



Systeme
soft

Программный комплекс Систэм Платформ

Систэм Платформ

Общее описание



© ООО «Систэм Софт», 2022-2022. Все права защищены.

Авторские права на данный документ принадлежат ООО «Систэм Софт». Копирование, перепечатка и публикация любой части или всего документа не допускается без письменного разрешения правообладателя.

Содержание

1. Назначение и особенности	6
2. Архитектура Систэм Платформ	7
3. SePlatform.Data collection Server	8
3.1. Сбор данных	8
3.2. Предоставление данных клиентам	8
3.3. Ядро	9
3.4. Резервирование	9
3.5. Логическая обработка данных	10
3.6. Генерация событий и тревог	10
3.7. Прочие возможности SePlatform.Data collection Server	10
3.8. Сервисное обслуживание SePlatform.Data collection Server	10
3.9. Архитектурная схема сервера	11
4. SePlatform.Historian	12
4.1. Сбор информации от серверов технологических данных	12
4.2. Хранение данных в SePlatform.Historian	13
4.3. Резервирование	13
4.4. Предоставление данных клиентам	13
5. SePlatform.AccessPoint	14
5.1. Объединение адресного пространства серверных компонентов	15
5.2. Поддержка связи с источником данных	15
6. SePlatform.Development Studio	16
6.1. Формирование физической и логической структуры проекта	16
6.2. Формирование конфигураций средств автоматизации	17
6.3. Формирование схемы развертывания проекта автоматизации на вычислительных средствах	17
6.4. Сборка конфигураций	18
6.5. Администрирование проекта автоматизации	18
6.6. Командная разработка проекта автоматизации	18
6.7. Характеристики	18
7. SePlatform.Tools	19
8. SePlatform.HMI	20
8.1. Визуальный редактор для построения мнемосхем	21
8.2. Взаимодействие с источниками данных	21
8.3. Объектно-ориентированный подход при разработке проектов	22
8.4. Поддержка скриптовых языков SePlatform.Om и JavaScript	23
8.5. Встраиваемые компоненты	23
9. SePlatform.HMI.WebViewer	26
10. SePlatform.HMI - приложения	27
10.1. SePlatform.HMI.Alarms	27
10.2. SePlatform.HMI.Trends	27
10.3. SePlatform.HMI.SecurityConfigurator	28
10.4. SePlatform.HMI.SetPoints	28
10.5. SePlatform.HMI.Explorer	29
10.6. SePlatform.HMI.Charts	29
10.7. SePlatform.HMI.Tables	29

10.8. SePlatform.HMI.IntegrityControl	30
11. SePlatform.HMI - дополнительные модули	31
11.1. SePlatform.HMI.Security	31
12. SePlatform.HMI - библиотеки	32
12.1. SePlatform.HMI.CommonLib	32
13. SePlatform.Security	33
13.1. Работа с пользователями	34
13.2. Работа с группами	34
13.3. Работа с приложениями	34
14. SePlatform.Domain	36
15. SePlatform.Mapping Server	37
16. Лицензирование Систэм Платформ	38
16.1. Ключи Sentinel	38
16.1.1. ОС Windows	38
16.1.1.1. Аппаратный ключ Sentinel HL	38
Обновление лицензии	39
16.1.1.2. Программный ключ Sentinel SL	40
Установка драйвера Sentinel HASP	41
Активация	41
Обновление	42
Утилита SePlatform Soft Rus.exe	43
Активация	43
Обновление лицензии	44
Перенос программного ключа на другой компьютер	45
16.1.2. ОС Linux	48
16.1.2.1. Установка SePlatform.License Server	48
16.1.2.2. Установка драйвера Sentinel HASP	49
16.1.2.3. Аппаратный ключ Sentinel HL	49
Обновление лицензии	49
16.1.2.4. Программный ключ Sentinel SL	51
Активация	51
Обновление	53
16.2. Ключи Guardant	54
16.2.1. ОС Windows	54
16.2.1.1. Аппаратный ключ Guardant Sign	54
Обновление	54
16.2.1.2. Программный ключ Guardant DL	56
Активация на компьютере с доступом в Интернет	57
Активация на компьютере без доступа в Интернет	59
Обновление на компьютере с доступом в Интернет	66
Обновление на компьютере без доступа в Интернет	68
Перенос на другой компьютер	75
16.2.2. ОС Linux	76
16.2.2.1. Установка SePlatform.License Server	77
16.2.2.2. Установка Guardant Control Center	77
16.2.2.3. Аппаратный ключ Guardant Sign	78
Обновление	78
16.2.2.4. Программный ключ Guardant DL	80
Активация на компьютере с доступом в Интернет	82
Активация на компьютере без доступа в Интернет	84

Обновление на компьютере с доступом в Интернет	92
Обновление на компьютере без доступа в Интернет	94
Перенос на другой компьютер	101
16.3. Решение проблем	102
17. Безопасное администрирование	103
17.1. Общие рекомендации	103
17.2. Рекомендации, применимые для компонентов Систэм Платформ	108
18. Правила брандмауэра	109
18.1. ОС Windows	109
18.1.1. Правила для входящих подключений	111
18.1.2. Правила для исходящих подключений	114
18.2. ОС Linux	118
18.3. Порты для входящих подключений	119
18.4. Порты для исходящих подключений	120
19. Работа в ОС Linux	123
19.1. (Astra Linux) Создание пользователя Operator с ограниченными правами	125

1. Назначение и особенности

Документ содержит краткое описание назначения, функционала и особенностей компонентов, входящих в программный комплекс Систэм Платформ. Документ предназначен для специалистов по разработке, внедрению и эксплуатации проектов автоматизации технологических и производственных процессов.

Программный комплекс Систэм Платформ разработан российским производителем программного обеспечения с применением современных подходов, успешно применяемых в IT-сфере.

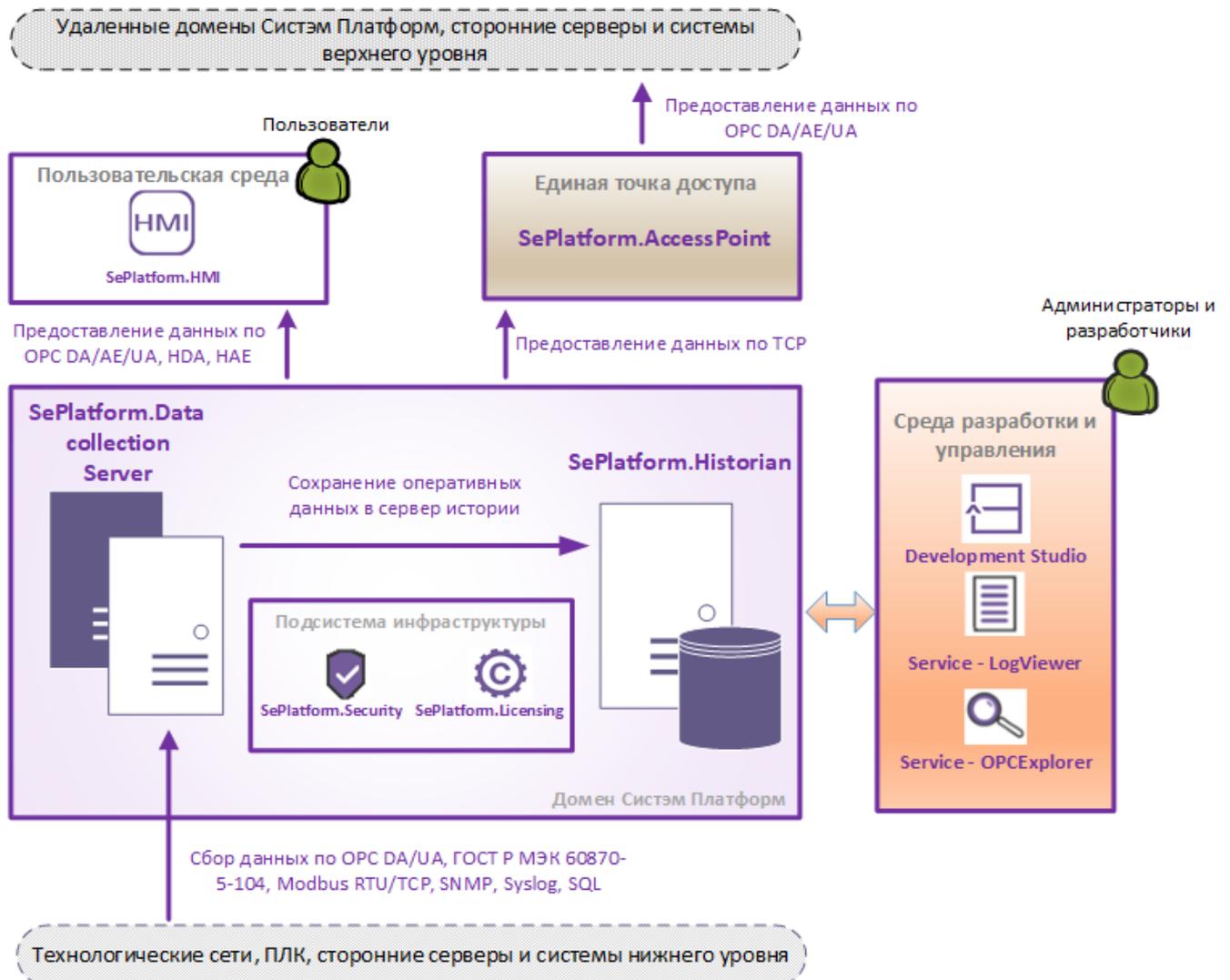
Систэм Платформ представляет собой программный комплекс, состоящий из различных компонентов, используемых для разработки, исполнения и сопровождения проектов автоматизации технологических и производственных процессов. Проекты автоматизации, разработанные с помощью инструментов Систэм Платформ, могут внедряться на локальных и территориально распределенных промышленных предприятиях. Функциональность Систэм Платформ полностью охватывают верхний уровень архитектуры АСУ ТП.

Систэм Платформ является единым программным решением для покрытия всех стадий жизненного цикла проекта автоматизации - начиная от проектирования и заканчивая сопровождением готового проекта.

Возможности Систэм Платформ:

- Современные инструменты разработки, внедрения, эксплуатации и сопровождения проектов автоматизации.
- Возможность работы с единым визуальным инструментом от стадии проектирования до стадии администрирования проекта автоматизации.
- Инструменты контроля согласованности и связанности проекта для исключения ошибок.
- Автоматизированные системы администрирования, развертывания и контроля версионности конфигураций проекта автоматизации.
- Надежные инструменты исполнения проектов автоматизации.
- Инструменты для мониторинга и управления технологическими объектами.
- Инструменты для логической обработки данных.
- Инструменты для сохранения и предоставления полной истории работы системы.
- Инструменты для визуального представления данных пользователю (мнемосхемы, таблицы, графики).
- Возможность интеграции встраиваемых компонентов Систэм Платформ в сторонние программные продукты.

2. Архитектура Систэм Платформ



Ключевой единицей инфраструктуры Систэм Платформ является домен - совокупность вычислительных средств для выполнения проекта автоматизации. Серверные компоненты домена выполняют целевые функции проекта: сбор данных от нижестоящих систем, логическую обработку данных, предоставление данных вышестоящим системам, хранение исторической информации и прочее. К подсистеме исполнения относятся **SePlatform.Data collection Server** и **SePlatform.Historian**.

SePlatform.AccessPoint - единая точка доступа, объединяющая серверные компоненты и удалённые домены Систэм Платформ (для построения распределённых систем), а также взаимодействие со сторонними приложениями и системами по стандартным протоколам и спецификациям.

Пользовательская среда обеспечивает работу с визуальной частью проекта автоматизации. К компонентам пользовательской среды относятся **SePlatform.HMI**.

Среда разработки и управления служит для создания, тестирования и отладки приложений и состоит из продуктов **SePlatform.Development Studio** и **SePlatform.Tools**. Среда используется также для выполнения централизованных задач по настройке и обслуживанию домена Систэм Платформ.

К подсистеме инфраструктуры относятся продукты **SePlatform.Security** (регламентирует безопасность и разграничение прав внутри домена), **SePlatform.Diagnostics** (выполняет функции комплексной диагностики, мониторинга и аудита), **SePlatform.License Server** (обеспечивает лицензирование продуктов внутри домена).

3. SePlatform.Data collection Server

SePlatform.Data collection Server - компонент Систэм Платформ, выполняющий следующие задачи:

- Сбор данных с устройств в ходе мониторинга контролируемых объектов.
- Предоставление данных клиентам по различным протоколам и спецификациям.
- Повышение надежности проекта за счёт резервирования.
- Логическая обработка данных в режиме реального времени.
- Генерация событий и тревог на основе полученных данных.

Сервер построен по модульному принципу, что позволяет конфигурировать его в зависимости от выполняемых задач и не создавать лишней нагрузки.

Количество экземпляров сервера на одном компьютере не ограничено, что позволяет использовать сервер в качестве конвертера протоколов или для создания демилитаризованных зон.

3.1. Сбор данных

SePlatform.Data collection Server обеспечивает опрос источников данных по различным протоколам и спецификациям.

Протокол/Спецификация	Модуль
ГОСТ Р МЭК 60870-5-104	IEC104 Master
Modbus TCP	Modbus TCP Master
Modbus RTU	Modbus RTU Master
OPC DA	OPC DA Client
OPC HDA	OPC HDA Client
OPC UA	OPC UA Client
TCP	HUB
SQL	SQL Connector
SNMP	SNMP Manager
ICMP	SNMP Manager
Файловый интерфейс	HUB
Syslog	Syslog Server

3.2. Предоставление данных клиентам

SePlatform.Data collection Server предоставляет данные клиентам по различным протоколам и спецификациям.

Протокол/спецификация	Модуль
ГОСТ Р МЭК 60870-5-104	IEC104 Slave
Modbus TCP	Modbus TCP Slave
Modbus RTU	Modbus RTU Slave
OPC DA	OPC DA Server
OPC HDA	OPC HDA Server
OPC AE	OPC AE Server
OPC UA	OPC UA Server
TCP	TCP Server
Файловый интерфейс	TCP Server

3.3. Ядро

Ядро SePlatform.Data collection Server является центральным компонентом сервера. Предназначено для реализации инфраструктуры сервера, интерфейсов работы с модулями, сигналами и их свойствами, остальными подсистемами. Ядро может производить значимые логические вычисления, требующие наибольшей скорости вычислений. Такой подход позволяет значительно повысить производительность работы сервера. Все вычисления производятся по описанным при конфигурировании алгоритмам.

Основные функции ядра SePlatform.Data collection Server:

- Пересчет значений из физических значений в инженерные и в обратном направлении. При пересчете используются линейная и линейная с изломом зависимости.
- Выполнение алгоритмов по событию, таймеру и расписаниям.
- Управление запуском и остановом модулей при старте и в процессе работы сервера.
- Управление состоянием сервера в рамках резервирования.
- Запись и чтение данных из ОБД.
- Управление модулями, отправка и принятие уведомлений об изменении значений сигналов.

3.4. Резервирование

SePlatform.Data collection Server реализует два вида резервирования:

- горячее резервирование
- полное дублирование

При горячем резервировании система позволяет настроить репликацию данных между резервируемыми серверами для поддержания оперативной базы данных резервного сервера в актуальном состоянии. Тонкая настройка сервера позволяет ограничивать функции сервера в состоянии резерва в широком диапазоне (полное или частичное отключение опроса и обработки данных).

При полном дублировании, серверы работают независимо друг от друга и оба доступны для работы с клиентами. В этом случае клиентское приложение само решает с каким сервером работать. При реализации

крупных распределенных проектов с организацией резервируемых пунктов управления возможно создание единой системы резервных пар серверов.

3.5. Логическая обработка данных

Одна из первостепенных задач сервера - промежуточная обработка данных. Для повышения производительности работы сервера, все вычисления, производимые при обработке параметров, вынесены на уровень ядра. За внутрисерверные вычисления отвечает модуль логики. Алгоритмы модуля логики составляются на специальном скриптовом языке SePlatform.Оm.

Возможности логической обработки данных:

- Пересчет значений из физических в инженерные и обратно (по линейной и линейной с изломом зависимостям).
- Пересчет значений сигналов по формуле.
- Выполнение алгоритмов по событию, таймеру или расписанию.
- Вызов функций из внешних динамических библиотек.
- Перехват генерируемых событий и тревог.

Специфичные задачи логической обработки:

- Разбор буфера для выделения кода технологического объекта и кода события (модуль Data Buffer).
- Опциональное изменение свойств сигнала Value, Quality или Timestamp (модуль Write VQT).

3.6. Генерация событий и тревог

На основе полученных и обработанных данных сервер может по заранее определенным правилам и алгоритмам генерировать и предоставлять пользователям сообщения о событиях и тревогах. Сервер генерирует события по нескольким алгоритмам срабатывания: дискретный переключатель, перечисление, отклонение, по уровню.

Возможности сервера по генерации событий и тревог:

- Генерация событий в рамках спецификации OPC AE.
- Предоставление информации о событиях в рамках спецификации OPC DA.
- Отправка информации о событиях по электронной почте (модуль рассылки событий).

3.7. Прочие возможности SePlatform.Data collection Server

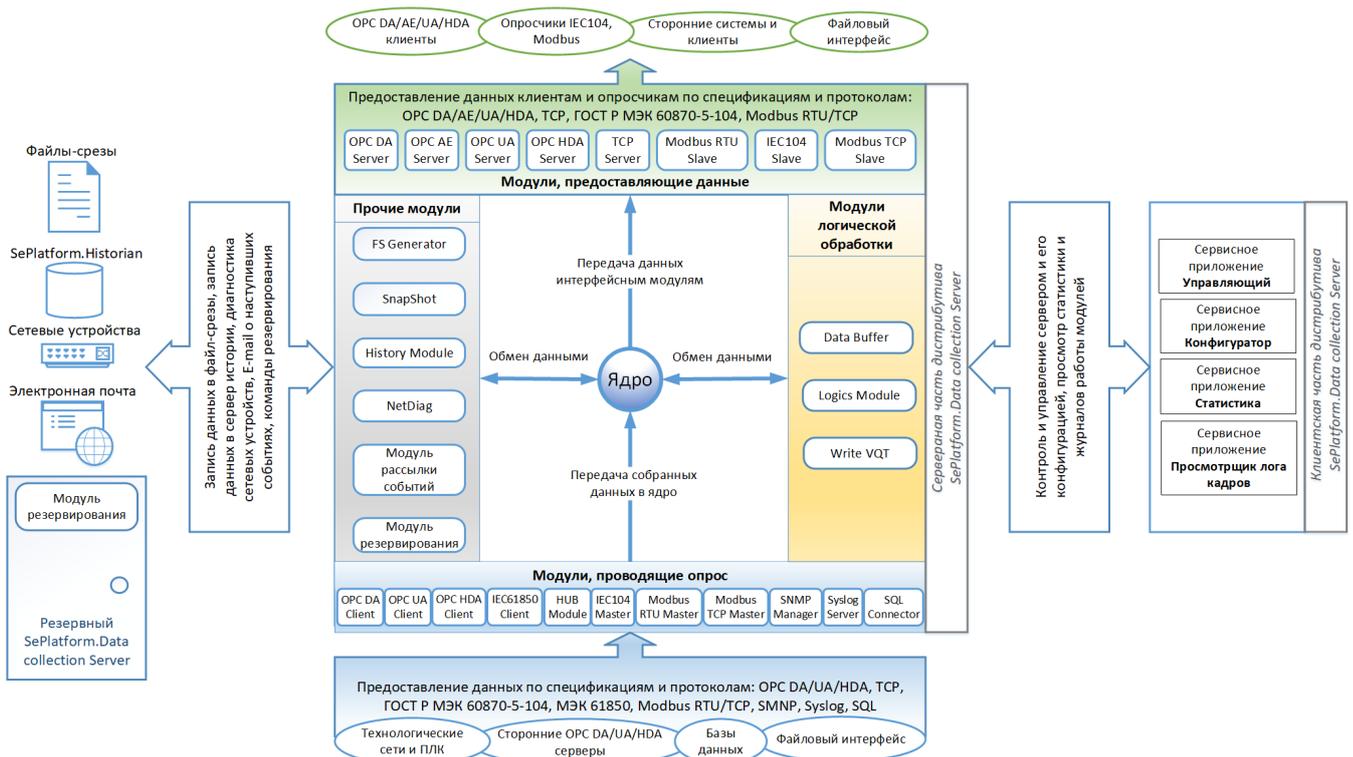
- Сохранение текущих значений сигналов в файл-срезы XML-формата (модуль SnapShot).
- Сохранение текущих значений сигналов в файл-срезы бинарного формата (модуль FS Generator).
- Диагностика сетевых устройств (модули NetDiag, NetDiag2).
- Предоставление данных для записи в сервер истории (модуль истории).

3.8. Сервисное обслуживание SePlatform.Data collection Server

Обслуживание сервера выполняется сервисными приложениями, которые входят в состав клиентской части дистрибутива SePlatform.Data collection Server:

- Редактирование конфигурации сервера выполняется с помощью сервисного приложения Конфигуратор.
- Просмотр статистической информации о работе сервера выполняется с помощью сервисного приложения Статистика.
- Просмотр журналов работы модулей сервера выполняется с помощью сервисного приложения Просмотрщик лога кадров.
- Также для сервисных и диагностических целей при работе с проектами автоматизации применяется набор инструментов SePlatform.Tools.

3.9. Архитектурная схема сервера

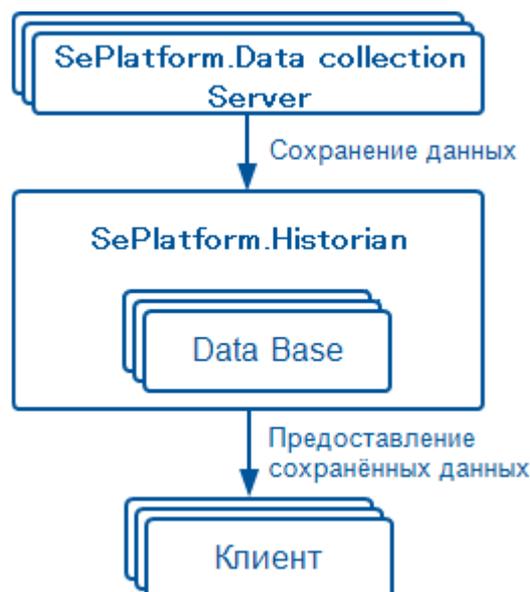


4. SePlatform.Historian

SePlatform.Historian - компонент Систэм Платформ для сбора и сохранения информации о технологическом процессе.

Возможности SePlatform.Historian:

- Сбор и хранение оперативных значений параметров технологического процесса.
- Сбор и хранение истории событий и тревог технологического процесса.
- Предоставление исторических данных клиентам.



Модуль истории в составе SePlatform.Data collection Server выполняет временное хранение данных на стороне сервера и передачу информации в хранилище SePlatform.Historian.

SePlatform.Historian предназначен для управления базами данных и предоставления хранимой исторической информации клиентам по протоколу OPC HDA. Сервер может обслуживать несколько БД одновременно.

Базы данных хранят данные, предоставляемые модулем истории. Используется БД, управляемая SePlatform.Historian. В одну БД могут сохраняться данные с нескольких независимых источников.

4.1. Сбор информации от серверов технологических данных

SePlatform.Data collection Server обеспечивает сбор, фильтрацию и запись технологических данных в SePlatform.Historian через модуль истории.

Модуль истории в составе SePlatform.Data collection Server позволяет:

- Указывать технологические параметры, по которым будет вестись история.
- Настраивать фильтрацию записываемых данных по времени и по значению.
- Обеспечить временное хранение данных для записи в файловом буфере при разрывах связи с SePlatform.Historian.
- Записывать данные в несколько резервируемых копий SePlatform.Historian.

Буфер временного хранения данных на стороне SePlatform.Data collection Server располагается на жестком диске, что предотвращает потерю данных при аварийном отключении компьютера сервера технологических данных. При следующем старте сервера непереданные данные будут повторно отправлены в SePlatform.Historian. Буферизация данных позволяет также сгладить пиковые нагрузки при большой интенсивности получения данных.

4.2. Хранение данных в SePlatform.Historian

Хранение данных ведется в суточных файлах данных для увеличения скорости доступа к данным. Сервер реализует механизмы сохранения и поиска необходимых данных, направленные на обеспечение максимальной производительности работы с дисковой подсистемой компьютера.

Глубина хранения данных ограничена размерами дискового пространства. Скорость записи и чтения данных не зависит от глубины хранения. Запись в сервер - транзакционная. Сервер обеспечивает высокую плотность записи хранимых данных на диск, уменьшая таким образом объемы читаемых с диска данных.

4.3. Резервирование

SePlatform.Historian позволяет формирование резервируемых хранилищ данных. При работе с резервируемыми хранилищами, данные из источника не удаляются, пока не пройдет запись во все хранилища. Поддерживается работа с несколькими резервируемыми хранилищами данных.

4.4. Предоставление данных клиентам

Предоставление данных клиентам осуществляется по:

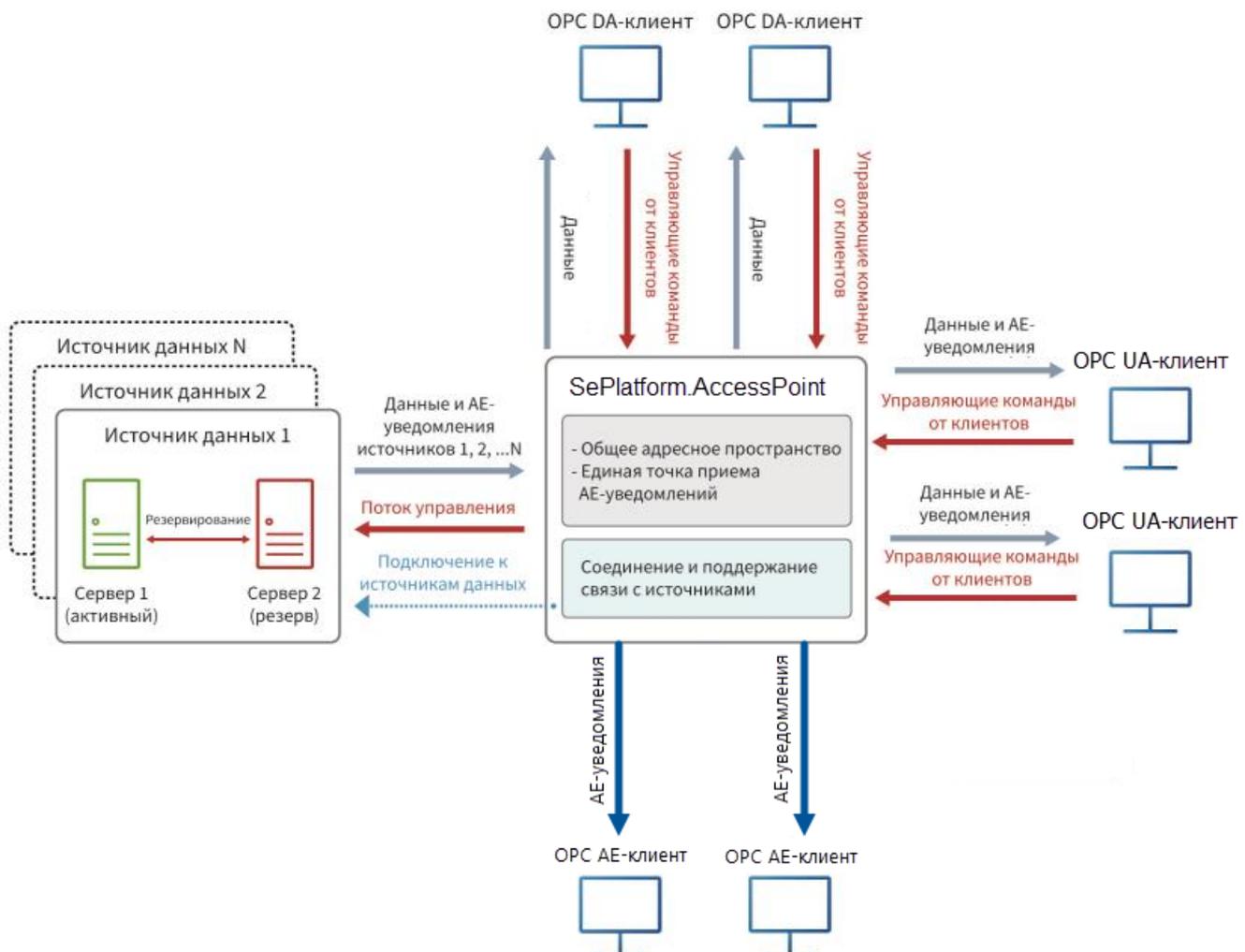
- OPC HDA, SQL и собственному протоколу передачи данных для истории значений технологических параметров.
- SQL и собственному протоколу передачи данных для истории событий.

5. SePlatform.AccessPoint

Компонент реализует функции сервера приложений и межуровневого транспорта. Предназначен для снижения нагрузки на технологические серверы и для транзитной передачи данных между доменами Систэм Платформ.

Возможности SePlatform.AccessPoint:

- Объединение сигналов различных OPC DA-источников в единое дерево сигналов.
- Объединение событий и тревог от различных OPC AE-источников.
- Поддержание связи с источниками данных при разрыве соединения.
- Передача OPC DA и OPC AE данных в виде TCP/IP-трафика в условиях различных сетевых топологий и работа в режиме каскадирования.
- Поддержка сбора данных по файловому интерфейсу.
- Доступ к данным SePlatform.AccessPoint осуществляется по спецификациям OPC DA, OPC AE, OPC UA.



5.1. Объединение адресного пространства серверных компонентов

SePlatform.AccessPoint позволяет объединять адресные пространства серверных компонентов, тем самым обеспечивая связь удаленных доменов Систэм Платформ. Клиенты подключаются к SePlatform.AccessPoint по спецификациям OPC DA, OPC UA и OPC AE как к единой точке доступа.

При построении проектов в нескольких доменах Систэм Платформ в больших распределенных системах есть возможность настраивать подключения отдельных экземпляров SePlatform.AccessPoint друг к другу. Это позволит оптимизировать инфраструктуру системы путем распределения источников данных между экземплярами SePlatform.AccessPoint и снизит нагрузку на каждый SePlatform.AccessPoint.

Возможности SePlatform.AccessPoint по объединению адресного пространства серверных компонентов:

- Объединение адресных пространств нескольких серверных компонентов.
- Постоянное поддержание связи с источниками данных.
- Получение и хранение актуальных конфигураций по каждому серверному компоненту.
- Трансляция измененных значений сигналов в общее адресное пространство.
- Предоставление подписки на общее адресное пространство серверных компонентов для OPC DA клиентов.
- Работа в качестве сервера приложений, который ограничивает нагрузку, создаваемую множеством клиентов при прямых подключениях к источникам данных.
- Обеспечение высокой скорости обмена данными и простой методики конфигурирования в условиях неоднородной сетевой топологии, благодаря использованию протокола на базе TCP/IP.

5.2. Поддержка связи с источником данных

SePlatform.AccessPoint обладает встроенной логикой переключения между серверами и каналами источника данных при разрыве соединения. Данная функция особенно полезна если источник данных представлен резервной парой серверов. SePlatform.AccessPoint автоматически проводит инициализацию всех каналов связи, а затем определяет активный сервер в составе источника данных.

В случае разрыва соединения SePlatform.AccessPoint пытается восстановить связь через резервный канал, если такой имеется. В случае отсутствия резервных каналов в составе активного сервера, SePlatform.AccessPoint переключается на работу с другим сервером и его каналами.

6. SePlatform.Development Studio

SePlatform.Development Studio - среда разработки и администрирования проектов автоматизации.

Возможности SePlatform.Development Studio:

- Сквозное описание физической структуры проекта автоматизации от уровня ПЛК до верхнего уровня.
- Сквозное описание логической структуры проекта автоматизации, а именно функций и данных объектов автоматизации применительно к средствам автоматизации различной функциональной направленности (сервера сбора данных, сервера истории, сервера межуровневого транспорта).
- Представление схемы развертывания проекта автоматизации на исполняющих компонентах.
- Компиляция и сборка конфигураций исполняющих компонентов Систэм Платформ.
- Управление развёртыванием конфигураций проекта в среде исполнения Систэм Платформ.

Среда разработки SePlatform.Development Studio может применяться в проектах автоматизации, построенных на базе Систэм Платформ. При использовании сторонних компонент в реализации проекта взаимодействие с ними производится по принципу «черного ящика» с определенными входами и выходами.

В основе построения проекта автоматизации с помощью SePlatform.Development Studio лежит объектная модель. Использование принципов такой модели позволяет представить автоматизируемые объекты приложения и компоненты среды исполнения в виде объектов.

Применение объектной модели позволяет:

- Использовать сквозное конфигурирование нескольких проектов.
- Многократно развертывать один проект в различных средах исполнения.
- Повторно использовать части проекта.
- Применять единые средства визуализации.

В SePlatform.Development Studio проект автоматизации разбивается на несколько частей. Выделяются физические объекты и их данные, на основе которых формируется проект приложения. Проект приложения разворачивается в среде исполнения. Описание структуры системы с указанием расположений функциональных узлов, каналов связи и физических серверов называется проектом развертывания. SePlatform.Development Studio позволяет синхронно формировать и модифицировать несколько проектов приложения и развертывания. Благодаря разделению каждого проекта на модули работу над проектом могут вести одновременно несколько пользователей.

6.1. Формирование физической и логической структуры проекта

Объекты физического уровня предназначены для моделирования в проекте структуры физически существующих объектов автоматизации. Структура объектов строится в соответствии с реальной иерархией в материальном мире.

В составе проекта приложения существуют следующие виды объектов:

- Физический объект - определяется в рамках проекта приложения. Может существовать в физическом мире, либо иметь вид вспомогательной структуры без определённого физического выражения.
- Логический объект - представляет собой компонент среды исполнения. Может существовать в физическом мире, либо отражать какой-либо процесс АСУ.

Объекту можно указать его тип. Тип определяет характеристики и поведение всех объектов этого типа. Использование типов позволяет быстро добавлять новые объекты, а также изменять и модифицировать все объекты.

Функции SePlatform.Development Studio в разрезе формирования физической структуры проекта:

- Определение физических и логических объектов проекта автоматизации.
- Определение типов физических объектов и их представлений в средствах автоматизации.
- Выделение логических данных объектов в виде сигналов сервера SePlatform.Data collection Server.
- Настройка атрибутов входящих и исходящих сигналов.

6.2. Формирование конфигураций средств автоматизации

В схеме развертывания проекта автоматизации каждое средство автоматизации представляет собой сервер ввода/вывода SePlatform.Data collection Server для возможности демонстрации последовательной передачи данных с устройства на устройство. После построения проекта по каждому средству автоматизации формируются конфигурации серверов SePlatform.Data collection Server. Конфигурации строятся на основе объектов и их сигналов, привязанных к средствам автоматизации.

На основе представлений физических объектов на логическом уровне появляется возможность просмотреть сформированное адресное пространство вычислительного средства. Адресное пространство доступно для преобразования и приведения к удобному для определения семантики сигналов виду. Иерархия аналогичных узлов адресного пространства строится параллельно. Такая возможность обеспечивается использованием общих групп сигналов, определенных на этапе создания проекта приложения.

Функции SePlatform.Development Studio в разрезе формирования конфигураций средств автоматизации:

- Определение папок дерева сигналов путем добавления представлений физических объектов.
- Формирование набора сигналов и распределение сигналов по папкам дерева сигналов. Добавление сигналов выполняется вследствие привязки объектов к физическим типам, а представлений объектов к представлениям логических типов.
- Формирование перечня свойств сигналов путем назначения атрибутов каждого сигнала внутри сокетов и дополнительных индивидуальных сигналов в представлениях типов.

6.3. Формирование схемы развертывания проекта автоматизации на вычислительных средствах

Проект автоматизации должен содержать схему развертывания проекта автоматизации на вычислительных средствах с указанием протоколов передачи данных. Схема развертывания необходима для определения привязки средств автоматизации к компьютерам, на которых они будут исполняться.

Для имитации средств автоматизации в проекте развертывания формируется перечень вычислительных средств. В составе каждого средства автоматизации определяется набор сетевых адаптеров для обеспечения связи по указанным протоколам. На каждом средстве автоматизации выполняется какая-то отдельная часть соответствующего проекта приложения. В схеме развертывания указывается, какие именно части будут включены в конфигурацию каждого вычислительного средства.

Функции SePlatform.Development Studio в разрезе формирования конфигураций средств автоматизации:

- Создание вычислительных средств для имитации средств автоматизации.
- Привязка модулей проекта приложения к вычислительным средствам для определения набора конфигурации сигналов.

- Настройка адресации сигналов.
- Добавление сетевых адаптеров (модулей SePlatform.Data collection Server) для каждого средства автоматизации в соответствии с протоколами передачи данных.
- Настройка параметров модулей.
- Настройка связи между вычислительными средствами для обеспечения передачи данных.

6.4. Сборка конфигураций

В результате компиляции проекта выполняется сборка проекта автоматизации и построение выходных конфигураций сервера SePlatform.Data collection Server.

6.5. Администрирование проекта автоматизации

В рамках администрирования проекта автоматизации, разработанного на базе Систэм Платформ, возможно управлять развертыванием конфигураций в нескольких средах исполнения. Для этого используется единый инструмент управления набором конфигураций всей системы.

Среда разработки SePlatform.Development Studio позволяет распространять построенную конфигурацию на несколько компьютеров одновременно. Процесс установки новых конфигураций называется дистрибуцией. С помощью дистрибуции возможно сократить время настройки и применения конфигураций в рамках большого числа серверов ввода/вывода и рабочих станций, работающих в проекте автоматизации.

Функции SePlatform.Development Studio в разрезе дистрибуции конфигураций:

- Применение разработанной конфигурации в сервер ввода/вывода.
- Подтверждение стабильности текущей конфигурации.
- Возврат к последней стабильной версии конфигурации.
- Индикация различия построенной и текущей конфигураций.

6.6. Командная разработка проекта автоматизации

Проект хранится в виде отдельных папок и файлов. Данная структура хранения даёт возможность одновременной работы над проектом нескольких человек. Рабочая копия каждого файла, расположенная на локальном компьютере, редактируется независимо от других и помещается в единое дерево файлов. В любое время есть возможность открыть ранее сохранённую версию файла. Корректировки и дополнения, внесённые разными разработчиками, могут объединяться и вноситься в одну из версий того или иного файла.

Для одновременной работы с проектом нескольких человек используется TortoiseSVN.

6.7. Характеристики

- При использовании сторонних компонент в реализации проекта взаимодействие с ними производится по принципу «черного ящика».
- Содержимое файлов проекта строится по принципам формата разработки документов .xml с учетом объектной модели приложения.
- Работа над проектами ведется как в визуальных редакторах, так и в текстовом виде по выбору пользователя.
- Количество запущенных копий на одном компьютере ограничено производительностью компьютера.

7. SePlatform.Tools

SePlatform.Tools - набор инструментов, предназначенных для сервисных и диагностических целей при работе с проектами автоматизации. В состав дистрибутива SePlatform.Tools входят приложения:

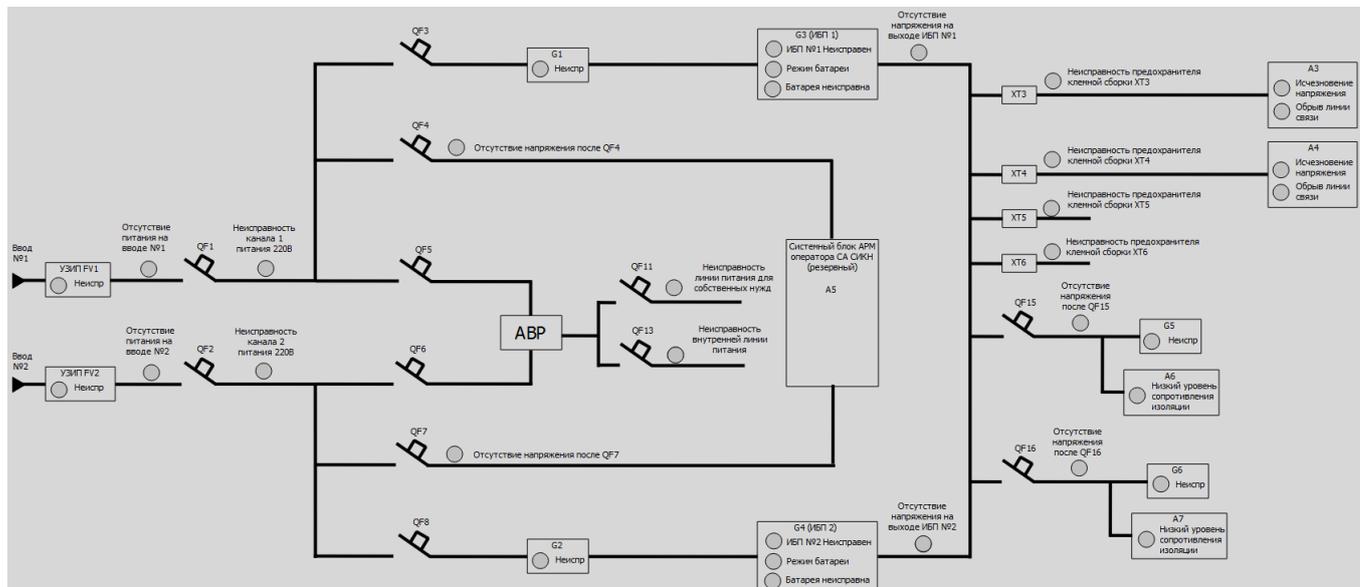
- Приложение Service - LogViewer предназначено для удобного просмотра журналов событий Windows с целью диагностики работоспособности системы.
- Приложение Service - OPCExplorer предназначено для использования в пунктах автоматизации технологических процессов. Применяется для просмотра и изменения значений сигналов, мониторинга событий, возникающих при изменении состояний технологических объектов и для графического отображения изменения значений сигналов.

8. SePlatform.HMI

SePlatform.HMI - среда разработки и исполнения визуальной части проектов автоматизации. Позволяет представлять объекты технологического процесса в виде статических и анимированных объектов мнемосхемы для мониторинга и управления процессом.

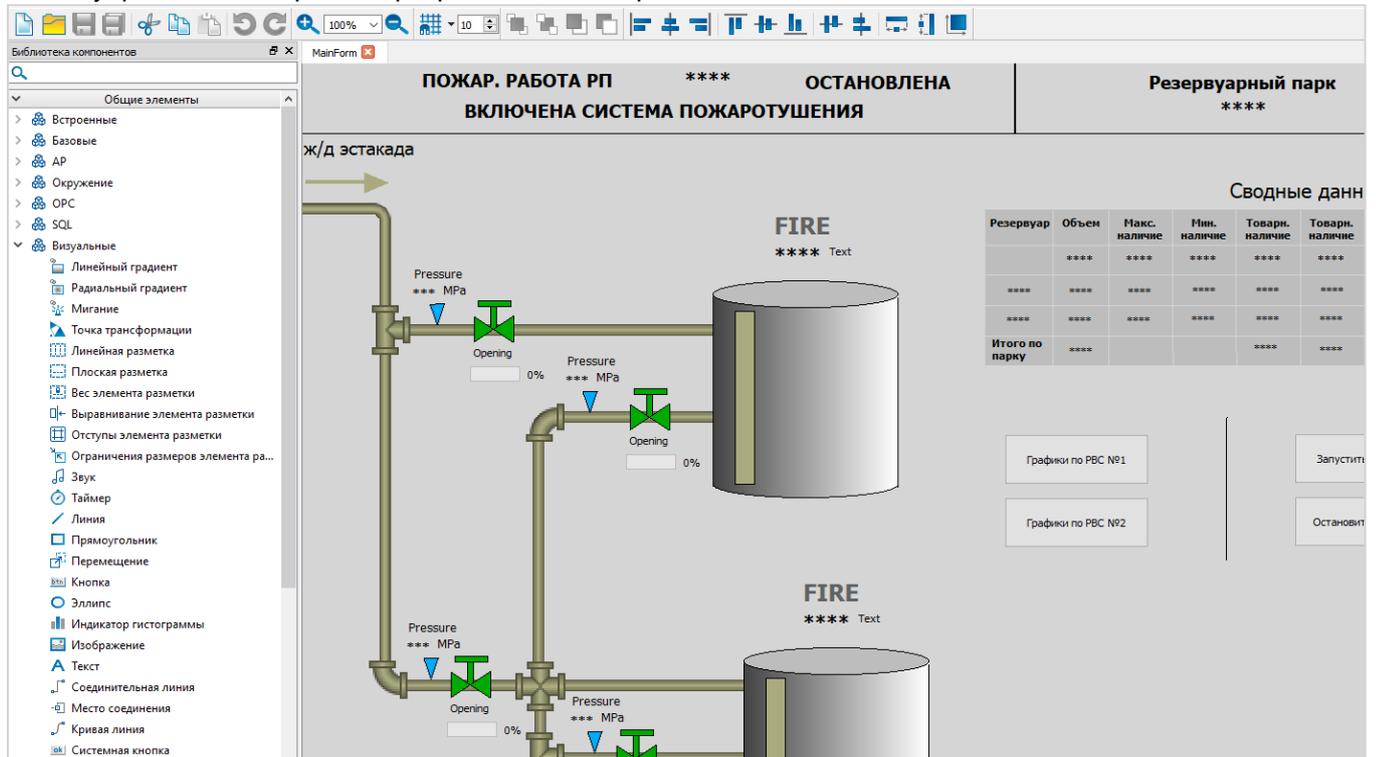
Возможности SePlatform.HMI:

- Визуальный редактор со стандартной библиотекой компонентов для построения мнемосхем;
- Взаимодействие с источником данных среды исполнения;
- Объектно-ориентированный подход при разработке проектов и возможность создания собственных типов графических объектов;
- Поддержка скриптовых языков SePlatform.Om и JavaScript.
- Взаимодействие с подсистемой безопасности SePlatform.Security.
- Взаимодействие с файловой системой, сетевым окружением и оборудованием компьютера.
- Компоненты автоматической разметки элементов мнемосхемы.
- Компоненты организации динамики на мнемосхеме.



8.1. Визуальный редактор для построения мнемосхем

SePlatform.HMI имеет стандартную библиотеку компонентов, позволяющую построить мнемосхему любой сложности. Элементы мнемосхемы могут быть расположены в различных слоях, видимостью которых можно управлять как в режиме разработки, так и в режиме исполнения.



8.2. Взаимодействие с источниками данных

Мнемосхемы, построенные с помощью SePlatform.HMI, позволяют не только визуализировать технологический процесс, но и управлять им.

Получение данных для визуализации и отправка команд осуществляется по стандартным спецификациям, поэтому в качестве источников данных могут выступать не только компоненты Систэм Платформ, но и компоненты других производителей.

SePlatform.HMI поддерживает работу с источниками данных в том числе и посредством скриптового языка, что позволяет реализовать логику любой сложности для управления объектами автоматизации.

8.3. Объектно-ориентированный подход при разработке проектов

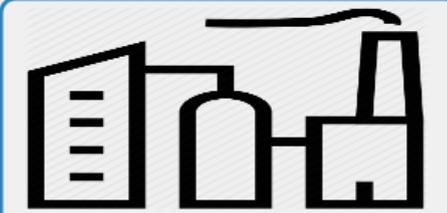
Для многократного применения однотипных объектов на мнемосхемах создаются типы графических объектов. Разработанный единожды тип графического объекта может многократно применяться на разных экранных формах проекта автоматизации.

Структура объекта

Имя	Описание
LU	Тип на основе Графический объект
Графические объекты	
Rectangle_1	Прямоугольник
Графические объекты	
Image_1	Изображение
Text_1	Текст
Данные	
Opcltem_1	Элемент OPC
OpSourceLU	Источник OPC
Параметры инициализации	
Source_init	Ссылка на Источник OPC
LUname	string

Главная мнемосхема

Демо-приложение Резервуарный парк



Линейный участок №1 "Иваново - Петрово"



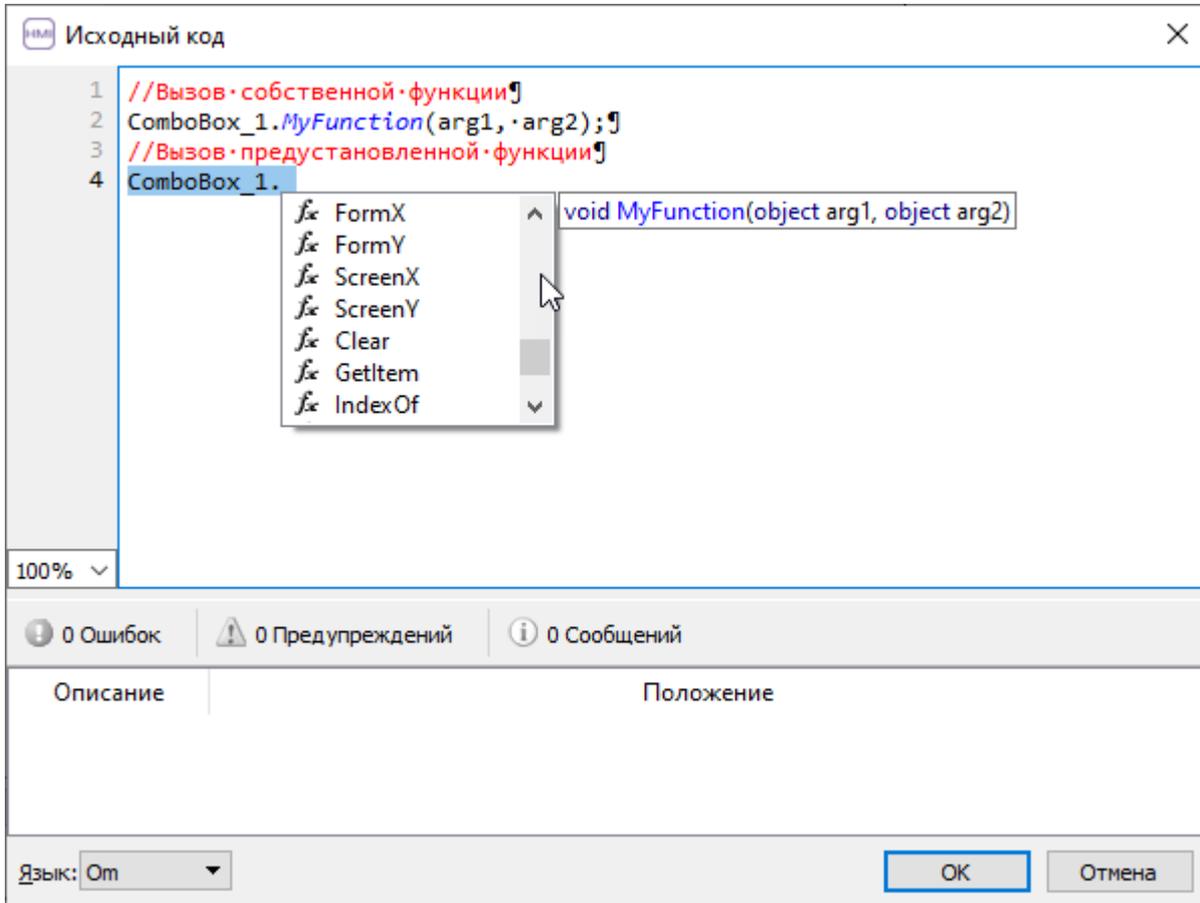
Линейный участок №2 "Петрово - Сидорово"



Линейный участок №3 "Сидорово - Смирново"

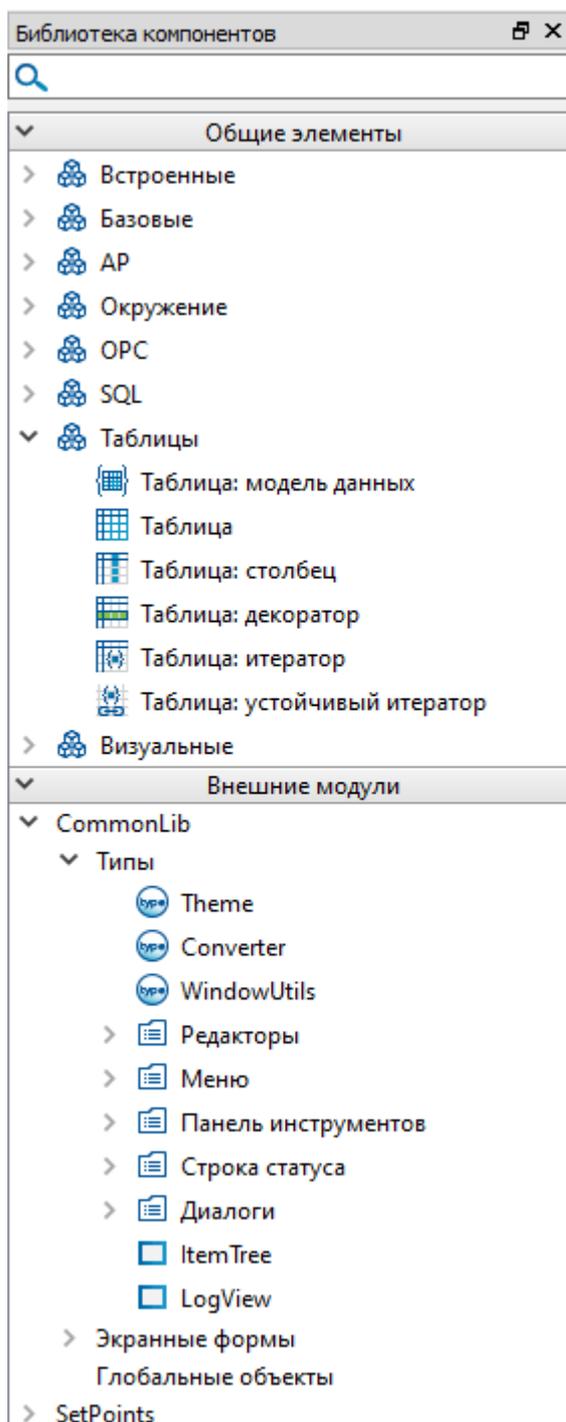
8.4. Поддержка скриптовых языков SePlatform.Om и JavaScript

SePlatform.Om является общим скриптовым языком для различных моделей данных продуктов Систэм Платформ. В SePlatform.HMI язык применяется для исполнения формул, обработчиков функций, обработчиков событий и т.д. Скриптовой язык JavaScript применяется для расширения стандартных возможностей языка SePlatform.Om.

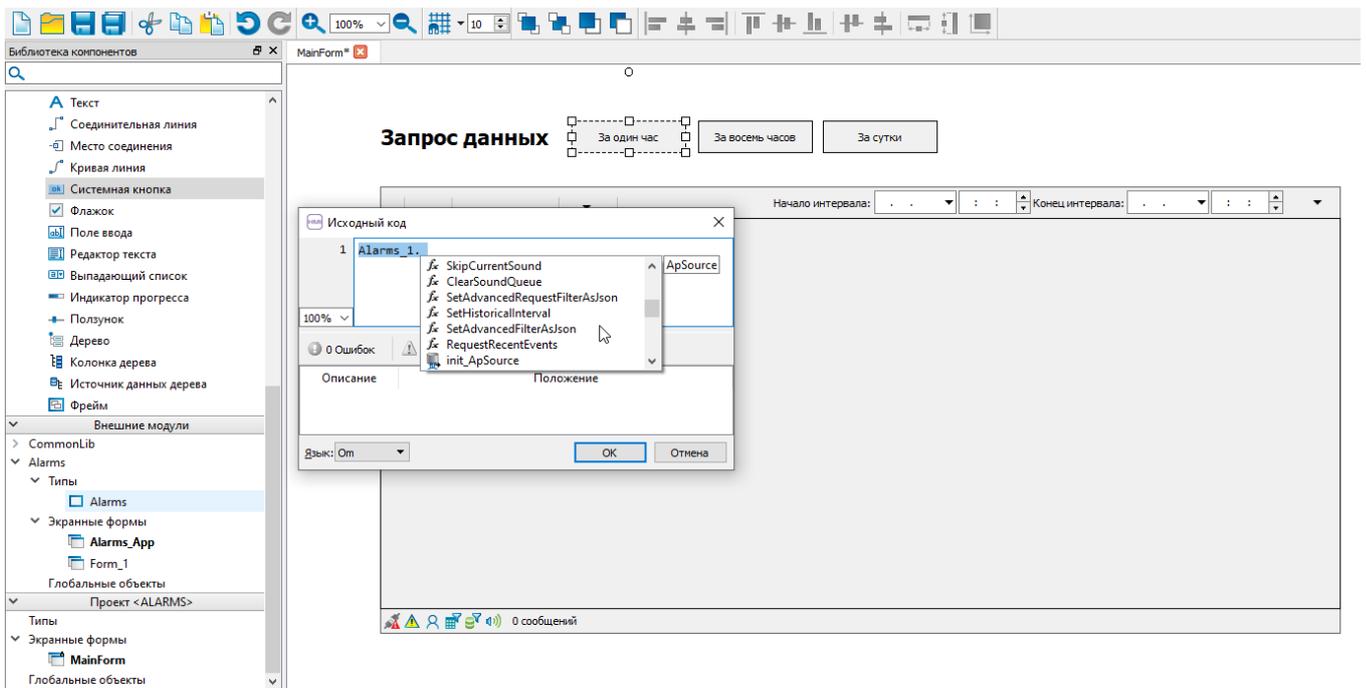


8.5. Встраиваемые компоненты

Стандартные возможности внутри проекта SePlatform.HMI можно расширять благодаря встраиванию дополнительных модулей. SePlatform.HMI позволяет подключать к проекту как библиотеки, реализованные средствами SePlatform.HMI (SePlatform.HMI.CommonLib, SePlatform.HMI.Charts, SePlatform.HMI.Tables, SePlatform.HMI.Security), так и внешние .Net библиотеки.



Некоторые компоненты, реализованные на базе SePlatform.HMI, возможно использовать как библиотеки, а также запускать как отдельные самостоятельные приложения вне прикладного проекта (SePlatform.HMI.Explorer, SePlatform.HMI.SecurityConfigurator, SePlatform.HMI.IntegrityControl, SePlatform.HMI.SetPoints, SePlatform.HMI.Alarms, SePlatform.HMI.Trends). Это готовые решения с собственным API, дающим возможность гибкой настройки работы компонентов под собственные задачи.



9. SePlatform.HMI.WebViewer

SePlatform.HMI.WebViewer позволяет просматривать мнемосхемы проекта SePlatform.HMI и взаимодействовать с ними через веб-интерфейс.

Функциональные возможности:

- преобразование проекта SePlatform.HMI в веб-приложение с предварительной компиляцией проекта;
- предоставление возможности удаленного доступа к мнемосхемам через веб-интерфейс;
- поддержка возможности подключения к веб-приложению с использованием безопасного соединения;
- предоставление возможности выбора тем оформления веб-приложения.

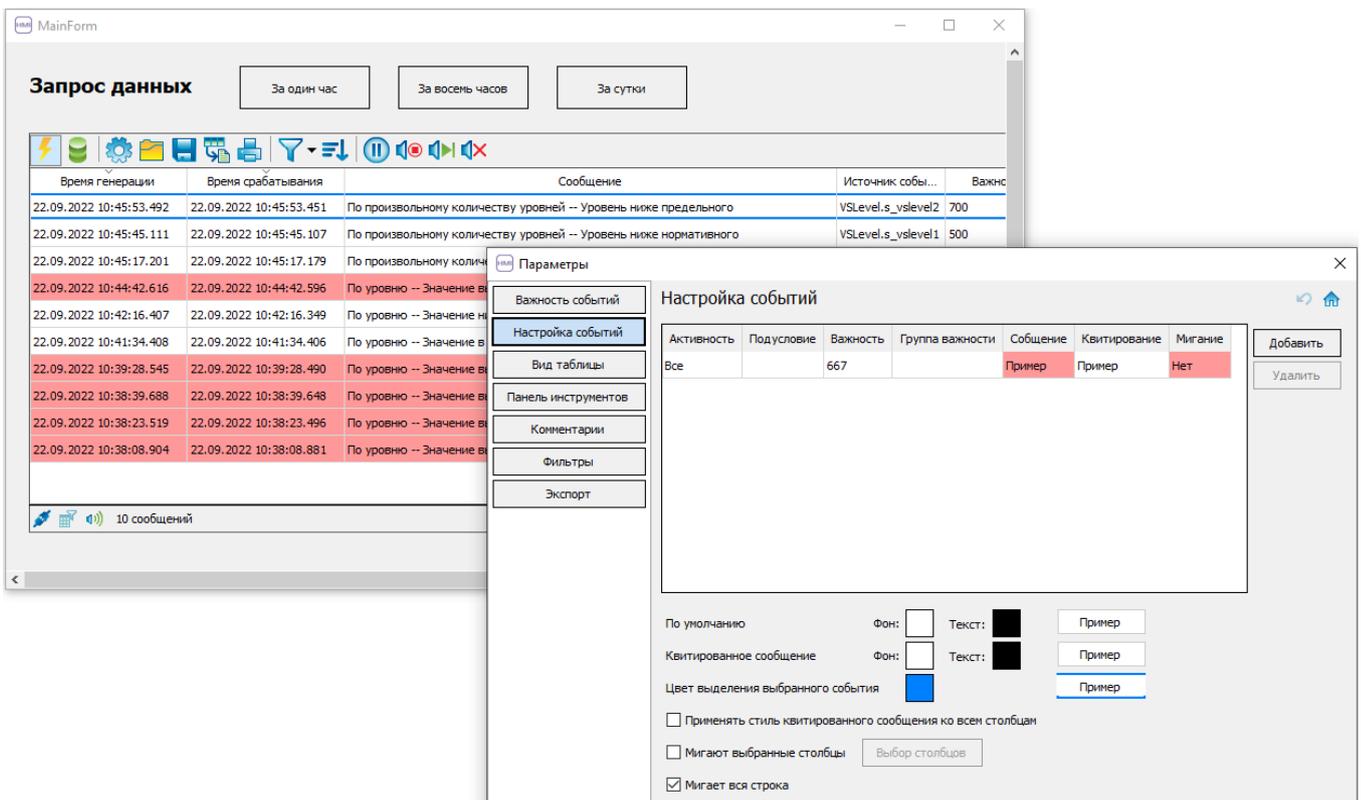
10. SePlatform.HMI - приложения

10.1. SePlatform.HMI.Alarms

SePlatform.HMI.Alarms - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих просматривать сообщения о событиях технологического процесса.

Предоставляемые возможности:

- просмотр оперативных сообщений, получаемых с локальных и удаленных серверов;
- просмотр истории событий;
- настройка звука, цвета и мигания цвета для сообщений о событиях разной важности;
- квитирование оперативных сообщений о событиях;
- фильтрация и сортировка сообщений о событиях;
- экспорт сообщений в файл формата *.csv, *.xlsx и *.pdf;
- печать списка сообщений.



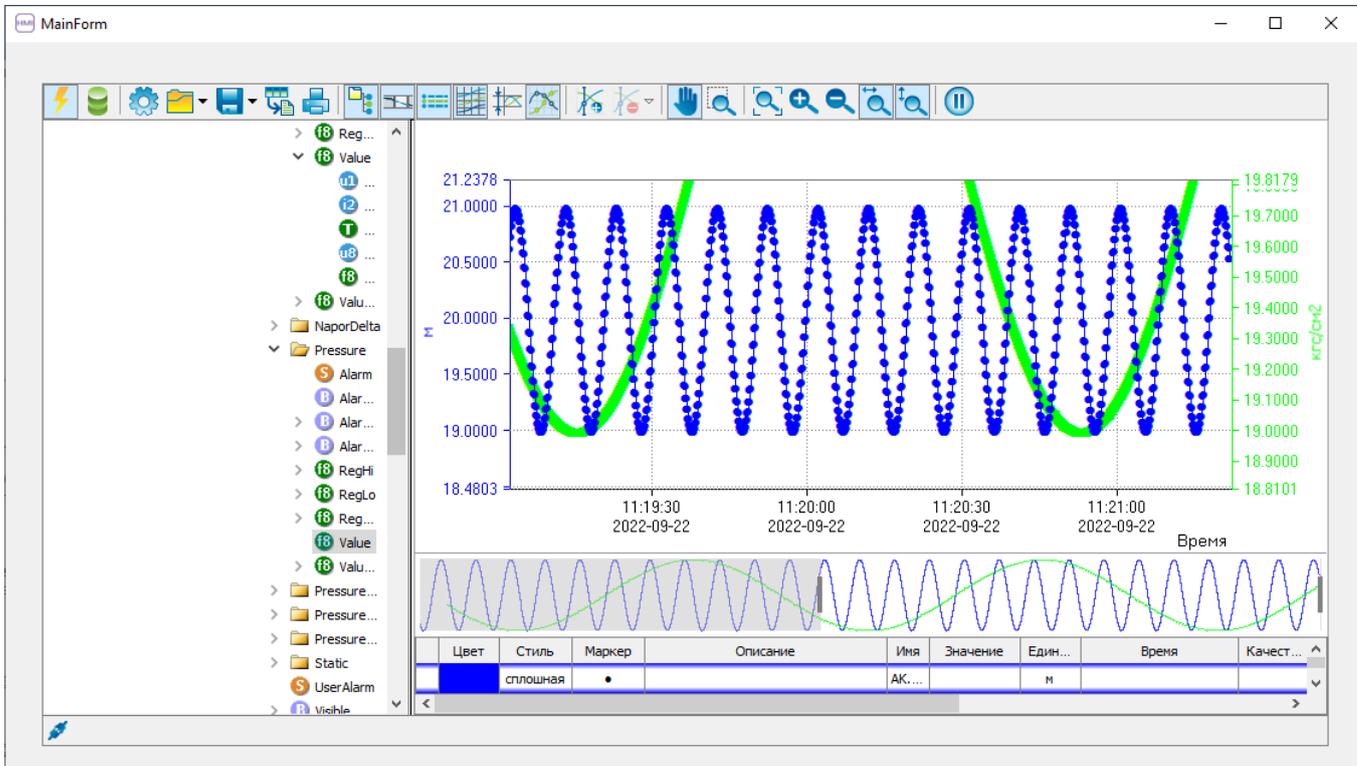
10.2. SePlatform.HMI.Trends

SePlatform.HMI.Trends - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих просматривать графики изменений параметров технологического процесса.

Предоставляемые возможности:

- просмотр графиков изменений параметров в реальном времени;
- просмотр истории значений;

- просмотр данных по сигналам в виде таблицы;
- сохранение списка сигналов и данных по сигналам в файл;
- загрузка списка сигналов и данных по сигналам из файла;
- масштабирование и позиционирование графиков;
- печать графиков.



10.3. SePlatform.HMI.SecurityConfigurator

SePlatform.HMI.SecurityConfigurator позволяет настраивать конфигурацию безопасности на сервере OpenLDAP.

Предоставляемые возможности:

- добавление пользователей/групп пользователей и назначения прав доступа к определенным функциям приложений;
- добавление приложений для отслеживания и контроля доступа пользователей к ним;
- объединение рабочих станций в кластерное рабочее место.

10.4. SePlatform.HMI.SetPoints

SePlatform.HMI.SetPoints - приложение для просмотра и редактирования уставок параметров технологического процесса. SePlatform.HMI.SetPoints можно запустить как отдельное приложение, либо встроить его в проект автоматизации, построенный на SePlatform.HMI.

SePlatform.HMI.SetPoints можно встраивать в проекты, работающие на ОС Windows и ОС Linux и доступные через веб-интерфейс.

The screenshot shows a window titled 'MainForm' with a tree view on the left and a data table on the right. The tree view shows a hierarchy: Санитарно-бытовой корпус > НПС 1 > Магистральные агрегаты > Временные установки > Магистральные нас... The table contains the following data:

Наименование	Идентификатор	Ед. изм.	Нижняя аварийная	Нижняя предупредител...	Нижняя тех...
Давление на напоре 00SRP52CP001	SRP52CP001	МПа			
Давление на напоре 00SRP52CP002	SRP52CP002	МПа			
Давление на напоре 00SRP98CP001	SRP98CP001	МПа			
Температура 00SRP90CT001 первого подшипника насоса	SRP90CT001	°C			
Температура 00SRP90CT002 второго подшипника насоса	SRP90CT002	°C			
Давление на напоре 00SRP98CP002	SRP98CP002	МПа			
Температура 00SRP90CT003 первого подшипника насоса	SRP90CT003	°C			
Температура 00SRP90CT004 второго подшипника насоса	SRP90CT004	°C			
Давление на напоре 00SRP96CP001	SRP96CP001	МПа			
Температура воздуха	SRP93CT001	°C			

10.5. SePlatform.HMI.Explorer

SePlatform.HMI.Explorer - прикладное решение на базе SePlatform.HMI, предназначенное для просмотра и изменения значений сигналов SePlatform.Data collection Server.

10.6. SePlatform.HMI.Charts

SePlatform.HMI.Charts - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих представлять данные, принятые от источника, в виде графиков.

Предоставляемые возможности:

- просмотр графиков оперативных данных по значениям, полученным с локальных и удаленных серверов;
- просмотр графиков исторических данных.

10.7. SePlatform.HMI.Tables

SePlatform.HMI.Tables - расширение среды разработки и исполнения SePlatform.HMI. Представляет собой библиотеку компонентов, позволяющих помещать в таблицу данные об оперативных событиях с источника либо формировать таблицы на основе любых собственных данных.

Предоставляемые возможности:

- заполнение невизуальной таблицы модели данными с источника;
- заполнение невизуальной таблицы модели данными, введенными вручную, для последующего хранения;

- визуализация таблицы, хранящейся в модели данных;
- декорирование визуальной таблицы.

10.8. SePlatform.HMI.IntegrityControl

SePlatform.HMI.IntegrityControl - приложение для ручного запуска контроля целостности файлов и папок на локальных/удаленных узлах и просмотра результатов проверки. Приложение используется как дополнение к компонентам SePlatform.Security и SePlatform.HMI.Security, т.к. контроль целостности выполняется с помощью этих компонентов.

SePlatform.HMI.IntegrityControl можно запустить как отдельное приложение, либо встраивать его в прикладные проекты, разработанные в SePlatform.HMI. Целевыми проектами могут быть проекты, работающие на ОС Windows, ОС Linux, а также доступные через веб-интерфейс.

11. SePlatform.HMI - дополнительные модули

11.1. SePlatform.HMI.Security

SePlatform.HMI.Security обеспечивает возможность разграничения доступа пользователей проекта автоматизации в соответствии с их должностными обязанностями.

Функциональные возможности:

- предоставление возможности редактирования и сохранения конфигурации безопасности на сервер OpenLDAP;
- обращение к серверу OpenLDAP для запроса и получения перечня прав текущего пользователя приложений;
- хранение информации о зарегистрированном пользователе и уведомление всех приложений о смене пользователя;
- контроль целостности файлов.

12. SePlatform.HMI - библиотеки

12.1. SePlatform.HMI.CommonLib

SePlatform.HMI.CommonLib - это расширение среды разработки и исполнения SePlatform.HMI.

Расширение представляет собой библиотеку компонентов, которые можно использовать в своих проектах автоматизации:

- диалоговые окна;
- контекстное меню;
- календарь;
- файловый менеджер;
- конвертер значений;
- дерево сигналов;
- журнал сообщений;
- компоненты безопасности;
- различные кнопки и индикаторы.

Внешний вид и функции компонентов можно настроить с помощью API.

13. SePlatform.Security

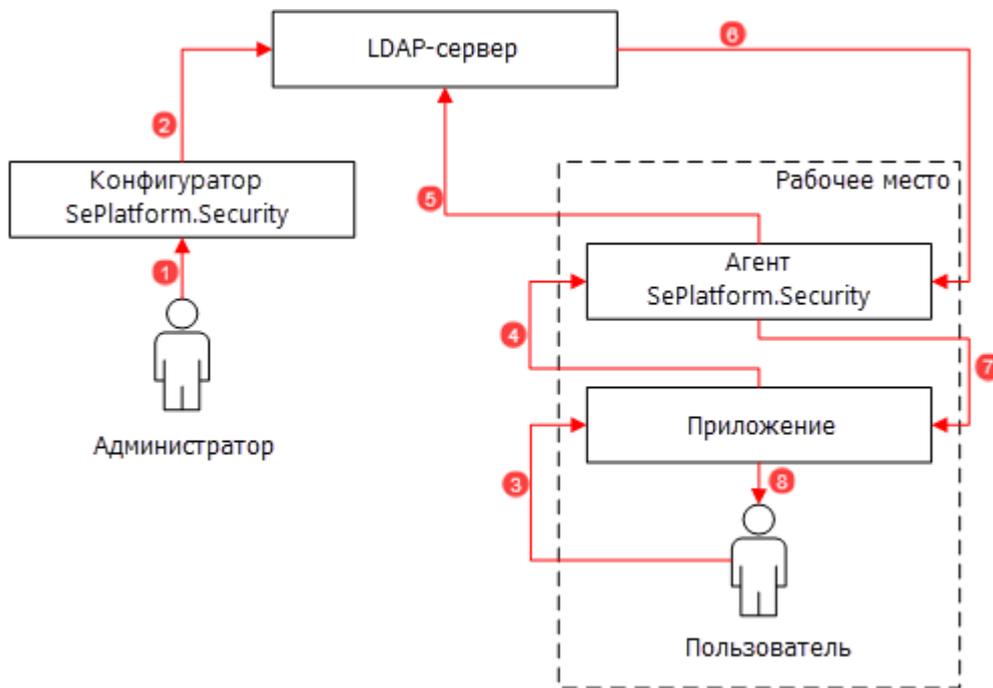
SePlatform.Security - часть инфраструктурной подсистемы SePlatform.Domain, которая обеспечивает окружение для работы других подсистем Систэм Платформ.

SePlatform.Security - система, обеспечивающая разграничение доступа пользователей проекта автоматизации с помощью их должностных инструкций. Система построена на протоколе доступа к каталогам - LDAP-сервер.

SePlatform.Security состоит из следующих компонентов:

- Программа SePlatform.Security.Configurator.
- Служба SePlatform.Security.Agent.

На рисунке ниже показан принцип работы SePlatform.Security.



Цифрами обозначены действия компонентов подсистемы:

№	Действие
1	Администратор вносит приложения и конфигурации прав пользователей для конкретного приложения в программу SePlatform.Security.Configurator.
2	Программа SePlatform.Security.Configurator сохраняет и записывает конфигурацию на LDAP-сервер.
3	Пользователь обращается к какому-либо приложению.
4	Приложение спрашивает у службы SePlatform.Security.Agent значение привилегий пользователя, который обратился к данному приложению.
5	Служба SePlatform.Security.Agent обращается к LDAP-серверу, чтобы он предоставил информацию о привилегиях для данного приложения.

№	Действие
6	LDAP-сервер передает службе SePlatform.Security.Agent запрашиваемую информацию.
7	Служба SePlatform.Security.Agent передает приложению права доступа пользователя, который обратился к данному приложению.
8	Приложение предоставляет пользователю только те данные, на которые у данного пользователя есть привилегии.

13.1. Работа с пользователями

Создание пользователей в системе безопасности производится для назначения прав администратора и выдачи пользователям прав доступа к определенным функциям приложений.

Отображаемое имя	Должность	Подразделение	Группы	Роли
Администратор	Администратор	IT-отдел	Администраторы	
Иванов Иван	Диспетчер	Отдел диспетчеров	Диспетчеры	Диспетчеры
Петров Петр	Оператор	Отдел операторов	Операторы	

13.2. Работа с группами

Создание групп в системе безопасности производится для объединения пользователей со схожими правами доступа к определенным функциям приложений.

Поиск

- [Администраторы](#)
- [Операторы](#)
- [Диспетчеры](#)

Администраторы

Администратор

13.3. Работа с приложениями

Приложения добавляются в систему безопасности для отслеживания и контроля доступа пользователей к ним.

Главная

Назад Вперед Обновить

Приложения Группы Пользователи

Добавить из файла Добавить Удалить

Логическое право Строковое право Добавить роль Сохранить в файл Экспорт в Excel

Навигация Разделы Приложения Права приложения

Поиск приложения

Application
HMI
ShowForms
Приложение для диспетчеров

Приложение для диспетчеров

Поиск права

Тип	Право
B	Ответы на звонки
S	Ответы на звонки от абонентов

14. SePlatform.Domain

Предназначен для выполнения инфраструктурных функций и объединения узлов исполняющих компонентов в единую сеть SePlatform.Net.

Предоставляемые возможности:

- позволяет одновременно разворачивать конфигурацию, построенную с помощью SePlatform.Development Studio, на нескольких экземплярах SePlatform.Data collection Server и SePlatform.AccessPoint;
- позволяет обновлять конфигурации SePlatform.Data collection Server и SePlatform.AccessPoint на узлах сети SePlatform.Net;
- мониторинг состояния работы исполняющих компонентов в домене;
- в связке с SePlatform.Security позволяет организовать единую точку доступа в группе распределенных АРМ.

15. SePlatform.Mapping Server

SePlatform.Mapping Server - компонент Систэм Платформ, с помощью которого возможно представление оперативных значений, истории значений и событий в реляционном виде.

Компонент реализован в виде расширения СУБД PostgreSQL и предоставляет SQL-доступ к данным Систэм Платформ, с возможностью изменения оперативных значений.

16. Лицензирование Систэм Платформ

Лицензия даёт пользователю право установки, запуска и использования компонентов Систэм Платформ в проектах автоматизации. Для получения лицензии необходим сервер лицензирования SePlatform.License Server и лицензионный ключ.

Лицензионный ключ содержит набор лицензий на компоненты Систэм Платформ. SePlatform.License Server запрашивает информацию о наличии лицензии на компонент Систэм Платформ в используемом лицензионном ключе. Полученную информацию о лицензии SePlatform.License Server предоставляет компоненту Систэм Платформ.



Существует два типа лицензионных ключей Систэм Платформ: аппаратный и программный.

Аппаратный ключ - это устройство, которое подключается к компьютеру через USB-разъём. Установка драйвера и активация лицензии для аппаратного ключа не требуется. Для лицензирования компонентов Систэм Платформ, установленных на компьютере, достаточно подключить аппаратный ключ в USB разъем данного компьютера.

Программный ключ - это программный аналог аппаратного ключа, который привязывает компоненты Систэм Платформ к конкретному компьютеру. Для лицензирования компонентов Систэм Платформ, установленных на компьютере, требуется активация лицензии.

Для лицензирования компонентов Систэм Платформ используются два вида лицензионных ключей: Sentinel и Guardant.

16.1. Ключи Sentinel

Для лицензирования компонентов Систэм Платформ используются два типа ключей: аппаратный ключ Sentinel HL и программный ключ Sentinel SL.

16.1.1. ОС Windows

В ОС Windows сервер лицензирования SePlatform.License Server устанавливается вместе с компонентами Систэм Платформ, поэтому отдельная установка SePlatform.License Server не требуется.

16.1.1.1. Аппаратный ключ Sentinel HL

Подключите аппаратный ключ Sentinel HL в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

Обновление лицензии

Обновление набора лицензий аппаратного ключа выполняется через web-интерфейс **Sentinel Admin Control Center**, который доступен по адресу <http://127.0.0.1:1947/> после установки драйвера Sentinel HASP.



ПРИМЕЧАНИЕ

Если драйвер Sentinel HASP не был установлен ранее, установите его, запустив установочный файл `HASPUserSetup.exe`.

Установочный файл на поставочном диске Систэм Платформ расположен в папке `\Сторонние компоненты\HASPDriver`. Также загрузить архив с драйвером для Windows `Sentinel_LDK_Run-time_setup.zip` можно со страниц:

- <https://cpl.thalesgroup.com/software-monetization/sentinel-drivers>
- <https://www.euromobile.ru/download-center/>

1. На компьютере с подключенным ключом в web-браузере откройте страницу <http://127.0.0.1:1947/>.

1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)	662678384	Sentinel HL Max	Без драйвера	6.09		Продукты Компоненты Сеансы Диагн. вкл. C2V

1.2. Сохраните файл образа ключа формата `*.c2v` на диске.



ПРИМЕЧАНИЕ

`*.c2v` - «Customer To Vendor» - файл образа ключа

Если кнопка **C2V** отсутствует в web-интерфейсе, то в разделе **Конфигурация** установите флаг **Создать файл C2V для ключа HASP** и нажмите кнопку **Применить**:



ПРИМЕЧАНИЕ

В ОС Windows при отсутствии в web-интерфейсе кнопки C2V для обновления набора лицензий аппаратного ключа можно воспользоваться утилитой SePlatform Soft Rus.exe.

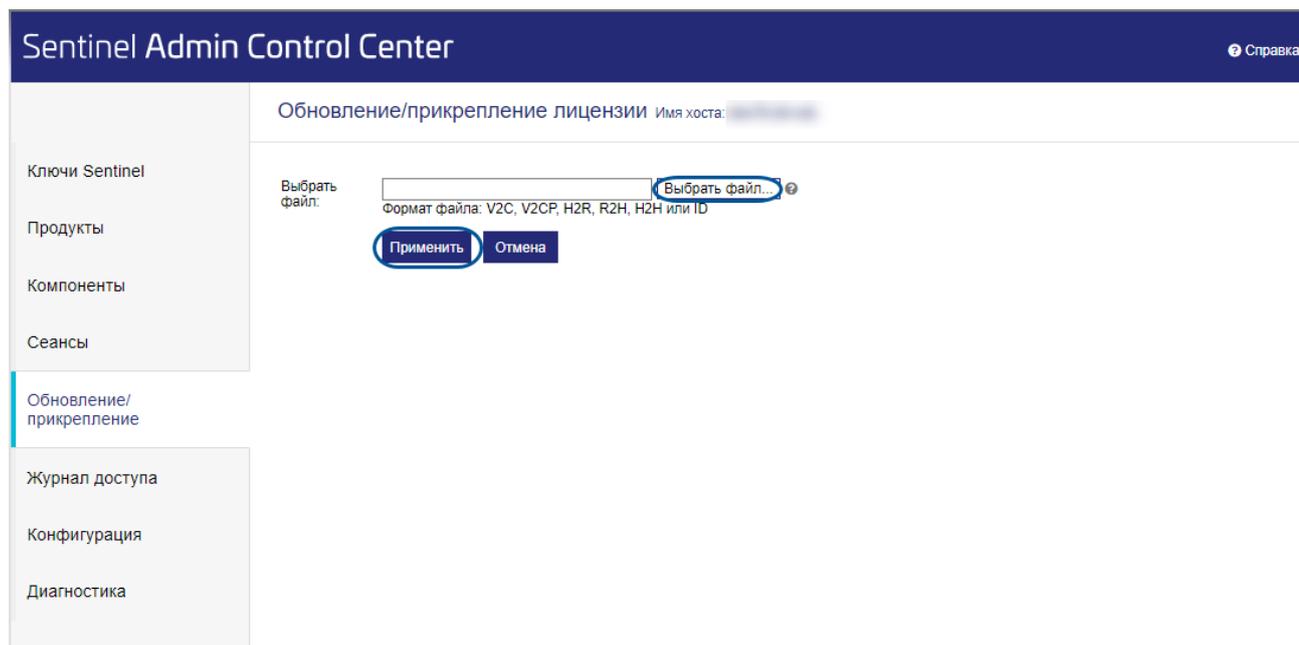
2. Сгенерированный файл образа ключа формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл обновления набора лицензий формата *.v2c.



ПРИМЕЧАНИЕ

*.v2c - «Vendor To Customer» - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата *.v2c и нажмите кнопку **Применить**.



4. Перезапустите службу сервера лицензирования **SePlatform.LicenseServer.Agent**, после чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

16.1.1.2. Программный ключ Sentinel SL

Для работы программного ключа Sentinel SL необходимо установить драйвер Sentinel HASP.

Активация и обновление набора лицензий программного ключа Sentinel SL выполняется через web-интерфейс **Sentinel Admin Control Center**, который доступен по адресу <http://127.0.0.1:1947/> после установки драйвера Sentinel HASP.

В ОС Windows для активации, обновления и переноса на другой компьютер программного ключа Sentinel SL Систэм Платформ можно использовать утилиту SePlatform Soft Rus.exe.



ОБРАТИТЕ ВНИМАНИЕ

Программный ключ Sentinel SL может быть активирован только на одном компьютере.

Установка драйвера Sentinel HASP

Чтобы установить драйвер Sentinel HASP, запустите установочный файл HASPUserSetup.exe, который на поставочном диске Систэм Платформ расположен в папке \Сторонние компоненты\HASPDriver. Также загрузить архив с драйвером для Windows Sentinel_LDK_Run-time_setup.zip можно со страниц:

- <https://cpl.thalesgroup.com/software-monetization/sentinel-drivers>
- <https://www.euromobile.ru/download-center/>

Активация

1. На компьютере в web-браузере откройте страницу <http://127.0.0.1:1947/>.

1.1. В разделе **Ключи Sentinel** для нового ключа SL нажмите кнопку **Отпечаток**.

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)		Зарезервировано для нового ключа SL	SL	8.43		Отпечаток

1.2. Сохраните файл формата *.c2v на диске.

✓ **ПРИМЕЧАНИЕ**
*.c2v - «Customer To Vendor» - файл образа системы

2. Сгенерированный файл образа системы формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл активации лицензии формата *.v2c.

✓ **ПРИМЕЧАНИЕ**
*.v2c - «Vendor To Customer» - файл активации лицензии

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл активации лицензии формата *.v2c и нажмите кнопку **Применить**.

4. Перезапустите службу сервера лицензирования **SePlatform.LicenseServer.Agent**, после чего программный ключ Sentinel SL будет активирован.

Обновление

1. На компьютере в web-браузере откройте страницу <http://127.0.0.1:1947/>.

1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)	557399356746929321	HASP SL AdminMode Переносимый		2.36		Продукты Компоненты Сеансы Сертификаты C2V

1.2. Сохраните файл образа ключа формата *.c2v на диске.



ПРИМЕЧАНИЕ

*.c2v - «Customer To Vendor» - файл образа ключа

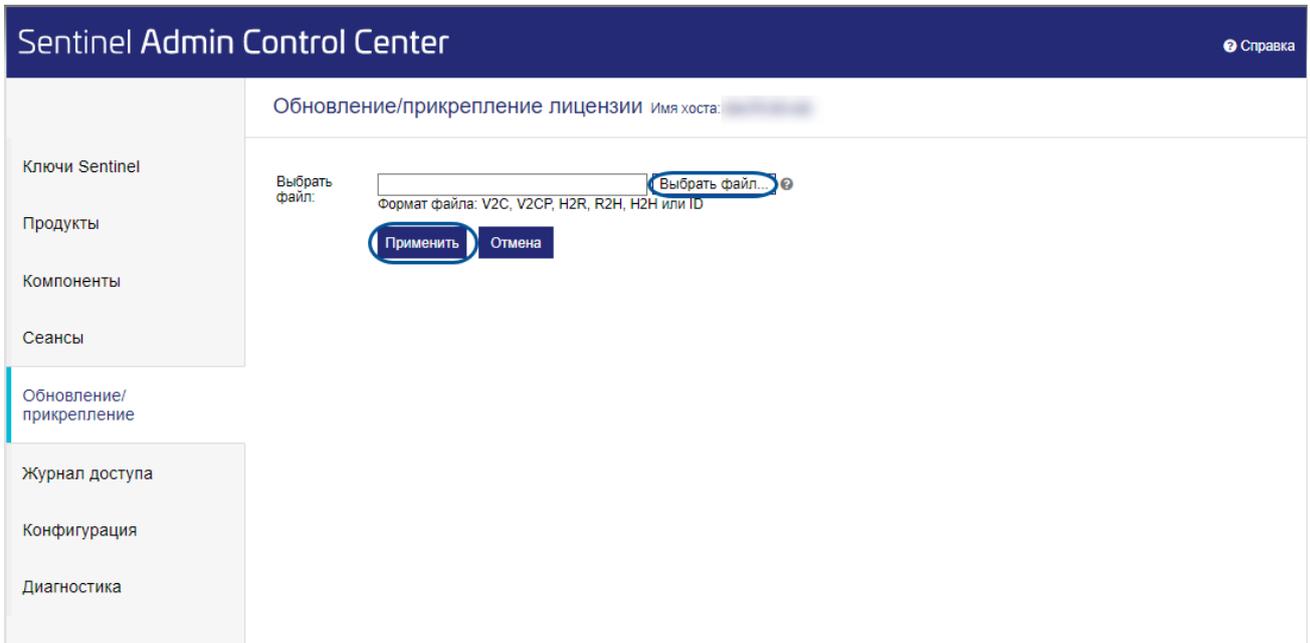
- Сгенерированный файл образа ключа формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл обновления набора лицензий формата *.v2c.



ПРИМЕЧАНИЕ

*.v2c - «Vendor To Customer» - файл набора лицензий

- Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата *.v2c и нажмите кнопку **Применить**.



- Перезапустите службу сервера лицензирования **SePlatform.LicenseServer.Agent**, после чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

Утилита SePlatform Soft Rus.exe

В ОС Windows для активации, обновления и переноса на другой компьютер программного ключа Sentinel SL Систэм Платформ может использоваться утилита SePlatform Soft Rus.exe, которая на поставочном диске Систэм Платформ расположена в папке \Сторонние компоненты\HASPDriver\SePlatform Soft Rus.



ПРИМЕЧАНИЕ

Если в процессе работы с утилитой появилось сообщение «**Ошибка обновления: Библиотека производителя не найдена**», то из папки утилиты скопируйте файл haspvlib_XXXXXX.dll в папку C:\Program Files (x86)\Common Files\Aladdin Shared\HASP.

Активация

- Запустите утилиту SePlatform Soft Rus.exe.
- На вкладке **Сбор информации** выберите переключатель **Установить новый ключ защиты** и нажмите кнопку **Собрать информацию**.

3. В открывшемся окне укажите место сохранения, имя файла и нажмите кнопку **Сохранить**. Файл формата *.c2v будет сохранен на диск.



ПРИМЕЧАНИЕ

*.c2v - «Customer To Vendor» - файл образа ключа

4. Отправьте на электронную почту support@systeme.ru письмо, содержащее:

- ключ продукта, указанный в сертификате из комплекта поставки;
- сохраненный файл формата *.c2v.

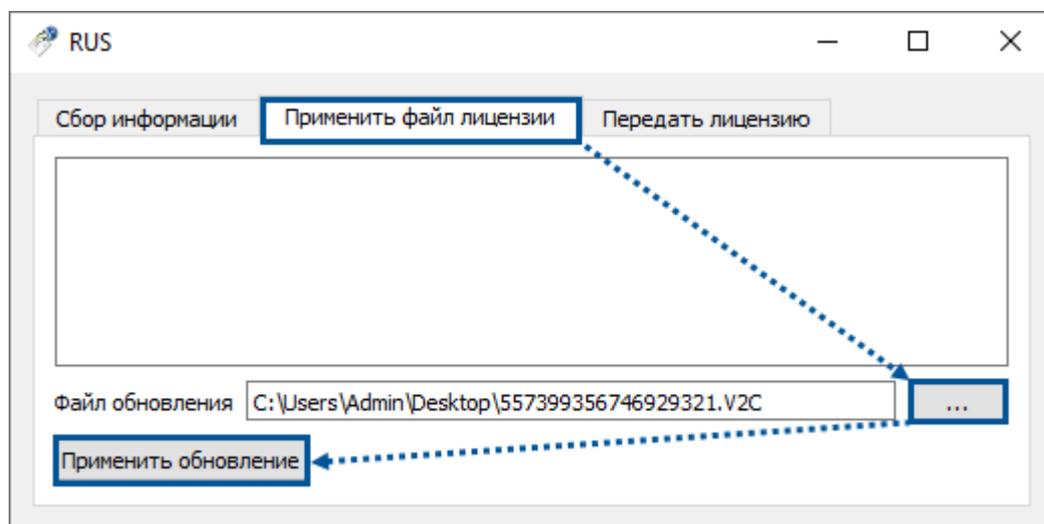
5. В ответном письме будет выслан файл формата *.v2c.



ПРИМЕЧАНИЕ

*.v2c - «Vendor To Customer» - файл набора лицензий

6. На вкладке **Применить файл лицензии** утилиты SePlatform Soft Rus.exe нажмите кнопку , выберите полученный файл формата *.v2c и нажмите кнопку **Применить обновление**.



Программный ключ Sentinel SL активирован.

7. Перезапустите службу сервера лицензирования SePlatform.LicenseServer.Agent.

Обновление лицензии

1. Запустите утилиту SePlatform Soft Rus.exe.

2. На вкладке **Сбор информации** выберите переключатель **Обновить существующий ключ защиты** и нажмите кнопку **Собрать информацию**.

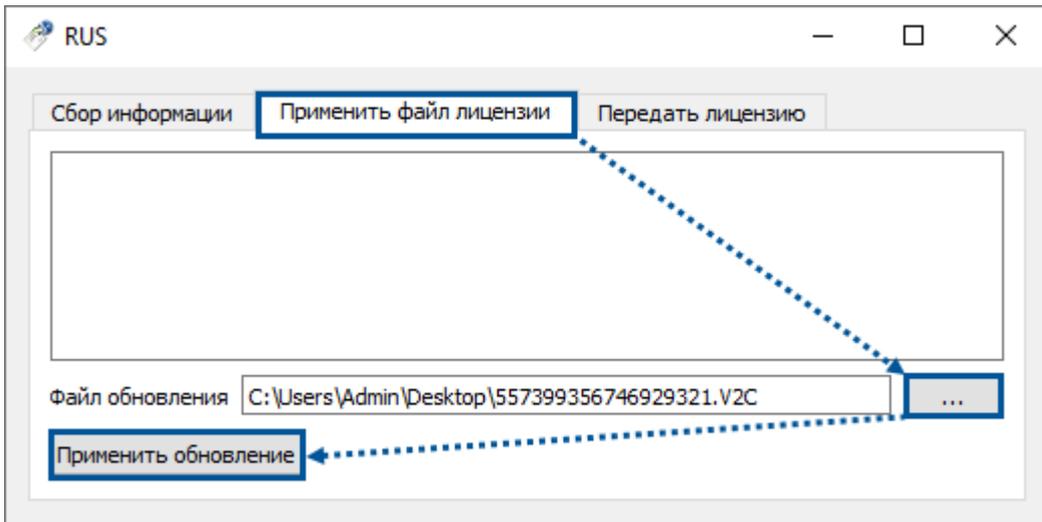
3. В открывшемся окне укажите место сохранения, имя файла образа ключа и нажмите кнопку **Сохранить**. Файл формата *.c2v будет сохранен на диск.

4. Отправьте на электронную почту support@systeme.ru письмо, содержащее:

- ключ продукта, указанный в сертификате из комплекта поставки;
- сохраненный файл формата *.c2v.

5. В ответном письме будет выслан файл обновления набора лицензий формата *.v2c.

6. На вкладке **Применить файл лицензии** утилиты SePlatform Soft Rus.exe нажмите кнопку , выберите полученный файл обновления набора лицензий формата *.v2c и нажмите кнопку **Применить обновление**.



Набор лицензий программного ключа Sentinel SL обновлён.

7. Перезапустите службу сервера лицензирования SePlatform.LicenseServer.Agent.

Перенос программного ключа на другой компьютер



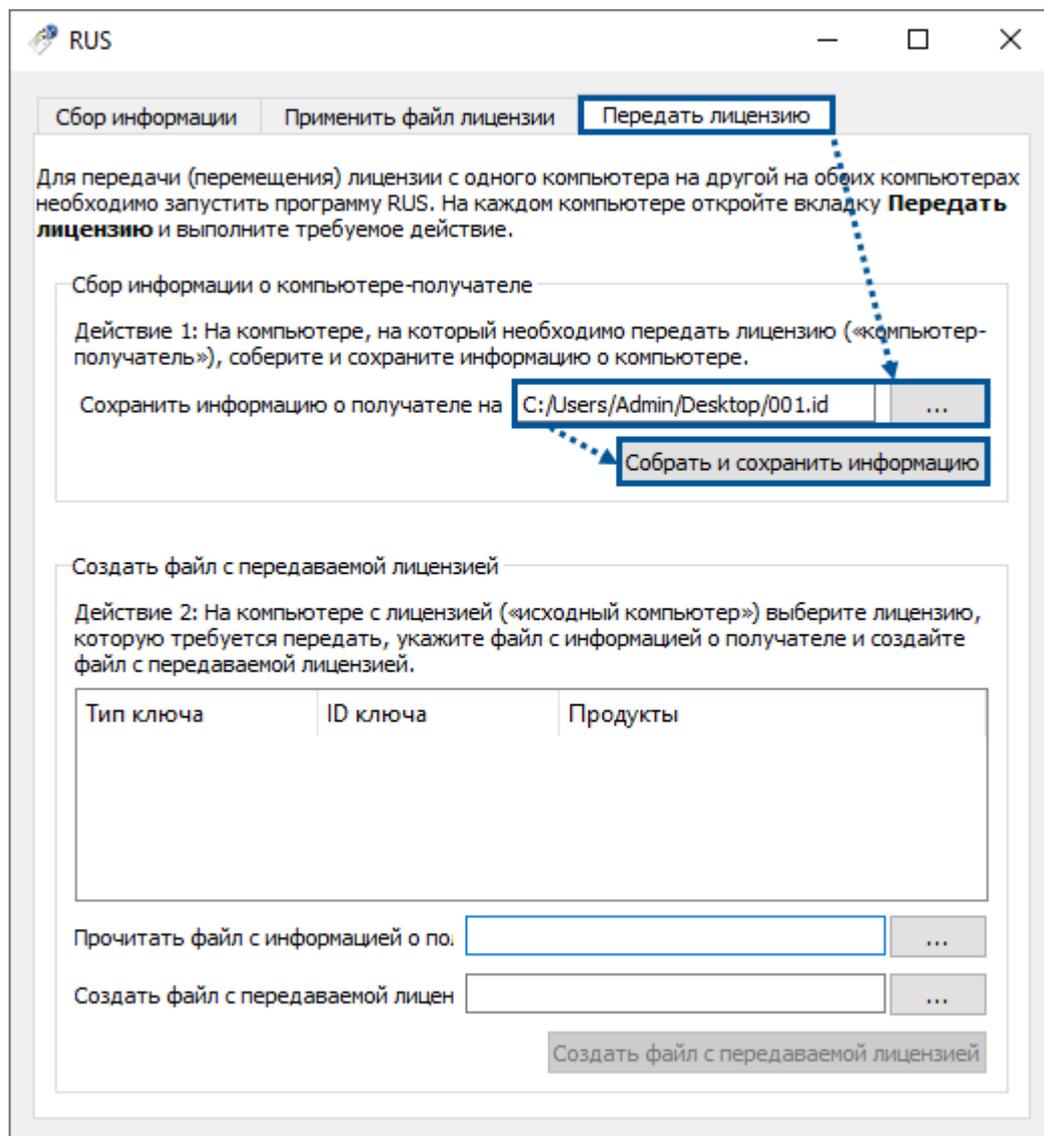
ОБРАТИТЕ ВНИМАНИЕ

На компьютере, на который требуется перенести программный ключ, должен быть установлен драйвер Sentinel HASP.

1. Запустите утилиту SePlatform Soft Rus.exe на компьютере, на который требуется перенести программный ключ.

2. На вкладке **Передать лицензию** выполните генерацию ID-файла с информацией о системе. Для этого нажмите кнопку **...**, укажите имя и путь для сохранения файла формата *.id и нажмите кнопку

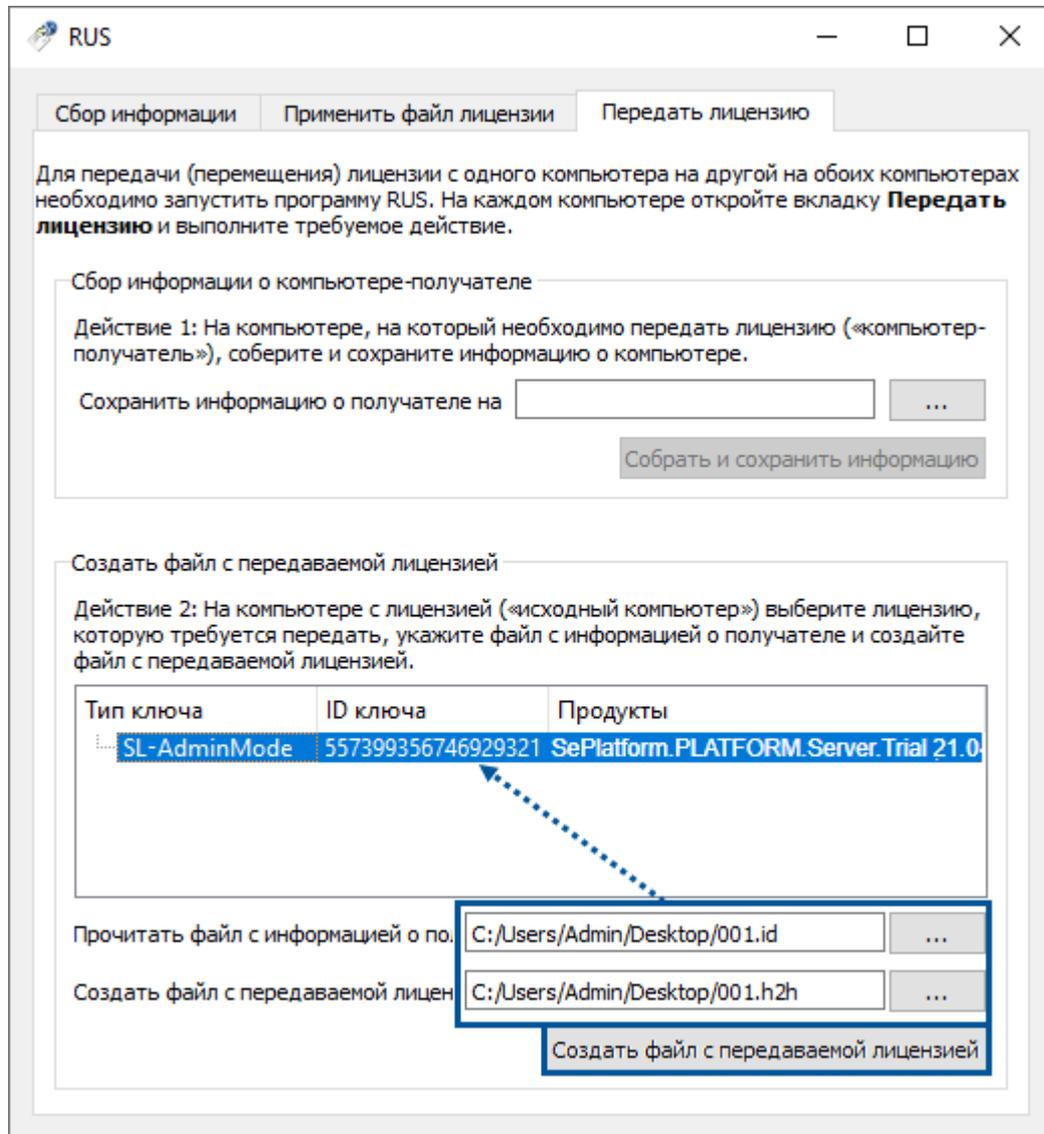
Собрать и сохранить информацию.



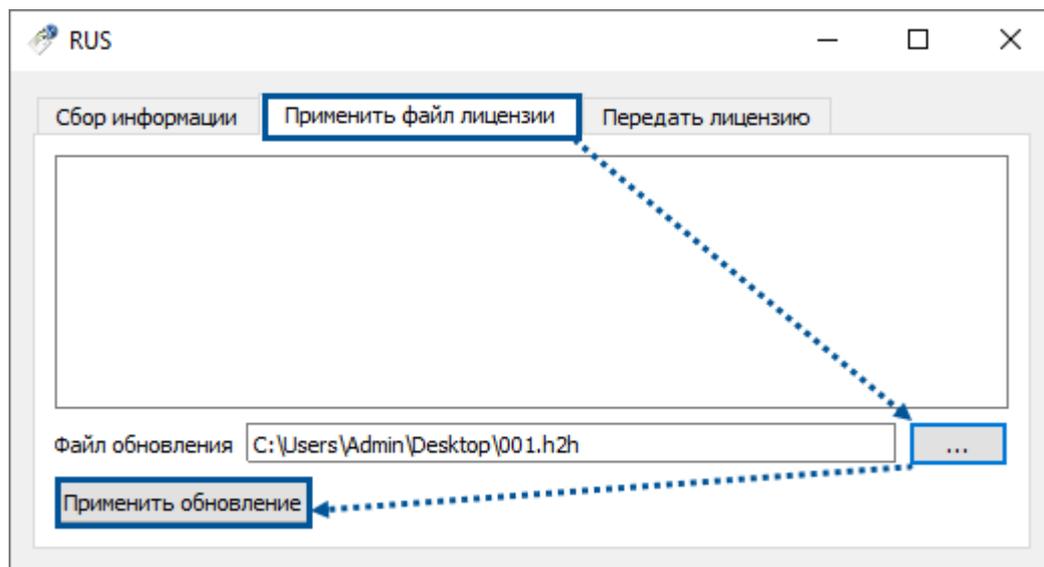
3. Запустите утилиту SePlatform Soft Rus.exe на компьютере, с которого требуется перенос программного ключа.

4. На вкладке **Передать лицензию**:

- укажите путь до файла формата *.id, сгенерированного на компьютере, на который требуется перенести программный ключ;
- укажите путь и имя для сохранения файла с ключом формата *.h2h;
- из списка ключей выберите ключ, который требуется перенести;
- выполните генерацию файла с переносимым ключом формата *.h2h, нажав кнопку **Создать файл с передаваемой лицензией**.



5. На компьютере, на который требуется перенести программный ключ, примените файл с переносимым ключом. Для этого на вкладке **Применить файл лицензии** нажмите кнопку , выберите сгенерированный файл формата *.h2h и нажмите кнопку **Применить обновление**.



Программный ключ Sentinel SL перенесен.

6. Перезапустите службу сервера лицензирования SePlatform.LicenseServer.Agent.

16.1.2. ОС Linux

Для лицензирования компонентов Систэм Платформ, установленных на компьютере с ОС Linux:

- установите сервер лицензирования SePlatform.License Server;
- установите драйвер Sentinel HASP.

16.1.2.1. Установка SePlatform.License Server

Установите сервер лицензирования, установочные пакеты которого на поставочном диске Систэм Платформ расположены в папке \SePlatform\SePlatform.License Server\x.x.x.



ОБРАТИТЕ ВНИМАНИЕ

Команда установки выполняется только от суперпользователя «root».

Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером. Установка пакета *.rpm с помощью пакетного менеджера YUM:

```
yum install seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета *.rpm с помощью пакетного менеджера RPM:

```
rpm -i seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета *.deb с помощью пакетного менеджера apt:

```
apt-get install seplatform.licensing.agent-x.x.x+xx.xxxxxx.deb
```

Установка пакета *.deb с помощью пакетного менеджера dpkg:

```
sudo dpkg -i seplatform.licensing.agent-x.x.x+xx.xxxxxx.deb
```

16.1.2.2. Установка драйвера Sentinel HASP

Чтобы установить драйвер Sentinel HASP:

1. Со страницы <https://cpl.thalesgroup.com/software-monetization/sentinel-drivers> или <https://www.euromobile.ru/download-center/> загрузите архив с драйвером для Linux Linux Sentinel_LDK_Run-time_linux.zip. При этом загруженный файл архива будет называться Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz.
2. Распакуйте загруженный архив Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz.
3. Распакуйте архив aksusbd-x.xx.x.tar.gz.
4. В папку с файлом dinst скопируйте файл библиотеки haspvlib_x86_64_xxxxxx.so, который на поставочном диске Систэм Платформ находится в папке \Сторонние компоненты\HASPDriver\linux-vlib.
5. Находясь в папке с файлами dinst и haspvlib_x86_64_xxxxxx.so, от суперпользователя «root» выполните команду:

```
./dinst .
```

16.1.2.3. Аппаратный ключ Sentinel HL

Подключите аппаратный ключ Sentinel HL в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

Обновление лицензии

Обновление набора лицензий аппаратного ключа выполняется через web-интерфейс **Sentinel Admin Control Center**, который доступен по адресу <http://127.0.0.1:1947/> после установки драйвера Sentinel HASP.

1. На компьютере с подключенным ключом в web-браузере откройте страницу <http://127.0.0.1:1947/>.
 - 1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.

Sentinel Admin Control Center Справка

Ключи Sentinel Имя хоста: [скрыто]

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)	662678384	Sentinel HL Max	Без драйвера	6.09		Продукты Компоненты Сеансы Диагн. вкл. C2V

1.2. Сохраните файл образа ключа формата *.c2v на диске.



ПРИМЕЧАНИЕ

*.c2v - «Customer To Vendor» - файл образа ключа

Если кнопка **C2V** отсутствует в web-интерфейсе, то в разделе **Конфигурация** установите флаг **Создать файл C2V для ключа HASP** и нажмите кнопку **Применить**:

Thales Sentinel ACC: Конфигура: x

localhost:1947/ru.17.0.alp/config.html

Дни до удаления старых файлов: 90

Записать PID в файл:

Создать файл C2V для ключа HASP Не включайте этот параметр, если только иное не рекомендовано производителем программного обеспечения.

Не загружать hasplmv.exe Примечание: ключи SL UserMode не будут видимы, если выбран этот параметр.

Применить Отмена Сбросить настройки

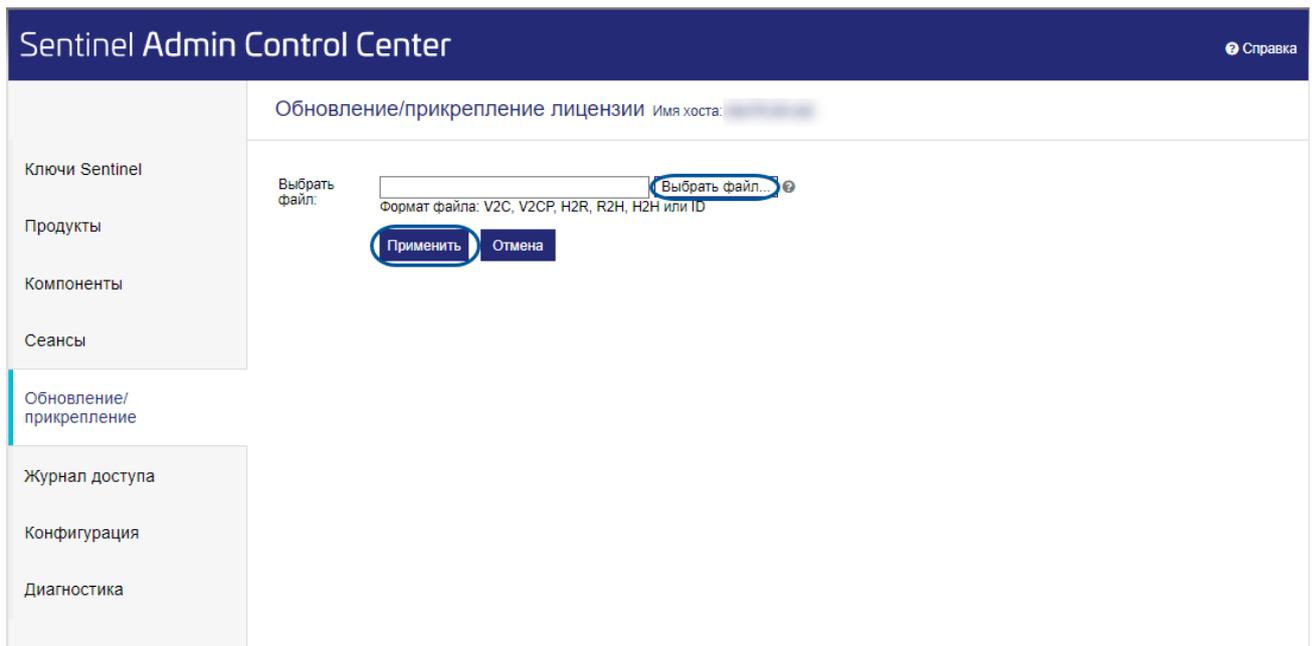
2. Сгенерированный файл образа ключа формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл обновления набора лицензий формата *.v2c.



ПРИМЕЧАНИЕ

*.v2c - «Vendor To Customer» - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата *.v2c и нажмите кнопку **Применить**.



The screenshot shows the 'Sentinel Admin Control Center' interface. The main header is dark blue with the title 'Sentinel Admin Control Center' and a 'Справка' (Help) link. A left sidebar contains navigation items: 'Ключи Sentinel', 'Продукты', 'Компоненты', 'Сеансы', 'Обновление/прикрепление' (highlighted), 'Журнал доступа', 'Конфигурация', and 'Диагностика'. The main content area is titled 'Обновление/прикрепление лицензии' and includes a host name field. Below this is a 'Выбрать файл:' label, an empty text input field, and a 'Выбрать файл...' button. Underneath, it specifies 'Формат файла: V2C, V2CP, H2R, R2H, H2H или ID'. At the bottom of this section are 'Применить' and 'Отмена' buttons.

4. Перезапустите сервис `seplatform.licenseserver.agent` командой:

```
systemctl restart seplatform.licenseserver.agent
```

После чего набор лицензий аппаратного ключа Sentinel HL будет обновлен.

16.1.2.4. Программный ключ Sentinel SL

Активация и обновление набора лицензий программного ключа Sentinel SL выполняется через web-интерфейс **Sentinel Admin Control Center**, который доступен по адресу `http://127.0.0.1:1947/` после установки драйвера Sentinel HASP.



ОБРАТИТЕ ВНИМАНИЕ

Программный ключ Sentinel SL может быть активирован только на одном компьютере.

Активация

1. На компьютере в web-браузере откройте страницу `http://127.0.0.1:1947/`.
 - 1.1. В разделе **Ключи Sentinel** для нового ключа SL нажмите кнопку **Отпечаток**.

Sentinel Admin Control Center ? Справка

Ключи Sentinel Имя хоста: [redacted]

Ключи Sentinel

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)		Зарезервировано для нового ключа SL	SL	8.43		Отчетчик

Продукты

Компоненты

Сеансы

Обновление/прикрепление

Журнал доступа

Конфигурация

Диагностика

1.2. Сохраните файл формата *.c2v на диске.



ПРИМЕЧАНИЕ

*.c2v - «Customer To Vendor» - файл образа системы

- Сгенерированный файл образа системы формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл активации лицензии формата *.v2c.



ПРИМЕЧАНИЕ

*.v2c - «Vendor To Customer» - файл активации лицензии

- Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл активации лицензии формата *.v2c и нажмите кнопку **Применить**.

Sentinel Admin Control Center ? Справка

Обновление/прикрепление лицензии Имя хоста: [redacted]

Выбор файла:

[Выбрать файл...](#)

Формат файла: V2C, V2CP, H2R, R2H, H2H или ID

[Применить](#) [Отмена](#)

Ключи Sentinel

Продукты

Компоненты

Сеансы

Обновление/прикрепление

Журнал доступа

Конфигурация

Диагностика

- Перезапустите сервис `seplatform.licenseserver.agent` командой:

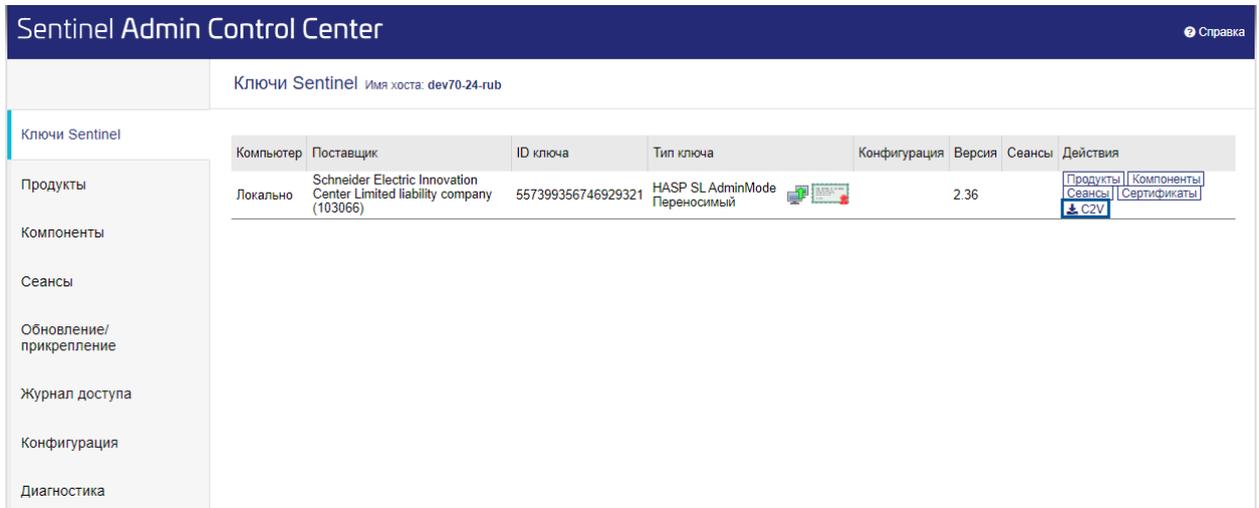
```
systemctl restart seplatform.licenseserver.agent
```

После чего программный ключ Sentinel SL будет активирован.

Обновление

1. На компьютере в web-браузере откройте страницу <http://127.0.0.1:1947/>.

1.1. В разделе **Ключи Sentinel** для нужного ключа нажмите кнопку **C2V**.



Sentinel Admin Control Center Справка

Ключи Sentinel Имя хоста: dev70-24-rub

Компьютер	Поставщик	ID ключа	Тип ключа	Конфигурация	Версия	Сеансы	Действия
Локально	Schneider Electric Innovation Center Limited liability company (103066)	557399356746929321	HASP SL AdminMode Переносимый		2.36		Продукты Компоненты Сеансы Сертификаты C2V

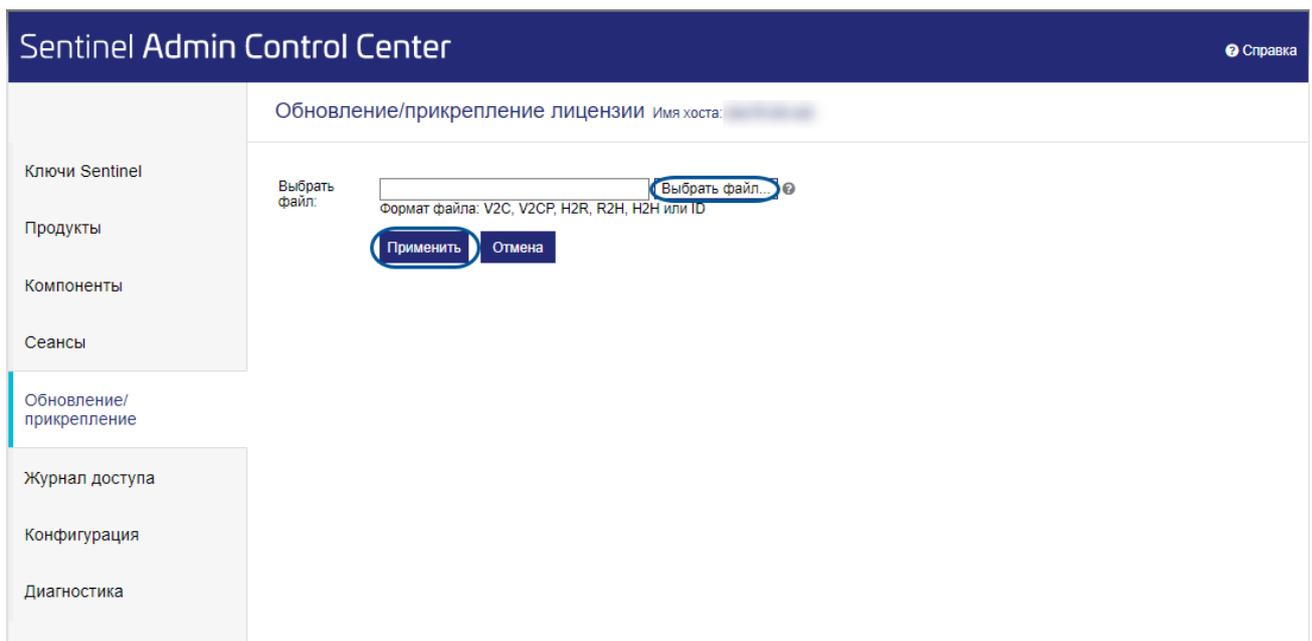
1.2. Сохраните файл образа ключа формата *.c2v на диске.

 **ПРИМЕЧАНИЕ**
*.c2v - «Customer To Vendor» - файл образа ключа

2. Сгенерированный файл образа ключа формата *.c2v отправьте на электронную почту support@systeme.ru. В ответном письме будет выслан файл обновления набора лицензий формата *.v2c.

 **ПРИМЕЧАНИЕ**
*.v2c - «Vendor To Customer» - файл набора лицензий

3. Перейдите в раздел **Обновление/прикрепление**. Нажмите кнопку **Выбрать файл...**, выберите полученный файл обновления набора лицензий формата *.v2c и нажмите кнопку **Применить**.



Sentinel Admin Control Center Справка

Обновление/прикрепление лицензии Имя хоста: [redacted]

Выбрать файл: [Выбрать файл...](#)

Формат файла: V2C, V2CP, H2R, R2H, H2H или ID

[Применить](#) [Отмена](#)

4. Перезапустите сервис `seplatform.licenseserver.agent` командой:

```
systemctl restart seplatform.licenseserver.agent
```

После чего набор лицензий программного ключа Sentinel SL будет обновлен.

16.2. Ключи Guardant

Для лицензирования компонентов Систэм Платформ используются два типа ключей: аппаратный ключ Guardant Sign и программный ключ Guardant DL.

16.2.1. ОС Windows

В ОС Windows сервер лицензирования SePlatform.License Server устанавливается вместе с компонентами Систэм Платформ, поэтому отдельная установка SePlatform.License Server не требуется.

16.2.1.1. Аппаратный ключ Guardant Sign

Подключите аппаратный ключ Guardant Sign в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

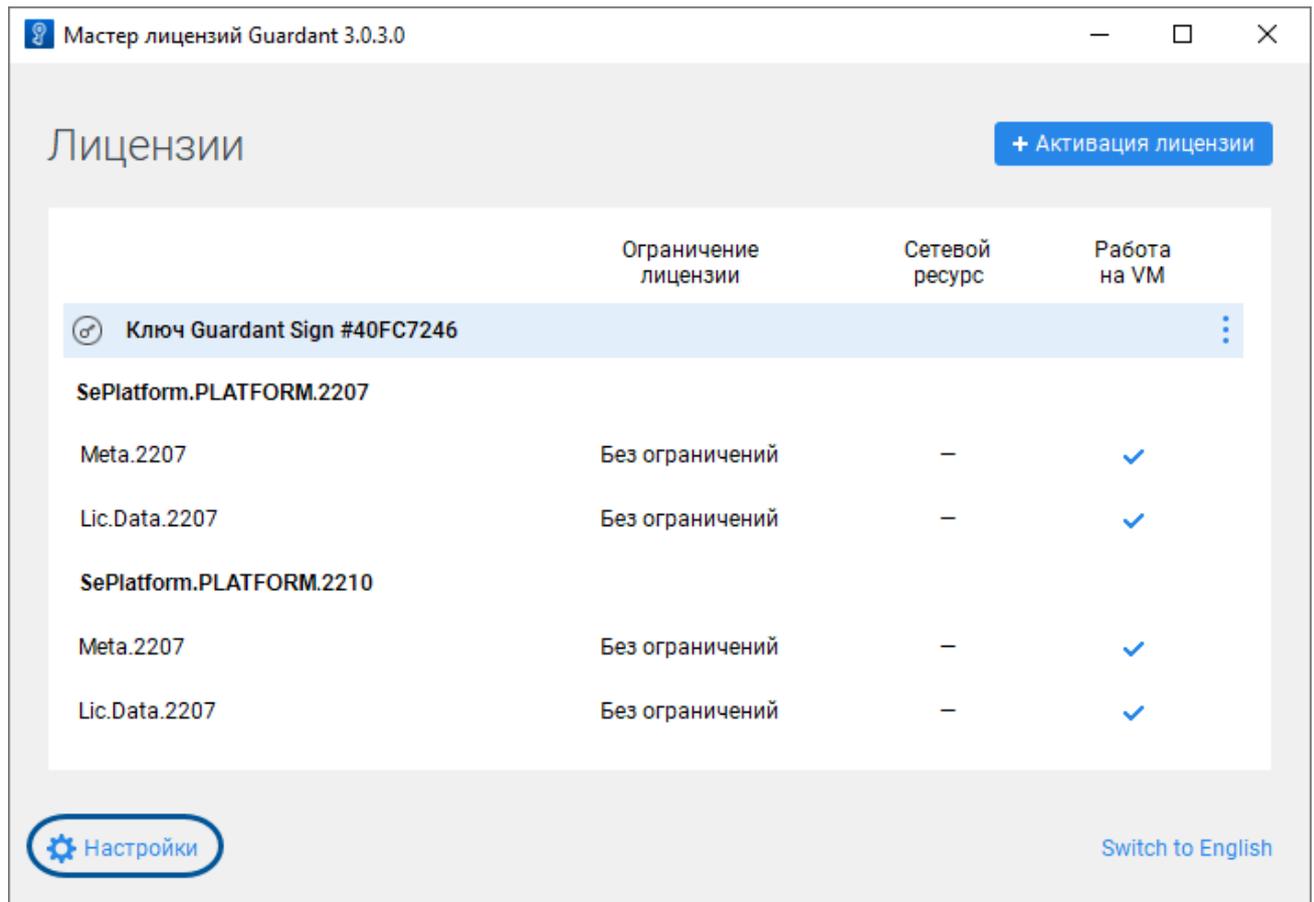
Обновление



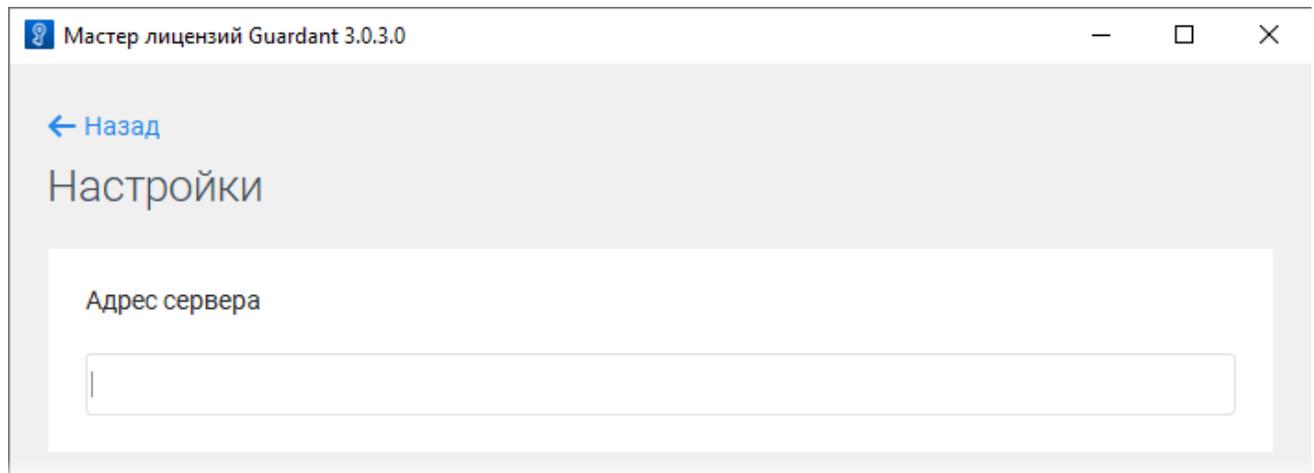
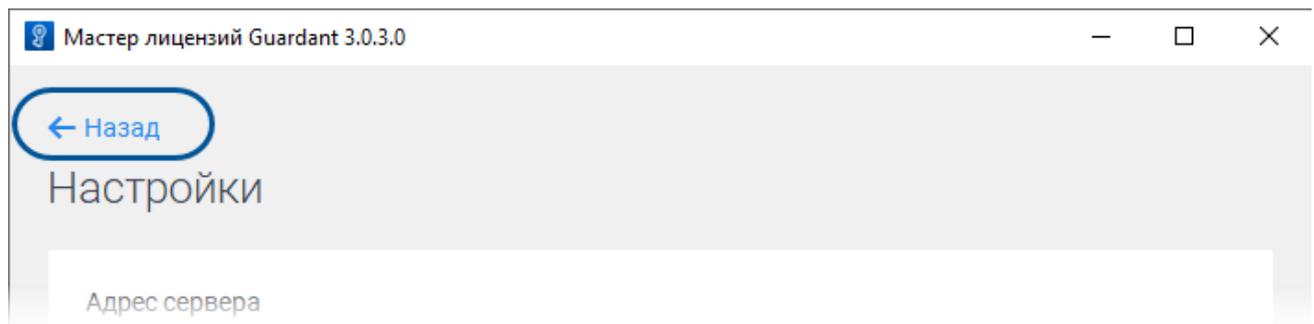
ОБРАТИТЕ ВНИМАНИЕ

Для обновления состава лицензии аппаратного ключа Guardant Sign требуется подключение к сети Интернет.

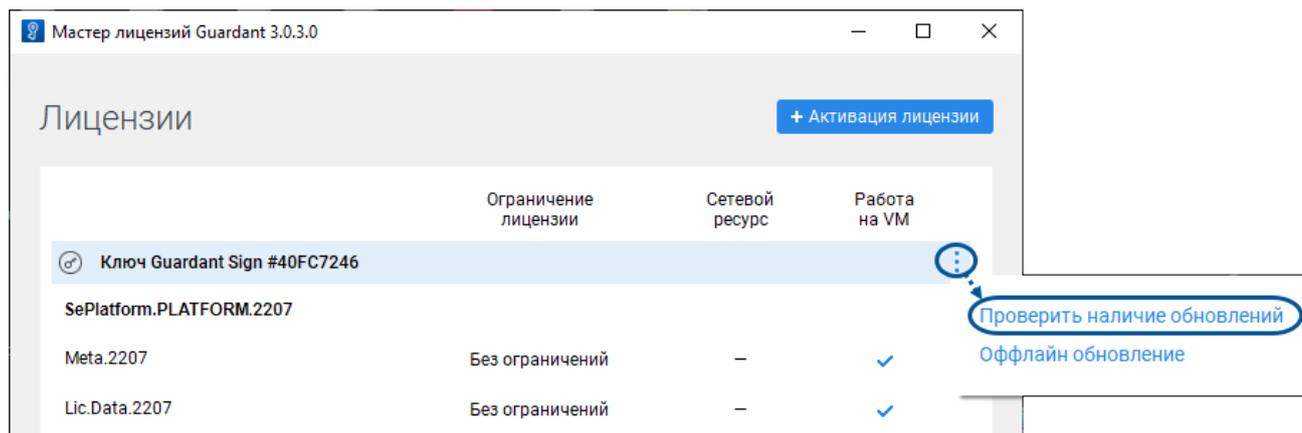
1. Запустите Мастер лицензий Guardant - приложение `license_wizard.exe`, которое на поставочном диске Систэм Платформ расположено в папке `\Стронние компоненты\Guardant\license_activation`.

2. Перейдите в **Настройки**:

3. Укажите адрес сервера обновления лицензий.

4. Вернитесь в окно **Лицензии**, нажав **Назад**.

5. В меню ключа выберите команду **Проверить наличие обновлений**.



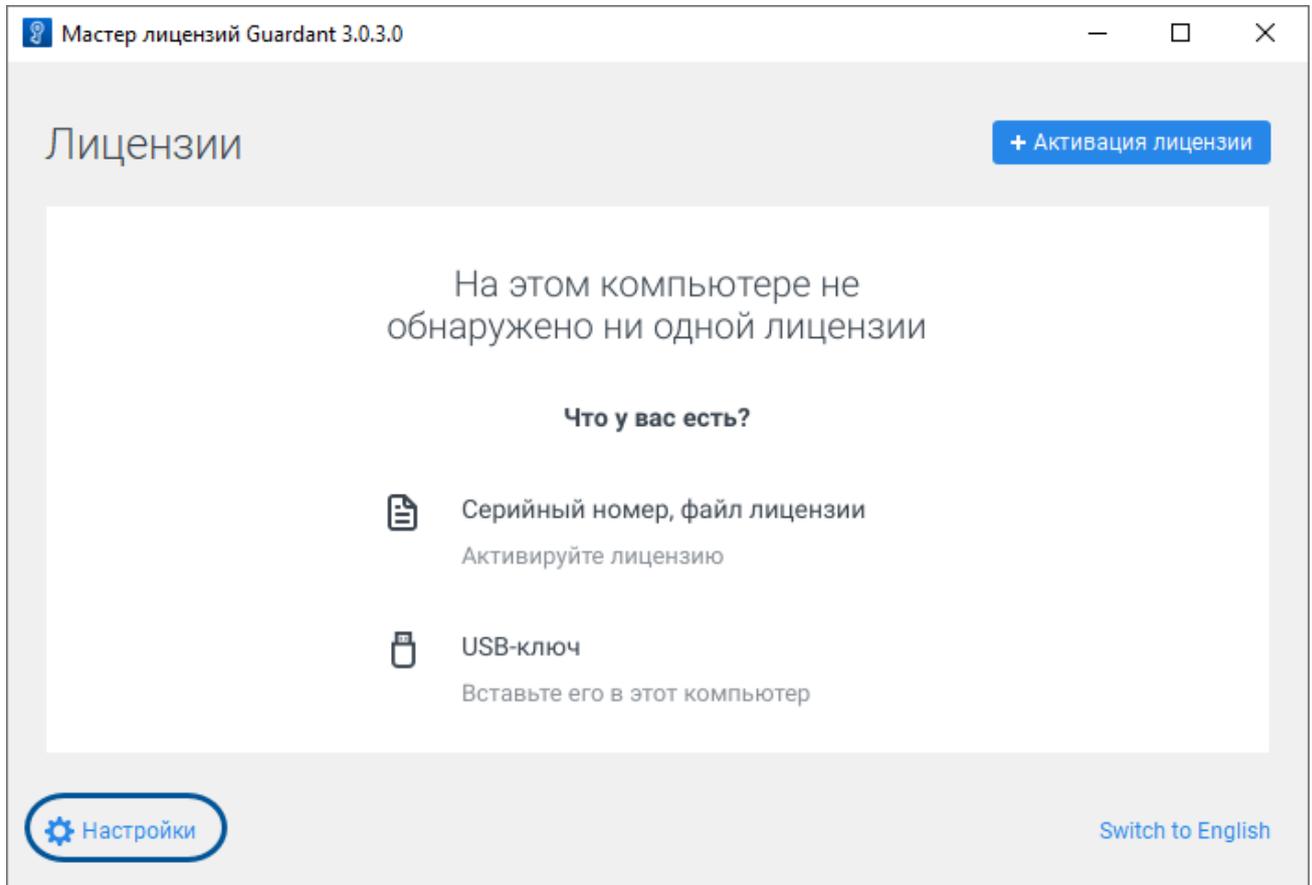
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

16.2.1.2. Программный ключ Guardant DL

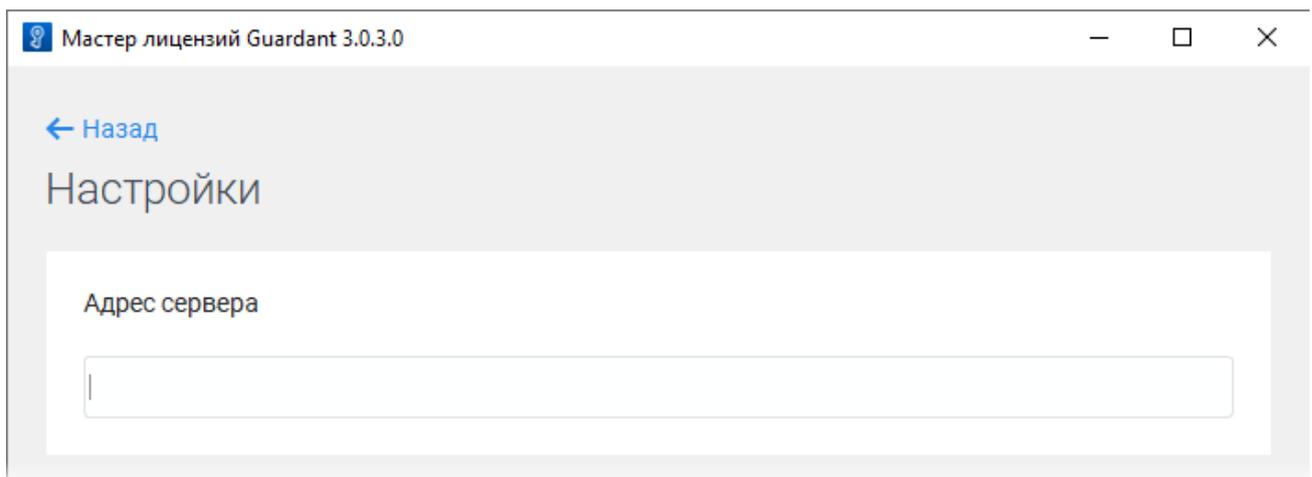
Активация, обновление и перенос лицензии программного ключа Guardant DL выполняется в приложении Мастер лицензий Guardant - `license_wizard.exe`, которое на поставочном диске Систэм Платформ расположено в папке `\Сторонние компоненты\Guardant\license_activation`.

Активация на компьютере с доступом в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



3. Укажите адрес сервера обновления лицензий.



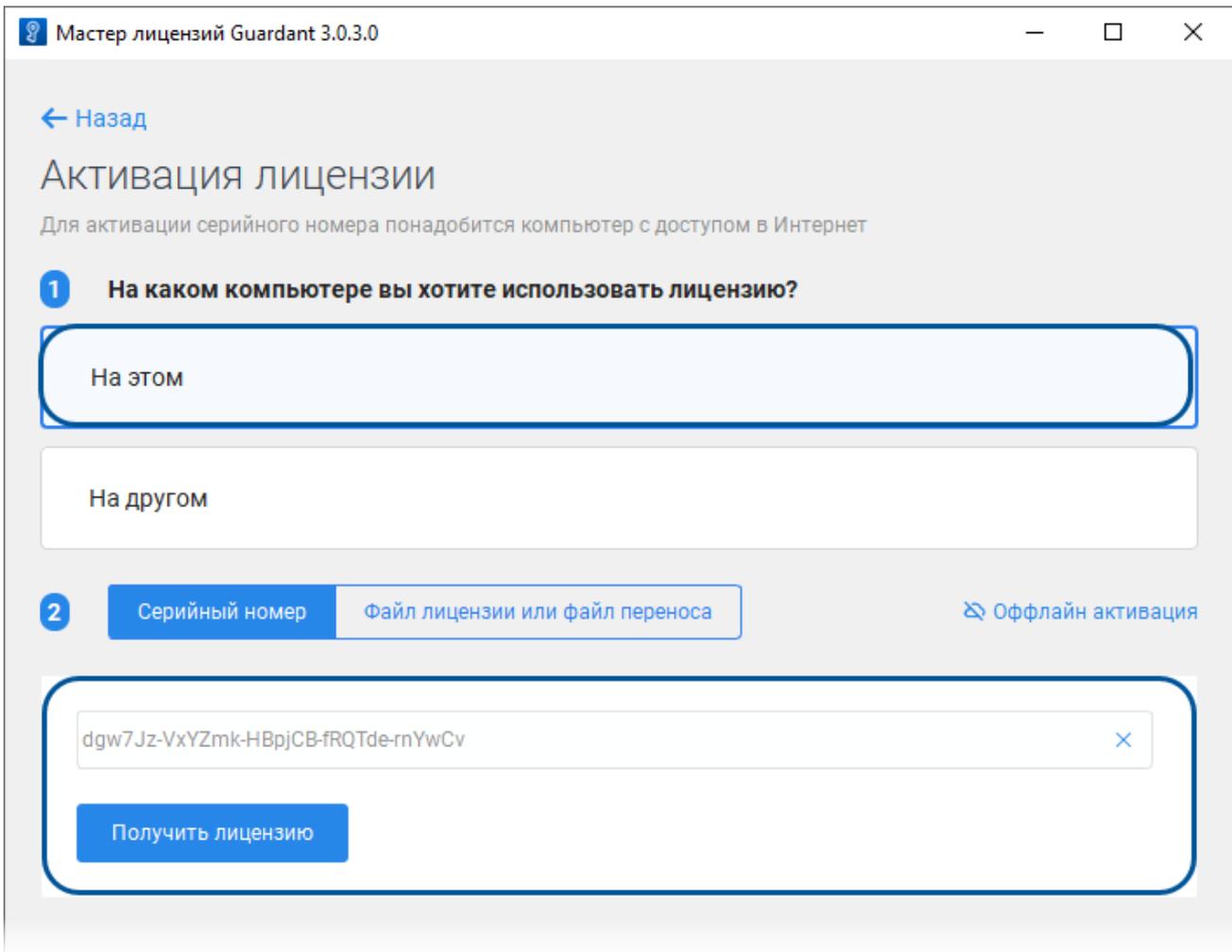
4. Вернитесь в окно **Лицензии**, нажав **Назад**.



5. В окне **Лицензии** нажмите кнопку **Активация лицензии**.



6. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом**, введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Получить лицензию**.

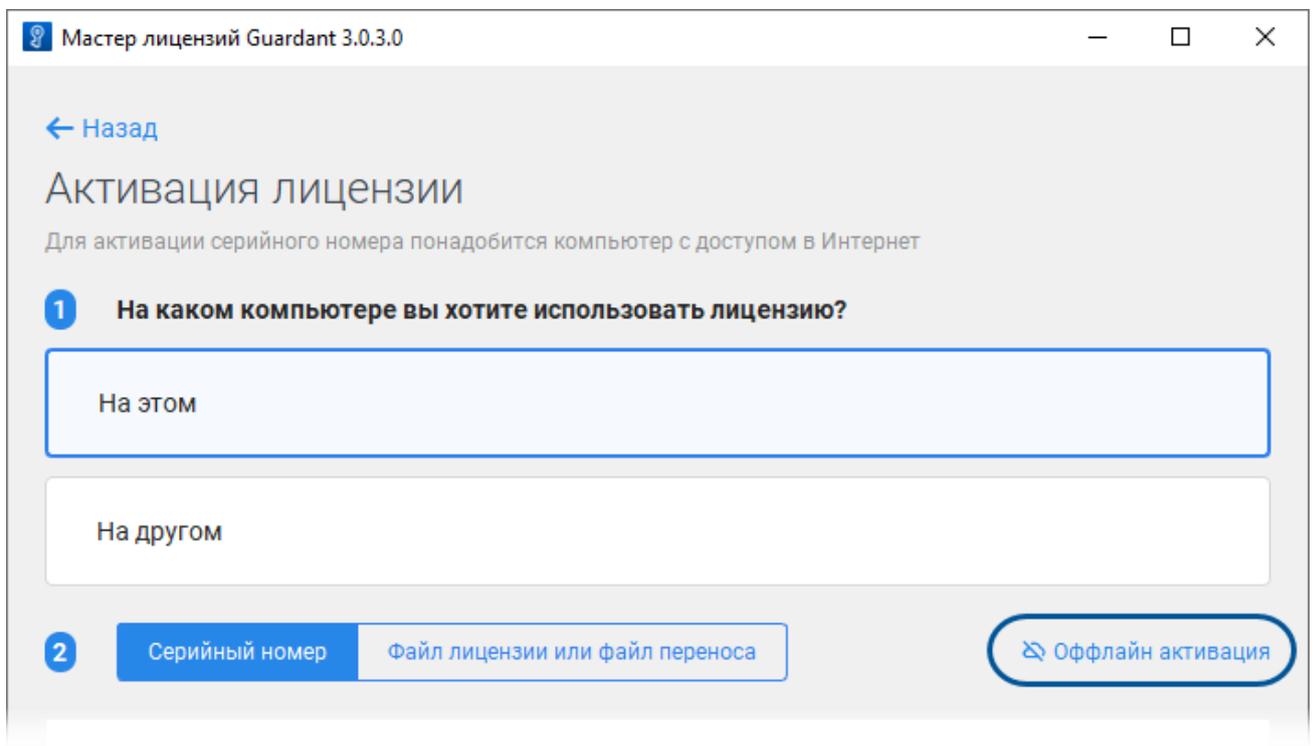


Активация на компьютере без доступа в Интернет

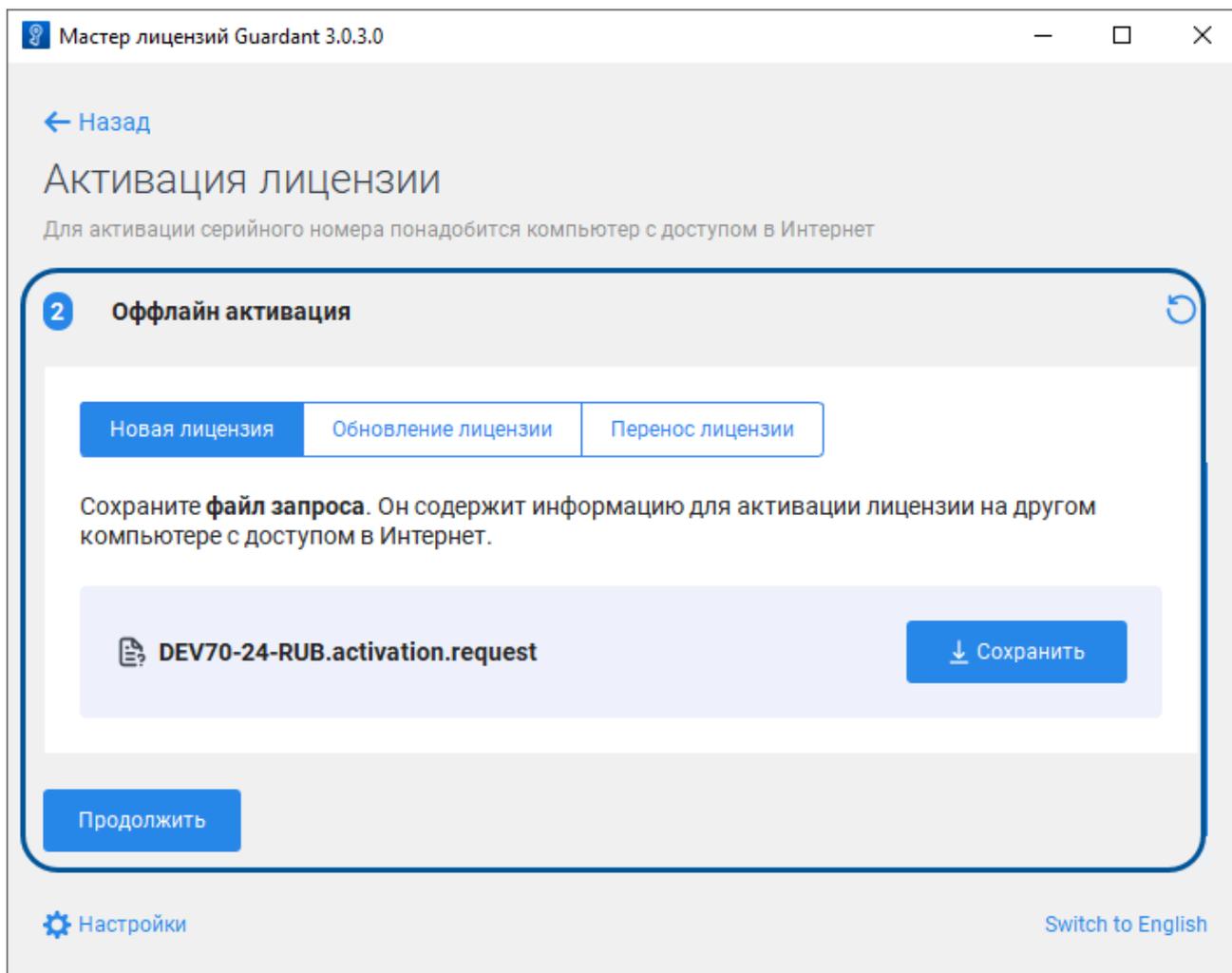
1. Запустите приложение Мастер лицензий Guardant.
2. Нажмите **Активация лицензии**.



3. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом** и нажмите **Оффлайн активация**.

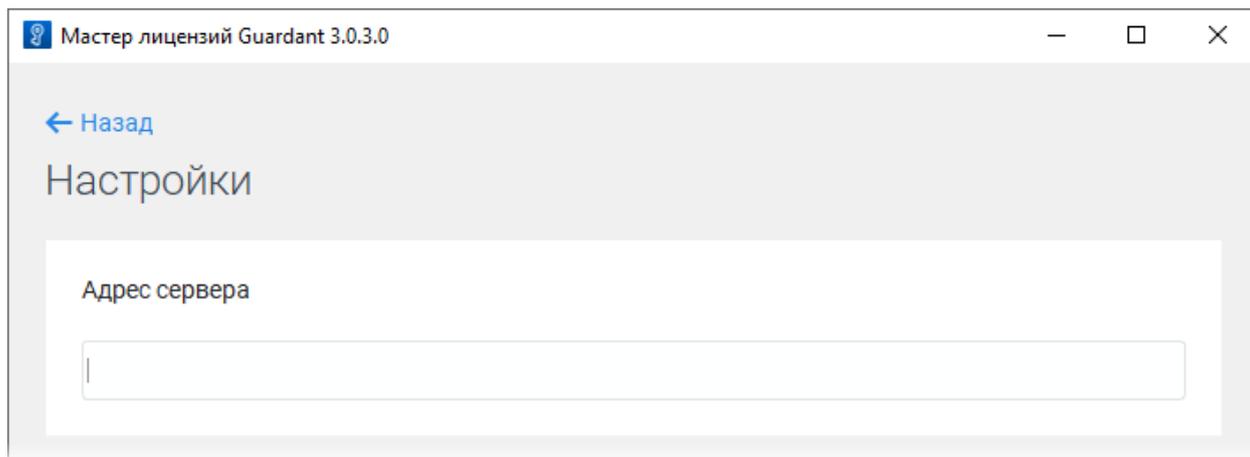


4. На вкладке **Новая лицензия** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата *.request и нажмите кнопку **Продолжить**.



5. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.

5.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.



5.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.



5.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.

Мастер лицензий Guardant 3.0.3.0

← Назад

Активация лицензии

Для активации серийного номера понадобится компьютер с доступом в Интернет

1 На каком компьютере вы хотите использовать лицензию?

На этом

На другом

2 Получите файл запроса на том компьютере, на котором хотите использовать программный продукт

- Запустите на нем приложение **Мастер лицензий Guardant**.
- Нажмите кнопку «**Активация лицензии**» → «**Использовать на этом компьютере**» → «**Оффлайн активация**».

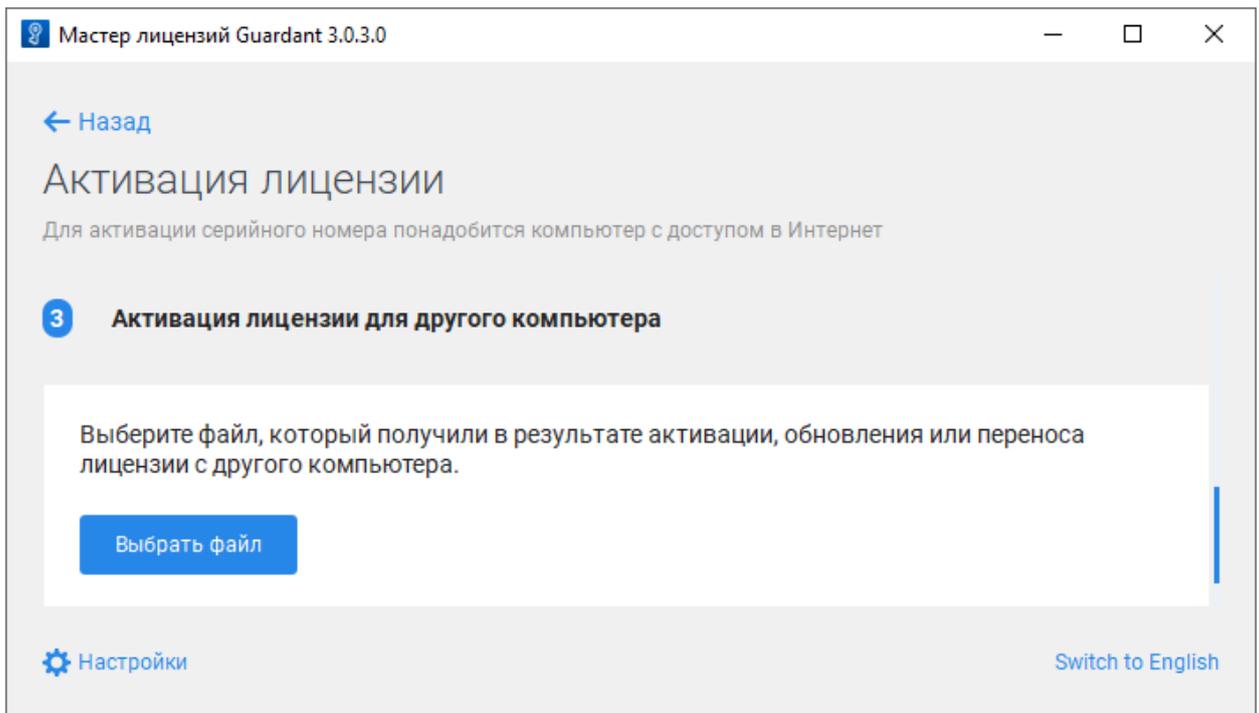
В результате вы получите **файл запроса**, который нужно использовать на этом или любом другом компьютере с доступом в Интернет.

Продолжить

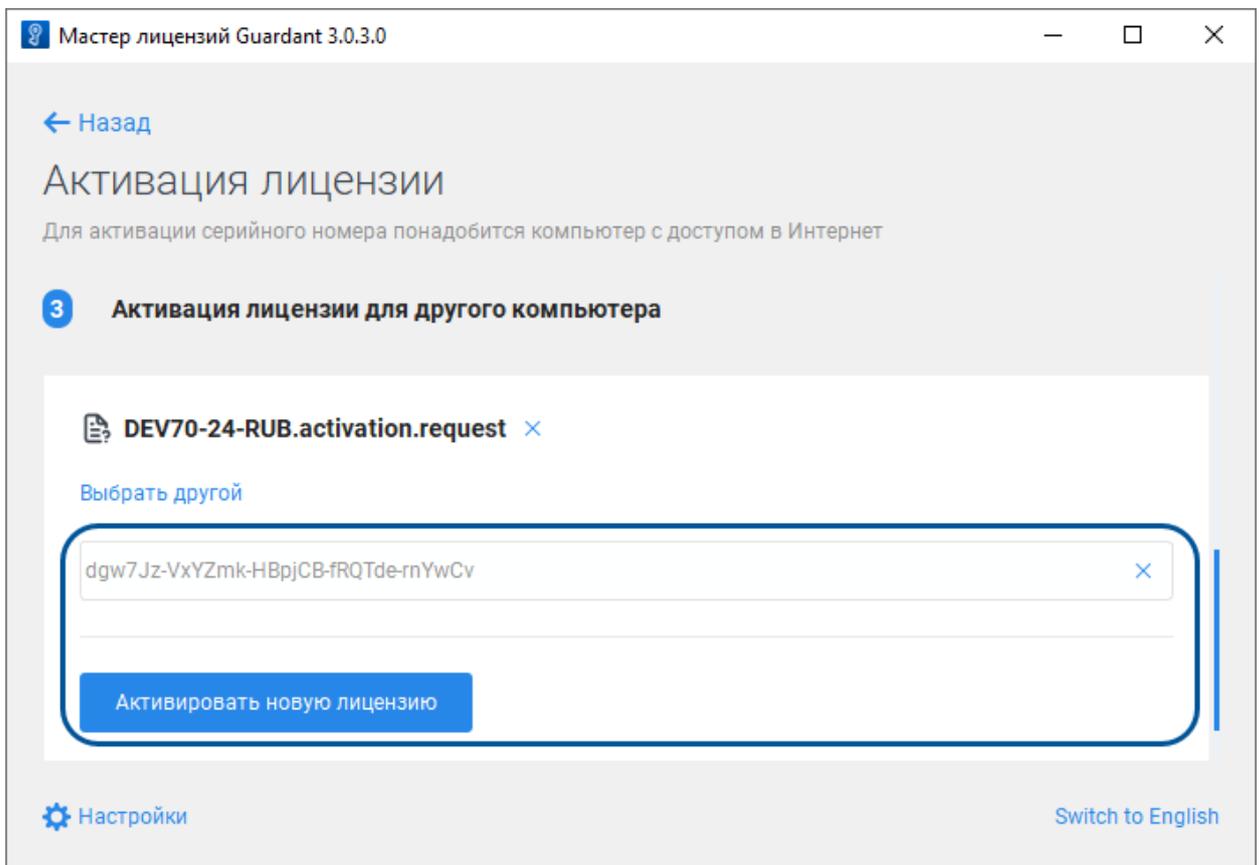
Настройки

Switch to English

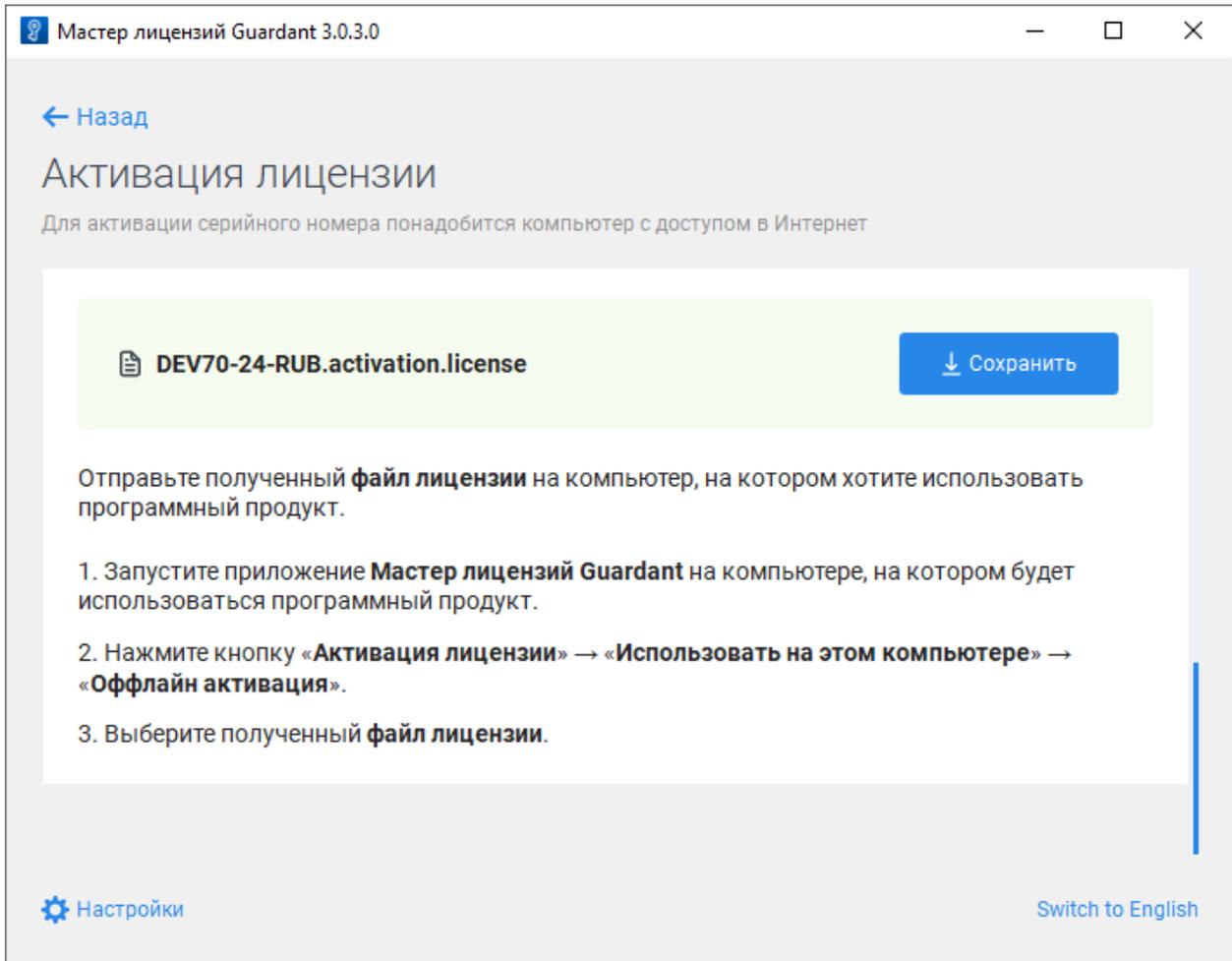
5.4. Нажмите кнопку **Выбрать файл** и выберите файл формата *.request, перенесенный с компьютера без доступа в Интернет.



5.5. Введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Активировать новую лицензию**.

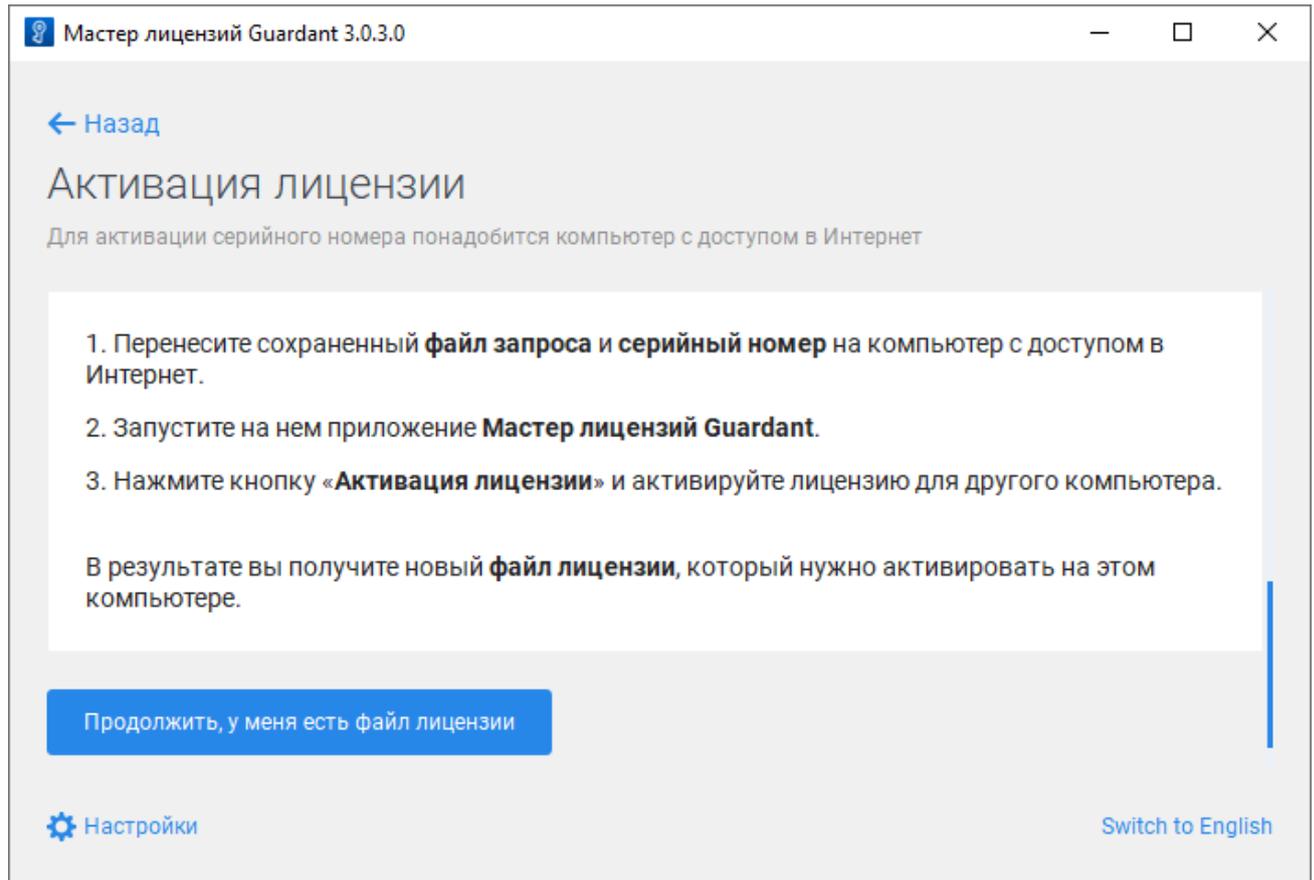


5.6. Нажмите кнопку **Сохранить** и сохраните на диске файл активации лицензии формата *.license.

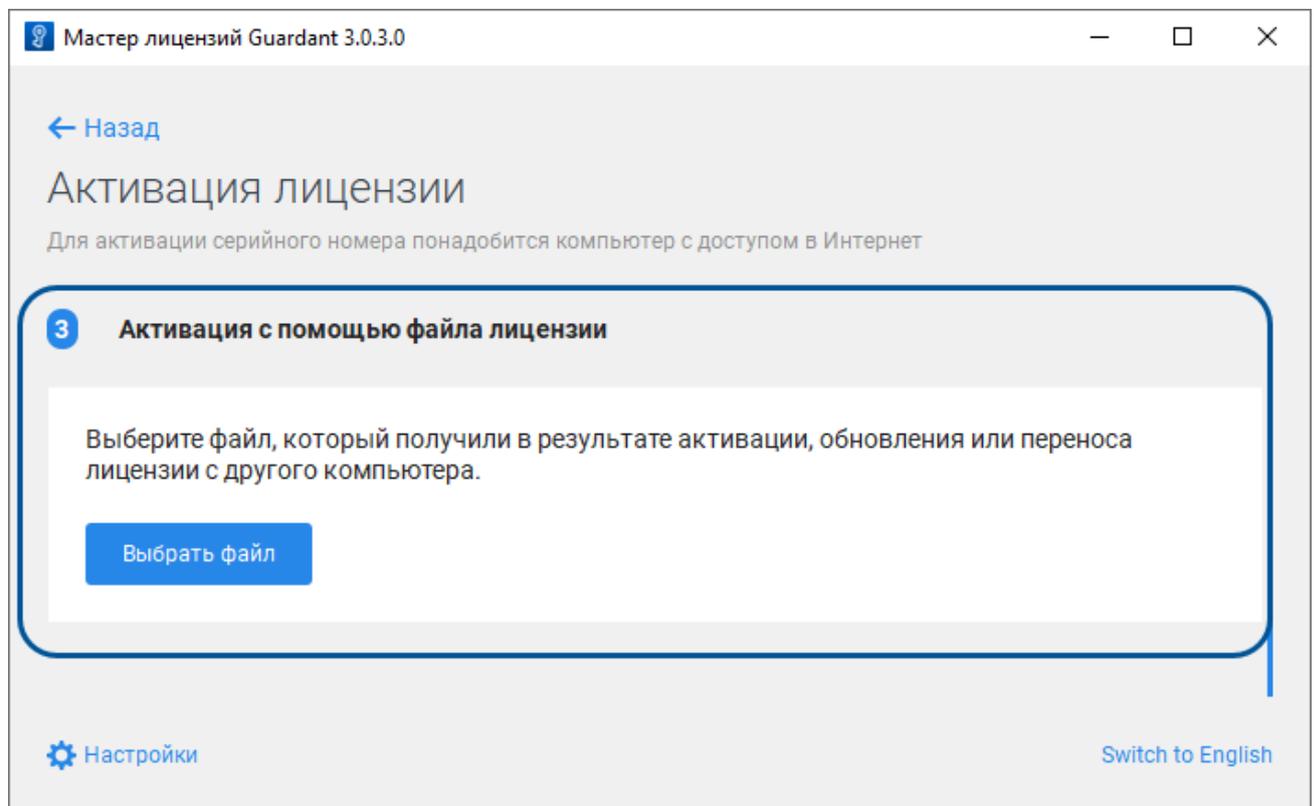


5.7. Перенесите полученный файл активации лицензии формата *.license на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

6. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии.**

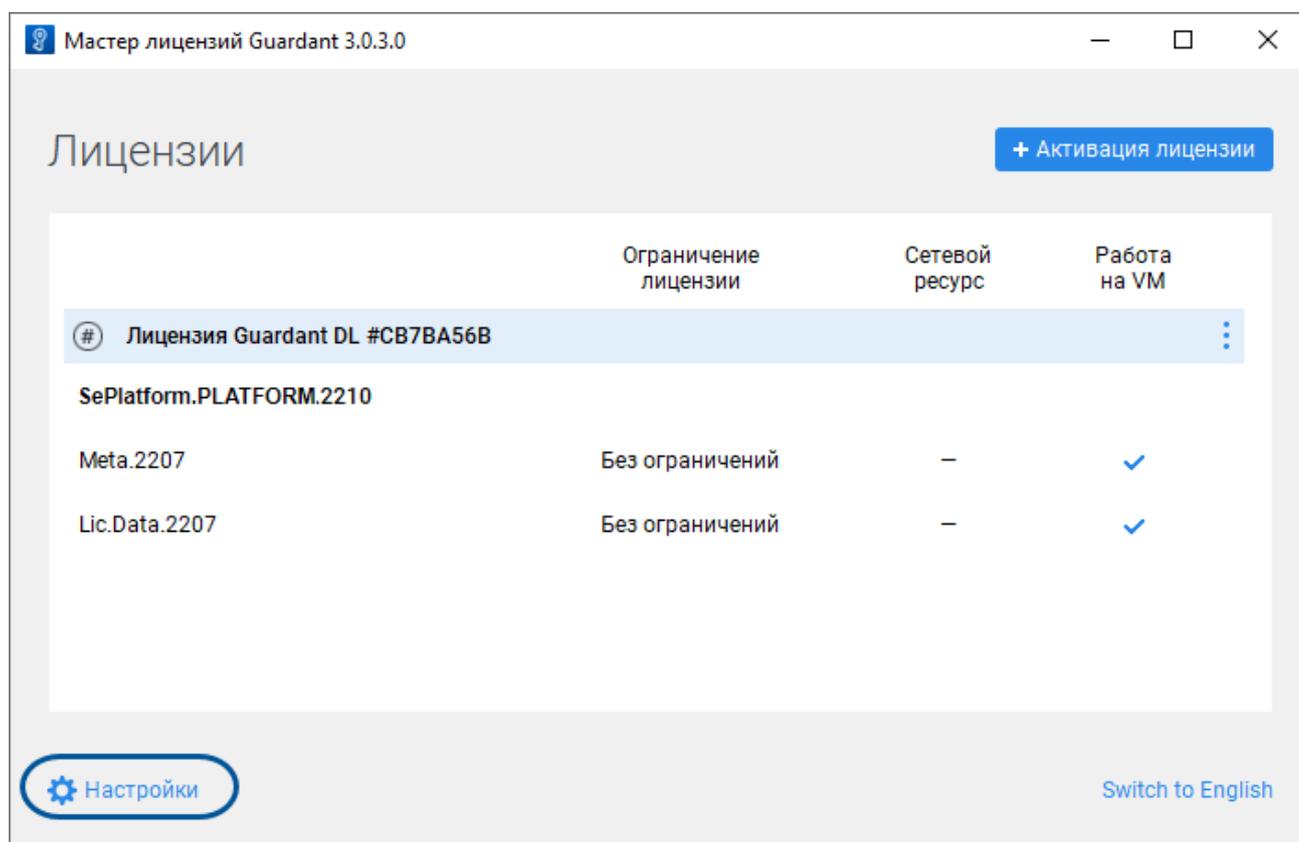


7. Нажмите кнопку **Выбрать файл** и выберите файл формата *.license, перенесенный с компьютера с доступом в Интернет.



Обновление на компьютере с доступом в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



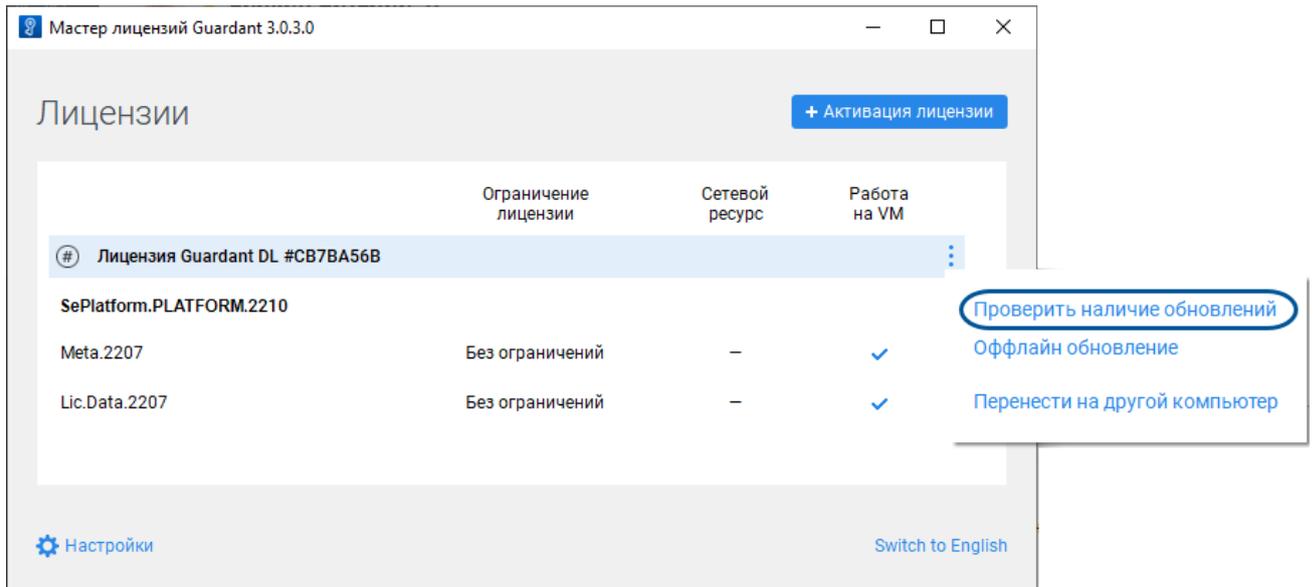
3. Укажите адрес сервера обновления лицензий.



4. Вернитесь в окно **Лицензии**, нажав **Назад**.



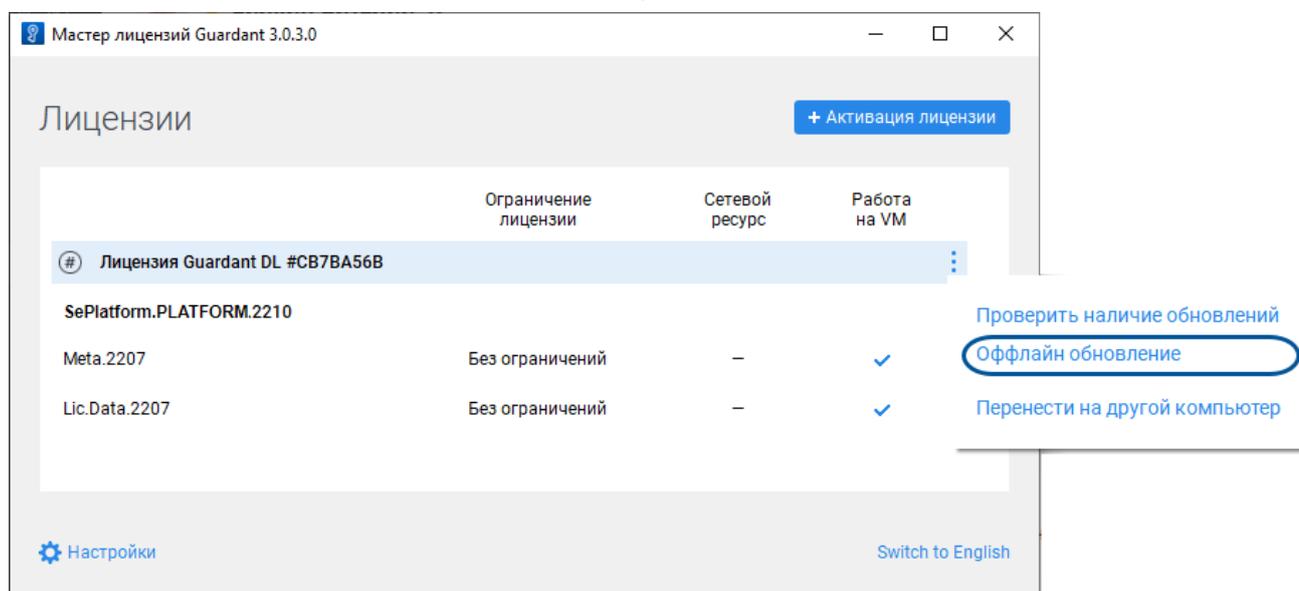
5. В окне **Лицензии** в меню ключа выберите команду **Проверить наличие обновлений**.



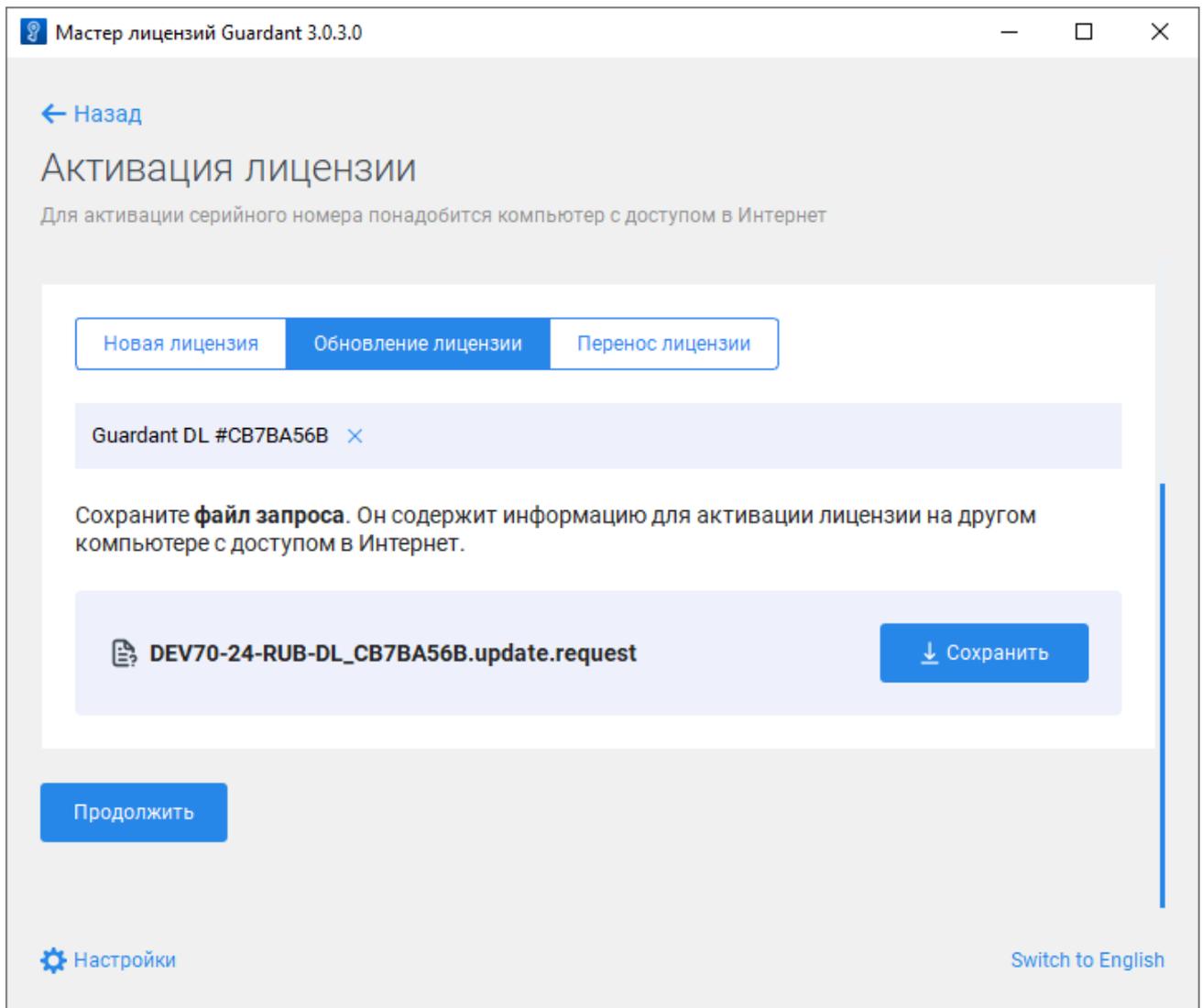
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

Обновление на компьютере без доступа в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Офлайн обновление**.

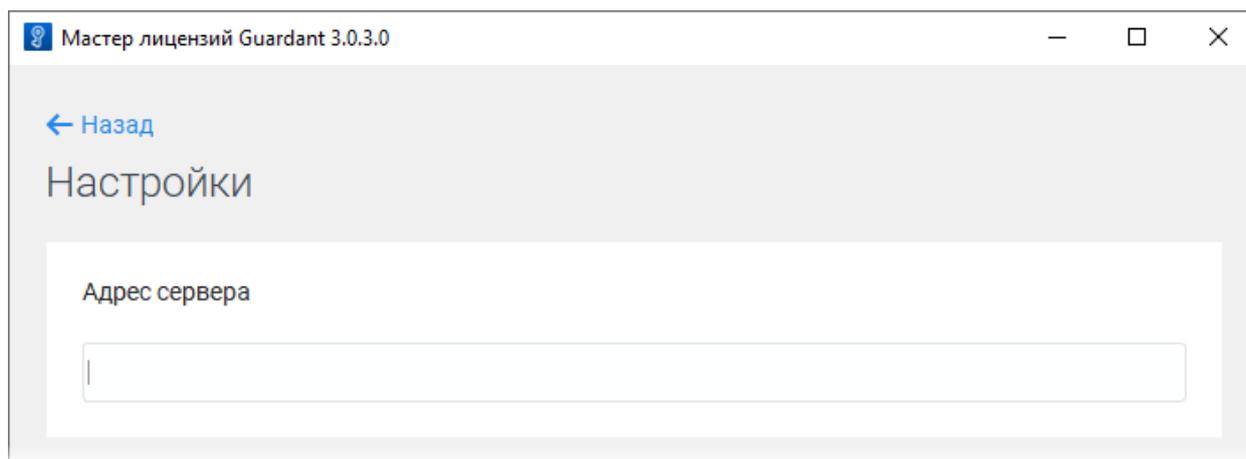


3. На вкладке **Обновление лицензии** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата *.request и нажмите кнопку **Продолжить**.

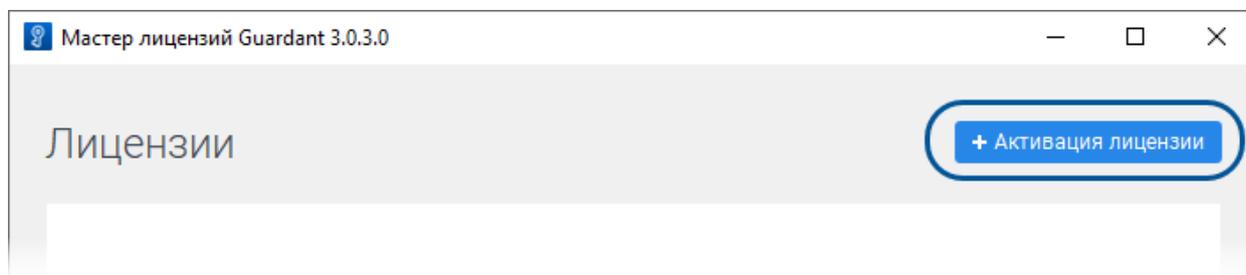


4. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.

4.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.



4.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензий**.



4.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.

Мастер лицензий Guardant 3.0.3.0

← Назад

Активация лицензии

Для активации серийного номера понадобится компьютер с доступом в Интернет

1 На каком компьютере вы хотите использовать лицензию?

На этом

На другом

2 Получите файл запроса на том компьютере, на котором хотите использовать программный продукт

1. Запустите на нем приложение **Мастер лицензий Guardant**.
2. Нажмите кнопку «**Активация лицензии**» → «**Использовать на этом компьютере**» → «**Оффлайн активация**».

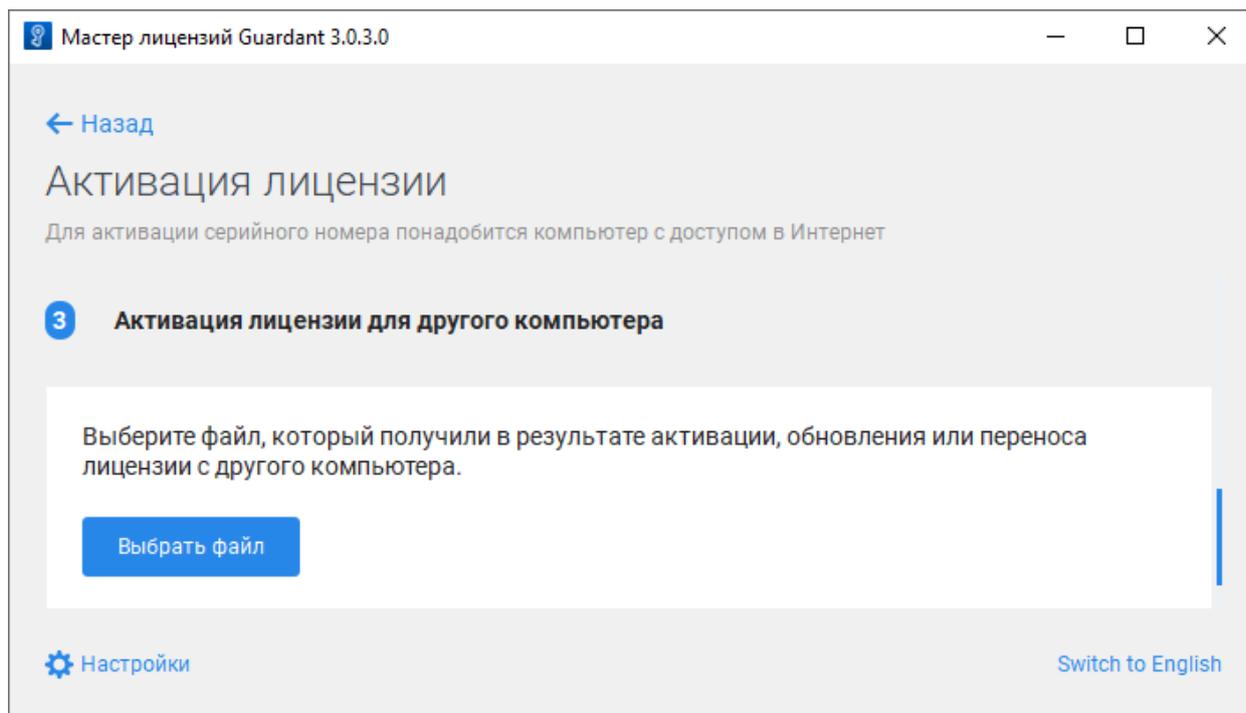
В результате вы получите **файл запроса**, который нужно использовать на этом или любом другом компьютере с доступом в Интернет.

Продолжить

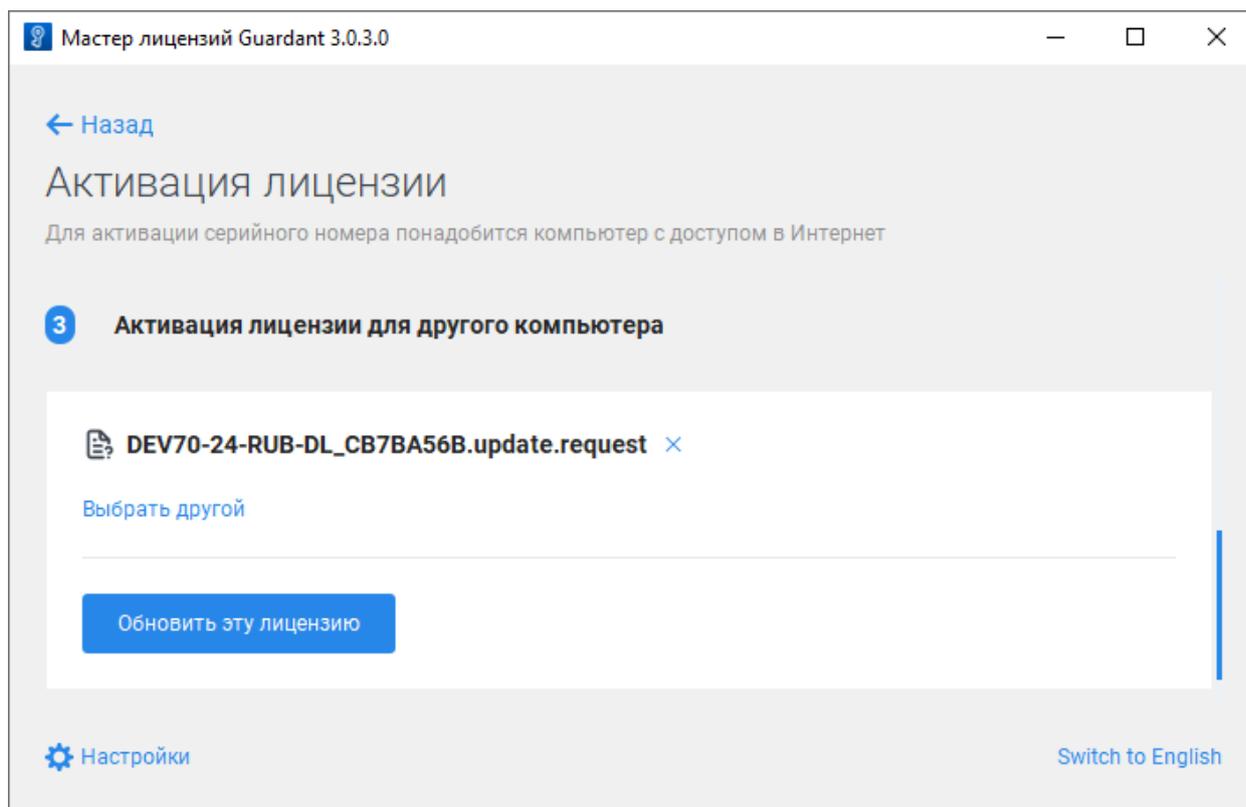
Настройки

Switch to English

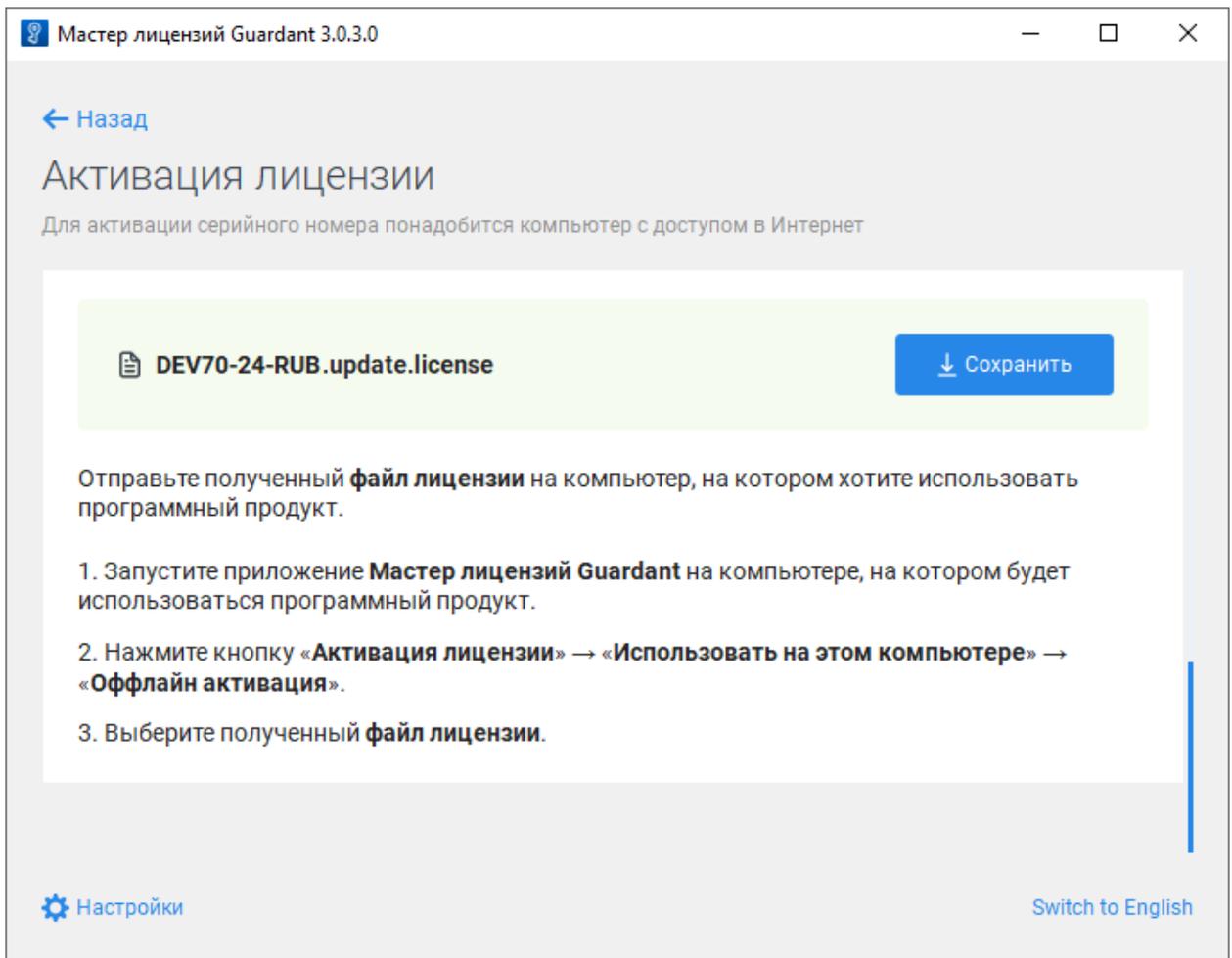
4.4. Нажмите кнопку **Выбрать файл** и выберите файл запроса формата *.request, перенесенный с компьютера без доступа в Интернет.



4.5. Нажмите кнопку **Обновить эту лицензию**.

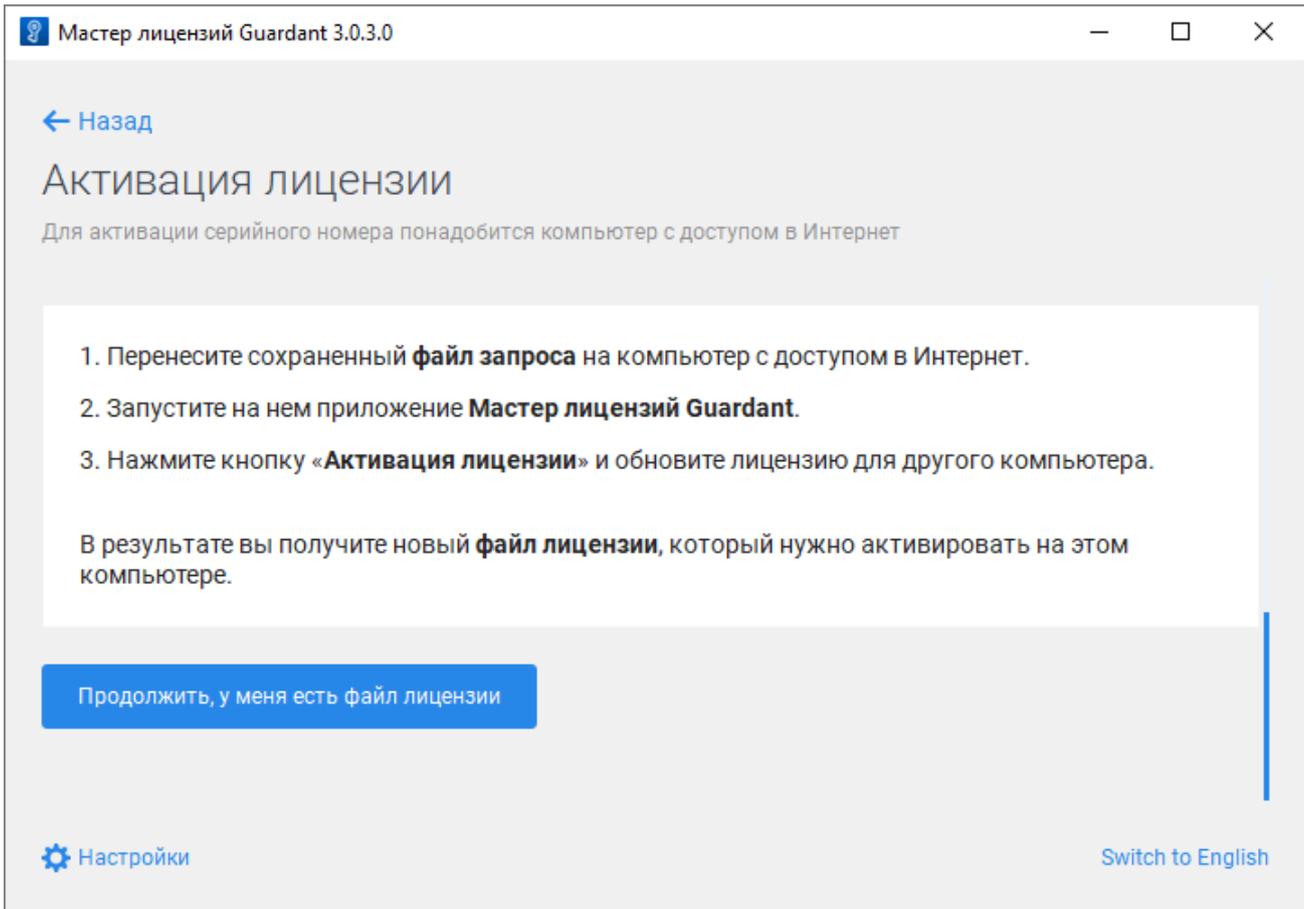


4.6. Нажмите кнопку **Сохранить** и сохраните на диске файл обновления лицензии формата *.license.

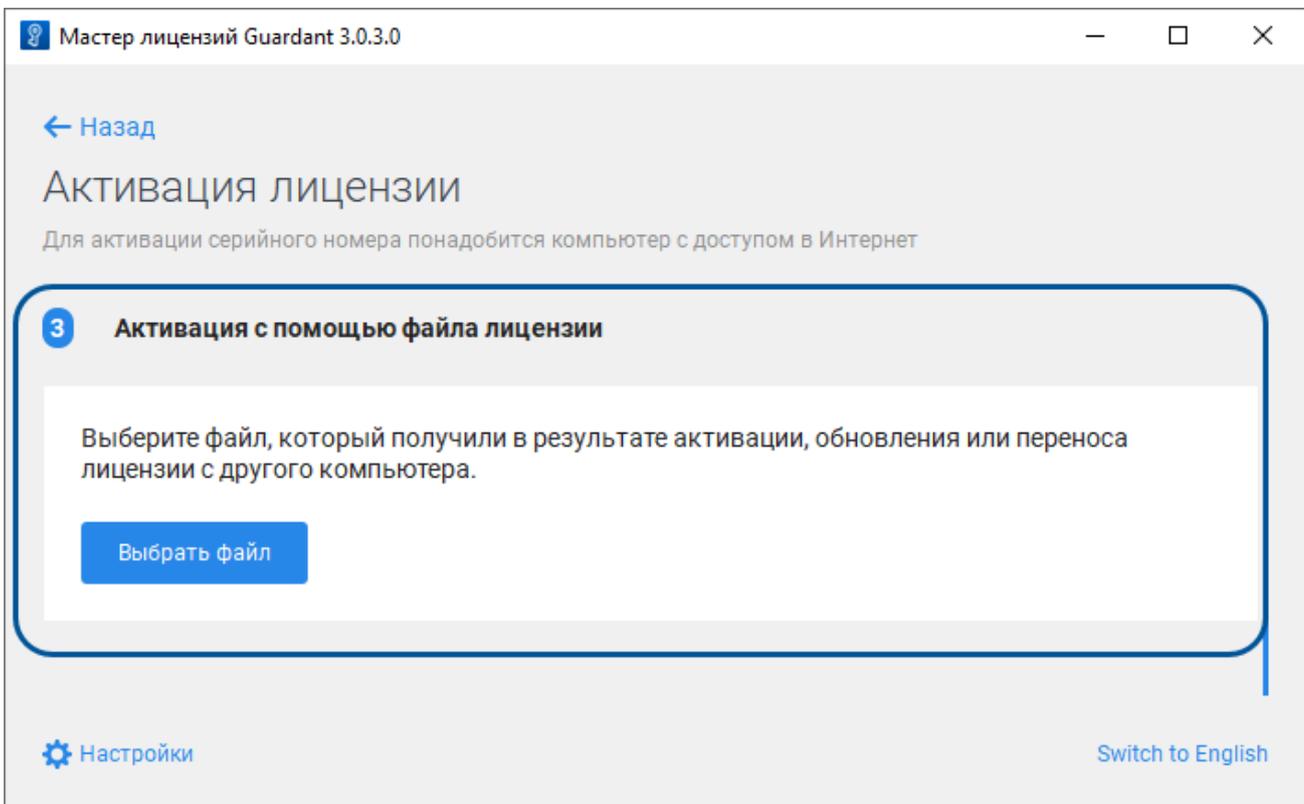


4.7. Перенесите полученный файл обновления лицензии формата *.license на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

5. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

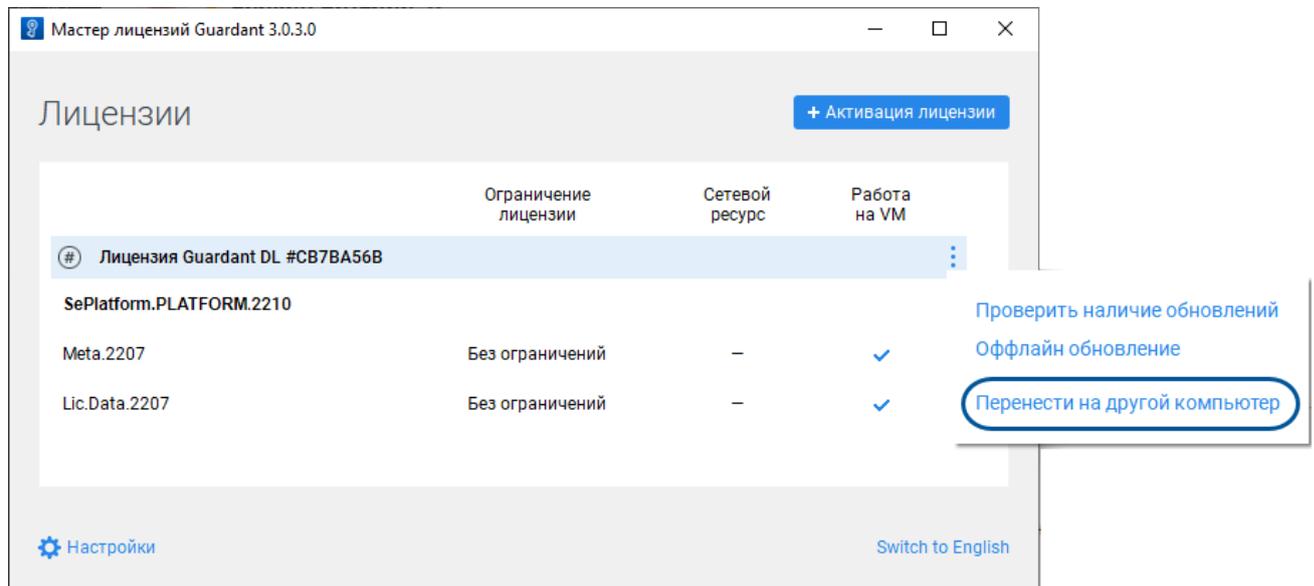


6. Нажмите кнопку **Выбрать файл** и выберите файл формата *.license, перенесенный с компьютера с доступом в Интернет.

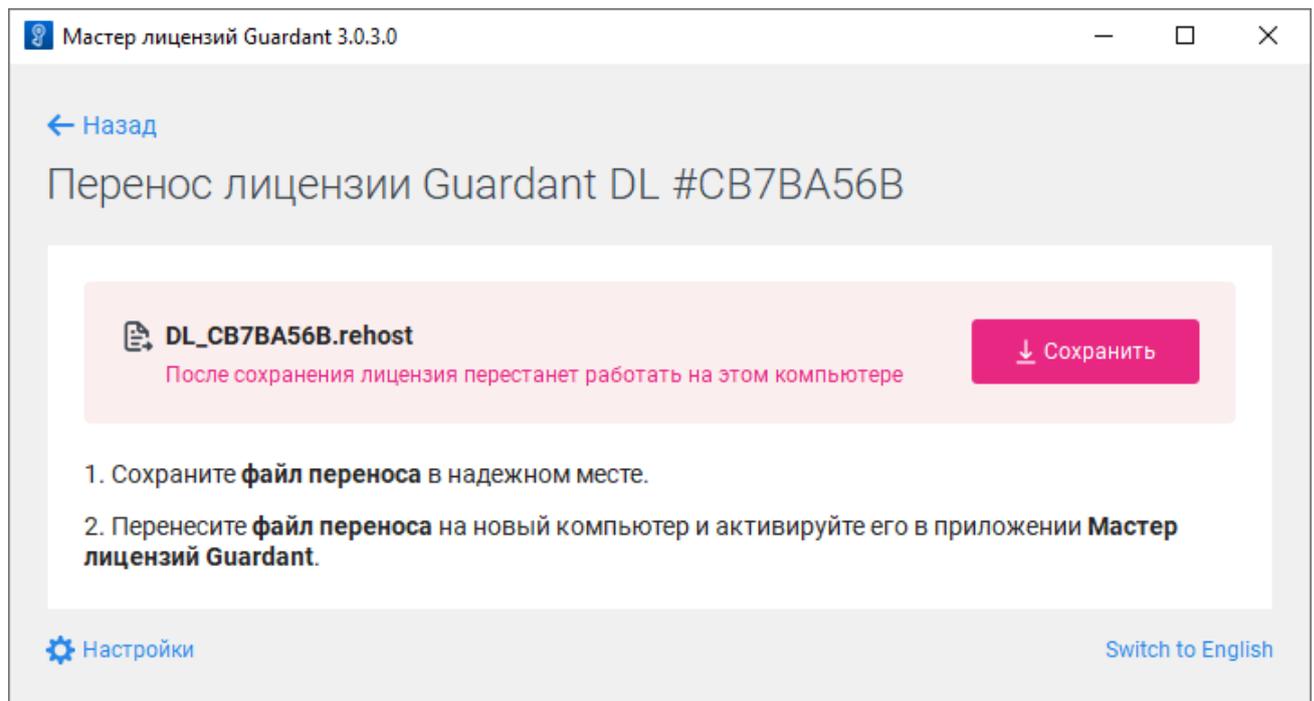


Перенос на другой компьютер

1. Запустите приложение Мастер лицензий Guardant.
2. В окне Лицензии в меню ключа выберите команду **Перенести на другой компьютер**.



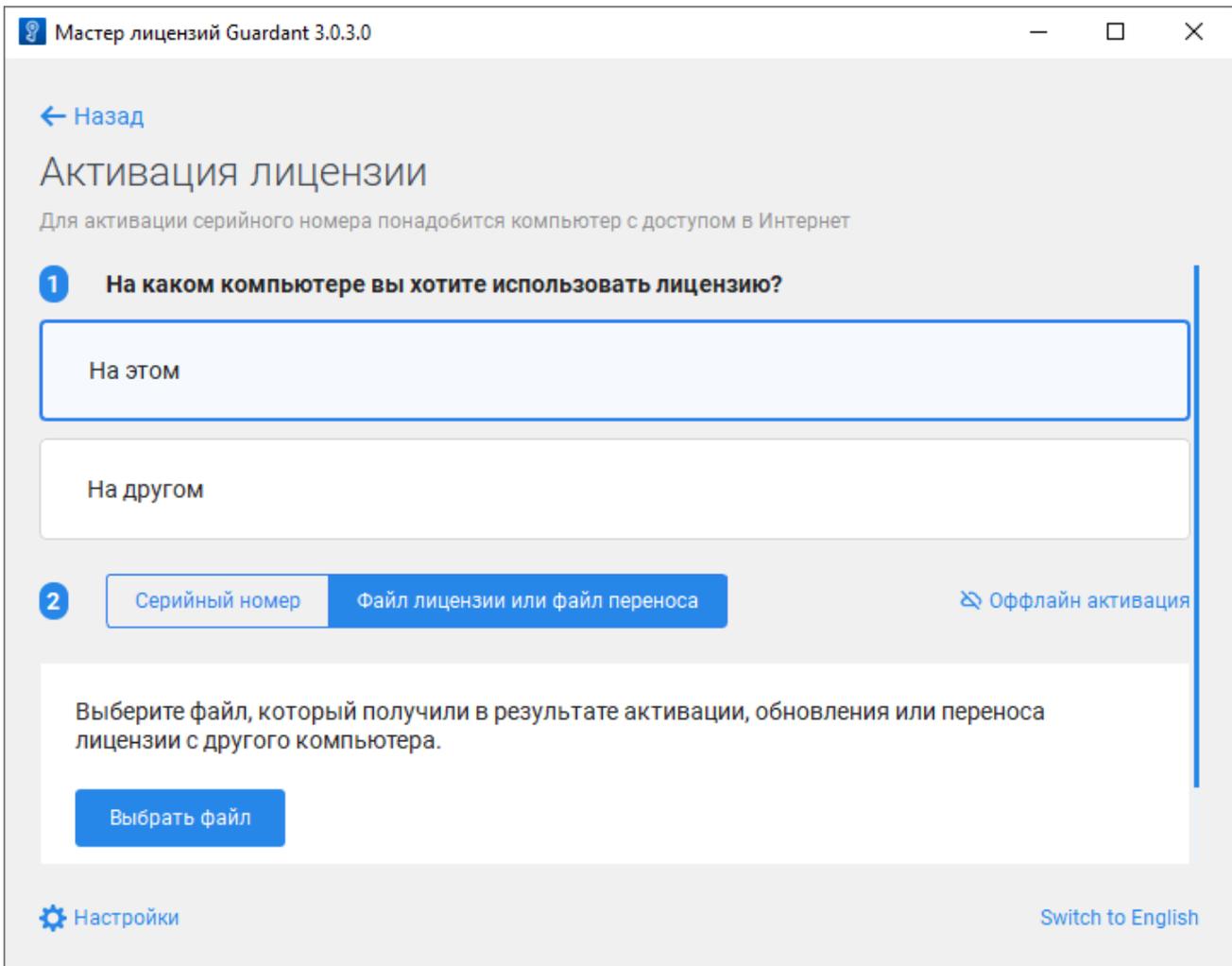
3. В окне **Перенос лицензии Guardant DL** нажмите кнопку **Сохранить** и сохраните на диске файл переноса формата *.rehost.



4. На другом компьютере запустите приложение Мастер лицензий Guardant и нажмите кнопку **Активация лицензии**.



5. Укажите компьютер, на котором будет использоваться лицензия - **На этом**, перейдите на вкладку **Файл лицензии** или **файл переноса**, нажмите кнопку **Выбрать файл** и выберите ранее сохраненный файл переноса формата *.rehost.



16.2.2. ОС Linux

Для лицензирования компонентов Систэм Платформ, установленных на компьютере с ОС Linux:

- > установите сервер лицензирования SePlatform.License Server;
- > установите Guardant Control Center.

16.2.2.1. Установка SePlatform.License Server

Установите сервер лицензирования, установочные пакеты которого на поставочном диске Систэм Платформ расположены в папке \SePlatform\SePlatform.License Server\x.x.x.

**ОБРАТИТЕ ВНИМАНИЕ**

Команда установки выполняется только от суперпользователя «root».

Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером. Установка пакета *.rpm с помощью пакетного менеджера YUM:

```
yum install seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета *.rpm с помощью пакетного менеджера RPM:

```
rpm -i seplatform.licensing.agent-x.x.x+xx.xxxxx.rpm
```

Установка пакета *.deb с помощью пакетного менеджера apt:

```
apt-get install seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

Установка пакета *.deb с помощью пакетного менеджера dpkg:

```
sudo dpkg -i seplatform.licensing.agent-x.x.x+xx.xxxxx.deb
```

16.2.2.2. Установка Guardant Control Center

Установите Guardant Control Center, установочные пакеты которого на поставочном диске Систэм Платформ расположены в папке \Стронние компоненты\Guardant\control_center.

**ОБРАТИТЕ ВНИМАНИЕ**

Команда установки выполняется только от суперпользователя «root».

Находясь в папке с установочным пакетом, запустите установку штатным пакетным менеджером. Установка пакета *.rpm с помощью пакетного менеджера YUM:

```
yum install grdcontrol-x.x-xxxx.rpm
```

Установка пакета *.rpm с помощью пакетного менеджера RPM:

```
rpm -i grdcontrol-x.x-xxxx.rpm
```

Установка пакета *.deb с помощью пакетного менеджера apt:

```
apt-get install grdcontrol-x.x_xxxx.deb
```

Установка пакета *.deb с помощью пакетного менеджера dpkg:

```
sudo dpkg -i grdcontrol-x.x_xxxx.deb
```

16.2.2.3. Аппаратный ключ Guardant Sign

Подключите аппаратный ключ Guardant Sign в USB разъем компьютера. Дополнительных действий не требуется. Ключ готов к работе.

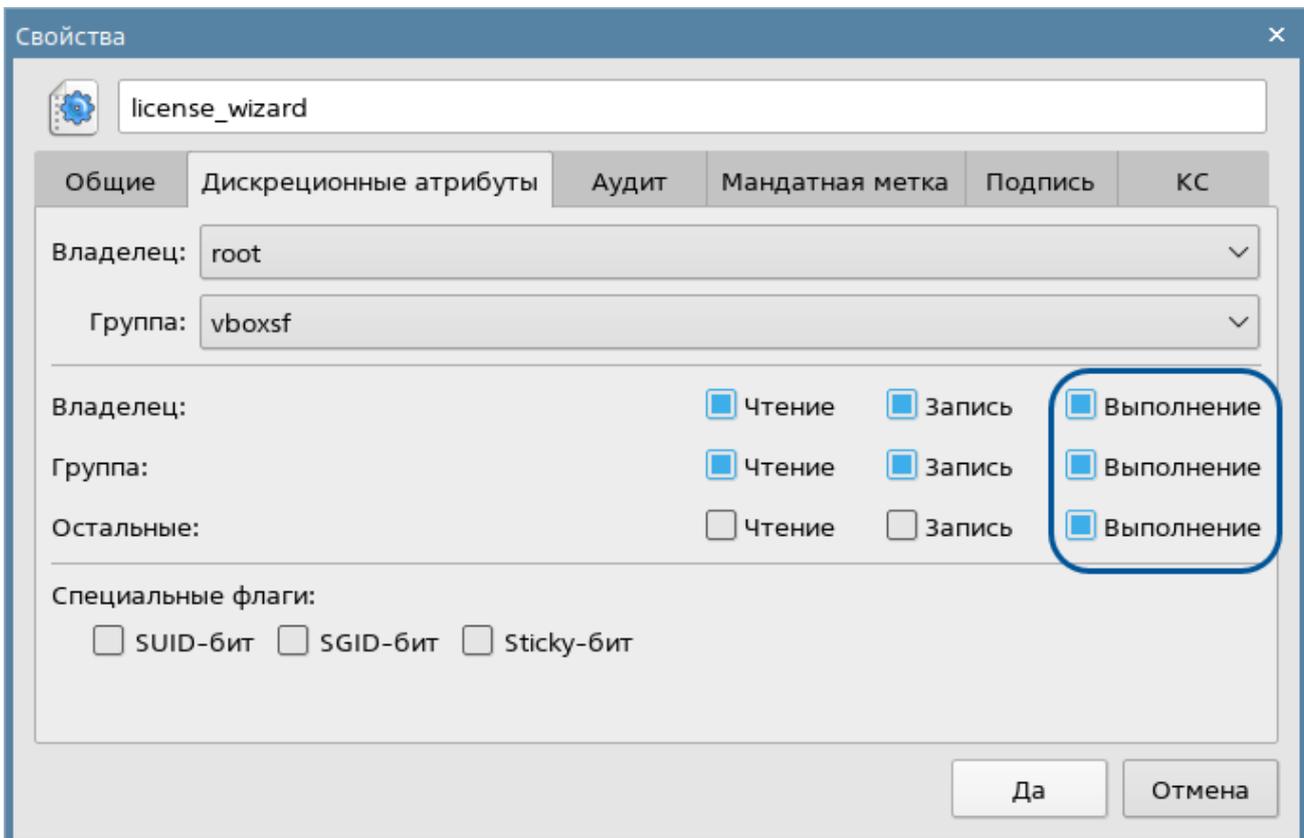
Обновление



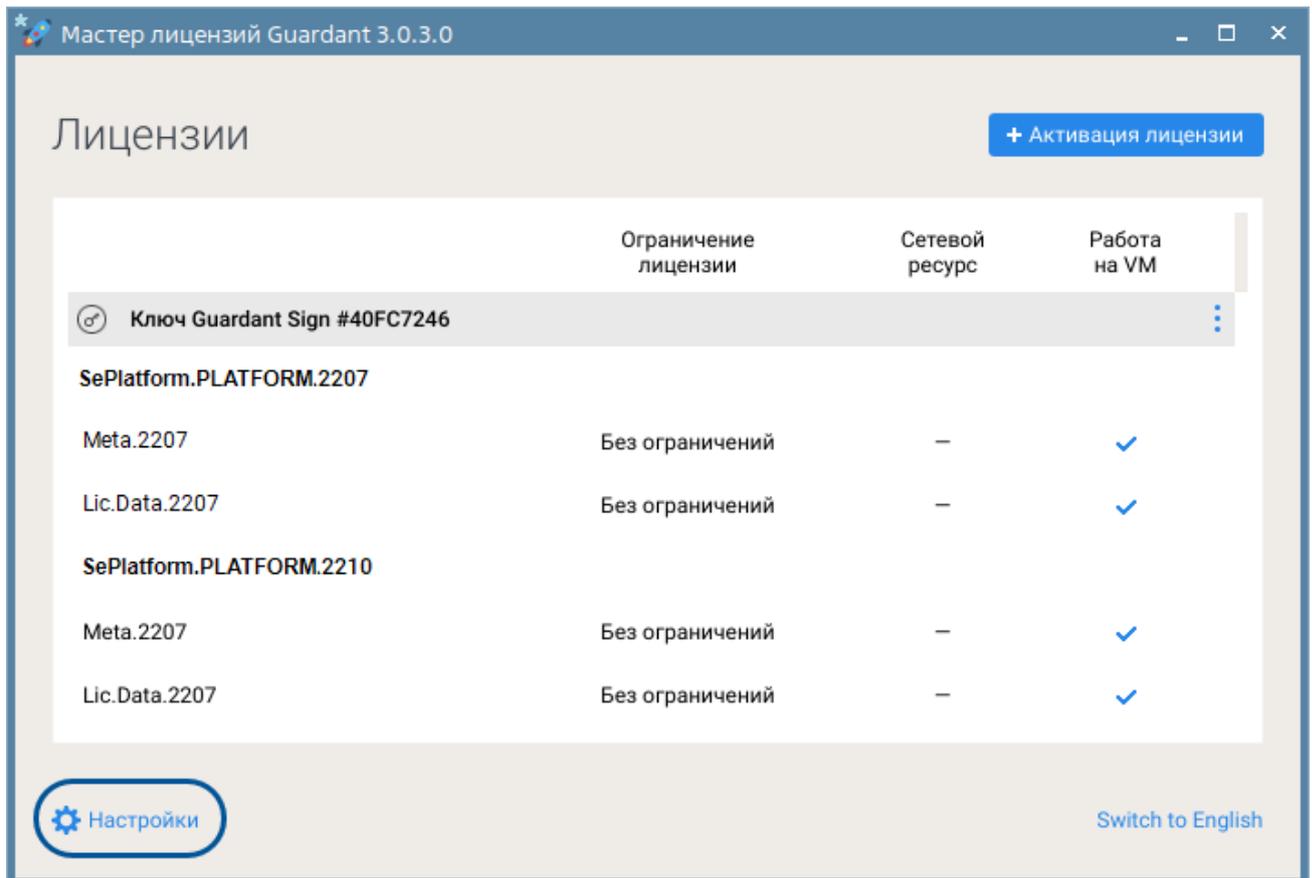
ОБРАТИТЕ ВНИМАНИЕ

Для обновления состава лицензии аппаратного ключа Guardant Sign требуется подключение к сети Интернет.

1. Исполняемому файлу `license_wizard`, который на поставочном диске Систэм Платформ расположен в папке \Сторонние компоненты\Guardant\license_activation, в свойствах установите права на запуск.



2. Запустите Мастер лицензий Guardant - исполняемый файл `license_wizard`.

3. Перейдите в **Настройки**:

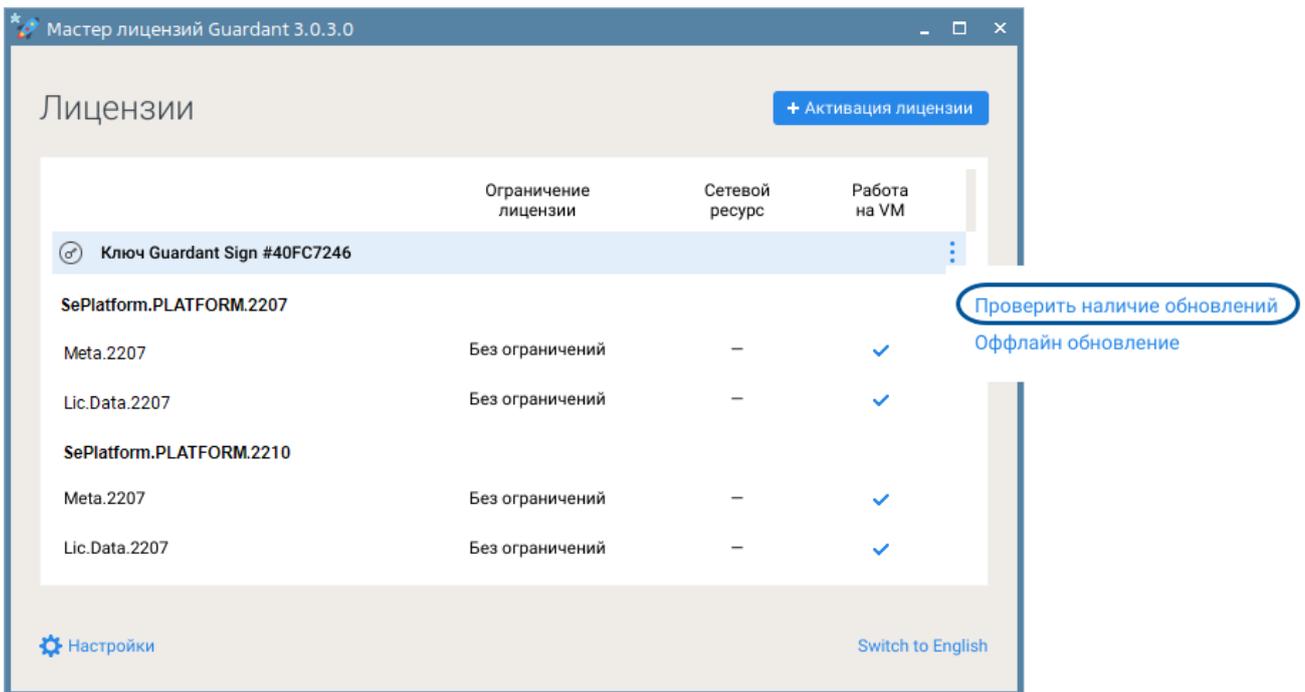
4. Укажите адрес сервера обновления лицензий:



5. Вернитесь в окно **Лицензии**, нажав **Назад**.



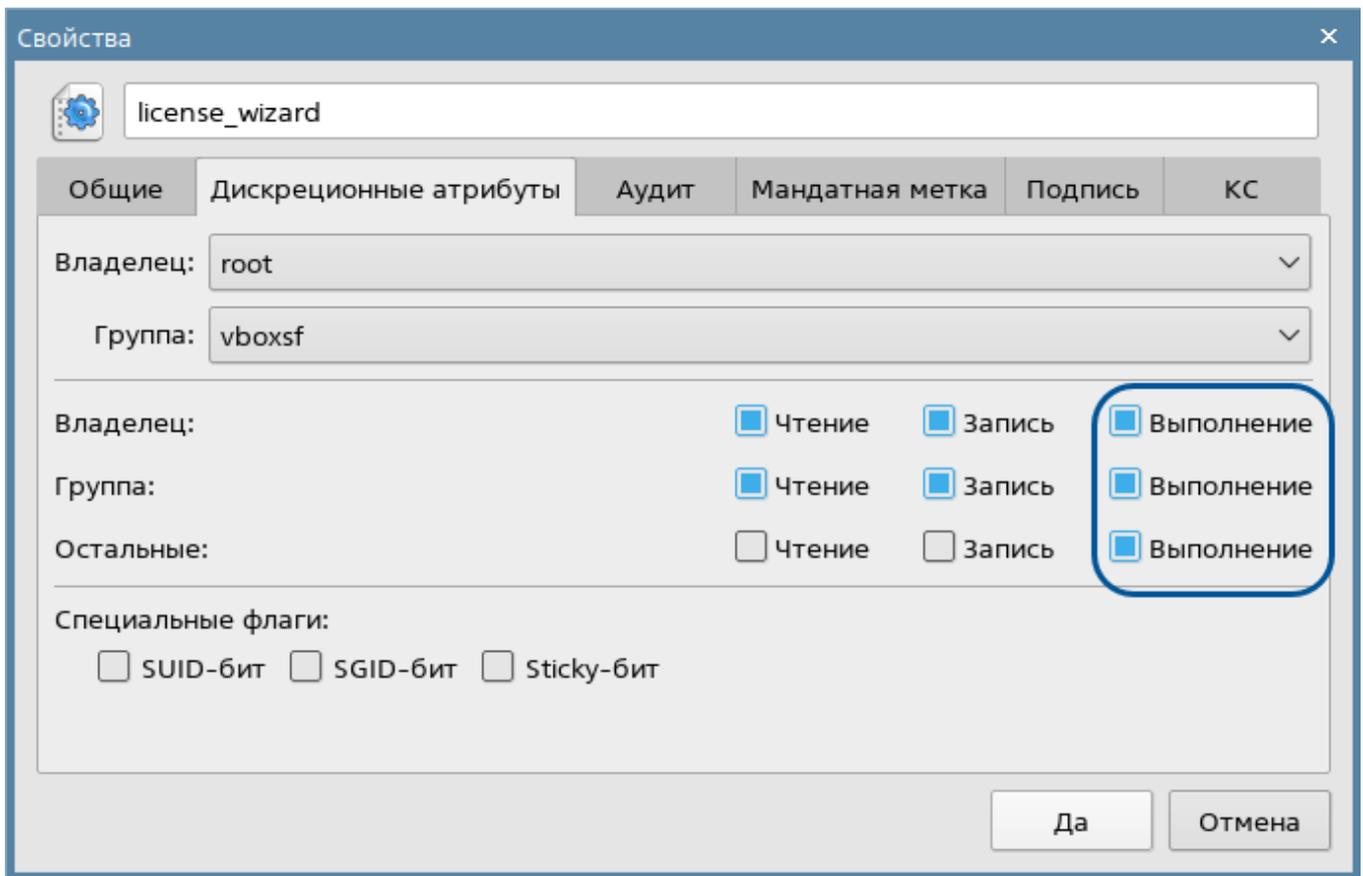
6. В меню ключа выберите команду **Проверить наличие обновлений**.



7. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

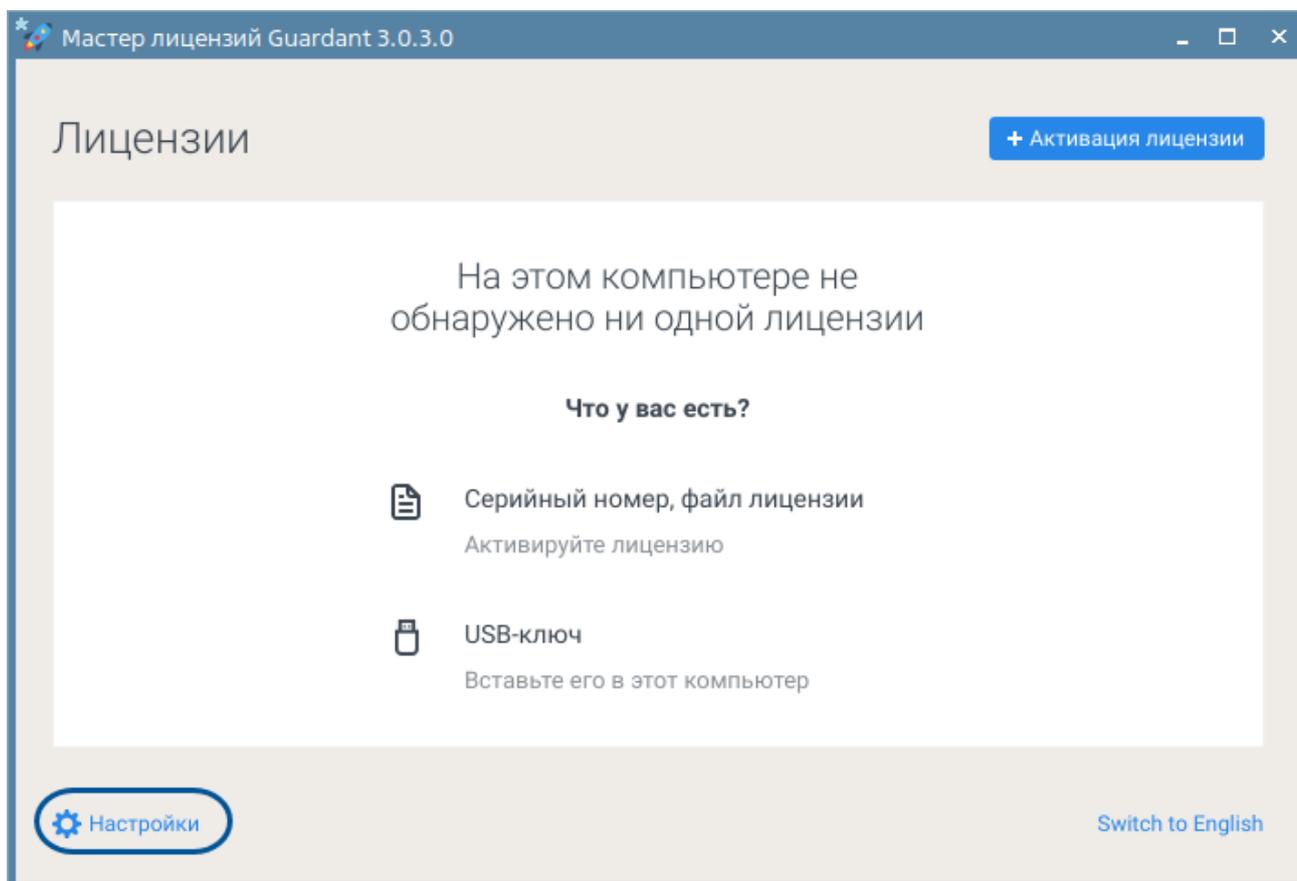
16.2.2.4. Программный ключ Guardant DL

Активация, обновление и перенос лицензии программного ключа Guardant DL выполняется в Мастере лицензий Guardant - исполняемый файл `license_wizard`, который на поставочном диске Систэм Платформ расположен в папке `\Сторонние компоненты\Guardant\license_activation`. В свойствах `license_wizard` установите права на запуск.



Активация на компьютере с доступом в Интернет

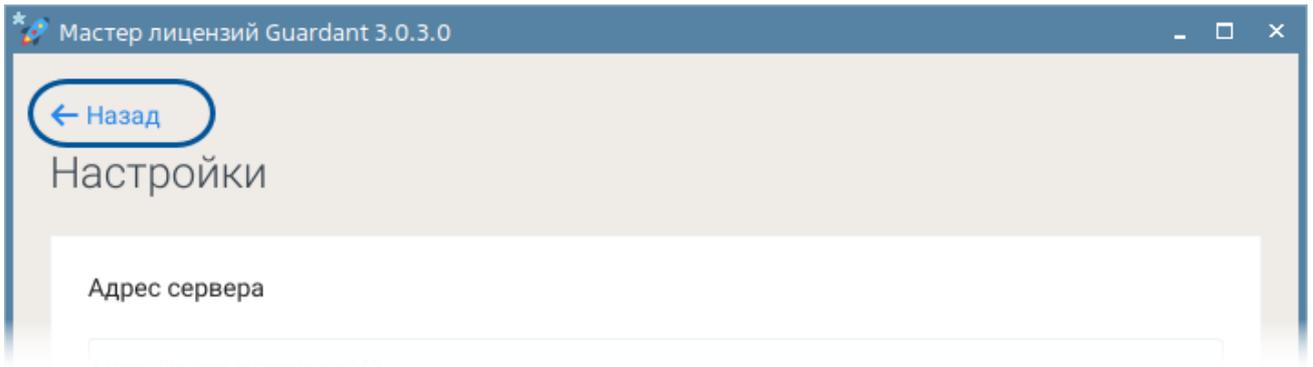
1. Запустите Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



3. Укажите адрес сервера обновления лицензий:



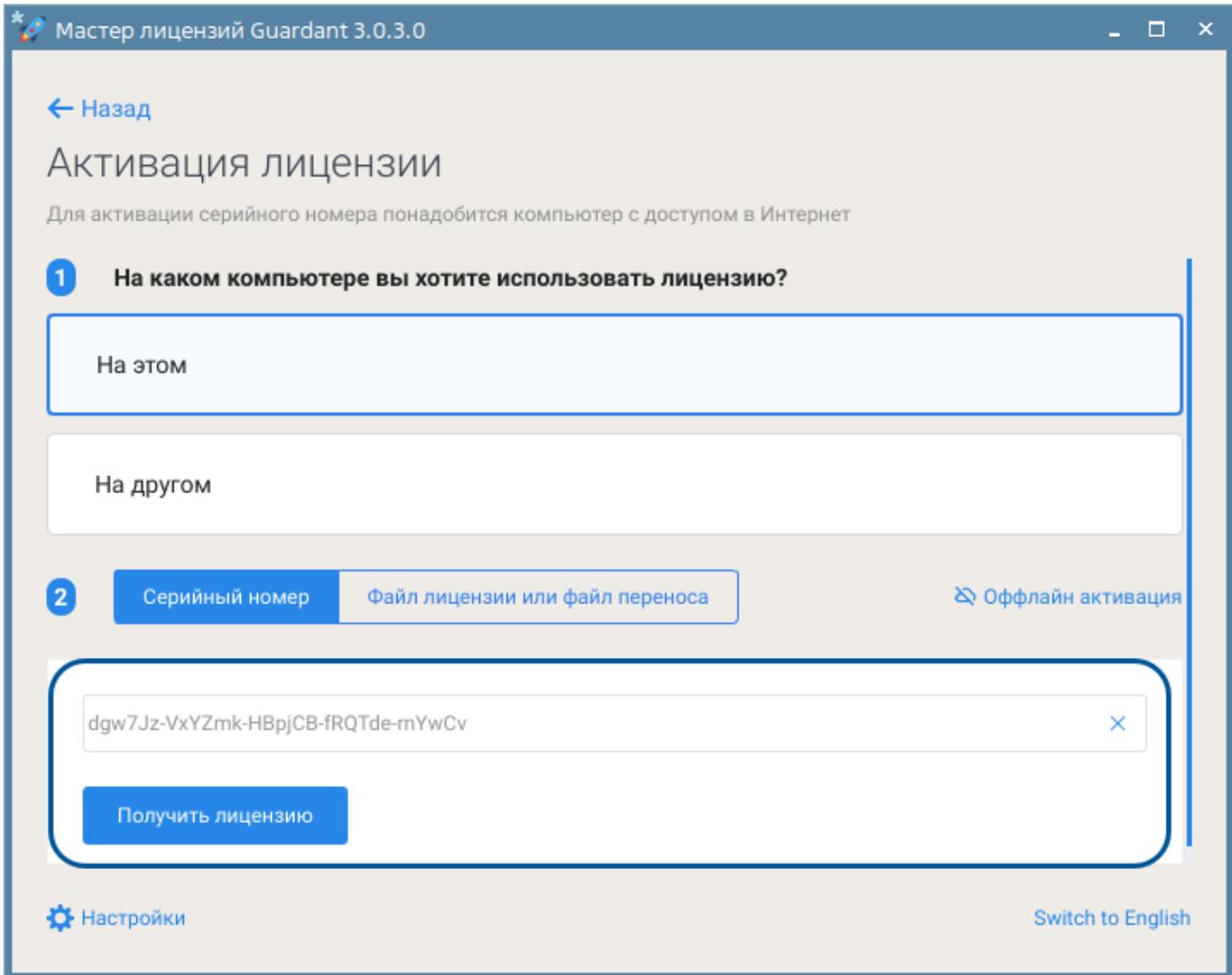
4. Вернитесь в окно **Лицензии**, нажав **Назад**.



5. В окне **Лицензии** нажмите **Активация лицензии**.



6. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом**, введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Получить лицензию**.

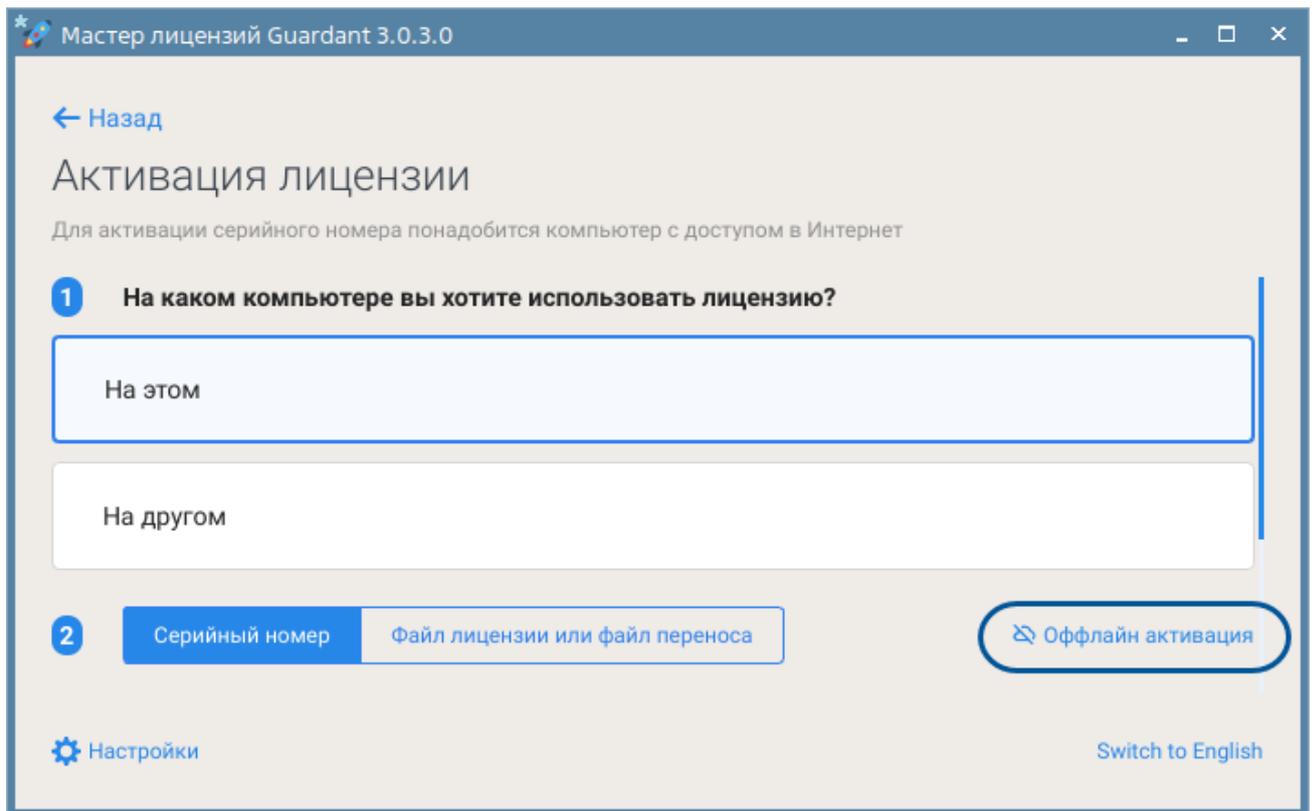


Активация на компьютере без доступа в Интернет

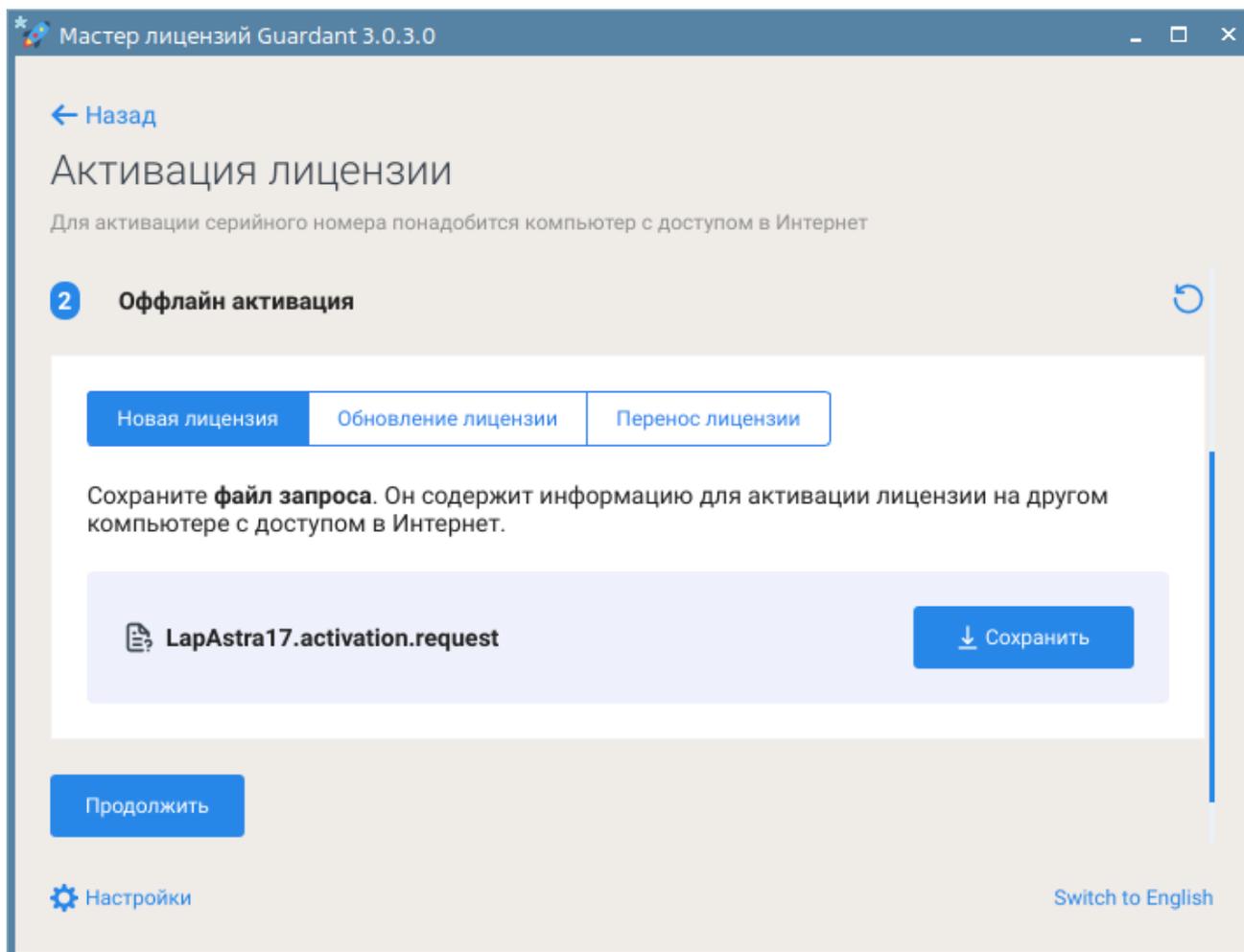
1. Запустите Мастер лицензий Guardant.
2. Нажмите **Активация лицензии**.



3. В окне **Активация лицензии** выберите компьютер, на котором будет использоваться лицензия - **На этом** и нажмите **Оффлайн активация**.



4. На вкладке **Новая лицензия** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата *.request и нажмите кнопку **Продолжить**.



5. Перейдите на компьютер с доступом в Интернет и запустите Мастер лицензий Guardant.

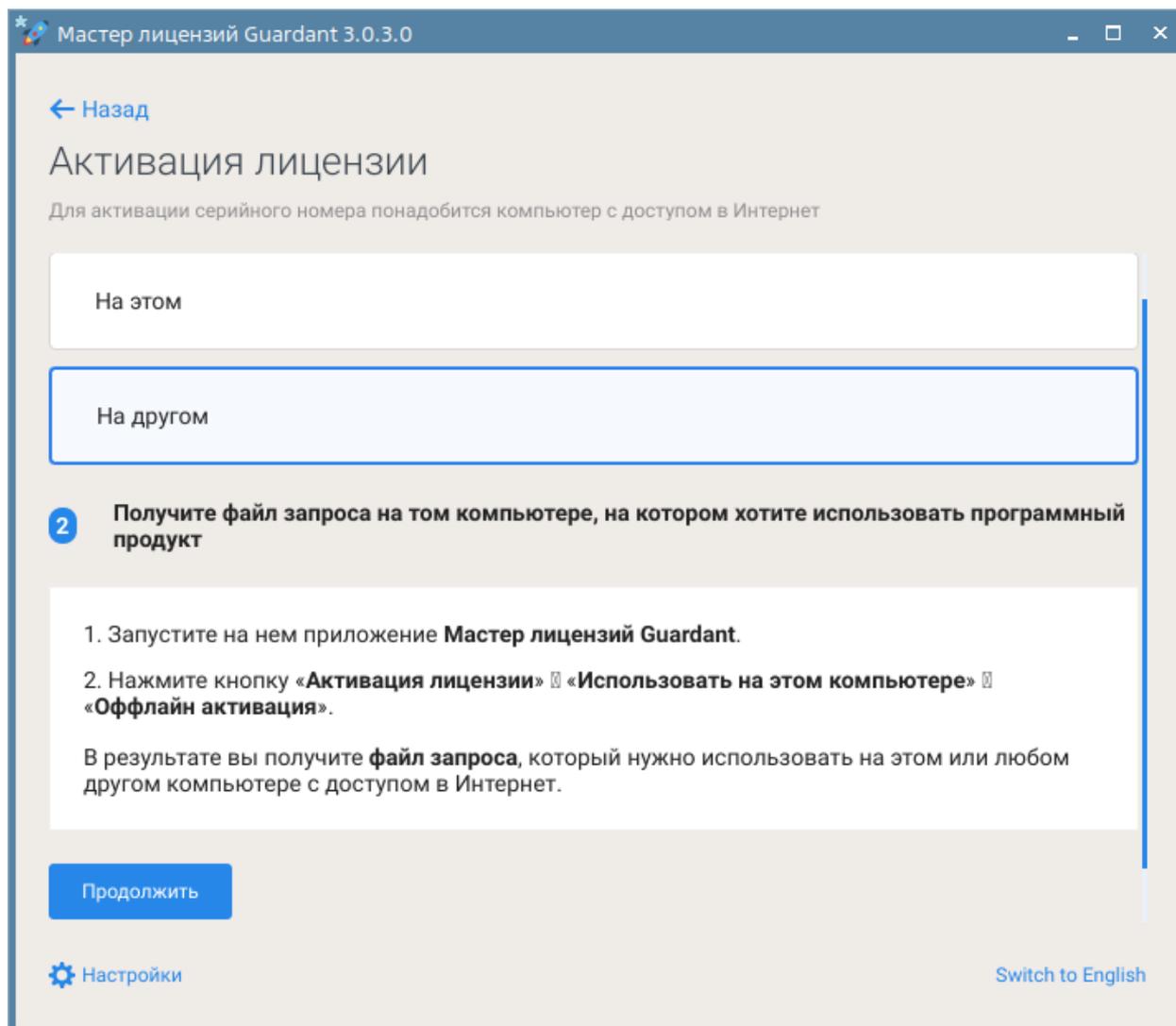
5.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.



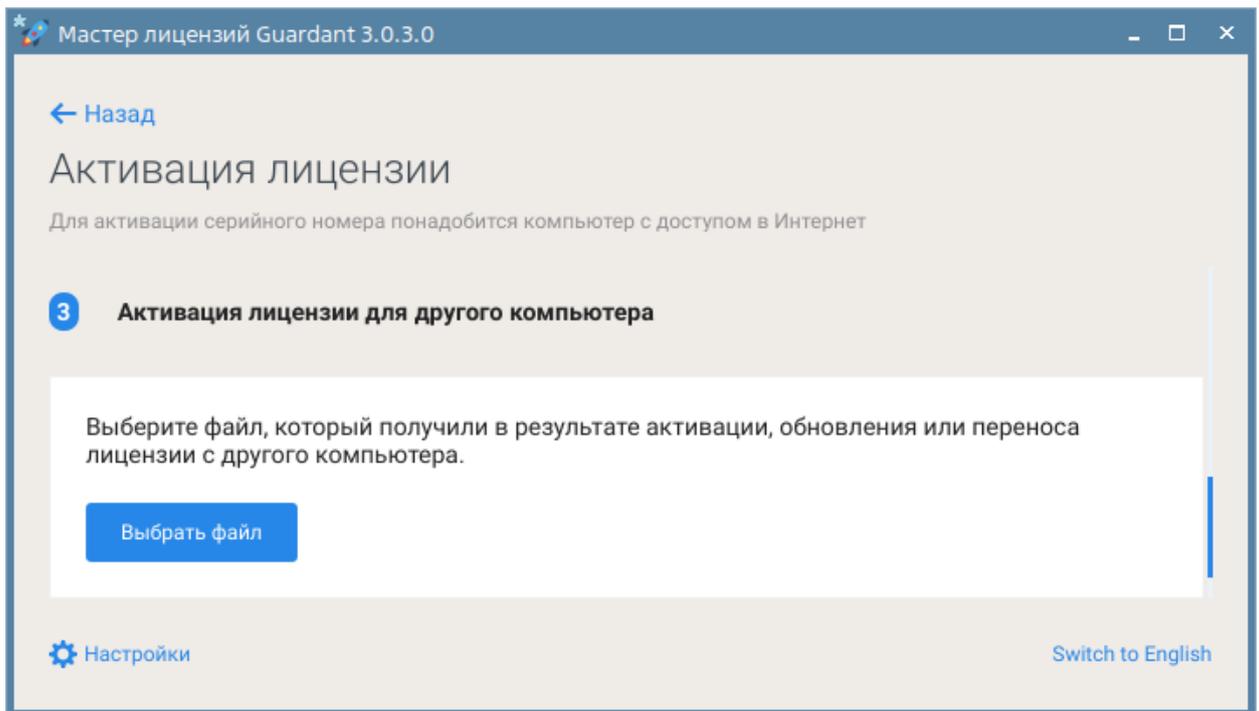
5.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензии**.



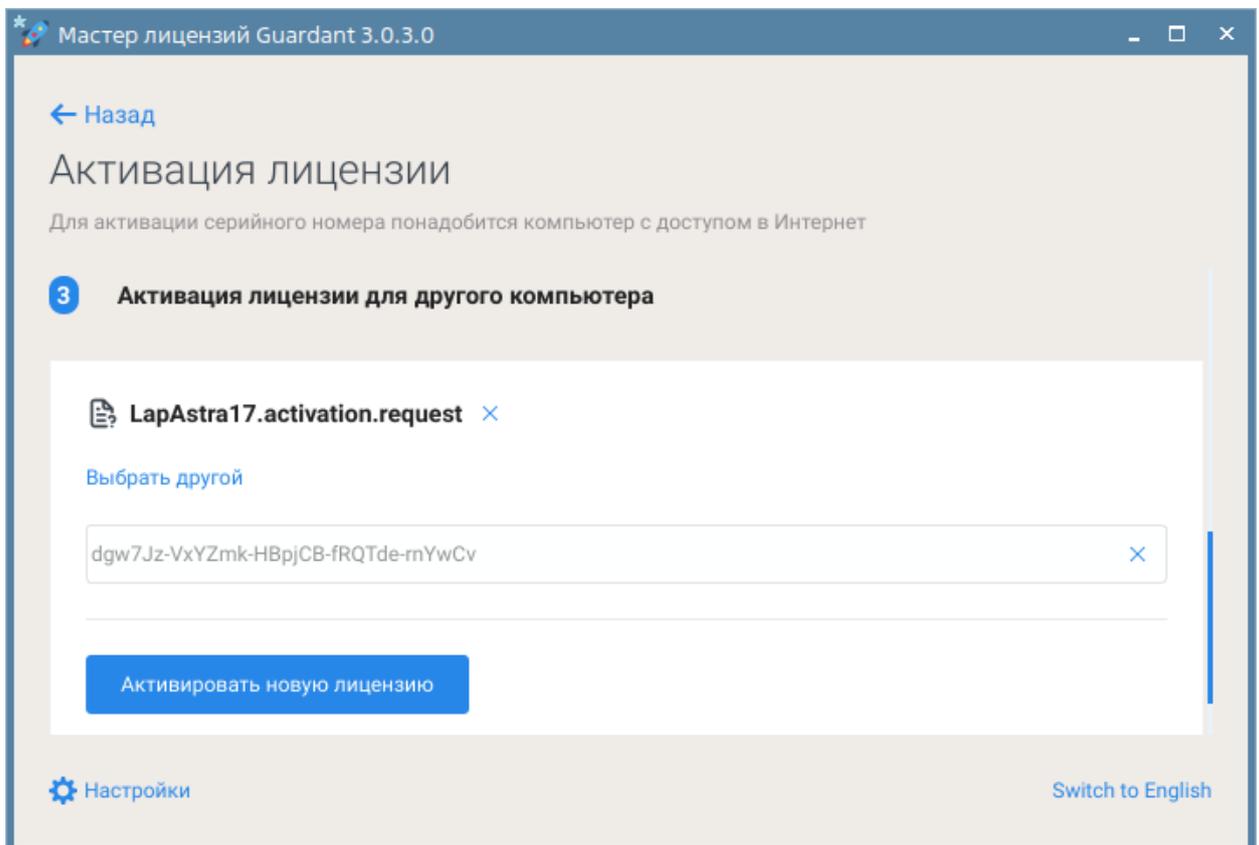
5.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



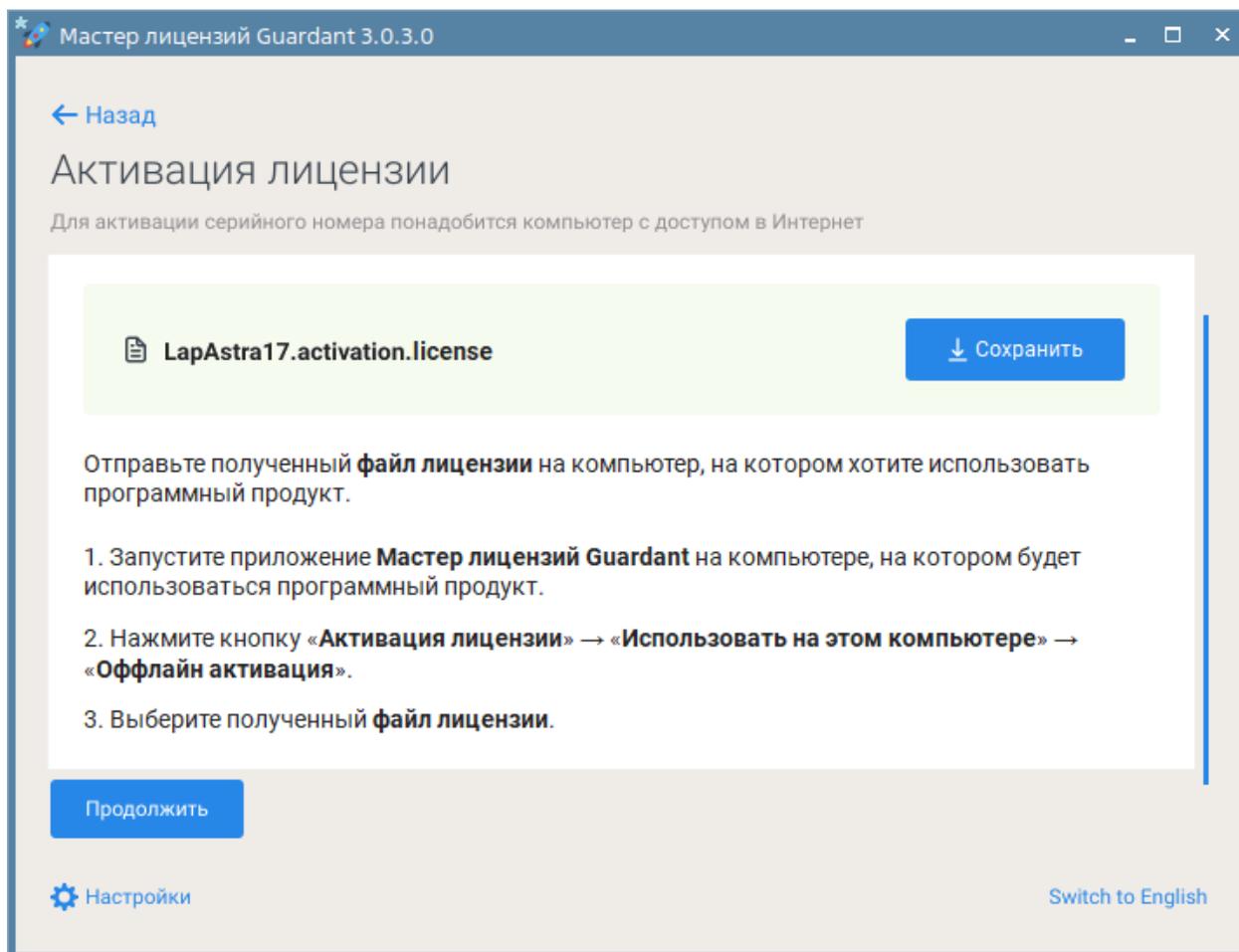
5.4. Нажмите кнопку **Выбрать файл** и выберите файл формата *.request, перенесенный с компьютера без доступа в Интернет.



5.5. Введите в поле ввода серийный номер программного ключа, указанный в сертификате, и нажмите кнопку **Активировать новую лицензию**.

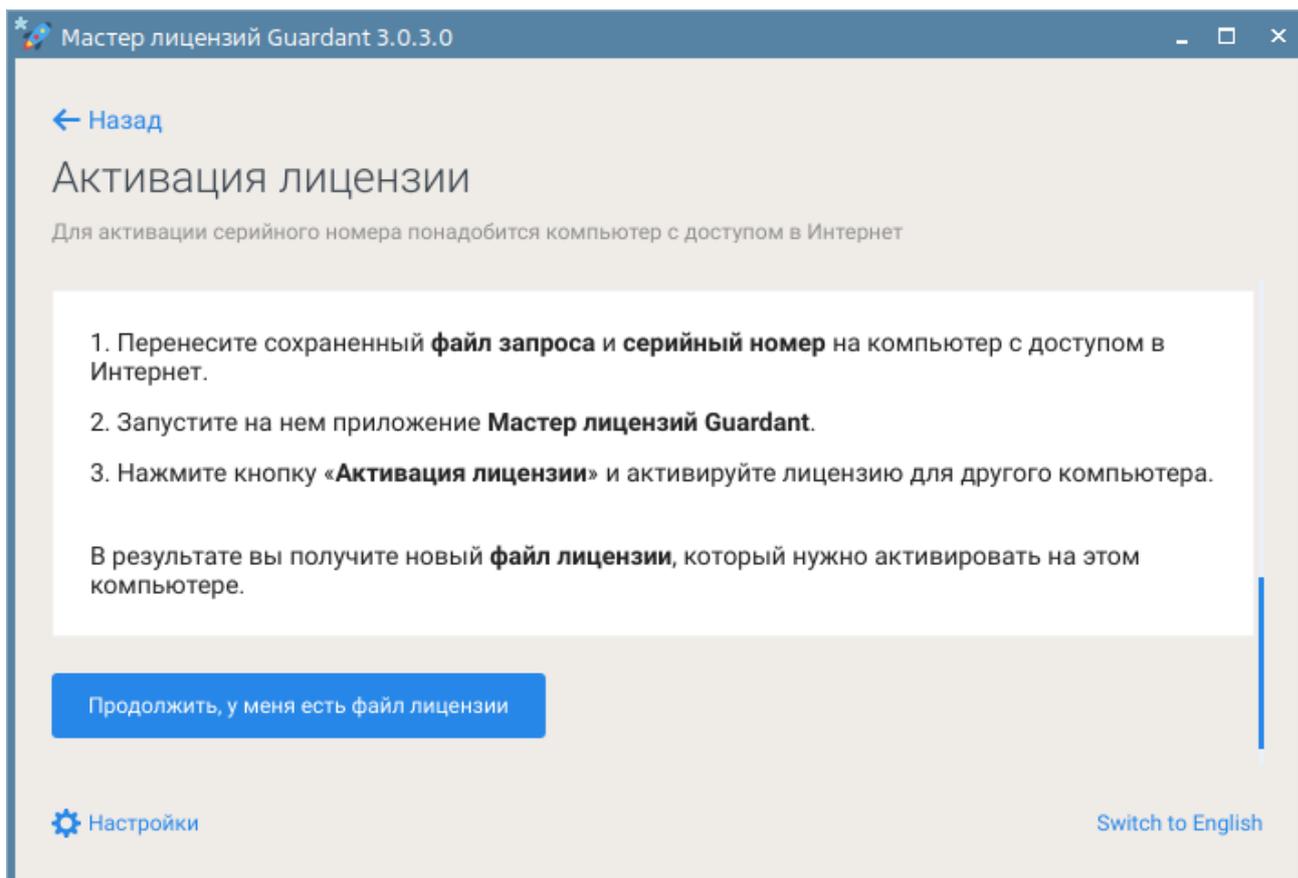


5.6. Нажмите кнопку **Сохранить** и сохраните на диске файл активации лицензии формата *.license.

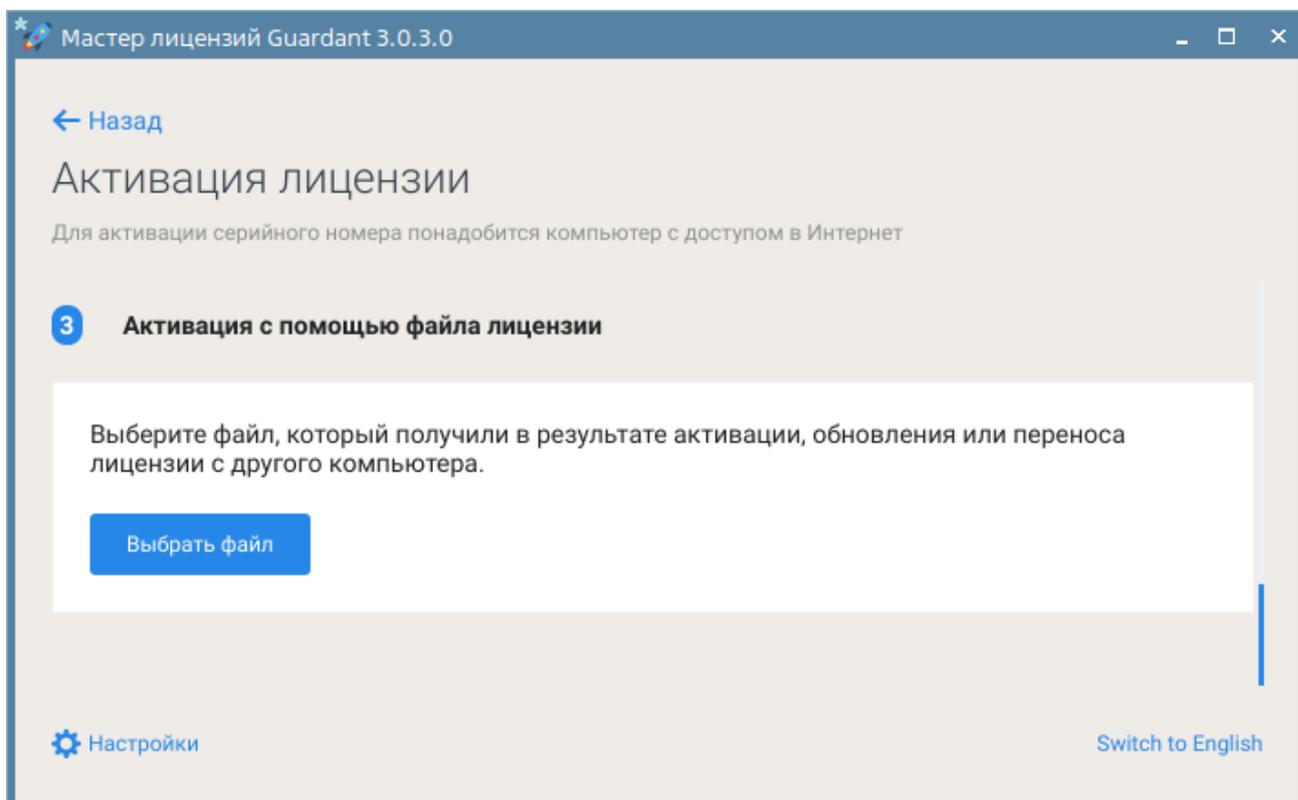


5.7. Перенесите полученный файл активации лицензии формата *.license на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

6. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

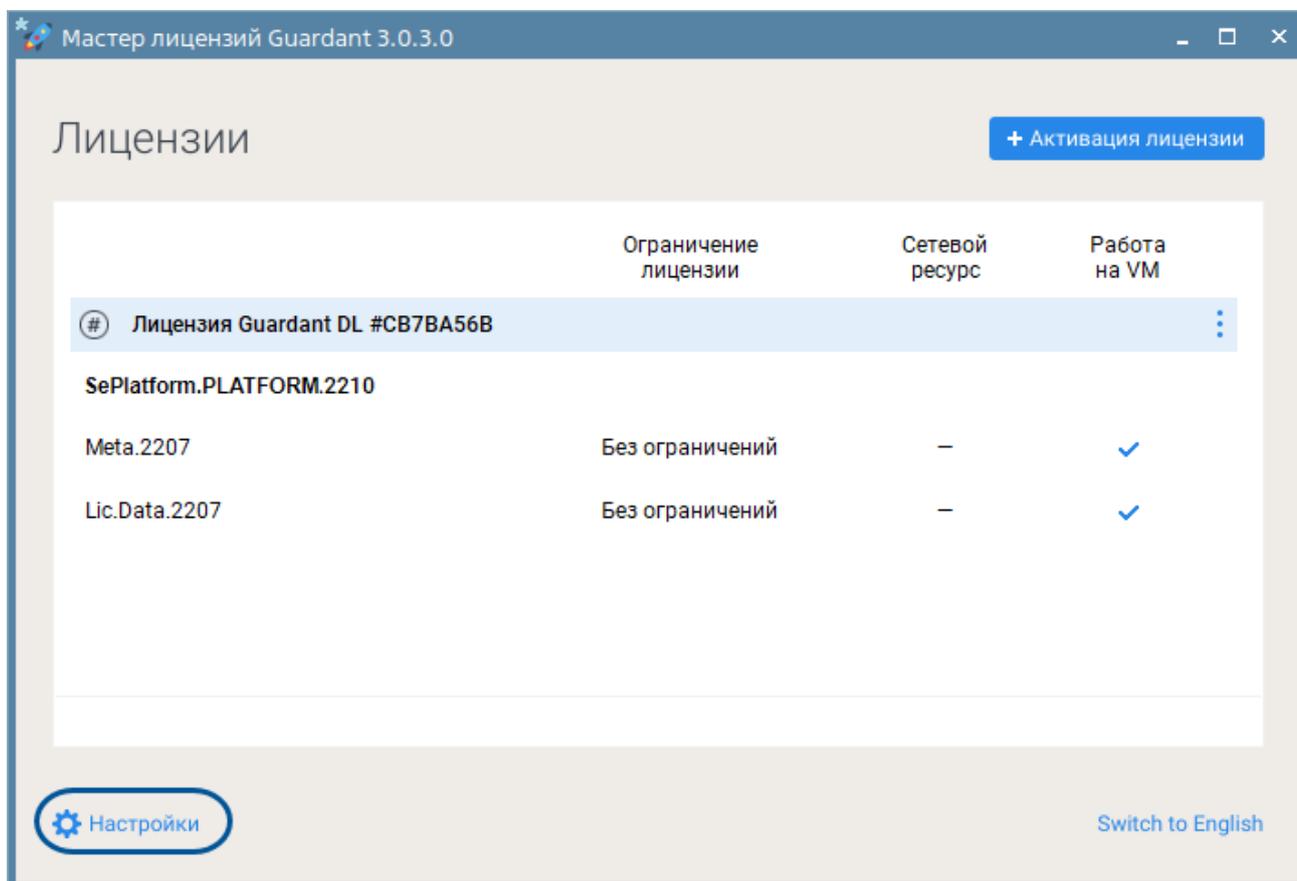


7. Нажмите кнопку **Выбрать файл** и выберите файл формата *.license, перенесенный с компьютера с доступом в Интернет.



Обновление на компьютере с доступом в Интернет

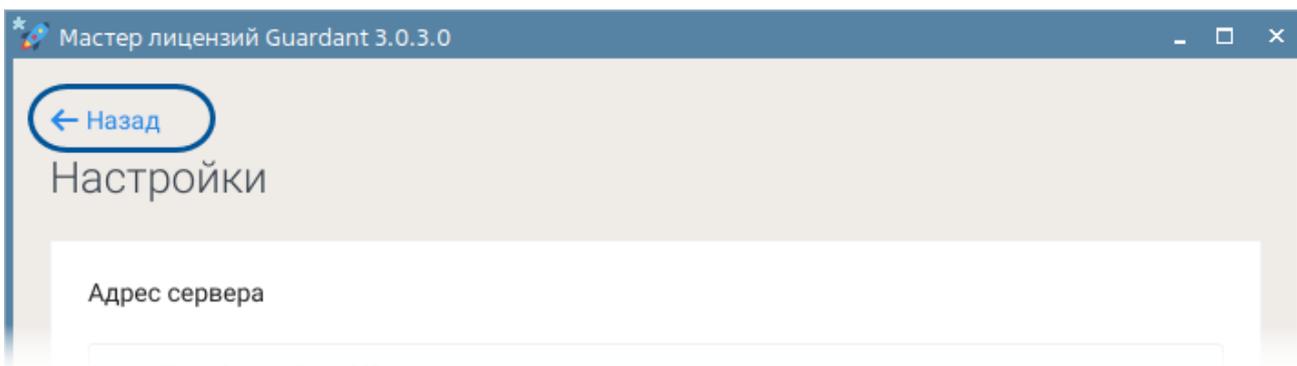
1. Запустите Мастер лицензий Guardant.
2. Перейдите в **Настройки**:



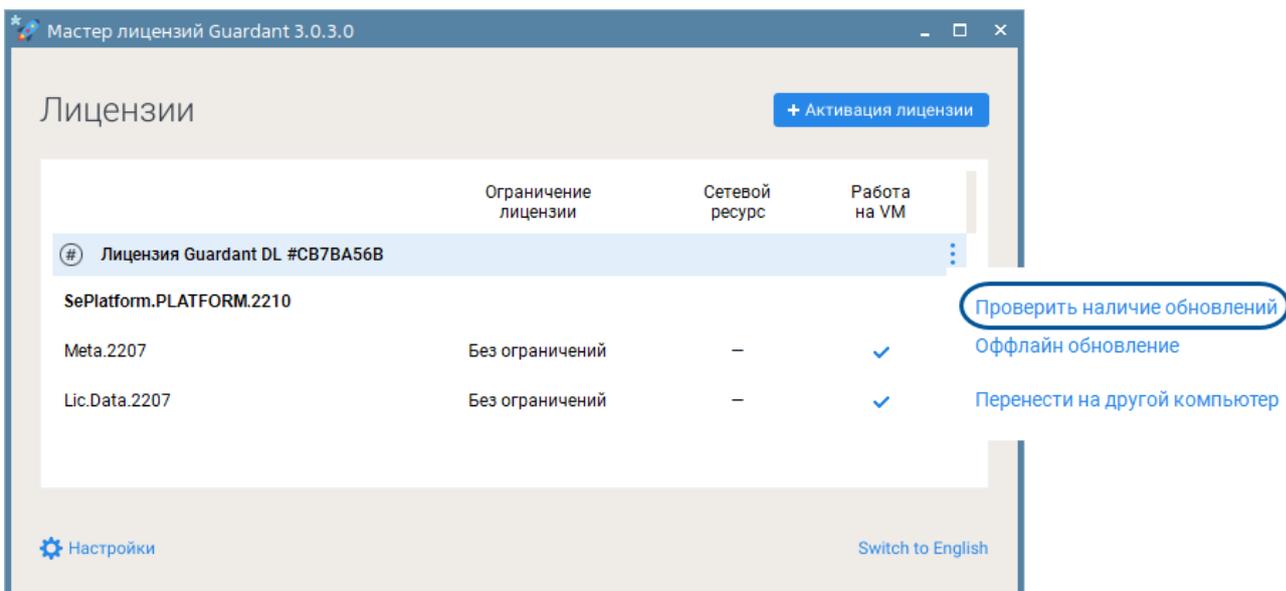
3. Укажите адрес сервера обновления лицензий:



4. Вернитесь в окно **Лицензии**, нажав **Назад**.



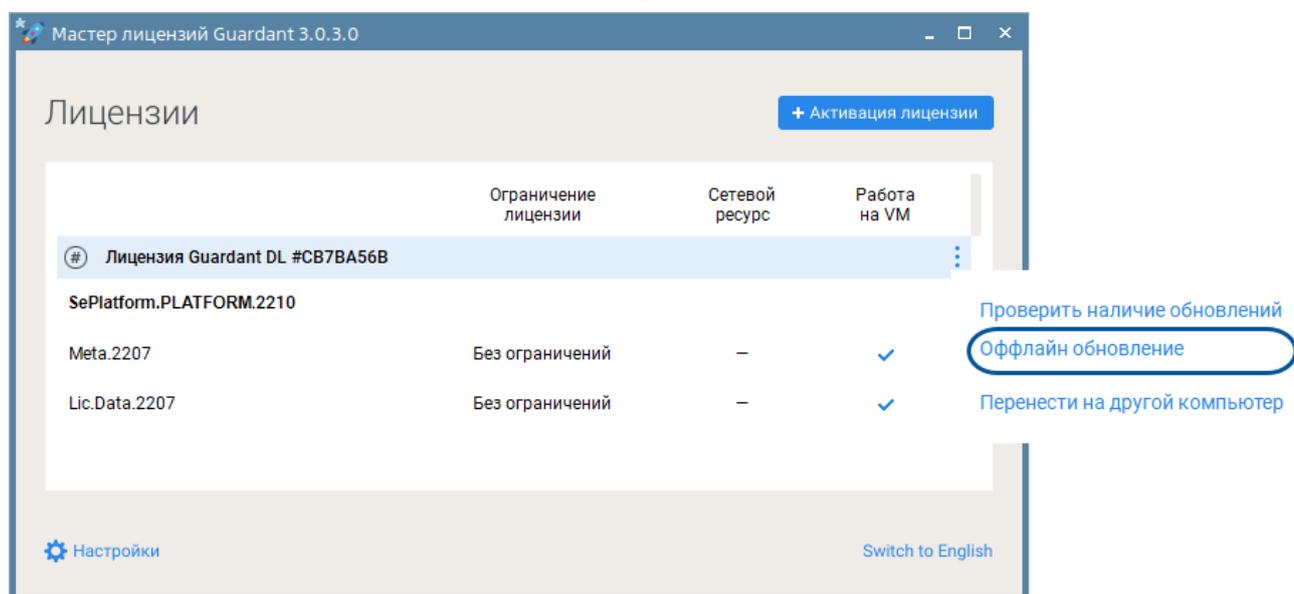
5. В окне **Лицензии** в меню ключа выберите команду **Проверить наличие обновлений**.



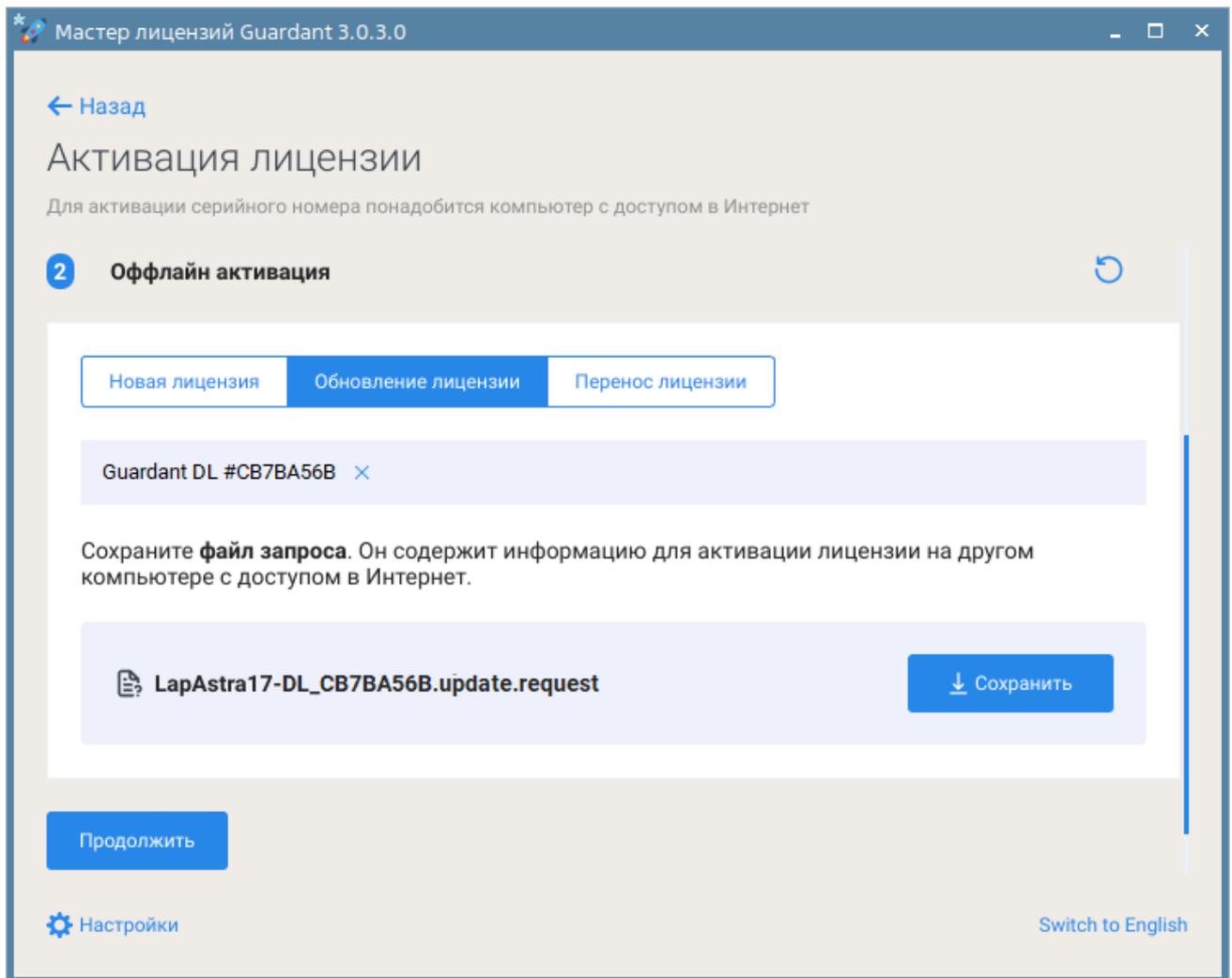
6. Если для ключа будут обнаружены обновления, то они отобразятся в списке **Обновления лицензий**. Для обновления лицензии ключа нажмите кнопку **Применить**.

Обновление на компьютере без доступа в Интернет

1. Запустите приложение Мастер лицензий Guardant.
2. В окне **Лицензии** в меню ключа выберите команду **Офлайн обновление**.



3. На вкладке **Обновление лицензии** нажмите кнопку **Сохранить**, сохраните на диске файл запроса формата *.request и нажмите кнопку **Продолжить**.



4. Перейдите на компьютер с доступом в Интернет и запустите приложение Мастер лицензий Guardant.

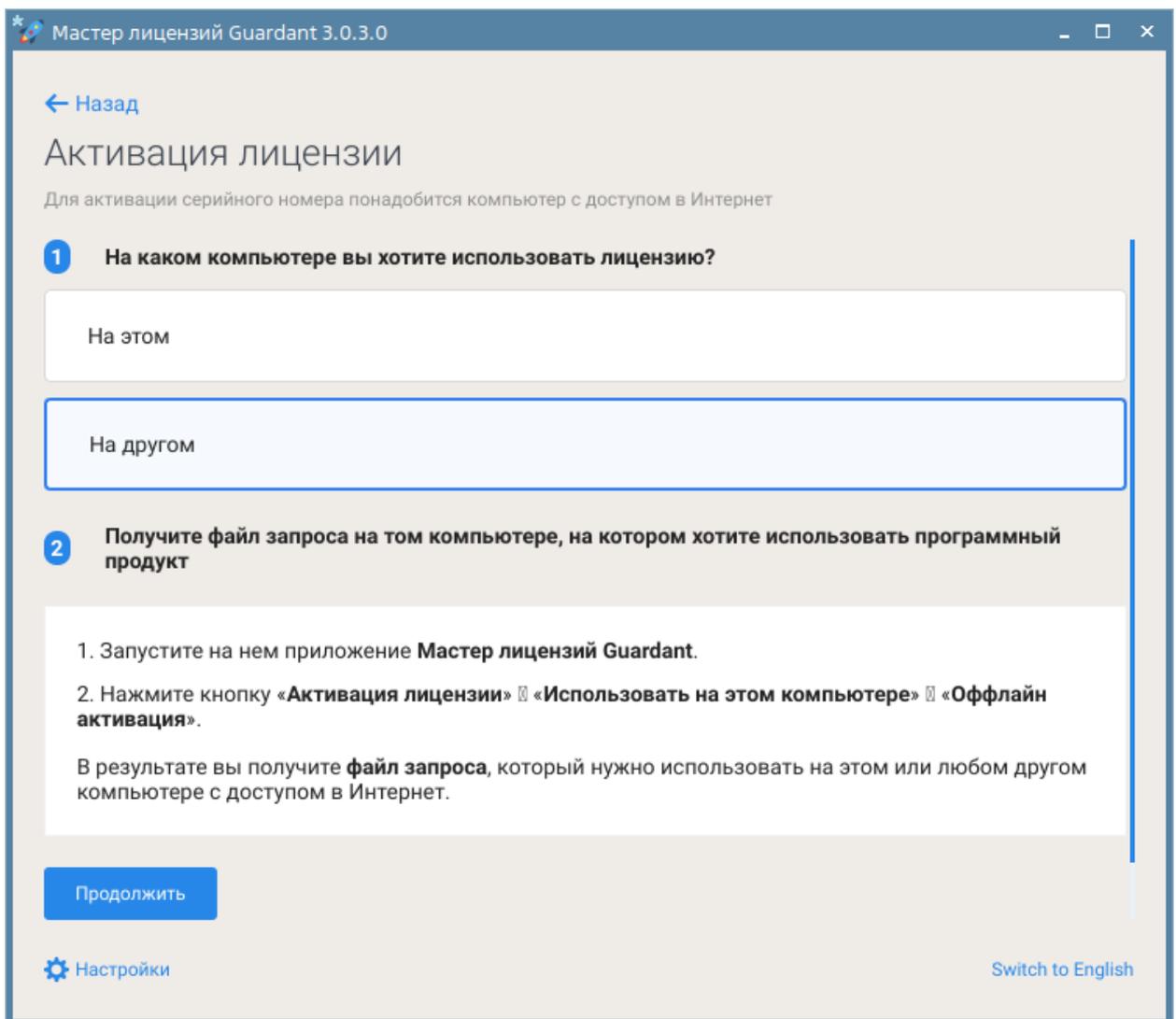
4.1. Перейдите в **Настройки** и укажите адрес сервера обновления лицензий.



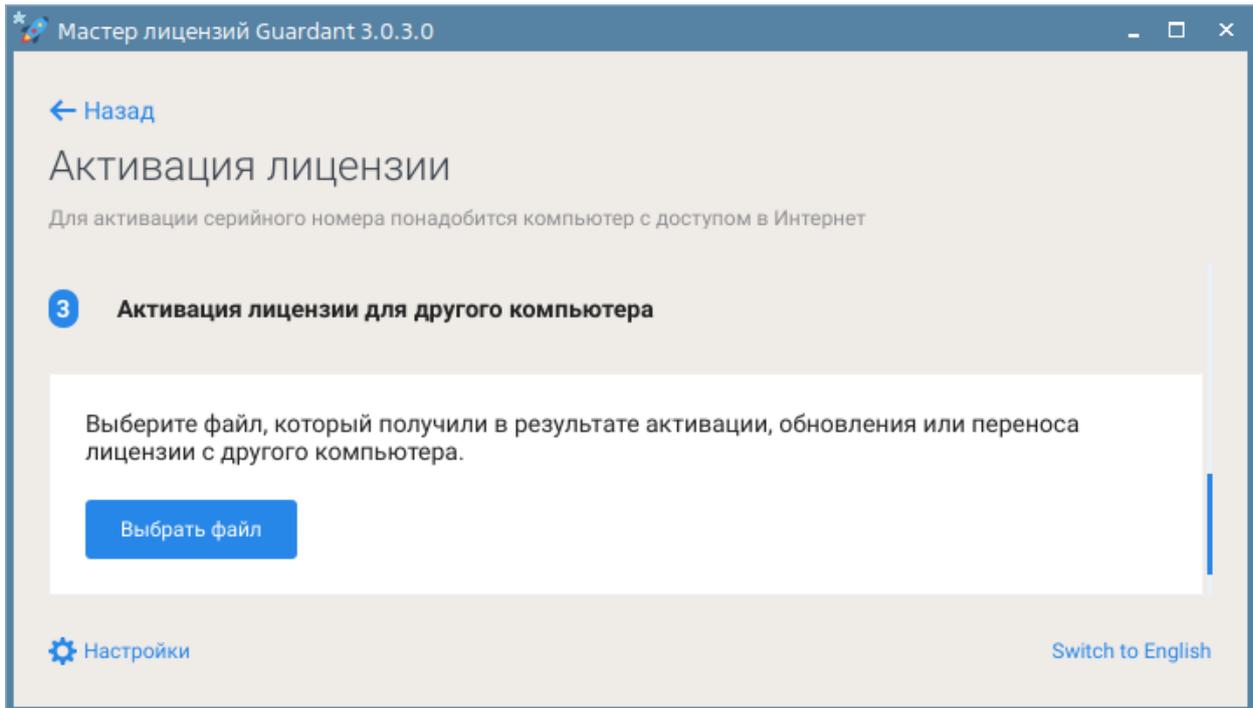
4.2. Вернитесь в окно **Лицензии** и нажмите кнопку **Активация лицензий**.



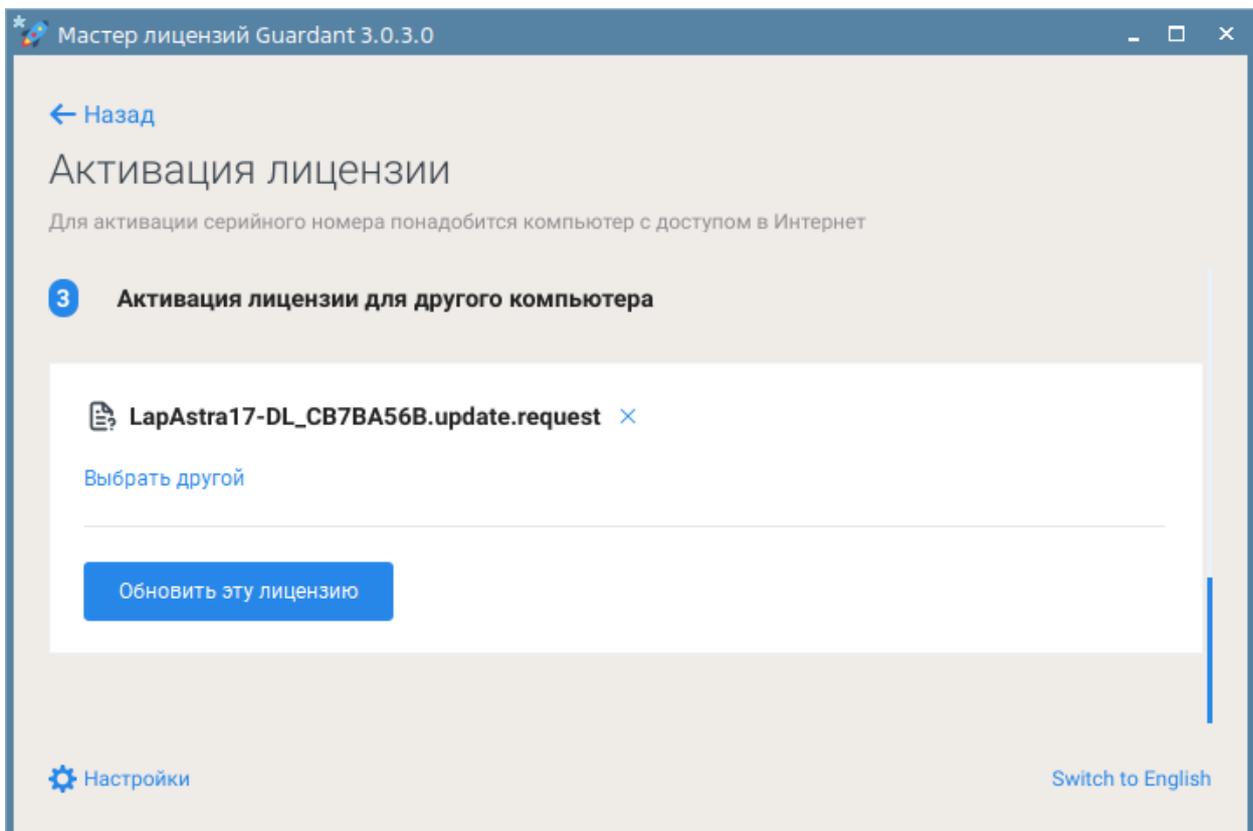
4.3. Укажите компьютер, на котором будет использоваться лицензия - **На другом** и нажмите кнопку **Продолжить**.



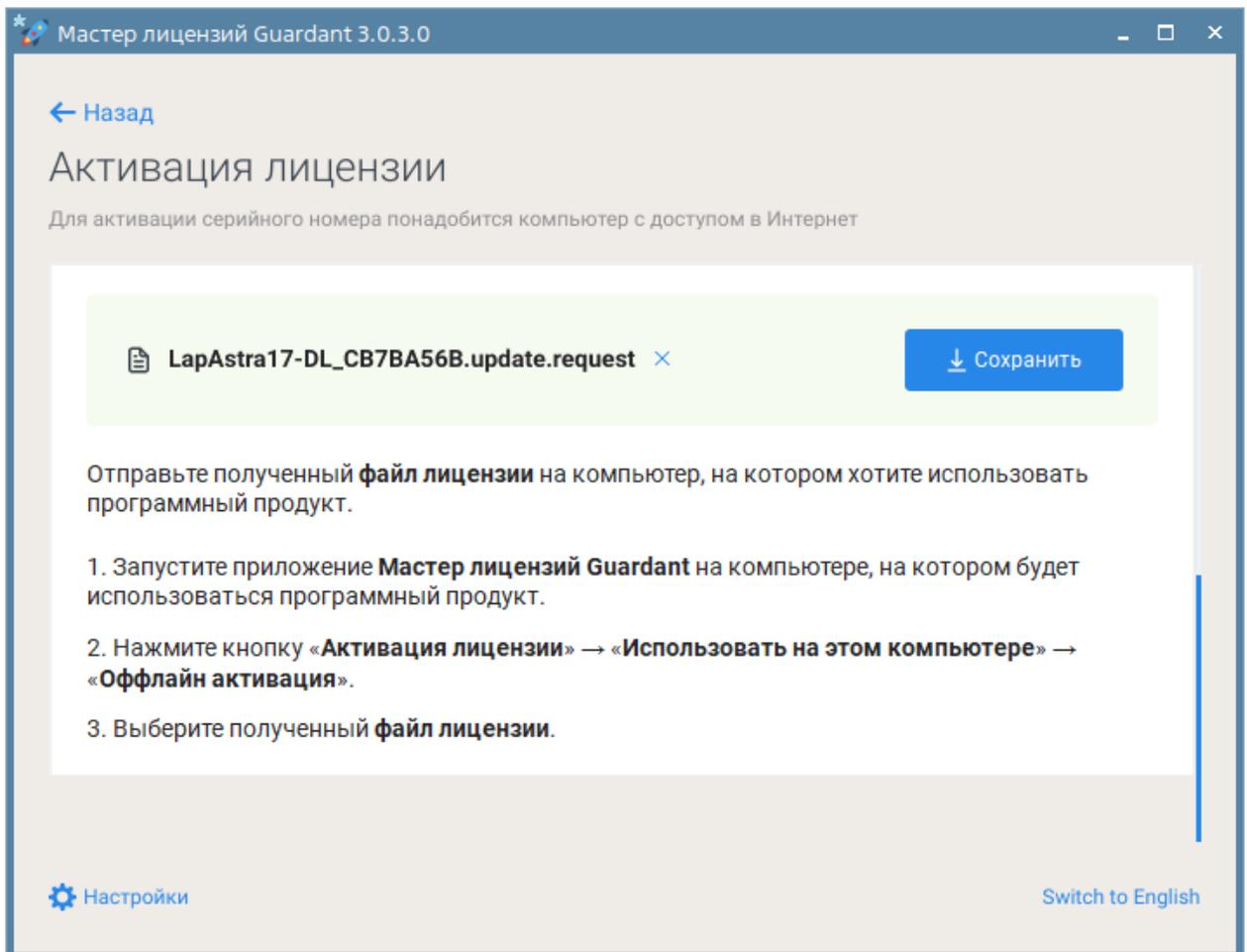
4.4. Нажмите кнопку **Выбрать файл** и выберите файл запроса формата *.request, перенесенный с компьютера без доступа в Интернет.



4.5. Нажмите кнопку **Обновить эту лицензию**.

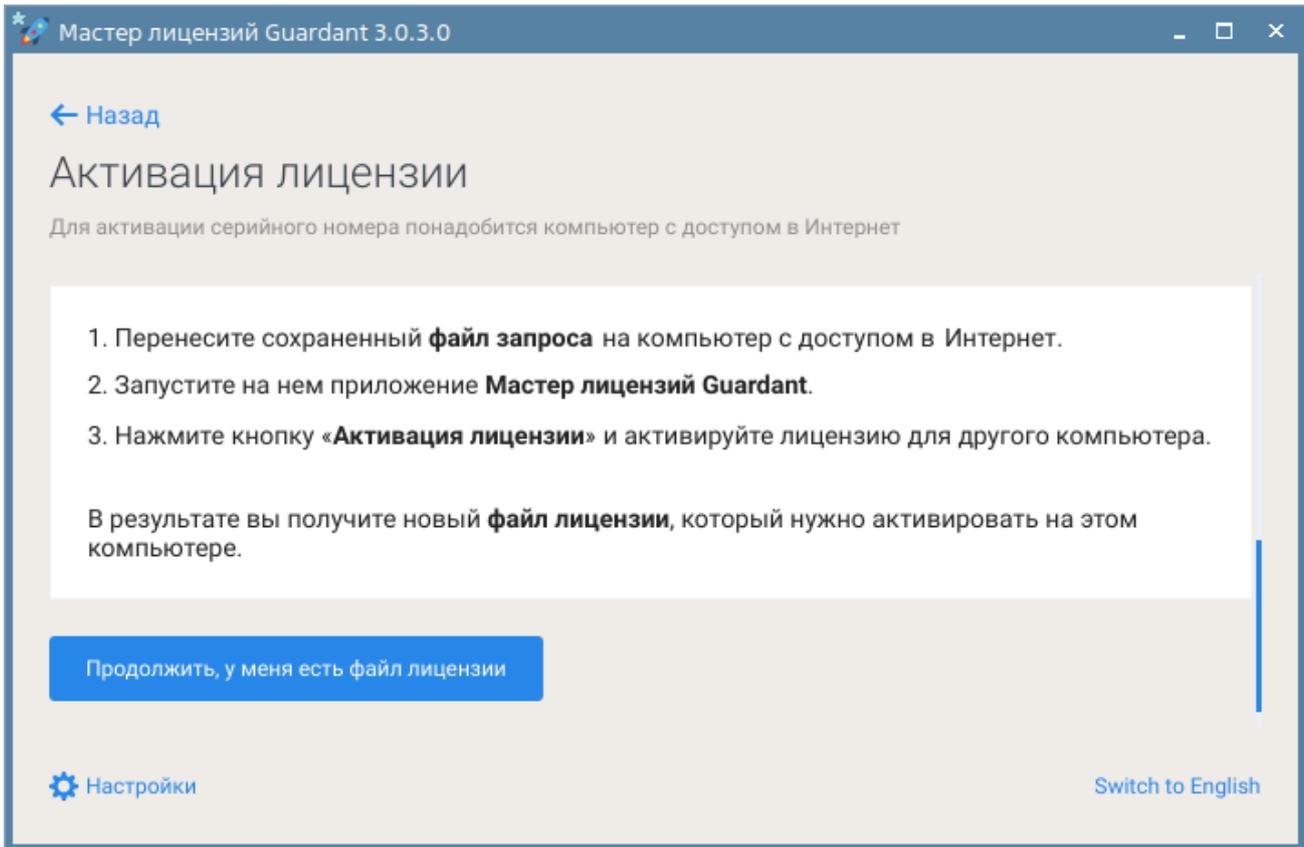


4.6. Нажмите кнопку **Сохранить** и сохраните на диске файл обновления лицензии формата *.license.

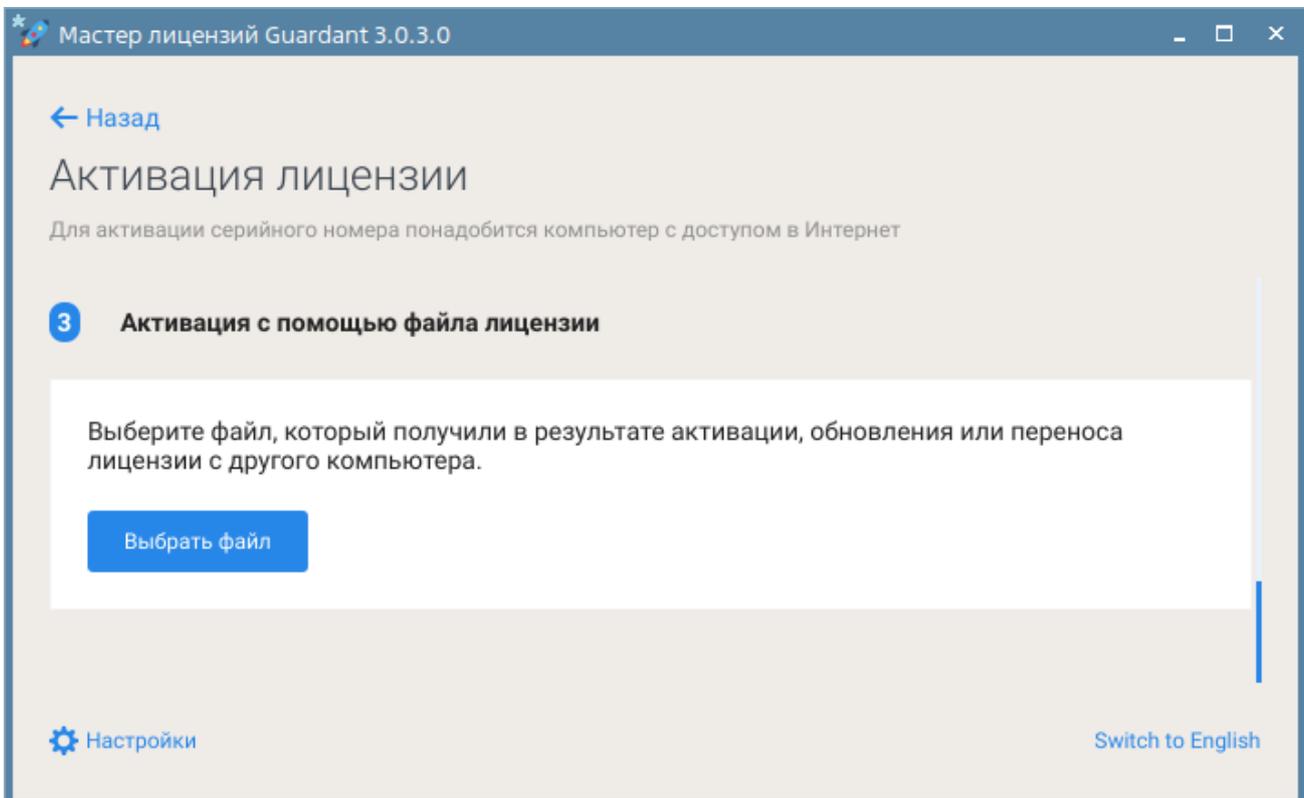


4.7. Перенесите полученный файл обновления лицензии формата *.license на компьютер без доступа в Интернет, на котором требуется активировать лицензию.

5. На компьютере без доступа в Интернет нажмите кнопку **Продолжить, у меня есть файл лицензии**.

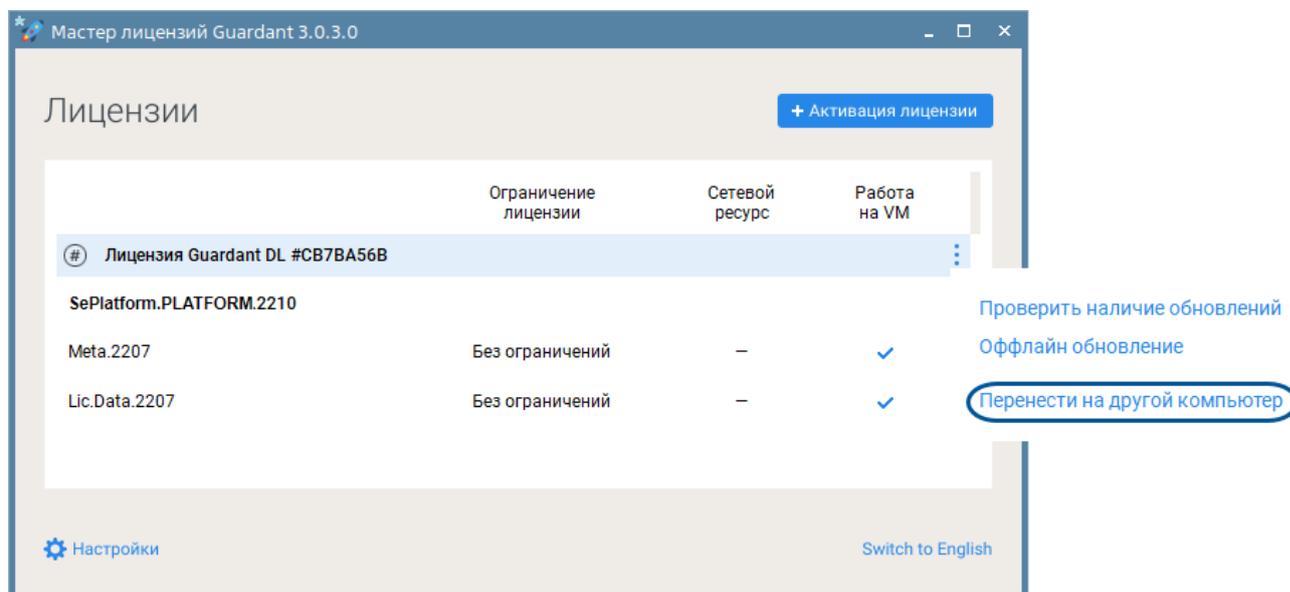


6. Нажмите кнопку **Выбрать файл** и выберите файл формата *.license, перенесенный с компьютера с доступом в Интернет.

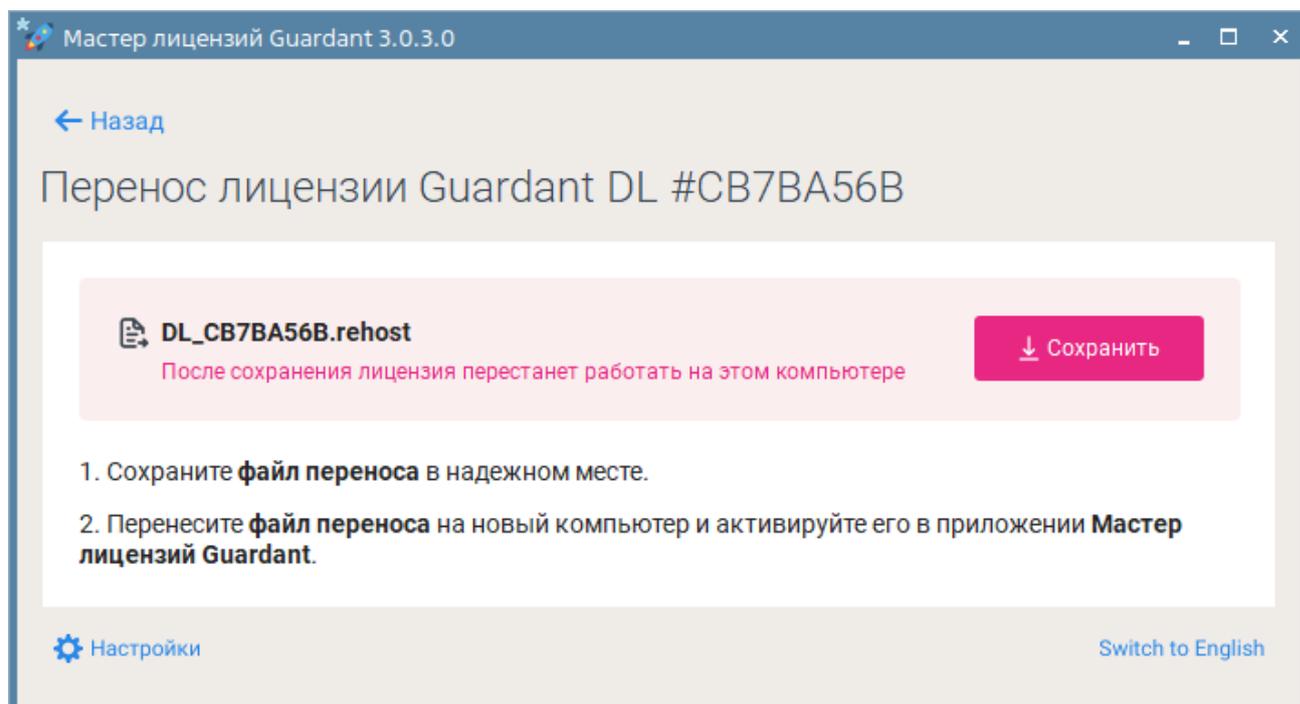


Перенос на другой компьютер

1. Запустите приложение Мастер лицензий Guardant.
2. В окне Лицензии в меню ключа выберите команду **Перенести на другой компьютер**.



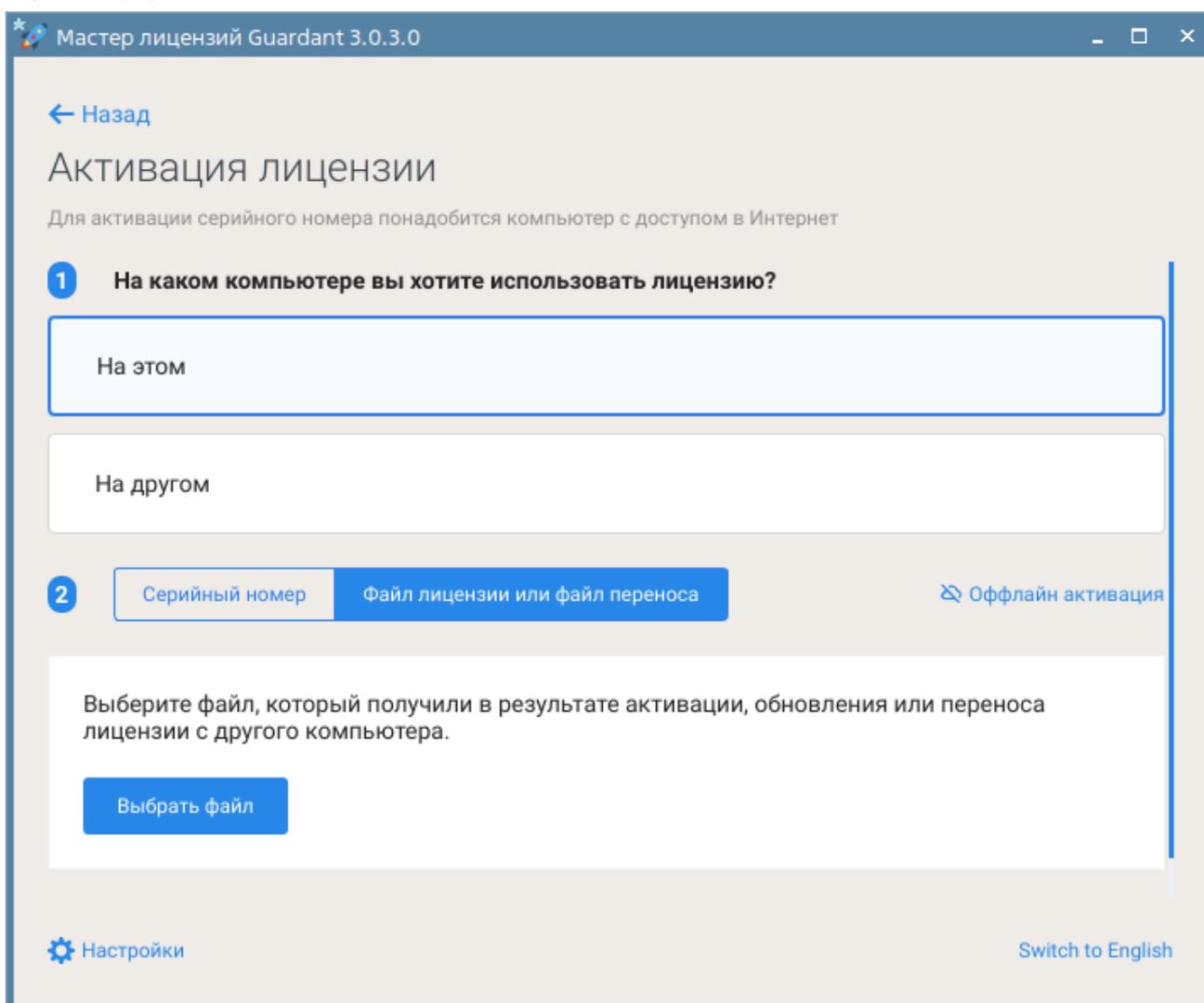
3. В окне **Перенос лицензии Guardant DL** нажмите кнопку **Сохранить** и сохраните на диске файл переноса формата *.rehost.



4. На другом компьютере запустите приложение Мастер лицензий Guardant и нажмите кнопку **Активация лицензии**.



5. Укажите компьютер, на котором будет использоваться лицензия - **На этом**, перейдите на вкладку **Файл лицензии** или **файл переноса**, нажмите кнопку **Выбрать файл** и выберите ранее сохраненный файл переноса формата *.rehost.



16.3. Решение проблем

В случае возникновения любых проблем при работе с аппаратными или программными ключами Систэм Платформ отправляйте на адрес электронной почты support@systeme.ru письмо, содержащее:

- ключ продукта или ID ключа, указанный в сертификате из комплекта поставки;
- описание возникшей проблемы.

17. Безопасное администрирование

Чтобы избежать сбоев в работе компонентов Систэм Платформ и снизить вероятность возникновения уязвимостей проекта автоматизации технологического процесса, следуйте рекомендациям по безопасному администрированию.

Несоблюдение рекомендаций может повлечь:

- потерю технологических данных;
- подачу ложных команд управления технологическому оборудованию;
- возникновение аварийных ситуаций;
- несвоевременное оповещение о наступивших событиях и авариях;
- потерю контроля над ходом технологического процесса;
- остановку технологического оборудования;
- нарушение безопасности производства;
- действие вредоносных программ.

Последствиями могут стать:

- финансовые потери предприятия;
- ситуации, связанные с потерей здоровья и жизни людей;
- техногенные аварии;
- экологические катастрофы.

17.1. Общие рекомендации

Ограничивайте доступ к техническим средствам

Чтобы предотвратить несанкционированный доступ посторонних лиц и негативное воздействие окружающей среды (пыль, влага), рекомендуем размещать технические средства (серверы, АРМ, сетевое оборудование) в серверных шкафах.

Несоблюдение данной рекомендации может привести к прекращению или сбоям в работе компонентов Систэм Платформ в результате:

- отключения оборудования;
- отсоединения кабелей;
- порчи или кражи оборудования;
- прочих физических воздействий, приводящих к отключению или поломке технических средств.

Используйте IPSec

Чтобы предотвратить несанкционированный доступ к сети и перехват пакетов данных, передаваемых по межсетевому протоколу IP, рекомендуем использовать IPSec в туннельном режиме для организации безопасного сетевого взаимодействия между удаленными компонентами Систэм Платформ.

Несоблюдение данной рекомендации несет угрозу перехвата, просмотра, изменения и прочих нежелательных действий с пакетами данных, передаваемыми между удаленными компонентами Систэм Платформ.

Ограничивайте число портов, используемых DCOM

Чтобы предотвратить несанкционированный доступ и повысить безопасность сетевого взаимодействия между удаленными компонентами Систэм Платформ, рекомендуем ограничивать число портов, используемых DCOM, до определенного диапазона. Затем рекомендуем настраивать межсетевой экран (брандмауэр):

- запретить входящий трафик на узел OPC;
- разрешить входящий трафик определенных узлов OPC через порт TCP 135;
- разрешить входящий трафик определенных узлов OPC через некоторый диапазон портов TCP.

Несоблюдение данной рекомендации несет угрозу несанкционированного подключения к сети, сетевых атак, проникновения вредоносных программ и других сетевых угроз, способных вызвать серьезные сбои в работе компонентов Систэм Платформ.

Используйте антивирусное ПО и обновляйте антивирусные базы

Чтобы избежать заражения серверов и АРМ компьютерными вирусами, рекомендуем использовать антивирусное ПО и регулярно обновлять антивирусные базы.

Антивирусное ПО, совместимое с Систэм Платформ:

- Антивирус Касперского;
- Avast Antivirus;
- Антивирус Dr.Web;
- ESET NOD32 Антивирус;
- Symantec Antivirus.

Несоблюдение данной рекомендации может привести к серьезным сбоям в работе компьютеров при заражении вирусами, например:

- внезапная перезагрузка или невозможность включения;
- вывод на экран посторонних сообщений;
- блокировка компьютера;
- замедление работы;
- удаление или изменение файлов приложений;
- форматирование жесткого диска;
- другие непредсказуемые ситуации.

Сбои в работе компьютеров приводят к замедлению, сбоям и прекращению работы компонентов Систэм Платформ.

Отключайте автоматическое обновление ПО

Чтобы избежать сбоев в работе серверов и АРМ, рекомендуем отключать автоматическое обновление ОС и антивирусного ПО.



ОБРАТИТЕ ВНИМАНИЕ

Обновлять ОС, антивирусное ПО, компоненты Систэм Платформ и ПО проекта автоматизации рекомендуем во время плановых работ по техническому обслуживанию и ремонту.

Несоблюдение данной рекомендации повышает вероятность сбоя в работе компонентов Систэм Платформ.

Блокируйте доступ к информации на внешнем накопителе

Чтобы предотвратить несанкционированное использование внешних накопителей, рекомендуем блокировать порты USB и приводы оптических дисков для учетных записей пользователей.



ПРИМЕЧАНИЕ

Подключив к системному блоку внешний накопитель, пользователь не увидит его в папке Мой компьютер или доступ к нему будет запрещён.

Несоблюдение данной рекомендации может привести к заражению компьютеров вредоносными программами, содержащимися на накопителях, а также утечке конфиденциальной информации предприятия.

Ограничивайте права и количество учетных записей пользователей

Чтобы предотвратить несанкционированный доступ к ПО серверов и АРМ, рекомендуем включать только учетные записи пользователей, предусмотренные проектом автоматизации. Для каждой учетной записи:

- устанавливайте сложные пароли;
- ограничивайте права пользователя в использовании ПО рамками должностных обязанностей.

Несоблюдение данной рекомендации несет угрозу несанкционированного доступа к ПО пользователей, не обладающих необходимыми знаниями, что может привести к ошибкам в работе с ПО, компонентами Систэм Платформ и управлении технологическим процессом.

Минимальные права учётной записи для запуска компонентов Систэм Платформ

Приложения и службы выполняются с правами учётной записи, от имени которой они запущены:

- Приложения запускаются от имени учётной записи пользователя, запустившего приложение.
- Службы по умолчанию запускаются от имени системной учётной записи LocalSystem - это специальная учётная запись, которую создаёт система. Для каждой службы можно изменить учётную запись, от имени которой она запускается ([стр. 106](#)).

Системная учётная запись обладает полными правами в системе. Права прочих учётных записей определяются системными группами пользователей, в которую эти учётные записи включены: Пользователи, Опытные пользователи, Администраторы и другие.

В таблице ниже для приложений и служб Систэм Платформ приведены требования к правам учётной записи, чтобы запущенное от её имени приложение/служба могли выполнять свои функции.

Компонент	Минимальные права учётной записи
SePlatform.Data collection Server SePlatform.AccessPoint	Для службы - системная учётная запись. Для сервисных приложений - Пользователь.
SePlatform.Historian	Системная учётная запись.
SePlatform.Development Studio	Пользователь.
SePlatform.HMI	Пользователь.

Компонент	Минимальные права учётной записи
SePlatform.Mapping Server	Сетевая служба (NetworkService).
SePlatform.Security	Пользователь. Для конфигурирования - Администратор.

Изменение учётной записи, от имени которой запускается служба

ОС Windows

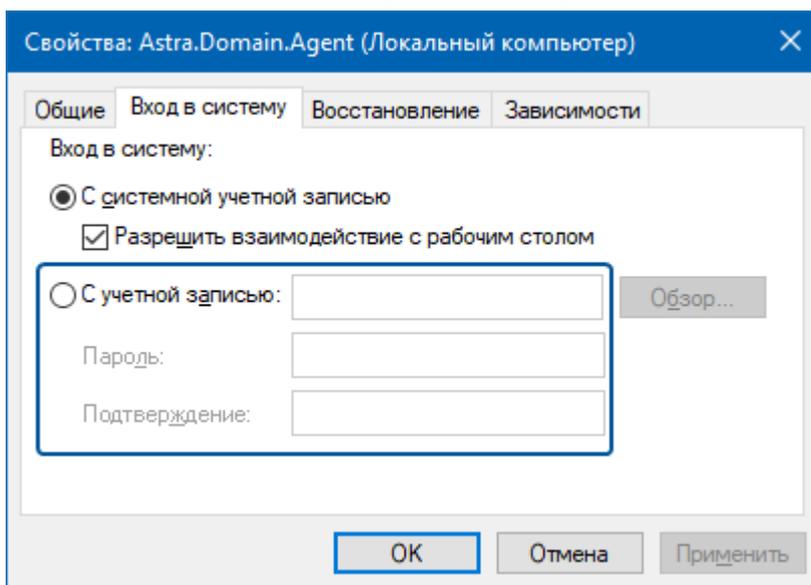
1. Откройте список служб.

Сделать это можно:

- в диспетчере задач на вкладке **Службы**
- открыть окно запуска «Win» + «R» и ввести

```
services.msc
```

2. В списке выберите службу и в контекстном меню откройте её свойства.
3. На вкладке **Вход в систему** укажите учётную запись, от имени которой служба будет исполняться.



ОБРАТИТЕ ВНИМАНИЕ

Если пароль пользователя впоследствии изменится, в свойствах службы он не обновится: потребуется повторно зайти в свойства службы и изменить пароль пользователя.

4. Чтобы изменения вступили в силу, перезапустите службу.



ОБРАТИТЕ ВНИМАНИЕ

Выполненные настройки сбрасываются при удалении или переустановке. Поэтому описанную выше настройку нужно выполнять после каждой установки; например, после установки более новой версии.

ОС Linux

Сервисы компонентов Систэм Платформ по умолчанию запускаются от имени суперпользователя «root». Для сервисов SePlatform.Data collection Server, SePlatform.AccessPoint, SePlatform.Historian и приложения SePlatform.HMI возможно переназначить пользователя, от имени которого будет запускаться сервис/приложение.

**ОБРАТИТЕ ВНИМАНИЕ**

Для работы сервисов SePlatform.Security и SePlatform.Domain требуются права суперпользователя «root», поэтому переназначать пользователя не рекомендуется.

**ОБРАТИТЕ ВНИМАНИЕ**

Для работы SePlatform.Mapping Server права суперпользователя «root» не требуются.

Чтобы сменить пользователя для сервисов SePlatform.Data collection Server, SePlatform.AccessPoint и SePlatform.Historian:

1. Откройте файл:

- /lib/systemd/system/seplatform-server.service (SePlatform.Data collection Server и SePlatform.AccessPoint);
- /lib/systemd/system/seplatform-historian-server.service (SePlatform.Historian).

2. В строках

```
User=root  
Group=root
```

измените пользователя «root» на пользователя, например, с пониженными привилегиями.

3. Чтобы применить измененную конфигурацию, выполните команду

```
sudo systemctl daemon-reload
```

4. Назначьте указанного выше пользователя владельцем папки с сервером (для SePlatform.Historian - папки с базой данных). Для этого выполните команду

```
sudo chown -R <user>;<group> /opt/SePlatform/SePlatform.Data collection Server/ (для  
SePlatform.Data collection Server и SePlatform.AccessPoint)  
sudo chown -R <user>;<group> <DatabasePath> (для SePlatform.Historian)
```

Чтобы запускать SePlatform.HMI от пользователя, отличного от «root», нужно назначить выбранного пользователя владельцем папки, в которой хранится проект. Для назначения владельца папки выполните команду

```
sudo chown -R <user>;<group> <ProjectPath>
```

Ограничивайте права доступа к системным папкам

Чтобы предотвратить несанкционированный доступ к файлам ОС и компонентов Систэм Платформ, рекомендуем ограничивать права доступа к системным папкам.

**ВАЖНО**

Не рекомендуем изменять права доступа к каталогам, в которые устанавливаются компоненты Систэм Платформ.

**ОБРАТИТЕ ВНИМАНИЕ**

Дистрибутивы компонентов Систэм Платформ не изменяют стандартные права доступа к системным каталогам.

Несоблюдение данной рекомендации несет угрозу подмены компонентов Систэм Платформ вредоносными программами, что может привести к серьезным сбоям в работе проекта автоматизации и всего технологического процесса.

17.2. Рекомендации, применимые для компонентов Систэм Платформ

Используйте системы контроля версий

Чтобы избежать утраты исходных файлов ПО проекта автоматизации, рекомендуем использовать системы контроля версий для хранения и контроля версионности исходных файлов проектов SePlatform.Development Studio и SePlatform.HMI.

Несоблюдение данной рекомендации повышает риск использования устаревших версий исходных файлов проекта автоматизации для доработок и корректировок.

Используйте пароли для доступа к SePlatform.Data collection Server и SePlatform.AccessPoint

Чтобы предотвратить несанкционированный доступ из сервисных приложений Конфигуратор, Статистика и Управляющий, настоятельно рекомендуем использовать пароли для доступа к SePlatform.Data collection Server и SePlatform.AccessPoint.

Несоблюдение данной рекомендации несет угрозу несанкционированных действий:

- изменение конфигураций;
- просмотр статистики;
- управление сервером или резервной парой серверов;
- несанкционированный обмен данными.

Несанкционированный доступ и действия могут стать причиной серьезных сбоев в работе компонентов Систэм Платформ, проекта автоматизации и всего технологического процесса.

18. Правила брандмауэра

Для корректной работы компонентов Систэм Платформ в системе, где используется брандмауэр, необходимо настроить правила для входящих и исходящих подключений.

В правилах для входящих подключений следует разрешить подключения к портам, через которые компоненты Систэм Платформ получают данные.

В правилах для исходящих подключений следует разрешить подключения к портам, через которые компоненты Систэм Платформ отправляют данные.

18.1. ОС Windows

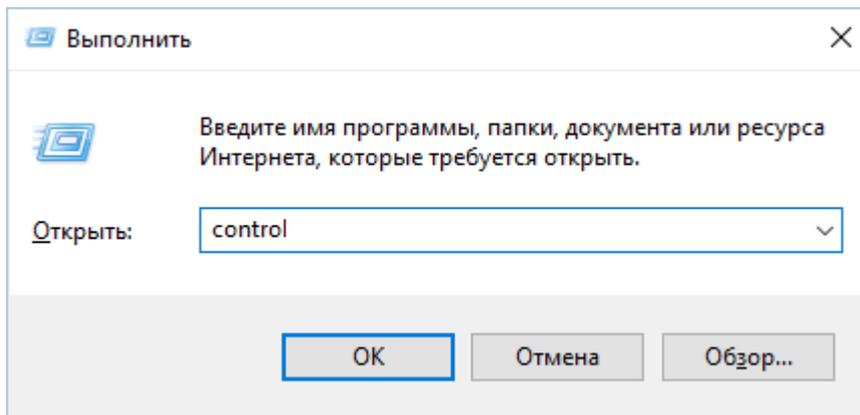


ОБРАТИТЕ ВНИМАНИЕ

Настройку правил встроенного брандмауэра Windows следует выполнять только если данный брандмауэр включен и используется в системе. Если в системе используется сторонний брандмауэр, то настройку правил следует выполнять в нём.

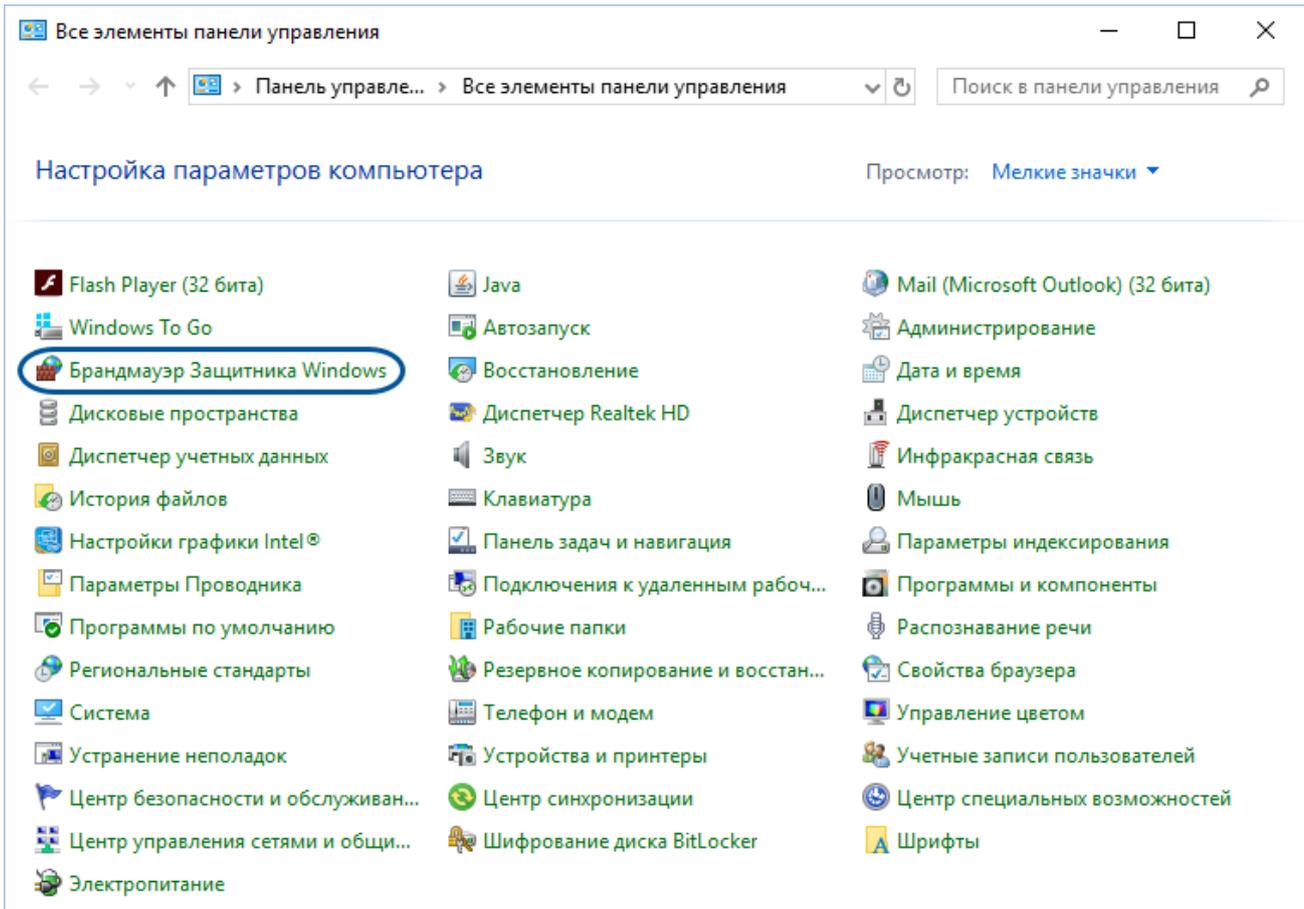
Чтобы настроить правила встроенного брандмауэра Windows:

1. Вызовите меню **Выполнить** комбинацией клавиш «Windows»+«R», введите команду control и нажмите кнопку **OK**.

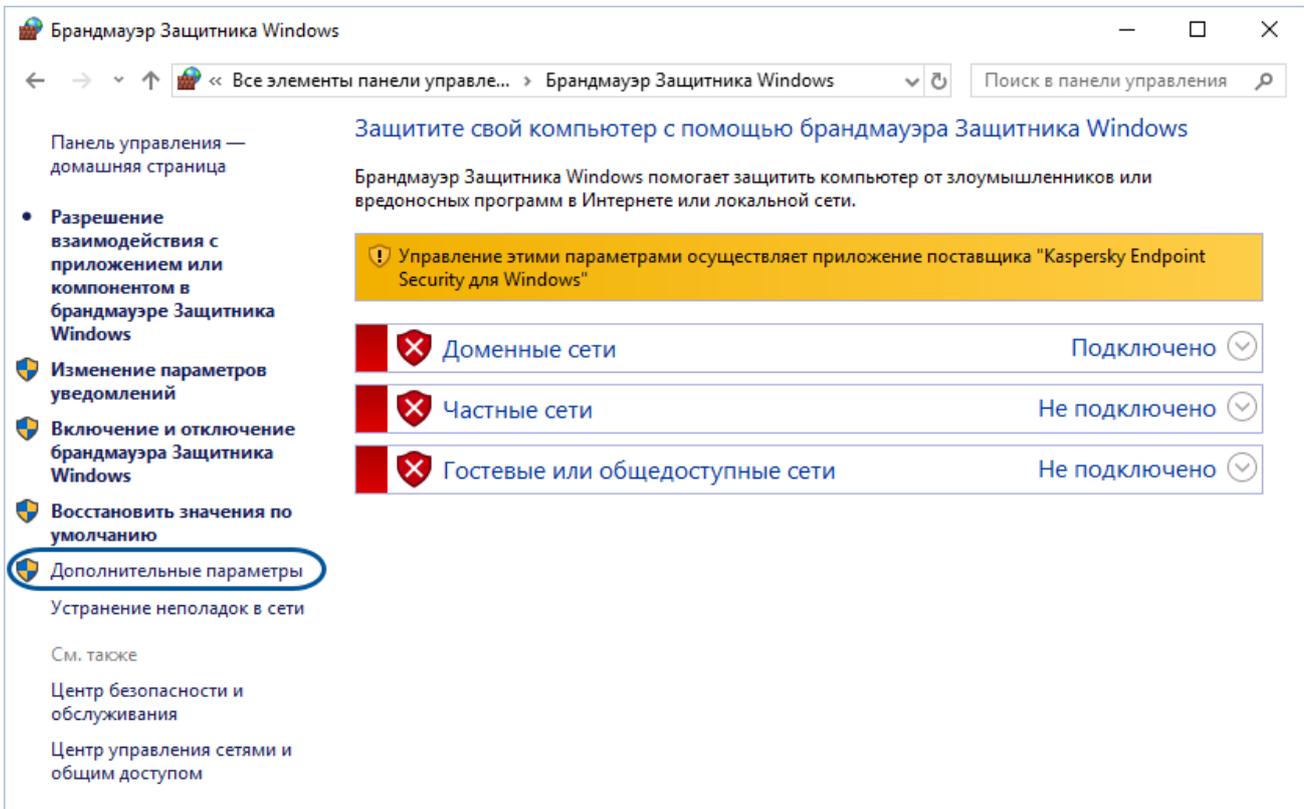


Либо пройдите по пути Пуск → Службные → Панель управления → Брандмауэр Защитника Windows.

2. В открывшемся окне элементов панели управления выберите элемент **Брандмауэр Защитника Windows**.



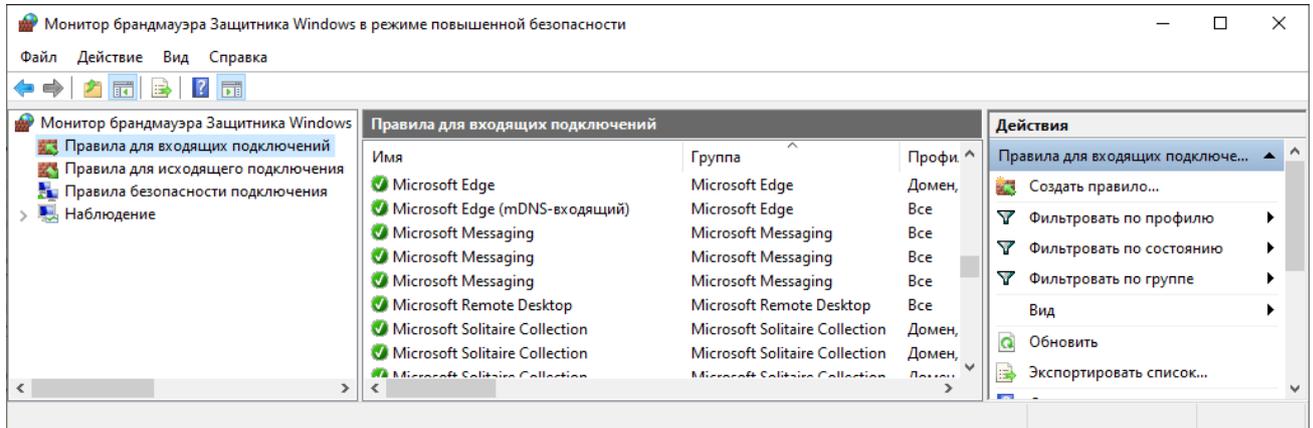
3. В окне **Брандмауэр Защитника Windows** выберите пункт **Дополнительные параметры**.



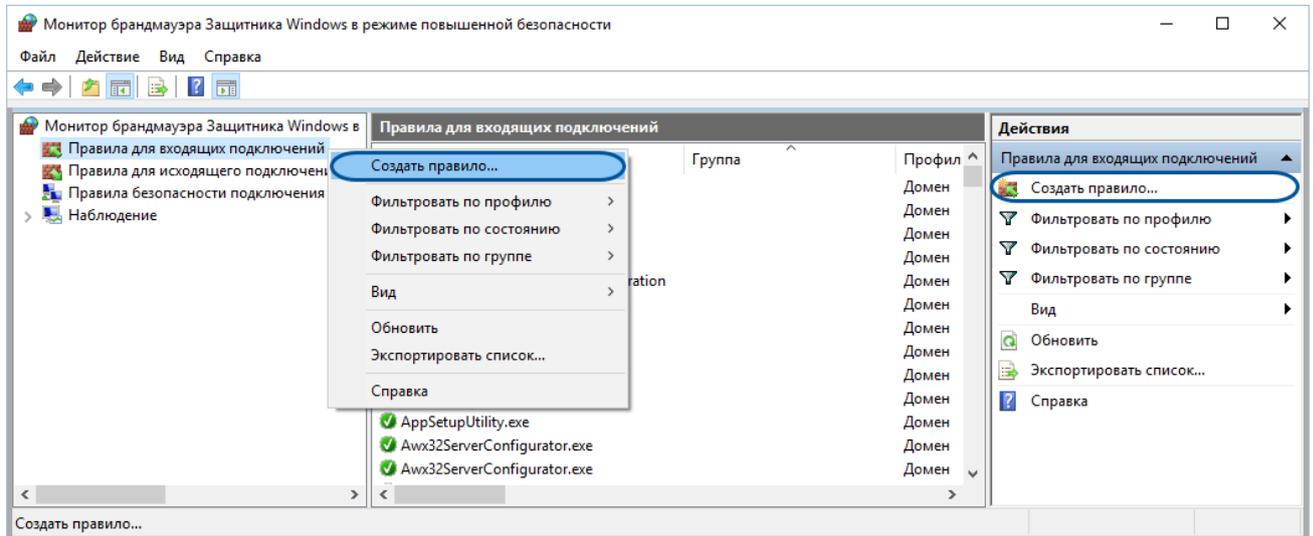
18.1.1. Правила для входящих подключений

Чтобы настроить правила для входящих подключений:

1. В окне **Монитор брандмауэра Защитника Windows** в режиме повышенной безопасности выберите пункт **Правила для входящих подключений**.



2. В контекстном меню или в области **Действия** выберите пункт **Создать правило...**



3. В окне **Мастер создания правила для нового входящего подключения** выберите тип подключения «**Для порта**» и нажмите кнопку **Далее**.

Мастер создания правила для нового входящего подключения

Тип правила

Выберите тип правила брандмауэра, которое требуется создать.

Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

Правило какого типа вы хотите создать?

- Для программы**
Правило, управляющее подключениями для программы.
- Для порта**
Правило, управляющее подключениями для порта TCP или UDP.
- Предопределенные**
BranchCache - обнаружение кэширующих узлов (использует WSD)
Правило, управляющее подключениями для операций Windows.
- Настраиваемые**
Настраиваемое правило.

< Назад **Далее >** Отмена

4. Выберите протокол, укажите порты, для которых требуется разрешить подключение и нажмите кнопку **Далее**.



ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для входящих подключений, приведены в разделе **Порты для входящих подключений** ([см. стр. 119](#)).

Мастер создания правила для нового входящего подключения

Протокол и порты

Укажите протоколы и порты, к которым применяется данное правило.

Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя

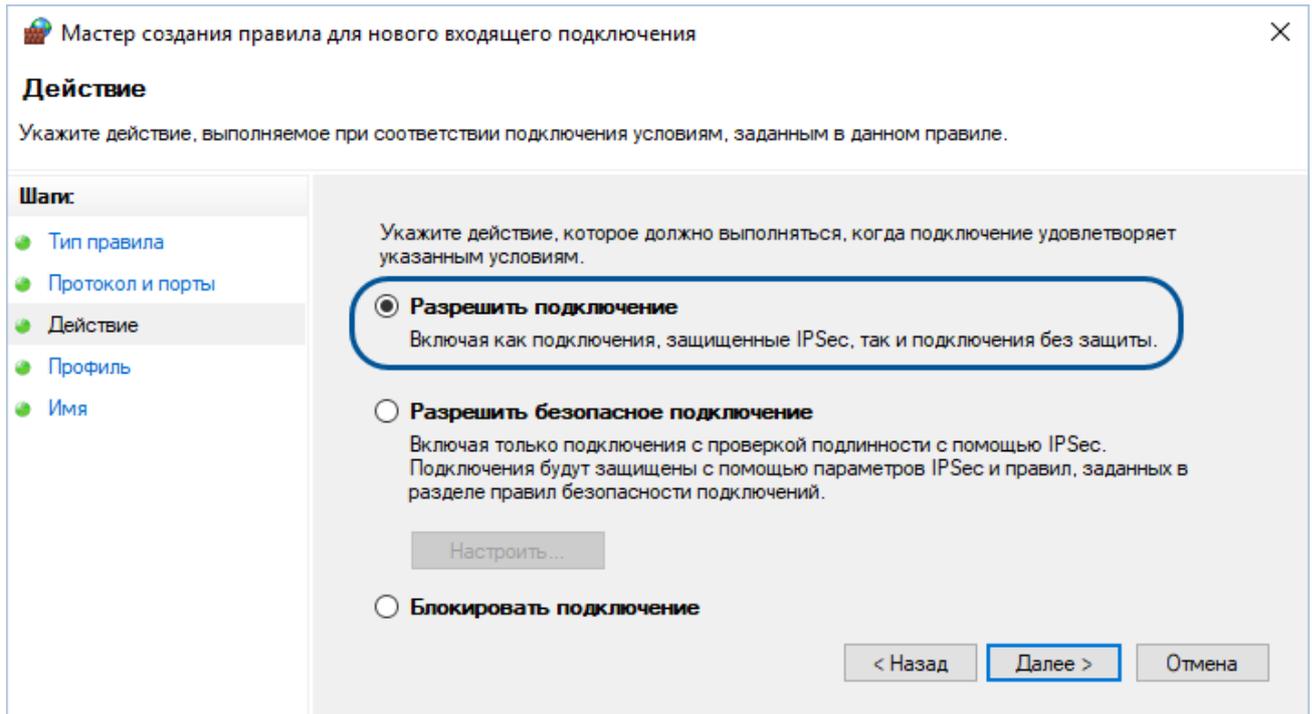
Укажите протокол, к которому будет применяться это правило.

- Протокол TCP**
- Протокол UDP**

Укажите порты, к которым будет применяться это правило.

- Все локальные порты**
- Определенные локальные порты:**
Пример: 80, 443, 5000-5010

< Назад **Далее >** Отмена

5. Выберите действие **Разрешить подключение** и нажмите кнопку **Далее**.

Мастер создания правила для нового входящего подключения

Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.

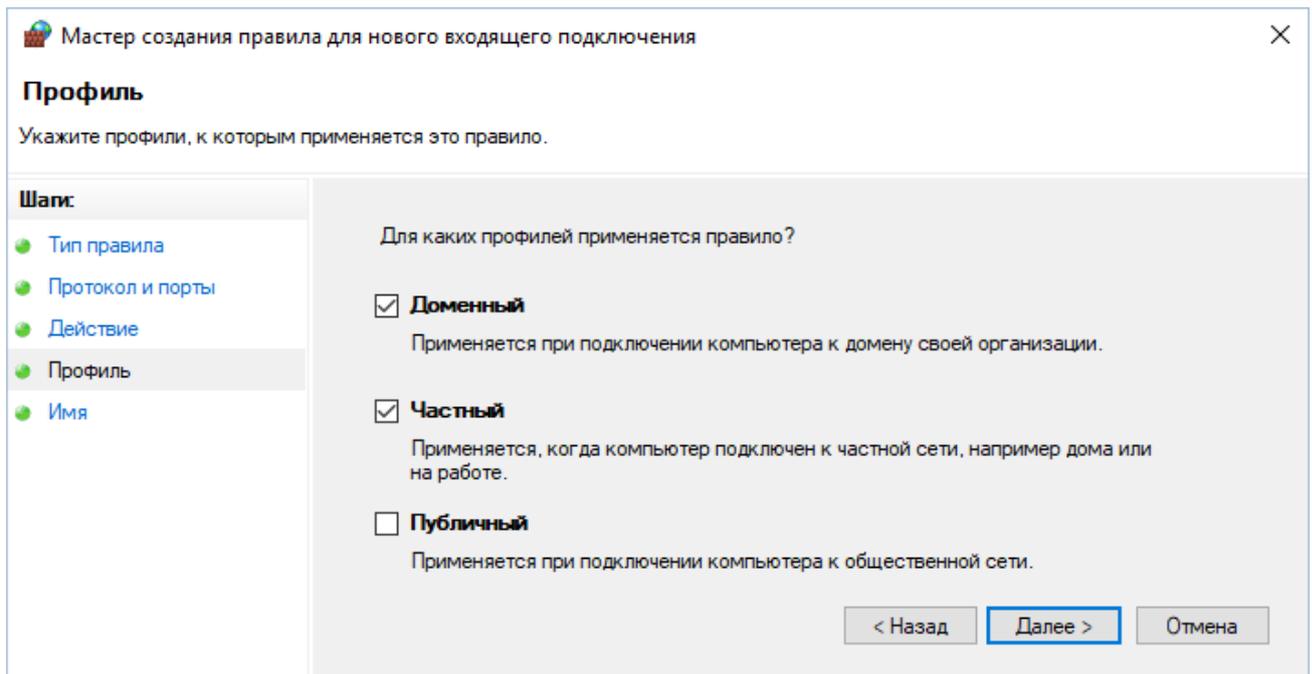
Шаги:

- Тип правила
- Протокол и порты
- Действие**
- Профиль
- Имя

Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

- Разрешить подключение**
Включая как подключения, защищенные IPSec, так и подключения без защиты.
- Разрешить безопасное подключение**
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.
[Настроить...](#)
- Блокировать подключение**

< Назад **Далее >** Отмена

6. Укажите профили, к которым будет применяться правило, установив соответствующие флаги, и нажмите кнопку **Далее**.

Мастер создания правила для нового входящего подключения

Профиль

Укажите профили, к которым применяется это правило.

Шаги:

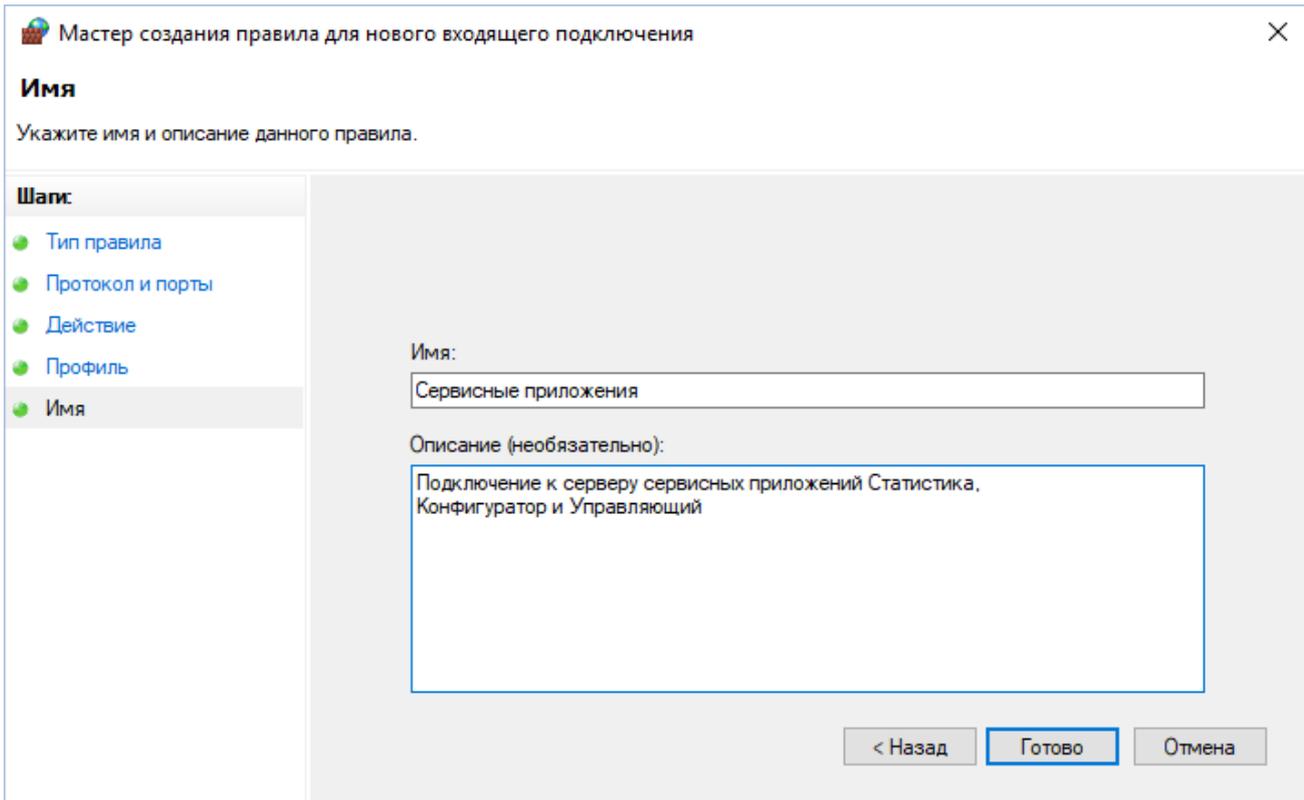
- Тип правила
- Протокол и порты
- Действие
- Профиль**
- Имя

Для каких профилей применяется правило?

- Доменный**
Применяется при подключении компьютера к домену своей организации.
- Частный**
Применяется, когда компьютер подключен к частной сети, например дома или на работе.
- Публичный**
Применяется при подключении компьютера к общественной сети.

< Назад **Далее >** Отмена

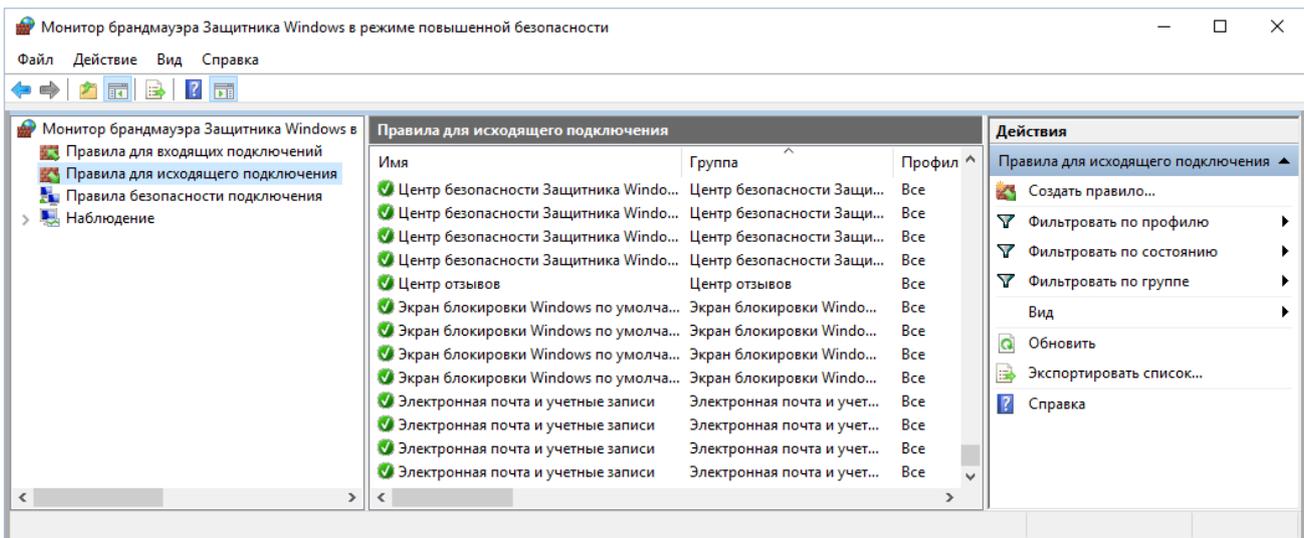
7. Укажите для создаваемого правила имя, описание и нажмите кнопку **Готово**.



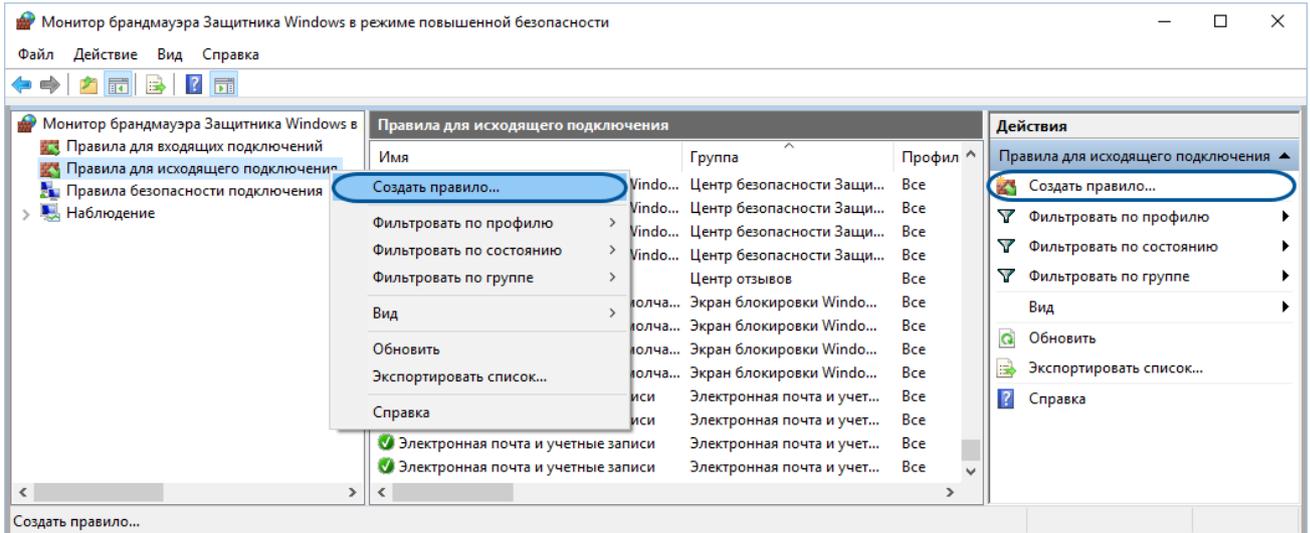
18.1.2. Правила для исходящих подключений

Чтобы настроить правила для исходящих подключений:

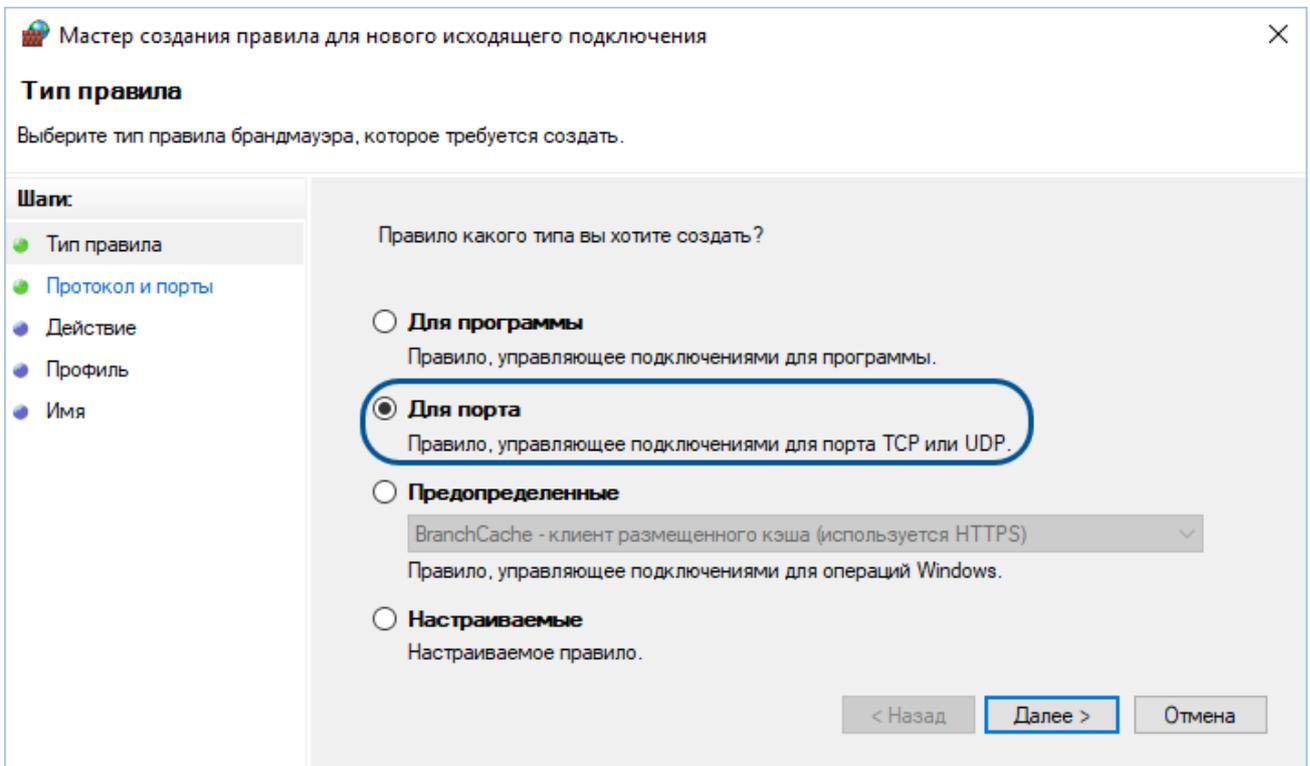
1. В окне **Монитор брандмауэра Защитника Windows** в режиме повышенной безопасности выберите пункт **Правила для исходящего подключения**.



2. В контекстном меню или в области Действия выберите пункт **Создать правило...**



3. В окне Мастер создания правила для нового исходящего подключения выберите тип подключения «Для порта» и нажмите кнопку **Далее**.



4. Выберите протокол, укажите порты, для которых требуется разрешить подключение и нажмите кнопку **Далее**.



ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для исходящих подключений, приведены в разделе **Порты для исходящих подключений** ([см. стр. 120](#)).

Мастер создания правила для нового исходящего подключения

Протокол и порты

Укажите протоколы и порты, к которым применяется данное правило.

Шаги:

- Тип правила
- Протокол и порты**
- Действие
- Профиль
- Имя

Укажите протокол, к которому будет применяться это правило.

Протокол TCP
 Протокол UDP

Применять это правило ко всем удаленным портам или только к определенным удаленным портам?

Все удаленные порты
 Определенные удаленные порты:

Пример: 80, 443, 5000-5010

5. Выберите действие **Разрешить подключение** и нажмите кнопку **Далее**.

Мастер создания правила для нового исходящего подключения

Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.

Шаги:

- Тип правила
- Протокол и порты
- Действие**
- Профиль
- Имя

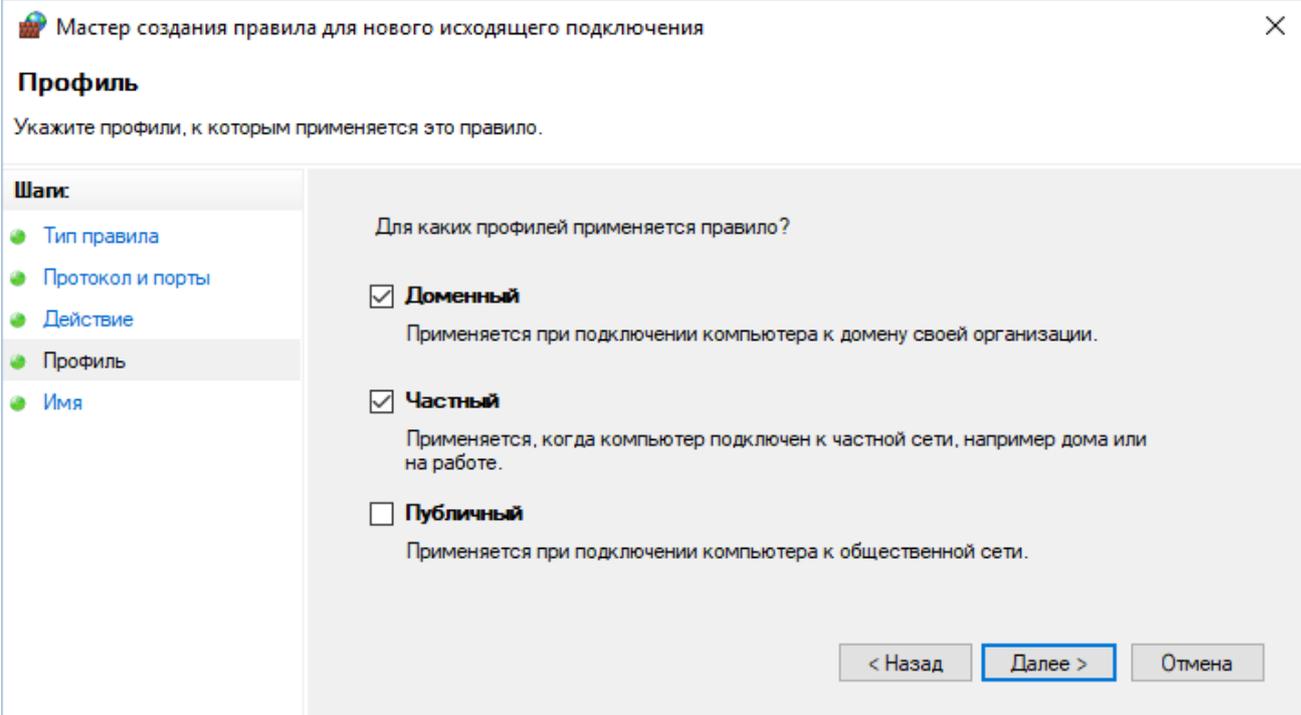
Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

Разрешить подключение
 Включая как подключения, защищенные IPSec, так и подключения без защиты.

Разрешить безопасное подключение
 Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

Блокировать подключение

6. Укажите профили, к которым будет применяться правило, установив соответствующие флаги, и нажмите кнопку **Далее**.



Мастер создания правила для нового исходящего подключения

Профиль

Укажите профили, к которым применяется это правило.

Шаги:

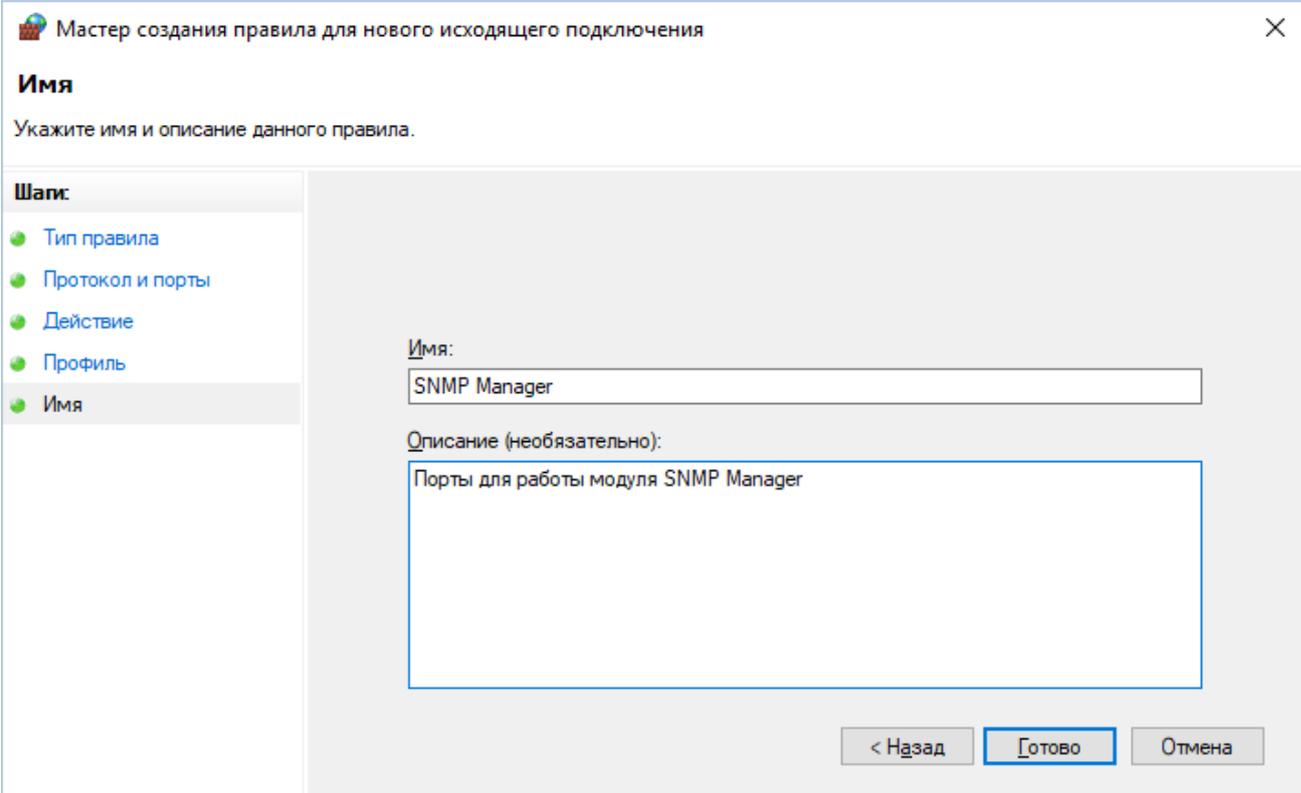
- Тип правила
- Протокол и порты
- Действие
- Профиль**
- Имя

Для каких профилей применяется правило?

- Доменный**
Применяется при подключении компьютера к домену своей организации.
- Частный**
Применяется, когда компьютер подключен к частной сети, например дома или на работе.
- Публичный**
Применяется при подключении компьютера к общественной сети.

< Назад **Далее >** Отмена

7. Укажите для создаваемого правила имя, описание и нажмите кнопку **Готово**.



Мастер создания правила для нового исходящего подключения

Имя

Укажите имя и описание данного правила.

Шаги:

- Тип правила
- Протокол и порты
- Действие
- Профиль
- Имя**

Имя:
SNMP Manager

Описание (необязательно):
Порты для работы модуля SNMP Manager

< Назад **Готово** Отмена

18.2. ОС Linux



ОБРАТИТЕ ВНИМАНИЕ

Настройку правил брандмауэра UFW следует выполнять только если данный брандмауэр установлен и используется в системе. Если в системе используется другой брандмауэр, то настройку правил следует выполнять в нём.



ПРИМЕЧАНИЕ

Чтобы установить брандмауэр UFW, выполните команду установки с помощью пакетного менеджера apt:

```
sudo apt install ufw
```

Чтобы настроить правила брандмауэра UFW:

1. Проверьте статус UFW командой:

```
sudo ufw status verbose
```

2. Если UFW отключен, то его необходимо включить. Для этого выполните команду:

```
sudo ufw enable
```

3. Запретите все входящие и исходящие подключения, если они не соответствуют правилам UFW, выполнив команды:

```
sudo ufw default deny incoming
```

```
sudo ufw default deny outgoing
```

4. Для настройки правил для входящих подключений выполните команду, с указанием порта и протокола, для которых требуется разрешить подключение:

```
sudo ufw allow in 4572/tcp
```



ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для входящих подключений, приведены в разделе Порты для входящих подключений ([см. стр. 119](#)).

5. Для настройки правил для исходящих подключений выполните команду, с указанием порта и протокола, для которых требуется разрешить подключение:

```
sudo ufw allow out 161/udp
```



ОБРАТИТЕ ВНИМАНИЕ

Протоколы и порты, используемые компонентами Систэм Платформ для исходящих подключений, приведены в разделе Порты для исходящих подключений ([см. стр. 120](#)).

18.3. Порты для входящих подключений

Порты, через которые компоненты Систэм Платформ получают данные, приведены в таблице.

Компонент	Порт	Примечание
SePlatform.Data collection Server	TCP:4572	Подключение к SePlatform.Data collection Server приложений Статистика, Конфигуратор, Управляющий
	TCP:4388	Модуль TCP Server - подключение клиентов
	TCP:6551	Модуль резервирования - порт основного канала для подключения резервной пары
	TCP:6552	Модуль резервирования - порт резервного канала для подключения резервной пары
	TCP:6514	Модуль Syslog Server - получение данных по TLS
	UDP:514	Модуль Syslog Server - получение данных по UDP
	TCP:8080	Модуль OPC UA - получение данных по протоколу HTTP/HTTPS
	TCP:62544	Модуль OPC UA - получение данных по протоколу OPC.TCP
	TCP:2404	Модуль IEC Slave - подключение опросчика
	TCP:502	Модуль Modbus TCP Slave - подключение опросчика
SePlatform.AccessPoint	TCP:4976	Подключение к SePlatform.AccessPoint приложений Статистика, Конфигуратор
	TCP:4949	Получение исторических данных от SePlatform.Historian
SePlatform.Imitator	TCP:4983	Подключение к SePlatform.Imitator приложений Статистика, Конфигуратор
SePlatform.Historian	TCP:3388	Подключение приложения Статистика
	TCP:4949	Сохранение данных
SePlatform.Domain	TCP:1000	SePlatform.Net.Agent
	TCP:1010	SePlatform.Domain.Agent
SePlatform.Security	TCP:389	LDAP-сервер - запросы данных пользователей, их прав, конфигурирование
SePlatform.License Server	TCP:15150	Подключение для запроса лицензий
	TCP:15151	Подключение приложения Статистика

Компонент	Порт	Примечание
SePlatform.HMI.WebViewer	TCP:8080	Незащищенные соединения по веб-сокету
	TCP:4430	Безопасные соединения по веб-сокету
SePlatform.Mapping Server	TCP:5432	Доступ к данным через PostgreSQL
SePlatform.Diagnostics	UDP:123	Служба NTPServer - настройка службы сервера времени SePlatform.Diagnostics
	UDP:161	Служба SNMP - настройка агента SNMP
	TCP:12550	Служба SNMP - режим ReadOnly
	TCP:12551	Служба SNMP - режим ReadOnly
	UDP:514	Служба Syslog - настройка сервера Syslog
	TCP:8001	Служба VoiceServer - настройка службы голосового сервера

18.4. Порты для исходящих подключений

Порты, через которые компоненты Систэм Платформ отправляют данные, приведены в таблице.

Компонент	Порт	Примечание
SePlatform.Data collection Server	TCP:4572	Для приложений Статистика, Конфигуратор, Управляющий
	TCP:3388	Предоставление статистики в SePlatform.Historian
	TCP:4949	Сохранение данных в SePlatform.Historian
	TCP:4388	Модуль TCP Server - предоставление данных клиентам
	UDP:161	Модуль SNMP Manager - опрос агента
	UDP:162	Модуль SNMP Manager - trap-уведомления
	TCP:6551	Модуль резервирования - порт основного канала для подключения к резервной паре
	TCP:6552	Модуль резервирования - порт резервного канала для подключения к резервной паре
	TCP:102	Модуль IEC-61850 Client - опрос устройств
	UDP:9600	Модуль FINS Client - опрос устройств
	TCP:8080	Модуль OPC UA Client - порт HTTP/HTTPS протокола
	TCP:62544	Модуль OPC UA Client - порт OPC.TCP протокола
	TCP:2404	Модуль IEC-104 Master - опрос подчиненной станцией
TCP:502	Модуль Modbus TCP Master -опрос подчиненной станцией	
SePlatform.AccessPoint	TCP:4388	Подключение к SePlatform.Data collection Server
SePlatform.Imitator	TCP:4949	Подключение к SePlatform.Historian для чтения истории, записи имитационных данных
SePlatform.Domain	TCP:1000	SePlatform.Net.Agent
	TCP:1010	SePlatform.Domain.Agent
SePlatform.Security	TCP:389	Конфигуратор, Агент
SePlatform.Development Studio	TCP:1000	SePlatform.Net.Agent
	TCP:1010	SePlatform.Domain.Agent
SePlatform.HMI.Designer	TCP:4388	Оперативные данные SePlatform.Data collection Server
	TCP:4949	Исторические данные SePlatform.Historian
SePlatform.HMI.Viewer	TCP:4388	Оперативные данные SePlatform.Data collection Server
	TCP:4949	Исторические данные SePlatform.Historian

Компонент	Порт	Примечание
SePlatform.Diagnostics	UDP:161	Контроль целостности, Монитор ресурсов
	TCP:12550	Контроль целостности, Монитор ресурсов
	TCP:12551	Контроль целостности, Монитор ресурсов
	TCP:11001	Контроль целостности
	UDP:123	Синхронизация времени
	TCP:12500	Удаленная конфигурация

19. Работа в ОС Linux

Некоторые продукты Систэм Платформ могут работать на компьютерах под управлением ОС семейства Linux (в документации на продукты - ОС Linux). Такие продукты поставляются в виде *.deb и *.rpm пакетов и после установки функционируют в виде сервисов.

Ниже приведена общая информация для всех компонентов, работающих в ОС семейства Linux.



ПРИМЕЧАНИЕ

Подробности о том, работает ли компонент в ОС семейства Linux и название его пакета/сервиса смотрите в документации на конкретный компонент.

Поддерживаемые ОС семейства Linux

- Centos
- Ubuntu
- Debian
- Astra Linux

Установка/удаление

В Centos (rpm-пакеты):

- Установить пакет:

```
sudo rpm -i <имя пакета>
```

- Удалить пакет:

```
sudo rpm -e <имя пакета>
```

В Ubuntu, Debian, Astra Linux (deb-пакеты):

- Установить пакет:

```
sudo dpkg -i <имя пакета>
```

- Удалить пакет:

```
sudo dpkg -r <имя пакета>
```

Пути

Директория расположения сервисов:

- Centos:

```
/usr/lib/systemd/system
```

- Ubuntu, Debian, Astra Linux:

```
/lib/systemd/system
```

Директория установки:

- Для всех ОС семейства Linux:
/opt/SePlatform/<имя продукта>

(Astra Linux) Список сервисов

1. Откройте **Панель управления**.
2. Выберите группу **Система**.
3. Перейдите в раздел **Инициализация системы**.

Команды работы с сервисами

- Запустить сервис:

```
sudo systemctl start <имя сервиса>
```

- Остановить сервис:

```
sudo systemctl stop <имя сервиса>
```

- Перезапустить сервис:

```
sudo systemctl restart <имя сервиса>
```

- Текущее состояние сервиса:

```
sudo systemctl status <имя сервиса>
```

- Посмотреть журнал:

```
sudo journalctl -u <имя сервиса> -n <количество> -f
```

где:

- -n <количество> - вывести последние n строк строк журнала (опциональный атрибут).
- -f - выводить журнал в режиме реального времени (опциональный атрибут).

(Astra Linux) Подключение установочных репозиториев

Монтирование образа диска

Если диск с ОС смонтирован в CD-ROM, дополнительных действий не требуется.

Если ОС была установлена с помощью загрузочного Flash-носителя:

1. Скопируйте образ диска в виде .iso файла на жёсткий диск в отдельную директорию (директорию монтирования).
2. Подключите образ диска.

```
sudo mount -o loop <путь до образа>.iso /<директория монтирования>
```

Подключение внешних репозиториев

1. Перейдите в директорию `/etc/apt` и откройте файл `sources.list`
2. Добавьте строку

```
deb [trusted=true] file://<путь до директории монтирования> <директории с дистрибутивами>
```

, где <директории с дистрибутивами> - список директорий, перечисленных через пробел.

3. Обновите базу данных пакетов

```
sudo apt update
```



ПРИМЕЧАНИЕ

Подробнее о подключении репозиториев с пакетами в ОС Astra Linux:
<https://wiki.astralinux.ru/pages/viewpage.action?pageId=3276859>

19.1. (Astra Linux) Создание пользователя Operator с ограниченными правами

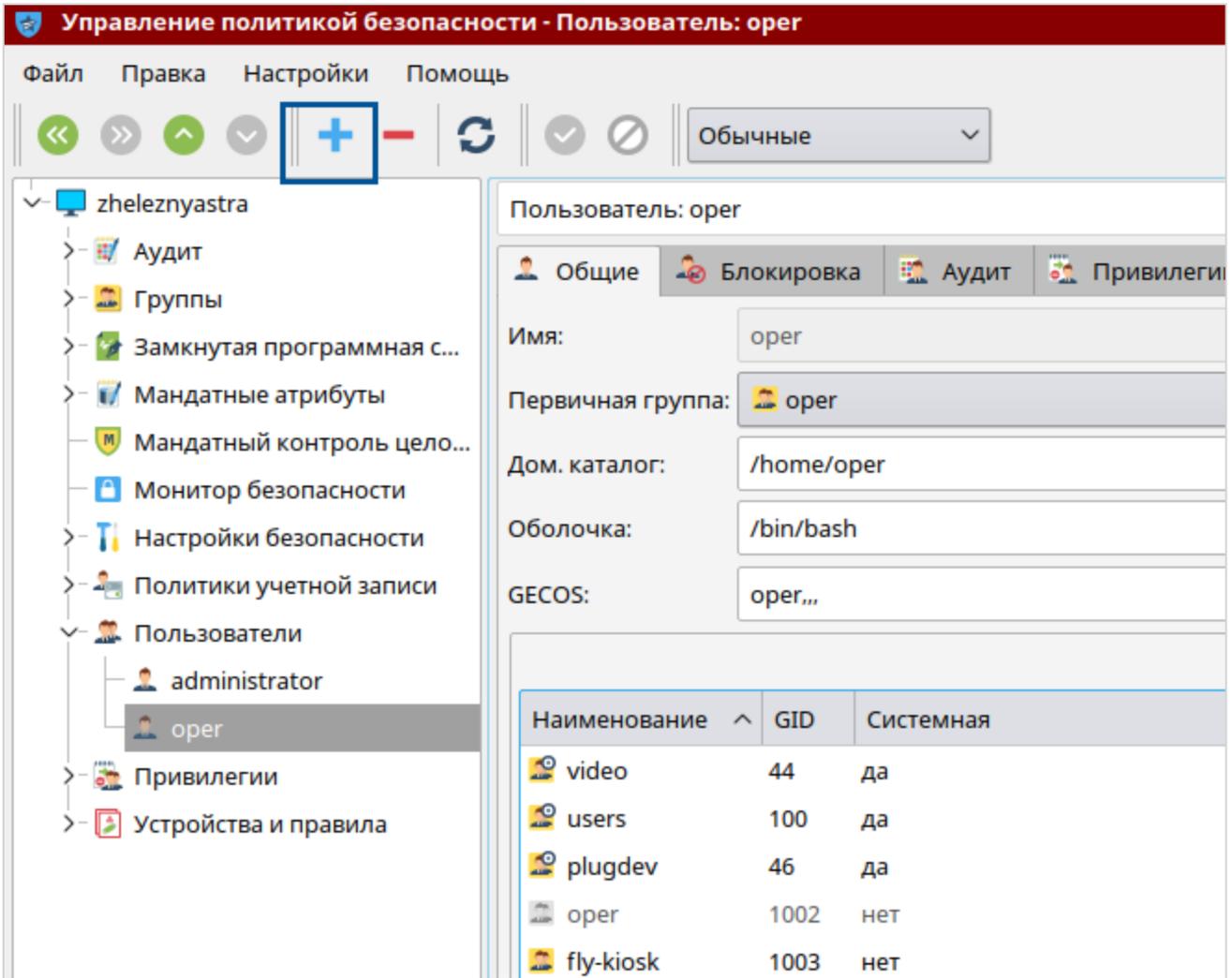
Откройте панель управления (меню Пуск).

Создание пользователя

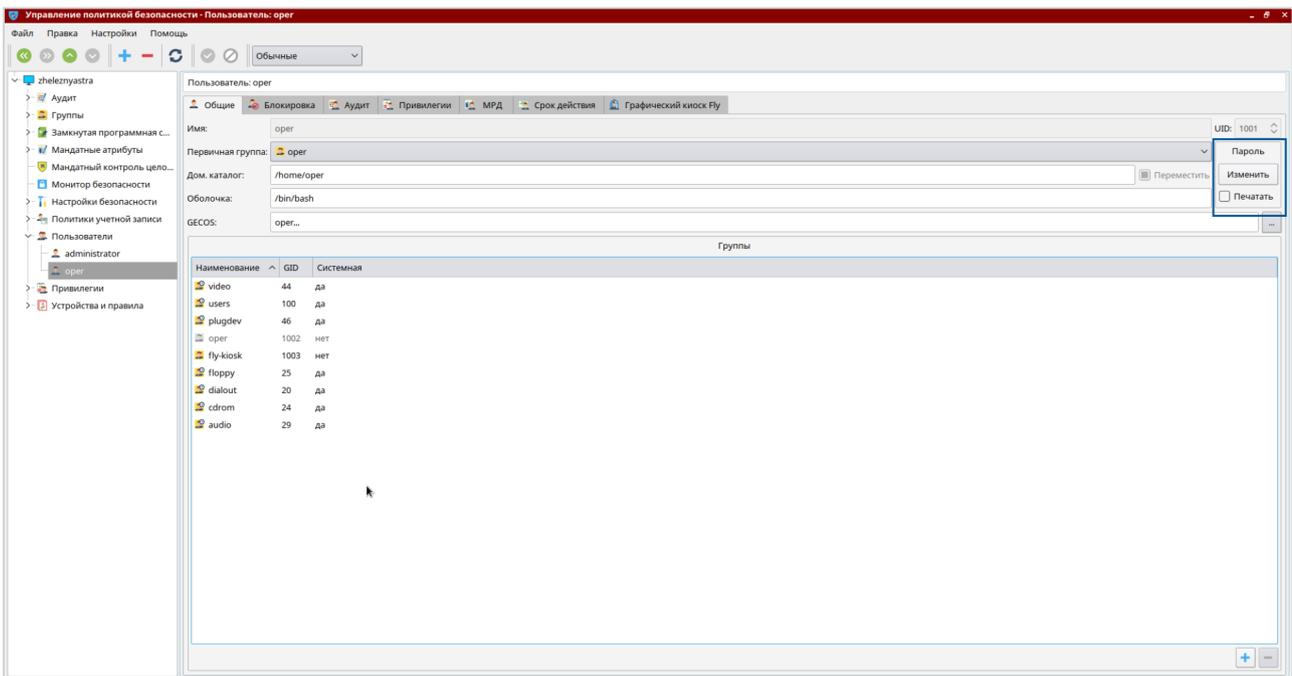
1. Перейдите в группу **Безопасность**.
2. Откройте раздел **Политика безопасности**.
3. Перейдите на узел **Пользователи**.

4. Добавьте нового пользователя кнопкой .

Укажите имя пользователя и подтвердите добавление.



5. Задайте первоначальный пароль пользователя, нажав кнопку Изменить.



6. Установите права пользователя (подробнее «F1»).

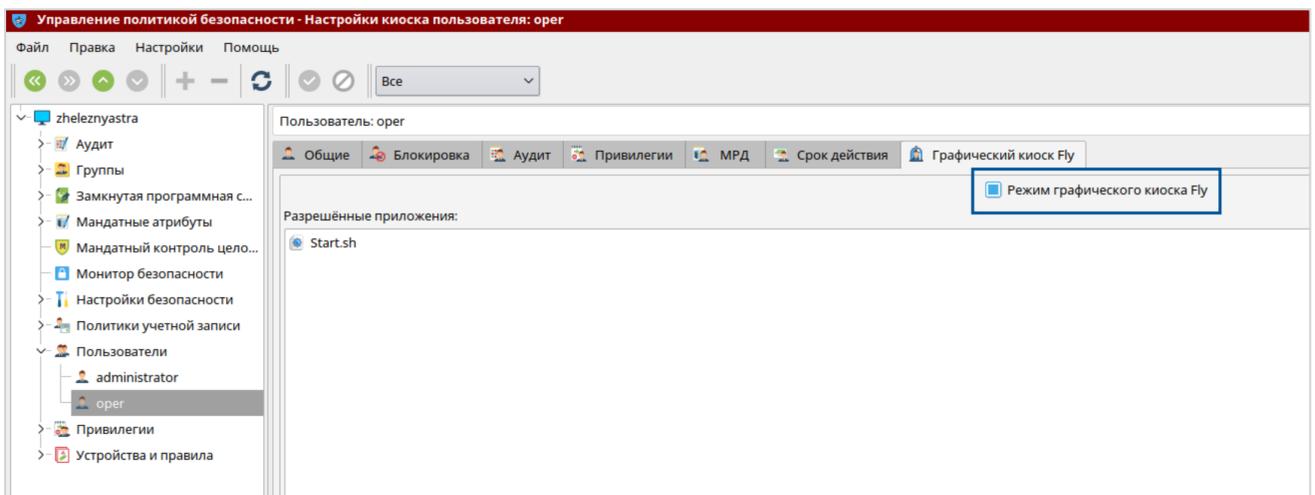


ОБРАТИТЕ ВНИМАНИЕ

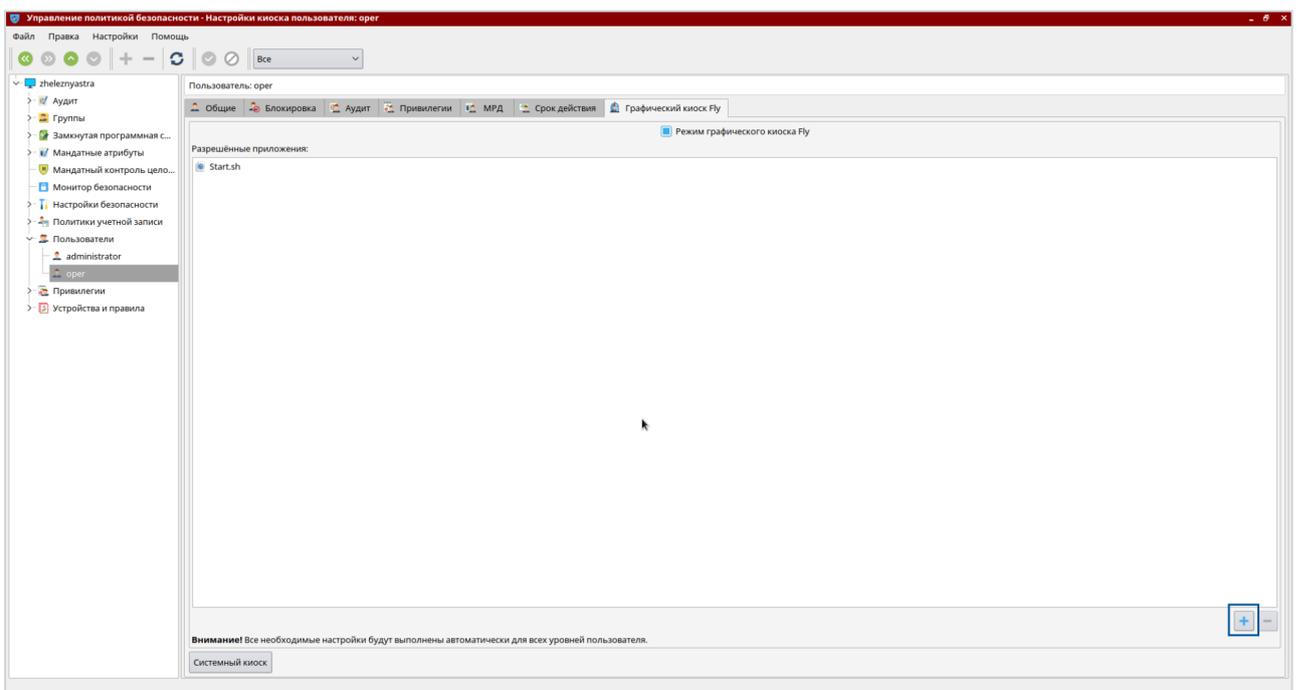
Для создания домашнего каталога нового пользователя необходимо хотя бы один раз войти в систему под этим пользователем.

Настройка режима графического киоска

1. Создайте скрипт для запуска приложения (например, проекта SePlatform.HMI).
2. Перейдите в группу **Безопасность**.
3. Откройте раздел **Политика безопасности**.
4. Перейдите на узел **Пользователи**.
5. Перейдите на вкладку **Графический киоск**.
6. Включите режим графического киоска.



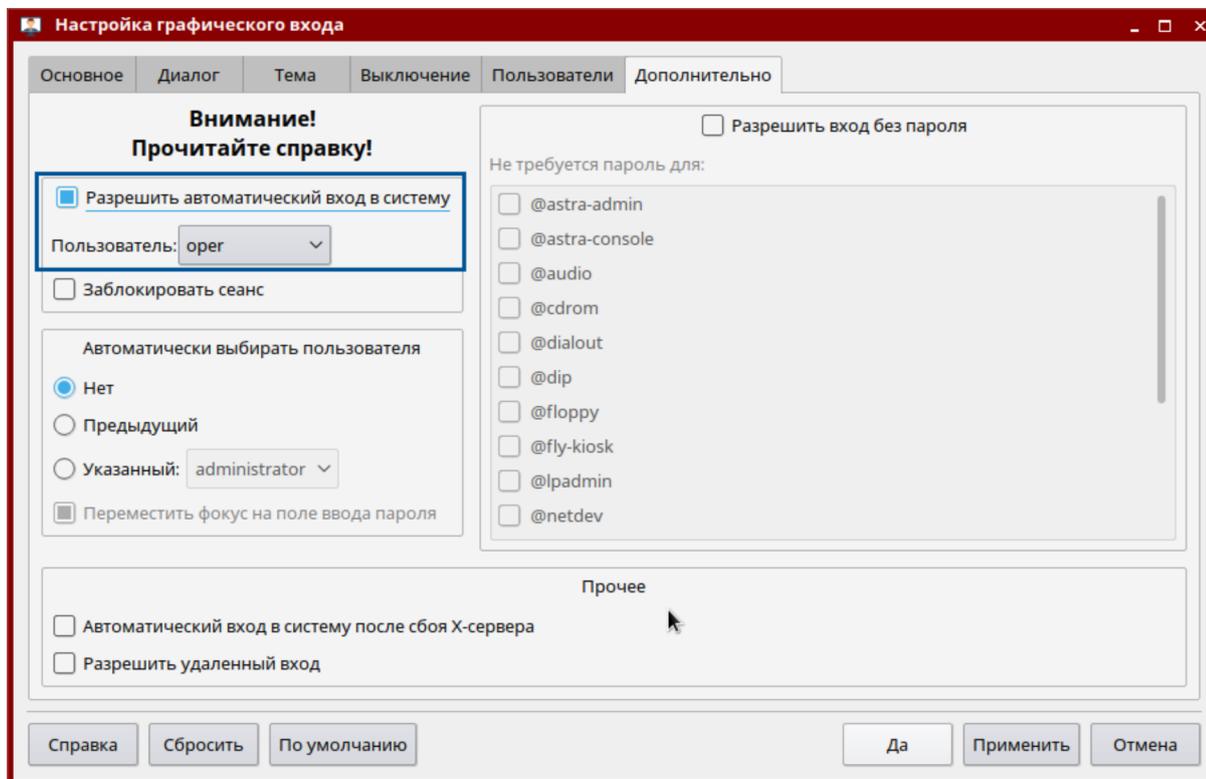
7. Добавьте разрешённое для выполнения приложение, нажав **+** и выбрав созданный скрипт.



8. Нажмите **Применить** изменения на панели инструментов.

Настройка автоматического входа пользователя

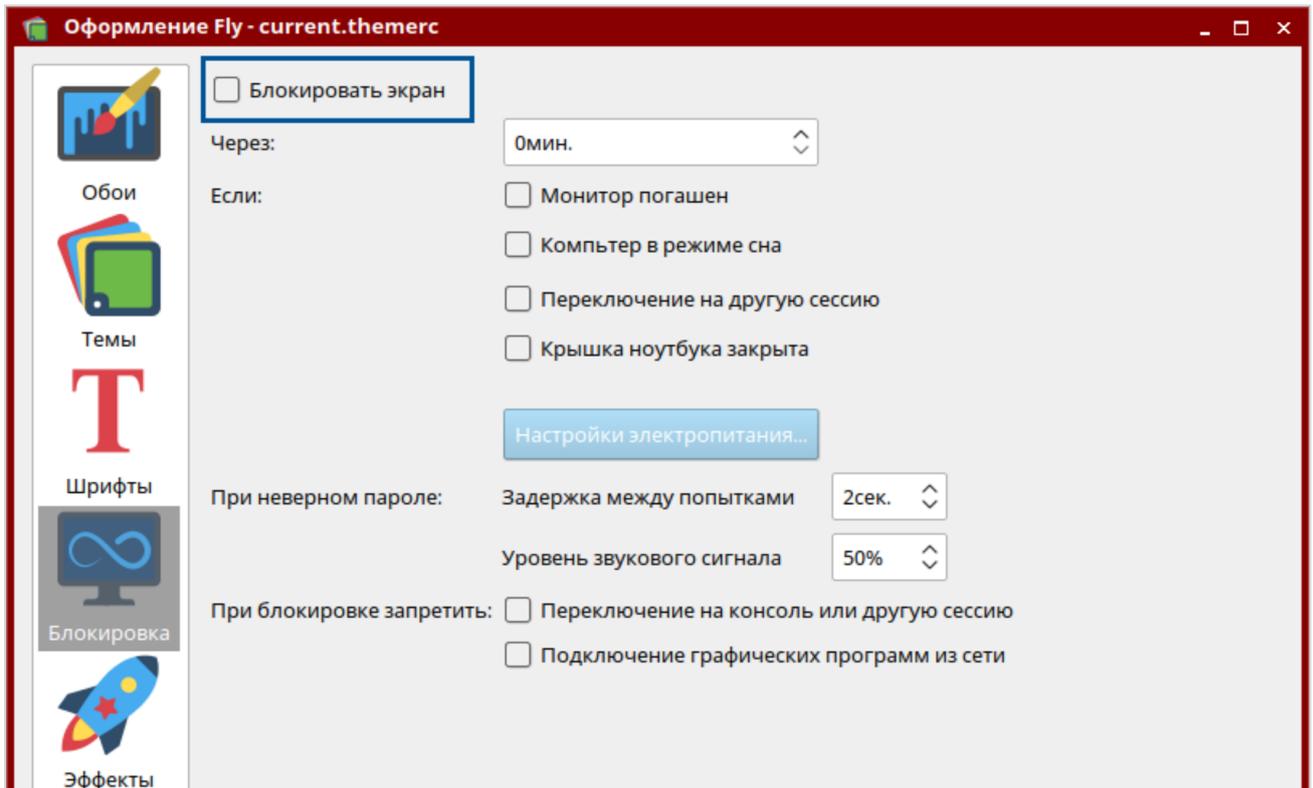
1. Перейдите в группу Система.
2. Откройте раздел **Вход в систему**.
3. Перейдите на вкладку **Дополнительно** и разрешите пользователю с ограниченным набором прав автоматический вход в систему.



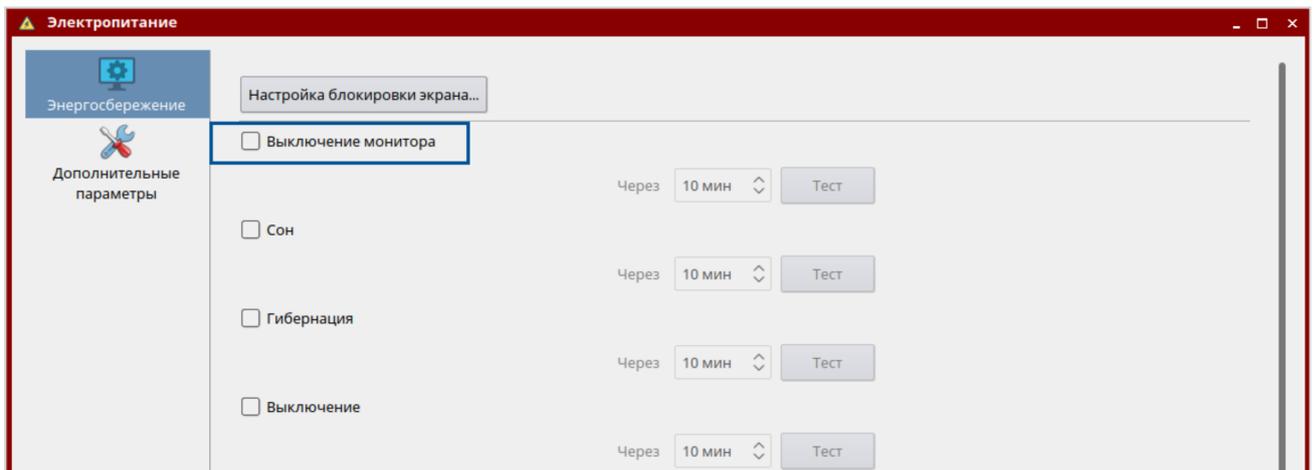
Настройка электропитания для выключения перехода в спящий режим при бездействии

1. Перейдите в группу Система.
2. Откройте раздел **Оформление Fly**.

3. Перейдите в группу **Блокировка** и снимите флаг **Блокировать экран**.



4. Нажмите кнопку **Настройка электропитания**.
5. В открывшемся окне снимите флаг **Выключение монитора**.



Запрет переключения между виртуальными терминалами

1. Перейдите в директорию настроек графической среды `/usr/share/X11/xorg.conf.d/`.
2. Создайте файл конфигурации.

```
sudo touch 50-novtswitch.conf
```

3. Запишите в файл флаг на запрет переключения между виртуальными терминалами из текущей графической среды:

```
sudo sh -c 'cat << EOF >> 50-novtswitch.conf
Section "ServerFlags"
Option "DontVTSwitch" "true"
EndSection
EOF'
```

4. Перезагрузите операционную систему.

Разрешение переключения между виртуальными терминалами

1. Перейдите в директорию настроек графической среды /usr/share/X11/xorg.conf.d/.
2. Удалите созданный файл ([стр. 129](#)) конфигурации с флагом запрета.

```
sudo rm 50-novtswitch.conf
```

3. Перезагрузите операционную систему.

```
sudo shutdown -r now
```