ООО "СВЕЙ"

Регистратор аварийных событий АУРА

Руководство по настройке АРМ для программного обеспечения AuraQt

Екатеринбург 29.01.2024

Содержание

Настоящий документ предназначен для настройки АРМ для доступа к веб-интерфейсу регистраторов АУРА, работающих под управлением программного обеспечения AuraQt.

Настоящий документ является выдержкой из полного руководства пользователя на ПО AuraQt, расширенной и дополненной в соответствии с типовыми вопросами и задачами, возникающими при первом подключении к регистратору после его получения от завода-изготовителя. Документ также содержит допущения, соответствующие заводским настройкам и заводскому комплекту поставки регистратора.

1. Общие сведения

Доступ к веб-интерфейсу регистраторов АУРА под управлением ПО AuraQt реализован с помощью аутентификации пользователя при помощи предъявления регистратору доверенного сертификата безопасности. Данная функция реализуется протоколом HTTPS и штатными средствами операционной системы и браузера.

Сертификат безопасности клиента должен быть доступен в операционной системе АРМ и быть прописан в списке доверенных сертификатов регистратора. Производитель предоставляет аппаратные токены со встроенными клиентскими сертификатами для доступа к регистратору.

В свою очередь, чтобы браузер АРМ доверял соединению с веб-интерфейсом регистратора по HTTPS, сертификат регистратора также требуется настроить в качестве доверенного в системе АРМ.

Кроме компьютера с браузером[1] для подключению к регистратору потребуются:

- Токен(ы)[2] для аутентификации пользователя (примерный внешний вид показан ниже)
- Флэш-накопитель с сертификатами, инструкциями и драйвером к токенам
- Сетевое подключение на уровне локальной сети

[1] Internet Explorer 11 (частичная поддержка), Edge, Chrome, Firefox или аналогичный под управлением операционной системы Windows (версии 7 или новее), Linux или аналогичной.

[2] Токены упаковываются с системным блоком и не выделяются отдельной позицией в накладной.

2. Настройка АРМ

2.1 Проверка связи по сетевому уровню

При первом подключении регистратора рекомендуется проверить его доступность на сетевом уровне. В простейшем случае регистратор и АРМ должны иметь адреса в одной подсети и быть соединены сетевыми портами, относящимися к этой подсети.

Узнать IP-адрес регистратора можно из следующих источников:

- Индикатор системного блока (не во всех исполнениях): клавиша F4 (Fn+F2)
- Паспорт регистратора
- Список стандартных заводских IP-адресов: 192.168.0.NN, 192.168.1.NN, ... 192.168.9.NN (по одному на каждый сетевой порт), где NN равно 99 или последним двум цифрам номера регистратора
- Веб-интерфейс (при настроенном доступе)

Например, регистратор подключается прямым сетевым кабелем к ноутбуку. Допустим, что со стороны регистратора используется сетевой порт LAN2, имеющий адрес 192.168.1.99 (маска 255.255.255.0 или /24). Тогда со стороны ноутбука на сетевом порту должен быть настроен другой адрес в той же подсети, например 192.168.1.100 (также с маской 255.255.255.0 или /24).

Проверить физическое подключение можно набрав команду “ping 192.168.1.99” в консоли АРМ (в команде ping прописать конкретный адрес вашего регистратора). При условии получения ответа от регистратора (как показано ниже) можно приступать к следующему разделу.

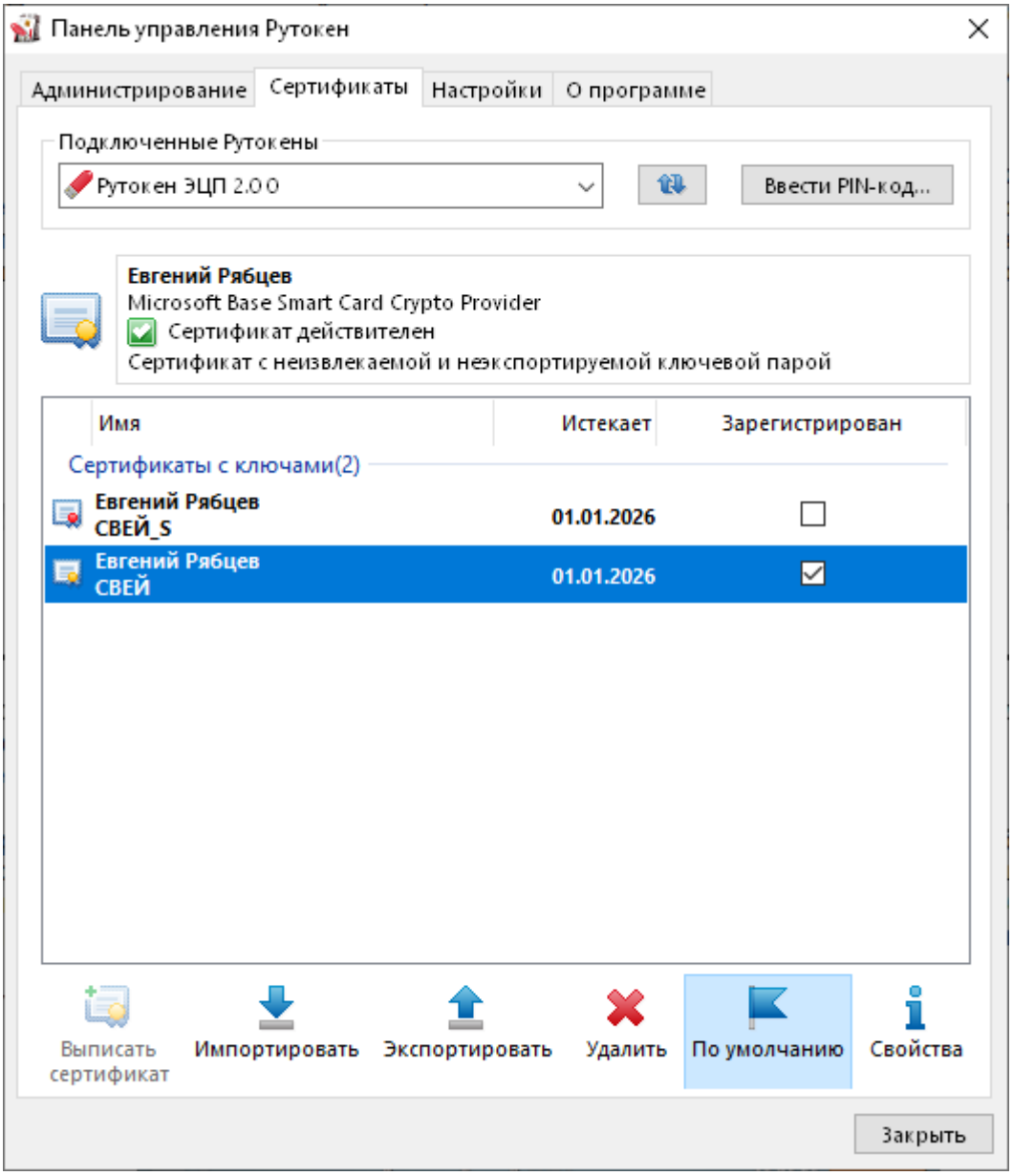
```
C:\Users\Sysadmin>ping 192.168.0.194

Обмен пакетами с 192.168.0.194 по с 32 байтами данных:
Ответ от 192.168.0.194: число байт=32 время=60мс TTL=64
Ответ от 192.168.0.194: число байт=32 время=28мс TTL=64
Ответ от 192.168.0.194: число байт=32 время=26мс TTL=64
Ответ от 192.168.0.194: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.0.194:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 60 мсек, Среднее = 28 мсек
```

2.2 Проверка работоспособности токена

На флэш-накопителе, поставляемом в комплекте с регистратором, имеется файл установки драйвера токена безопасности для операционных систем Windows: “rtDrivers.exe”. Этот драйвер следует установить до начала работы с токенами. При необходимости, новейшую версию драйвера, в том числе для других операционных систем, можно получить с сайта производителя токена.

Проверить работу токена можно в панели управления Рутокен, которая устанавливается вместе с драйвером (найти либо ярлык на рабочем столе, либо в панели "Пуск"). Если токен корректно определяется и на нём есть записанные сертификаты, их можно увидеть во вкладке "Сертификаты" как показано ниже.

В комплект поставки обычно входит по два токена на каждый системный блок - один без права изменения конфигурации и один с полными правами. Токены упаковываются с системным блоком и не выделяются отдельной позицией в накладной. При поставке партии регистраторов одному заказчику, все токены из одной партии могут подходить ко всем регистраторам этой партии.

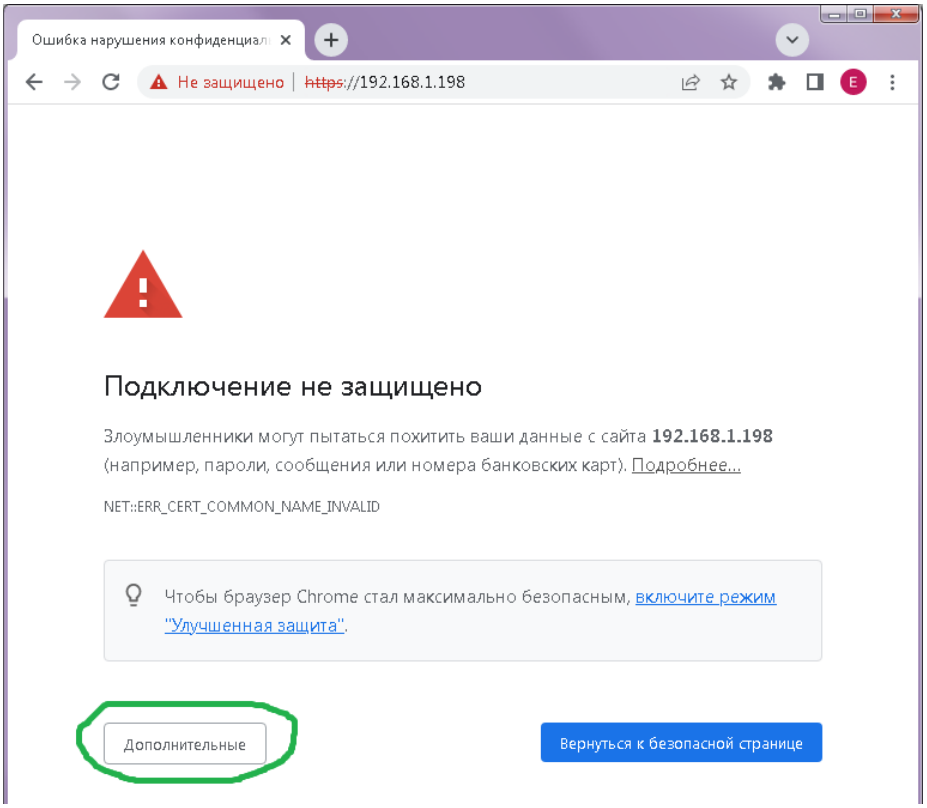


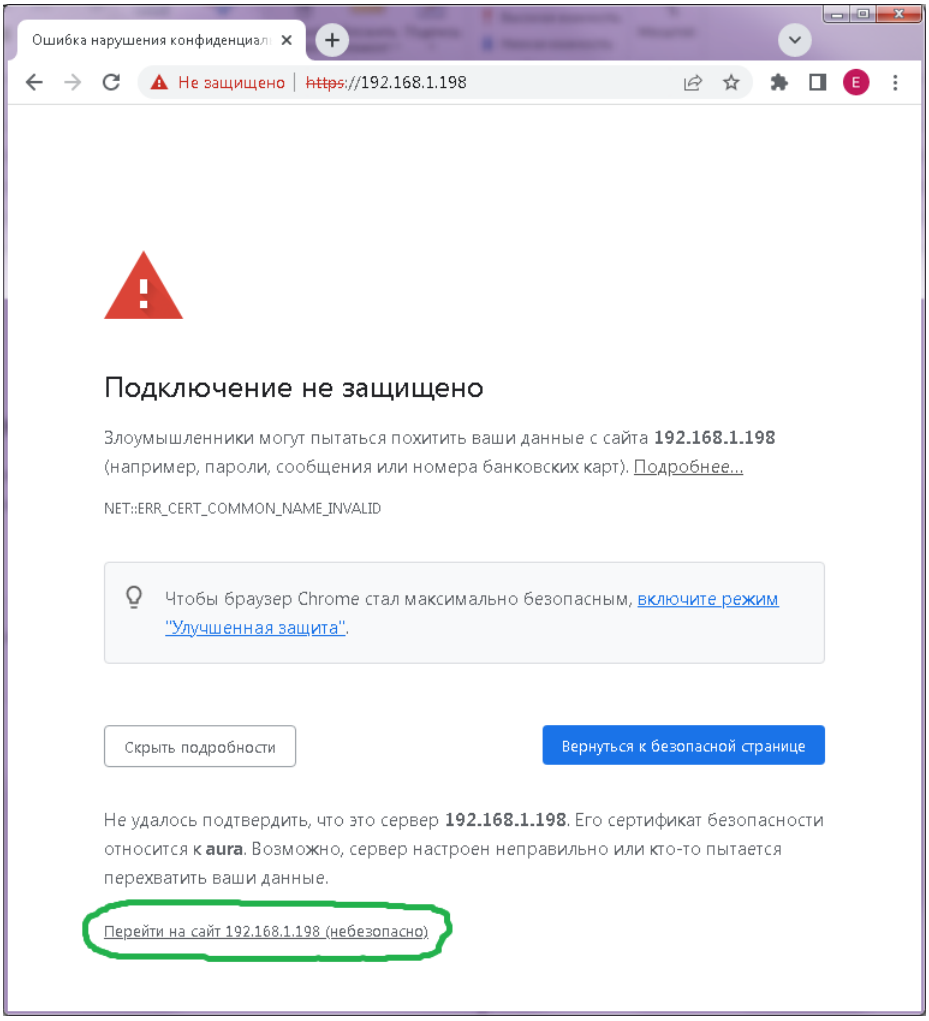
2.3 Первоначальное подключение к веб-интерфейсу регистратора

Взаимодействие с регистратором осуществляется через веб-интерфейс, открываемый в браузере следующим образом:

- К свободному USB-интерфейсу АРМ подключается токен.
- В адресной строке браузера набирается https://IP_адрес_или_имя_регистратора и, в ответ на приглашение, выбирается сертификат, который хранится в подключенном токене. Если вводить имя или адрес регистратора без указания "https://", доступ к веб-интерфейсу предоставлен не будет.
- В зависимости от того, настроены ли серверные сертификаты (см. следующий раздел), браузер может отобразить предупреждение безопасности, которое можно проигнорировать, нажав "Дополнительные" и "Перейти на сайт …" как показано ниже.
- Появится окно выбора клиентского сертификата, в котором следует выбрать сертификат, хранящийся на подключенном токене.
- После выбора сертификата из списка и нажатия кнопки "ОК", появится окно ввода PIN-кода от токена. По умолчанию вводится PIN-код "12345678".

На этом моменте уже можно работать с регистратором (если нет - см. п. 2.6). Для того чтобы браузер доверял сертификату браузера и не отображал предупреждения безопасности, требуется внести сертификаты регистратора в список доверенных как показано в следующем разделе.

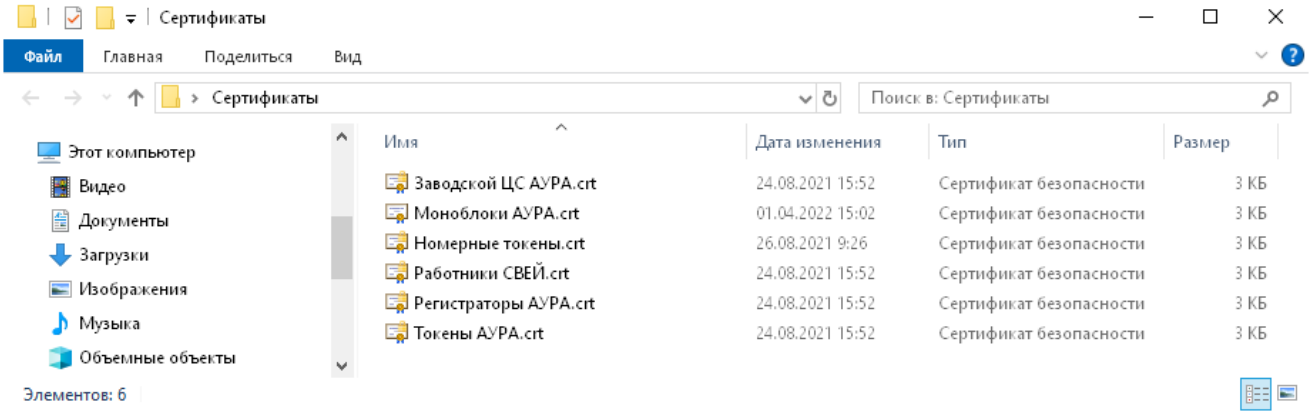

Ошибка нарушения конфиденциал
Не защищено | https://192.168.1.198
Подключение не защищено
Злоумышленники могут пытаться похитить ваши данные с сайта 192.168.1.198 (например, пароли, сообщения или номера банковских карт). Подробнее...
NET::ERR_CERT_COMMON_NAME_INVALID
Чтобы браузер Chrome стал максимально безопасным, включите режим "Улучшенная защита".
Дополнительные
Вернуться к безопасной странице


Ошибка нарушения конфиденциал
Не защищено | https://192.168.1.198
Подключение не защищено
Злоумышленники могут пытаться похитить ваши данные с сайта 192.168.1.198 (например, пароли, сообщения или номера банковских карт). Подробнее...
NET::ERR_CERT_COMMON_NAME_INVALID
Чтобы браузер Chrome стал максимально безопасным, включите режим "Улучшенная защита".
Скрыть подробности
Вернуться к безопасной странице
Не удалось подтвердить, что это сервер 192.168.1.198. Его сертификат безопасности относится к aura. Возможно, сервер настроен неправильно или кто-то пытается перехватить ваши данные.
Перейти на сайт 192.168.1.198 (небезопасно)

2.4 Установка сертификатов для доверенного подключения браузера по HTTPS

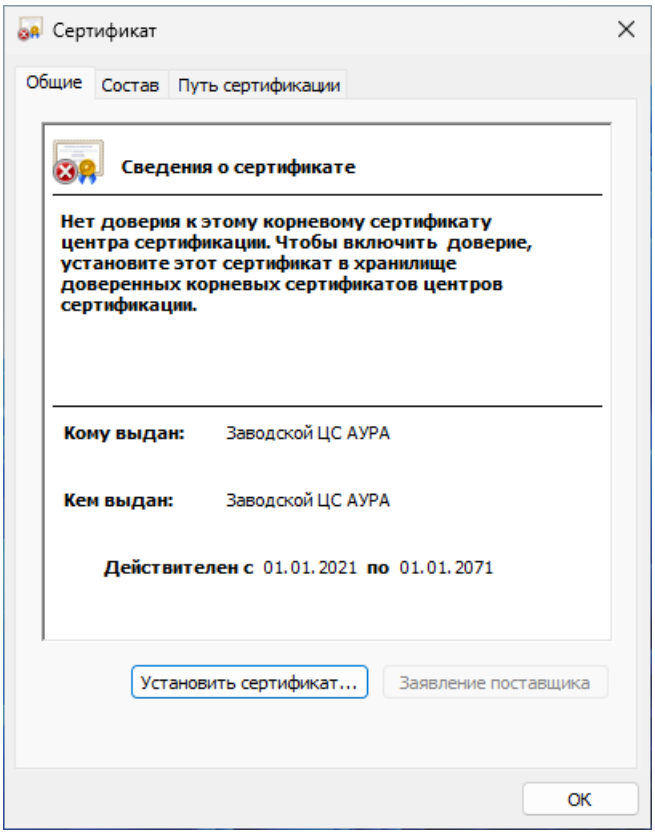
Первым условием, которое необходимо выполнить чтобы браузер доверял соединению с регистратором, является установка корневого и промежуточного сертификатов, которыми подписан сертификат регистратора, в список доверенных сертификатов операционной системы.

Сертификаты поставляются на флэш-диске в комплекте с регистратором, например, как показано ниже.

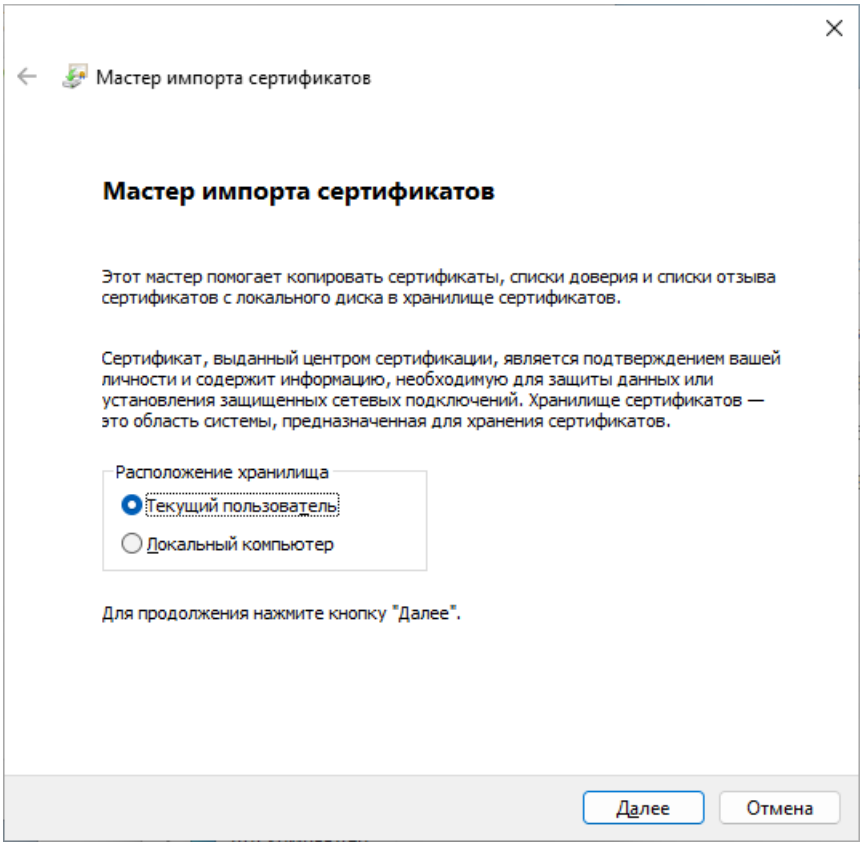


В простейшем случае достаточно установить сертификаты "Заводской ЦС АУРА" и "Регистраторы АУРА". Остальные сертификаты служат для проверки пользовательских сертификатов и браузером не используются.

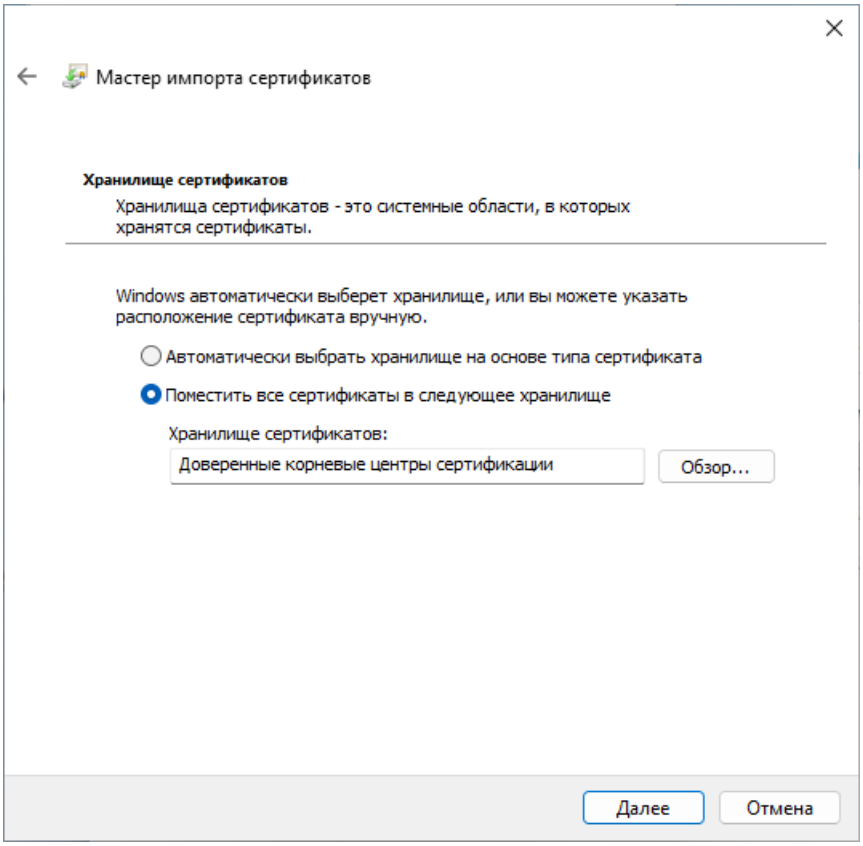
Для установки сертификата "Заводской ЦС АУРА.crt" откройте двойным щелчком мыши окно "Сертификат":



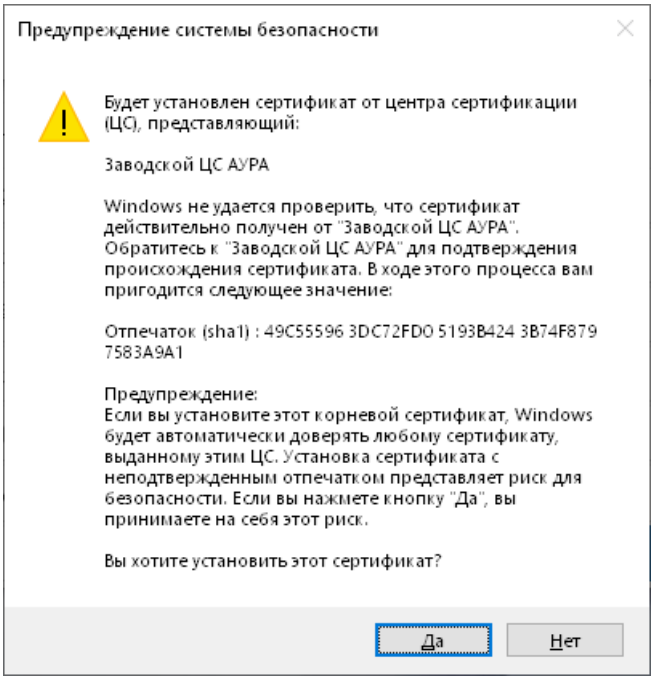
Нажмите кнопку "Установить сертификат", откроется окно "Мастер импорта сертификатов". Выберите пункт "Расположение хранилища" - "Текущий пользователь", "Далее".



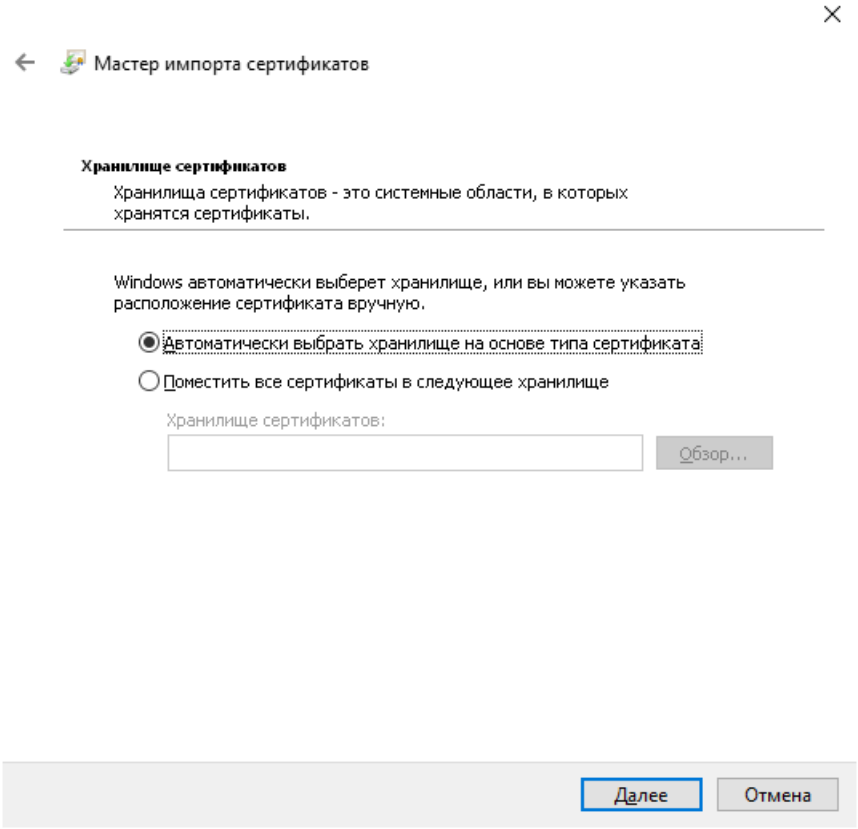
Затем, выберите пункт "Поместить все сертификаты в следующее хранилище" - нажмите кнопку "Обзор" - выберите пункт "Доверенные корневые центры сертификации" - "ОК". Затем, нажмите "Далее" и "Готово".



Откроется окно "Предупреждение системы безопасности", нажмите "Да".



Затем установите сертификат "Регистраторы АУРА.crt" (и, необязательно, остальные сертификаты из комплекта поставки) аналогичным образом, но на шаге "Хранилище сертификатов" оставляя выбор пункта "Автоматически выбрать хранилище на основе типа сертификата".



На этом этапе уже можно обращаться к регистратору со стандартным IP-адресом (192.168.x.99). Если на регистраторе используется другой IP-адрес, перейдите к следующему разделу.

2.5 Привязка доменного имени aura к нестандартному IP-адресу регистратора

Сертификат регистратора содержит предустановленный список IP-адресов. В заводской поставке это могут быть доменные адреса "aura", "aura-1234", IP-адреса "192.168.0.99", "192.168.1.99", "192.168.2.99" и т.д. до "192.168.9.99".

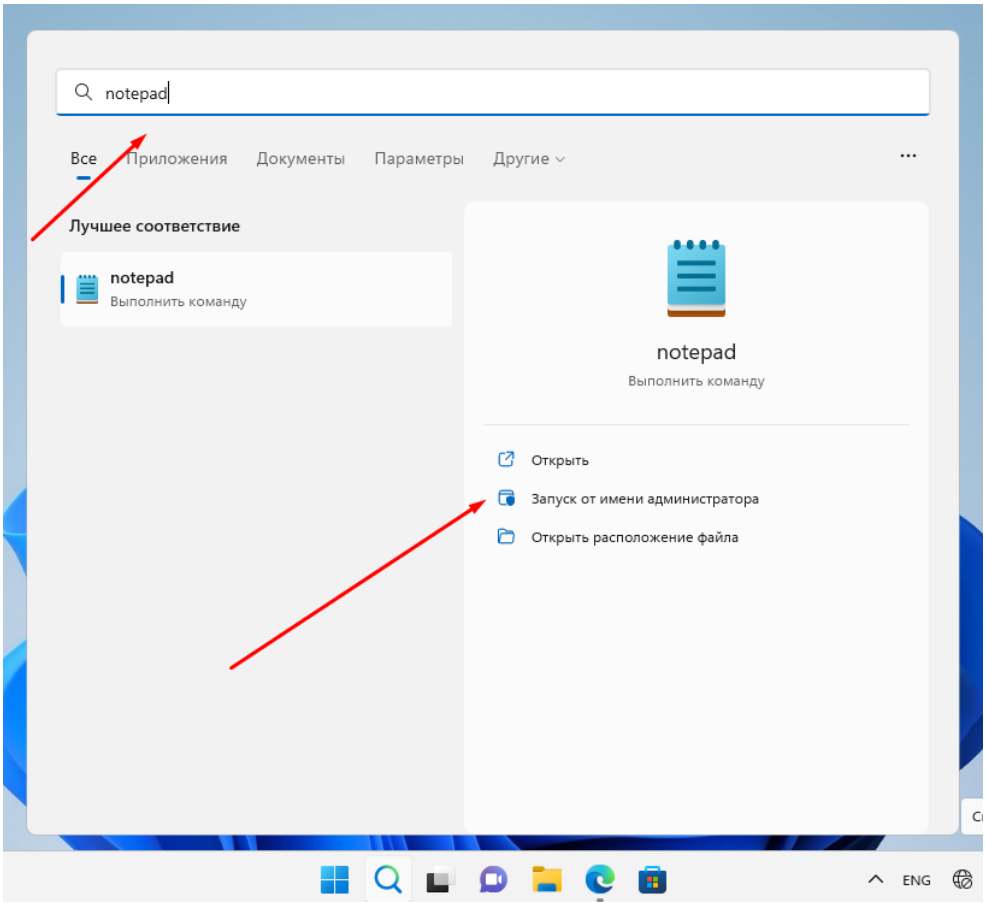
Ваш регистратор может быть настроен на другой произвольный IP-адрес. В этом случае, при подключении к веб-интерфейсу браузер будет выводить ошибку. Это связано с тем, что фактический адрес не соответствует прописанному в сертификате регистратора. Вы можете игнорировать ошибку, нажав кнопку "Дополнительные" и "Перейти на сайт … (небезопасно)".

Чтобы устранить это предупреждение, следует сделать выполнить одну из следующих операций:

- Заменить сертификат регистратора на новый, содержащий фактически используемые IP-адреса (за получением сертификата обратитесь к производителю регистратора).
- Прописать соответствие имени aura адресу регистратора (описывается ниже).

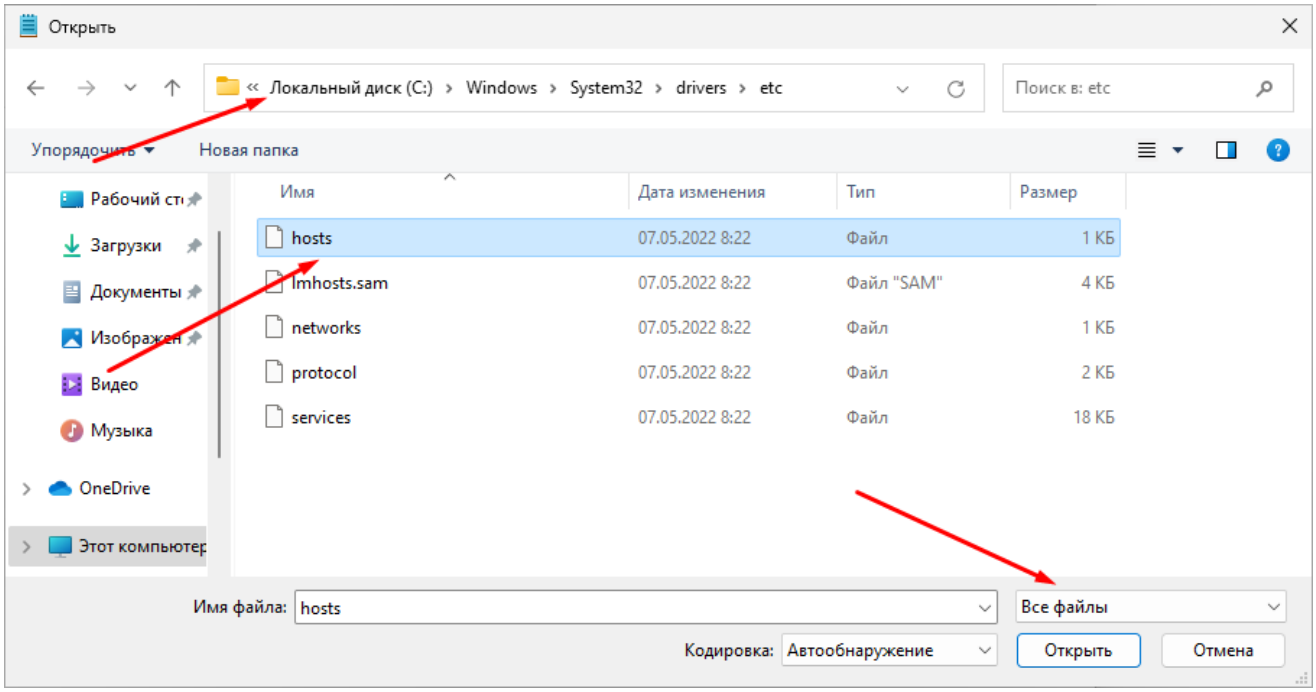
В данном разделе описывается изменение защищённого системного файла hosts, в котором настраивается соответствие доменов IP-адресам.

Откройте программу "Блокнот" в режиме администратора следующим образом: нажмите "Пуск" - наберите в поиске "notepad" или "Блокнот" и запустите его в режиме администратора (для изменения системного файла).

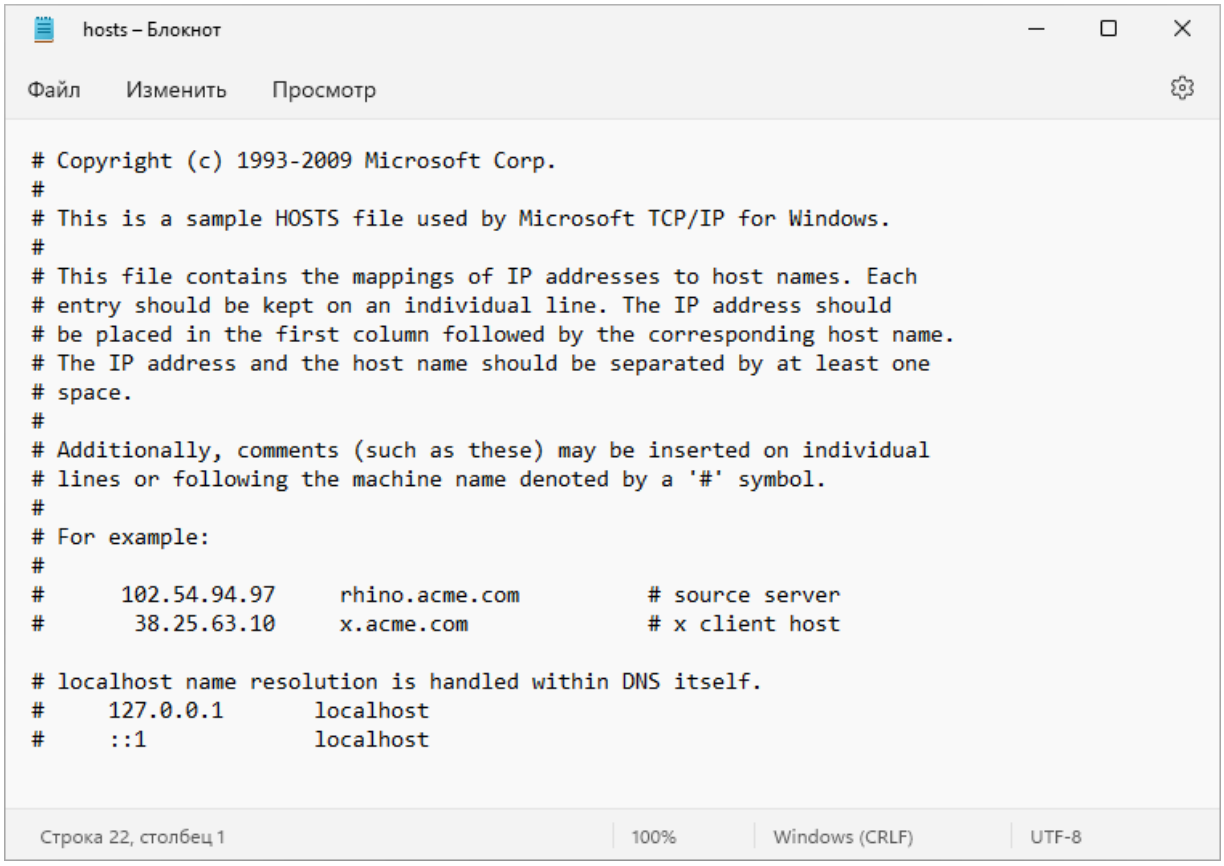


Во всплывающем окне с вопросом "Разрешить этому приложению…" нажмите кнопку "Да". Откроется окно "Блокнота". Далее нажмите пункт меню "Файл", "Открыть".

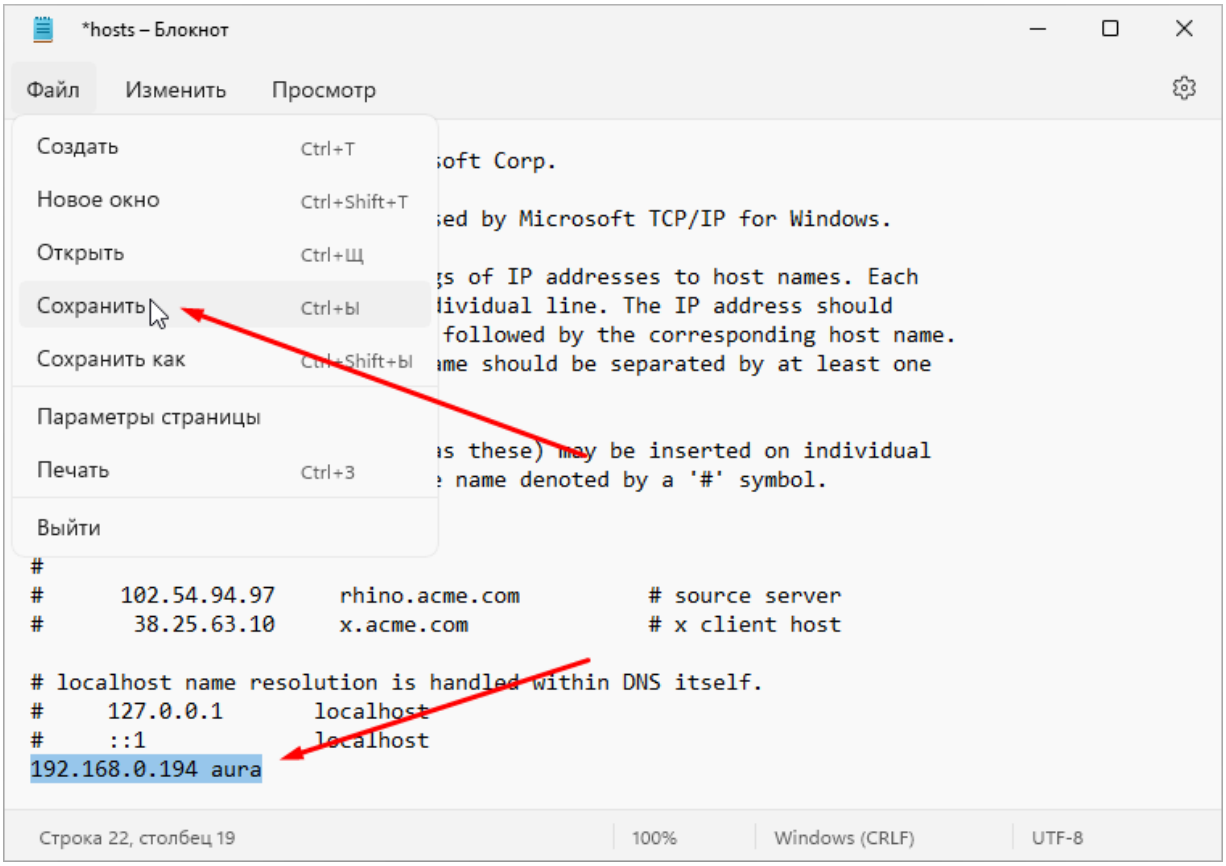
В окне "Открыть" откройте папку "Локальный диск (C:) / Windows / System32 / drivers / etc". В нижнем правом углу окна выберите тип показываемых файлов "Все файлы". Появится возможность выбрать файл "hosts", откройте его.



Появится содержимое файла hosts:



В самом низу файла добавьте новую строчку с IP-адресом регистратора и словом aura как показано ниже и сохраните сделанные изменения.

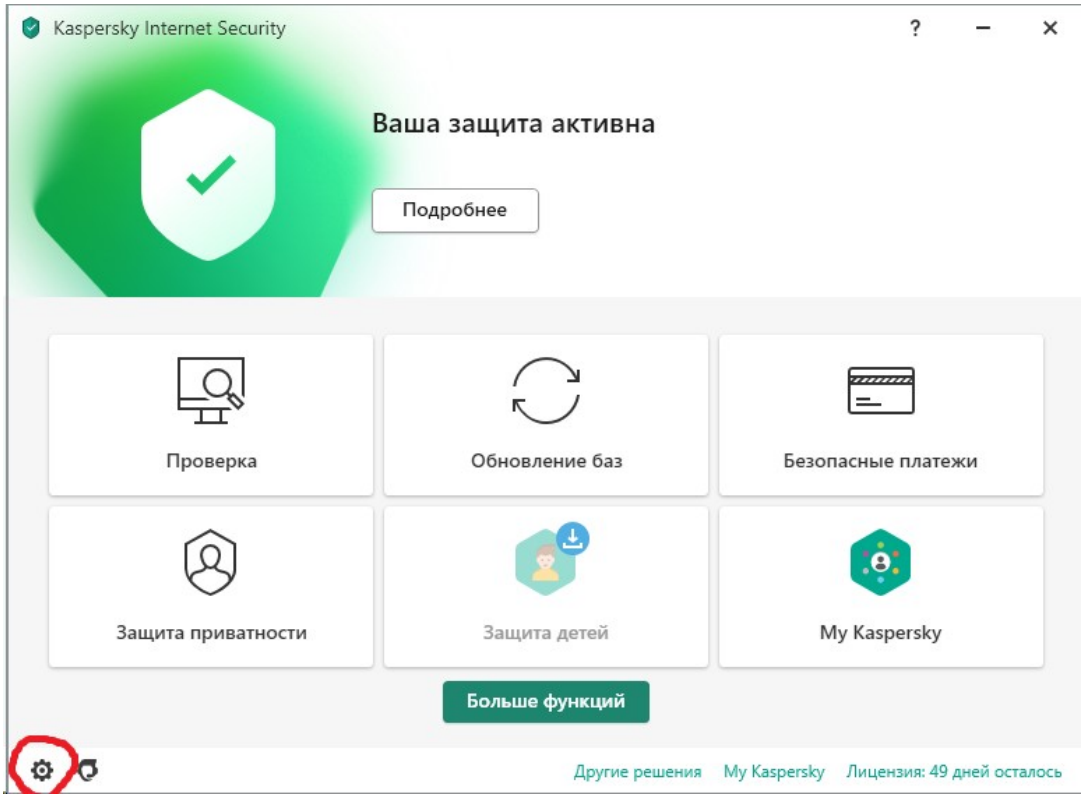


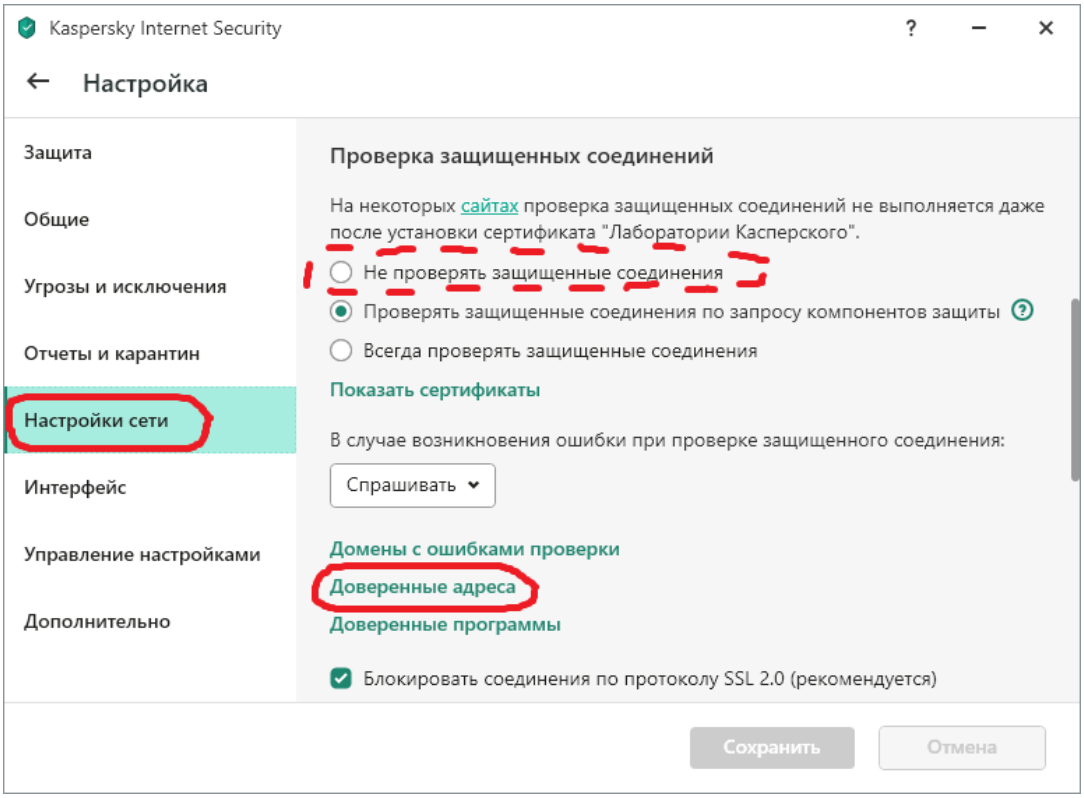
Проверить доступ к регистратору можно подключив токен, открыв браузер и пройдя по адресу https://aura.

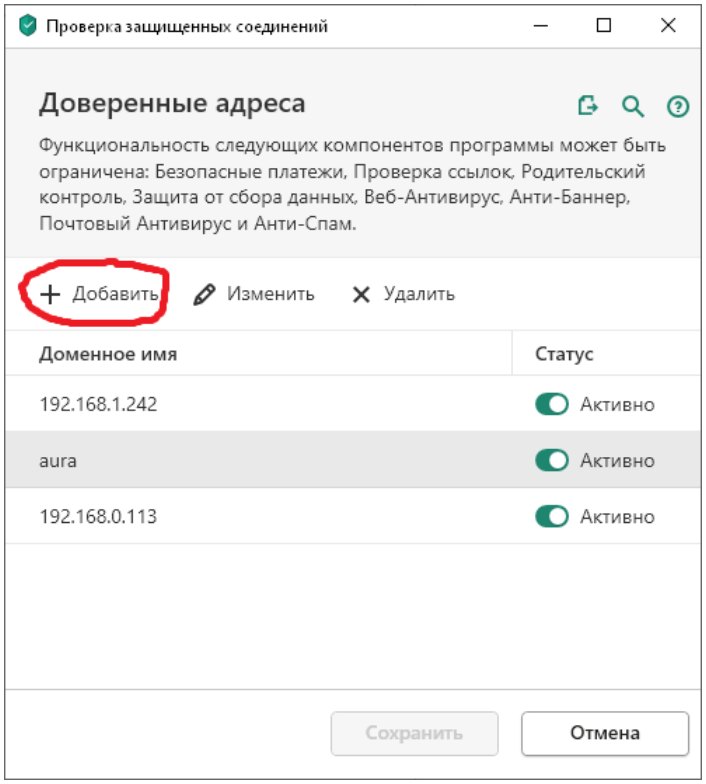
Если веб-интерфейс не отображается, то это может быть вызвано работой антивируса (если он установлен). Настройка на примере антивируса Kaspersky Internet Security описывается в следующем разделе.

2.6 Влияние прокси и антивирусных программ

Прокси-серверы и антивирусные программы могут вмешиваться в прямое взаимодействие между браузером и регистратором, разрывая прямое TLS-соединение между ними и заменяя его на два отдельных соединения, между которыми находится прокси / антивирус. Это не всегда работает корректно, особенно с клиентскими цифровыми сертификатами на аппаратных носителях. При работе с регистраторами АУРА рекомендуется вносить их в исключения прокси / антивируса для разрешения соединения браузера с регистратором напрямую. Например, в Kaspersky Internet Security это делается так (сплошной линией обведены требуемые действия; пунктирной линией обведены альтернативные действия на время частой смены адресов - например, наладки):


Kaspersky Internet Security
Ваша защита активна
Подробнее
Проверка
Обновление баз
Безопасные платежи
Защита приватности
Защита детей
My Kaspersky
Больше функций
Другие решения
My Kaspersky
Лицензия: 49 дней осталось


Kaspersky Internet Security
Настройка
Защита
Общие
Угрозы и исключения
Отчеты и карантин
Настройки сети
Интерфейс
Управление настройками
Дополнительно
Проверка защищенных соединений
На некоторых сайтах проверка защищенных соединений не выполняется даже после установки сертификата "Лаборатории Касперского".
Не проверять защищенные соединения
Проверять защищенные соединения по запросу компонентов защиты
Всегда проверять защищенные соединения
Показать сертификаты
В случае возникновения ошибки при проверке защищенного соединения:
Спрашивать
Домены с ошибками проверки
Доверенные адреса
Доверенные программы
Блокировать соединения по протоколу SSL 2.0 (рекомендуется)
Сохранить
Отмена


Проверка защищенных соединений
Доверенные адреса
Функциональность следующих компонентов программы может быть ограничена: Безопасные платежи, Проверка ссылок, Родительский контроль, Защита от сбора данных, Веб-Антивирус, Анти-Баннер, Почтовый Антивирус и Анти-Спам.
Добавить
Изменить
Удалить
Доменное имя
Статус
192.168.1.242
Активно
aura
Активно
192.168.0.113
Активно
Сохранить
Отмена