в интерфейсе вкладки **IPv4**;
2) группы элементов **Фильтр** (рис. 84), в которую входит таблица **Протоколы**, где отображены формы выбора, десятичные значения, названия и описания транспортных протоколов, текстовое поле **Другие протоколы** для указания дескрипторов протоколов, не отображенных в списке (при необходимости указать несколько дескрипторов, протоколы разделяются символом «,»), текстовые поля **Локальный IP**, **Удаленный IP** – адрес источника и адрес назначения;
3) группы элементов **Действие** (рис. 85), задающей правила обработки входящих и исходящих сетевых пакетов.

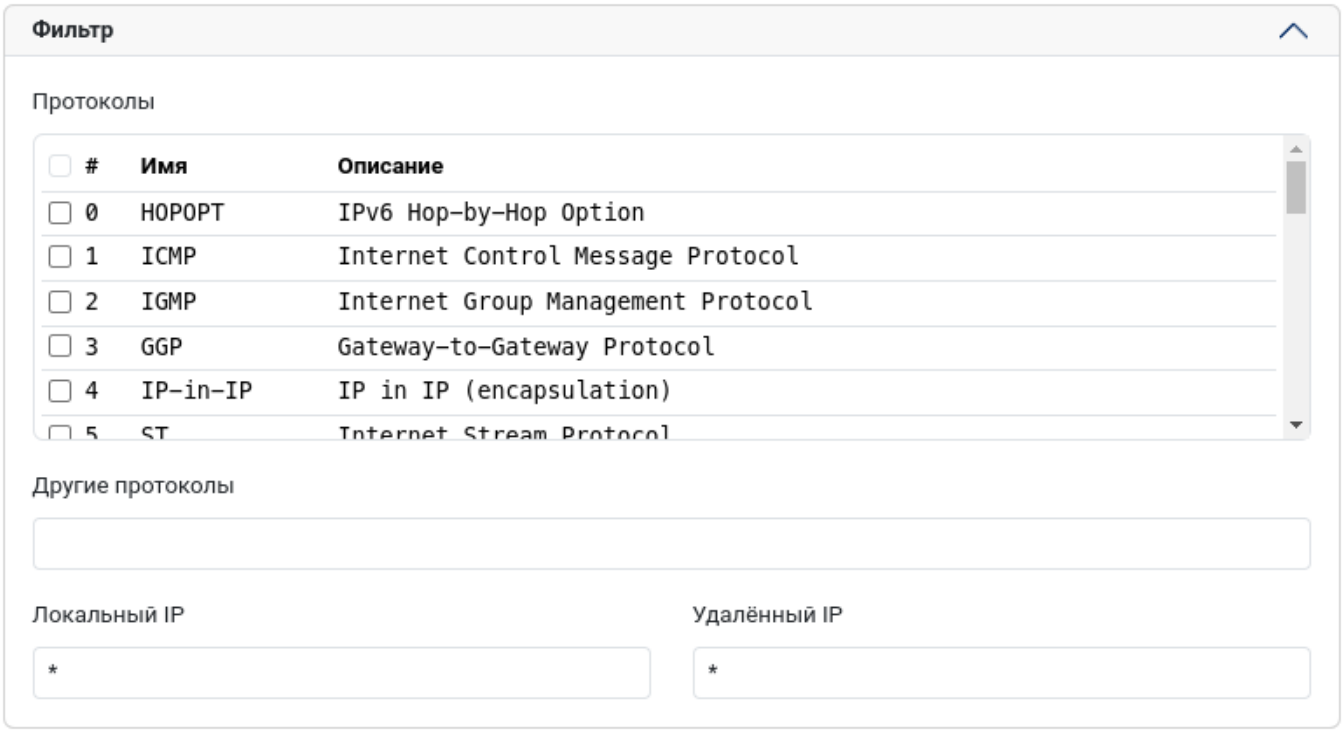


Рис. 84 – Межсетевой экран. IPv4. Добавить транспортное правило. Фильтр

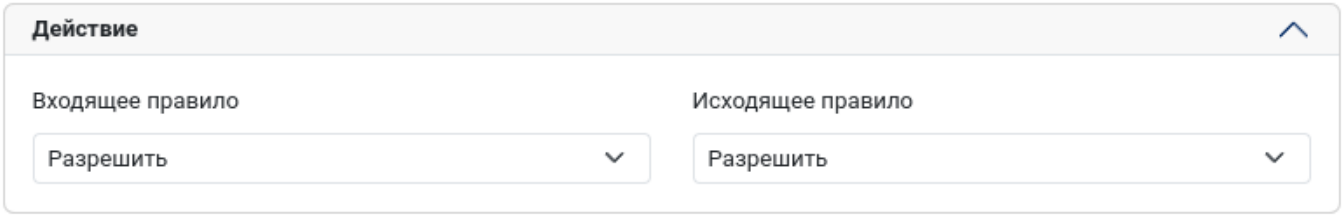


Рис. 85 – Межсетевой экран. IPv4. Добавить транспортное правило. Действие

Вкладка **IPv6** (рис. 86) полностью идентична вкладке **IPv4**, за исключением формата задания IP-адресов.

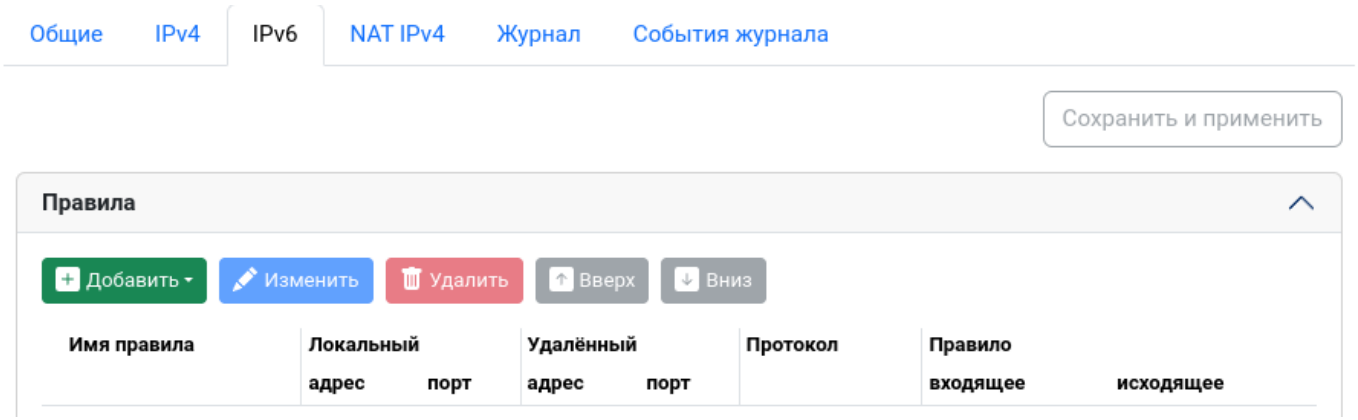


Рис. 86 – Межсетевой экран. IPv6

IPv6 адреса задаются восемью шестнадцатеричными числами, разделенными двоеточием. Диапазон каждой составляющей от 0 до FFFF. Для адресов IPv6, так же, как и для IPv4, поддерживается формат задания в виде диапазона в любой из составляющей адреса. Вместо диапазона от 0 до FFFF то можно указать просто звездочку («*»). Если каждая составляющая равна «*», то вместо адреса «*:*:*:*:*:*:*:*» можно задать «*».

Для **IPv6** поддерживается общий формат задания адресов.

1) если элемент адреса начинается с нуля, но при этом не равен нулю, то нули в начале можно не записывать, например, адрес «FF43:0000:0000:0000:0462:B1A2:0079:1235» идентичен «FF43:0000:0000:0000:462:B1A2:79:1235»;
2) если в адресе встречаются несколько подряд идущих нулевых элементов, то их можно заменить двоеточием, например, адрес «FF43:0000:0000:0000:462:B1A2:79:1235» идентичен адресу «FF43::462:B1A2:79:1235».

Примечание. Данный алгоритм действий можно сделать только для одной группы подряд идущих нулевых элементов. Т.е. адрес «FF43:0000:0000:0000:462:0000:0000:1235» нельзя записать в виде «FF43::462::1235». Можно либо так «FF43::462:0000:0000:1235», либо «FF43:0000:0000:0000:462::1235».

На вкладке **NAT IPv4** (рис. 87) отображается кнопка **Сохранить и применить** для применения измененных настроек, а также группа элементов **Правила**

состоящая из кнопок **Добавить**, **Изменить**, **Удалить**, **Вверх**, **Вниз** для управления соответствующими правилами.

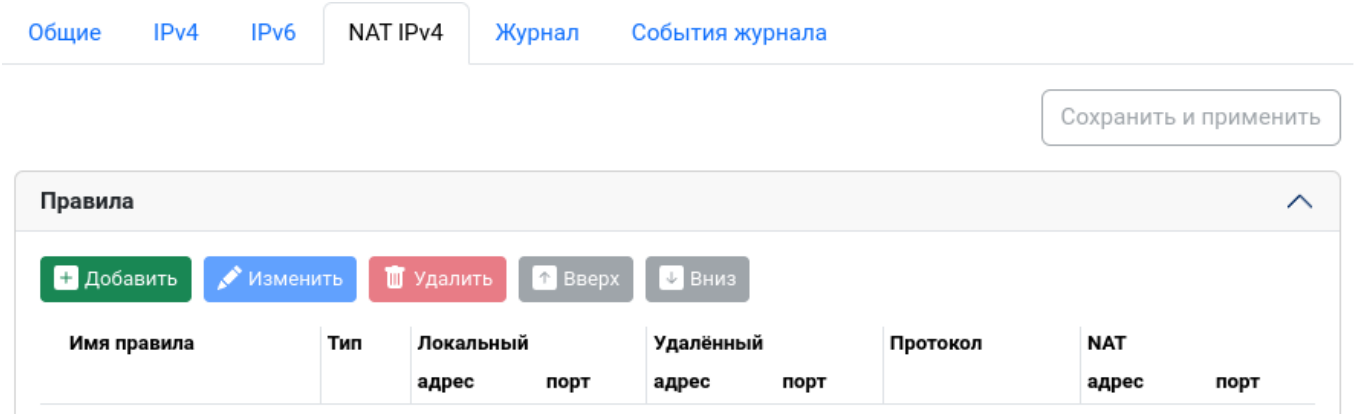


Рис. 87 – Межсетевой экран. NAT IPv4

После нажатия кнопки **Добавить** появляется диалог настройки трансляции IP-адресов (рис. 88), состоящий из:

1) текстового поля **Имя правила**, предназначенного для идентификации правила в интерфейсе вкладки **NAT IPv4** раздела **Межсетевой экран** графического интерфейса программного комплекса ШХУНА;
2) группы элементов **Фильтр** (рис. 89), состоящей из списка множественного выбора **Протоколы** для указания необходимых транспортных протоколов, текстового поля **Другие протоколы**, где можно указать дескрипторы протоколов, отсутствующие в списке, текстовых полей **Локальный IP**, **Локальные порты** и **Удаленный IP**, **Удаленные порты** для настройки трансляции адресов;
3) группы элементов **Действие**, состоящая из выпадающего списка **Тип** для выбора способа трансляции адреса (SNAT/DNAT) (рис. 90). При выборе типа SNAT в каждом пакете, проходящем через фильтр будет заменен адрес источника, тип DNAT будет заменять адрес назначения;
4) **NAT адрес / NAT порты** – адрес шлюза (пограничного сетевого интерфейса), который будет осуществлять трансляцию IP-адресов между локальной и удаленной сетями.

Рис. 88 – Межсетевой экран. NAT IPv4. Добавить правило

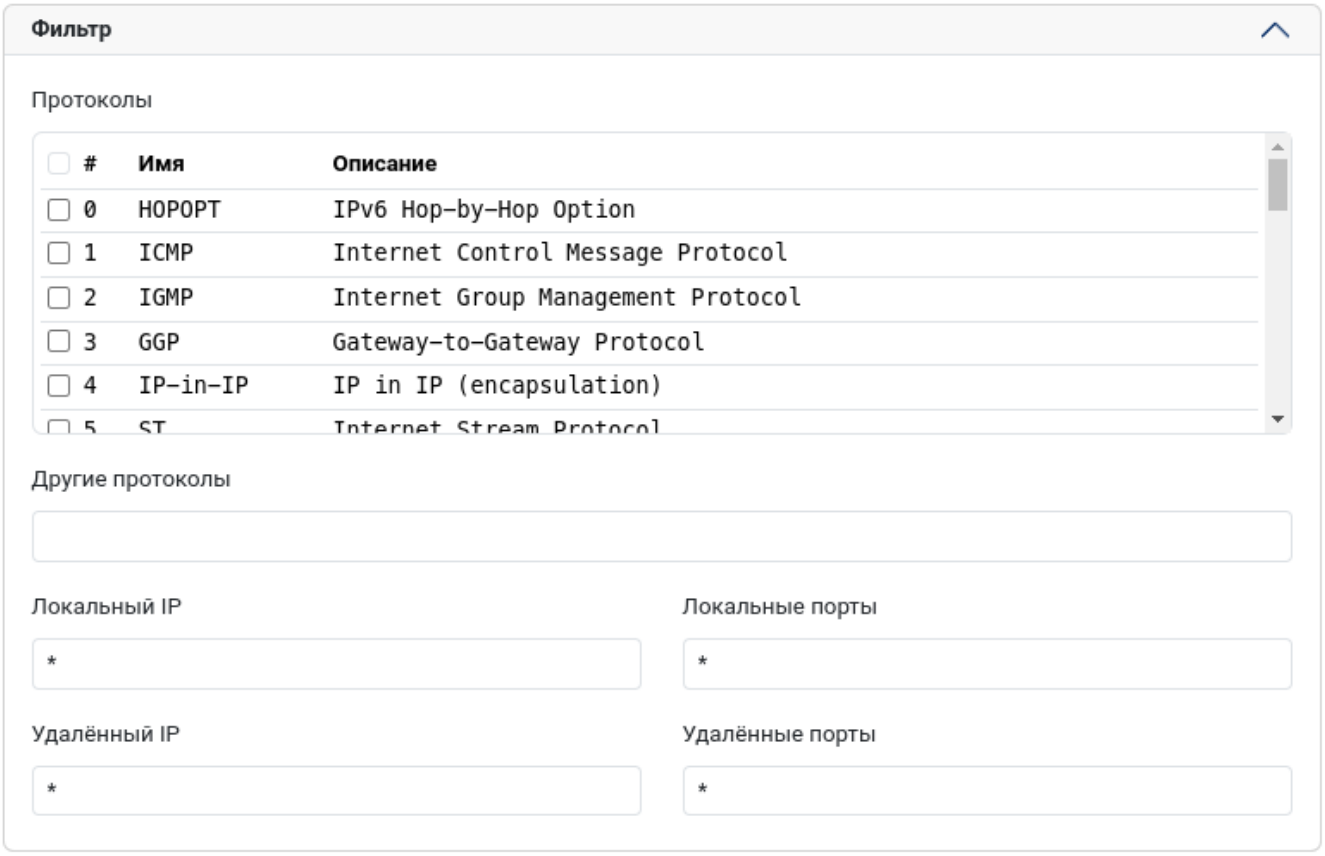


Рис. 89 – Межсетевой экран. NAT IPv4. Добавить правило. Фильтр

Рис. 90 – Межсетевой экран. NAT IPv4. Добавить правило. Действие

На вкладке **Журнал** отображаются события, сгенерированные модулем межсетевого экрана, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 91) используется для настройки того, где будет записано то или иное событие.

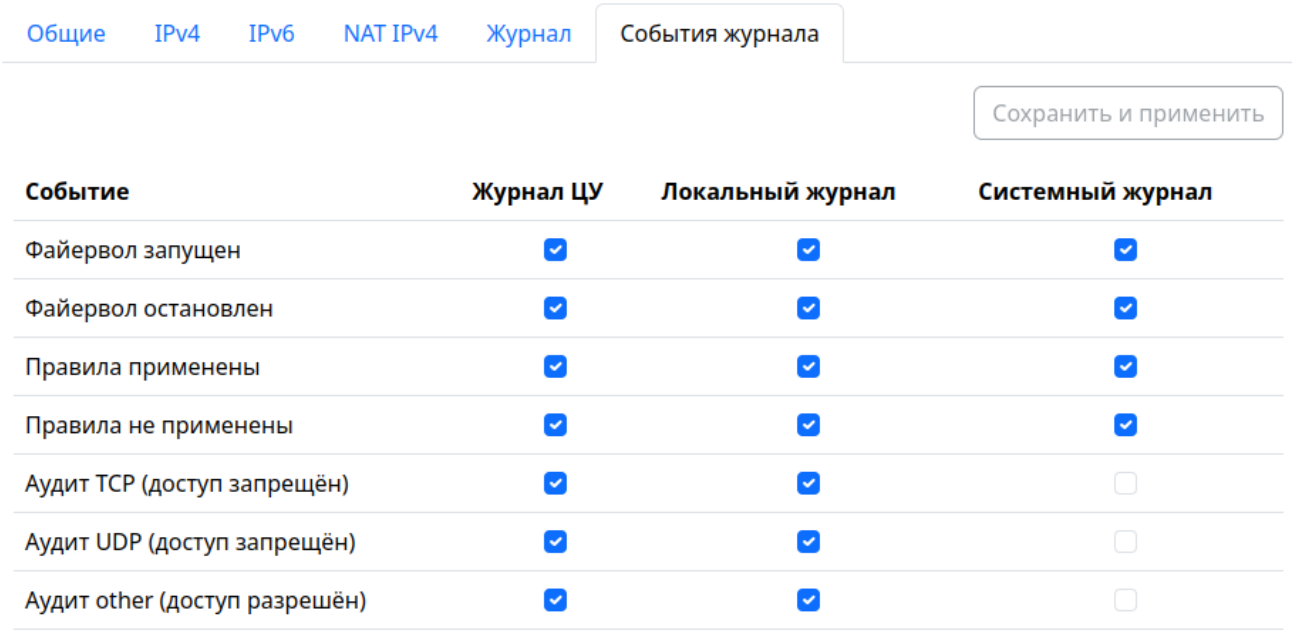


Рис. 91 – Межсетевой экран. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.10. Раздел Карантин

Раздел **Карантин** предназначен для безопасного хранения инфицированных и/или подозрительных объектов, обнаруженных во время антивирусной проверки (компонентами **Монитор** или **Антивирусный сканер**).

На вкладке **Информация об объектах** (рис. 92) предоставлен список объектов, попавших в **Карантин** при антивирусной проверке.

На вкладке отображаются: элемент выбора файла для помещения в **Карантин** (после нажатия кнопки **Выберите файл** будет показан стандартный диалог оконного менеджера для выбора файла), кнопка **Загрузить файл** для загрузки файла в **Карантин**, группа элементов **Объекты**, состоящая из:

1) кнопки **Восстановить** – для восстановления объекта по первоначальному пути (для ложных срабатываний);
2) кнопки **Восстановить в** – для восстановления по выбранному пользователем пути;
3) кнопки **Удалить** – удаления файла и записи о нем из Карантина.

При работе со списком объектов есть возможность выбрать несколько или все элементы списка для совершения одновременного действия. Для выбора нескольких элементов необходимо отметить форму выбора в левой колонке таблицы списка. Для выбора всех элементов необходимо отметить форму выбора рядом с названием столбца таблицы **Имя объекта**.

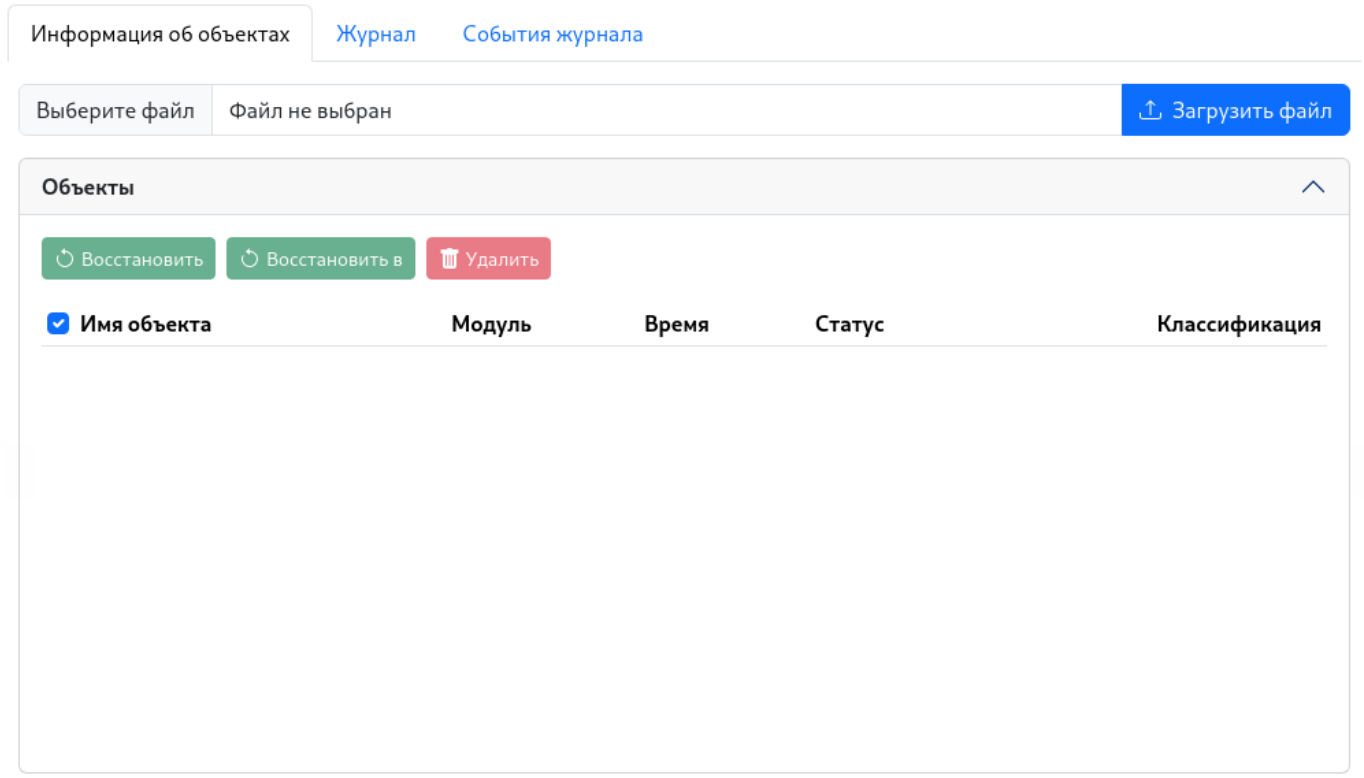


Рис. 92 – Карантин. Информация об объектах

На вкладке **Журнал** отображаются события, сгенерированные модулем карантин, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 93) используется для настройки того, где будет записано то или иное событие.

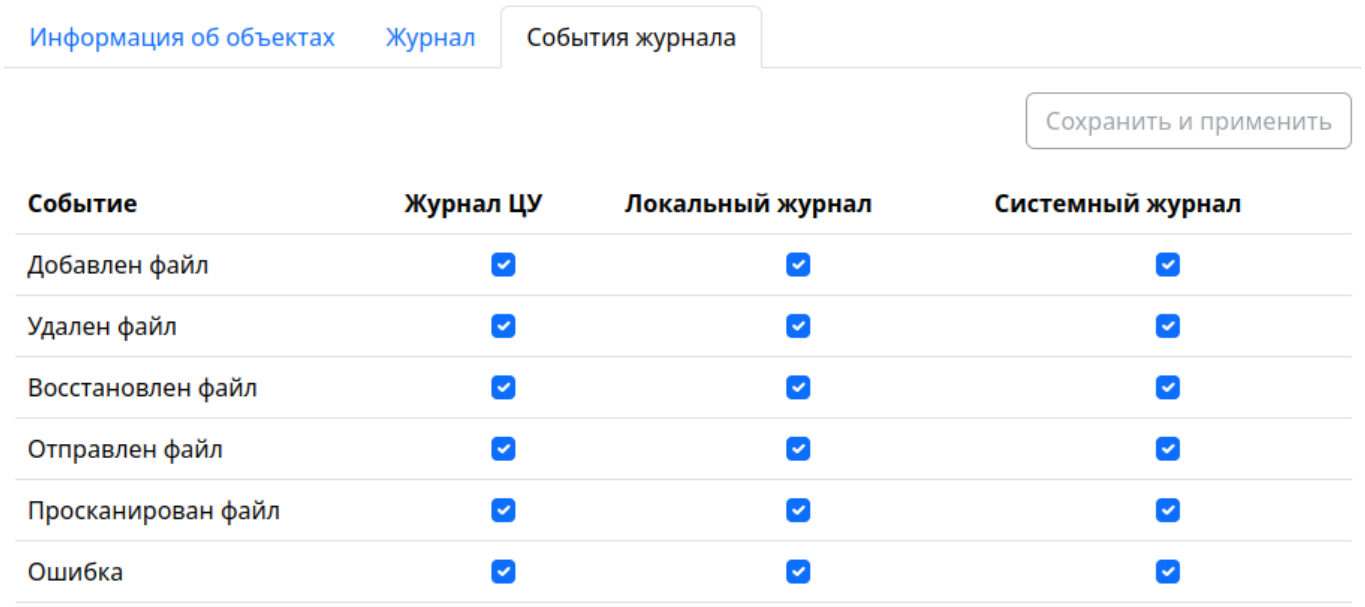


Рис. 93 – Карантин. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.11. Раздел Целостность

Раздел **Целостность** предназначен для настройки задачи контроля неизменности файлов, директорий и устройств СВТ.

На вкладке **Файлы и устройства** (рис. 94) расположены следующие элементы:

1) кнопка раскрывающегося списка **Проверить** – для проверки неизменности файлов и устройств;
2) кнопка раскрывающегося списка **Сохранить** – для сохранения данных о неизменности файлов и устройств;
3) кнопка **Сохранить и применить** – для применения измененных настроек;
4) группа элементов **Файлы** – для управления путями и масками контроля неизменности.

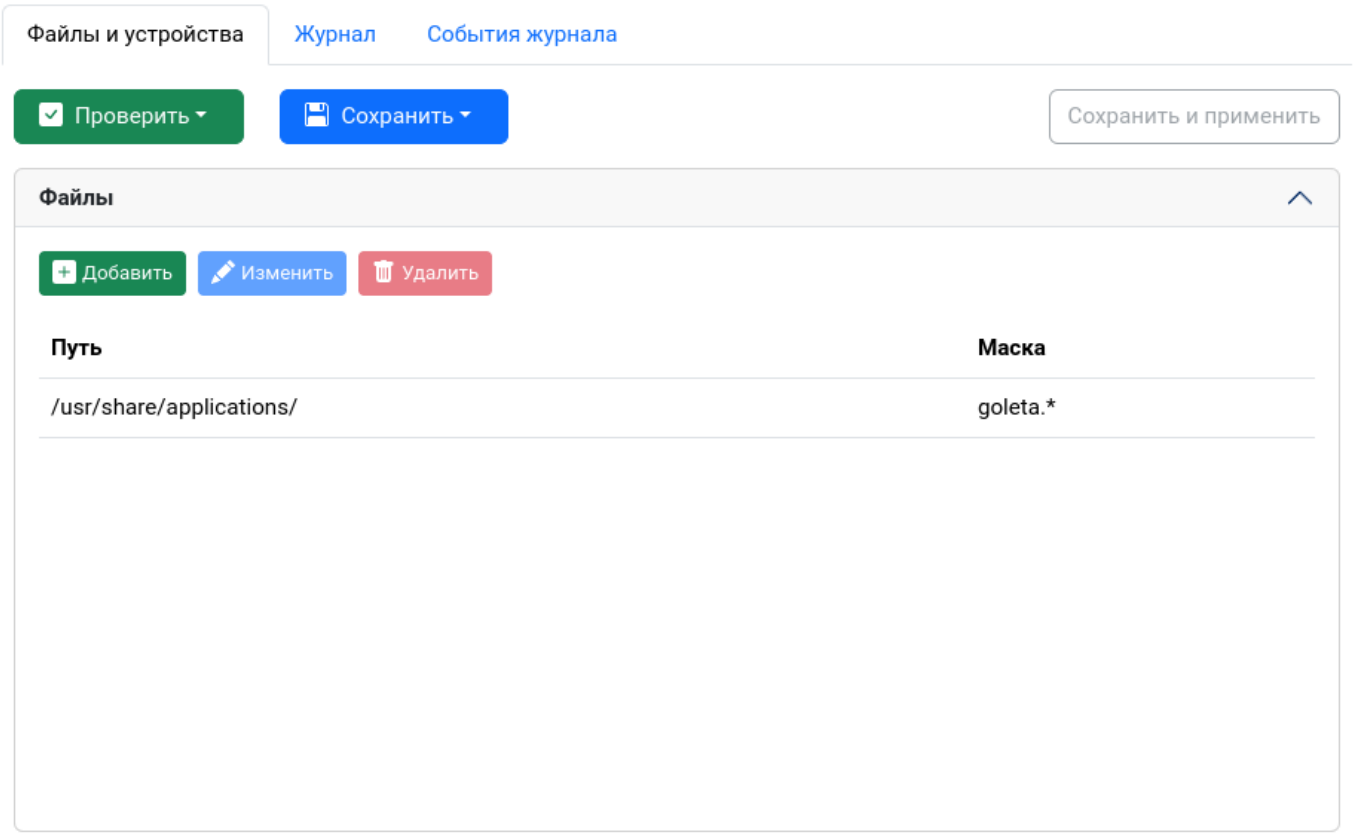


Рис. 94 – Целостность. Файлы и устройства

При нажатии на кнопку раскрывающегося списка **Проверить** будет предложено проверить неизменность файлов или неизменность устройств.

При нажатии на кнопку раскрывающегося списка **Сохранить** будет предложено сохранить неизменность файлов или неизменность устройств.

Группа элементов **Файлы** состоит из:

1) кнопки **Добавить** – для добавления пути к директории и маски файла для контроля неизменности;
2) кнопки **Изменить** – для изменения существующей записи;
3) кнопки **Удалить** – для удаления существующей записи.

После добавления элемента он будет отображен в таблице в составе группы элементов.

На вкладке **Журнал** отображаются события, сгенерированные модулем контроля неизменности, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 95) используется для настройки того, где будет записано то или иное событие.

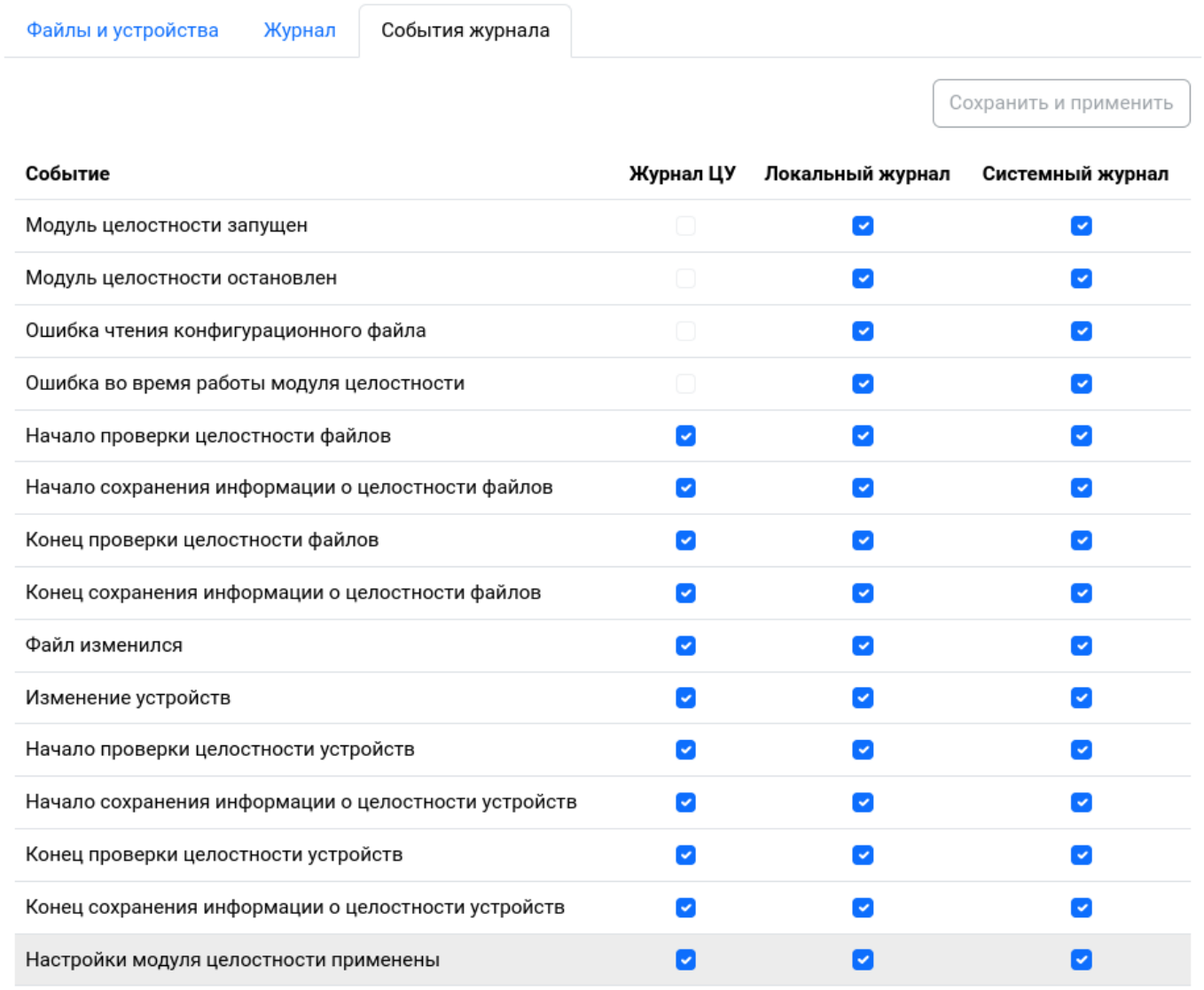


Рис. 95 – Целостность. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.4.12. Раздел Шредер

Раздел **Шредер** предназначен для настройки и запуска модуля удаления программного комплекса ШХУНА.

На вкладке **Настройки** (рис. 96) отображаются:

1) кнопка **Запустить** – запуск модуля удаления;
2) кнопка **По умолчанию** – сброс настроек по умолчанию;
3) кнопка **Сохранить и применить** – применение измененных настроек;
4) группа элементов **Шаблоны**;
5) группа элементов **Пути и маски** для выбранного шаблона.

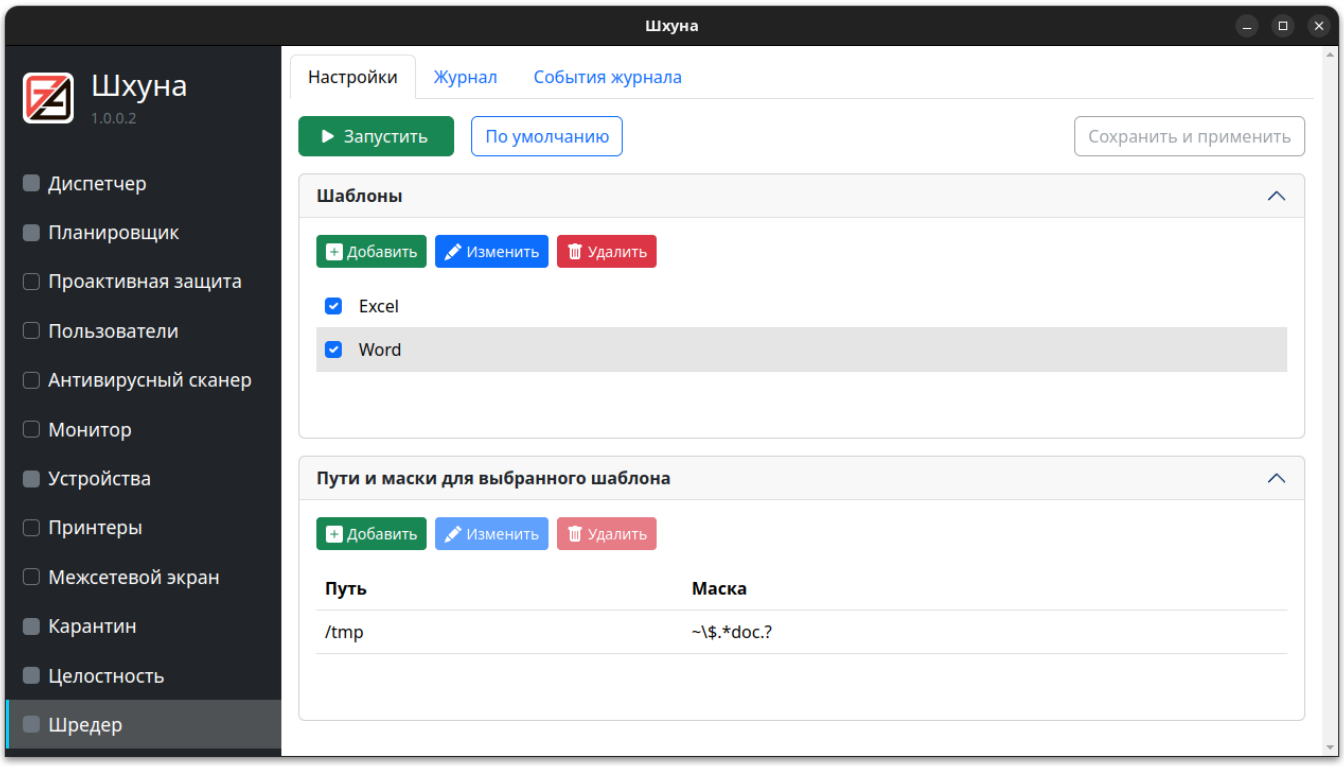


Рис. 96 – Шредер. Настройки

Для настройки шаблона необходимо нажать кнопку **Добавить** в списке имен шаблонов и в появившемся диалоговом окне (рис. 97) ввести имя для идентификации шаблона в списке (например, Excel). После этого необходимо нажать кнопку **Добавить** в группе элементов **Пути и маски для выбранного шаблона**. В появившемся диалоговом окне (рис. 98) необходимо выбрать (или ввести вручную) директорию поиска (например, `/tmp`) и маску для поиска файлов (например, `~\$.*.xls.?`).

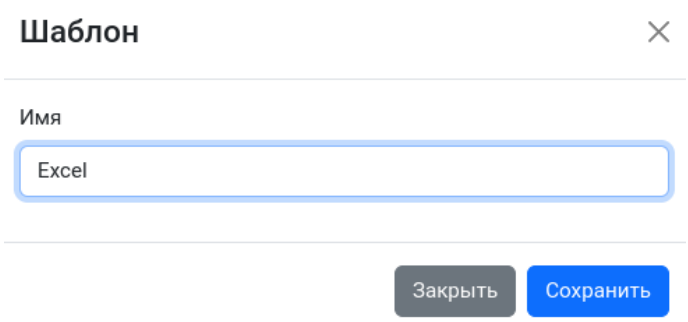


Рис. 97 – Шредер. Имя шаблона

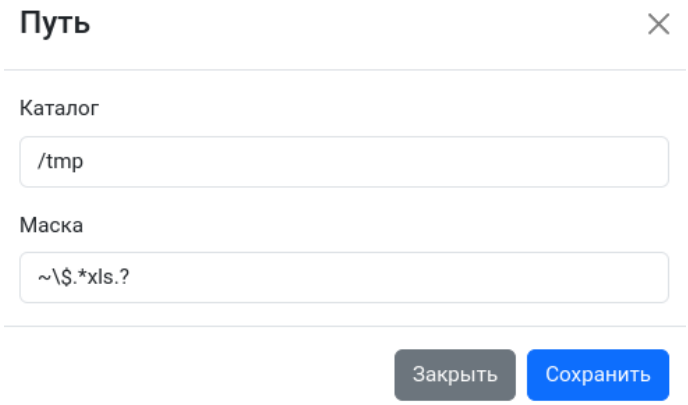


Рис. 98 – Шредер. Пути и маски для выбранного шаблона

Примечание. Формирование масок файлов происходит по правилам составления регулярных выражений. Для составления регулярных выражений необходимо соблюдать следующие правила:

1) регулярное выражение состоит из буквенно-цифрового набора, символов «$», «^», «*», «?»;
2) символы «$», «^», «*», «?» интерпретируются, соответственно, как конец строки, начало строки, любое количество символов, один любой символ;
3) если необходимо использовать символы «$», «^», «*», «?» в качестве элементов имени файла, их необходимо «экранировать», предваряя их написание символом «\»;
4) маска из примера: «~\$.*.xls.?» означает набор файлов, имя которых начинается с символа «~», после которого должен находиться символ «$». Далее имя файла может представлять из себя любой набор символов в конце

которых последовательность «.xls», после которой может быть еще один любой символ.

На вкладке **Журнал** отображаются события, сгенерированные модулем контроля неизменности, отмеченные соответствующими формами выбора на вкладке **События журнала**.

Вкладка **События журнала** (рис. 99) используется для настройки того, где будет записано то или иное событие.

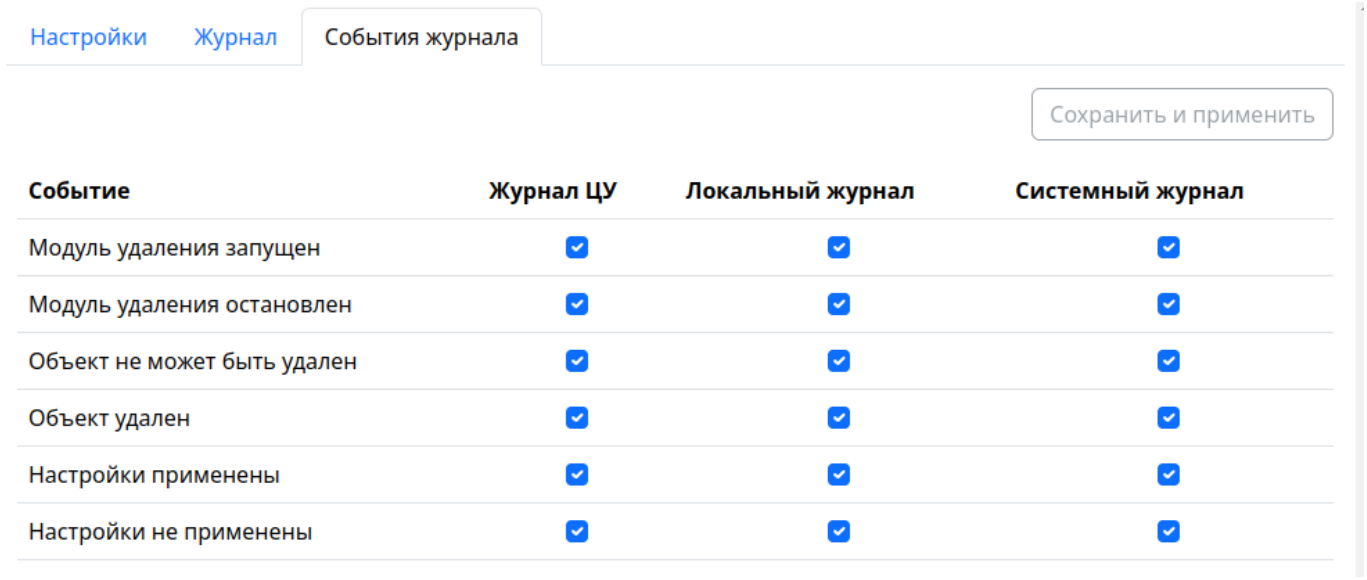


Рис. 99 – Шредер. События журнала

Примечание. При использовании программного комплекса ШХУНА необходимо учитывать, что по умолчанию комплекс записывает в журналы все генерируемые события. При эксплуатации программного комплекса ШХУНА администратором безопасности должно быть принято решение о сохранении либо сокращении перечня записываемых событий, с учетом опыта использования СЗИ конкретной информационной системы.

4.5. Исполнение ЦУ

4.5.1. Активация продукта

После установки продукта необходимо обновить информацию о лицензии, предоставив регистрационный ключ.

Для этого необходимо запустить веб-интерфейс ЦУ, авторизоваться (см. п. 4.6) и обновить регистрационный ключ с помощью кнопки **Обновить ключ** на странице **Главная** (рис. 100).

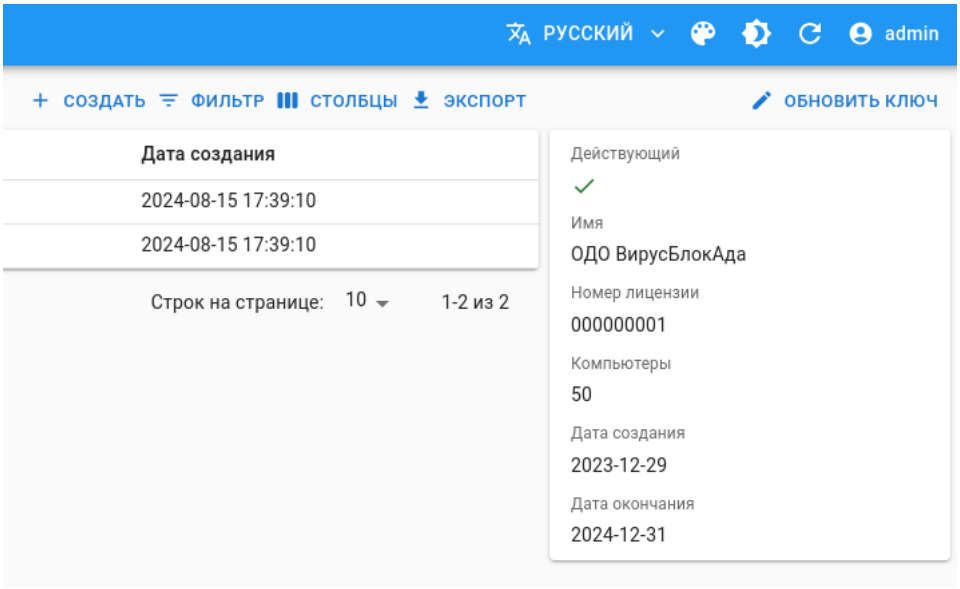


Рис. 100 – ЦУ. Обновить ключ

Окно выбора лицензии показано на рис. 101.

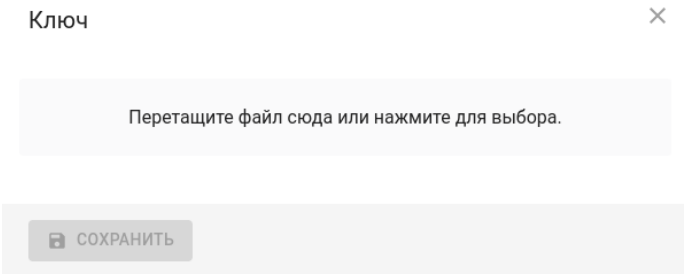


Рис. 101 – ЦУ. Обновить ключ. Окно выбора лицензии

После выбора файла лицензии программный комплекс ШХУНА перейдет в полнофункциональный режим, о чем будет свидетельствовать соответствующий знак ✓ и полная информация о лицензии (рис. 100).

4.6. Работа ЦУ

Для доступа к графическому интерфейсу ЦУ в адресной строке браузера используйте IP-адрес СВТ, на котором установлен ЦУ, а в качестве данных авторизации для первого запуска: **«admin/1234qwer!»** (роль Администратор) и **«observer/asdf4321$»** (роль Наблюдатель).

Последующее изменение данных авторизации и управление пользователями осуществляет Администратор (в целях обеспечения безопасности он должен установить новые пароли, которые будут не совпадать с паролями авторизации для первого запуска).

Внешний вид страницы авторизации представлен на рис. 102.

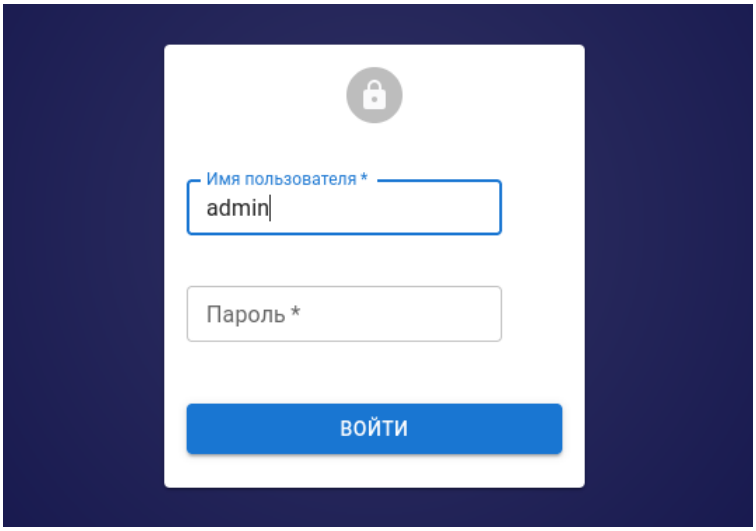


Рис. 102 – ЦУ. Страница авторизации

4.6.1. Раздел Главная

На главной странице представлены интерфейс управления пользователями (включая назначение ролей), а также информация о ключевом файле (лицензии) и возможность его изменения/обновления (рис. 103).

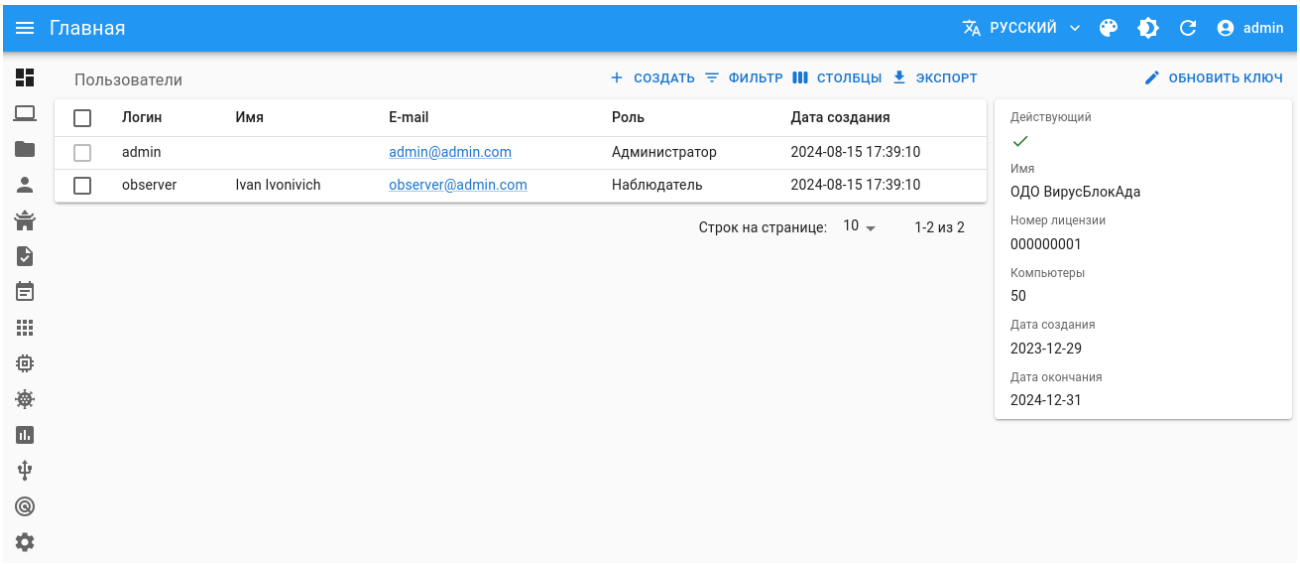


Рис. 103 – ЦУ. Раздел «Главная»

Раздел **Главная** содержит область управления пользователями ЦУ (рис. 104).

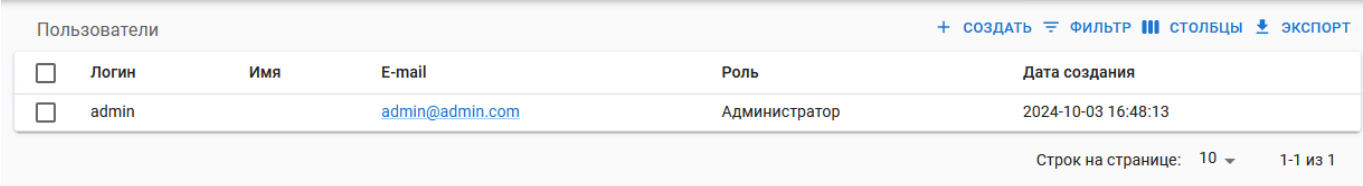


Рис. 104 – ЦУ. Раздел «Главная».
Управление пользователями ЦУ. Администратор

Также раздел **Главная** содержит область, где осуществляется управление лицензией и ключевым файлом (рис. 105).

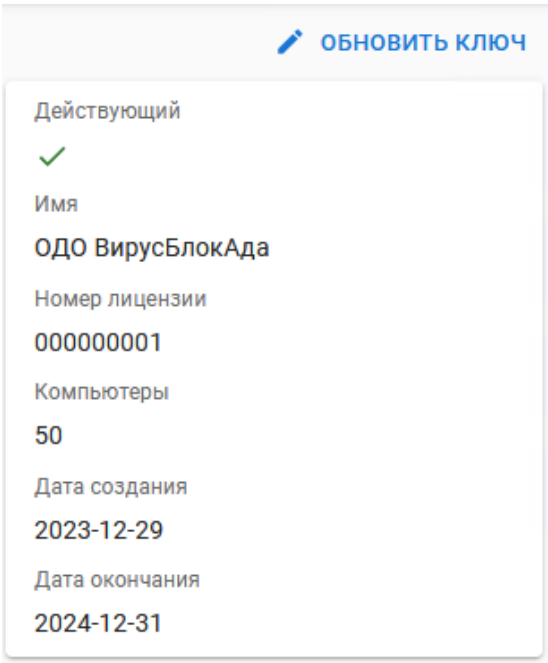


Рис. 105 – ЦУ. Раздел «Главная».
Управление лицензией

При первом входе в графический интерфейс ЦУ пользователю будет выдано предупреждение об отсутствующем лицензионном ключе (рис. 106).

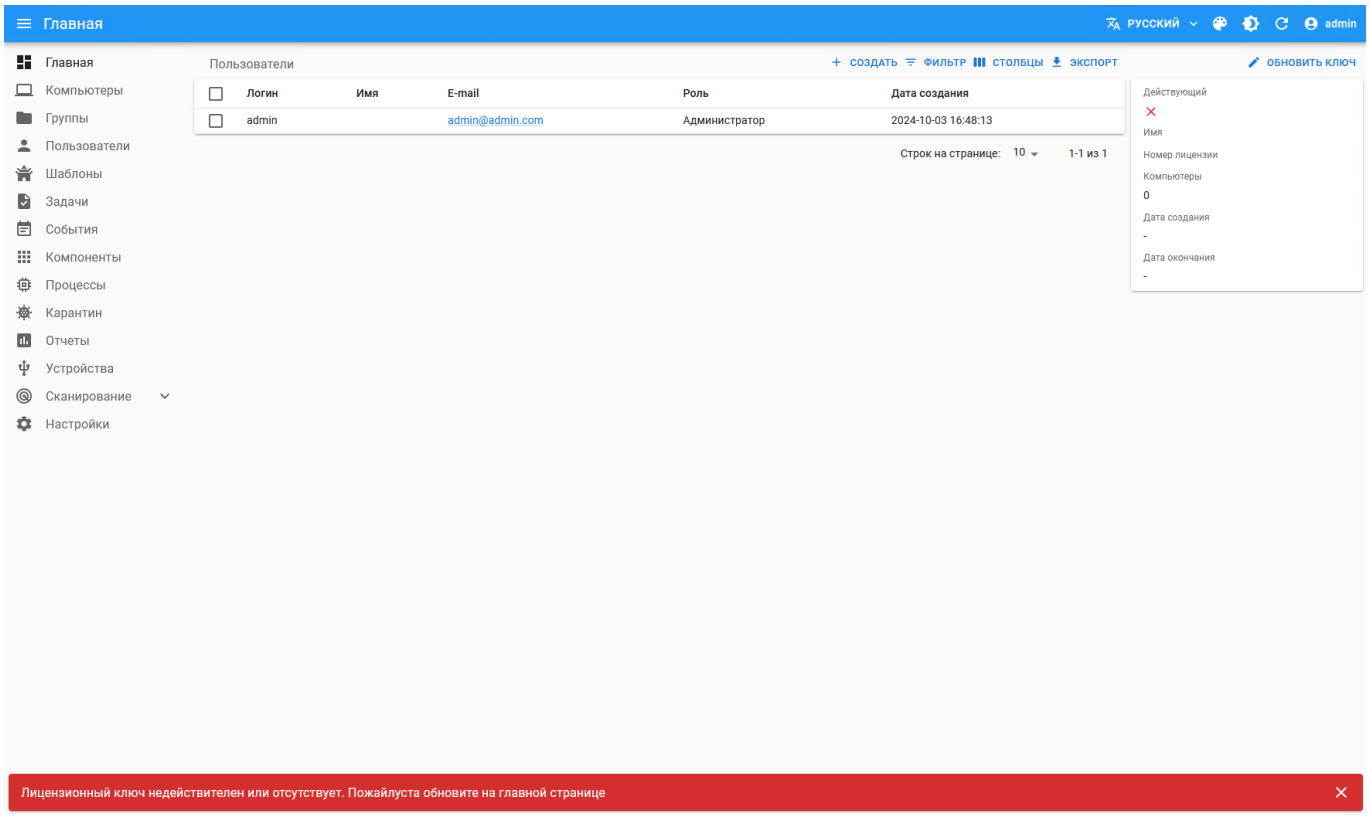


Рис. 106 – ЦУ. Раздел «Главная».
Недействительная лицензия

Добавить новый ключевой файл можно при помощи кнопки **Обновить ключ**: в открывшемся модальном диалоговом окне осуществляется выбор необходимого файла с расширением .key (рис. 107).

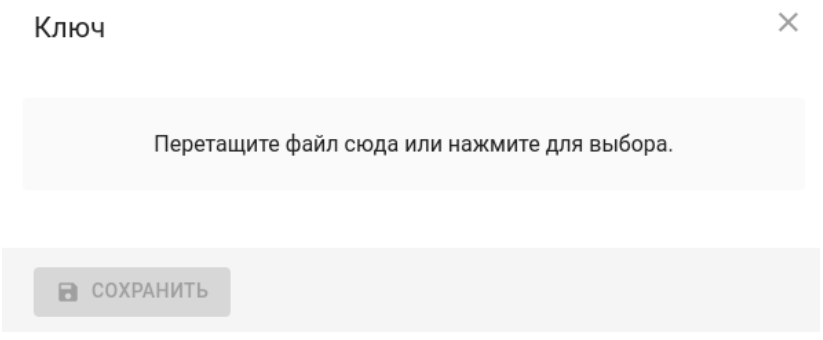


Рис. 107 – ЦУ. Обновить ключ. Окно выбора лицензии

После нажатия на кнопку **Сохранить** выбранный ключевой файл добавится в ЦУ и отобразится в соответствующей информационной секции.

В секции ключевого файла будет отображено:

– действителен ли текущий ключ или не действителен;
– имя организации или лица, для которого выдан ключевой файл;
– номер лицензии;
– количество компьютеров доступных в этом варианте лицензии;
– дата создания ключевого файла;
– дата окончания действия ключевого файла.

Секция **Пользователи** представляет собой таблицу с перечислением существующих пользователей ЦУ. Информация о пользователе включает в себя поля:

– логин;
– имя пользователя;
– e-mail;
– роль;
– дата создания учетной записи.

Кнопка **Создать** служит для добавления нового пользователя (рис. 108).

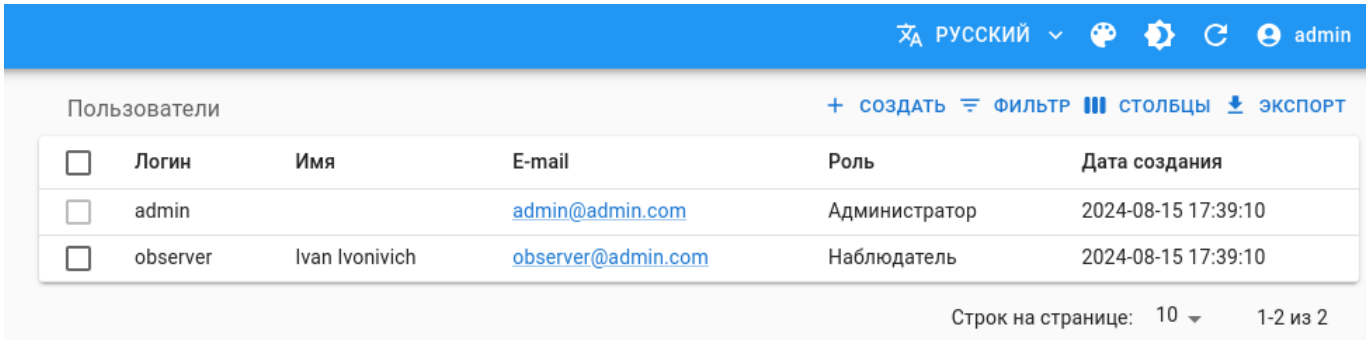


Рис. 108 – ЦУ. Раздел «Главная».
Пользователи. Подробно

Для создания нового пользователя в форме **Создать** (рис. 109) необходимо указать логин, под которым новый пользователь будет входить в систему, имя, адрес электронной почты, пароль и выбрать возможную роль (Администратор – доступны все действия, Наблюдатель – роль с ограниченными правами, предназначенная для наблюдения за событиями аудита).

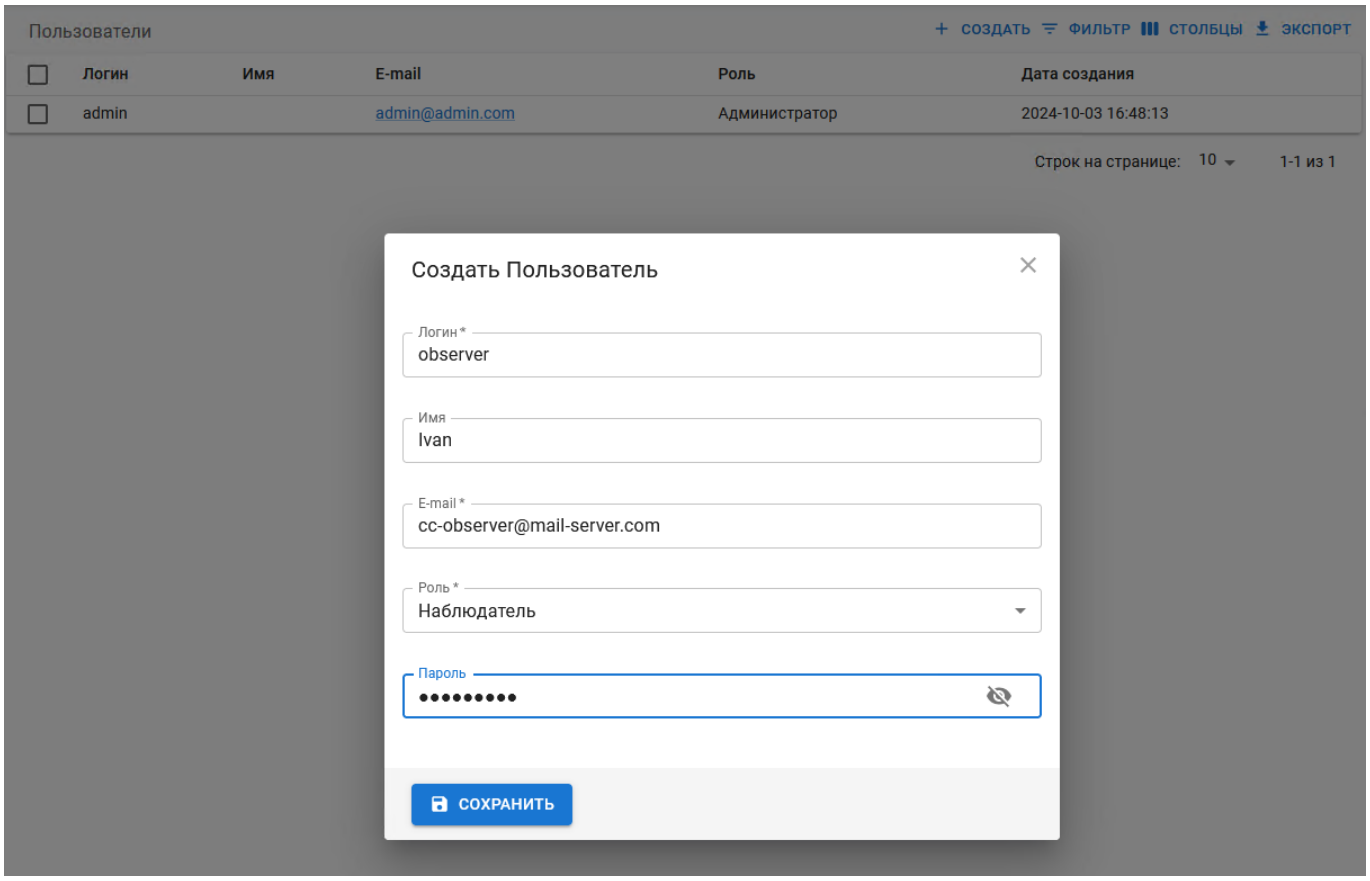


Рис. 109 – ЦУ. Раздел «Главная».
Пользователи. Создание нового пользователя

После сохранения созданного пользователя его данные можно изменить по нажатию ЛКМ в области полей **Логин**/**Имя**. Удалить выбранный профиль пользователя можно при помощи кнопки **Удалить**.

Также существует возможность осуществлять поиск пользователей по определенным критериям при помощи фильтра, используя кнопку **Фильтр** (рис. 108). Выполнить поиск можно по полям таблицы **Пользователи**.

Результаты работы фильтра сразу же отображаются в таблице **Пользователи** после заполнения всех необходимых полей. Сбросить значение фильтров можно нажав на кнопку **Фильтр** повторно.

Кнопка **Столбцы** предоставляет возможность выбора отображаемых колонок на странице для текущей сессии пользователя. Выбор столбцов осуществляется при помощи выпадающего списка.

Возможно выполнить настройку очередности показа столбцов при помощи

перетаскивания имени столбца в списке. Для этого предназначен элемент управления .

Данные находящиеся в таблице **Пользователи** могут быть экспортированы с помощью кнопки **Экспорт** (рис. 108).

Существует возможность выбрать количество отображаемых строк на странице. Это можно выполнить с помощью элемента **Строк на странице** (с возможными значениями: 5, 10, 25, 50).

4.6.2. Раздел Компьютеры

Выбор раздела **Компьютеры** в графическом интерфейсе ЦУ осуществляется выбором соответствующего пункта в левом меню (рис. 110).

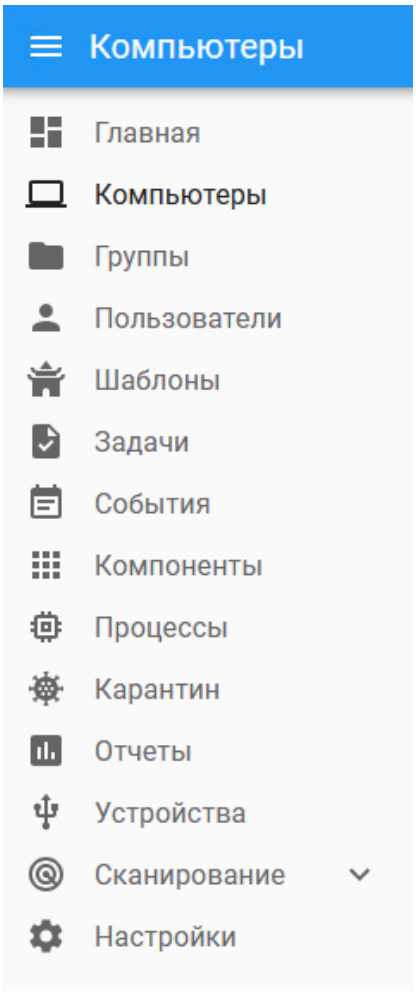


Рис. 110 – ЦУ. Раздел Компьютеры. Выбор пункта меню

Раздел **Компьютеры** предназначен для мониторинга и управления подключенными к сети устройствами. На этой странице отображается список

компьютеров с информацией об их состоянии, типе и версии ОС, пользователях, версии установленного программного обеспечения и активности. Администратор может наглядно оценить состояние каждого компьютера, видеть активные устройства, проверять наличие лицензий, создавать задачи для управления компьютерами, а также фильтровать и экспортировать данные для дальнейшего анализа (рис. 111).

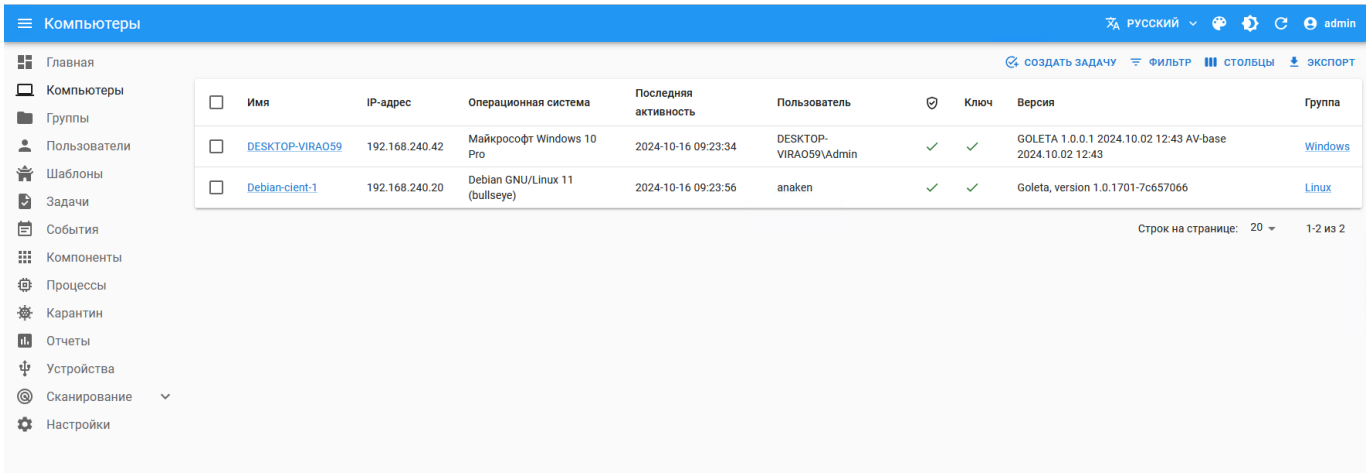


Рис. 111 – ЦУ. Раздел Компьютеры. Общий вид

На странице **Компьютеры** отображается список подключенных к ЦУ компьютеров (рис. 112).

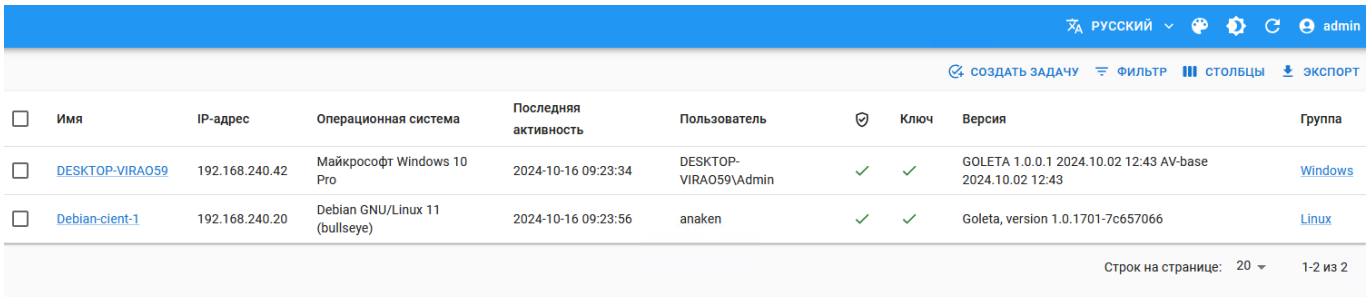


Рис. 112 – ЦУ. Раздел Компьютеры. Таблица

Примечание. Некоторые из столбцов таблицы скрыты (по умолчанию) настройками, которые можно изменить с помощью кнопки **Столбцы** в правой верхней части графического интерфейса ЦУ (рис. 113).

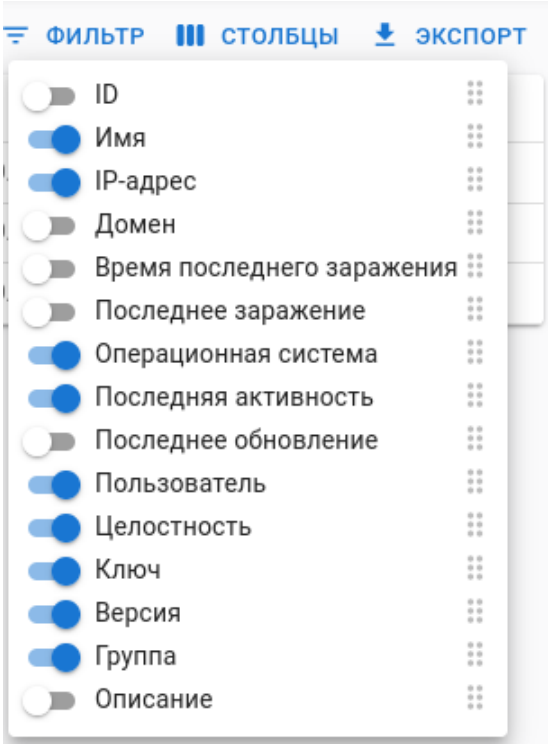


Рис. 113 – ЦУ. Раздел Компьютеры. Таблица. Выбор столбцов

Перечень столбцов таблицы **Компьютеры** содержит:

1) **Имя** – имя клиентского СВТ в сети (пример: `DESKTOP-VIRAO59`, `Debian-client-1`);
2) **IP-адрес** – IP-адрес каждого компьютера (пример: `192.168.240.42`, `192.168.240.20`);
3) **Операционная система** – информация о типе и версии установленной ОС. (пример: `Майкрософт Windows 10 Pro`, `Debian GNU/Linux 11 (bullseye)`);
4) **Последняя активность** – время последней зафиксированной активности компьютера (пример: `2024-10-16 09:23:34`);
5) **Пользователь** – имя пользователя, под которым был выполнен вход на данный компьютер (пример: `DESKTOP-VIRAO59\Admin`, `anaken`);
6) **Целостность** – индикатор состояния неизменности программного комплекса ШХУНА (пример: иконка ✓ в этом столбце указывает, что целостность программного комплекса ШХУНА не нарушена);
7) **Ключ** – индикатор состояния лицензии или защиты компьютера (пример: иконка ✓ в этом столбце указывает, что ключ является действующим);

8) **Версия** – версия установленного ПО (пример: `GOLETA 1.0.0.1 2024.10.02 12:43 AV-base 2024.10.02 12:43`);
9) **Группа** – группа, к которой относится данный компьютер (пример: `Windows` или `Linux`);
10) **ID** – столбец с порядковым номером компьютера;
11) **Домен** – имя домена которому принадлежит компьютер (пример: `WORKGROUP`);
12) **Время последнего заражения** – дата и время последнего обнаружения ВПО на данном клиентском СВТ;
13) **Последнее заражение** – информация об имени найденного заражения;
14) **Последнее обновление** – дата и время, когда было выполнено обновление клиентской части программного комплекса ШХУНА;
15) **Описание** – текстовая информация, которую можно добавить к компьютеру.

В правой верхней части графического интерфейса ЦУ (рис. 112) находятся кнопки для выполнения различных действий:

1) **Создать задачу** – позволяет создать новую задачу для одного или нескольких клиентских СВТ;
2) **Фильтр** – дает возможность отфильтровать компьютеры по заданным параметрам;
3) **Столбцы** – настройка отображаемых столбцов в таблице;
4) **Экспорт** – экспорт данных о компьютерах в файл `.csv`-формата.

Также под таблицей находится выпадающее меню, при помощи которого можно установить количество строк, отображаемых на странице и общее количество записей.

Получить детальную информацию о подключенном к ЦУ клиентском СВТ, можно при помощи нажатия ЛКМ по имени компьютера. Будет выведена детальная информация о данном компьютере (рис. 114).

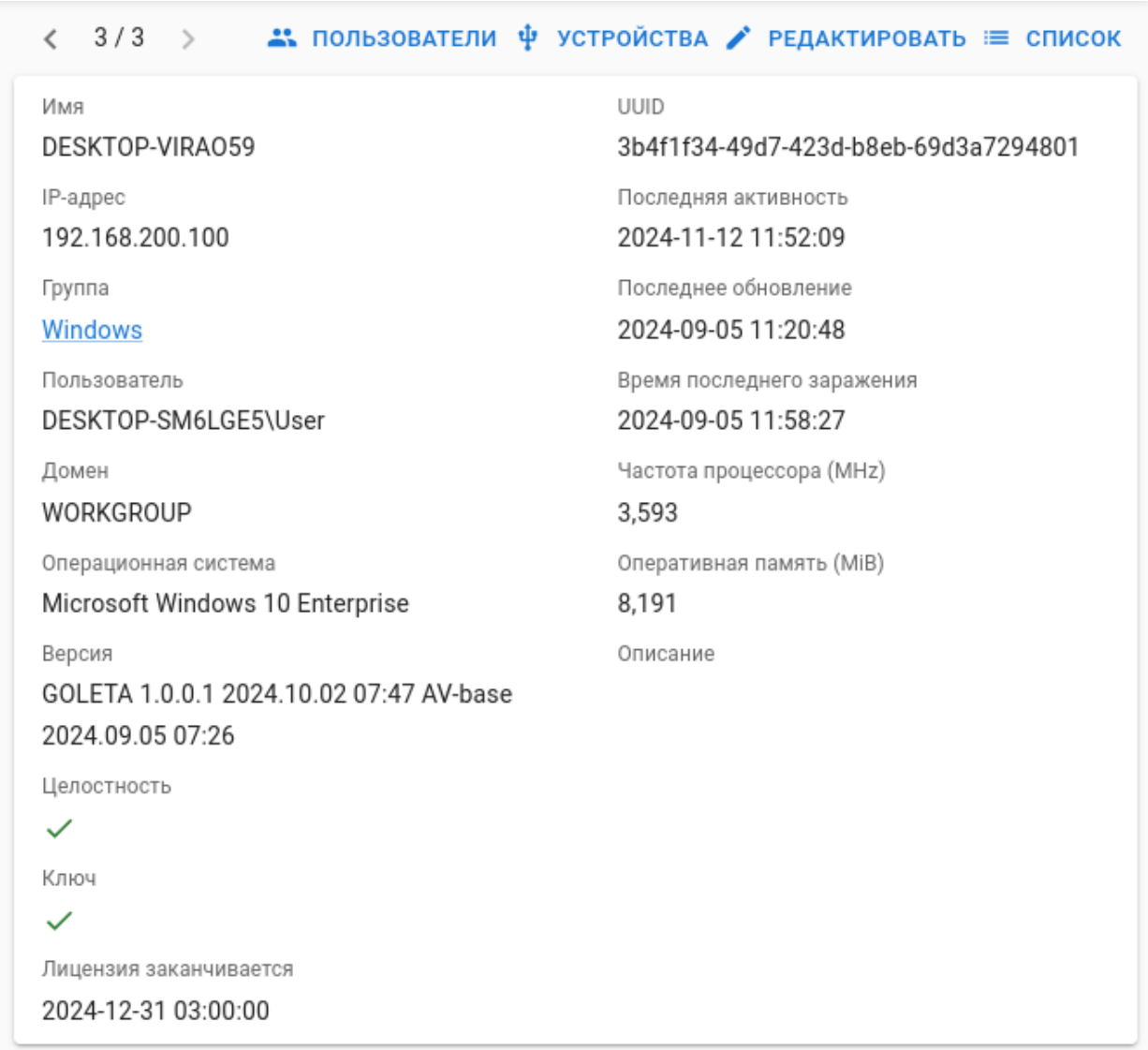


Рис. 114 – ЦУ. Раздел Компьютеры.
Детальная информация о компьютере

В верхней правой части расположены элементы навигации в виде кнопок. В результате нажатия на кнопку **Пользователи** будет осуществлен переход на страницу со всеми пользователями, которые присутствуют в ОС на клиентском СВТ.

В результате нажатия на кнопку **Устройства** будет осуществлен переход на страницу устройств, которые зарегистрированы на компьютере, детальная информация о котором выбрана. При этом автоматически будет применен фильтр ограничивающий список устройств, подсоединенных только к данному компьютеру.

В результате нажатия на кнопку **Редактировать** будет выведен диалог, который позволит отредактировать некоторые поля детальной информации о выбранном

компьютере. Например, можно добавить описание, которое будет отображено в таблице компьютеров (рис. 112). Также в этом диалоге можно определить к какой группе должен относиться этот компьютер. Для этого следует выбрать группу из выпадающего списка **Группа**.

В результате нажатия на кнопку **Список** будет выполнен переход на страницу **Компьютеры** с отображением таблицы всех компьютеров.

4.6.2.1. Создание и отправка задач

Одна из ключевых функций страницы **Компьютеры**, помимо оперативного контроля текущего состояния клиентского СВТ – это возможность назначения широкого спектра задач для настройки и управления клиентскими СВТ. Для создания новой задачи предназначена кнопка **Создать задачу**, которая приведет к открытию модального диалога (рис. 115).

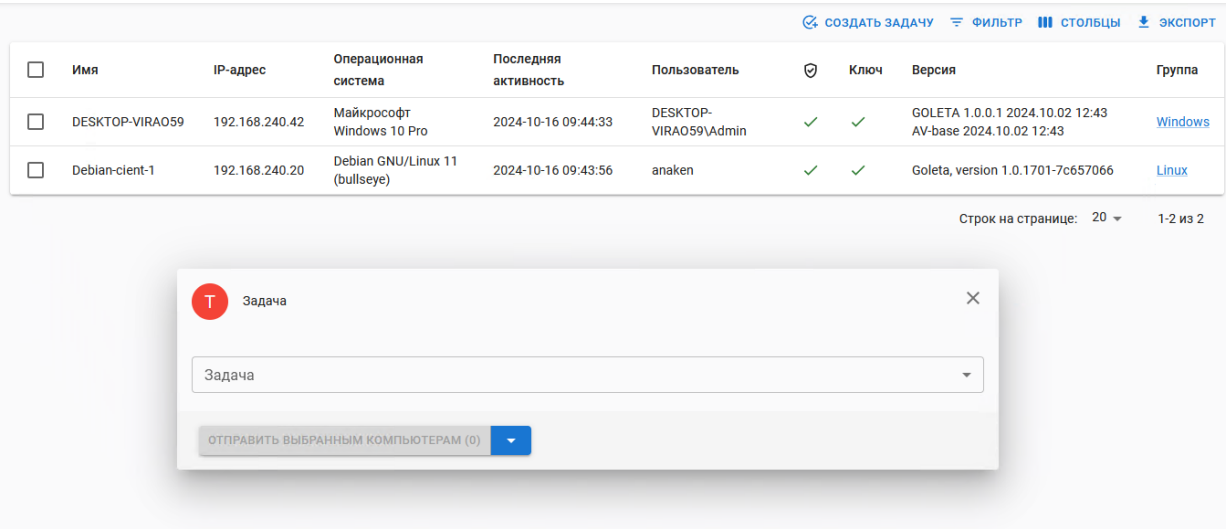


Рис. 115 – ЦУ. Раздел Компьютеры.
Создать задачу

Задачу можно выдать всем компьютерам сразу, только одному компьютеру или нескольким компьютерам по выбору. Для этого предназначены флажки в левой части таблицы **Компьютеры**. Выбрать компьютеры для исполнения задачи можно в любой момент работы с задачей: как до открытия диалогового окна **Задача**, так и с открытым диалоговым окном задачи. Еще один способ выдачи выбранной задачи (определенным компьютерам или всем сразу) доступен при помощи выпадающего списка внизу окна **Задача** (рис. 116).

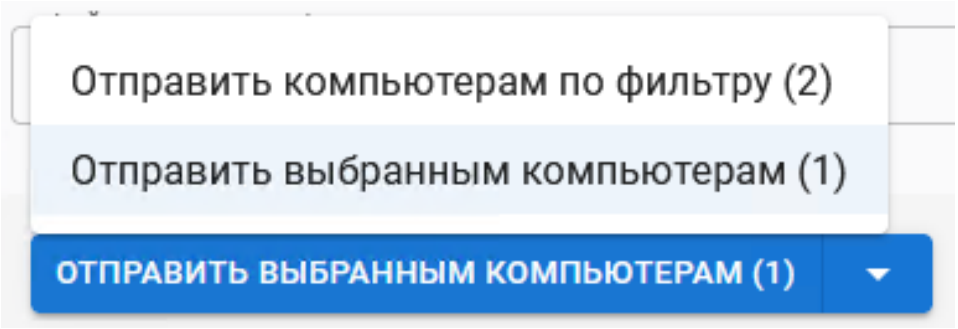


Рис. 116 – ЦУ. Раздел Компьютеры.

Способ выдачи задачи

4.6.2.2. Перечень существующих задач

Пользователю ЦУ доступны следующие задачи для отправки клиентским СВТ:

1) Создать процесс;
2) Отправить файл;
3) Запустить сканер;
4) Запросить файлы отчета;
5) Получить информацию о системе;
6) Получить список принтеров;
7) Получить список программ;
8) Получить список процессов;
9) Получить состояния компонентов;
10) Получить список файлов в карантине;
11) Настроить диспетчер;
12) Настроить агент;
13) Настроить монитор;
14) Настроить сканер;
15) Настроить карантин;
16) Настроить межсетевой экран;
17) Настроить планировщик;
18) Настроить проверку целостности;
19) Настроить модуль удаления;
20) Запустить очистку;

21) Выдать политики;
22) Проверить целостность;
23) Включить / выключить монитор;
24) Обновить все;
25) Обновить ключ;
26) Отсоединить агент.

4.6.2.3. Задача «Создать процесс»

Отправка данной задачи приведет к запуску указанного в командной строке исполняемого файла. Для консольных приложений есть возможность указывать доступные ключи запуска.

В строке ввода **Командная строка** (рис. 117) необходимо указать приложение, установленное на клиентском СВТ, которое требуется запустить.

Примечание. Необходимо учитывать различия в системных соглашениях конкретных версий ОС Windows и ОС Linux для успешного запуска приложений.

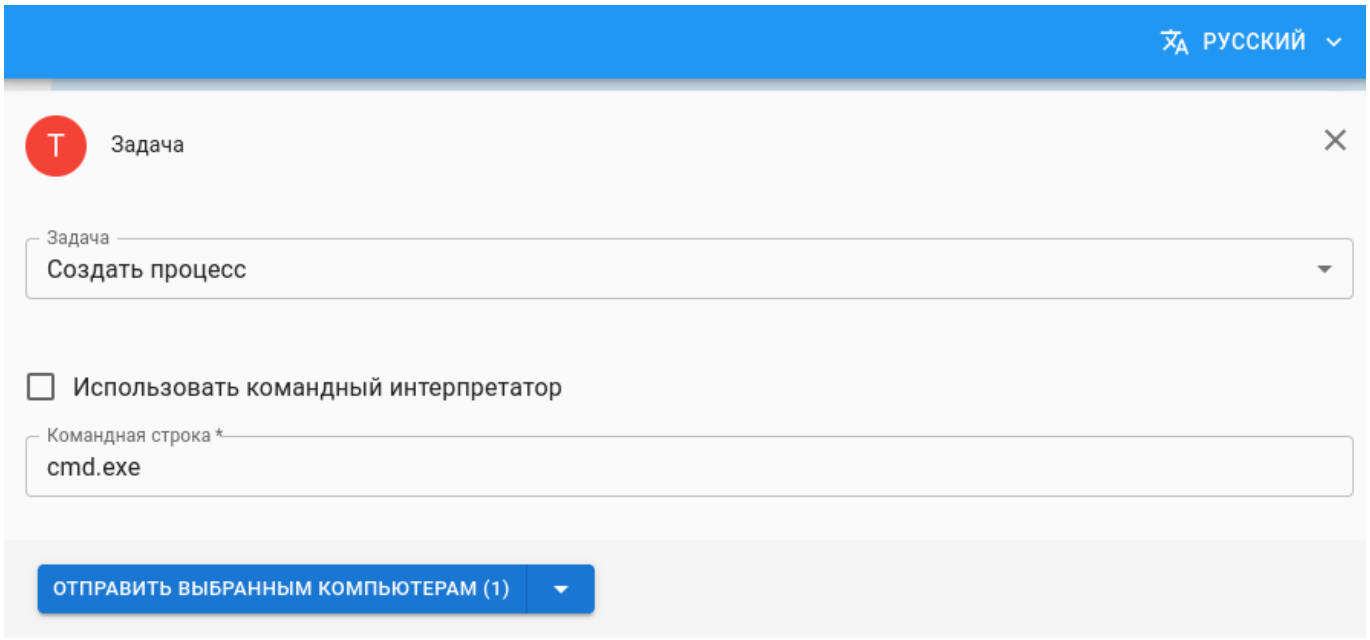


Рис. 117 – ЦУ. Раздел Компьютеры.
Задача «Создать процесс»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.4. Задача «Отправить файл»

Данная задача позволяет отправлять выбранные файлы на компьютеры с установленной клиентской частью программного комплекса ШХУНА.

Для выполнения этой процедуры необходимо перетащить выбранные файлы прямо в окно браузера либо воспользоваться системным файловым менеджером, нажав на область диалогового окна **Перетащите файлы сюда или нажмите для выбора**. Также необходимо указать полный путь и имя файла который будет создан на клиентском СВТ, учитывая специфику формирования полного пути в ОС Windows (рис. 118) и Linux (рис. 119).

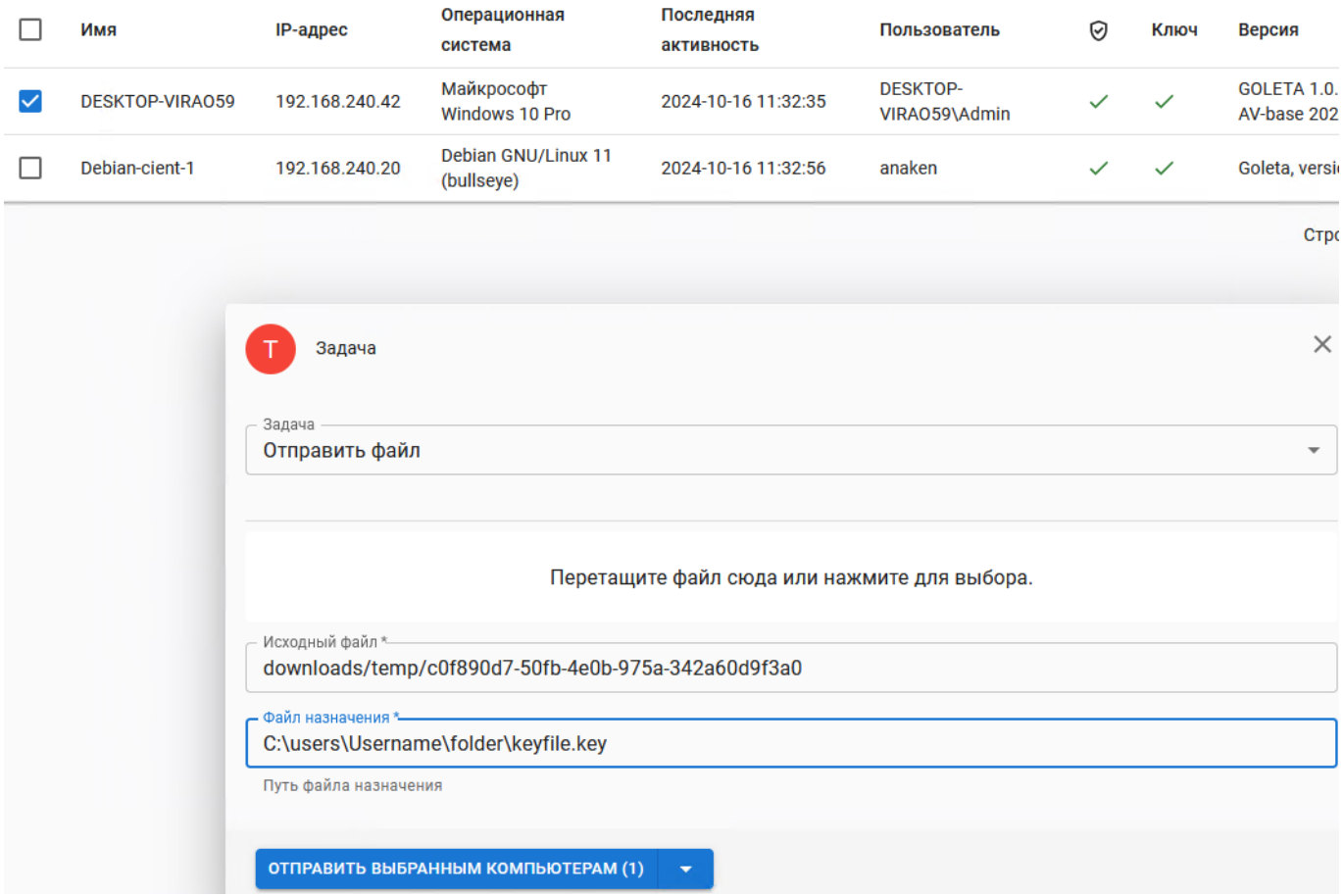


Рис. 118 – ЦУ. Раздел Компьютеры.
Задача «Отправить файл». ОС Windows

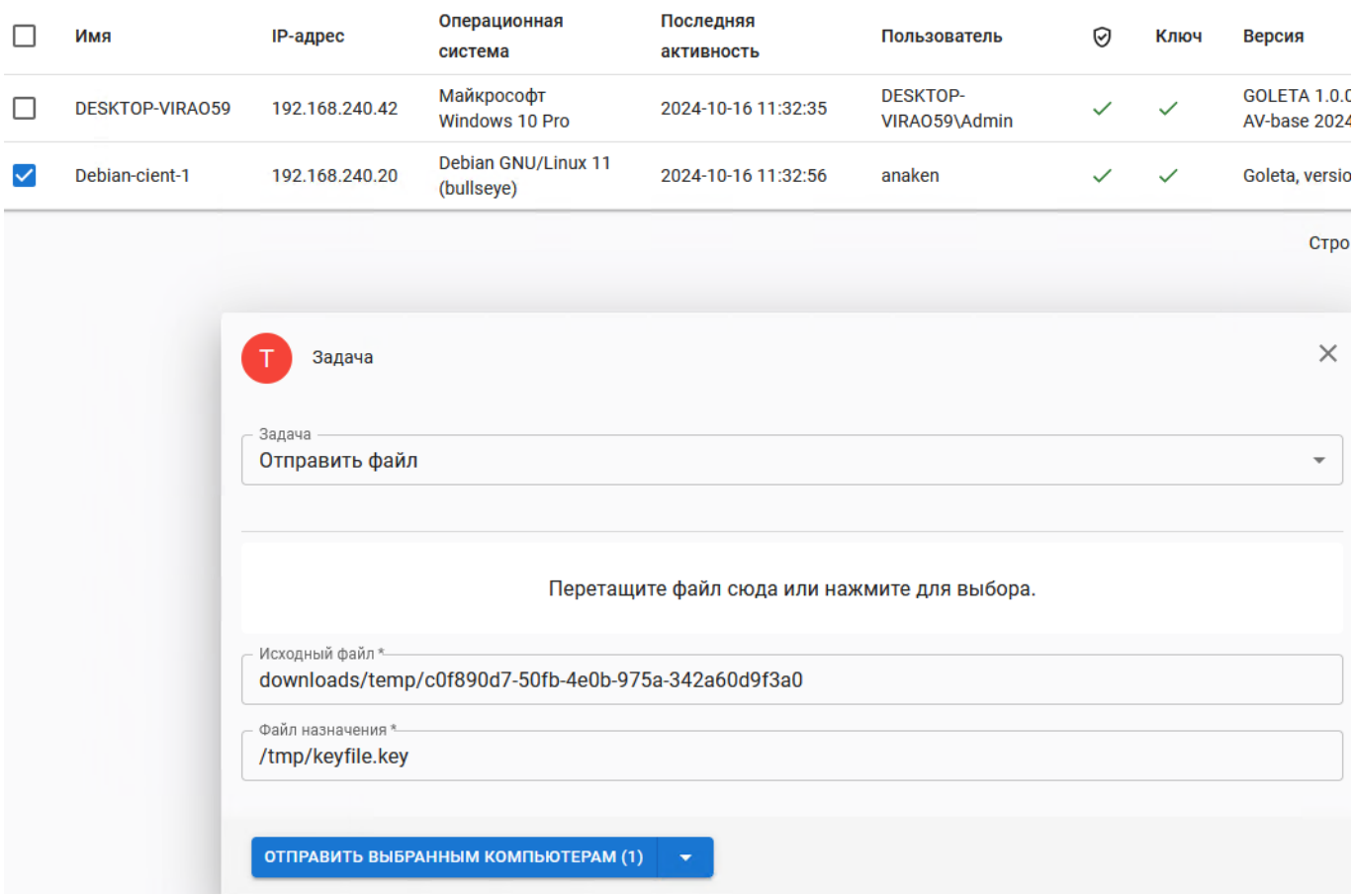


Рис. 119 – ЦУ. Раздел Компьютеры.
Задача «Отправить файл». ОС Linux

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.5. Задача «Запустить сканер»

Задача «Запустить сканер» предназначена для запуска компонента антивирусного сканера модуля контроля данных программного комплекса ШХУНА на клиентском СВТ (рис. 120).

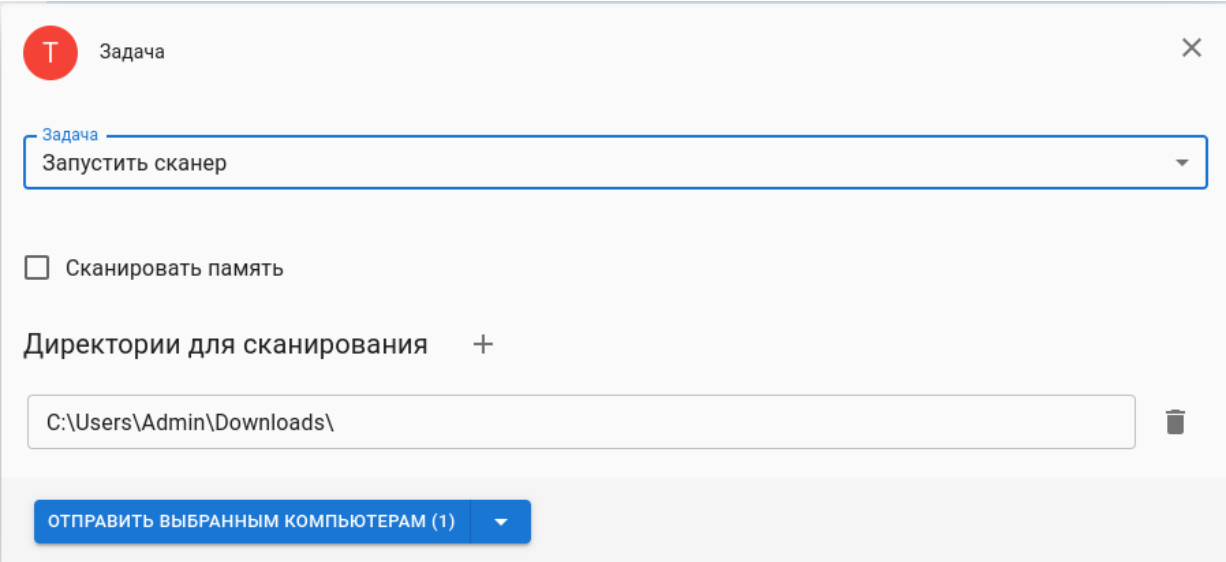


Рис. 120 – ЦУ. Раздел Компьютеры.
Задача «Запустить сканер»

Доступны следующие параметры:

1) Сканировать память – проверка данных, содержащихся в ОЗУ клиентского СВТ;
2) Директории для сканирования – можно указать одну или несколько директорий (используя кнопку +).

4.6.2.6. Задача «Запросить файлы отчета»

Клиентская часть программного комплекса ШХУНА генерирует собственные файлы отчета. Задача «Запросить файлы отчета» (рис. 121) предназначена для получения ЦУ этих отчетов (см. п. 4.6.11) и для последующего их анализа. Данная задача не имеет дополнительных настроек.

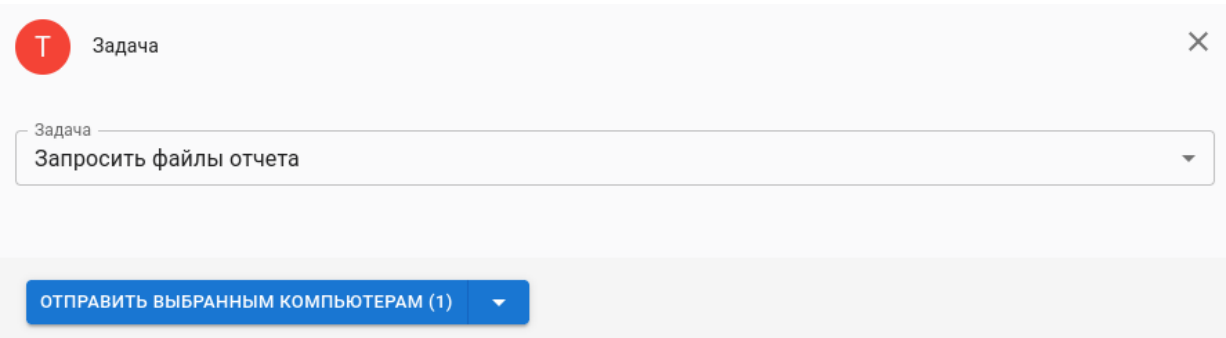


Рис. 121 – ЦУ. Раздел Компьютеры.
Задача «Запросить файлы отчета»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.7. Задача «Получить информацию о системе»

Данная задача (рис. 122) позволяет запросить информацию о выбранной системе, не дожидаясь установленного интервала времени для периодической отсылки. Задача не содержит дополнительных настроек. Результаты работы данной задачи отображаются в детальном описании компьютера.

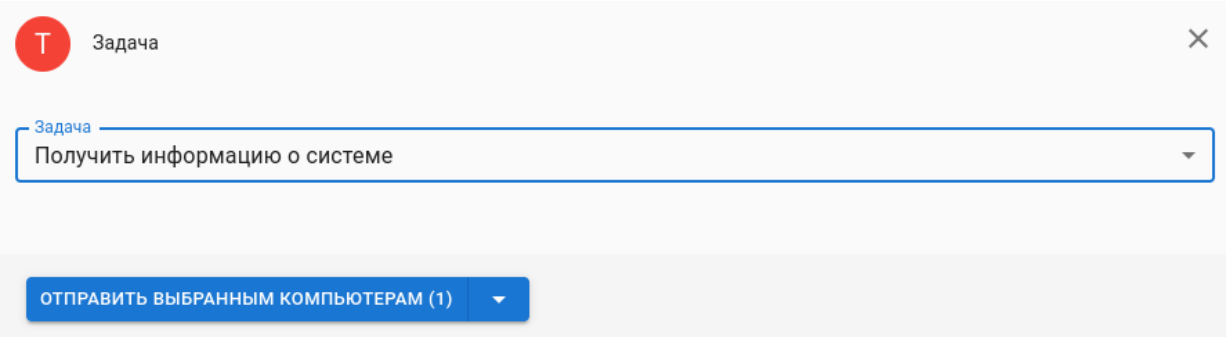


Рис. 122 – ЦУ. Раздел Компьютеры.
Задача «Получить информацию о системе»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.8. Задача «Получить список принтеров»

Данная задача (рис. 123) предназначена для запроса списка установленных на клиентских СВТ принтеров. Данная задача не имеет дополнительных параметров.

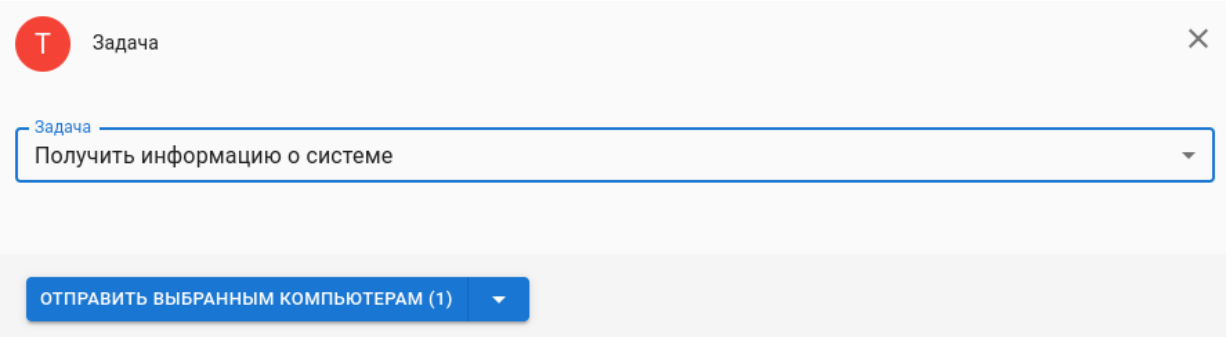


Рис. 123 – ЦУ. Раздел Компьютеры. Задача «Получить список принтеров»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру**.

4.6.2.9. Задача «Получить список программ»

Данная задача предназначена для получения списка программ установленных на клиентском СВТ, подсоединенном к ЦУ. Результаты выполнения данной задачи отобразятся на странице Шаблоны, в разделе приложения. Данная задача не имеет дополнительных параметров.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна (рис. 124).

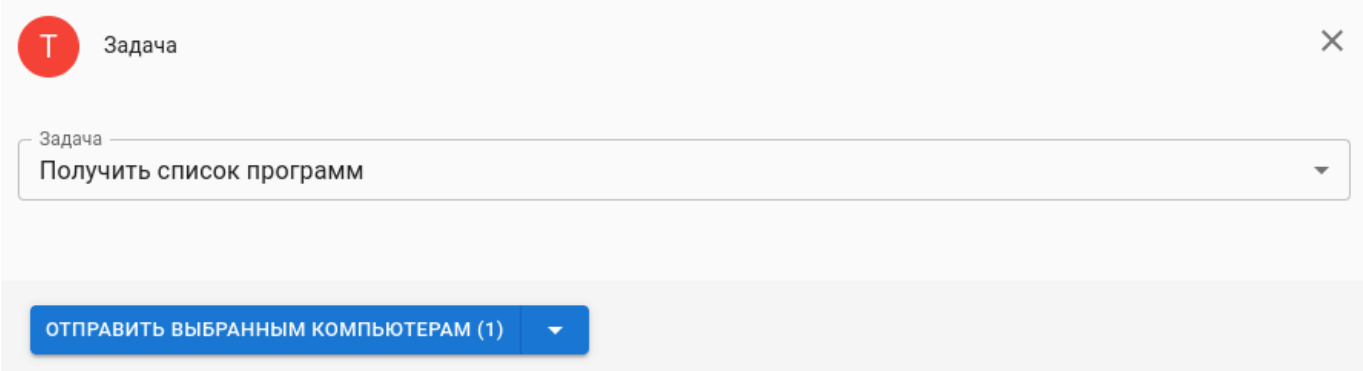


Рис. 124 – ЦУ. Раздел Компьютеры. Задача «Получить список программ»

4.6.2.10. Задача «Получить список процессов»

Данная задача предназначена для запроса на получение списка процессов, запущенных на клиентских СВТ, подключенных к ЦУ. Результаты выполнения данной задачи будут отображены на странице Процессы. Данная задача не имеет дополнительных параметров.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна (рис. 125).

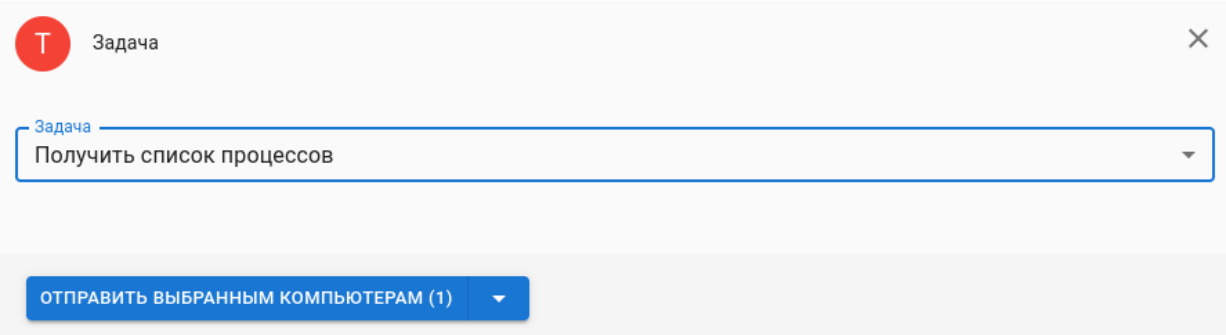


Рис. 125 – Задача «Получить список процессов»

4.6.2.11. Задача «Получить состояния компонентов»

Данная задача предназначена для получения состояния компонентов программного комплекса ШХУНА и формирования запроса текущего состояния компонентов на клиентском СВТ, подключенного к ЦУ. Результаты выполнения данной задачи будут отображены на странице Компоненты.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна (рис. 126).

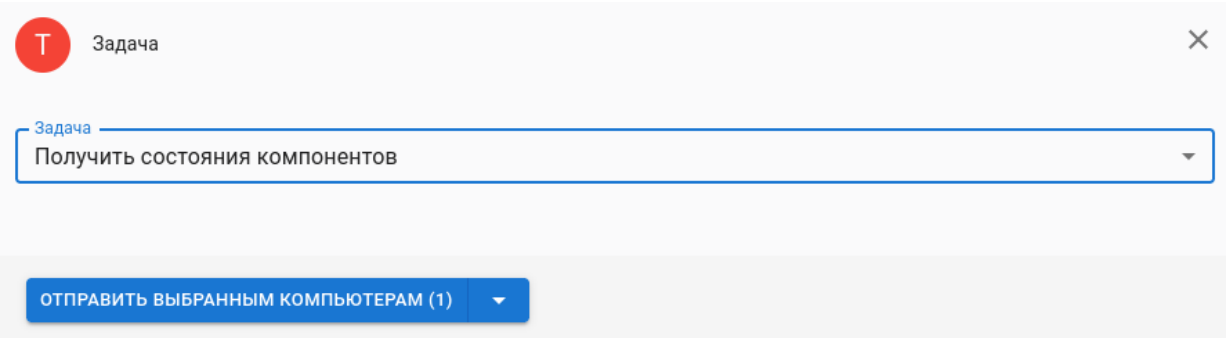


Рис. 126 – Задача «Получить состояния компонентов»

4.6.2.12. Задача «Получить список файлов в карантине»

Данная задача предназначена для получения списка файлов в карантине и формирования запроса к модулю контроля данных, компоненту Карантин клиентской части программного комплекса ШХУНА на получение хранящихся файлов. Файлы, запрошенные при помощи этой задачи, появятся на странице **Карантин**. Данная задача не имеет дополнительных параметров.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна (рис. 127).

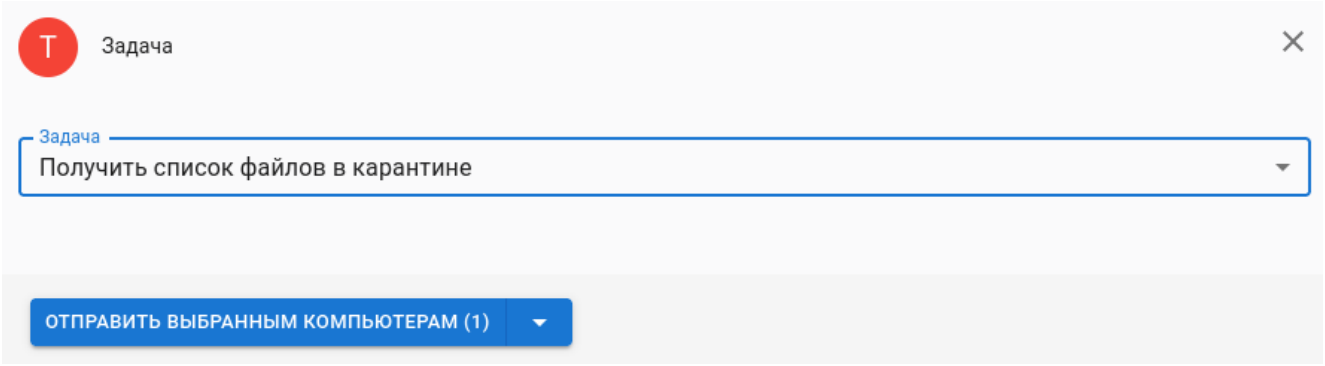


Рис. 127 – Задача «Получить список файлов в карантине»»

4.6.2.13. Задача «Настроить диспетчер»

Данная задача предназначена для выполнения настройки компонента Диспетчер на клиентском СВТ, подключенном к ЦУ. Настройки разделены на несколько логических частей, которые соответствуют вкладкам **Обновление** (рис. 128), **Прокси-сервер** (рис. 129) и **Пользователи** (рис. 130).

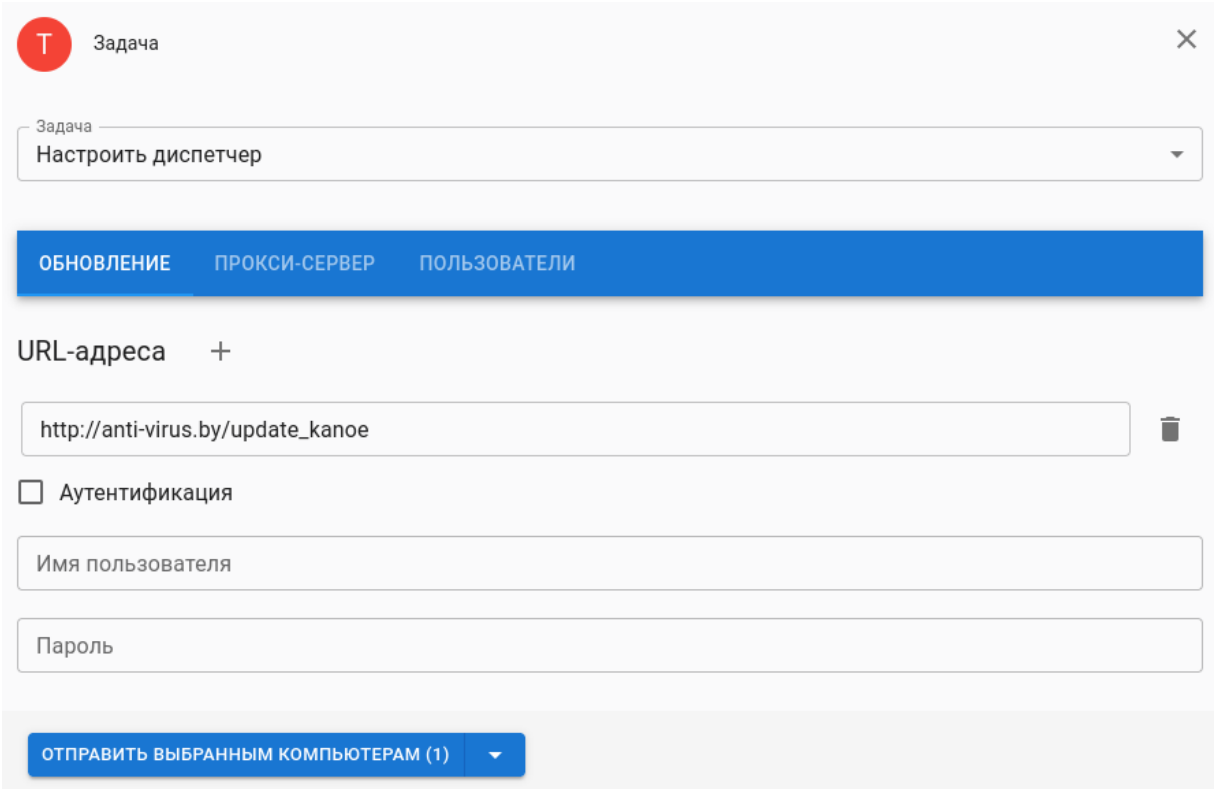


Рис. 128 – Задача «Настроить диспетчер». Обновление

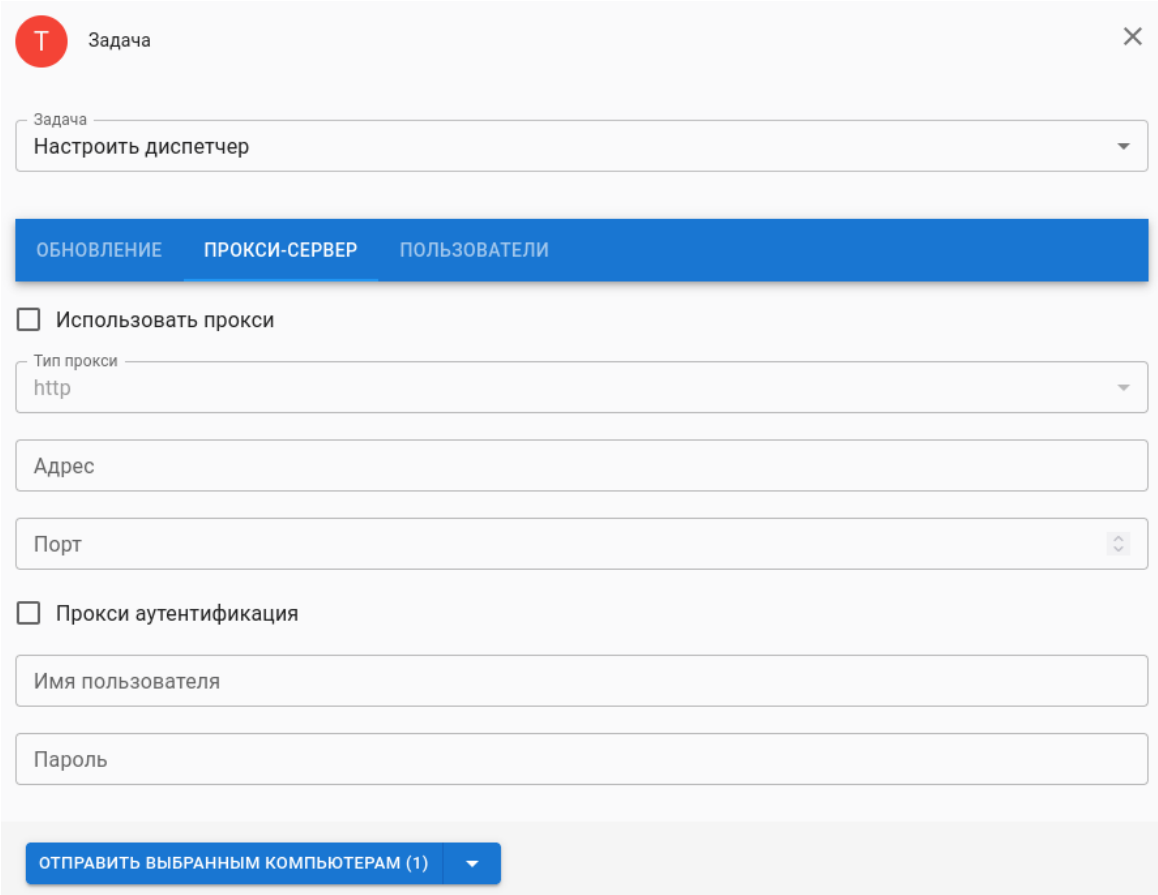


Рис. 129 – Задача «Настроить диспетчер». Прокси-сервер

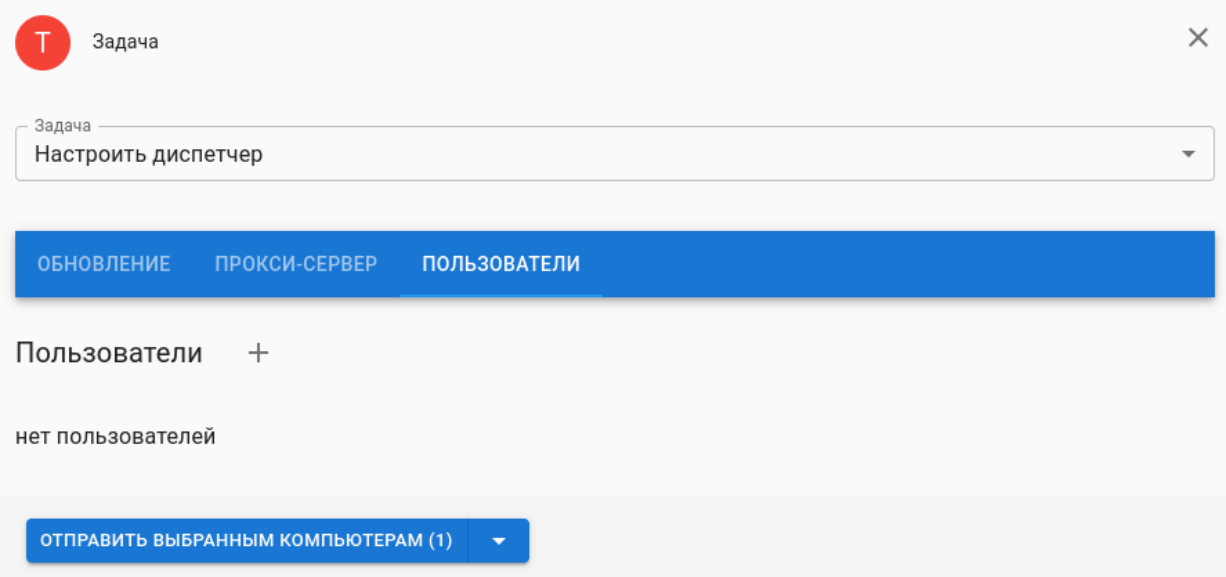


Рис. 130 – Задача «Настроить диспетчер». Пользователи

Вкладка **Пользователи** позволяет настроить защиту клиентской части программного комплекса ШХУНА от несанкционированного доступа. После выдачи задачи по настройке Диспетчера в графический интерфейс клиентской части

программного комплекса ШХУНА сможет войти только указанный в этих настройках пользователь

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.14. Задача «Настроить агент»

Данная задача предназначена для выполнения настройки модуля «Агент удаленного администрирования».

Настройка **Интервал отправки состояния (минуты)** – позволяет настроить интервал отправки событий агентом в минутах. Настройка **Интервал проверки ключа (дни)** – позволяет настроить период проверки даты окончания ключа.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна (рис. 131).

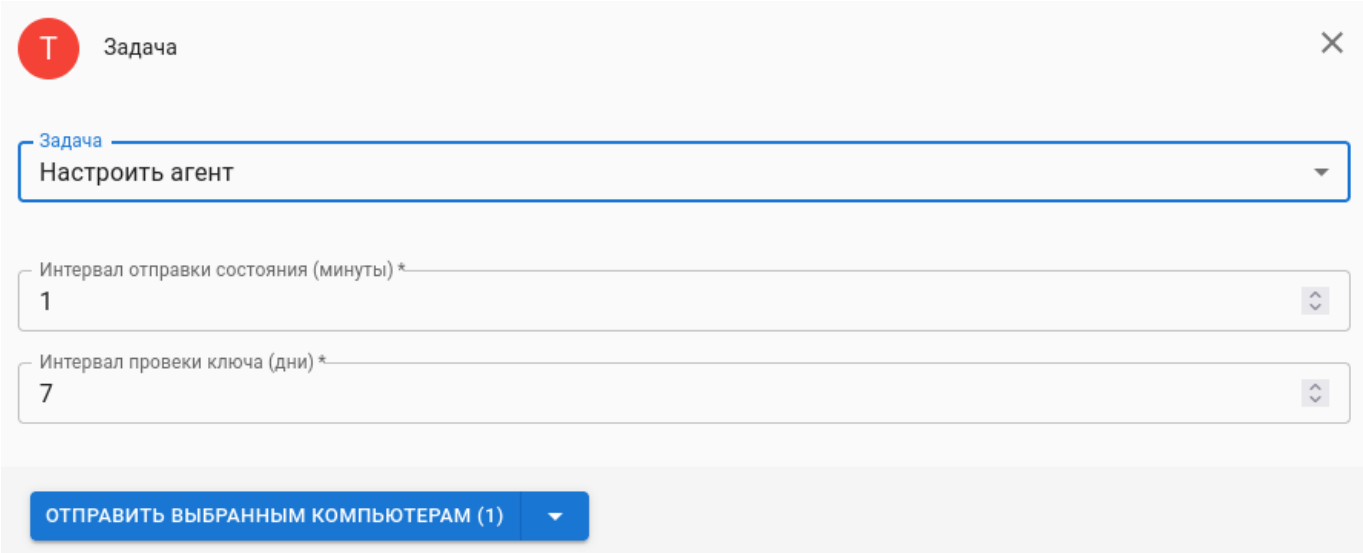


Рис. 131 – Задача «Настроить агент»

4.6.2.15. Задача «Настроить монитор»

Данная задача предназначена для выполнения настройки компонента Монитор модуля контроля данных программного комплекса ШХУНА (рис. 132 и рис. 133).

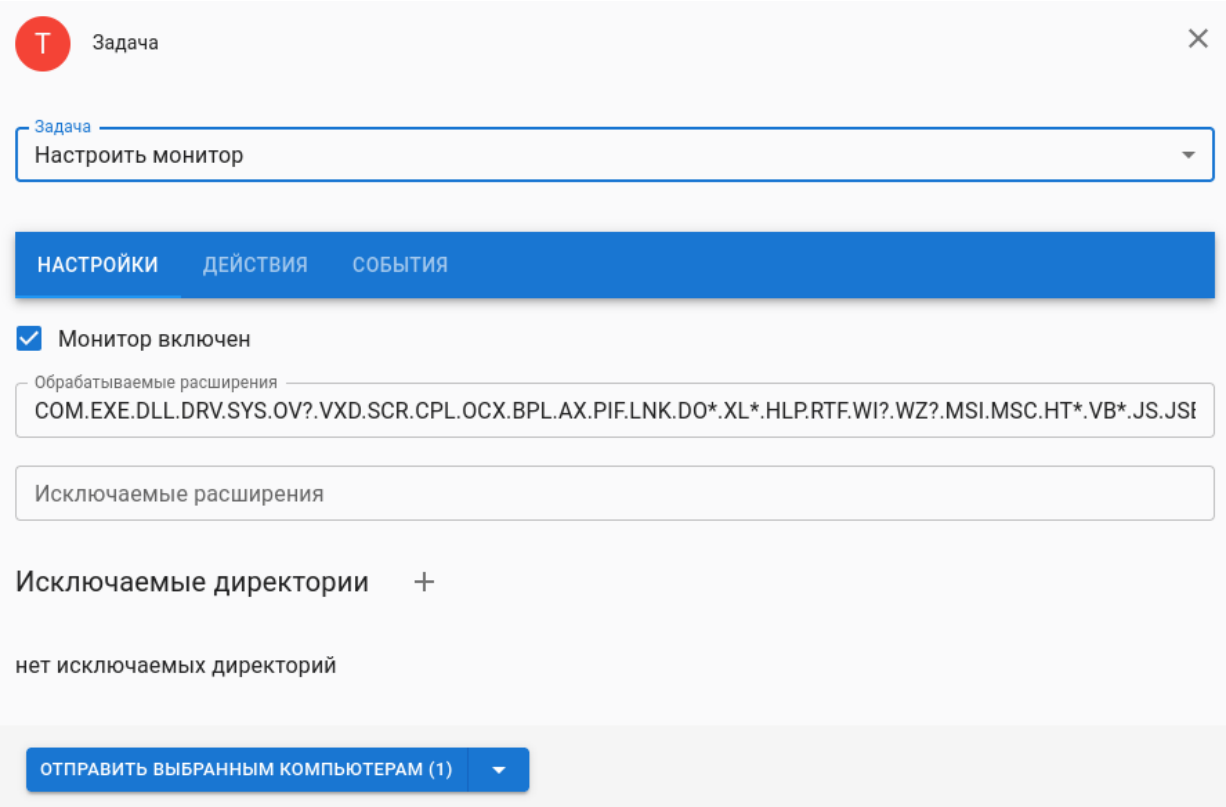


Рис. 132 – Задача «Настроить монитор». Настройки

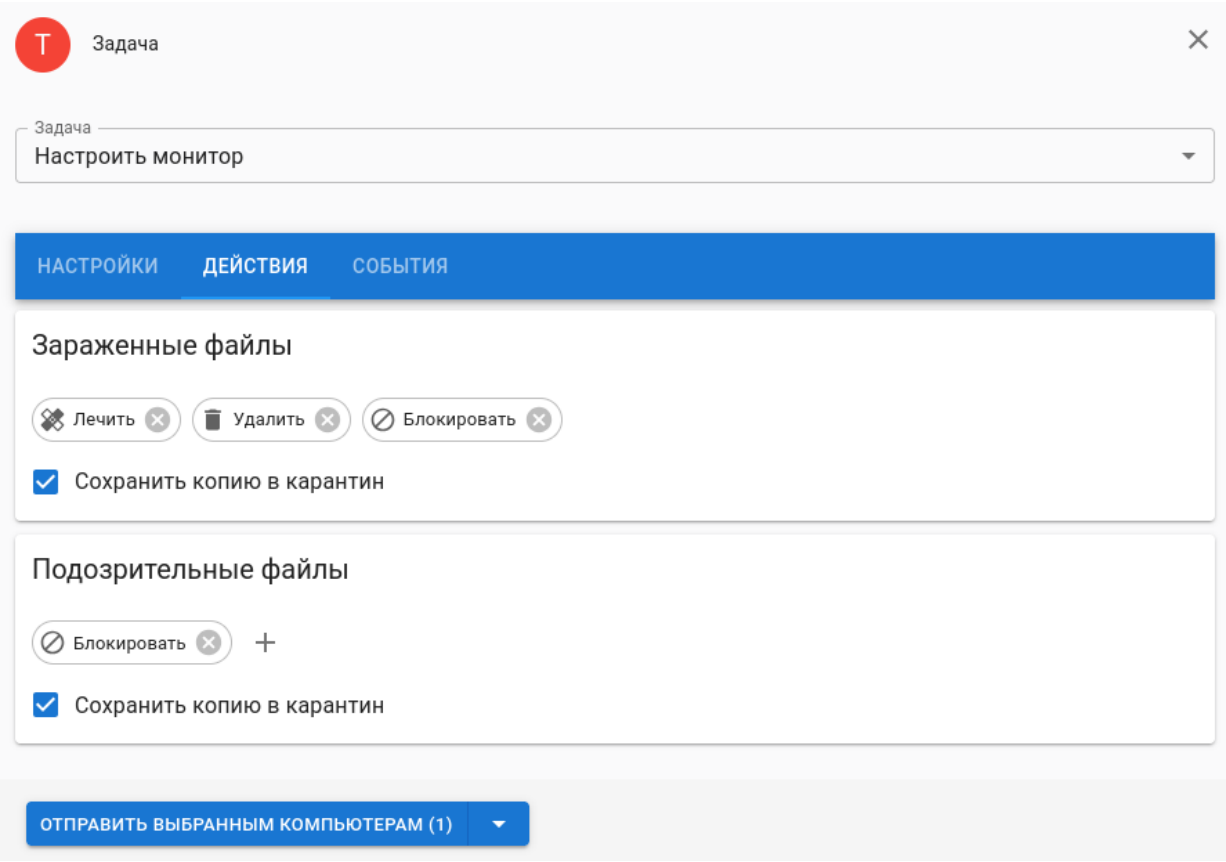


Рис. 133 – Задача «Настроить монитор». Действия

Вкладка **События** (рис. 134) позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно.

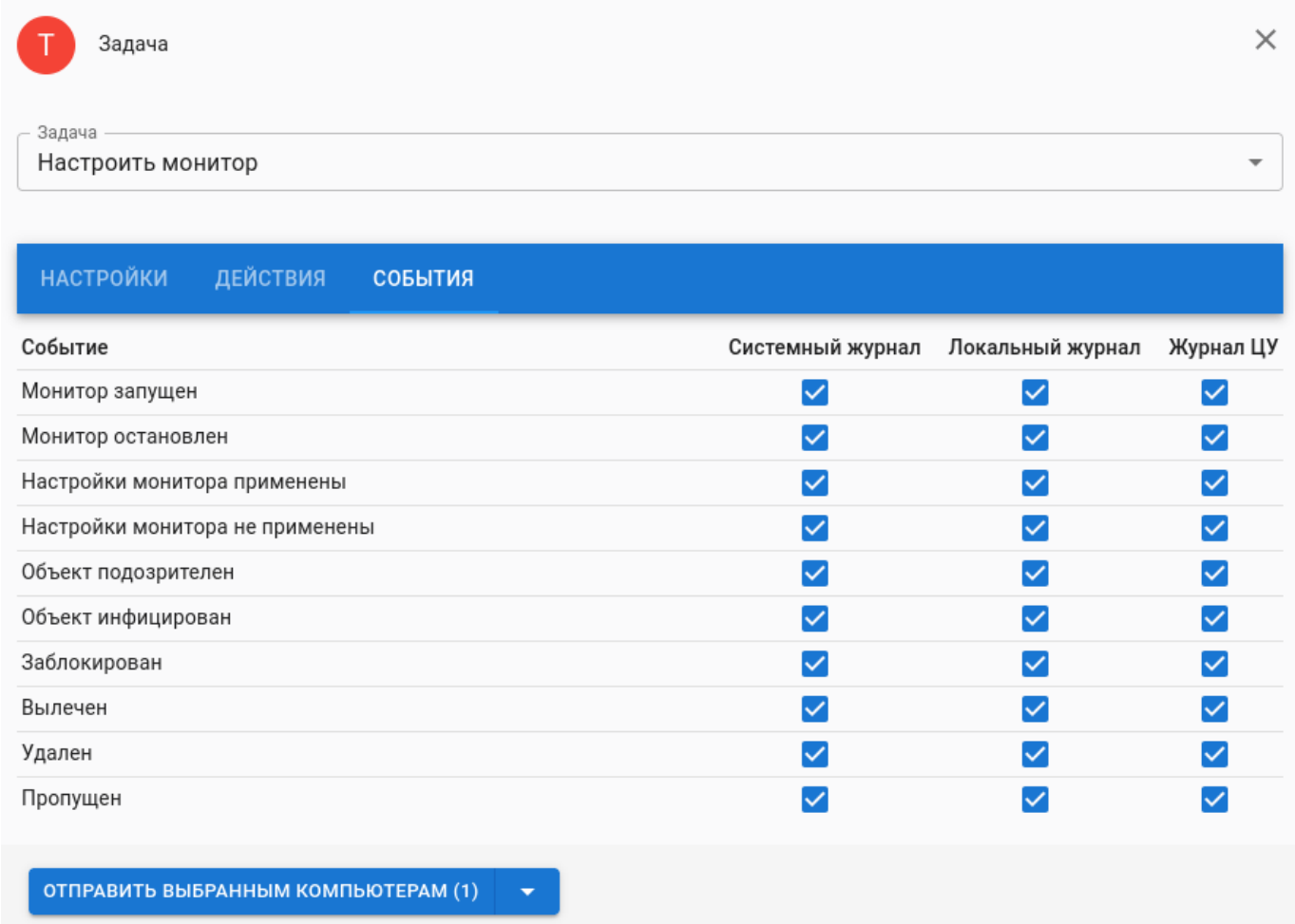


Рис. 134 – Задача «Настроить монитор». События

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.16. Задача «Настроить сканер»

Данная задача предназначена для выполнения настройки компонента Сканер модуля контроля данных программного комплекса ШХУНА (рис. 135 и рис. 136).

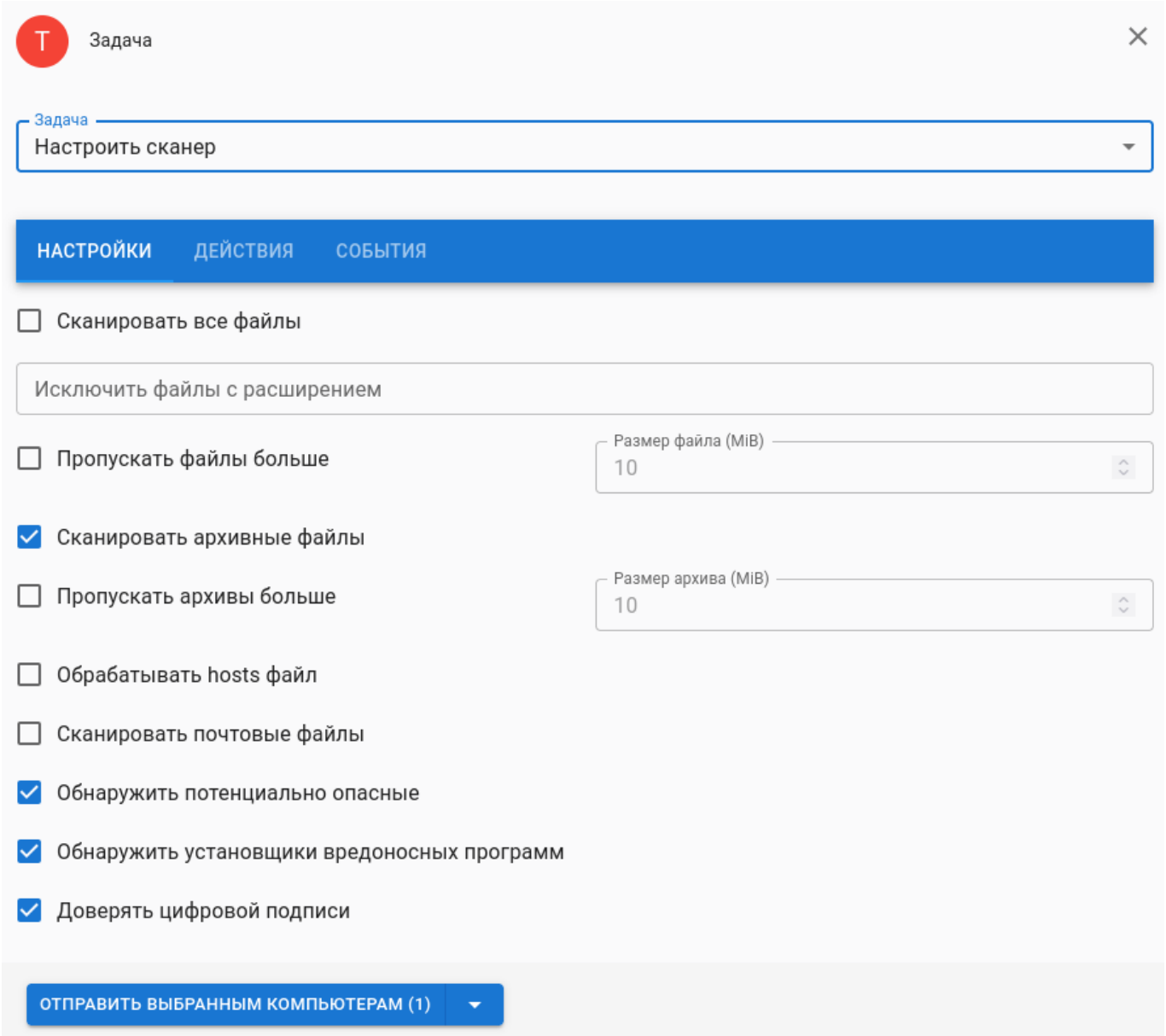


Рис. 135 – Задача «Настроить сканер». Настройки

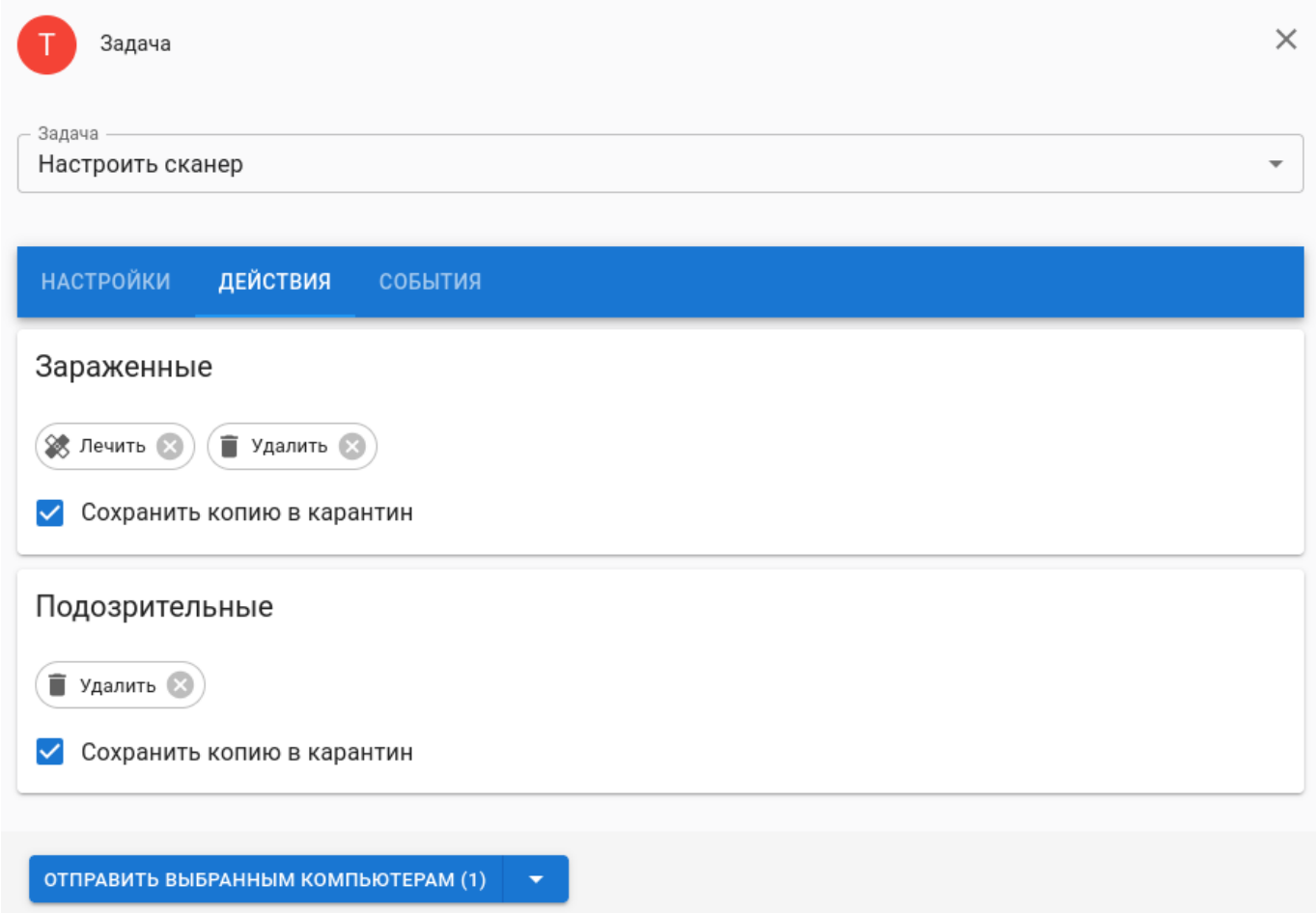


Рис. 136 – Задача «Настроить сканер». Действия

Вкладка **События** (рис. 137) позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно.

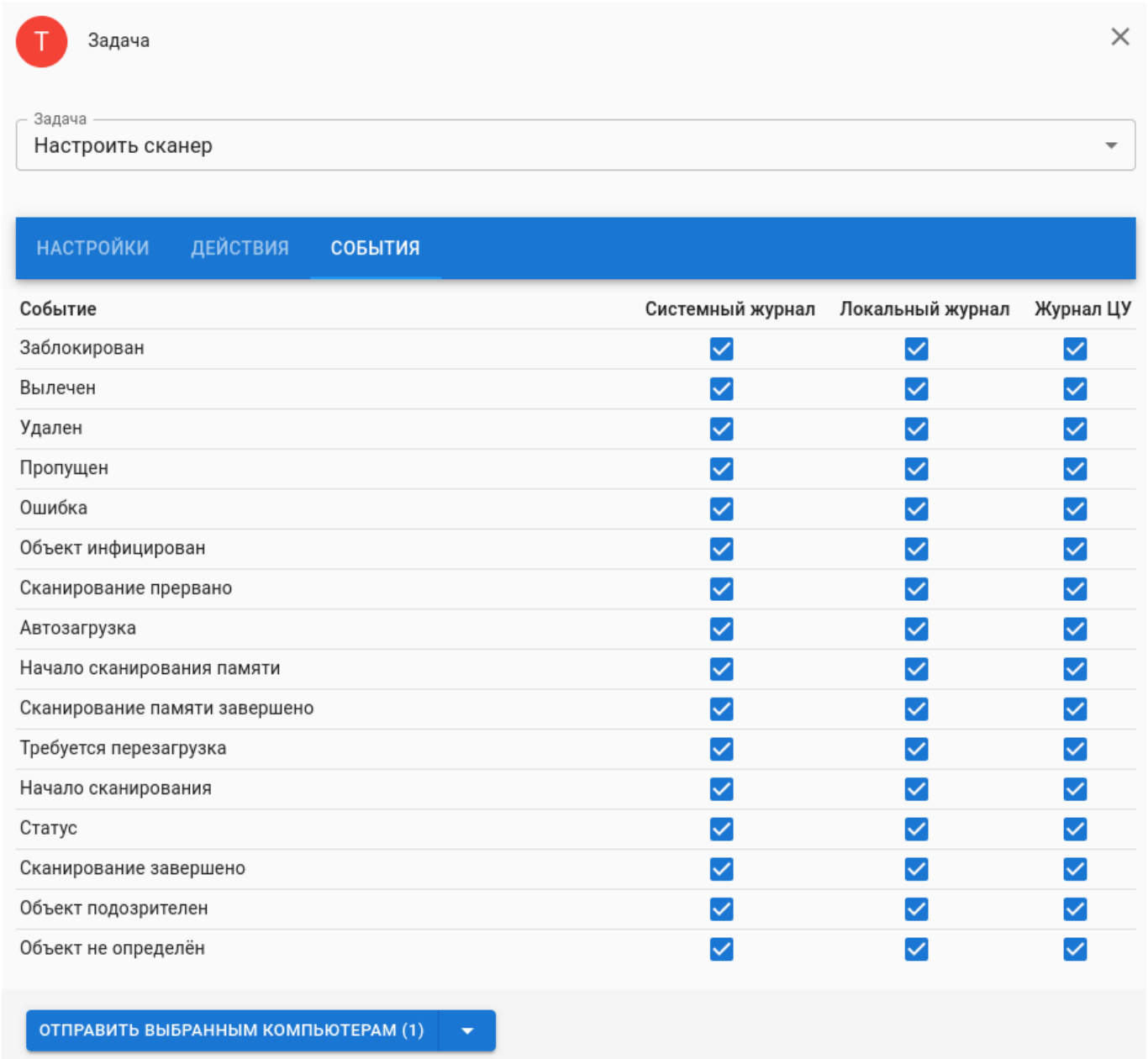


Рис. 137 – Задача «Настроить сканер». События

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.17. Задача «Настроить карантин»

Данная задача предназначена для выполнения настройки компонента Карантин модуля контроля данных программного комплекса ШХУНА (рис. 138).

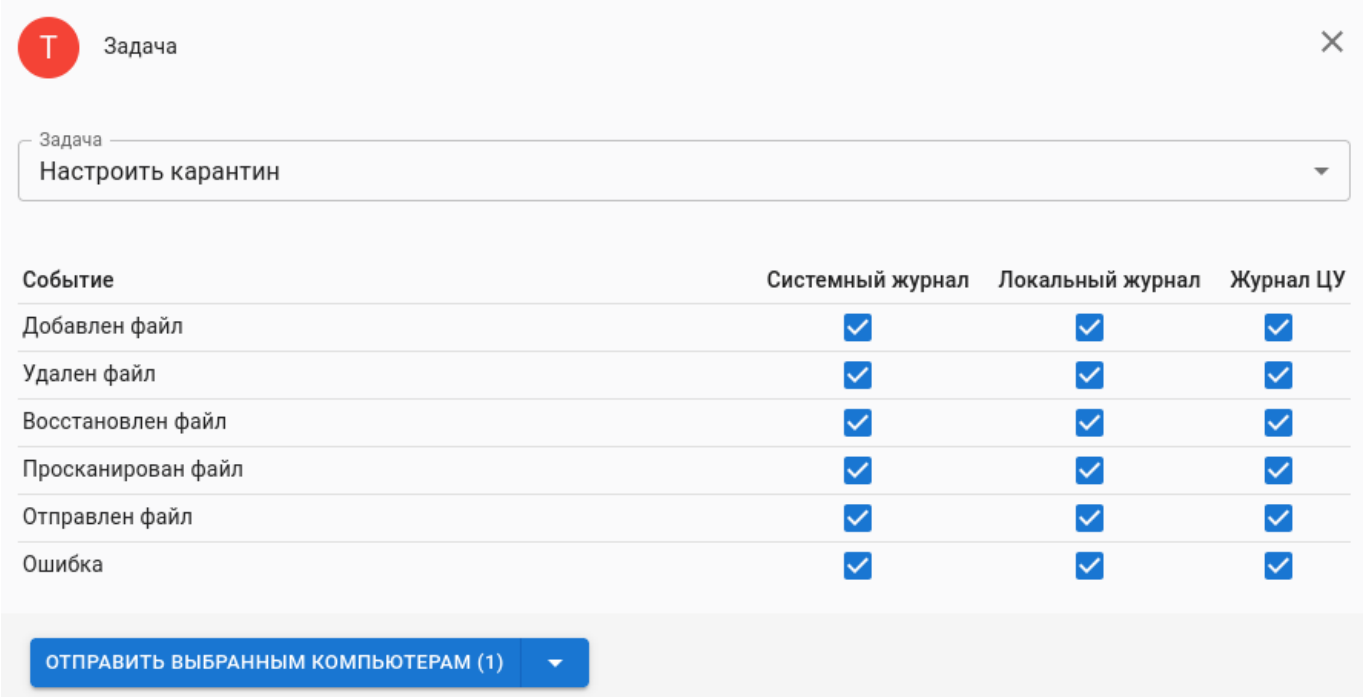


Рис. 138 – Задача «Настроить карантин»

Окно настроек позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.18. Задача «Настроить межсетевой экран»

Данная задача предназначена для выполнения настройки модуля межсетевого экранирования программного комплекса ШХУНА.

Выбор параметров осуществляется на основе практик responsive UI (адаптивного интерфейса), т.е. путем использования элементов управления, непосредственно появляющихся в результате взаимодействия пользователя с формой.

Выпадающий список **Политика** (рис. 139) содержит пункты с предустановленными настройками разрешенных портов:

1) **Открытая** – разрешено все;
2) **Закрытая** – запрещено все, кроме получения сетевого адреса и портов ЦУ;
3) **Доменная** – данные наборы правил разрешают получение сетевого адреса, взаимодействие модуля «Агент удаленного администрирования» с ЦУ, обнаружение ПЭВМ в сети и предоставление общего доступа к файлам; 135 порт (DCOM) для UDP, 389 порт (LDAP) для TCP и UDP, 636 порт (LDAPS) для TCP, 88 порт (Kerberos) для TCP, 123 порт (NTP) для UDP;
4) **Частная** – данные наборы правил разрешают получение сетевого адреса, взаимодействие модуля «Агент удаленного администрирования» с ЦУ, обнаружение ПЭВМ в сети и предоставление общего доступа к файлам.

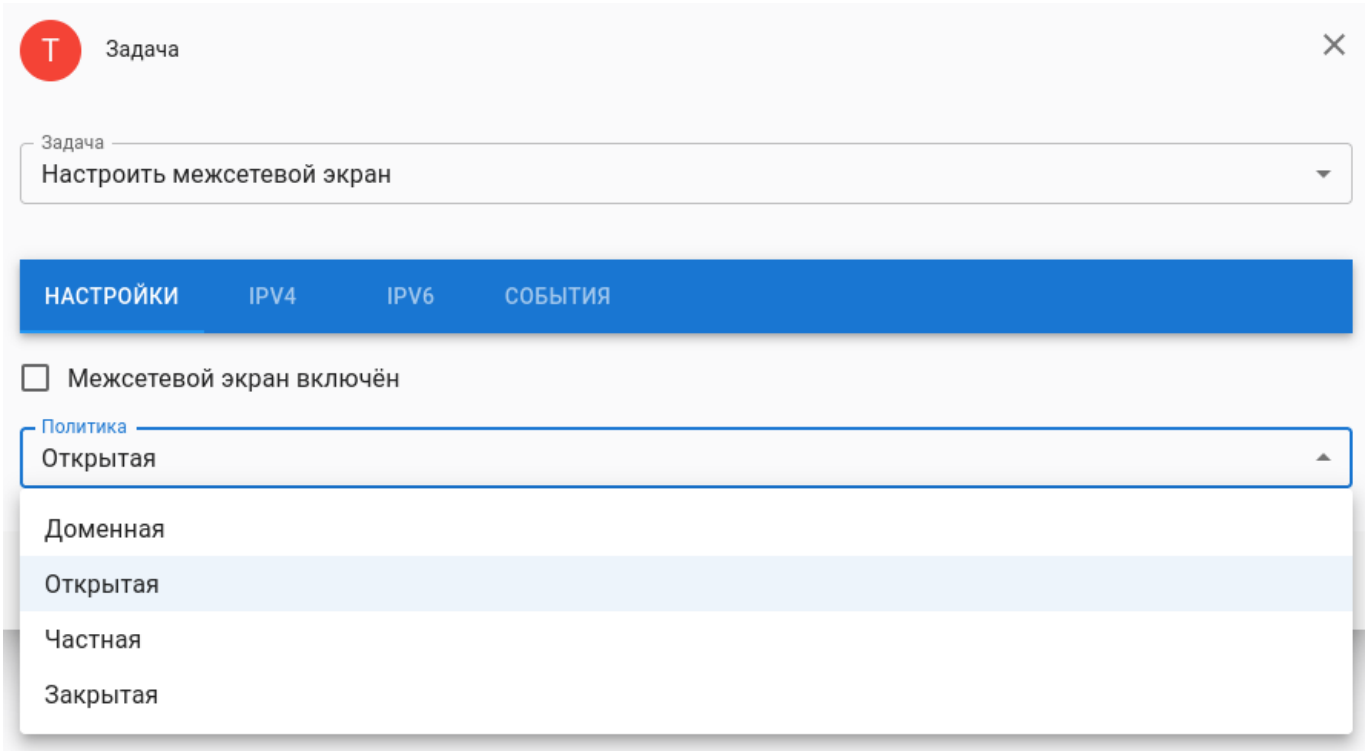


Рис. 139 – Задача «Настроить межсетевой экран». Настройки

Настройки, относящиеся к **IPv4** (рис. 140) и **IPv6** (рис. 141) изменяются схожим образом.

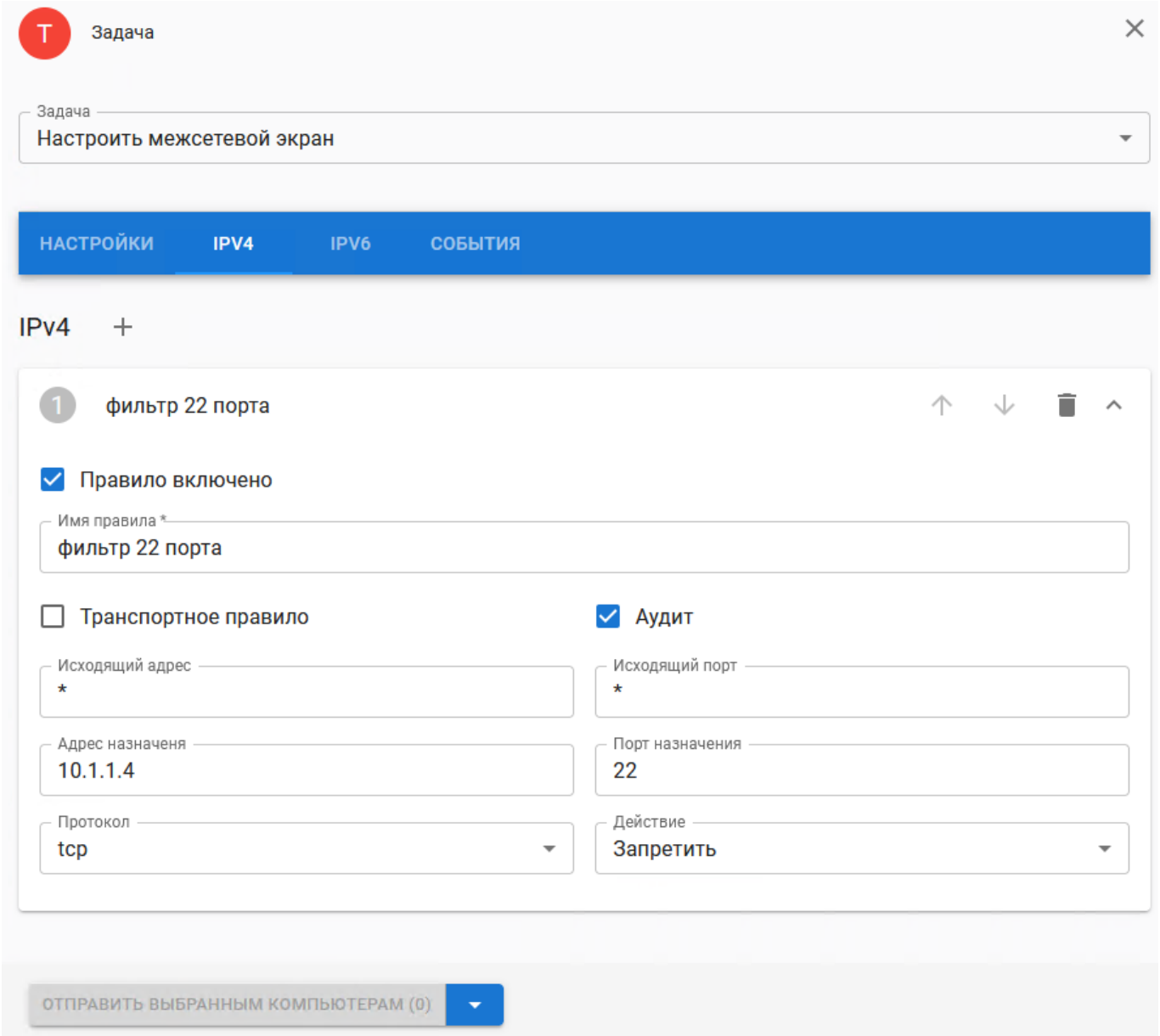


Рис. 140 – Задача «Настроить межсетевой экран». IPv4

Создать новую запись в таблице правил можно нажав на иконку + в верхней части формы. Будет создано пустое правило. После нажатия ЛКМ по этому правилу раскроется диалоговое окно настроек данного правила.

Параметры, доступные для редактирования:

1) **Правило включено** – позволяет активировать или деактивировать правило;
2) **Имя правила (обязательно)** – используется для задания уникального имени правила. Поле помечено красным, если имя не указано, поскольку оно является обязательным для сохранения правила;

3) **Транспортное правило** – позволит создать правило транспортного уровня;
4) **Аудит** – активирует ведение журнала событий, связанных с данным правилом;
5) **Исходящий адрес** – поле для указания исходящего IP-адреса;
6) **Исходящий порт** – поле для задания исходящего порта;
7) **Адрес назначения** – поле для указания целевого IP-адреса;
8) **Протокол** – позволяет выбрать используемый протокол (TCP, UDP);
9) **Порт назначения** – поле для задания порта назначения.

Выпадающий список **Действие** позволяет выбрать одно из действий:

1) **Разрешить отправку**;
2) **Разрешить получение**;
3) **Разрешить отправку и получение**;
4) **Запретить**.

Транспортное правило позволяет указать действие для любого из существующих транспортных протоколов. Транспортное правило требует указания исходящего адреса, адреса назначения протокола и действия над сетевым пакетом.

Номер протокола – это общепринятая международной некоммерческой организацией IANA (Internet Assigned Numbers Authority) величина в виде натурального числа, список возможных значений которых находится по адресу `https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml`.

Созданные правила работают сверху вниз. Для изменения очередности правил предназначены иконки  и в правой части правила. Также там присутствует иконка удаления правила  .

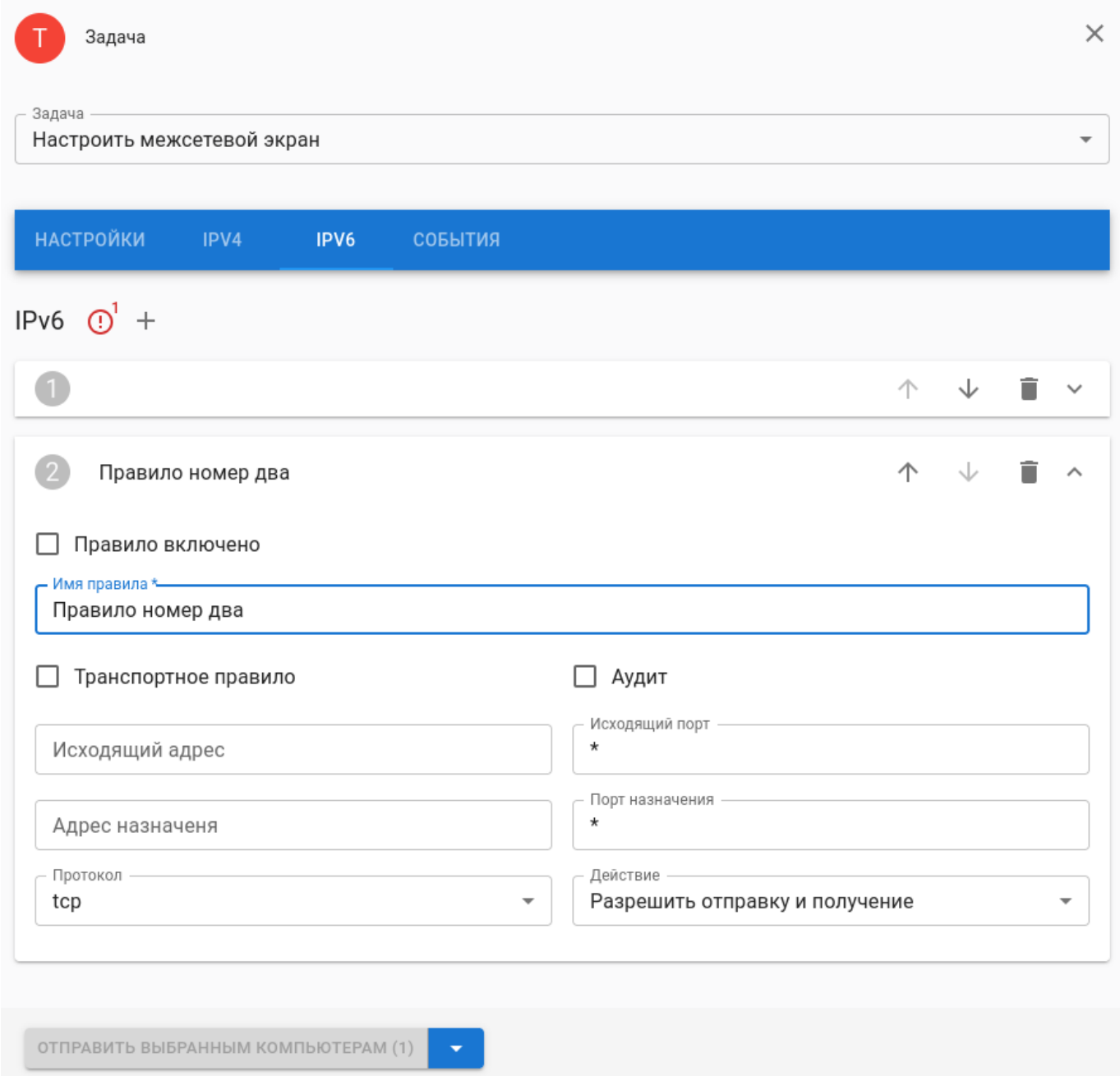


Рис. 141 – Задача «Настроить межсетевой экран». IPv6

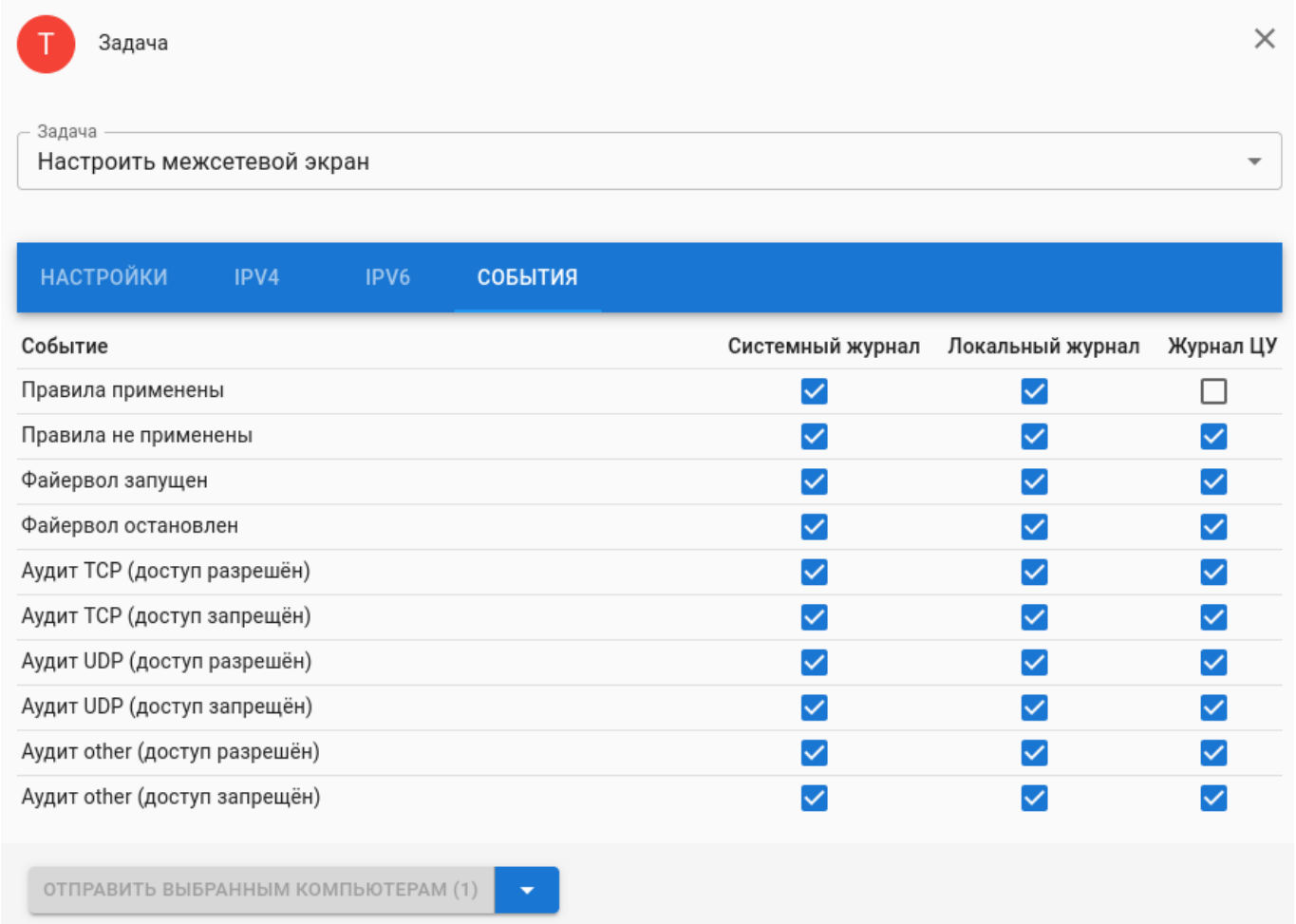


Рис. 142 – Задача «Настроить межсетевой экран». События

Вкладка **События** (рис. 142) позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.19. Задача «Настроить планировщик»

Данная задача предназначена для выполнения настройки компонента Планировщик модуля взаимодействия программного комплекса ШХУНА и выполнения клиентскими СВТ определенных операций в автоматическом режиме.

Создать новую форму для задачи можно при помощи иконки +. При нажатии

ЛКМ по заголовку формы откроется более детальный вид, где возможно настроить параметры выбранной задачи (рис. 143).

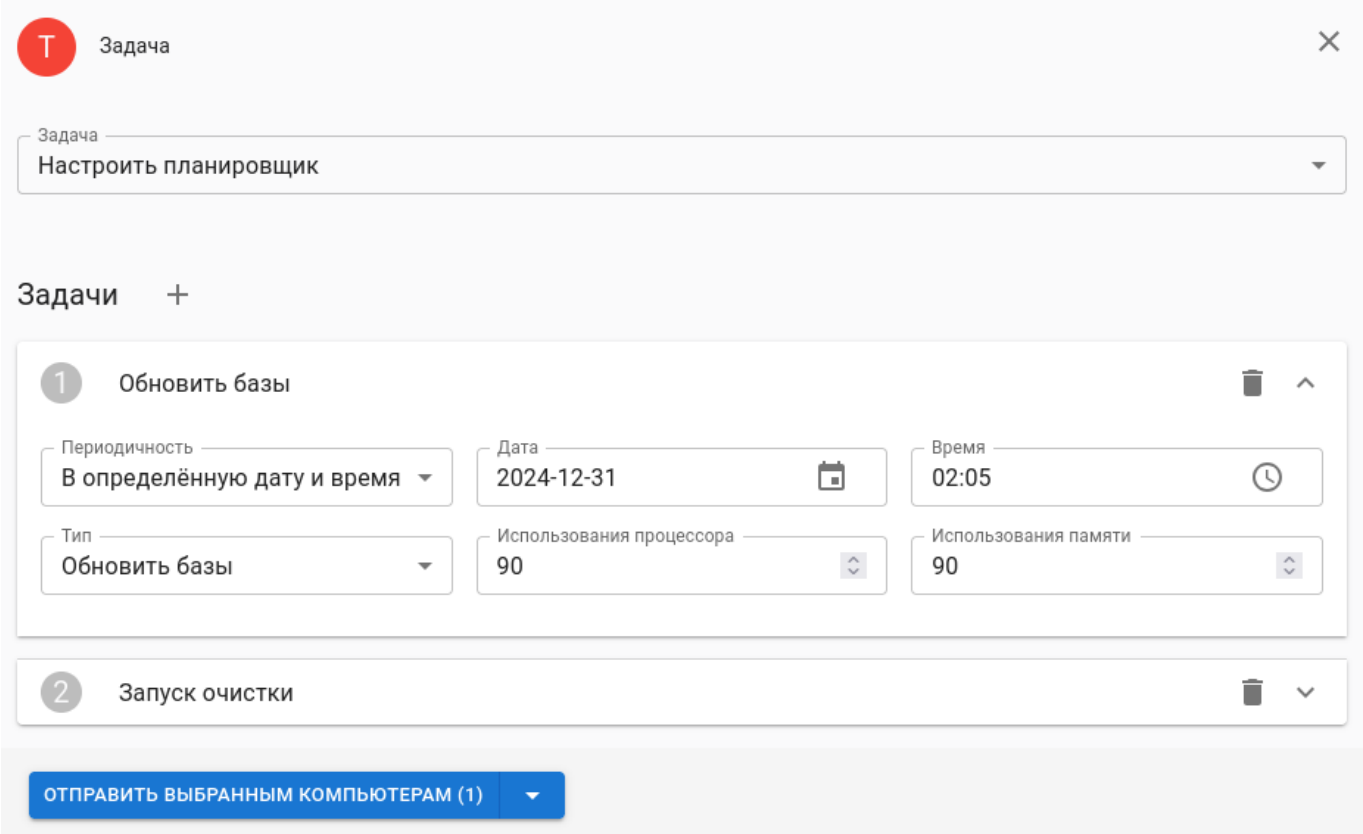


Рис. 143 – Задача «Настроить планировщик»

Параметры детальной настройки:

1) **Тип**;
2) **Периодичность**;
3) **Дата**;
4) **Время**;
5) **Использование процессора**;
6) **Использование памяти**.

Возможные значения параметра **Тип** (тип задач автоматизации):

1) **Начать сканирование** – выполняет запуск компонента антивирусный Сканер модуля контроля данных. Для запуска используются текущие настройки сканера, определенные в политике, либо выданные при помощи задачи;

2) **Обновить базы** – выполняет обновление антивирусных баз клиентской части программного комплекса ШХУНА;
3) **Обновить Агент** – выполняет обновление модуля «Агент удаленного администрирования»;
4) **Проверить целостность устройств** – будет выполнена проверка целостности устройств модулем неизменности программного комплекса ШХУНА. Для проведения данной проверки необходимо предварительно выполнить сохранение состояния устройств;
5) **Проверить целостность файлов** – будет выполнена проверка целостности файлов модулем неизменности программного комплекса ШХУНА. Для проведения данной проверки необходимо предварительно выполнить сохранение целостности файлов;
6) **Проверить целостность реестра** – будет выполнена проверка целостности реестра ОС Windows модулем неизменности программного комплекса ШХУНА. Для данной проверки необходимо необходимо предварительно выполнить сохранение целостности реестра. Задача исполняется **только** для ОС Windows;
7) **Сохранить состояние устройств** – будет выполнена операция сохранения состояния устройств, установленных на клиентских СВТ;
8) **Сохранить состояние файлов** – будет выполнена операция сохранения состояния файлов на основе настроек, установленных в модуле неизменности клиентской части программного комплекса ШХУНА;
9) **Сохранить состояние реестра** – будет выполнена операция сохранения состояния реестра ОС Windows на основе настроек, установленных в модуле неизменности клиентской части программного комплекса ШХУНА;
10) **Запуск очистки** – будет выполнена операция запуска на исполнение модуля удаления на основе настроек, установленных в модуле удаления клиентской части программного комплекса ШХУНА.

Возможные значения параметра **Периодичность**:

1) **При запуске** – не требует указания даты и времени, так как задача будет выполнена при старте ОС;

2) **В определенную дату и время** – требует заполнения даты и времени;
3) **Каждый час** – не требует заполнения даты и времени, так как задача будет выполняться каждый час;
4) **Ежедневно в указанное время** – не требует заполнения даты. Требует заполнения времени, так как задача будет выполняться в указанное время каждый день.

Возможные значения параметры **Дата** и **Время** устанавливаются графическим способом, используя элементы управления **Календарь** (в поле установки даты) и **Часы** (в поле установки времени), которые доступны только для типов задач, подразумевающих указание даты/времени.

Параметры **Использование процессора** (ограничивает выполнение задачи в случае высокой загруженности процессора на клиентском СВТ) и **Использование памяти** (ограничивает выполнение задачи в случае недостаточного количества памяти на клиентском СВТ) являются целочисленными значениями от 0 до 100 %.

Можно задать несколько задач. Для этого необходимо воспользоваться иконкой + . Задачи будут выполняться по очереди.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.20. Задача «Настроить проверку целостности»

Данная задача предназначена для выполнения настройки модуля неизменности программного комплекса ШХУНА. Модуль выполняет сохранение указанных в настройках параметров сущностей (файлы, устройства, реестр ОС Windows) и в последующем контролирует их состояние.

Можно задать несколько шаблонов (рис. 144) или ключей реестра (рис. 145) для проверки целостности. Для этого необходимо использовать иконку + . Для свертывания/развертывания детальных настроек используется элемент управления в правом крае списка. Для удаления созданного шаблона необходимо воспользоваться иконкой 🗑 в правом углу списка.

В поле **Путь** необходимо ввести существующий на клиентском СВТ путь

к директории, целостность которой необходимо контролировать. В поле **Маска** требуется ввести критерии, по которым будет производиться сохранение файлов для контроля целостности (можно использовать т.н. glob-синтаксис). Например, **«*.txt»** указывает на то, что необходимо сохранить все файлы с расширением **«.txt»**.

Ветки реестра ОС Windows (registry keys) задаются стандартным для ОС Windows способом.

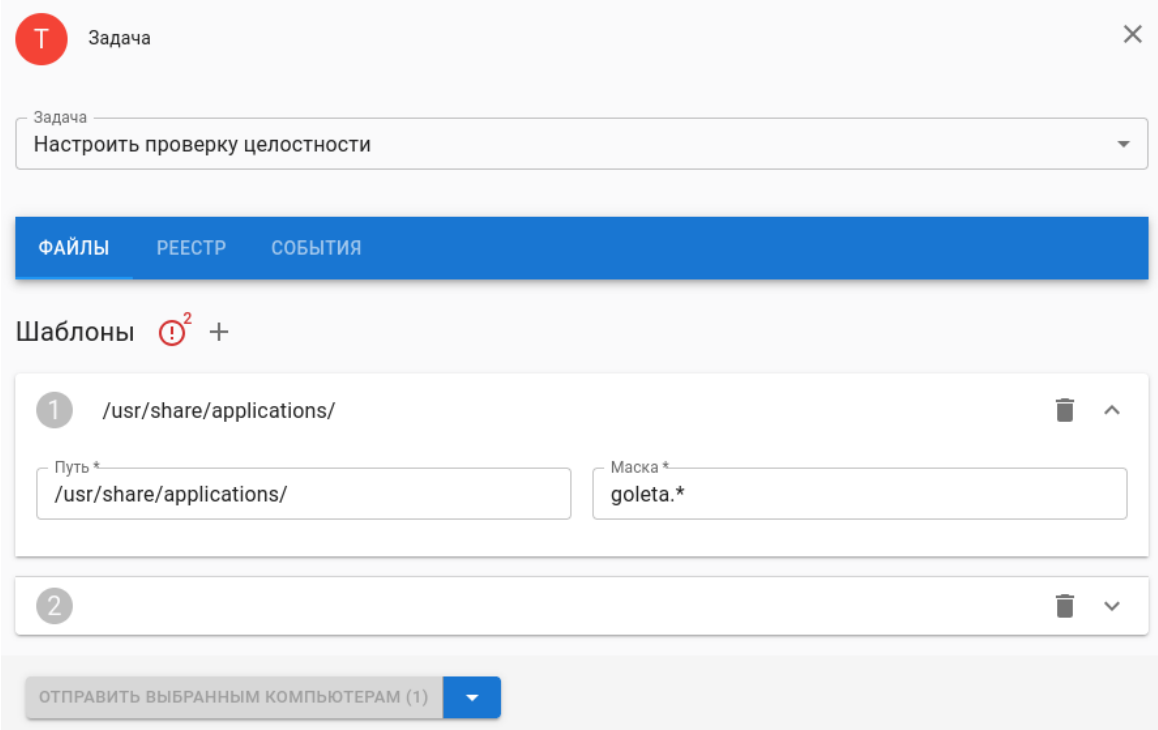


Рис. 144 – Задача «Настроить проверку целостности». Файлы

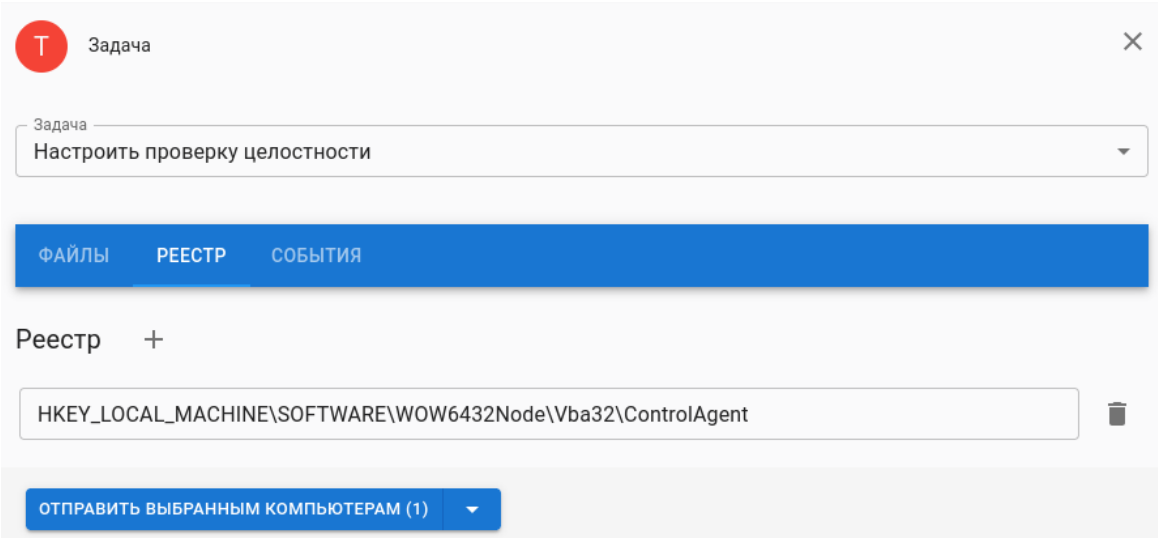


Рис. 145 – Задача «Настроить проверку целостности». Реестр ОС Windows

Вкладка **События** (рис. 146) позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно.

Снятый флажок означает, что событие не будет зарегистрировано в выбранном журнале.

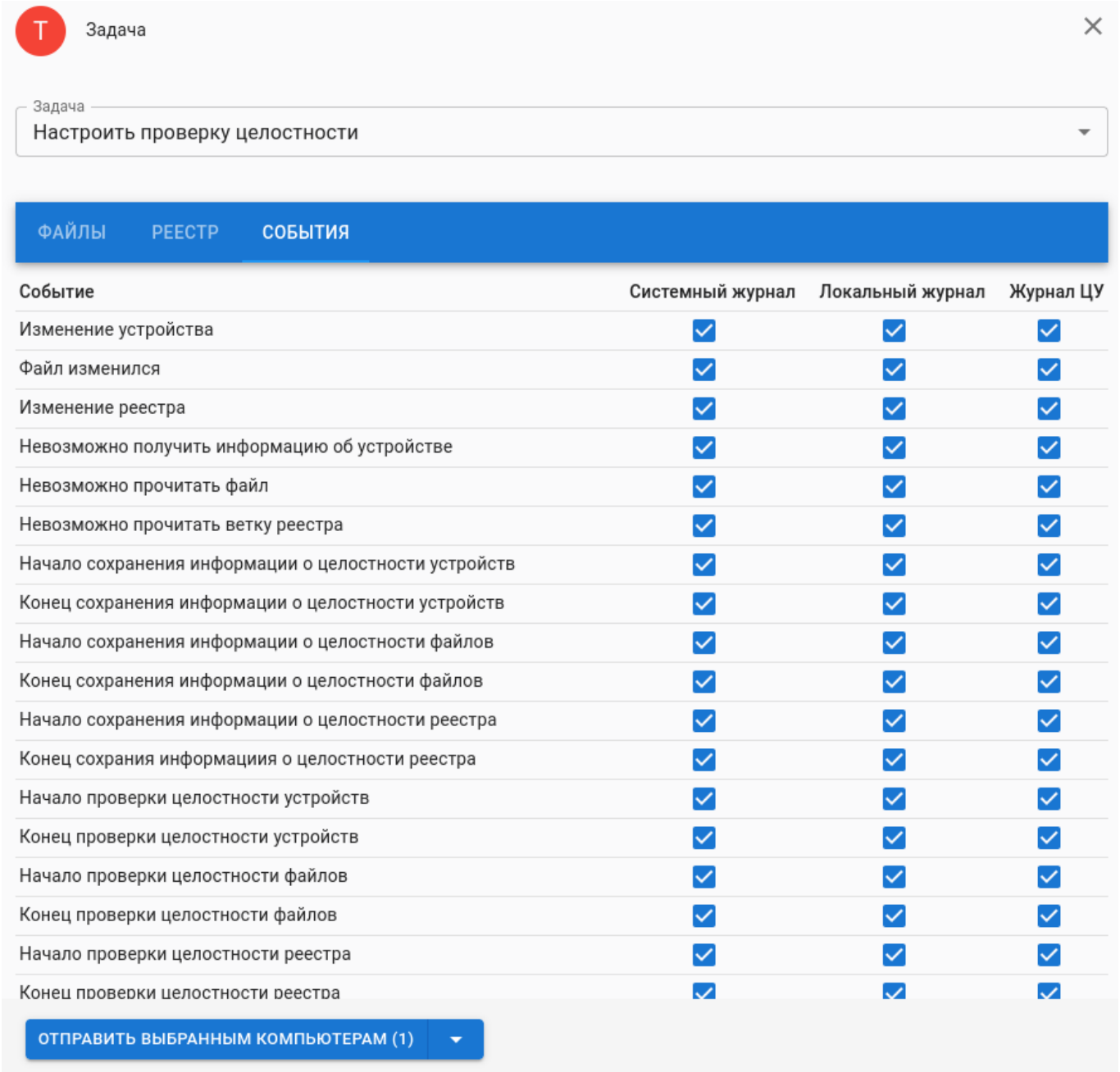


Рис. 146 – Задача «Настроить проверку целостности». События

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.21. Задача «Настроить модуль удаления»

Данная задача предназначена для выполнения настройки модуля удаления программного комплекса ШХУНА.

Настройки модуля удаления разделены на две вкладки: **Шаблоны** (рис. 147) и **События** (рис. 148).

На вкладке **Шаблоны** выполняется создание и настройка шаблонов модуля удаления.

В первую очередь необходимо ввести имя шаблона. Флажок **Шаблон включен** определяет, будет ли данный шаблон активен при работе модуля удаления.

В разделе пути требуется указывать существующий путь к директории, а также маску по которой будет осуществляться удаление файлов.

Необходимо учитывать разницу в формировании путей к директориям в ОС Windows и ОС Linux.

Для задания маски можно использовать регулярные выражения.

В одном шаблоне может быть несколько путей к файлам, предназначенным для удаления.

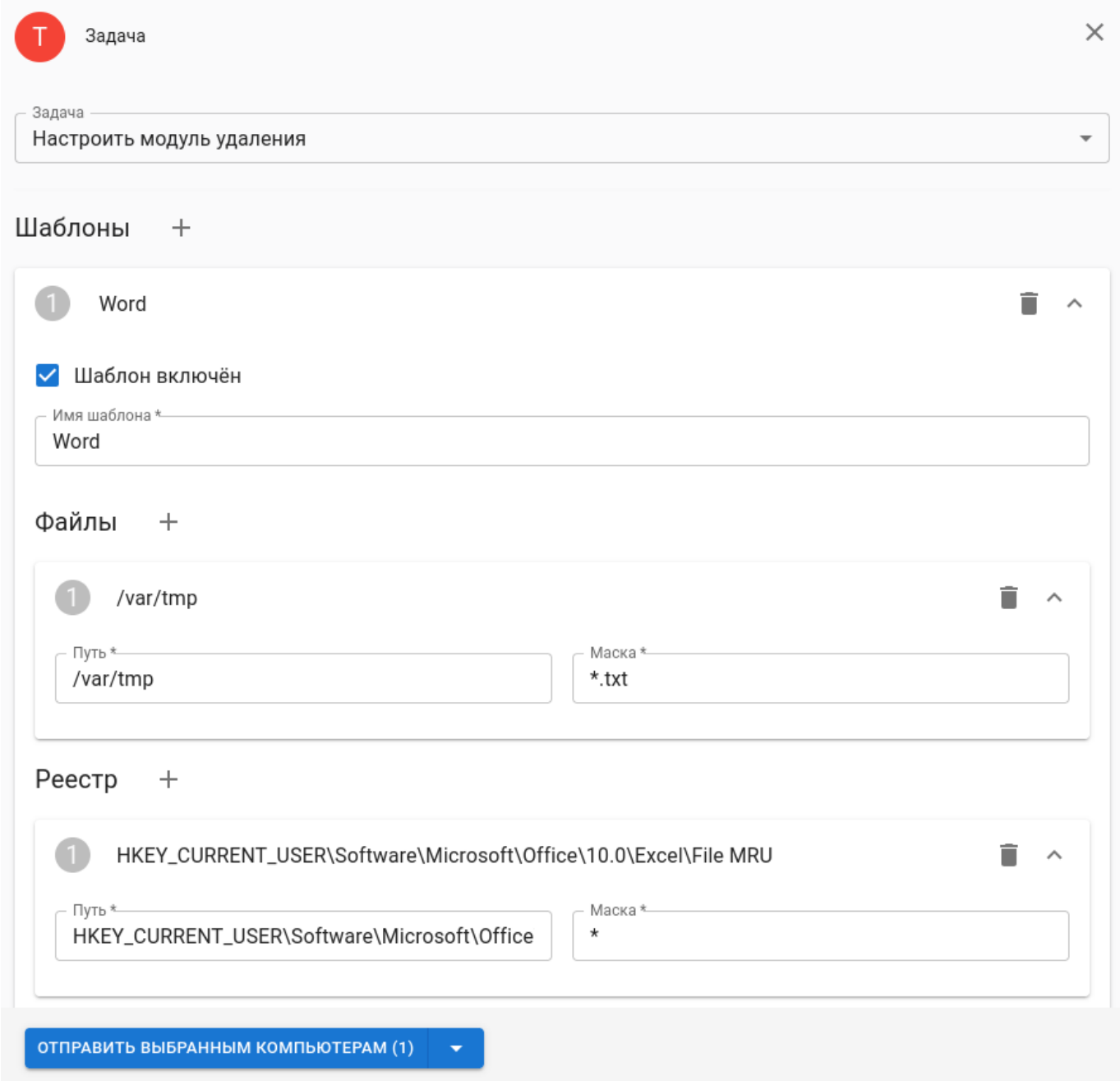


Рис. 147 – Задача «Настроить модуль удаления». Шаблоны

Ветки реестра Windows (registry keys) задаются стандартным для ОС Windows способом.

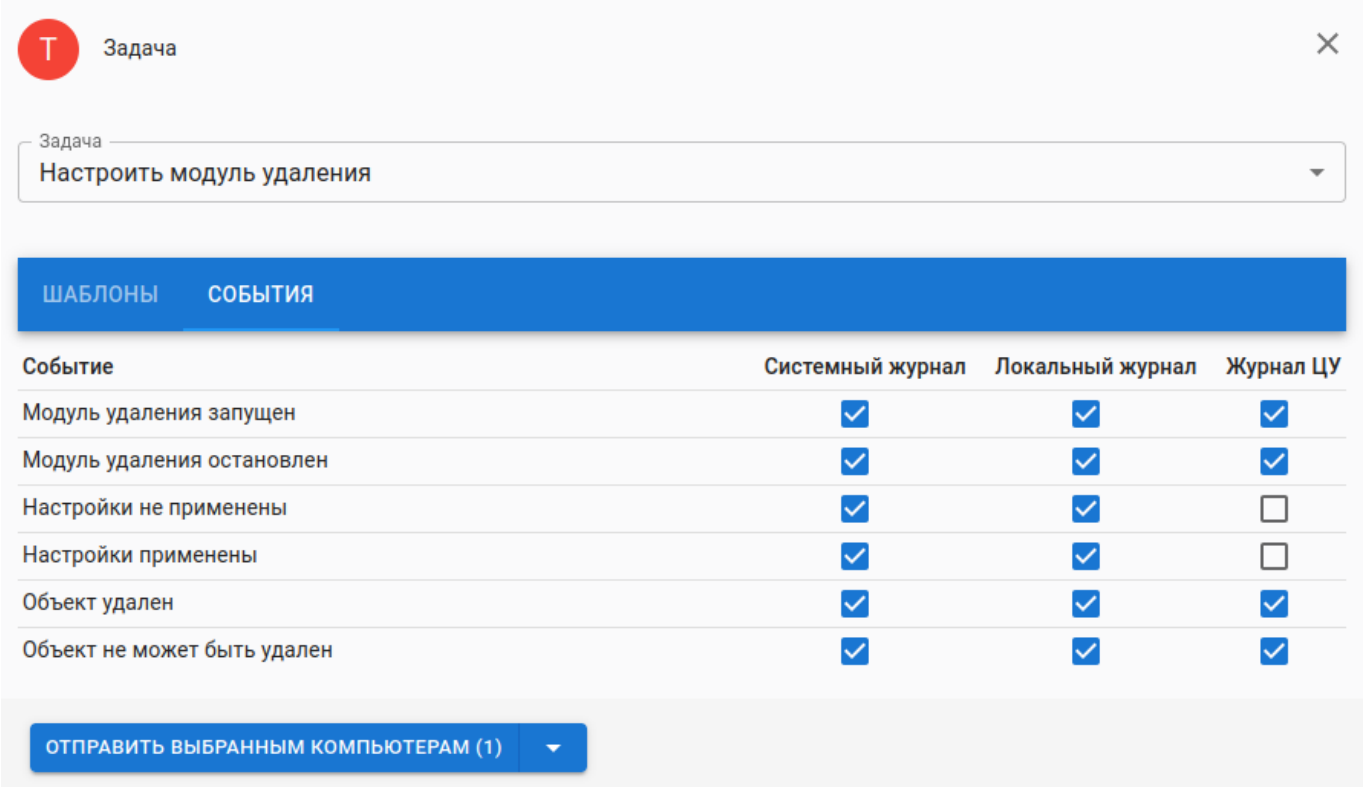


Рис. 148 – Задача «Настроить модуль удаления». События

Вкладка **События** позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно. Снятый флажок означает, что событие не будет зарегистрировано в выбранном журнале.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.22. Задача «Запустить очистку»

Данная задача (рис. 149) предназначена для выполнения удаления/затирания модулем удаления программного комплекса ШХУНА на клиентском СВТ.

В результате выполнения на клиентском СВТ будет обеспечено удаление и затирание (secure erase) файлов, определенных в настройках модуля удаления.

Примечание. В ОС Windows также может быть выполнено удаление всех значений реестра, определенных настройками модуля удаления.

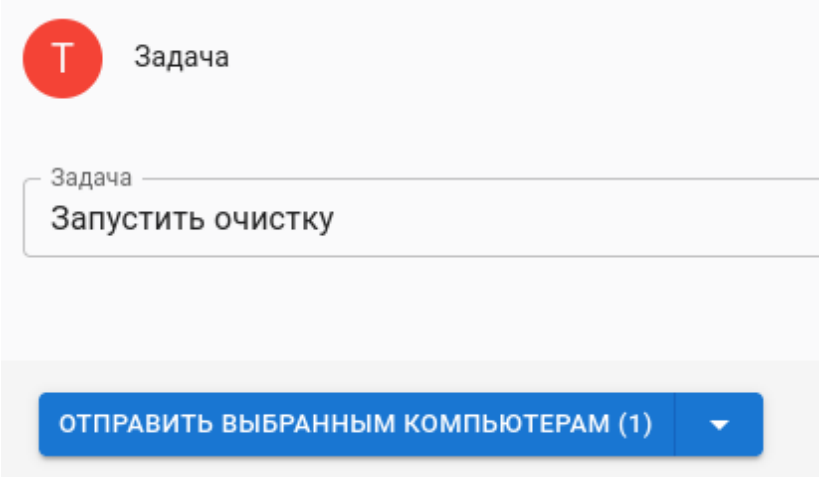


Рис. 149 – Задача «Запустить очистку»

Чтобы сформированная задача была выдана выбранным компьютерам необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.23. Задача «Выдать политики»

Данная задача (рис. 150) предназначена для отправки политик, определенных в разделе **Группы** (см. п. 4.6.3), на клиентские СВТ.

Задача «Выдать политики» не имеет дополнительных параметров.

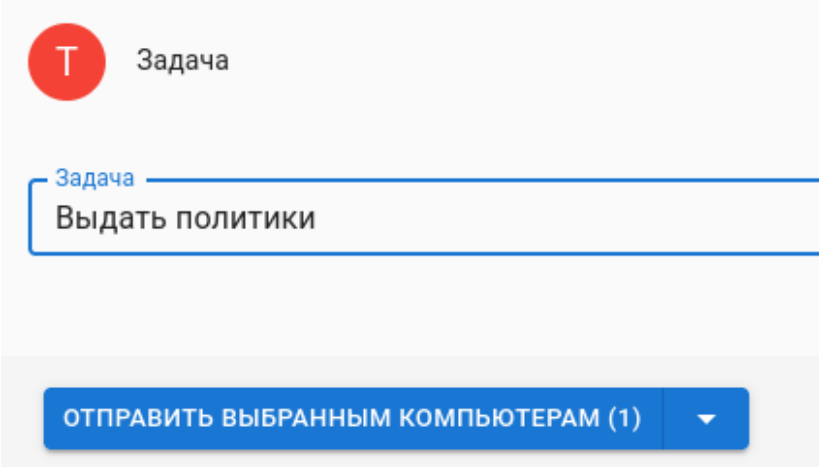


Рис. 150 – Задача «Выдать политики»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.24. Задача «Проверить целостность»

Данная задача (рис. 151) предназначена для выполнения модулем неизменности программного комплекса ШХУНА соответствующих задач .

Возможные типы действий (меню **Команда**):

1) **Проверить**;
2) **Сохранить**.

Возможные объекты действий (меню **Компонент**):

1) **Файлы**;
2) **Реестр**;
3) **Устройства**.

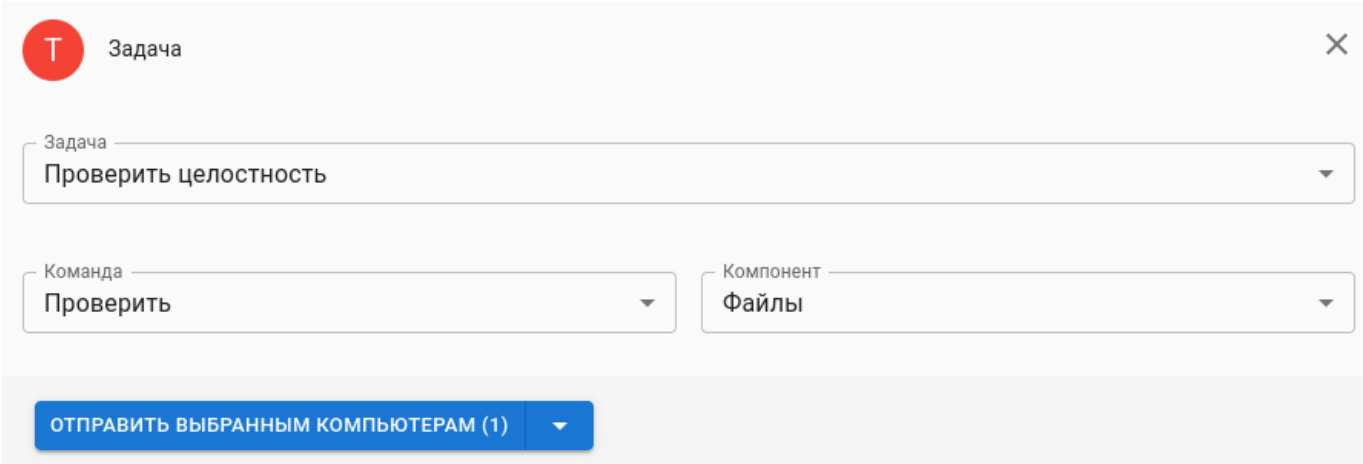


Рис. 151 – Задача «Проверить целостность»

В результате выдачи задачи с выбранными значениями полей **Команда** и **Компонент** на клиентском СВТ будет выполнено одно из следующих действий:

- сохранение состояния файлов (**Сохранить**, компонент **Файлы**);
- сохранение состояния реестра Windows (**Сохранить**, компонент **Реестр**);
- сохранение состояния устройства (**Сохранить**, компонент **Устройства**);
- проверка состояния файлов (**Проверить**, компонент **Файлы**);
- проверка состояния реестра Windows (**Проверить**, компонент **Реестр**);
- проверка состояния устройства (**Проверить**, компонент **Устройства**).

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.25. Задача «Включить / выключить монитор»

Данная задача (рис. 152) предназначена для выполнения включения или выключения компонента Монитор модуля контроля данных программного комплекса ШХУНА на клиентском СВТ.

Установка выбора **Включен** указывает, что компонент Монитор предполагается к включению, снятие выбора – предполагает его выключение.

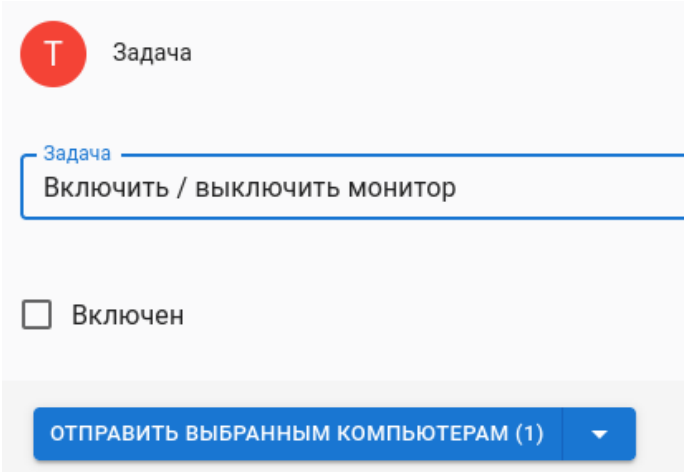


Рис. 152 – Задача «Включить / выключить монитор»

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.26. Задача «Обновить все»

Данная задача (рис. 153) предназначена для выполнения обновления клиентской части программного комплекса ШХУНА на клиентском СВТ.

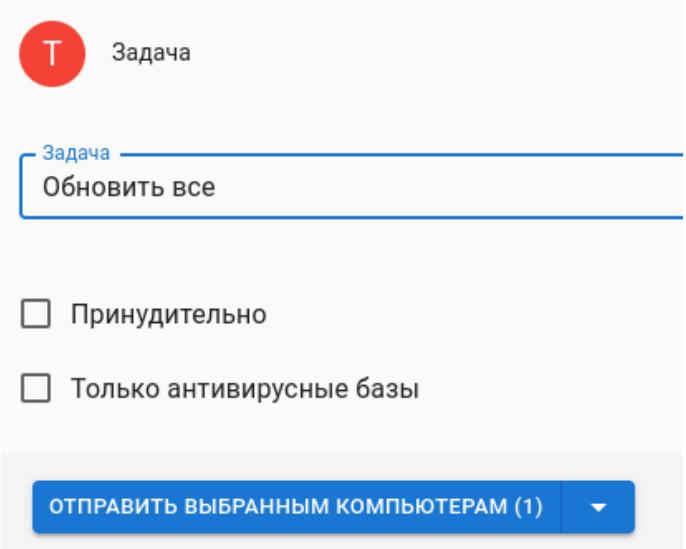


Рис. 153 – Задача «Обновить все»

Пункт **Принудительно** – предназначен для формирования задачи принудительного обновления модулей клиентской части программного комплекса ШХУНА. Для клиентских СВТ под управлением ОС Windows может произойти перезагрузка СВТ.

Пункт **Только антивирусные базы** – предназначен для формирования задачи на обновление только антивирусных баз. Это гарантированно не приведет к обновлению исполняемых модулей и перезагрузке ОС.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.27. Задача «Обновить ключ»

Данная задача (рис. 154) предназначена для выполнения обновления/установки ключевого файла (лицензии) для клиентской части программного комплекса ШХУНА. В качестве ключевого файла будет использоваться текущая лицензия, установленная на ЦУ.

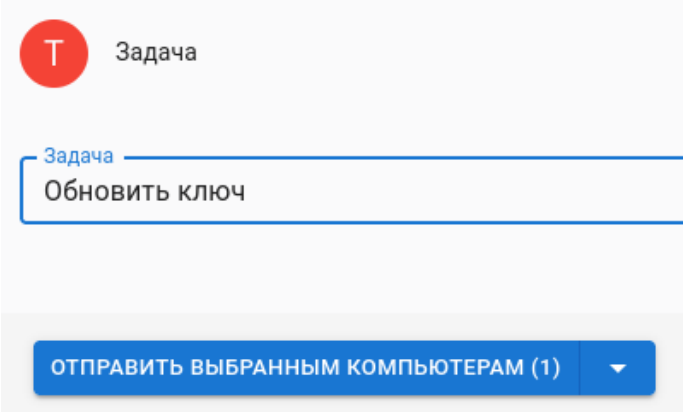


Рис. 154 – Задача «Обновить ключ»

Данная задача не имеет дополнительных параметров.

Чтобы сформированная задача была выдана выбранным компьютерам, необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.2.28. Задача «Отсоединить агент»

Данная задача (рис. 155) предназначена для выполнения отключения модуля «Агент удаленного администрирования» клиентской части программного комплекса ШХУНА от текущего ЦУ. Тем самым администратор ЦУ потеряет управление над выбранными клиентскими СВТ.

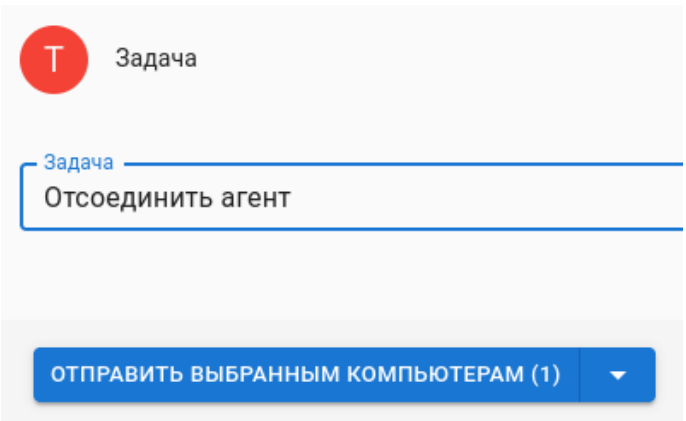


Рис. 155 – Задача «Отсоединить агент»

Данная задача не имеет дополнительных параметров.

Чтобы сформированная задача была выдана выбранным компьютерам,

необходимо нажать на кнопку **Отправить выбранным компьютерам** / **Отправить компьютерам по фильтру** в нижней части диалогового окна.

4.6.3. Раздел Группы

Раздел **Группы** (рис. 156) предназначен для объединения компьютеров в группы и назначения им специально сформированных политик.

Политика – набор определяемых администратором безопасности настроек, которые будут в автоматическом режиме переданы клиентскому СВТ входящему в текущую группу.

На главной странице представлены графическое отображение групп с учетом иерархии (в виде древоподобной структуры). Корневая группа является обязательной (переименовать или удалить ее невозможно). По умолчанию уже созданы группы с именами Windows и Linux. В них представлены базовые настройки политик по умолчанию.

Администратор безопасности должен выполнить детальную настройку политик самостоятельно, исходя из нужд организации, ее задач и организационной структуры.

Новую подгруппу можно создать при помощи кнопки **Создать**. Кнопка **Экспорт** предназначена для сохранения данных во внешний формат представления данных (CSV – comma-separated values text file format).

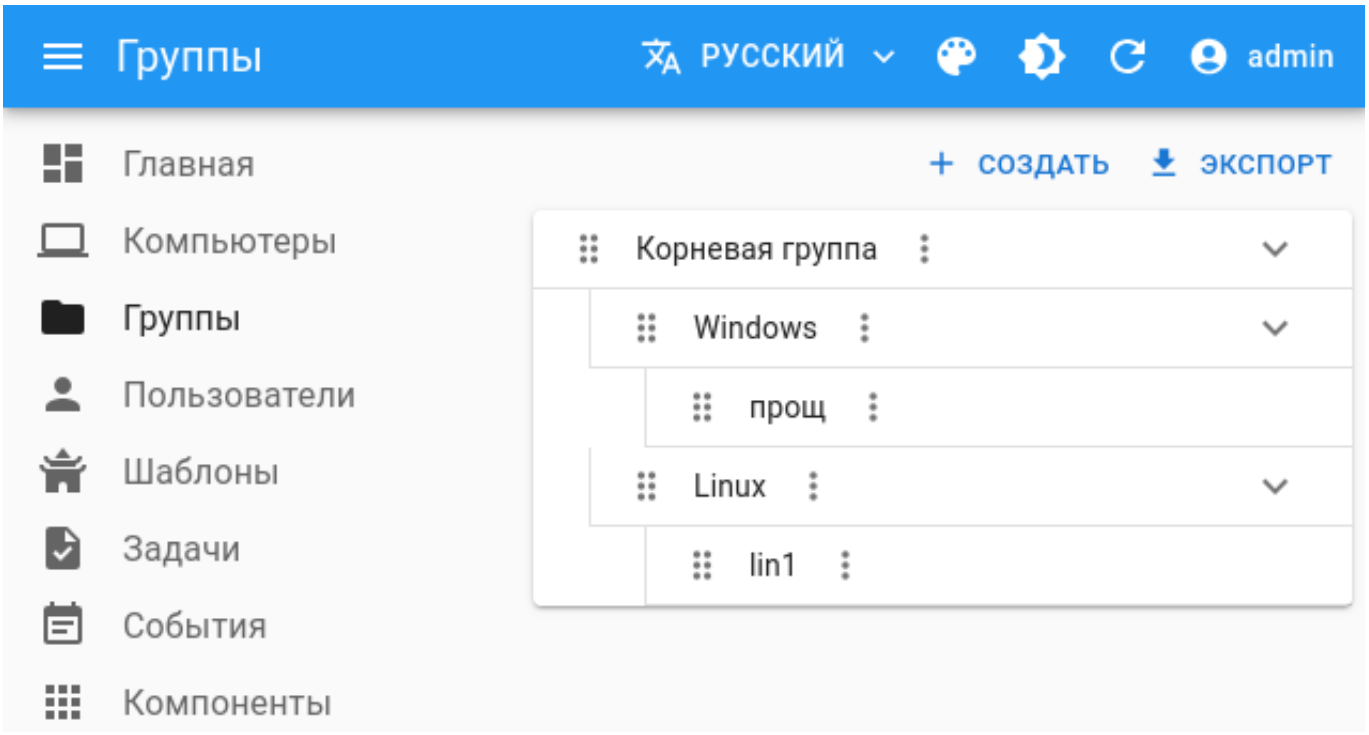


Рис. 156 – Раздел «Группы». Общий вид

Для того, чтобы создать новую группу, необходимо нажать на кнопку **Создать** и заполнить появившуюся форму **Создать группу** (рис. 157). В этой форме можно указать, какая из существующих групп будет являться родительской для этой новой группы.

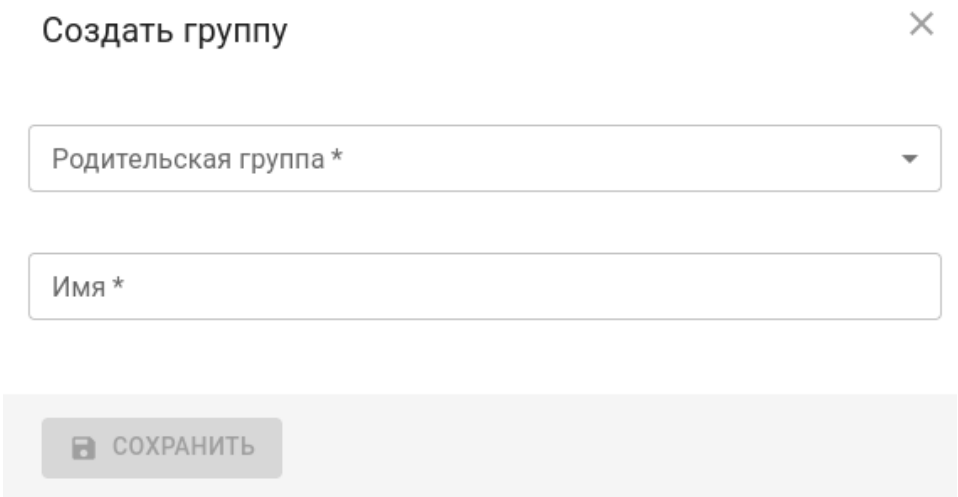


Рис. 157 – Раздел «Группы». Создание новой группы

Пример новой созданной группы изображен на рис. 158.

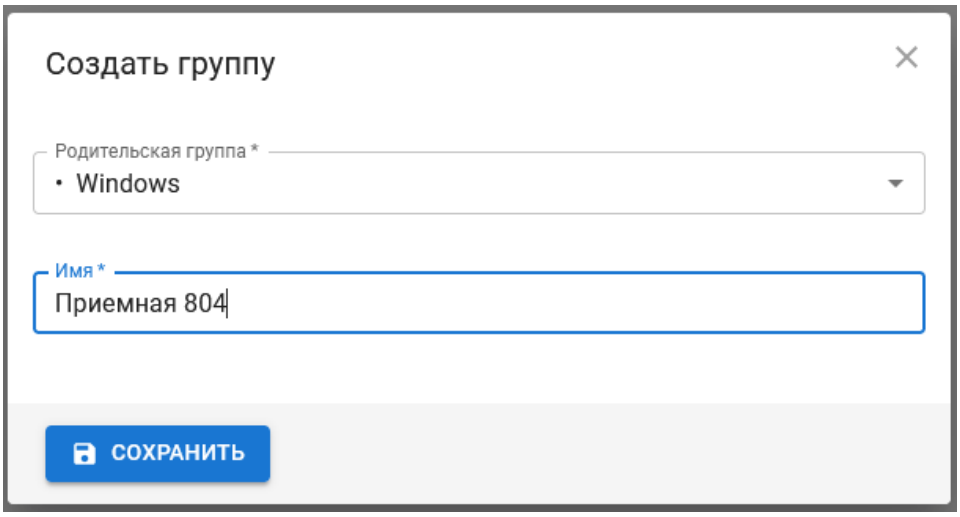


Рис. 158 – Раздел «Группы». Пример новой группы

Общий вид иерархии групп после новой созданной группы изображен на рис. 159.

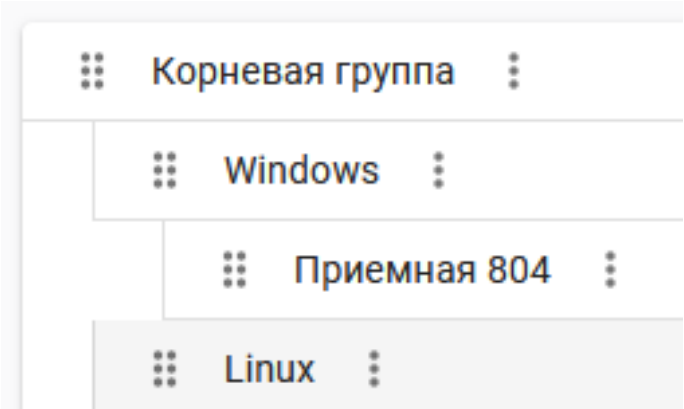


Рис. 159 – Раздел «Группы». Пример новой группы.
Общий вид иерархии

Настройка иерархии групп осуществляется с помощью приема drag-and-drop («перетягивания», удерживая ЛКМ). После создания группы ее можно перенести в любое место текущей иерархии. Перенос осуществляется перемещением указателя манипулятора типа «мышь» с удержанием ЛКМ на элементе с иконкой ⠿ .

Например, группу можно перенести в подкатегорию **Корневая группа**, либо перенести ее в любую из существующих групп, сделав ее дочерней.

Выполнить действия по настройке группы можно, нажав на элемент управления, который визуально представлен иконкой ⋮ справа от элемента с названием группы. В меню доступно изменение, переименование и удаление группы (рис. 160).

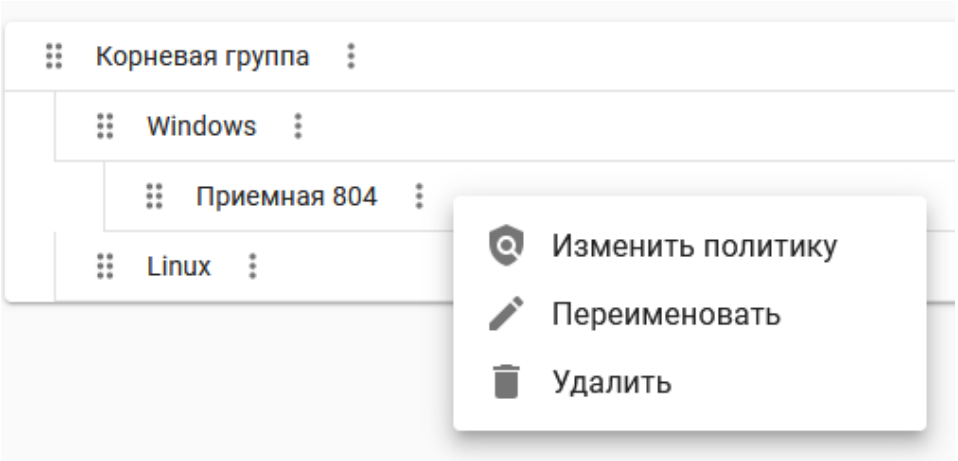


Рис. 160 – Раздел «Группы». Действия над группой

Кнопка **Изменить политику** позволяет перейти к детальным настройкам политик.

4.6.3.1. Изменение политик

Политика представляет собой список настроек, которые клиентская часть программного комплекса ШХУНА получает в автоматическом режиме. Это позволяет гарантировать, что подключенное к ЦУ клиентское СВТ будет функционировать с указанными Администратором настройками. Также позволяет осуществить принудительный возврат к установленным Администратором настройкам (в случае их изменения через графический интерфейс клиента программного комплекса ШХУНА).

Настройки политик, которые соответствуют разделам клиентской части программного комплекса ШХУНА (рис. 161):

1) **Диспетчер**;
2) **Планировщик**;
3) **Сканер**;
4) **Монитор**;
5) **Межсетевой экран**;
6) **Карантин**;
7) **Проверка целостности**;
8) **Модуль удаления**;
9) **Управление устройствами**;

10) **Проактивная защита**.

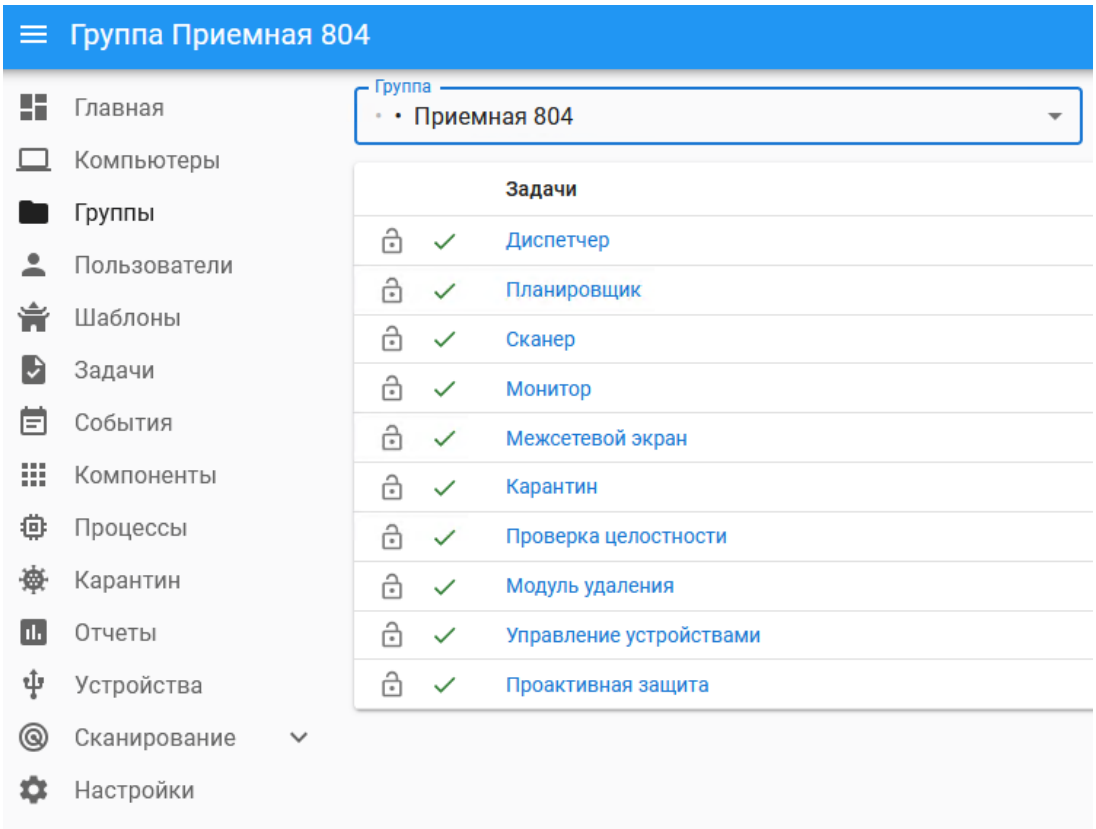


Рис. 161 – Раздел «Группы». Политики группы

	Задачи	Определена в группе
	Диспетчер	Корневая группа
	Планировщик	Корневая группа
	Сканер	Корневая группа
	Монитор	Windows
	Межсетевой экран	Корневая группа
	Карантин	Корневая группа
	Проверка целостности	Корневая группа
	Модуль удаления	Windows
	Управление устройствами	Корневая группа
	Проактивная защита	Windows

Рис. 162 – Раздел «Группы». Политики группы. Детально

Настройка наследования осуществляются в форме, вызываемой по нажатию ЛКМ на имени категории (**Диспетчер**, **Планировщик** и т.д.).

Открыв любую из настроек политики (рис. 163), в верхней части можно увидеть два пункта, которые определяют правила наследования: **Использовать родительские настройки**, **Запретить наследование**, а также пункт **Включена**.

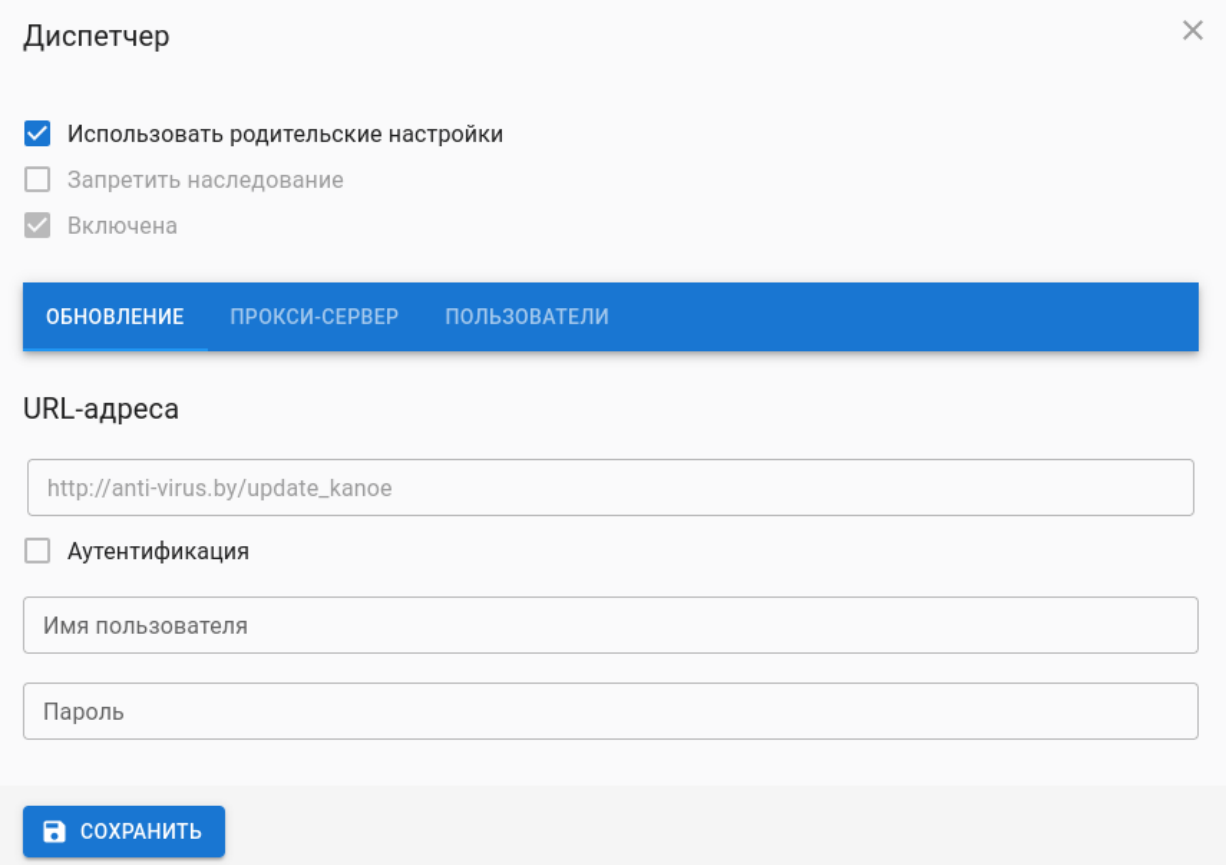


Рис. 163 – Раздел «Группы». Политики групп. Диспетчер

Использовать родительские настройки – означает полное заимствование настроек модуля из настроек выполненных в родительской, по отношению к текущей, группе. Это позволяет выполнить настройки модуля однократно и автоматически распространить эти настройки для всех дочерних групп. Изменение настроек в родительской группе будет автоматически передано всем дочерним. Однако в любой части этой цепочки можно снять выбор пункта **Использовать родительские настройки** и переопределить настройки для группы.

Запретить наследование – предписывает всем дочерним группам использовать только текущие настройки политики для выбранного модуля. Ни на каком из уровней цепочки наследования правил политики для выбранного модуля не будет возможности

переопределения настроек политики для выбранного модуля. На странице **Группы** – такая политика будет отображена с иконкой «закрытый замок».

Включена – означает, что политика будет применена.

4.6.3.2. Настройка политик. Управление устройствами

В данном разделе сосредоточены настройки модуля управления доступом в той его части, что касается управления устройствами.

Настройки логически подразделяются на несколько категорий: **Общие**, **Классы**, **USB**, **События**.

Вкладка **Общие** (рис. 164) содержит настройку применения правил по умолчанию для USB Mass Storage устройств. Из выпадающего списка можно выбрать варианты:

1) **Блокировать запись** (Запретить запись) – информация со вставленного устройства может быть прочитана, однако запись на это устройство будет запрещена;
2) **Пропустить** (Разрешить / Ничего не делать) – полный доступ на запись и чтение для вставленного устройства;
3) **Блокировать** (Запретить) – устройство не доступно как для записи, так и для чтения.

Выбор пункта **Управлять сетевыми устройствами» определяет**, будет ли передана соответствующая настройка на клиентскую часть программного комплекса ШХУНА.

Вкладка **Классы** (рис. 165) содержит настройки для классов устройств, которые контролирует модуль управления доступом к устройствам на клиентском СВТ, а также действия над соответствующими классами. Из выпадающего списка можно выбрать следующие варианты действий:

1) **По умолчанию**;
2) **Запретить** (Блокировать);
3) **Разрешить** (Пропустить);
4) **Запретить запись** (Блокировать запись).

Полное применение настроек для классов на клиентском СВТ под управлением ОС Windows требует перезагрузки ОС.

Вкладка **USB** (рис. 166) содержит настройки поддерживаемых для контроля USB-классов. USB-класс может быть разрешен, либо запрещен для функционирования.

Вкладка **События** позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно (рис. 167).

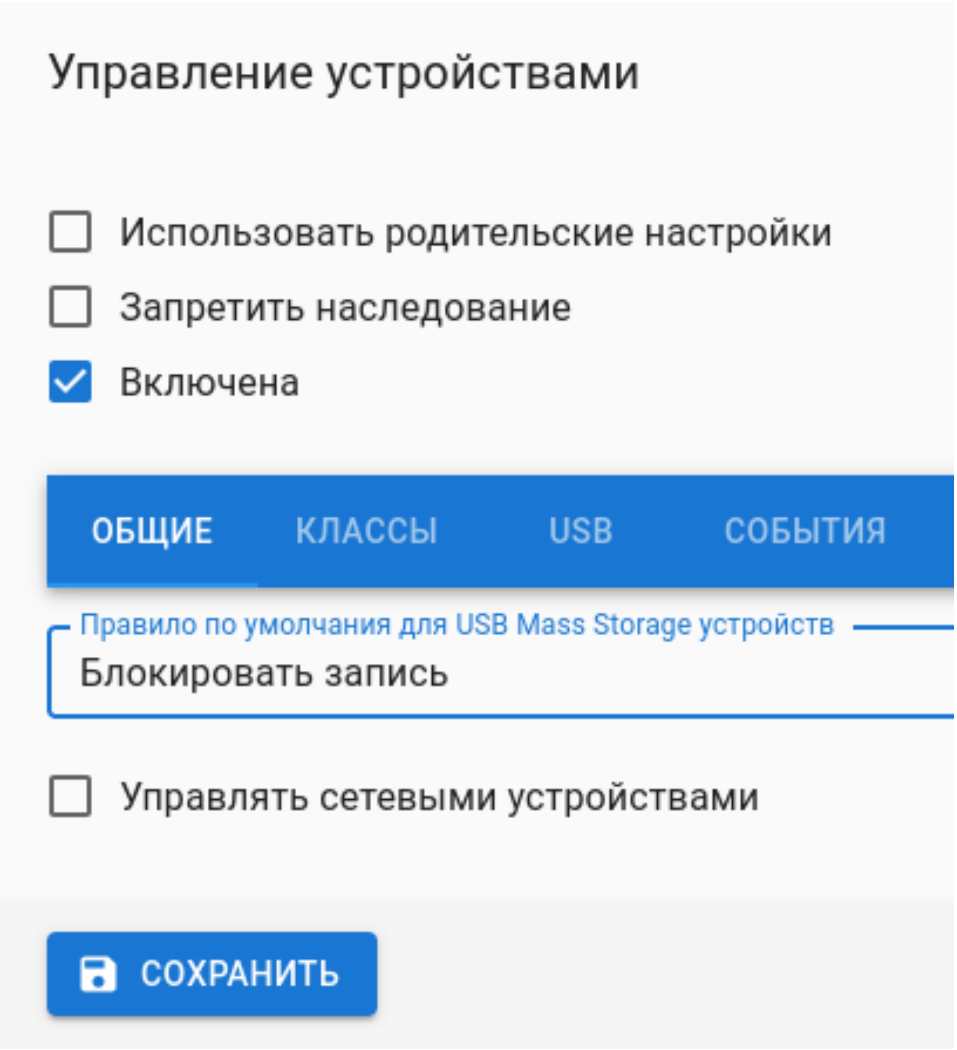


Рис. 164 – Раздел «Группы». Настройка политик.
Управление устройствами. Общие

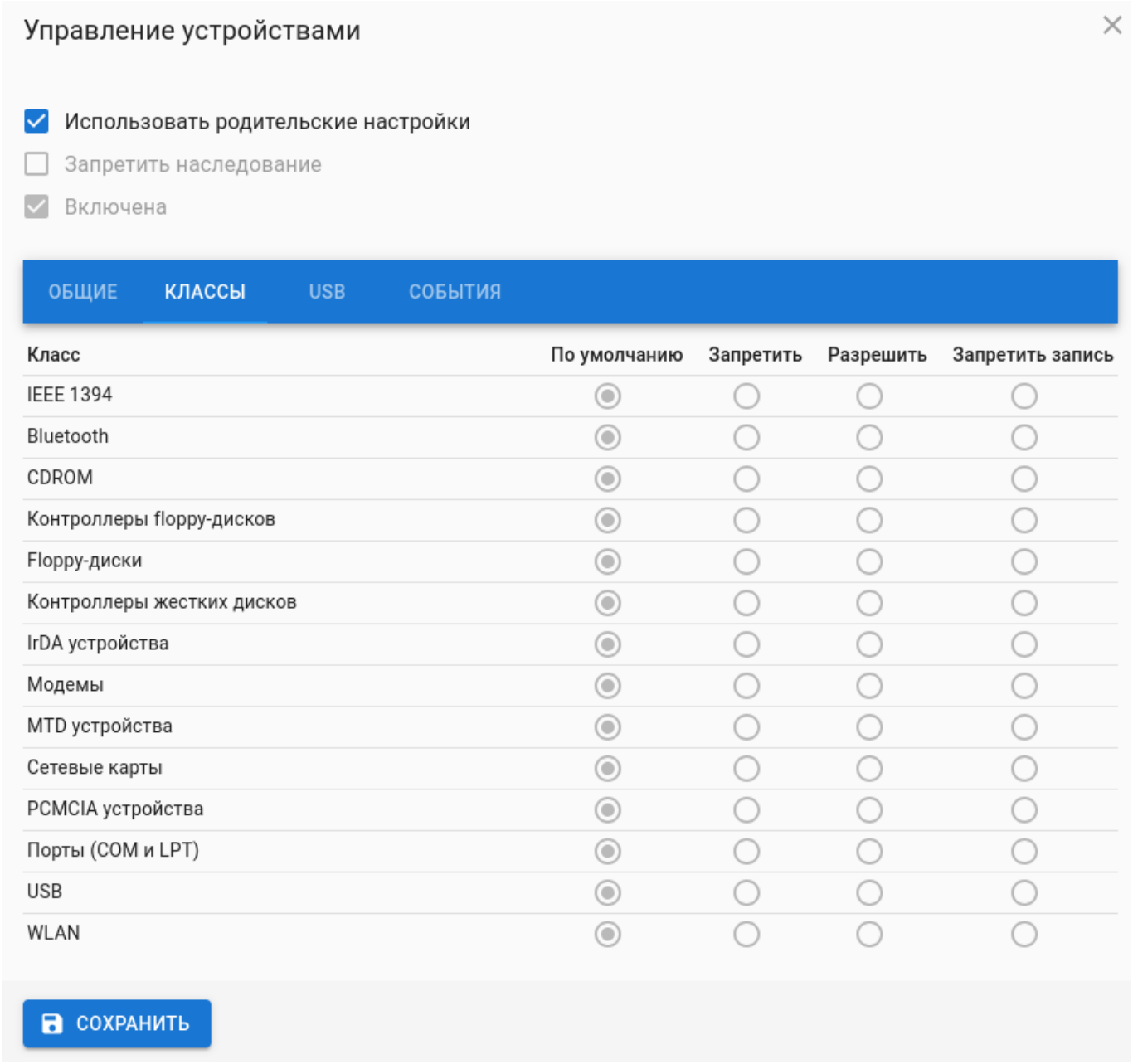


Рис. 165 – Раздел «Группы». Настройка политик.
Управление устройствами. Классы

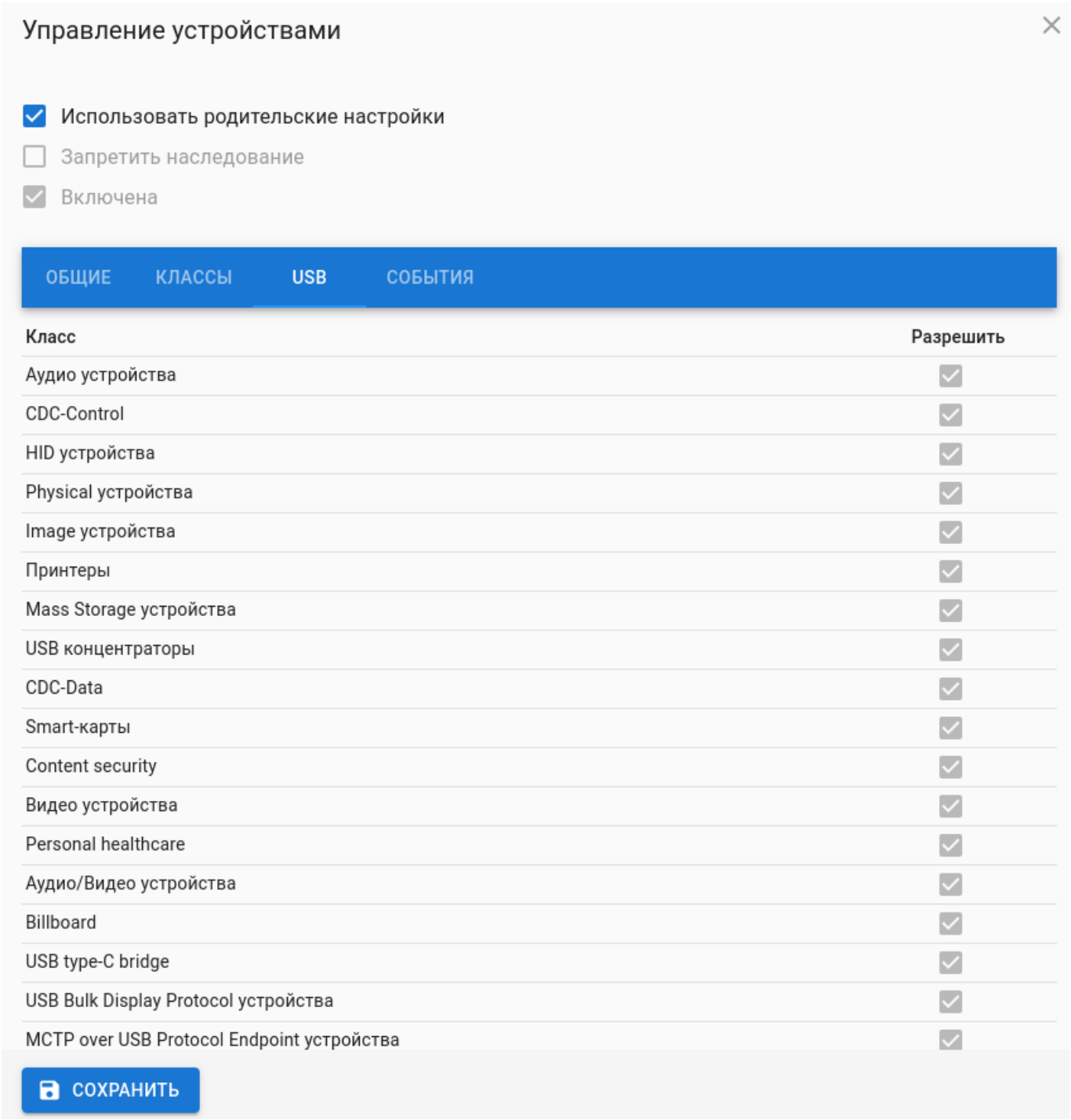


Рис. 166 – Раздел «Группы». Настройка политик.
Управление устройствами. USB

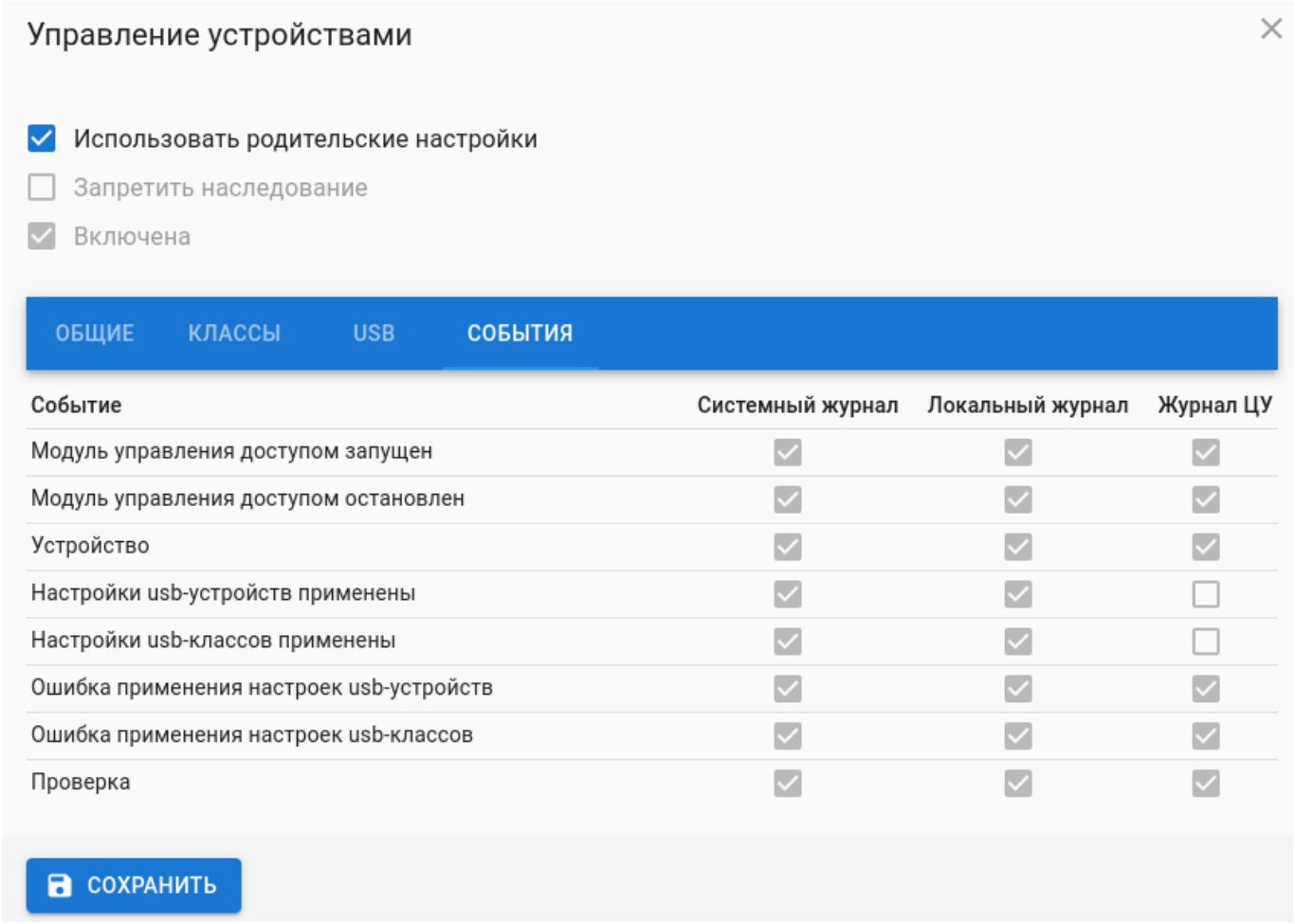


Рис. 167 – Раздел «Группы». Настройка политик.
Управление устройствами. События

4.6.3.3. Настройка политик. Проактивная защита

В данном разделе сосредоточены настройки компонента Проактивная защита модуля контроля данных.

Настройки логически подразделяются на несколько категорий: **Аудит**, **Защищаемые объекты**, **Пользователи**, **Принтеры**, **События**.

Вкладка **Аудит** (рис. 168) обеспечивает включение контроля действий пользователя на основе расширений программ (например, «.pdf», «.txt» и т.д.). При необходимости увидеть информацию об открытии файлов с расширением «.txt» необходимо выбрать пункт **Включен**, а также указать в строке ввода расширение `txt`.

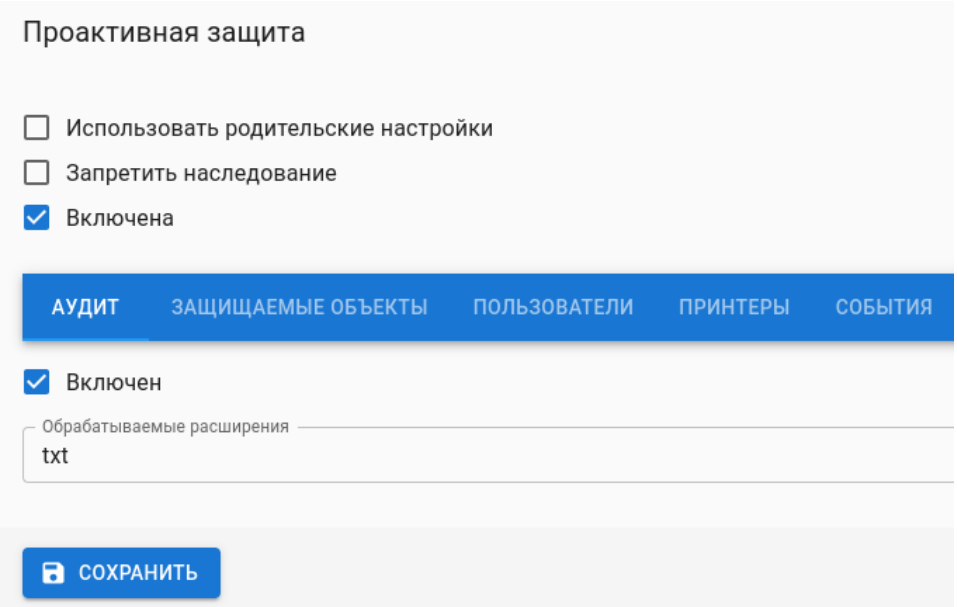


Рис. 168 – Раздел «Группы». Настройка политик.
Проактивная защита. Аудит

Вкладка **Защищаемые объекты** (рис. 169) предоставляет настройки компонента Проактивная защита. Пункт **Защита объектов включена** определяет, будет ли активной защита объектов после выдачи этой политики на клиентское СВТ. Каждая из доступных настроек представляет собой выпадающий список выбора, который предварительно необходимо сформировать в разделе **Шаблоны**. В результате выбора **Включена** список будет добавлен в настройки защищаемых объектов.

Типы объектов, которые обрабатываются компонентом Проактивная защита, следующие:

1) **Защищенные директории** – данный тип объектов представляет собой директории, запись и чтение которых доступны только доверенным приложениям;
2) **Защищенные файлы** – список конкретных файлов, запись и чтение которых доступны только доверенным приложениям;
3) **Директории (только чтение)** – список директорий, доступ к которым открыт всем пользователям и процессам только на чтение. Полный доступ имеют только приложения, перечисленные в списке доверенных;
4) **Файлы (только чтение)** – список файлов, доступ к которым открыт всем

пользователям и процессам только на чтение. Полный доступ имеют только приложения, перечисленные в списке доверенных;

5) **Разрешенные директории** – список директорий, которые будут исключены из защиты. Доступ к содержимому директорий могут получить все пользователи и процессы. Однако необходимо учитывать настройки родительской директории: когда директория внесена в список **Защищенные директории** переход к разрешенной директории может быть выполнен только путем прямого перехода по полному пути;
6) **Разрешенные файлы** – список файлов, которые будут исключены из защиты. Доступ к таким файлам могут получить все пользователи и процессы. Следует учитывать настройки родительских директорий. В некоторых случаях может потребоваться ввод полного пути к файлам;
7) **Доверенные приложения** – список приложений, в котором будет разрешен полный доступ ко всем защищаемым компонентом Проактивная защита объектам;
8) **Защищенные приложения** – приложения, которые будут защищены. Завершить такие процессы может только доверенный процесс. Например, приложение «Блокнот» («Notepad») из списка **Защищенные приложения** невозможно завершить из Диспетчера задач ОС или при помощи команды «kill»;
9) **Защищенные ключи реестра** – список ключей реестра ОС Windows, доступ к которым может получить только доверенное приложение;
10) **Ключи реестра (только чтение)** – список ключей реестра, доступ к которым открыт только на чтение. Изменение, удаление или создание новых записей в таких разделах невозможно;
11) **Защищенные значения реестра** – список значений реестра, доступ к которым есть только у доверенных приложений;
12) **Значения реестра (только чтение)** – список значений реестра, доступ к которым есть только на чтение. Изменение или удаление таких назначений невозможно.

Общий подход к работе со списками защищаемых объектов следующий:

1) на странице **Шаблоны** – создается список объектов и сохраняется с соответствующим именем;
2) на странице **Группы** в выпадающем списке защищаемых объектов устанавливается флажок напротив имени списка объектов;
3) сохраняется политика защищаемых объектов.

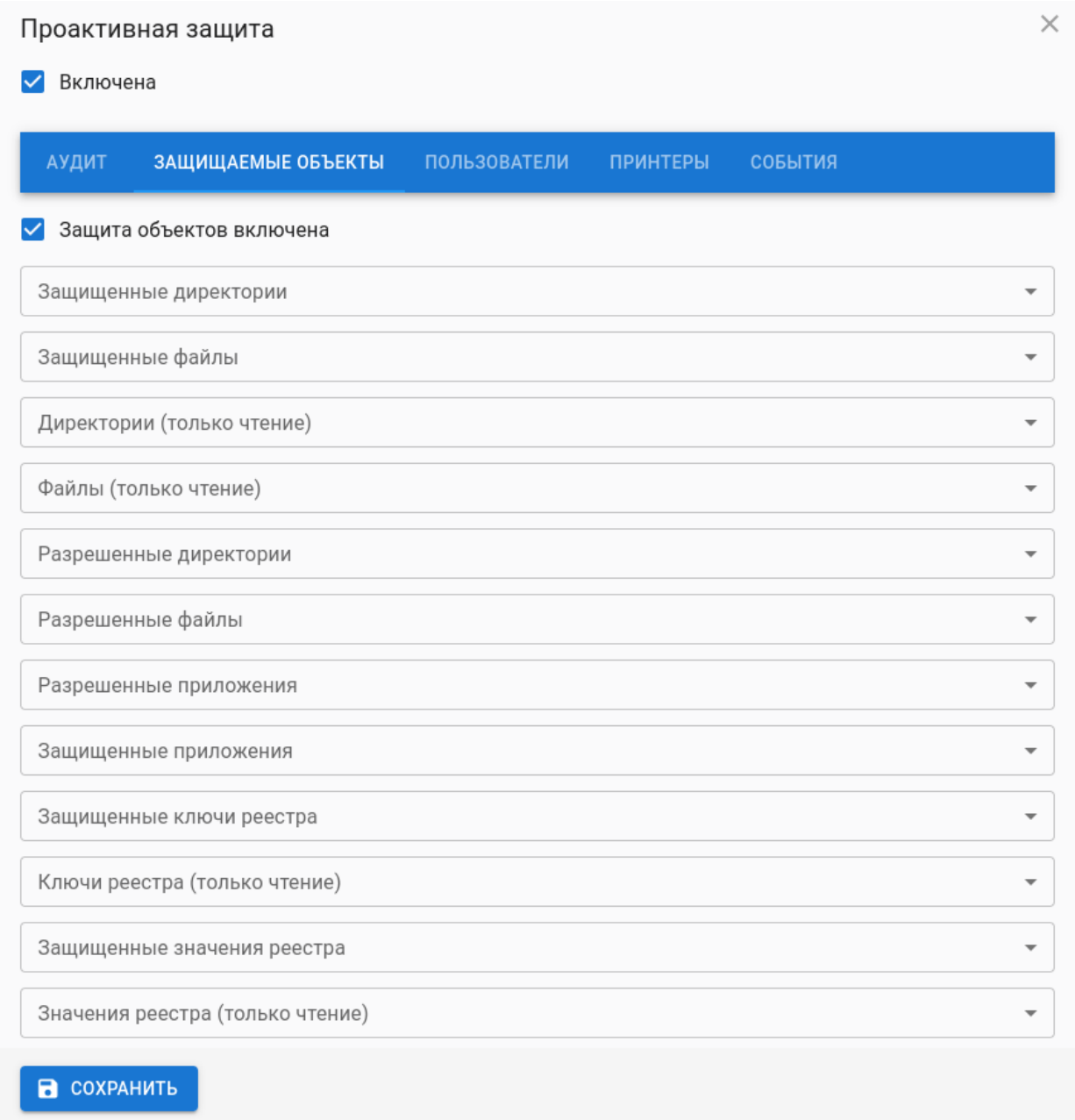


Рис. 169 – Раздел «Группы». Настройка политик.
Проактивная защита. Защищаемые объекты

Вкладка **Пользователи** (рис. 170) предоставляет настройки компонента Проактивная защита, касающиеся Пользователей.

Флажок **Фильтрация действий пользователей включена** определяет, будет ли включена фильтрация действий пользователя после выдачи этой политики на клиентское СВТ.

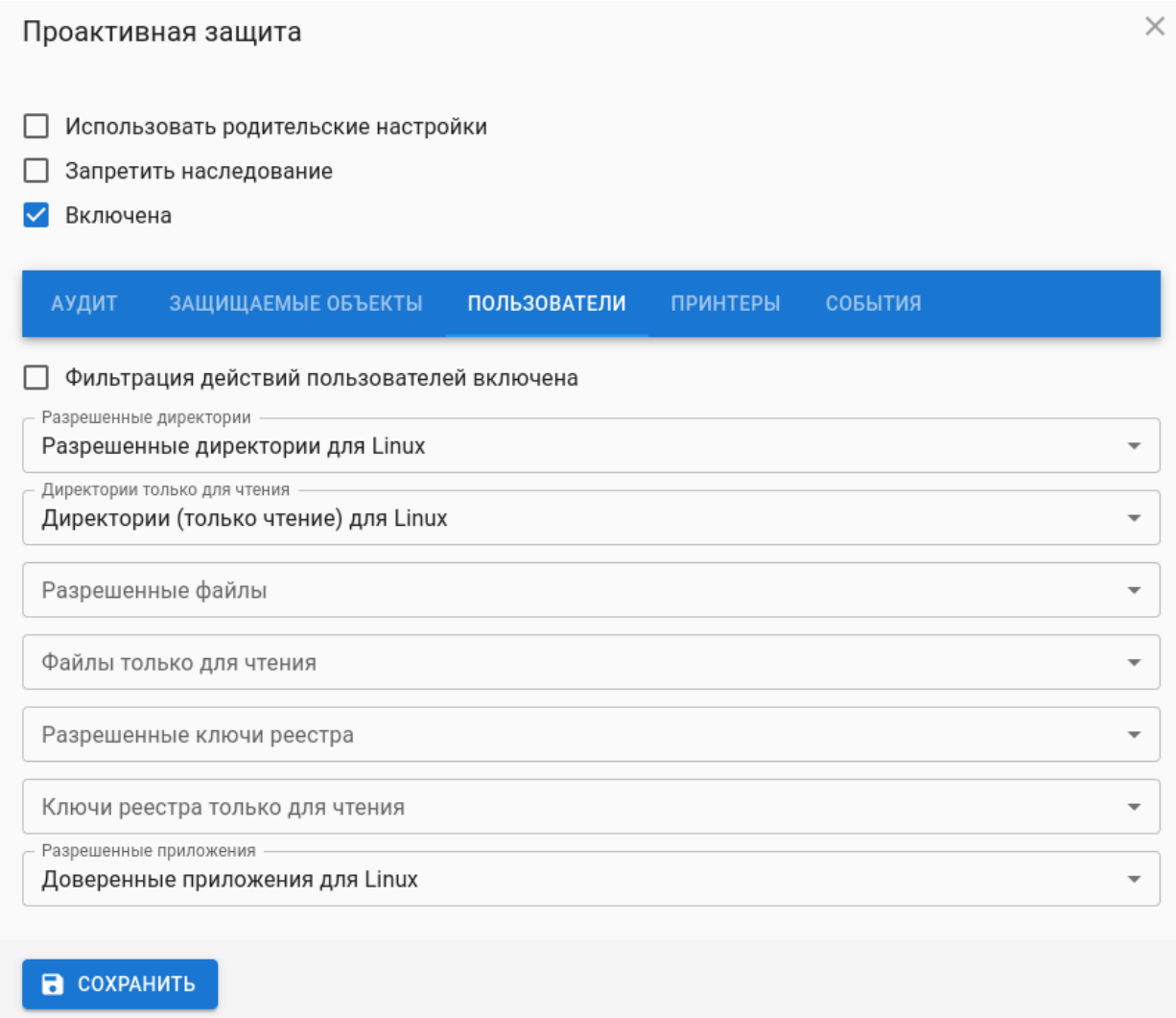


Рис. 170 – Раздел «Группы». Настройка политик.
Проактивная защита. Пользователи

На данной вкладке представлены возможные настройки действий пользователя, в каждом выпадающем списке есть возможность выбора списка объектов, которые формируется на странице Шаблоны:

1) **Разрешенные директории** – указанные в этом списке директории будут доступны пользователю. Все остальные – будут закрыты для доступа;

2) **Директории только для чтения** – указанные директории будут доступны только для чтения. Создание или модификация – запрещены;
3) **Разрешенные файлы** – перечисленные в этом списке файлы будут доступны пользователю;
4) **Файлы только для чтения** – перечисленные в этом списке файлы будут доступны пользователю только на чтение;
5) **Разрешенные ключи реестра** – ключи реестра для ОС Windows, к которым предоставляется полный доступ;
6) **Ключи реестра только для чтения** – ключи реестра для ОС Windows, доступ к которым ограничен только чтением;
7) **Доверенные приложение** – пользователю для исполнения будут разрешены только те программы, которые перечислены в этом списке. Важно учитывать, что для большинства сложных программ чаще всего требуется разрешение служебных общесистемных утилит или других исполняемых файлов, вызываемых основной программой.

Вкладка **Принтеры** (рис. 171) предоставляет настройки компонента Проактивная защита, касающиеся управления принтерами.

Флажок **Контроль принтеров** позволяет активировать контроль принтеров компонентом Проактивная защита.

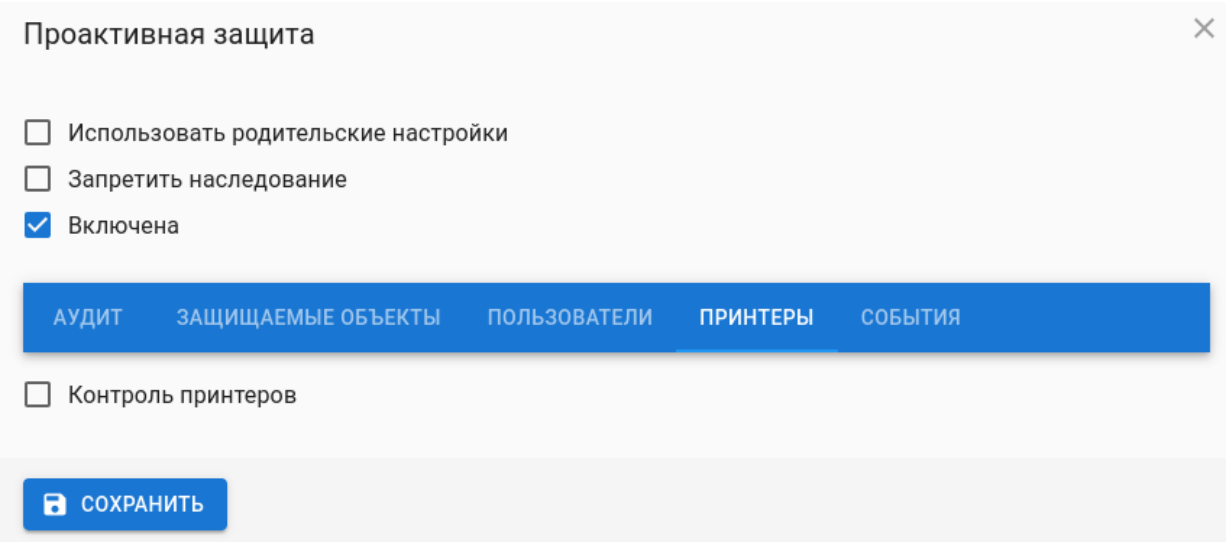


Рис. 171 – Раздел «Группы». Настройка политик.
Проактивная защита. Принтеры

Вкладка **События** (рис. 172) предоставляет настройки компонента Проактивная защита, касающиеся управления событиями: позволяет указать, какие виды событий будут сохранены в системный журнал, локальный журнал или журнал ЦУ соответственно. Снятие флажка означает, что событие не будет зарегистрировано в выбранном журнале.

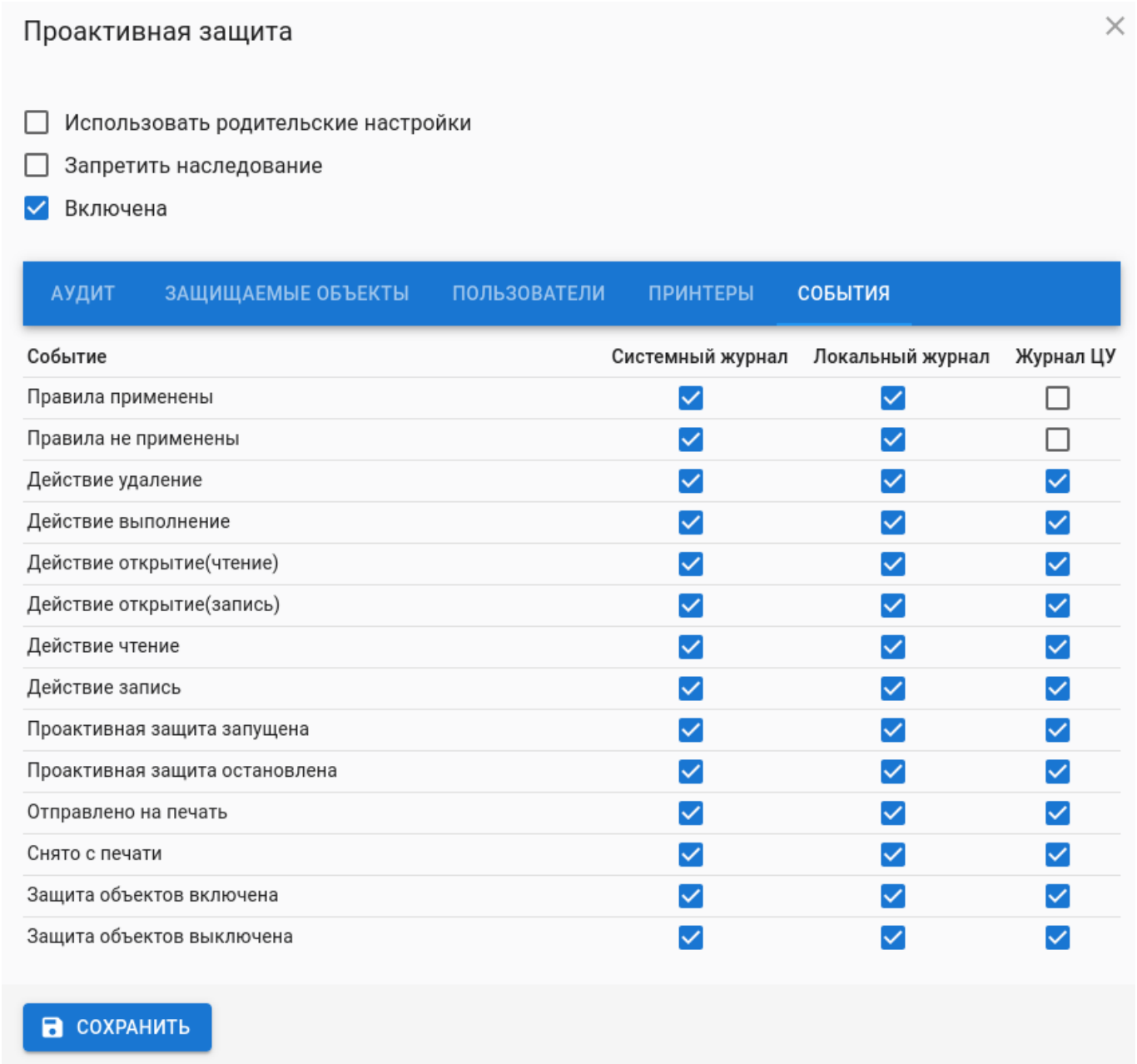


Рис. 172 – Раздел «Группы». Настройка политик.
Проактивная защита. События

4.6.4. Раздел Пользователи

Раздел «Пользователи» (рис. 173) предназначен для настройки компонента Проактивная защита модуля управления доступом, в той его части, которая соответствует управлению пользователями. Эти настройки позволяют настроить доступ к ресурсам компьютера для конкретных пользователей. Страница представляет собой список всех пользователей, которые ЦУ получает при помощи служебного пакета в автоматическом режиме.

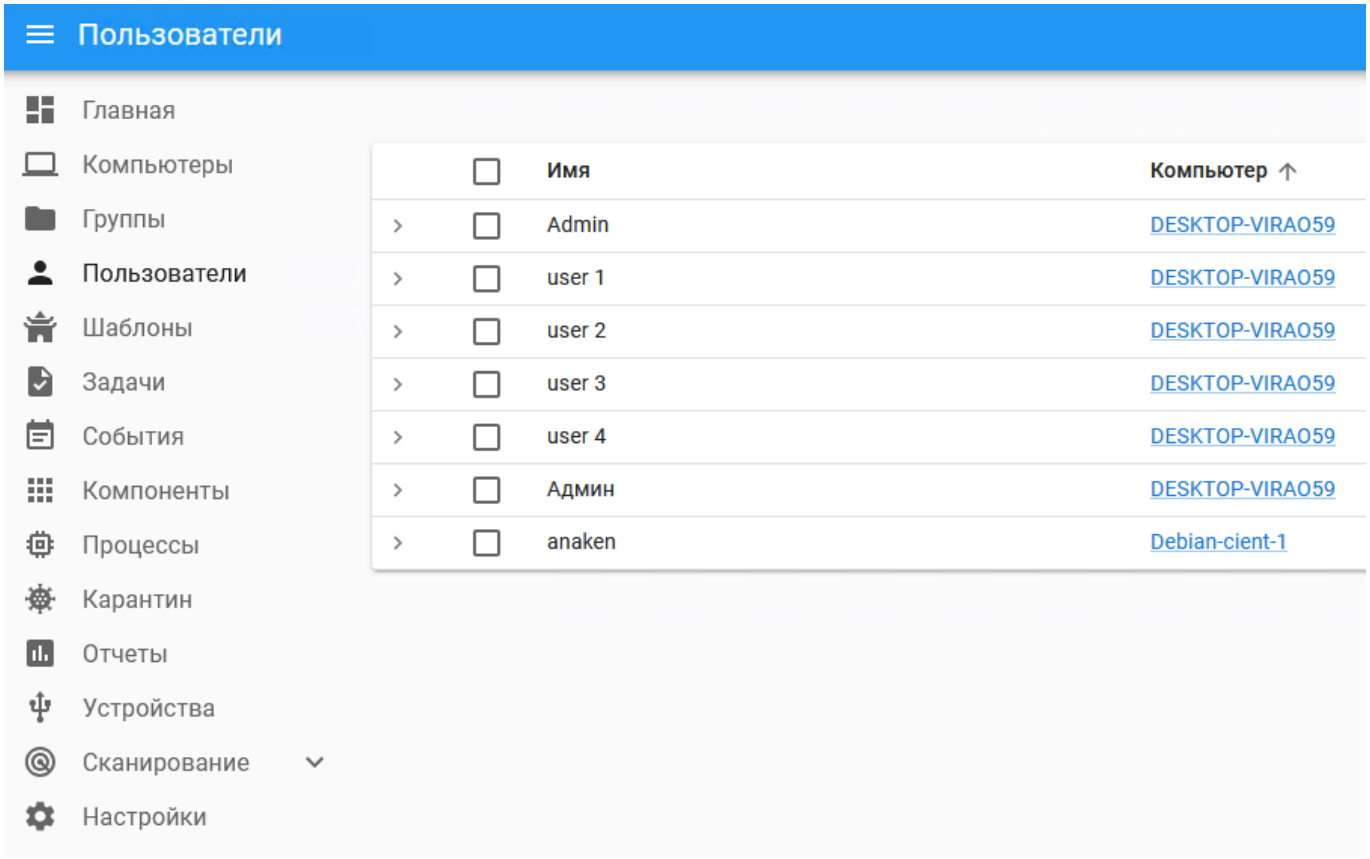


Рис. 173 – Раздел «Пользователи». Общий вид

Для успешного получения имени пользователя, его учетная запись должна быть активирована на клиентском СВТ (хотя бы один раз выполнен вход от имени этого пользователя).

В верхней правой части страница находится фильтр, с помощью которого можно осуществить выбор пользователя по заданным критериям.

Раскрыть детальные настройки для каждого пользователя (рис. 174) можно при помощи кнопок › / ⌄ .

В раскрывающейся области расположены следующие настройки, отнесенные к выбранному пользователю:

1) **Разрешенные директории** – по умолчанию существуют предустановленные директории, доступ к которым не ограничен (обусловлены типом ОС на клиентском СВТ);
2) **Директории только для чтения** – директории, доступ к которым будет ограничен для выбранного пользователя только чтением;
3) **Разрешенные файлы** – файлы, доступ к которым будет осуществляться без ограничений;
4) **Файлы только для чтения** – файлы, доступ пользователя к которым будет только для чтения;
5) **Разрешенные ключи реестра** – по умолчанию существуют предустановленные ключи реестра, позволяющие выбранному пользователю работать с ресурсами ОС (обусловлены требованиями ОС Windows);
6) **Ключи реестра только для чтения** – ключи реестра, изменение которых будет запрещено;
7) **Доверенные приложения** – по умолчанию существуют предустановленные доверенные приложения, позволяющие работать комплексу на клиентском СВТ;
8) **Разрешенные принтеры** – принтеры, которые доступны пользователю для печати.

Примечания:

1. Если очистить все настройки пункта **Разрешенные директории**, то после активации **Контроля действий пользователя**, войти в учетную запись будет невозможно.

2. Если полностью очистить все настройки пункта **Разрешенные ключи реестра**, то после активации **Контроля действий пользователя**, войти в учетную запись будет невозможно.

3. Если очистить все настройки пункта **Доверенные приложения**, то после активации **Контроля действий пользователя**, все приложения, кроме нескольких

общесистемных, окажутся заблокированными для запуска, в том числе и графический интерфейс пользователя клиентской части программного комплекса ШХУНА.

Основой для работы с этими списками являются шаблоны, настраиваемые в разделе **Шаблоны**.

Каждая опция настроек представляет собой выпадающий список, в который в автоматическом режиме встраиваются соответствующие шаблоны.

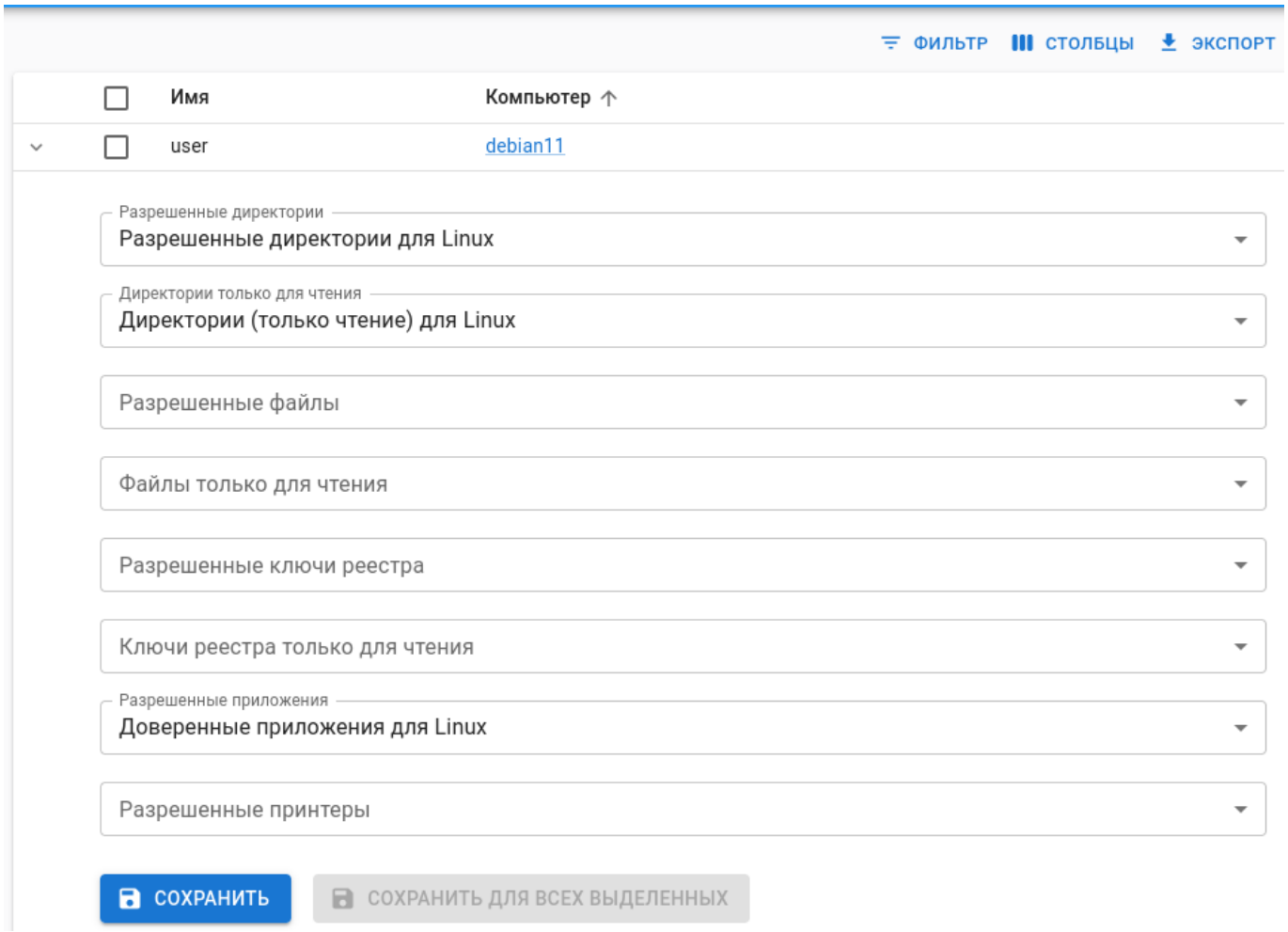


Рис. 174 – Раздел «Пользователи». Детально

4.6.5. Раздел Шаблоны

Раздел **Шаблоны** предназначен для формирования и сохранения шаблонов значений, которые могут быть использованы при создании политик (см. п. 4.6.3.1).

Примечание. Для того, чтобы СВТ могло успешно корректно функционировать, программный комплекс ШХУНА поставляет список доверенных

предустановленных в соответствующих ОС программ (рис. 175). Ознакомиться с данным списком можно выбрав ⋮ и нажав **Записи** (для ОС Windows – рис. 176, для ОС Linux – рис. 177).

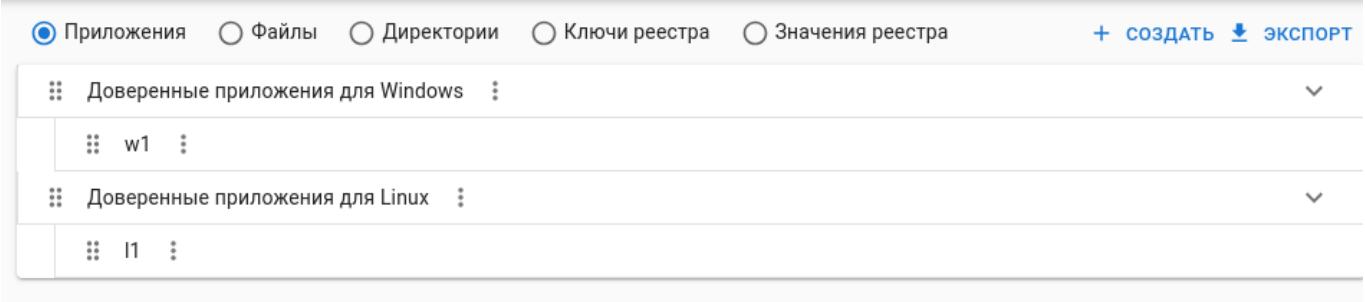


Рис. 175 – Раздел «Шаблоны». Приложения

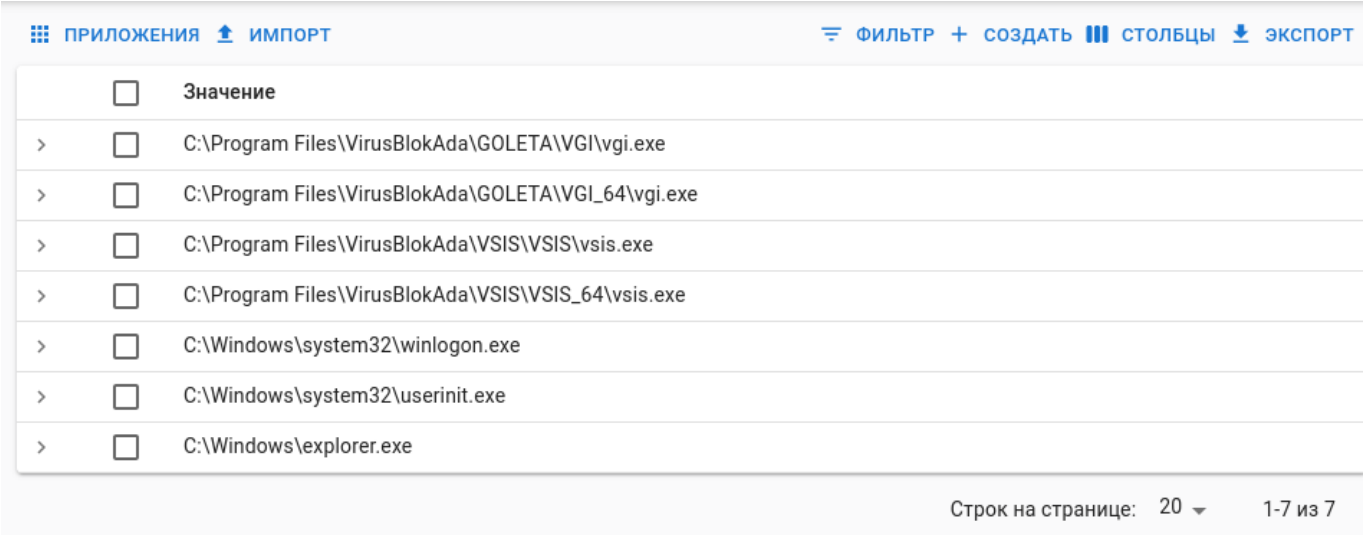


Рис. 176 – Раздел «Шаблоны». Доверенные приложения для ОС Windows

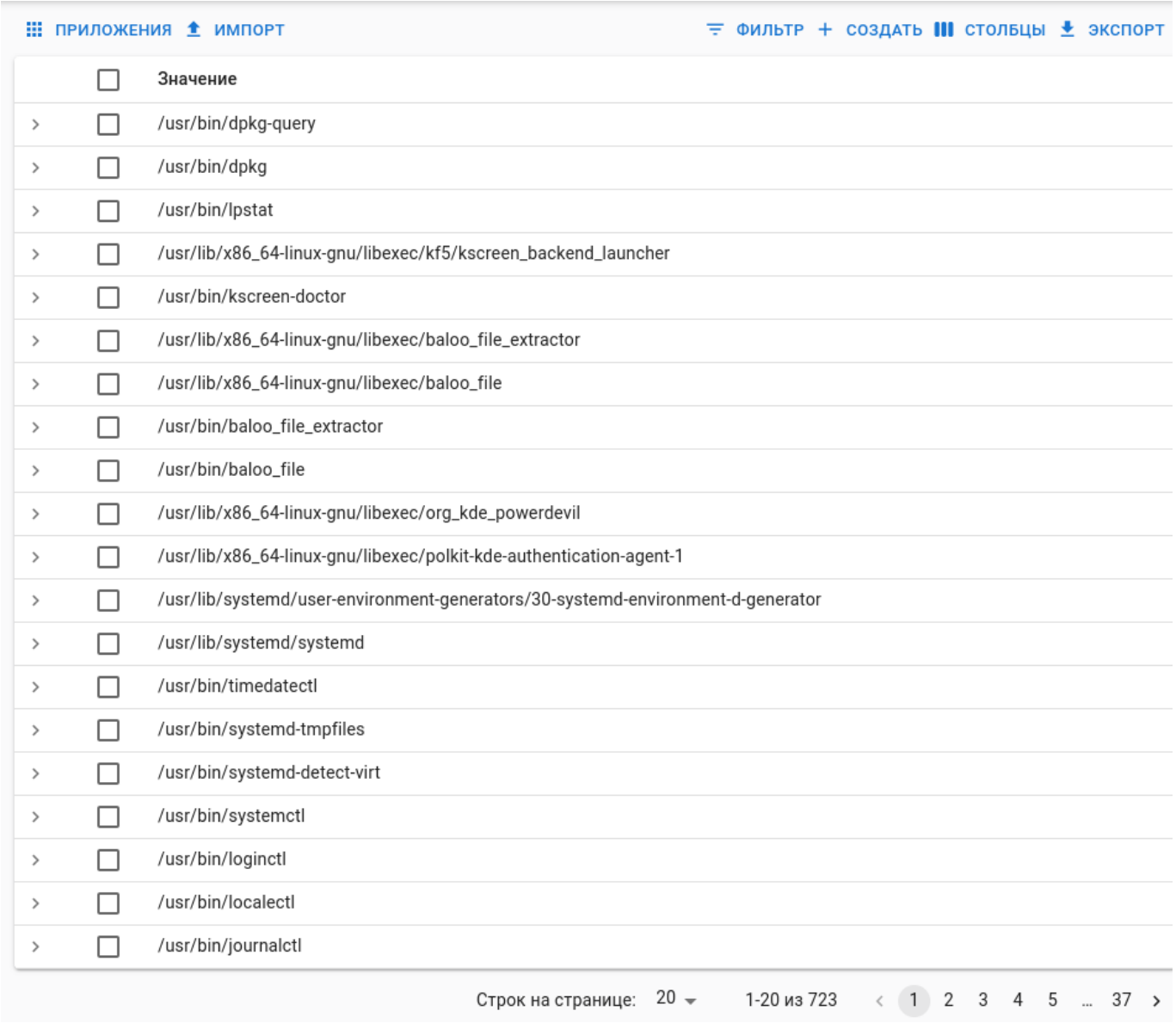


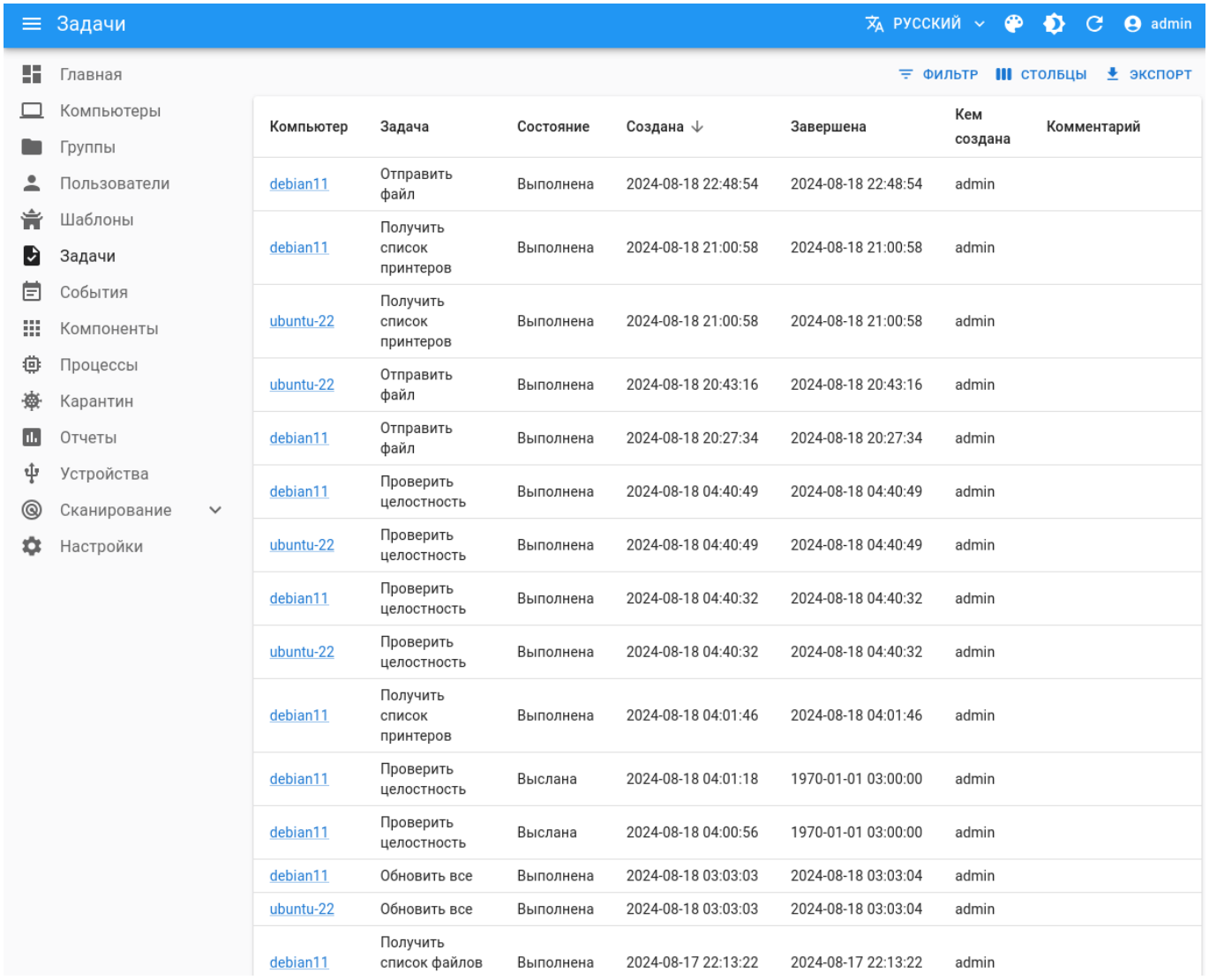
Рис. 177 – Раздел «Шаблоны». Доверенные приложения для ОС Linux

Категории значений, которые могут быть использованы для шаблонов в разделе **Шаблоны**:

1) **Приложения**;
2) **Файлы**;
3) **Директории**;
4) **Ключи реестра**;
5) **Значения реестра**.

4.6.6. Раздел Задачи

Раздел **Задачи** (рис. 178) предназначен для отображения событий хода выполнения сформированных и отправленных задач. Задачи отправляются с ЦУ на клиентские СВТ, на которых установлен программный комплекс ШХУНА.



Компьютер	Задача	Состояние	Создана	Завершена	Кем создана	Комментарий
debian11	Отправить файл	Выполнена	2024-08-18 22:48:54	2024-08-18 22:48:54	admin	
debian11	Получить список принтеров	Выполнена	2024-08-18 21:00:58	2024-08-18 21:00:58	admin	
ubuntu-22	Получить список принтеров	Выполнена	2024-08-18 21:00:58	2024-08-18 21:00:58	admin	
ubuntu-22	Отправить файл	Выполнена	2024-08-18 20:43:16	2024-08-18 20:43:16	admin	
debian11	Отправить файл	Выполнена	2024-08-18 20:27:34	2024-08-18 20:27:34	admin	
debian11	Проверить целостность	Выполнена	2024-08-18 04:40:49	2024-08-18 04:40:49	admin	
ubuntu-22	Проверить целостность	Выполнена	2024-08-18 04:40:49	2024-08-18 04:40:49	admin	
debian11	Проверить целостность	Выполнена	2024-08-18 04:40:32	2024-08-18 04:40:32	admin	
ubuntu-22	Проверить целостность	Выполнена	2024-08-18 04:40:32	2024-08-18 04:40:32	admin	
debian11	Получить список принтеров	Выполнена	2024-08-18 04:01:46	2024-08-18 04:01:46	admin	
debian11	Проверить целостность	Выслана	2024-08-18 04:01:18	1970-01-01 03:00:00	admin	
debian11	Проверить целостность	Выслана	2024-08-18 04:00:56	1970-01-01 03:00:00	admin	
debian11	Обновить все	Выполнена	2024-08-18 03:03:03	2024-08-18 03:03:04	admin	
ubuntu-22	Обновить все	Выполнена	2024-08-18 03:03:03	2024-08-18 03:03:04	admin	
debian11	Получить список файлов	Выполнена	2024-08-17 22:13:22	2024-08-17 22:13:22	admin	

Рис. 178 – Раздел «Задачи». Общий вид

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

Перечень столбцов данных:

1) **Компьютер** – имя компьютера;

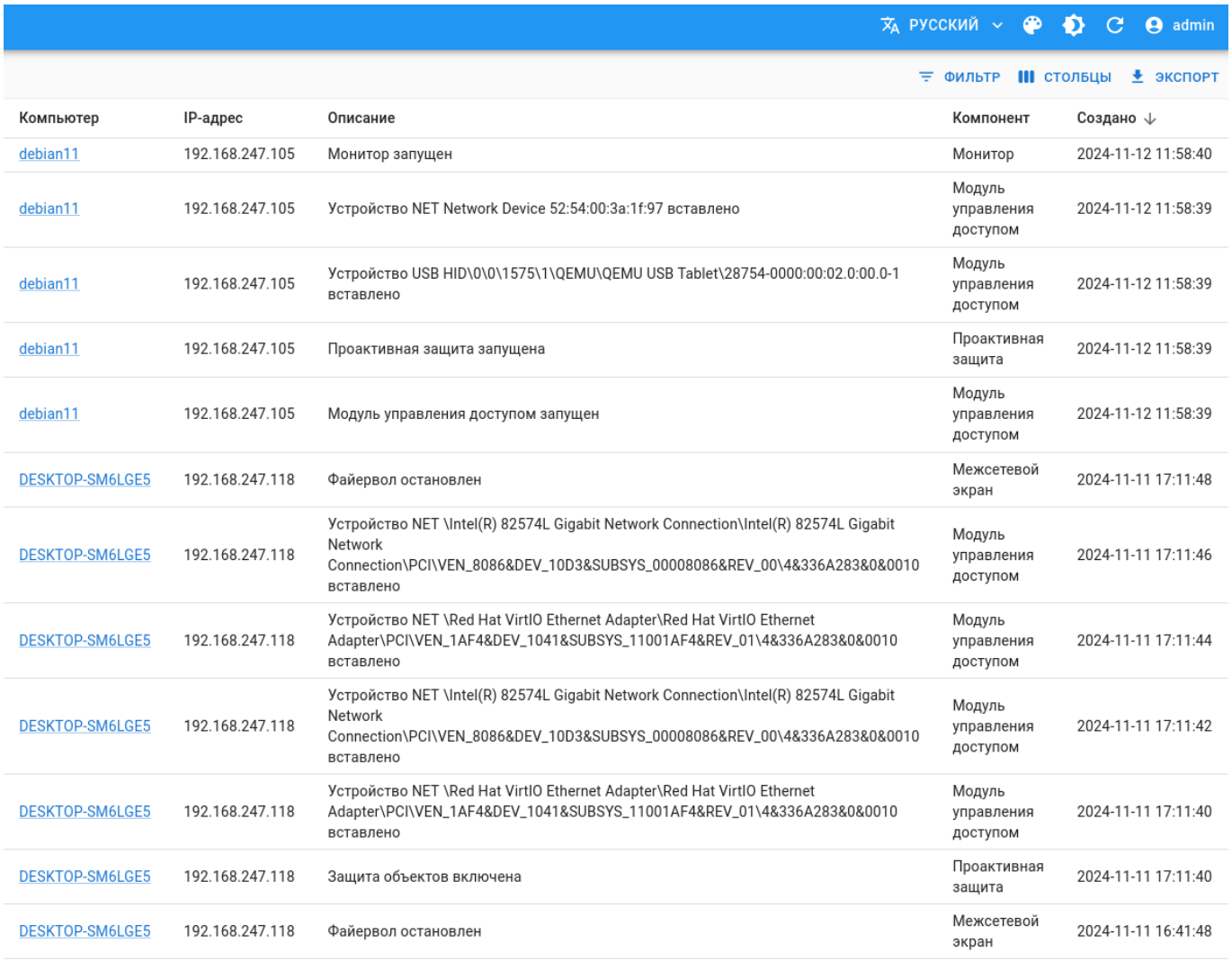
2) **Задача** – имя задачи, которая была отправлена из раздела **Компьютеры** (см. п. 4.6.2.2);
3) **Состояние** – состояние задачи на момент просмотра события;
4) **Создана** – дата и время создания (формирования задачи) вместе с отправкой;
5) **Завершена** – дата и время завершения задачи (успешного или неуспешного – в зависимости от состояния задачи);
6) **Кем создана** – имя пользователя ЦУ, сформировавшего и отправившего задачу клиентскому СВТ;
7) **Комментарий** – любая дополнительная информация, доступная к просмотру.

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера) можно получить детальную информацию о задаче. Конкретная информация отличается в зависимости от типа задачи (см. п. 4.6.2.2).

4.6.7. Раздел События

Раздел **События** (рис. 179) предназначен для отображения событий, в том числе событий аудита, поступающих от подключенных к данному ЦУ клиентских СВТ. События отправляются на ЦУ от клиентских СВТ, на которых установлен программный комплекс ШХУНА.



Компьютер	IP-адрес	Описание	Компонент	Создано
debian11	192.168.247.105	Монитор запущен	Монитор	2024-11-12 11:58:40
debian11	192.168.247.105	Устройство NET Network Device 52:54:00:3a:1f:97 вставлено	Модуль управления доступом	2024-11-12 11:58:39
debian11	192.168.247.105	Устройство USB HID\0\0\1575\1\QEMU\QEMU USB Tablet\28754-0000:00:02.0:00.0-1 вставлено	Модуль управления доступом	2024-11-12 11:58:39
debian11	192.168.247.105	Проактивная защита запущена	Проактивная защита	2024-11-12 11:58:39
debian11	192.168.247.105	Модуль управления доступом запущен	Модуль управления доступом	2024-11-12 11:58:39
DESKTOP-SM6LGE5	192.168.247.118	Файервол остановлен	Межсетевой экран	2024-11-11 17:11:48
DESKTOP-SM6LGE5	192.168.247.118	Устройство NET \Intel(R) 82574L Gigabit Network Connection\Intel(R) 82574L Gigabit Network Connection\PCI\VEN_8086&DEV_10D3&SUBSYS_00008086&REV_00\4&336A283&0&0010 вставлено	Модуль управления доступом	2024-11-11 17:11:46
DESKTOP-SM6LGE5	192.168.247.118	Устройство NET \Red Hat VirtIO Ethernet Adapter\Red Hat VirtIO Ethernet Adapter\PCI\VEN_1AF4&DEV_1041&SUBSYS_11001AF4&REV_01\4&336A283&0&0010 вставлено	Модуль управления доступом	2024-11-11 17:11:44
DESKTOP-SM6LGE5	192.168.247.118	Устройство NET \Intel(R) 82574L Gigabit Network Connection\Intel(R) 82574L Gigabit Network Connection\PCI\VEN_8086&DEV_10D3&SUBSYS_00008086&REV_00\4&336A283&0&0010 вставлено	Модуль управления доступом	2024-11-11 17:11:42
DESKTOP-SM6LGE5	192.168.247.118	Устройство NET \Red Hat VirtIO Ethernet Adapter\Red Hat VirtIO Ethernet Adapter\PCI\VEN_1AF4&DEV_1041&SUBSYS_11001AF4&REV_01\4&336A283&0&0010 вставлено	Модуль управления доступом	2024-11-11 17:11:40
DESKTOP-SM6LGE5	192.168.247.118	Защита объектов включена	Проактивная защита	2024-11-11 17:11:40
DESKTOP-SM6LGE5	192.168.247.118	Файервол остановлен	Межсетевой экран	2024-11-11 16:41:48

Рис. 179 – Раздел «События». Общий вид

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

Перечень столбцов данных:

1) **Компьютер** – имя компьютера;
2) **IP-адрес** – IPv4 или IPv6 адрес, соответствующий компьютеру, с которого пришло событие;
3) **Описание** – тип, категория или любые другие данные, описывающие событие;

4) **Компонент** – имя компонента программного комплекса ШХУНА, от которого пришло событие;
5) **Создано** – дата и время возникновения события на клиентском СВТ.

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию о событии. Конкретная информация отличается в зависимости от типа события.

4.6.8. Раздел Компоненты

Раздел **Компоненты** (рис. 180) предназначен для отображения состояния компонентов программного комплекса ШХУНА на клиентских СВТ, подключенных к данному ЦУ. Информация о компонентах отправляется на ЦУ от клиентских СВТ, на которых установлен программный комплекс ШХУНА.

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

Перечень столбцов данных:

1) **Компьютер** – имя компьютера;
2) **Компонент** – наименование компонента программного комплекса ШХУНА;
3) **Состояние** – состояние компонента на компьютере, подключенном к ЦУ (Запущен, Остановлен, Установлен).

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию о компоненте.

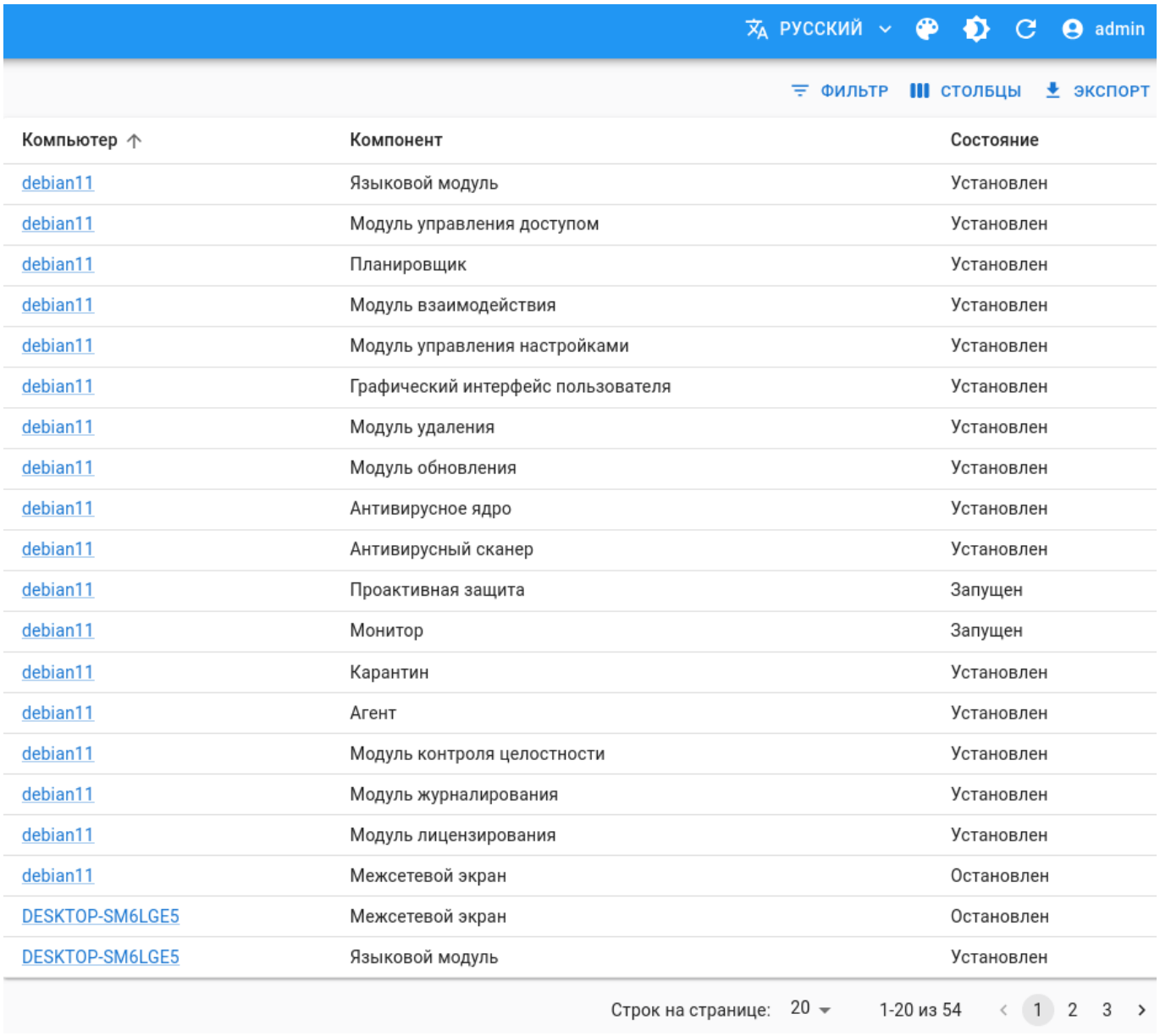


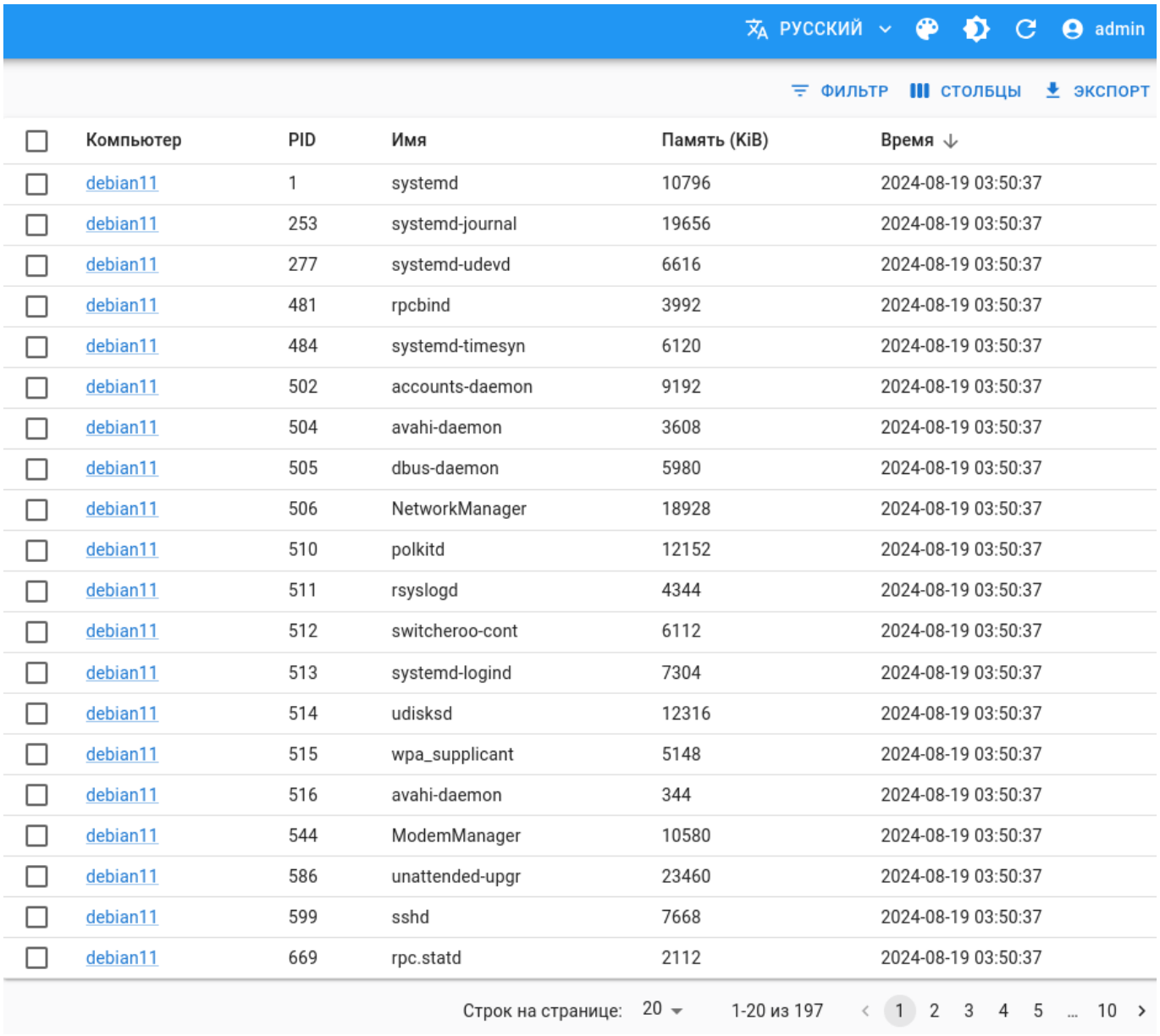
Рис. 180 – Раздел «Компоненты». Общий вид

4.6.9. Раздел Процессы

Раздел **Процессы** (рис. 181) предназначен для отображения программных процессов в ОС на клиентских СВТ, подключенных к данному ЦУ. Информация о процессах отправляется с клиентских СВТ, на которых установлен программный комплекс ШХУНА, на ЦУ.

Аналогично остальным разделам графического интерфейса ЦУ данные здесь

отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.



Компьютер	PID	Имя	Память (KiB)	Время
debian11	1	systemd	10796	2024-08-19 03:50:37
debian11	253	systemd-journal	19656	2024-08-19 03:50:37
debian11	277	systemd-udevd	6616	2024-08-19 03:50:37
debian11	481	rpcbind	3992	2024-08-19 03:50:37
debian11	484	systemd-timesyn	6120	2024-08-19 03:50:37
debian11	502	accounts-daemon	9192	2024-08-19 03:50:37
debian11	504	avahi-daemon	3608	2024-08-19 03:50:37
debian11	505	dbus-daemon	5980	2024-08-19 03:50:37
debian11	506	NetworkManager	18928	2024-08-19 03:50:37
debian11	510	polkitd	12152	2024-08-19 03:50:37
debian11	511	rsyslogd	4344	2024-08-19 03:50:37
debian11	512	switcheroo-cont	6112	2024-08-19 03:50:37
debian11	513	systemd-logind	7304	2024-08-19 03:50:37
debian11	514	udisksd	12316	2024-08-19 03:50:37
debian11	515	wpa_supplicant	5148	2024-08-19 03:50:37
debian11	516	avahi-daemon	344	2024-08-19 03:50:37
debian11	544	ModemManager	10580	2024-08-19 03:50:37
debian11	586	unattended-upgr	23460	2024-08-19 03:50:37
debian11	599	sshd	7668	2024-08-19 03:50:37
debian11	669	rpc.statd	2112	2024-08-19 03:50:37

Рис. 181 – Раздел «Процессы». Общий вид

Перечень столбцов данных:

1) **Компьютер** – имя компьютера;
2) **PID** – численный идентификатор процесса (является натуральным числом, уникальный на выбранном компьютере);
3) **Имя** – текстовый идентификатор процесса (не является уникальным для выбранного компьютера);

4) **Память (KiB)** – использование ОЗУ данным процессом (величина в кибибайтах);
5) **Время** – дата и время полученных данных.

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию о процессе, а также завершить его (kill process) с помощью нажатия на кнопку **Завершить** (рис. 182).

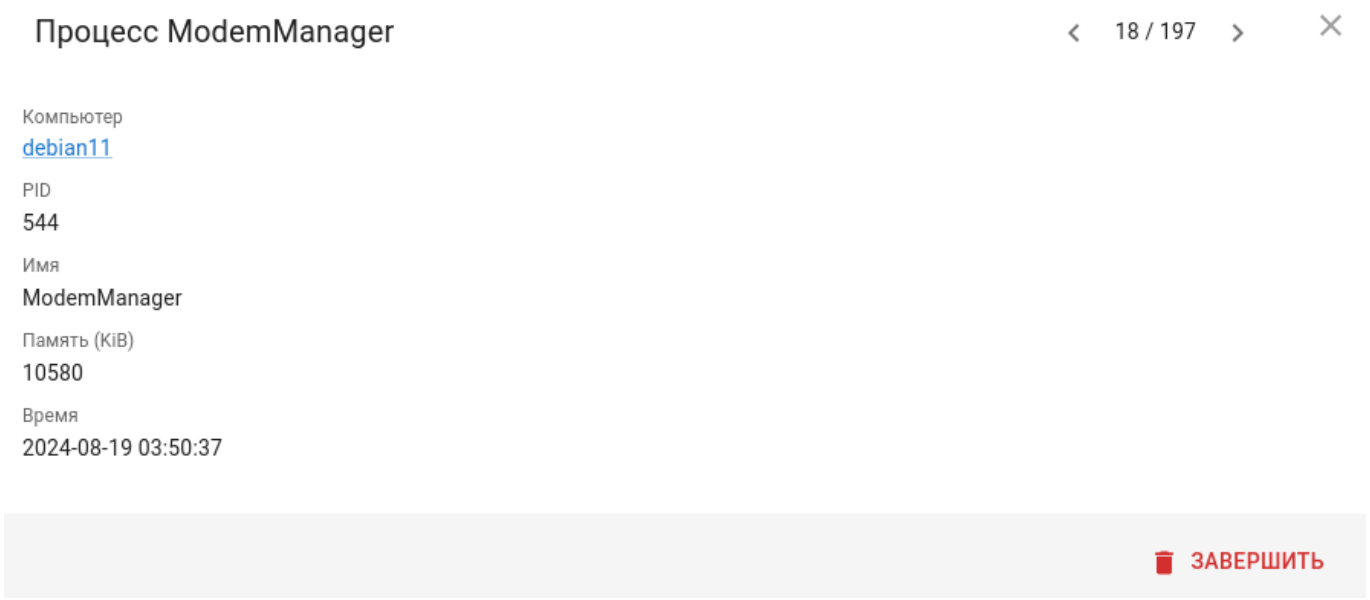


Рис. 182 – Раздел «Процессы». Завершить процесс

4.6.10. Раздел Карантин

Раздел **Карантин** (рис. 183) предназначен для отображения состояния файлов из карантина, которые были получены от подключенных к данному ЦУ клиентских СВТ.

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

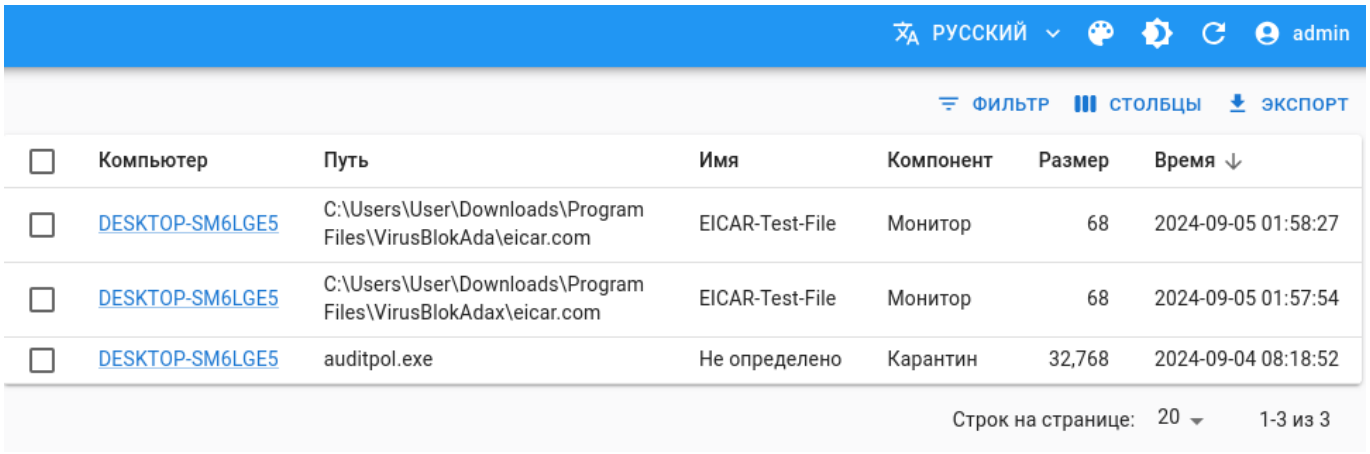


Рис. 183 – Раздел «Карантин». Общий вид

Перечень столбцов данных:

1) **Компьютер** – имя клиентского СВТ;
2) **Путь** – полный путь к файлу на клиентском СВТ;
3) **Имя** – наименование объекта карантина (если файл инфицирован – имя ВПО);
4) **Компонент** – имя компонента программного комплекса ШХУНА, из которого файл был отправлен в карантин;
5) **Размер** – размер файла (например, в байтах);
6) **Время** – дата и время отправки файла в карантин.

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию об объекте карантина, а также скачать и восстановить его, в том числе указав иной путь восстановления (рис. 184, кнопки **Скачать**, **Восстановить**, **Восстановить в** соответственно).

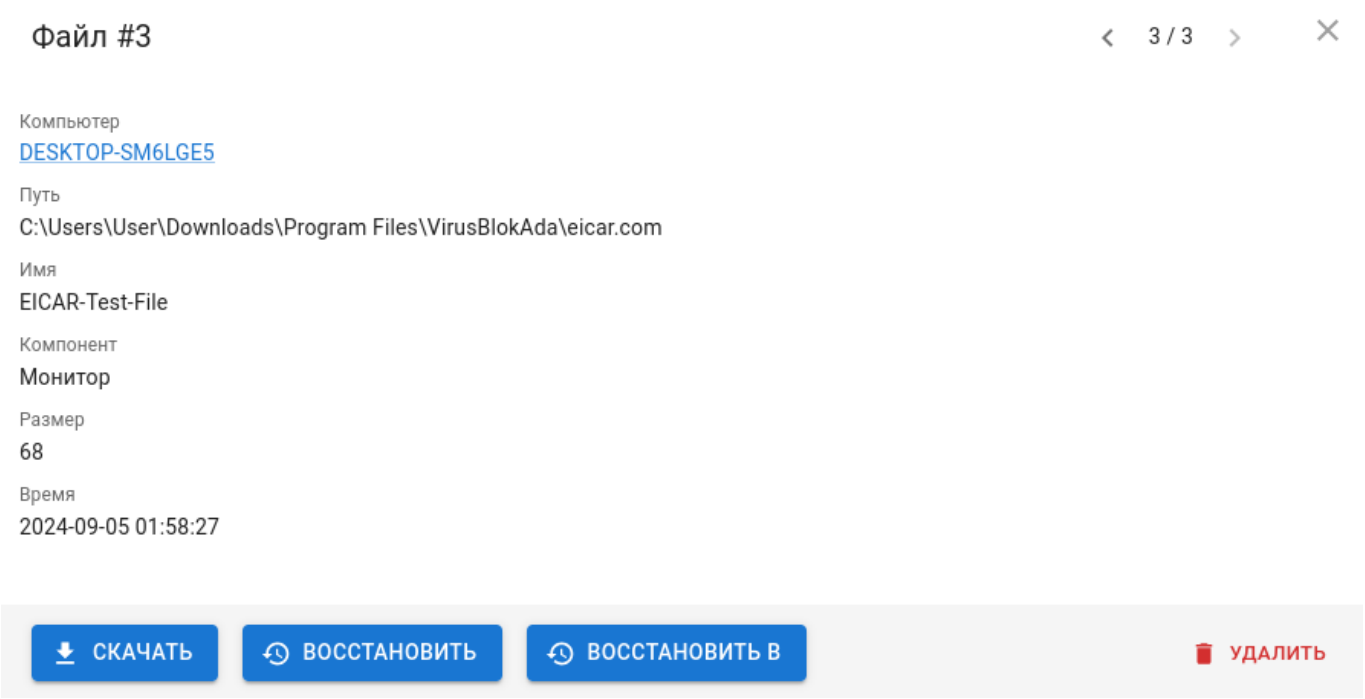


Рис. 184 – Раздел «Карантин». Операции над файлом из карантина

4.6.11. Раздел Отчеты

Раздел **Отчеты** (рис. 185) предназначен для отображения перечня файлов отчета, которые были получены от подключенных к данному ЦУ клиентских СВТ (см. задачу «Запросить файлы отчета», п. 4.6.2.6).

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

Перечень столбцов данных:

1) **Компьютер** – имя клиентского СВТ, которому соответствует отчет;
2) **Имя** – имя файла отчета (.zip-архива);
3) **Размер** – размер занимаемого отчетом места на диске (величина в байтах);
4) **Время** – дата и время полученных данных.

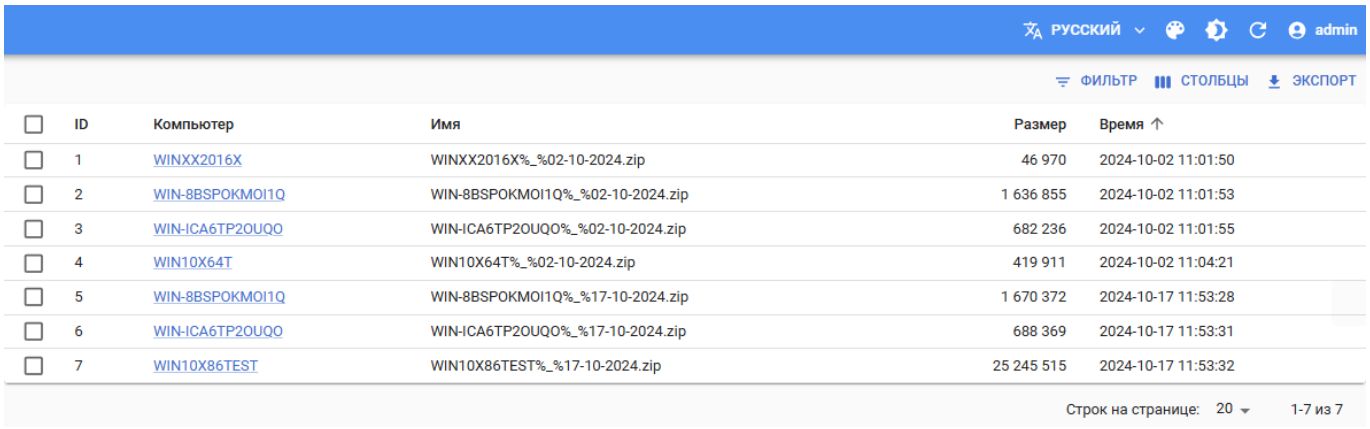


Рис. 185 – Раздел «Отчеты». Общий вид

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

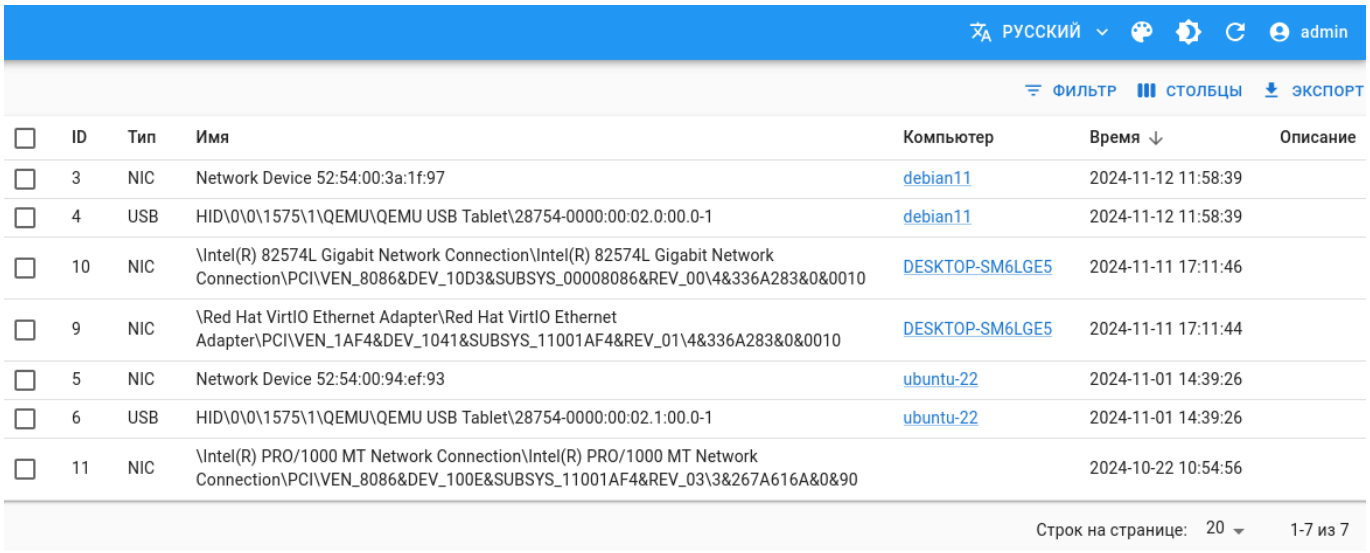
По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию об отчете, а также скачать его или удалить (рис. 186, кнопки **Скачать** и **Удалить** соответственно).

Рис. 186 – Раздел «Отчеты». Операции над файлом отчета

4.6.12. Раздел Устройства

Раздел **Устройства** (рис. 187) предназначен для отображения перечня

сетевых (NIC) и USB-устройств, которые были получены от подключенных к данному ЦУ клиентских СВТ, а также для управления этими устройствами.



	ID	Тип	Имя	Компьютер	Время	Описание
☐	3	NIC	Network Device 52:54:00:3a:1f:97	debian11	2024-11-12 11:58:39	
☐	4	USB	HID\0\0\1575\1\QEMU\QEMU USB Tablet\28754-0000:00:02.0:00.0-1	debian11	2024-11-12 11:58:39	
☐	10	NIC	\Intel(R) 82574L Gigabit Network Connection\Intel(R) 82574L Gigabit Network Connection\PCI\VEN_8086&DEV_10D3&SUBSYS_00008086&REV_00\4&336A283&0&0010	DESKTOP-SM6LGE5	2024-11-11 17:11:46	
☐	9	NIC	\Red Hat VirtIO Ethernet Adapter\Red Hat VirtIO Ethernet Adapter\PCI\VEN_1AF4&DEV_1041&SUBSYS_11001AF4&REV_01\4&336A283&0&0010	DESKTOP-SM6LGE5	2024-11-11 17:11:44	
☐	5	NIC	Network Device 52:54:00:94:ef:93	ubuntu-22	2024-11-01 14:39:26	
☐	6	USB	HID\0\0\1575\1\QEMU\QEMU USB Tablet\28754-0000:00:02.1:00.0-1	ubuntu-22	2024-11-01 14:39:26	
☐	11	NIC	\Intel(R) PRO/1000 MT Network Connection\Intel(R) PRO/1000 MT Network Connection\PCI\VEN_8086&DEV_100E&SUBSYS_11001AF4&REV_03\3&267A616A&0&90		2024-10-22 10:54:56	

Строк на странице: 20 1-7 из 7

Рис. 187 – Раздел «Устройства». Общий вид

Аналогично остальным разделам графического интерфейса ЦУ данные здесь отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать. Также доступен экспорт всех записей в `.csv`-формате.

Перечень столбцов данных:

1) **ID** – внутренний идентификатор устройства, используемый ЦУ;
2) **Тип** – тип устройства (USB, NIC);
3) **Имя** – текстовый идентификатор, содержащий детальную информацию об устройстве (в зависимости от его типа и предоставляемых ОС данных);
4) **Компьютер** – имя клиентского СВТ, которому соответствует устройство;
5) **Время** – дата и время полученных данных;
6) **Описание** – любые иные текстовые данные, которые могут описывать устройство (произвольная информация, которая может быть добавлена Администратором ЦУ для дополнительной идентификации устройства).

По нажатию ЛКМ на элементе с именем компьютера, можно получить детальную информацию о нем (как и в разделе **Компьютеры**).

По нажатию ЛКМ на любом другом элементе (кроме имени компьютера), можно получить детальную информацию об управлении данным устройством (рис. 188).

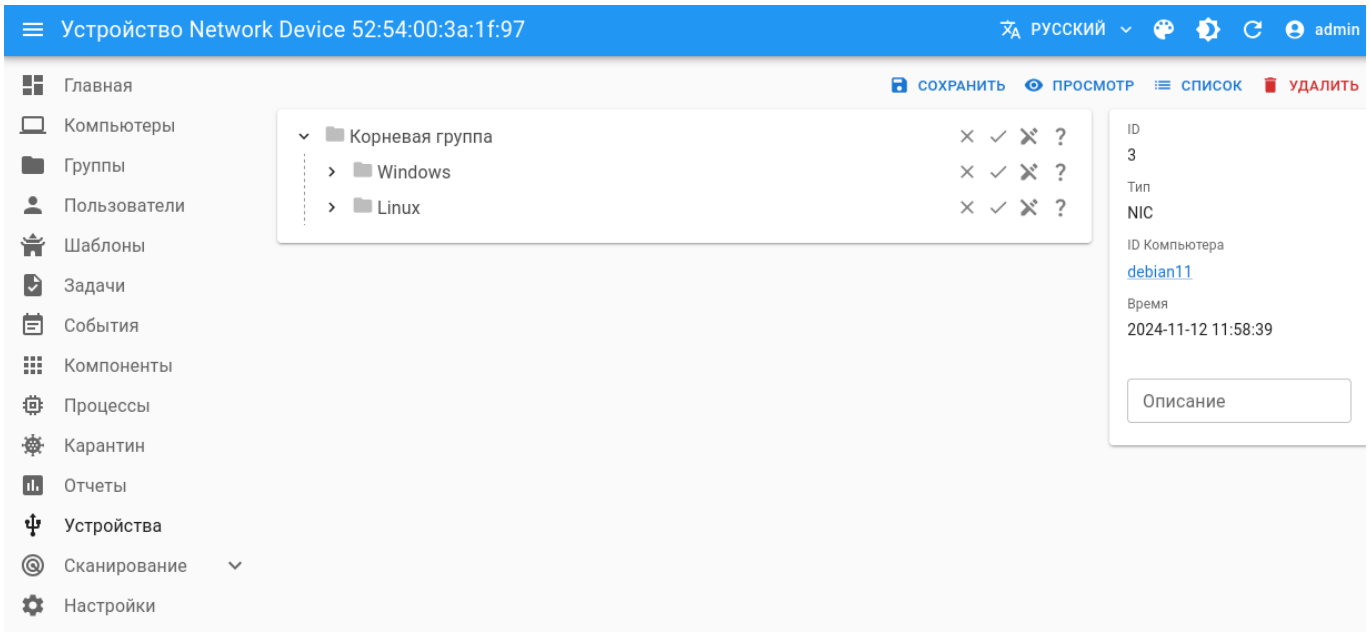


Рис. 188 – Раздел «Устройства».
Управление NIC или USB устройством

В верхней правой части формы находятся кнопки **Сохранить**, **Просмотр**, **Список**, **Удалить**.

В правой части формы находится группа, описывающая соответствующие поля устройства, там же есть возможность задать/изменить поле **Описание**.

В основной (центральной) части формы отображается дерево групп компьютеров, зарегистрированных в ЦУ (рис. 189).

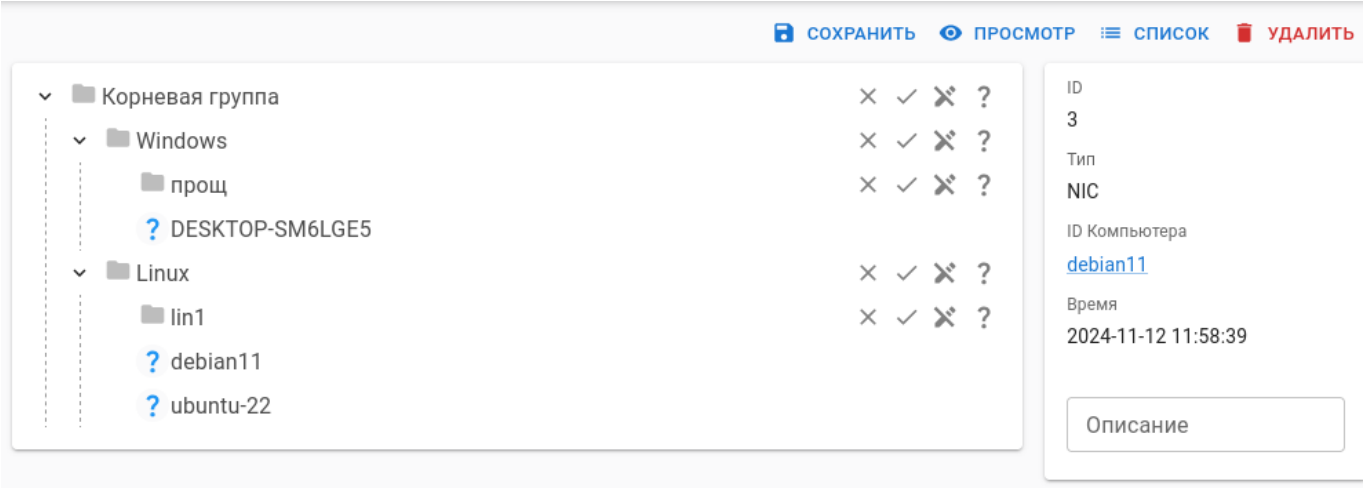


Рис. 189 – Раздел «Устройства».
Дерево групп компьютеров

В поле **Описание** можно добавить служебную информацию для текущего устройства. Например, внести фамилию пользователя, за которым закреплен USB-накопитель или его инвентарный номер.

Определить действия над выбранным устройством можно, как индивидуально для компьютера, так и для группы компьютеров, или для всех групп в целом.

Каждое устройство может находиться в следующих состояниях:

1) **По умолчанию** – требуется решение Администратора для выбора действия над указанным устройством. Для USB-носителей также будет применена Политика Группы для действий над неизвестными устройствами (настройки **Управление устройствами: Правило по умолчанию для USB Mass Storage устройств**) (иконка ?);
2) **Разрешено** (Пропустить) – устройство будет разрешено к использованию без ограничений (иконка ✓);
3) **Запрещено** (Блокировать) – устройство будет запрещено к использованию (иконка ✕);
4) **Блокировать запись** (Запретить запись) – устройство будет запрещено к записи, но разрешено к чтению (иконка 🔧).

Для сохранения изменений, совершенных на странице, необходимо нажать кнопку **Сохранить**.

4.6.13. Раздел Сканирование

Раздел **Сканирование** (рис. 190) предназначен для сканирования сети в целях обнаружения компьютеров сети, на которых можно осуществить удаленную установку клиентской части программного комплекса ШХУНА (подготовительные процедуры описаны в п. 4.1 Подготовка к установке).

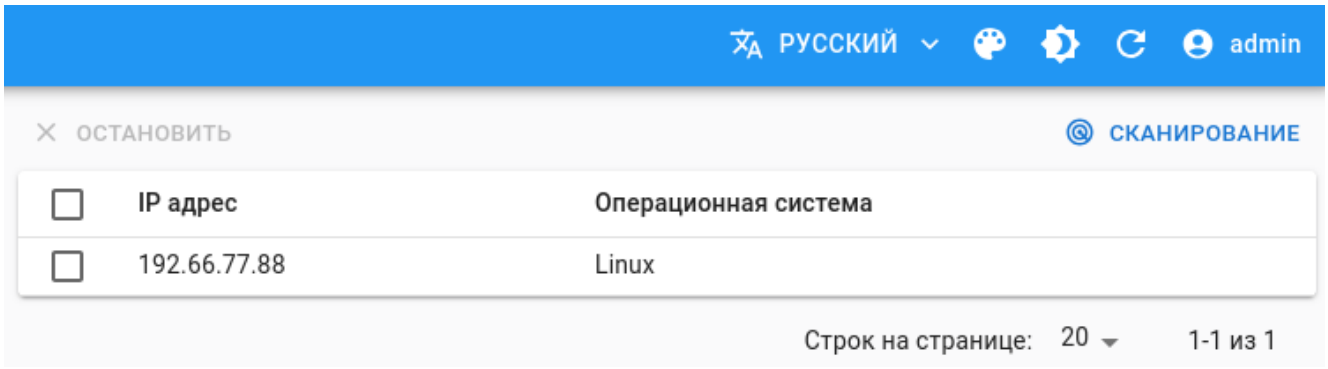


Рис. 190 – Раздел «Сканирование». Общий вид

По нажатию на кнопку **Сканирование** будет открыта форма **Начать сканирование** (рис. 191), в которой указывается участок сети, где будет производиться поиск компьютеров для установки клиентской части программного комплекса ШХУНА (начало и конец промежутка сканирования – с адреса А по адрес Б; в виде валидного IPv4 или IPv6 адреса). По нажатию на кнопку **Сканировать** формы **Начать сканирование** начнется непосредственный поиск компьютеров в указанном участке сети. Для его завершения необходимо нажать кнопку **Остановить** (преждевременная остановка поиска) или дождаться завершения сканирования.

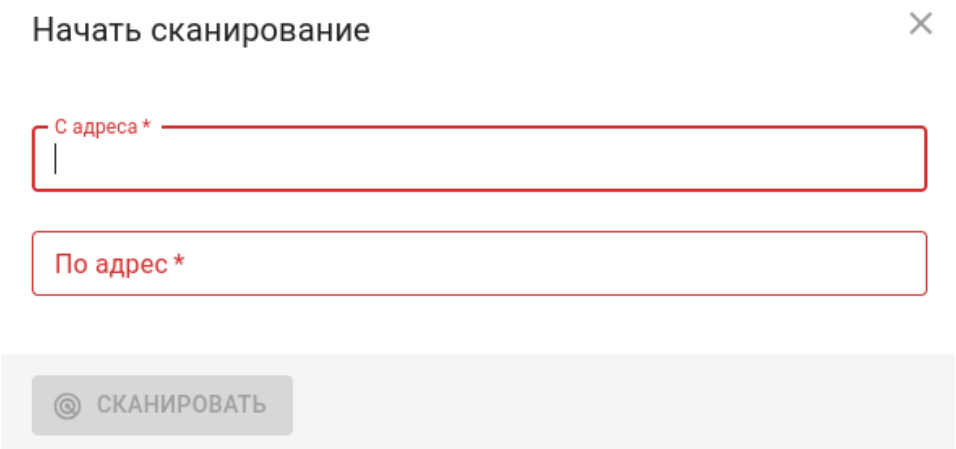


Рис. 191 – Раздел «Сканирование». Начать сканирование

Результаты сканирования отображаются в табличном виде (аналогично остальным разделам графического интерфейса ЦУ).

Перечень столбцов данных:

1) **IP адрес** – валидный IPv4 или IPv6 адрес компьютера, обнаруженного в заданном участке сети;
2) **Операционная система** – найденная ОС на клиентском СВТ.

Для выбора компьютеров используется левая колонка таблицы. Выбранные компьютеры отмечены флажком ☑ (рис. 192). Если компьютер удовлетворяет требованиям предварительной подготовки, то на него можно установить клиентскую часть программного комплекса ШХУНА. Для этого нажмите кнопку **Установить**. В результате откроется форма **Установка** (см. рис. 193), где необходимо указать данные авторизации для суперпользователя или локального администратора, уполномоченного проводить установку ПО на клиентских СВТ.

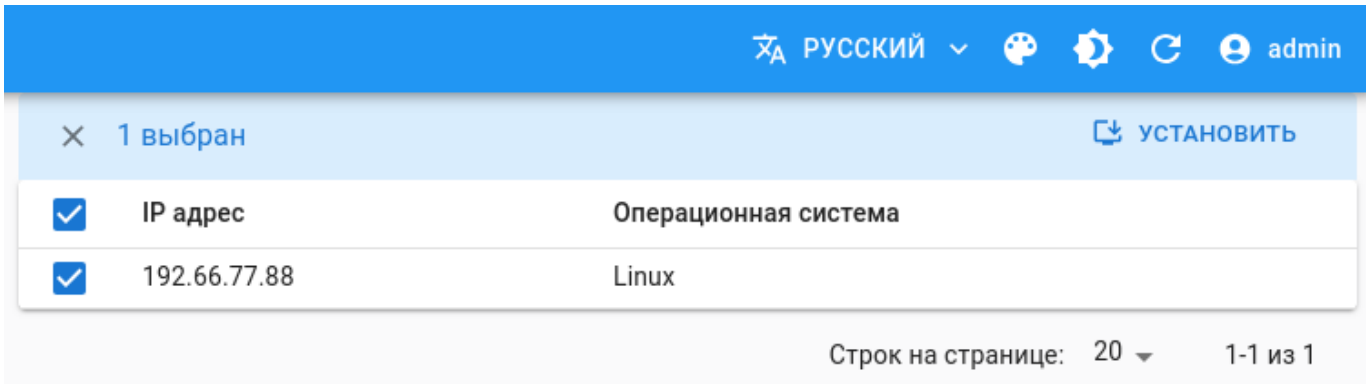


Рис. 192 – Установка клиентской части программного комплекса ШХУНА на выбранное СВТ

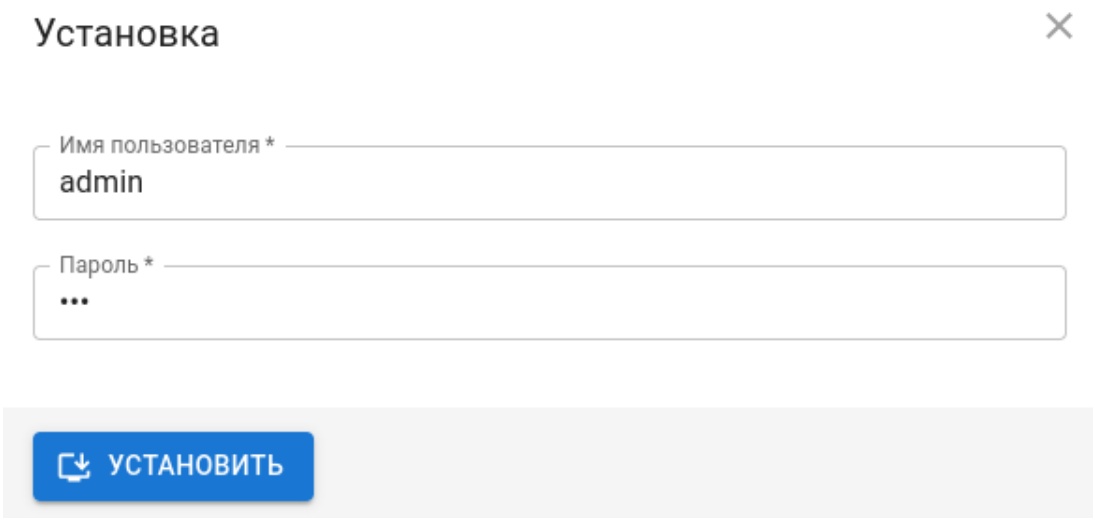


Рис. 193 – Установка клиентской части программного комплекса ШХУНА на выбранное СВТ

Данные авторизации администратора установки

4.6.13.1. Подраздел Установки

Результаты и ход установки (которая была инициирована в разделе **Сканирование**) можно отследить в подразделе **Установки** (см. рис. 194). Аналогично остальным разделам графического интерфейса ЦУ данные отображаются в табличном виде. Эти данные можно фильтровать, столбцы данных – скрывать.

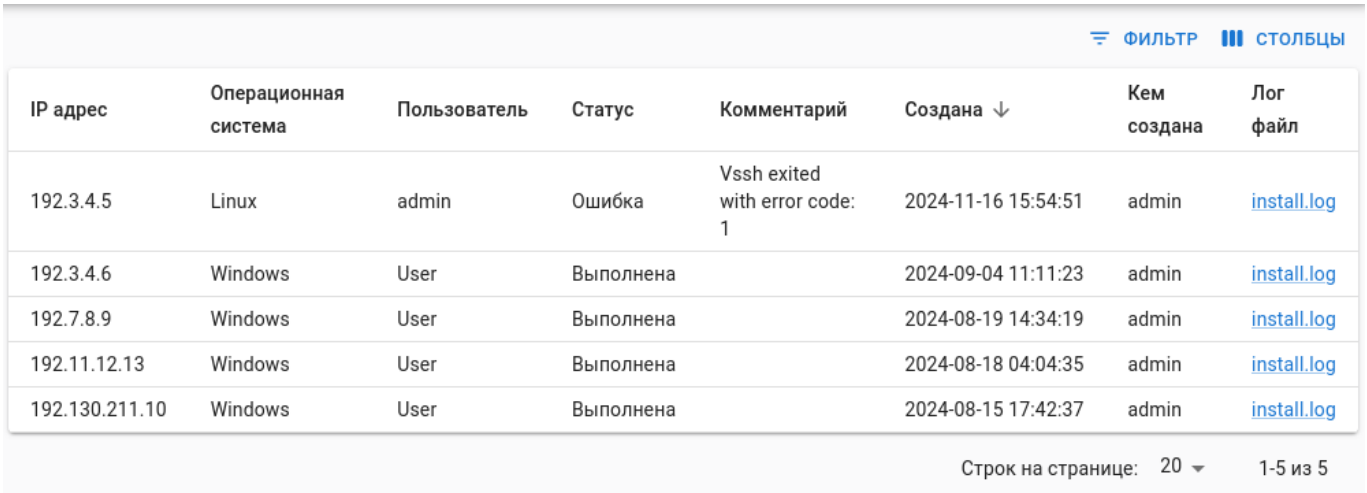


Рис. 194 – Раздел «Сканирование». Подраздел «Установки»

Результаты и ход установки

Перечень столбцов данных:

1) **IP адрес** – валидный IPv4 или IPv6 адрес компьютера, обнаруженного в заданном участке сети;
2) **Операционная система** – найденная ОС на клиентском СВТ;
3) **Пользователь** – имя пользователя, от имени которого производилась установка на клиентском СВТ;
4) **Статус** – текущее состояние установки;
5) **Комментарий** – важные сообщения, возникшие в ходе установки;
6) **Создана** – время создания события;
7) **Кем создана** – имя пользователя ЦУ, который инициировал установку;
8) **Лог файл** – файла журнала, созданный в процессе установки.

По нажатию на соответствующий элемент в столбце **Лог файл** таблицы подраздела **Установки** произойдет загрузка и чтение файла журнала, созданного в процессе установки для выбранного клиентского СВТ.

4.6.14. Раздел Настройки

Раздел **Настройки** предназначен для:

1) отображения информации о ЦУ: правообладателе, версии продукта, публичного ключа подписи пакетов (вкладка **О программе**);
2) произведения обновления ЦУ уполномоченным администратором комплекса (вкладка **Обновление**);
3) настройки параметров авторизации (вкладка **Авторизация**);
4) настройки параметров системы обслуживания ЦУ (вкладка **Обслуживание**);
5) настройки параметров уведомления администратора посредством электронной почты (вкладка **Почта**);

4.6.14.1. О программе

На данной вкладке (рис. 195) отображаются следующие поля:

1) **Версия** – отображает версию текущего установленного ЦУ.
2) **Публичный ключ для подписи пакетов** – содержит информацию об открытом ключе, при помощи которого можно выполнить подсоединение уже

установленной клиентской части программного комплекса ШХУНА к ЦУ (см. рис. 26).

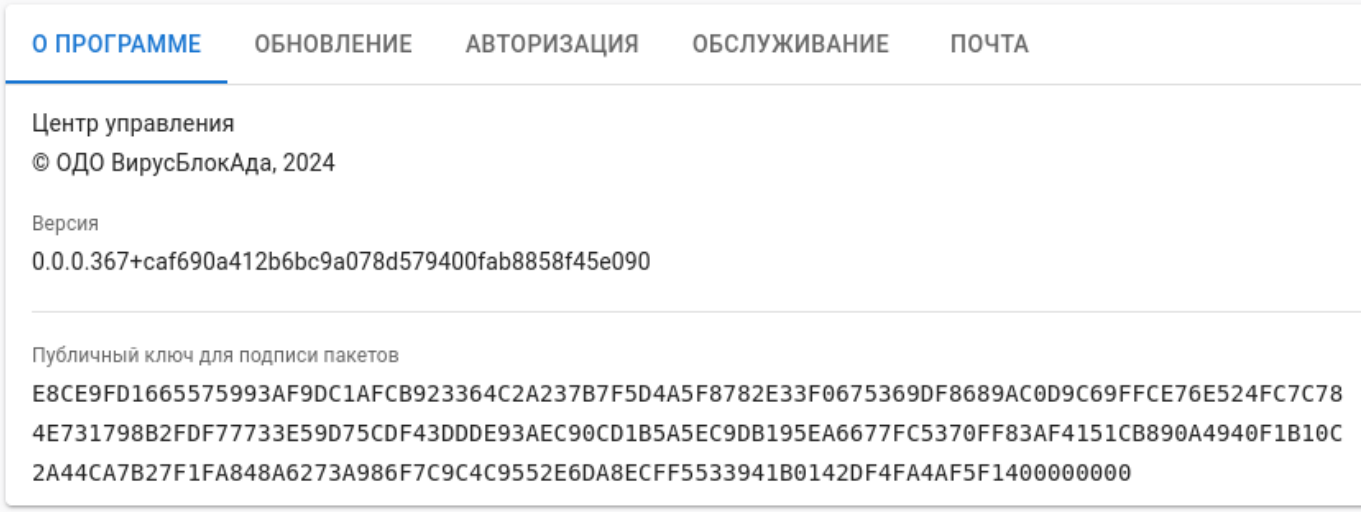


Рис. 195 – Раздел «Настройки». Вкладка «О программе»

4.6.14.2. Обновление

Поле **URL для обновления** предназначено для указания пути к ресурсу обновления ЦУ. Для запуска процедуры обновления необходимо нажать кнопку **Обновить Центр управления** (рис. 196). В результате успешного обновления в автоматическом режиме будут обновлены файлы ЦУ; веб-страница, содержащая информацию о версии будет также обновлена автоматически.

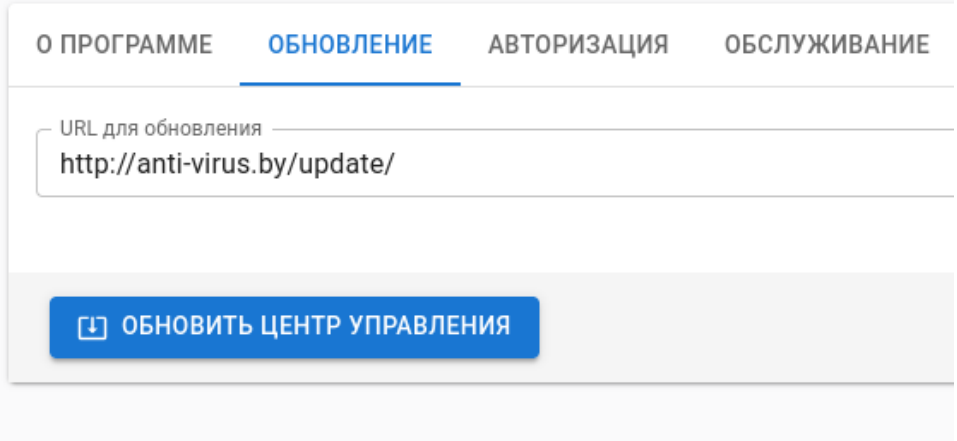


Рис. 196 – Раздел «Настройки». Вкладка «Обновление»

4.6.14.3. Авторизация

На данной вкладке (рис. 197) сосредоточены настройки, связанные с пользовательской сессией в веб-интерфейсе ЦУ.

При бездействии пользователя предполагается, что через установленный промежуток времени сессия будет прервана. В таком случае пользователь будет вынужден повторно осуществить ввод имени и пароля.

Данное событие произойдет по окончании времени указанного в поле **Таймаут refresh-токена**.

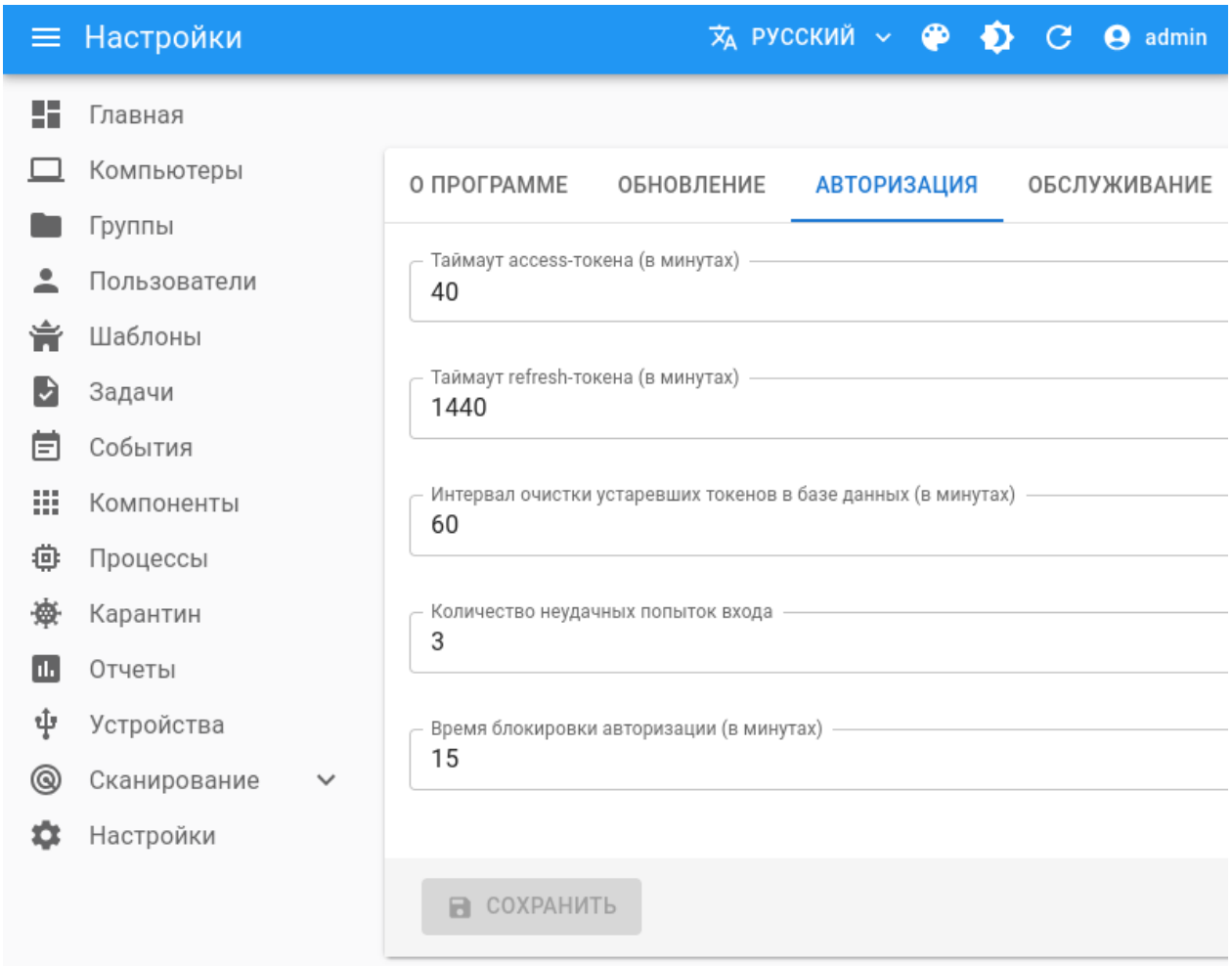


Рис. 197 – Раздел «Настройки». Вкладка «Авторизация»

Поле **Таймаут access-токена** определяет время, через которое будет выполнен запрос на генерацию нового access-токена.

Время, указанное в строке **Интервал очистки устаревших токенов в базе данных** определяет, когда будут уничтожены истекшие токены.

При превышении заданного с помощью поля **Количество неудачных попыток входа** числа попыток аутентификации происходит автоматическая блокировка полей интерфейса аутентификации.

Поле **Время блокировки авторизации (в минутах)** определяет время (числовое значение в минутах) блокировки доступа к интерфейсу аутентификации. Блокировка наступает после серии попыток аутентификации с неверными логином и/или паролем (см. поле **Количество неудачных попыток входа**).

4.6.14.4. Обслуживание

На данной вкладке сосредоточены настройки, связанные с системой обслуживания ЦУ, которая обеспечивает очистку устаревших и неактуальных записей аудита, а также настройки пороговых значений для её проведения.

Администратор может включать, либо выключать систему обслуживания ЦУ с помощью переключателя **Включить / выключить обслуживание** (рис. 198).

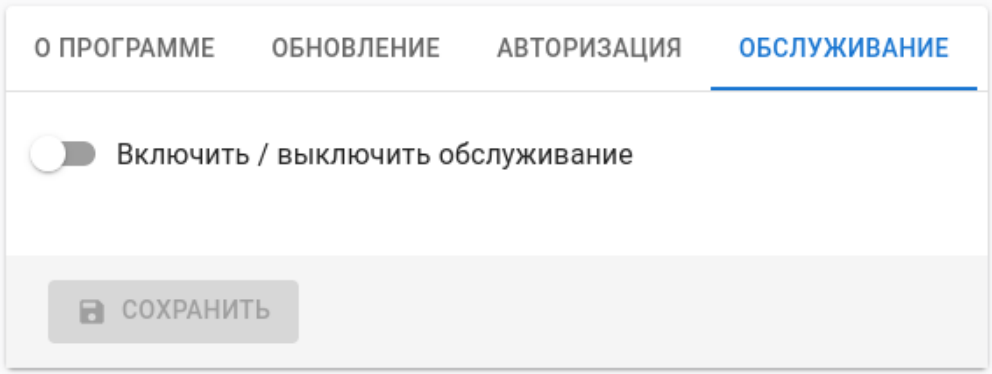


Рис. 198 – Раздел «Настройки». Вкладка «Обслуживание»

Хранилищем данных ЦУ является его БД. С течением времени база может значительно увеличиться в размерах, снижая эффективность работы ЦУ.

Примечание. Необходимо следить за размером БД ЦУ. Чем больше ее размер, тем больше требования к аппаратным ресурсам сервера БД. Настоятельно рекомендуется периодически делать резервные копии БД.

Данные об устаревших событиях можно удалить из БД. Очистка БД от событий производится системой обслуживания ЦУ в автоматическом режиме.

Примечание. Данные настройки могут быть произведены только с использованием учетной записи администратора.

После установки переключателя **Включить / выключить обслуживание** в положение «включено» в интерфейсе пользователя будут показаны дополнительные поля настроек (рис. 199).

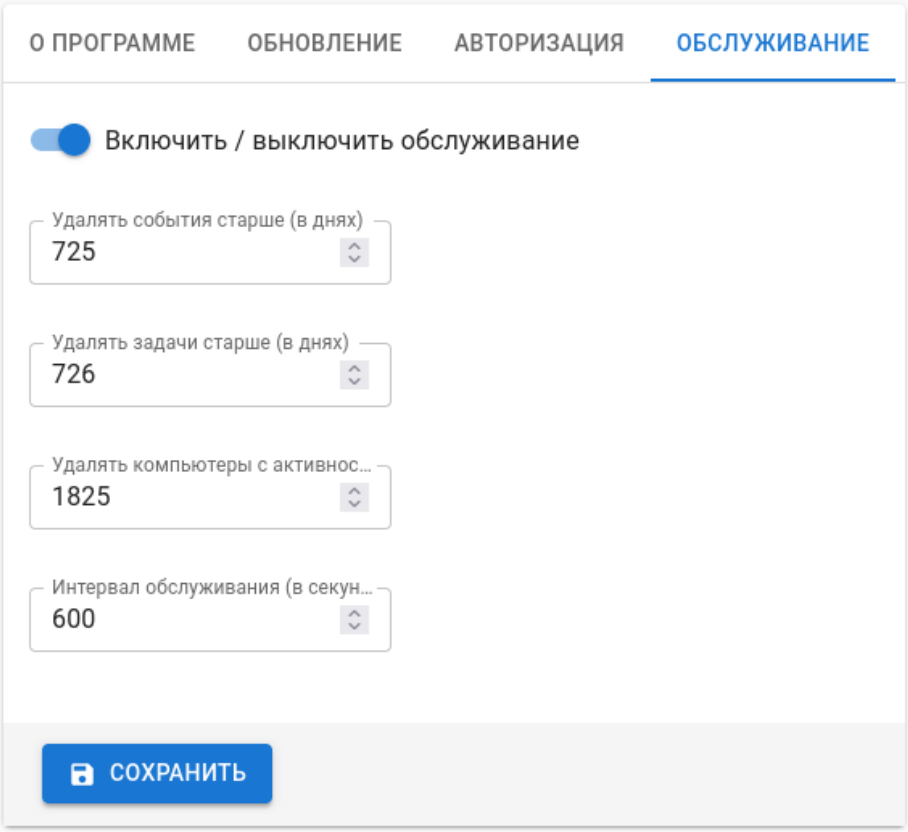


Рис. 199 – Раздел «Настройки». Вкладка «Обслуживание». Настройки

Доступные поля настроек:

1) **Удалять события старше (в днях)** – количество дней, по истечении которых события будут удалены из БД;
2) **Удалять задачи старше (в днях)** – количество дней, по истечении которых задачи будут удалены из БД;
3) **Удалять компьютеры с активностью старше (в днях)** – количество дней, по истечении которых события на компьютерах будут удалены из БД;
4) **Интервал обслуживания (в секундах)** – значение в секундах периода, по истечении которого сервис производит проверку БД на предмет очистки событий и обновления состояния задач.

Для применения заданных Администратором настроек системы обслуживания ЦУ необходимо нажать на кнопку **Сохранить**.

4.6.14.5. Почта

На данной вкладке сосредоточены настройки ЦУ, связанные с системой уведомления средствами электронной почты, которая обеспечивает уведомление уполномоченных администраторов о действиях в случае удаления устаревших данных аудита (рис. 200), которые были определены в п. 4.6.14.4.

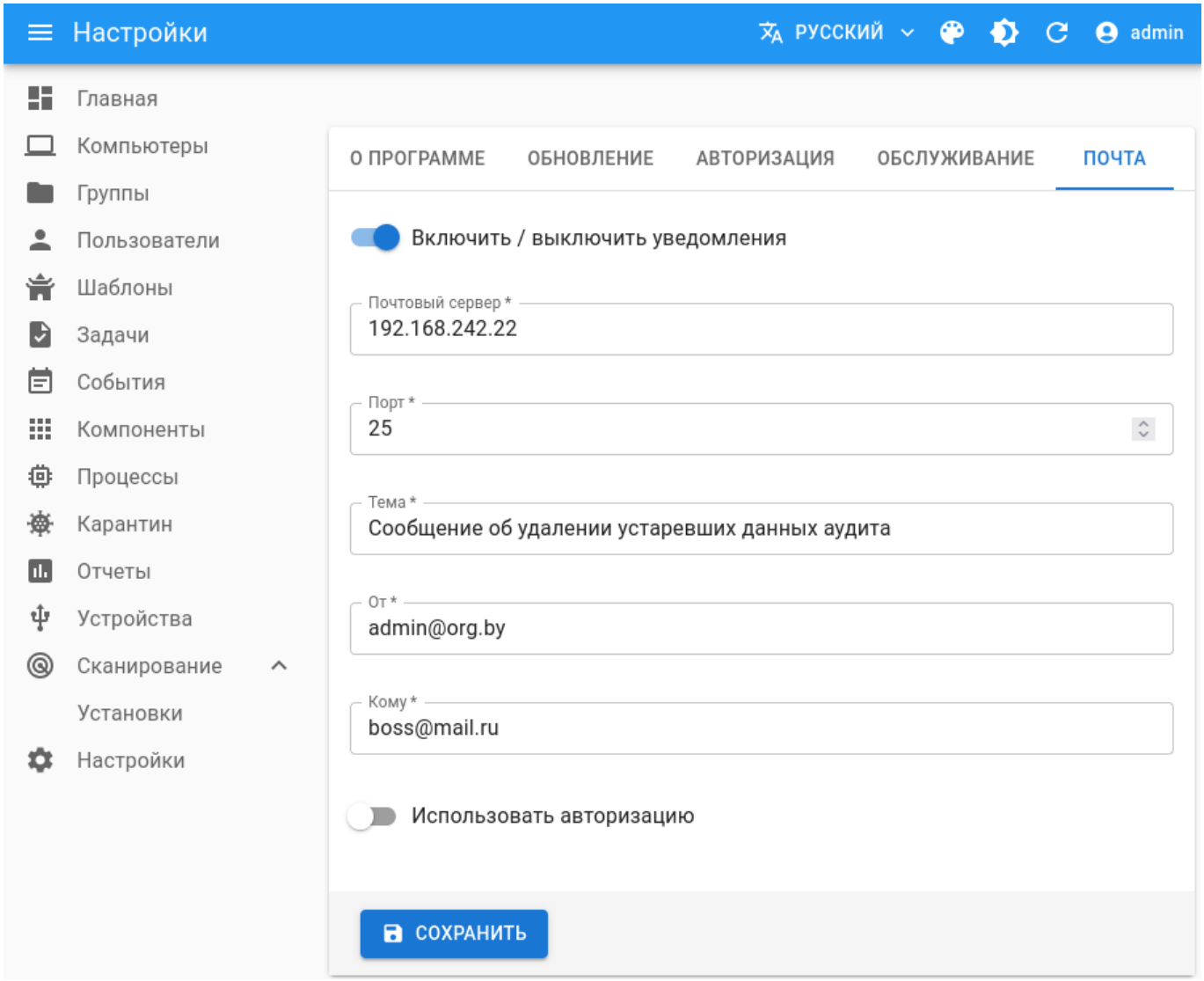


Рис. 200 – Раздел «Настройки». Вкладка «Почта»

После установки переключателя **Включить / выключить уведомления** в положение «включено» в интерфейсе пользователя будут отображены основные поля настроек. Данный переключатель управляет включением либо выключением системы уведомления средствами электронной почты ЦУ.

После установки переключателя **Использовать авторизацию** в положение «включено» в интерфейсе пользователя будут показаны дополнительные поля настроек (рис. 201).

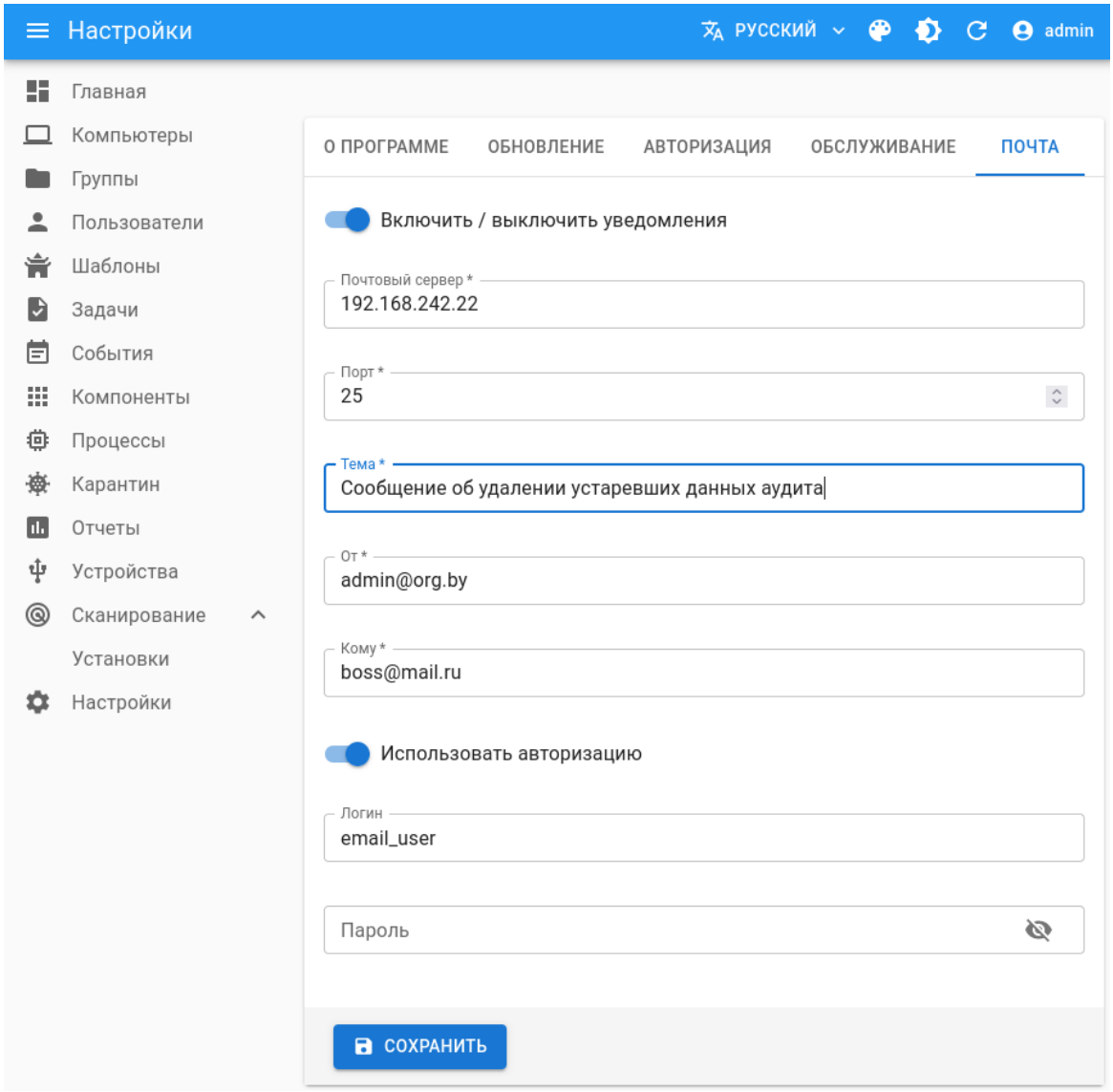


Рис. 201 – Раздел «Настройки». Вкладка «Почта». Настройки авторизации

Доступные поля основных настроек:

1) **Почтовый сервер** – IP-адрес или имя СВТ с настроенным почтовым сервером (SMTP);
2) **Порт** – порт почтового сервера;
3) **Тема** – тема письма электронной почты;
4) **От** – адрес электронной почты отправителя;
5) **Кому** – адрес электронной почты получателя.

Доступные поля дополнительных настроек (настроек авторизации):

1) **Логин** – имя пользователя для авторизации на почтовом сервере;
2) **Пароль** – пароль пользователя, участвующего в авторизации с указанным логином.

Для применения заданных Администратором настроек системы уведомления средствами электронной почты необходимо нажать на кнопку **Сохранить**.

4.6.15. Панель быстрого доступа

Веб-оснастка графического интерфейса ЦУ предполагает наличие в верхней части экрана специальной панели (рис. 202).

Рис. 202 – Панель быстрого доступа. Общий вид

На ней располагаются следующие элементы:

1) кнопка сворачивания боковой панели меню (иконка);
2) название текущего выбранного раздела/подраздела боковой панели меню или элемента, над которым оперирует пользователь ЦУ;
3) переключатель языка (русский, английский);
4) переключатель темы графического интерфейса (по умолчанию, минимальная) (иконка);
5) переключатель режима темы графического интерфейса (светлая, темная) (иконка);
6) кнопка **Обновить** (иконка);
7) переключатель пользователя (выход из учетной записи) (иконка).

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					
1	–	182	–	181	182	ИАДВ.1-2025	–		19.03.2025
2	–	183	–	182	183	ИАДВ.2-2025	–		15.10.2025

2		15.10.2025
№ изм.	Подп.	Дата