TrustGate

Руководство администратора

infotecs

© ОАО «ИнфоТеКС Интернет Траст», 2022

ФРКЕ.00233-01 32 01

Версия продукта 2.4

Этот документ входит в комплект поставки ПО TrustGate, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС Интернет Траст».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС Интернет Траст»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 3 этаж

Телефон: +7 (495) 137-83-23, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт:

Служба технической поддержки:, +7 (495) 137-70-47

Содержание

Введение 4
О документе 5
Для кого предназначен документ 5
Соглашения документа 5
О программе 7
Структура и ролевая модель TrustGate 7
Требования к серверу TrustGate 8
Требования к АРМ администратора 9

Глава 1. Установка, настройка и обновление 10
Установка TrustGate с использованием преднастроек 11
Настройка TrustGate 15
Аутентификация в веб-интерфейсе АРМ администратора 15
Описание интерфейса АРМ администратора 16
Регистрация лицензии TrustGate 18
Создание учетной записи персонала 21
Добавление организаций 23
Настройки организации для отправки запросов в ЕСИА 26
Создание учетной записи оператора 26
Настройки пользователя для отправки запросов в ЕСИА 30
Настройка файловой интеграции 31
Обновление TrustGate 32
Проверка работоспособности TrustGate 34

Глава 2. Администрирование TrustGate 35
Резервное копирование базы данных TrustGate 36
Восстановление базы данных TrustGate из копии 38
Изменение параметров криптопровайдера 39
Настройка сценария идентификации в ЕСИА 40
Просмотр параметров запросов 42

Приложение А. Глоссарий 46

Введение

О документе

Документ является руководством по администрированию ПО TrustGate. Данное ПО предоставляет кредитным и иным организациям (далее — организация) возможность для передачи сведений и отправки запросов на предоставление информации в Систему межведомственного электронного взаимодействия – СМЭВ.

Для кого предназначен документ

Документ предназначен для сотрудников организаций, выполняющих установку, первичную настройку и последующее администрирование ПО TrustGate.

Информация в документе рассчитана на администраторов, которые имеют навыки работы с операционной системой (далее — ОС) Linux.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.

Обозначение	Описание
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

При описании команд в данном документе используются следующие условные обозначения:

- Команды, которые могут быть выполнены только в режиме администратора, содержат приглашение с символом «#». Например:

```
hostname# admin config list
```

- Команды, которые могут быть выполнены в режиме и пользователя, и администратора, содержат приглашение с символом «>». Например:

```
hostname> alg restart
```

- При описании в документе параметры, которые должны быть заданы пользователем, заключены в угловые скобки «<>»:

```
inet bonding delete <номер>
```

При вводе в командный интерпретатор параметры, которые должны быть заданы пользователем, вводятся без угловых скобок:

```
hostname# inet bonding delete 1
```

- При описании в документе необязательные параметры или ключевые слова заключены в квадратные скобки «[]». Например:

```
firewall <тип> add name @<имя> <состав> [exclude <исключения>]
```

При вводе в командный интерпретатор необязательные параметры или ключевые слова вводятся без квадратных скобок. Например:

```
hostname# firewall interface-object add name @intgroup interface eth0 interface
eth1
```

- Если при вводе команды можно указать один из нескольких параметров, при описании в документе допустимые варианты заключены в фигурные скобки «{}» и разделены вертикальной чертой «|». Например:

```
inet ntp mode {on | off}
```

Если при вводе команды можно указать один из нескольких параметров, то при вводе в командный интерпретатор выбранные варианты параметров вводятся без фигурных скобок. Например:

```
hostname# inet ntp mode off
```

О программе

С помощью ПО TrustGate вы можете создавать и отправлять запросы на регистрацию данных и на предоставление информации в различные ведомства и организации.

Запросы и ответы на запросы представляют собой электронные документы, информация в которых представлена в регламентированных формах.

Структура и ролевая модель TrustGate

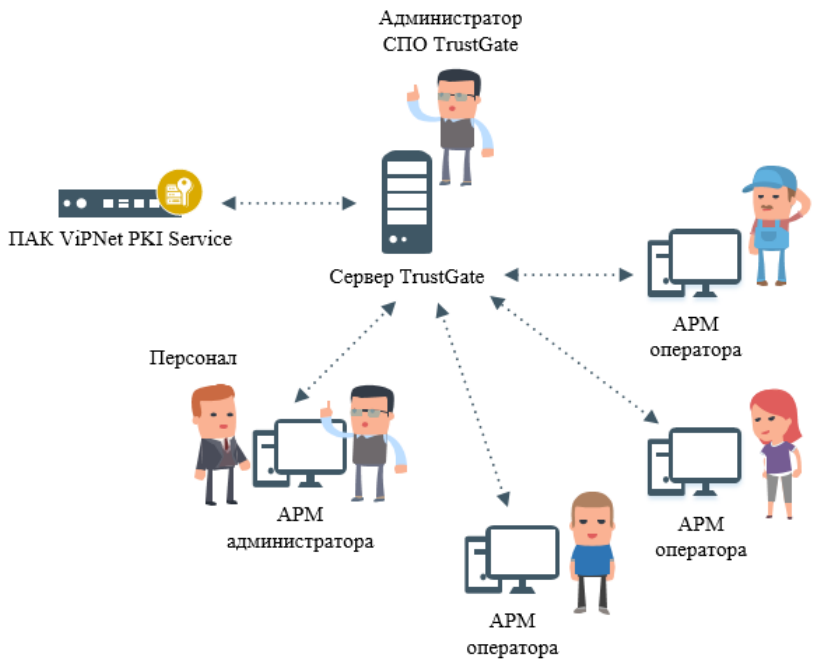


Рисунок 1. Компоненты структуры СПО TrustGate и их взаимосвязь

- Администратор - устанавливает ПО TrustGate на сервер, обновляет и администрирует, отвечает за эксплуатацию сервера и ПО. Учетная запись администратора создается при установке ПО TrustGate и используется для первичного входа в веб-интерфейс автоматизированного рабочего места (далее – АРМ) администратора с целью создания учетной записи персонала.
- Персонал - в веб-интерфейсе АРМ администратора настраивает взаимодействие со СМЭВ (добавление организаций, пользователей, загрузка справочной информации), и частично администрирует ПО TrustGate (обновление справочников, настройка сценариев работы, изменение шаблонов документов, просмотр параметров запросов операторов). Учетная запись персонала создается администратором.
- Оператор - в веб-интерфейсе АРМ оператора формирует и отправляет запросы в СМЭВ. Учетная запись оператора создается персоналом.

Требования к серверу TrustGate

Минимальные требования (от 1 до 50 АРМ операторов):

- Процессор — Intel Xeon с частотой от 2,5 ГГц с количеством ядер 4 и более.
- Объем оперативной памяти — не менее 8 Гбайт.
- Для отправки запросов в ЕБС — видеокарта NVIDIA с поддержкой CUDA версии 7.0 и выше.
- Свободное место на жестком диске — не менее 500 Гбайт.
- Операционная система:
  - Astra Linux SE 1.6 (Смоленск) — если организация будет отправлять запросы в ЕБС.
  - Linux Ubuntu 16.04 — для работы с другими государственными информационными системами.

Внимание! Запрещается использовать измененные или отладочные версии ОС (такие, как Debug или Checked Build).

На сервере перед установкой ПО TrustGate должен быть установлен актуальный пакет обновления ОС и все известные критические обновления, опубликованные производителем ОС.

- Средство криптографической защиты информации (далее — СКЗИ):
  - ПАК ViPNet PKI Service (см. глоссарий, стр. 46) — если организация будет отправлять запросы в ЕБС.

    Компьютер с ПАК должен быть связан по сети с сервером TrustGate.
  - Программа ViPNet CSP (см. глоссарий, стр. 46) — для отправки запросов в другие государственные информационные системы.

    Программа ViPNet CSP входит в дистрибутив ПО TrustGate, устанавливается на сервер при установке ПО. Для работы программы требуется контейнер ключей, который содержит закрытый ключ, и сертификат с открытым ключом.
- Сертифицированные средства защиты информации, которые включают средства антивирусной защиты и средства противодействия компьютерным атакам.

Оптимальные требования (от 50 до 200 АРМ операторов):

- Процессор — Intel Xeon с частотой от 2,5 ГГц с количеством ядер 8 и более.
- Объем оперативной памяти — не менее 16 Гбайт.
- Для отправки запросов в ЕБС — видеокарта NVIDIA с поддержкой CUDA версии 7.0 и выше.
- Свободное место на жестком диске — не менее 500 Гбайт.
- Операционная система:

- Astra Linux SE 1.6 (Смоленск) — если организация будет отправлять запросы в ЕБС.
- Linux Ubuntu 16.04 — для работы с другими государственными информационными системами.

Внимание! Запрещается использовать измененные или отладочные версии ОС (такие, как Debug или Checked Build).

На сервере перед установкой ПО TrustGate должен быть установлен актуальный пакет обновления ОС и все известные критические обновления, опубликованные производителем ОС.

- Средство криптографической защиты информации (далее — СКЗИ):
  - ПАК ViPNet PKI Service (см. глоссарий, стр. 46) — если организация будет отправлять запросы в ЕБС.

    Компьютер с ПАК должен быть связан по сети с сервером TrustGate.
  - Программа ViPNet CSP (см. глоссарий, стр. 46) — для отправки запросов в другие государственные информационные системы.

    Программа ViPNet CSP входит в дистрибутив ПО TrustGate, устанавливается на сервер при установке ПО. Для работы программы требуется контейнер ключей, который содержит закрытый ключ, и сертификат с открытым ключом.
- Сертифицированные средства защиты информации, которые включают средства антивирусной защиты и средства противодействия компьютерным атакам.

Требования к АРМ администратора

АРМ администратора представляет собой рабочее место специалиста, который выполняет операции по настройке и администрированию ПО TrustGate.

Рекомендуемые требования к АРМ администратора:

- Процессор — Intel или AMD с количеством ядер 2 и более.
- Объем оперативной памяти — не менее 1 Гбайт.
- Свободное место на жестком диске — не менее 500 Мбайт.
- Любая операционная система.
- Браузер Google Chrome версии 67 и выше.

1

Установка, настройка и обновление

Установка TrustGate с использованием преднастроек

Установку ПО TrustGate выполняет администратор операционной системы (root).

Перед началом установки:

- Убедитесь, что у вас есть установочный файл ПО TrustGate — `g2g_ng_dist-<номер сборки>.zip`.
- Если ПО TrustGate будет эксплуатироваться совместно с программой ViPNet CSP, удостоверьтесь, что у вас есть бинарный файл, который содержит контейнер ключей (закрытый ключ для подписи и расшифровки запросов) и сертификат (открытый ключ для проверки подлинности вашей подписи и зашифровки входящих сообщений).

  Файл предоставляется компанией ОАО «ИнфоТеКС Интернет Траст». Обязательно разместите его на сервере перед установкой ПО.

  Программа ViPNet CSP входит в дистрибутив ПО TrustGate, устанавливается на сервер при установке ПО.

Примечание. ViPNet CSP не входит в дистрибутив TrustGate для ЕБС.

- Если ПО TrustGate будет эксплуатироваться совместно с ПАК ViPNet PKI Service, свяжите его по сети с сервером.

  Подробнее см. в документе «Программно-аппаратный комплекс ViPNet PKI Service. Руководство администратора».

- Убедитесь, что сервер, на котором будет развернуто ПО, соответствует требованиям безопасности. Подробнее о требованиях см. документе «TrustGate Требования безопасности при эксплуатации» (входит в комплект поставки).

Для установки выполните следующие действия:

1. Распакуйте дистрибутив ПО в произвольный каталог с помощью команды:

   ```
   hostname# unzip -x g2g_ng_dist-<номер сборки>.zip
   ```

2. Перейдите в каталог `libs` и создайте в нем каталог `containers` с помощью команд:

   ```
   hostname# cd <каталог дистрибутива>/libs
   hostname# mkdir containers
   ```

3. Перейдите в каталог `containers` и создайте в нем файл `config.json` с помощью команд:

   ```
   hostname# cd containers
   hostname# nano config.json
   ```

Примечание. Вы можете использовать любой текстовый редактор, который у вас установлен.

- Если ПО TrustGate будет эксплуатироваться совместно с программой ViPNet CSP, тогда добавьте в файл `config.json` следующие строки:

```
{
    «containers»: [
      {
            «path»: «<абсолютный путь к контейнеру ключей>»,
            «password»: «<пароль от контейнера ключей>»
      }
    ]
}
```

Примечание. Если у организации несколько контейнеров ключей, параметры `path` и `password` для каждого контейнера можно задать в фигурных скобках через запятую.

Если после установки ПО изменился путь или пароль к контейнеру, появился новый контейнер ключей или устарел текущий, обязательно внесите эти изменения в json-файл (см. Изменение параметров криптопровайдера на стр. 39).

- Если ПО TrustGate будет эксплуатироваться совместно с ПАК ViPNet PKI Service, тогда добавьте в файл `config.json` следующие строки:

```
{
    «pki_service»: {
            «url»: «http://<адрес>:<порт>,где установлен ПАК ViPNet PKI
    Service»,
            «accounts»: [
                  {
                        «login»: «<имя пользователя для доступа к ПАКу>»,
                        «password»: «<пароль для доступа к ПАКу>»
                  }
            ]
    }
}
```

Примечание. Если у организации несколько учетных записей на ViPNet PKI Service, параметры `login` и `password` для каждой учетной записи можно задать в фигурных скобках через запятую.

Если после установки ПО изменился адрес ПАКа, была добавлена новая учетная запись пользователя или устарела текущая, обязательно внесите эти изменения в json-файл (см. Изменение параметров криптопровайдера на стр. 39).

4 Перейдите в каталог, который содержит распакованный дистрибутив ПО TrustGate, при помощи команды:

```
hostname# cd <каталог дистрибутива>
```

5 Запустите установку ПО TrustGate с помощью команды:

```
hostname# sudo python install.py -v -c installation.config
```

`installation.config` является файлом конфигурации в формате JSON. Если не будет указан необходимый ключ, то программа задаст соответствующий вопрос для его настройки в процессе установки.

Возможные ключи файла `installation.config`:

- **subnet** — маска подсети для запуска системы.

> **Примечание.** Вы можете указать любую маску, кроме 170.20.x.x и сетей, которые уже используются в рамках организации.
>
> Вы также можете указать маску подсети из примера — 192.168.0.0/16.

- **no_ssl** — если установлено значение false, то при первой установке необходимо ввести параметры для создания самоподписанного сертификата.

> **Примечание.** SSL-сертификат обеспечивает защищенное соединение между АРМ оператора и сервером TrustGate. Вы можете разместить свой сертификат и ключ по пути: `<каталог дистрибутива>/g2g/nginx`, с именами файлов `g2g_nginx.crt` и `g2g_nginx.key` соответственно. Доступ к закрытому ключу должен осуществляться без указания пароля.
>
> Обязательно сформируйте сертификат, если организация будет отправлять запросы в ЕБС.

- **uz1_flag** — если установлено значение true, то будет включен усиленный уровень защиты.
- **no_proxy** — если установлено значение false, то необходимо указать параметры прокси-сервера
- **config** — адрес прокси-сервера (например, `http://<host>:<port>`).
- **no_netdata** — если установлено значение false, то будет произведена установка netdata для мониторинга системы.

6 В конце установки создайте учетную запись администратора:

- Введите имя учетной записи (`Input admin username`).
- Введите пароль (`Input admin password`).
- Нажмите клавишу **Enter**.

Внимание! Обязательно создайте учетную запись администратора, так как она необходима для дальнейшей настройки ПО TrustGate (см. Структура и ролевая модель TrustGate на стр. 7).

Если вы отменили создание учетной записи, то для ее повторного формирования выполните команду:

```
hostname# docker exec -it g2g_web_1 python manage.py createsuperuser
```

В результате ПО TrustGate будет установлено на сервер. Информация о процессах, происходящих при установке, записывается в файл `install.log`, расположенный в каталоге `/var/log/trust_gate/`. Информация о введенных настройка сохранится в файле `installation.config`.

После успешного завершения установки на 80 или 443 (если был создан SSL-сертификат) порту автоматически запускается веб-сервис.

Настройка TrustGate

Для первичной настройки ПО TrustGate выполните действия, перечисленные ниже.

Таблица 3. Последовательность действий при первичной настройке

	Действие	Ссылка
☐	Зарегистрируйте лицензию	Регистрация лицензии ПО TrustGate (на стр. 18)
☐	Создайте учетную запись персонала для настройки и последующего администрирования программы	Создание учетной записи персонала (на стр. 21)
☐	Добавьте организации, от имени которых будет осуществляться отправка запросов в СМЭВ	Добавление организаций (на стр. 23)
☐	Создайте учетные записи пользователей, которые будут работать с запросами	Создание учетной записи оператора (на стр. 26)
☐	Загрузите необходимые справочники	Загрузка справочной информации (на стр. 31)
☐	Проверьте работоспособность ПО TrustGate	Проверка работоспособности TrustGate (на стр. 34)

Совет. Рекомендуем распечатать список и отмечать в нем шаги по мере их выполнения.

Аутентификация в веб-интерфейсе АРМ администратора

Для аутентификации в веб-интерфейсе АРМ администратора выполните следующие действия:

1. В адресной строке браузера введите адрес сервера TrustGate.
2. На странице аутентификации введите имя учетной записи и пароль к ней.

Внимание! При первичном входе, регистрации и обновлении лицензии и для создания учетной записи персонала, используйте учетные данные администратора, которые были указаны в процессе установки ПО TrustGate на сервер (см. Установка TrustGate на стр. 10).

Для настройки взаимодействия со СМЭВ (добавление организаций, создание учетных записей операторов, загрузка справочной информации) и для администрирования ПО TrustGate (обновление справочников, настройка сценария работы с ЕБС, изменение шаблонов документов, просмотр параметров запросов операторов) используйте учетные данные персонала (см. Создание учетной записи персонала на стр. 21).

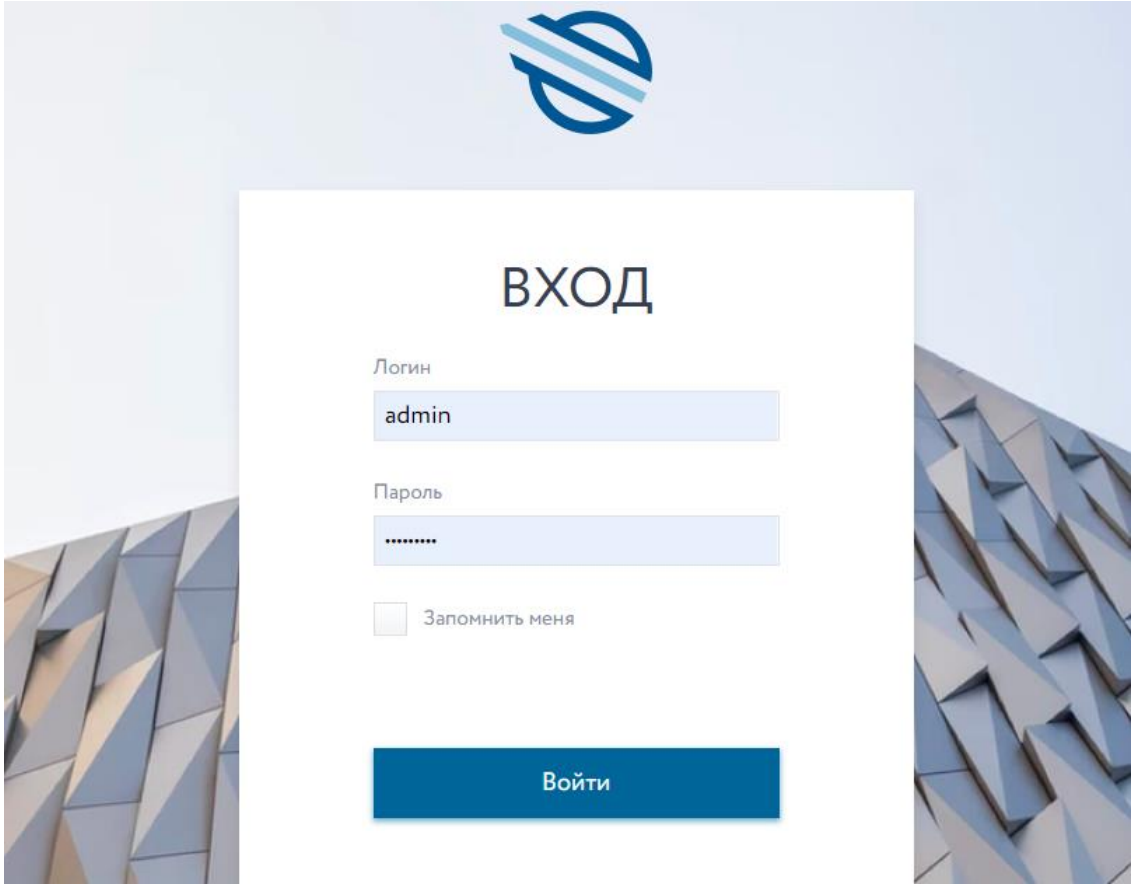


Рисунок 2. Авторизация в веб-интерфейсе TrustGate с использованием учетной записи администратора

3 Чтобы сохранить в браузере параметры доступа к учетной записи, установите флажок **Запомнить меня**. Это позволит повторно не указывать имя пользователя и пароль при последующих обращениях к веб-интерфейсу АРМ администратора.

Внимание! Сохранение параметров доступа ведет к снижению уровня безопасности.

---

4 Нажмите кнопку **Войти**.

Описание интерфейса АРМ администратора

Внешний вид главной страницы веб-интерфейса АРМ администратора TrustGate будет различаться в зависимости от того, вошли вы с использованием учетной записи администратора или персонала:

Элементы веб-интерфейса TrustGate, доступные администратору:

1 Ссылка **TrustGate** — с помощью этой ссылки вы можете перейти на главную страницу веб-интерфейса АРМ администратора.

2 Раздел **Список пользователей** — с помощью этого раздела вы можете перейти к списку учетных записей персонала.

3 Меню **Пользователь** — с помощью этого меню вы можете сменить пароль от вашей учетной записи или выйти из веб-интерфейса АРМ администратора.

4 Панель инструментов — содержит поле фильтрации, необходимое для поиска учетных записей пользователей (операторов), и кнопки с действиями, которые можно совершить с учетной записью (создать новую, отредактировать, заблокировать или разблокировать существующую).

5 Панель просмотра — содержит список учетных записей персонала, которые имеют доступ к веб-интерфейсу АРМ администратора.

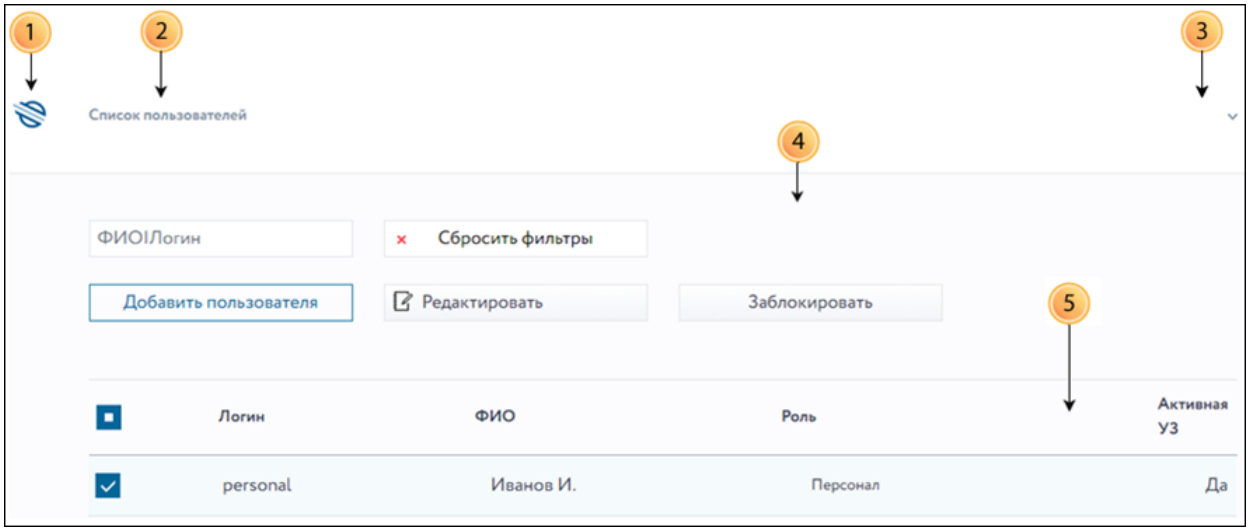


Рисунок 3. Главная страница веб-интерфейса TrustGate для администратора

Элементы веб-интерфейса TrustGate, доступные персоналу:

1 Ссылка **TrustGate** — с помощью этой ссылки вы можете перейти на главную страницу веб-интерфейса АРМ администратора.

2 Раздел **Список пользователей** — с помощью этого раздела вы можете перейти к списку учетных записей операторов.

3 Раздел **Список организаций** — с помощью этого раздела вы можете перейти к списку всех организаций, от имени которых можно отправлять запросы в СМЭВ.

4 Раздел **Справочники** — с помощью этого раздела вы можете перейти на страницу, на которой происходит загрузка и обновление справочной информации, настройка сценариев и шаблонов документов, необходимых для взаимодействия со СМЭВ.

5 Раздел **Запросы** — с помощью этого раздела вы можете перейти к списку всех запросов в формате XML.

6 Меню **Пользователь** — с помощью этого меню вы можете сменить пароль от вашей учетной записи или выйти из веб-интерфейса АРМ администратора.

7 Панель инструментов — содержит поле фильтрации, необходимое для поиска учетных записей пользователей (операторов), и кнопки с действиями, которые можно совершить с учетной записью (создать новую учетную запись, отредактировать, заблокировать или разблокировать существующую).

8 Панель просмотра — содержит список учетных записей пользователей, которые имеют доступ к веб-интерфейсу АРМ оператора.

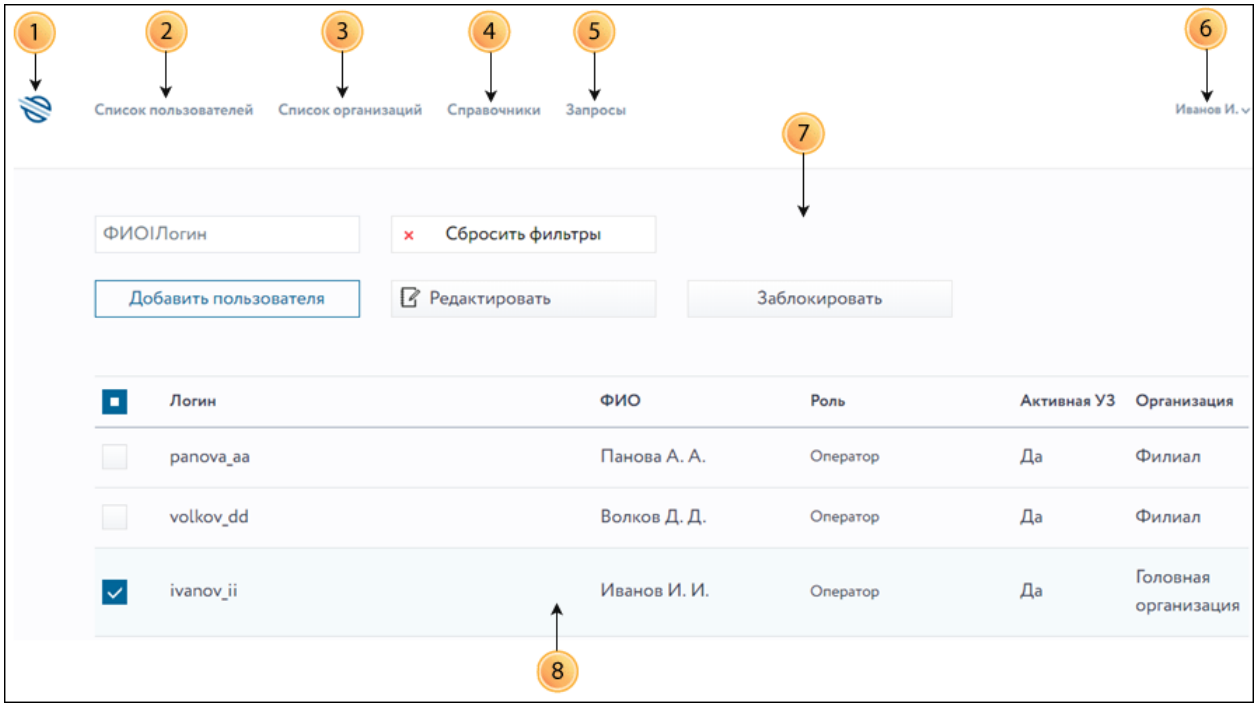


Рисунок 4. Главная страница веб-интерфейса TrustGate для персонала

Регистрация лицензии TrustGate

В комплект поставки ПО TrustGate входит файл лицензии, который включает следующую информацию:

- срок действия основной лицензии для работы с ПО;
- расширение возможностей основной лицензии:
  - количество АРМ администраторов — количество сотрудников организации, авторизованных с использованием учетной записи персонала (см. Структура и ролевая модель TrustGate на стр. 7), которые могут одновременно работать с ПО;
  - количество АРМ пользователей — количество сотрудников организации, авторизованных с использованием учетной записи оператора (см. Структура и ролевая модель TrustGate на стр. 7), которые могут одновременно работать с ПО;
  - количество АРМ пользователей для работы с ЕБС — количество сотрудников организации, авторизованных с использованием учетной записи оператора (см. Структура и ролевая модель TrustGate на стр. 7), которые могут одновременно отправлять запросы на регистрацию биометрических образцов клиентов в ЕБС;
  - пакеты сервисов — запросы, которые организация может отправлять в СМЭВ. Список доступных запросов описан в разделе Добавление организаций (на стр. 23) в 6 пункте.

Для работы с ПО TrustGate зарегистрируйте вашу лицензию. Для этого выполните следующие действия:

1 Войдите в веб-интерфейс АРМ администратора с использованием учетной записи администратора (см. Аутентификация в веб-интерфейсе АРМ администратора на стр. 15).

2 На главной странице веб-интерфейса выберите раздел **Лицензирование**.

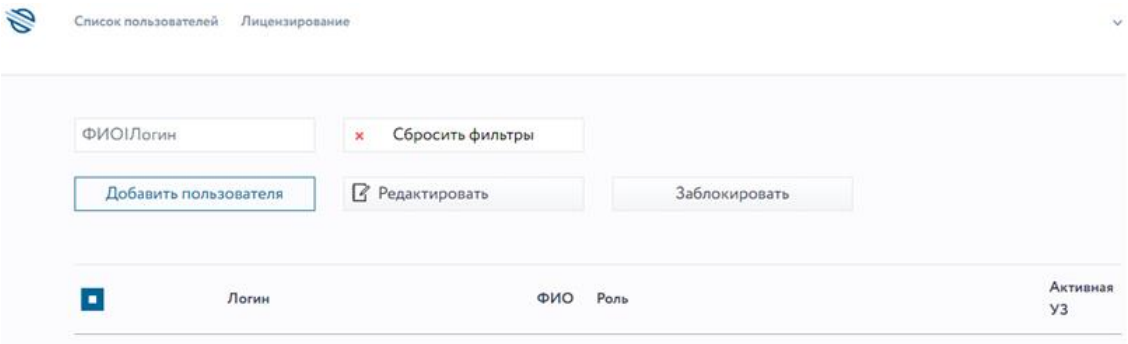


Рисунок 5. Главная страница веб-интерфейса

3 В группе **Новая лицензия** нажмите кнопку **Добавить файл** и выберите файл лицензии ПО TrustGate (`*.itcslic`) или перенесите нужный файл в область, выделенную пунктирной линией.

Рисунок 6. Добавление файла лицензии

4 Дождитесь загрузки файла лицензии на сервер TrustGate.

Когда лицензия будет загружена, в таблице **Лицензия** вы увидите ее параметры.

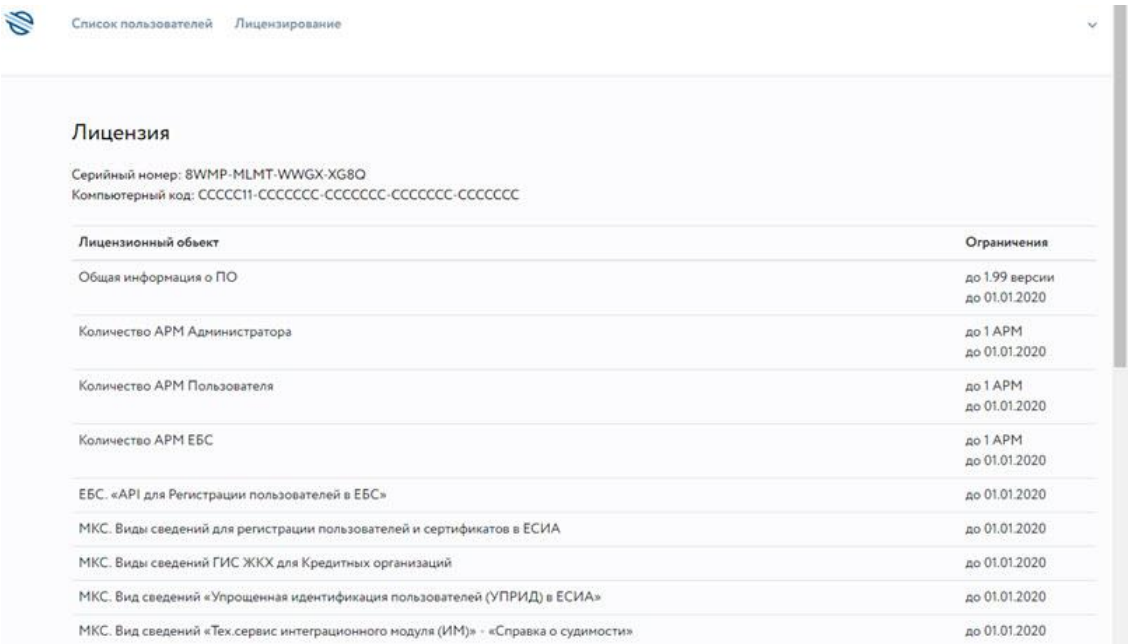


Рисунок 7. Просмотр данных лицензии

5 Запросите код регистрации лицензии. Для этого отправьте письмо на электронную почту —. В содержании письма укажите серийный номер лицензии и компьютерный код (код сервера TrustGate).

Примечание. Серийный номер лицензии и компьютерный код отображаются в таблице **Лицензия**.

Компьютерный код вычисляется автоматически в зависимости от конфигурации компьютера.

---

6 Дождитесь письма с кодом регистрации лицензии.

7 В таблице **Список лицензий** в столбце **Регистрационный код** щелкните ссылку **Регистрация**, введите код, полученный в письме, и нажмите кнопку **Сохранить**.

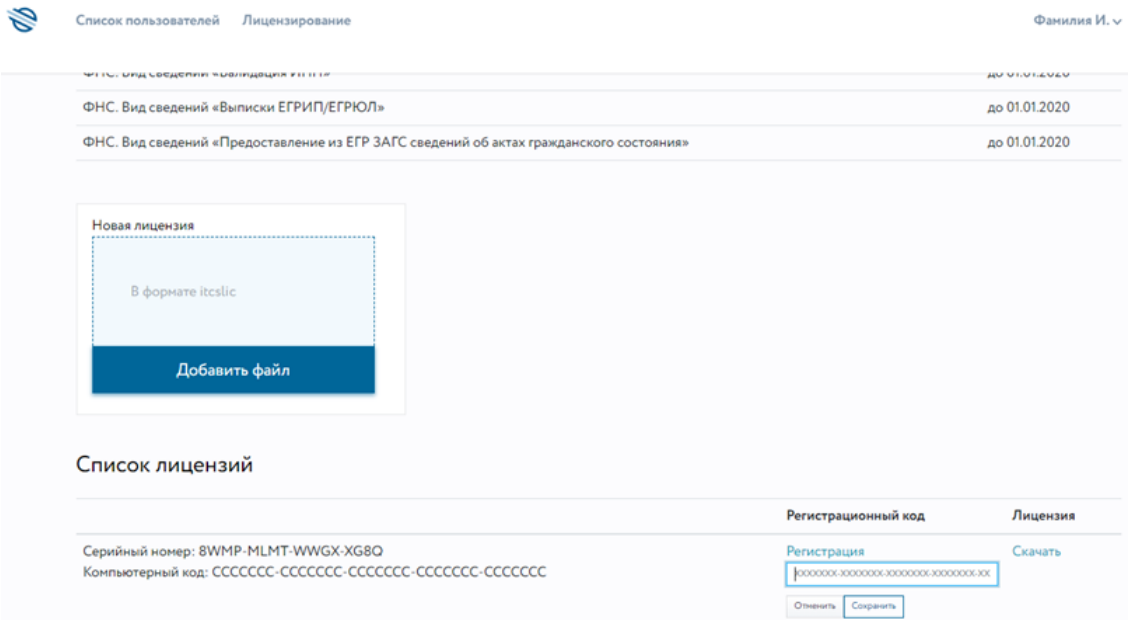


Рисунок 8. Регистрация лицензии

Код регистрации лицензии отобразится в столбце **Регистрационный код**.

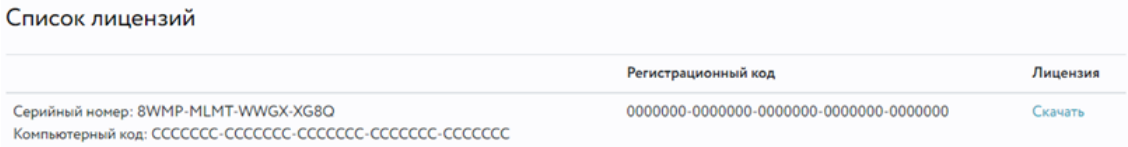


Рисунок 9. Лицензия зарегистрирована

Если срок действия основной лицензии истек или вы решили расширить возможности текущей лицензии, обновите лицензию (см. Обновление лицензии TrustGate на стр. 40).

Создание учетной записи персонала

Для первичной настройки и дальнейшего администрирования ПО TrustGate создайте пользователя с полными правами на работу с ПО TrustGate - персонал (см. Структура и ролевая модель TrustGate на стр. 7). Для этого выполните следующие действия:

1 Войдите в веб-интерфейс АРМ администратора с использованием учетной записи администратора (см. Аутентификация в веб-интерфейсе АРМ администратора на стр. 15).

2 На главной странице веб-интерфейса нажмите кнопку **Добавить пользователя**.

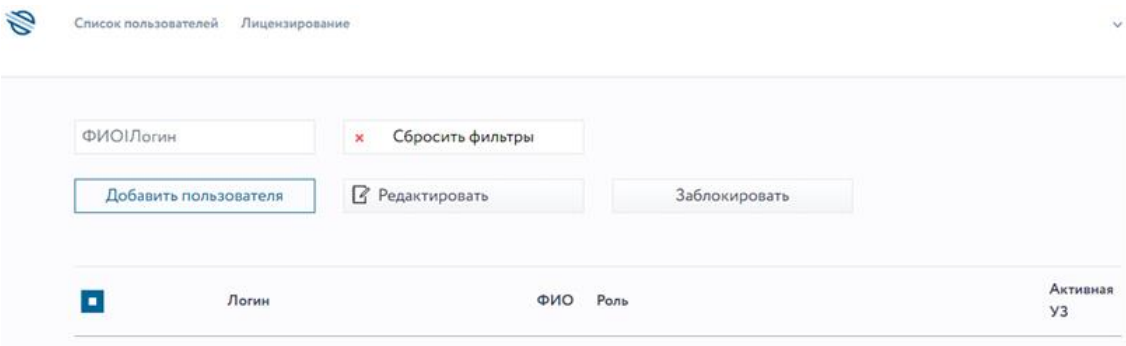


Рисунок 10. Создание учетной записи персонала

3 На странице **Создать пользователя** заполните следующие поля:

- **Логин и пароль** — параметры учетной записи для последующей идентификации пользователя в веб-интерфейсе АРМ администратора TrustGate.

Внимание! Пароль должен удовлетворять следующим требованиям:

- Пароль должен включать цифры и буквы.
- При создании пароля можно использовать только цифры, буквы латинского алфавита и специальные символы.
- Длина пароля — не менее 16 символов.

- **Фамилия**, **Имя** и **Отчество** — ФИО пользователя указываются при необходимости.
- Чтобы на время отключить учетную запись пользователя, снимите флажок **Активен**.
- Нажмите кнопку **Сохранить**.

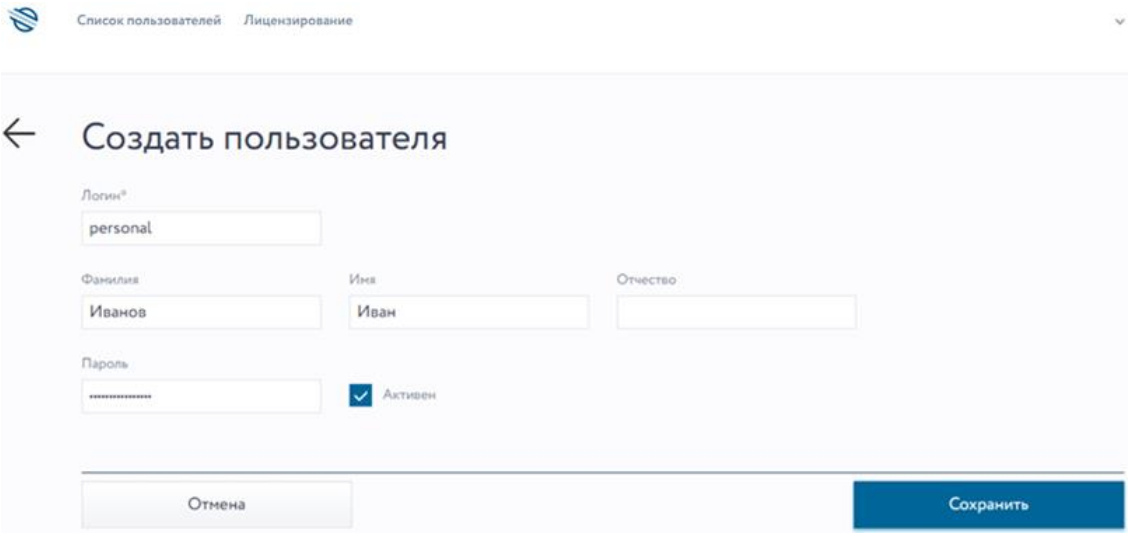


Рисунок 11. Заполнение параметров нового пользователя

Примечание. Все пользователи, которые создаются администратором, имеют полные права на работу с ПО TrustGate (роль «Персонал»).

После создания учетная запись пользователя доступна в разделе **Список пользователей**.

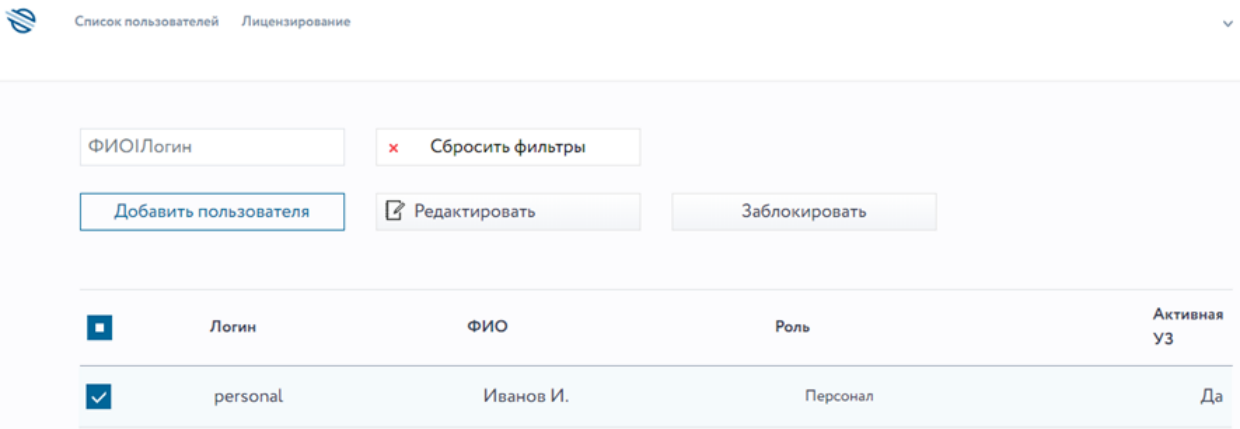


Рисунок 12. Список учетных записей персонала

Добавление организаций

Для взаимодействия со СМЭВ необходимо создать организацию, от имени которой будут формироваться исходящие запросы.

Организация — это та компания, которая использует ПО TrustGate для оказания услуг населению. Если организация имеет разветвленную структуру, добавьте все филиалы, которые будут работать с ПО.

Чтобы создать организацию, выполните следующие действия:

1 Войдите в веб-интерфейс АРМ администратора с использованием учетной записи персонала (см. Аутентификация в веб-интерфейсе АРМ администратора на стр. 15).

2 На главной странице веб-интерфейса выберите раздел **Список организаций**.

3 На странице **Список организаций** нажмите кнопку **Добавить организацию**.

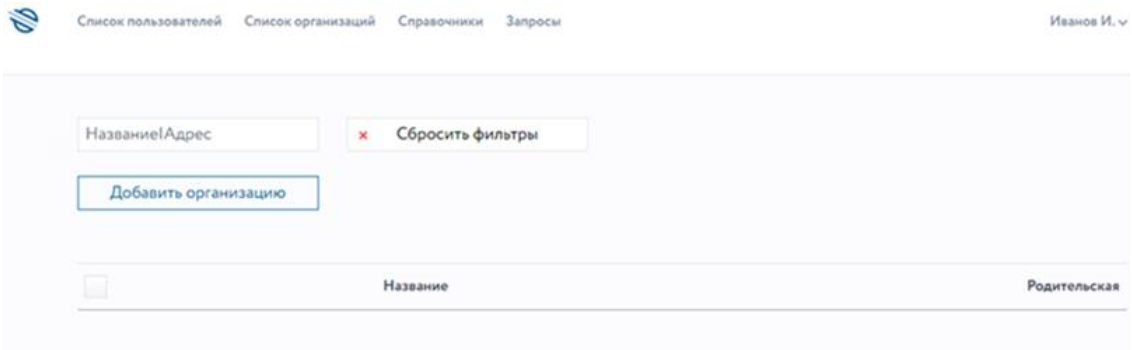


Рисунок 13. Создание организации

4 На странице **Добавить организацию** заполните следующие поля:

- **Родительская организация**. Может быть указана, если добавляемая организация является филиалом созданной ранее организации.

- **Название организации**. Информация используется для вывода в печатных формах.
- **Адрес** — юридический адрес организации. Информация используется для вывода в печатных формах.

5 На странице **Добавить организацию** создайте список запросов, которые будут отправляться от имени организации.

Чтобы выбрать запрос, дважды щелкните пункт в списке **Список доступных сервисов**. Запрос будет перенесен в список **Список выбранных сервисов**.

Чтобы удалить выбранный запрос, дважды щелкните пункт в списке **Список выбранных сервисов**. Запрос будет перенесен обратно в список **Список доступных сервисов**.

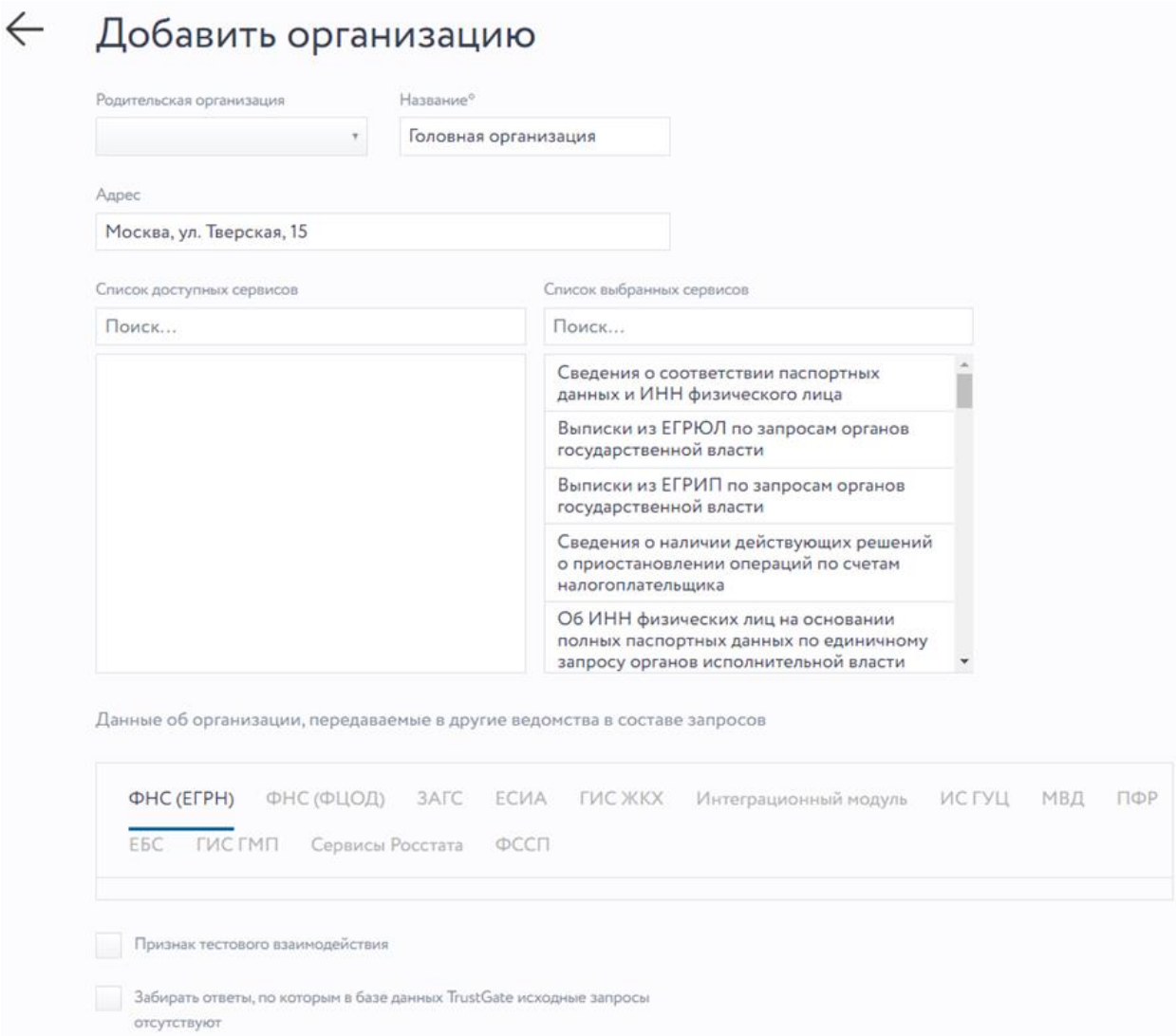


Рисунок 14: Заполнение параметров новой организации

6 На странице **Добавить организацию** в группе **Данные об организации, передаваемые в другие ведомства в составе запроса** укажите информацию, необходимую для отправки запросов.

Примечание. В случае если указана родительская организация, ее данные для запросов автоматически подставятся для новой организации.

При необходимости вы можете вручную прописать данные подчиненной организации для запросов. В этом случае они будут иметь приоритет над данными родительской организации.

Для всех запросов обязательно укажите следующую информацию:

- **Адрес в СМЭВ3** — адрес электронного сервиса продуктивного контура СМЭВ3.
- **Мнемоника** — мнемоника точки подключения к СМЭВ (см. глоссарий, стр. 47).
- **Сертификат** организации, от имени которой отправляются запросы в СМЭВ.

Остальные данные и необходимость их заполнения будут зависеть от выбранных для организации запросов

Флажок **Признак тестового взаимодействия** необходим только в случае отладки. При работе в продуктивном контуре снимите его.

Флажок **Забирать ответы, по которым в базе данных TrustGate исходные запросы отсутствуют** следует устанавливать, когда необходимо получать ответы на запросы, которые были удалены после отправки.

7 Нажмите кнопку **Сохранить**.

После создания организация доступна в разделе **Список организаций**.

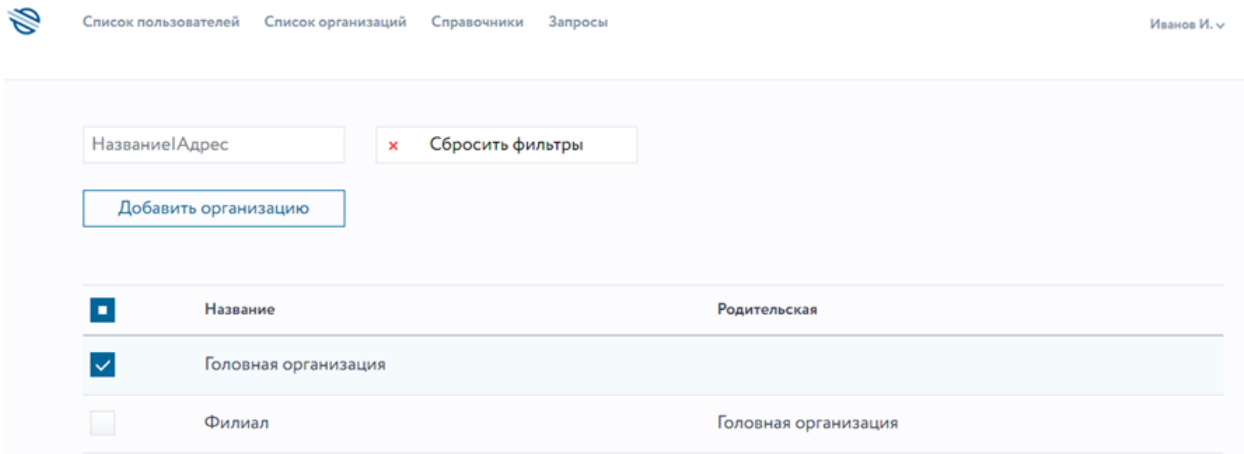


Рисунок 15. Список организаций

Настройки организации для отправки запросов в ЕСИА

Если для организации выбраны сервисы Единой системы идентификации и аутентификации — ЕСИА, в параметрах организации в группе **Данные об организации, передаваемые в другие ведомства в составе запроса** появляется вкладка **ЕСИА.**

Здесь, помимо обязательных для всех запросов данных, укажите **Код маршрутизации на ЕСИА среду**. Код выбирается из предустановленного справочника.

Внимание! Для работы с продуктивным контуром СМЭВ следует выбрать значение — **PROD**.

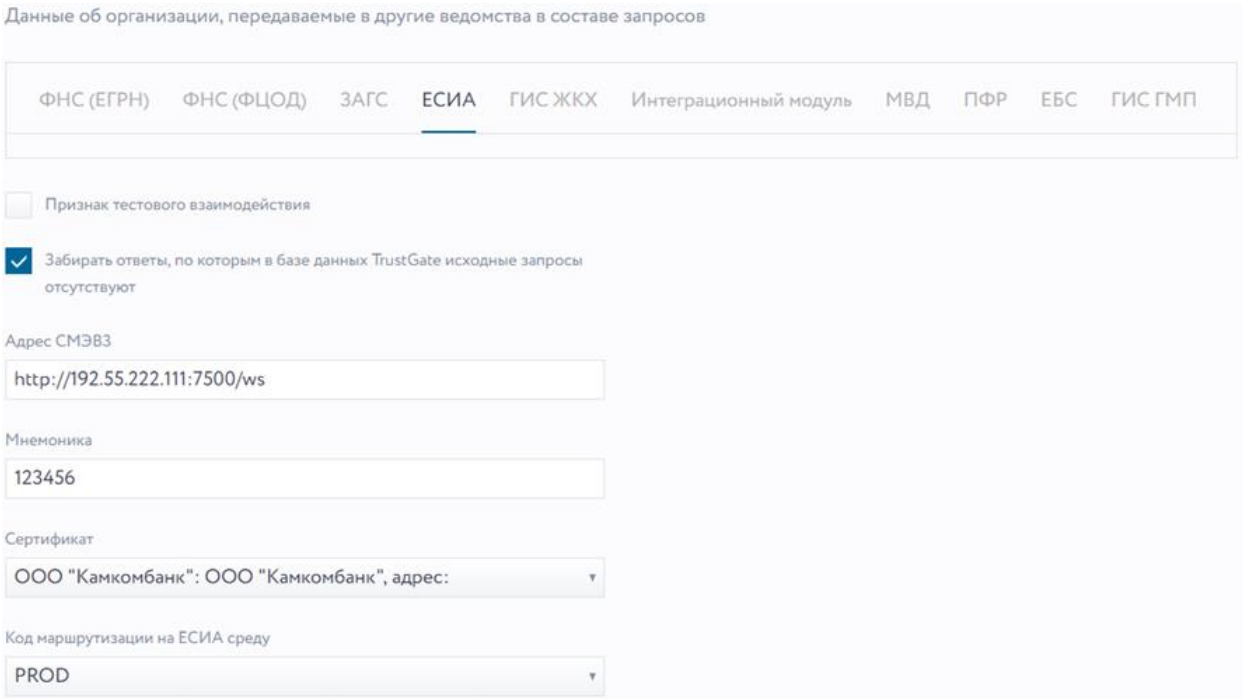


Рисунок 166. Ввод данных организации для отправки запросов в ЕСИА

Создание учетной записи оператора

Для формирования и отправки запросов в государственные и муниципальные организации создайте пользователя с ограниченными правами на работу с ПО TrustGate — оператора (см. Структура и ролевая модель TrustGate на стр. 7).

Чтобы создать учетную запись оператора, выполните следующие действия:

1. Войдите в веб-интерфейс АРМ администратора с использованием учетной записи персонала (см. Аутентификация в веб-интерфейсе АРМ администратора на стр. 15).
2. На главной странице веб-интерфейса нажмите кнопку **Добавить пользователя**.

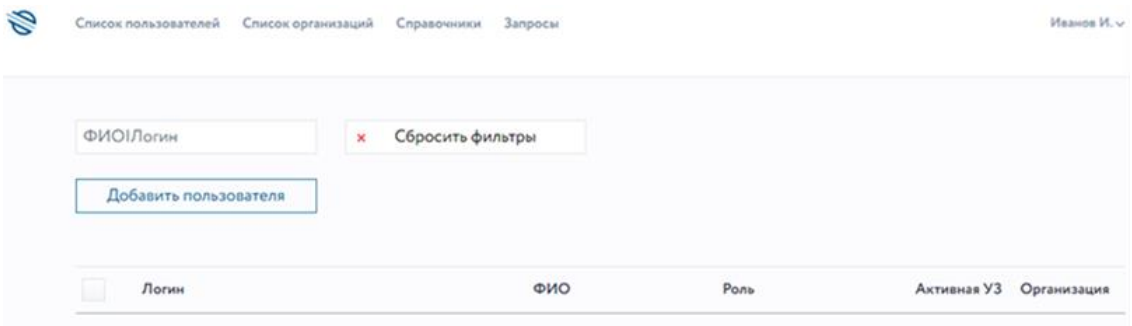


Рисунок17. Создание учетной записи оператора

3 На странице **Создать пользователя** заполните следующие поля:

- **Организация**.

  Пользователю будут доступны все сервисы, назначенные выбранной организации (см. Добавление организаций на стр. 23).

- **Логин и пароль —** параметры учетной записи для последующей идентификации пользователя в веб-интерфейсе АРМ оператора.
- **Фамилия**, **Имя** и **Отчество.** Информация используется для вывода в печатных формах.
- Чтобы на время отключить учетную запись пользователя, снимите флажок **Активен**.

4 На странице **Создать пользователя** вы можете выбрать для пользователю любые сервисы, назначенные организации, к которой он относится (см. Добавление организаций на стр. 23).

Чтобы выбрать запрос, дважды щелкните пункт в списке **Список доступных сервисов**. Запрос будет перенесен в список **Список выбранных сервисов**.

Чтобы удалить выбранный запрос, дважды щелкните пункт в списке **Список выбранных сервисов**. Запрос будет перенесен обратно в список **Список доступных сервисов**.

5 На странице **Создать пользователя** вы можете назначить пользователю дополнительные права на работу с ПО TrustGate:

- **Глава подразделения** — оператор с этими правами сможет просматривать запросы всех операторов той организации, к которой принадлежит сам.

  Примечание. Если оператор принадлежит к организации, у которой существует подчиненная организация, то он, помимо своих запросов, может просматривать запросы всех операторов подчиненной организации.

- **Обработка задач** - оператор с этими правами сможет брать в работу любые задачи, в которых он указан в качестве исполнителя.

  Примечание. Если оператору назначены права **Глава подразделения**, то ему доступны задачи как своего подразделения, так и подчиненных.

- **Создание операции по идентификации ЕСИА** - оператор с этими правами сможет создавать операции по идентификации ЕСИА.

- **Просмотр операций по идентификации ЕСИА** - оператор с этими правами сможет просматривать результат идентификации ЕСИА, включая историю выполнения операций по идентификации.
- **Удаление запросов —** оператор с этими правами сможет удалить любой свой запрос.

> **Примечание**. Если оператор принадлежит к организации, у которой существует подчиненная организация, то ему также доступно удаление запросов всех операторов подчиненной организации.
>
> Если оператору назначены права **Глава подразделения**, то он может удалять запросы всех операторов той организации, к которой принадлежит сам.

Удаление запроса очищает всю информацию о нем (без возможности восстановления).

Если был удален запрос в статусе **Ожидание ответа**, то ответ на него получен не будет. Чтобы получать ответы на удаленные запросы, в параметрах организации установите флажок **Забирать ответы, по которым в базе данных TrustGate исходные запросы отсутствуют (см.** Добавление организаций **на стр. 23).**

- **Ожидание ответа от остановленных** — оператор с этими правами сможет перевести запрос, который не был обработан СМЭВ из-за ошибки, в статус **Ожидание ответа**. В этом статусе запрос будет обработан СМЭВ сразу, как только ошибка будет устранена.
- **Создание выгрузки «Вложения в запросах»** - оператор с этими правами сможет выгружать файлы, прикрепленные к запросам.

Чтобы назначить права, дважды щелкните пункт в списке **Список прав**. Права будут перенесены в список **Список выбранных прав**.

Чтобы убрать назначенные права, дважды щелкните пункт в списке **Список выбранных прав**. Права будут перенесены обратно в список **Список прав.**

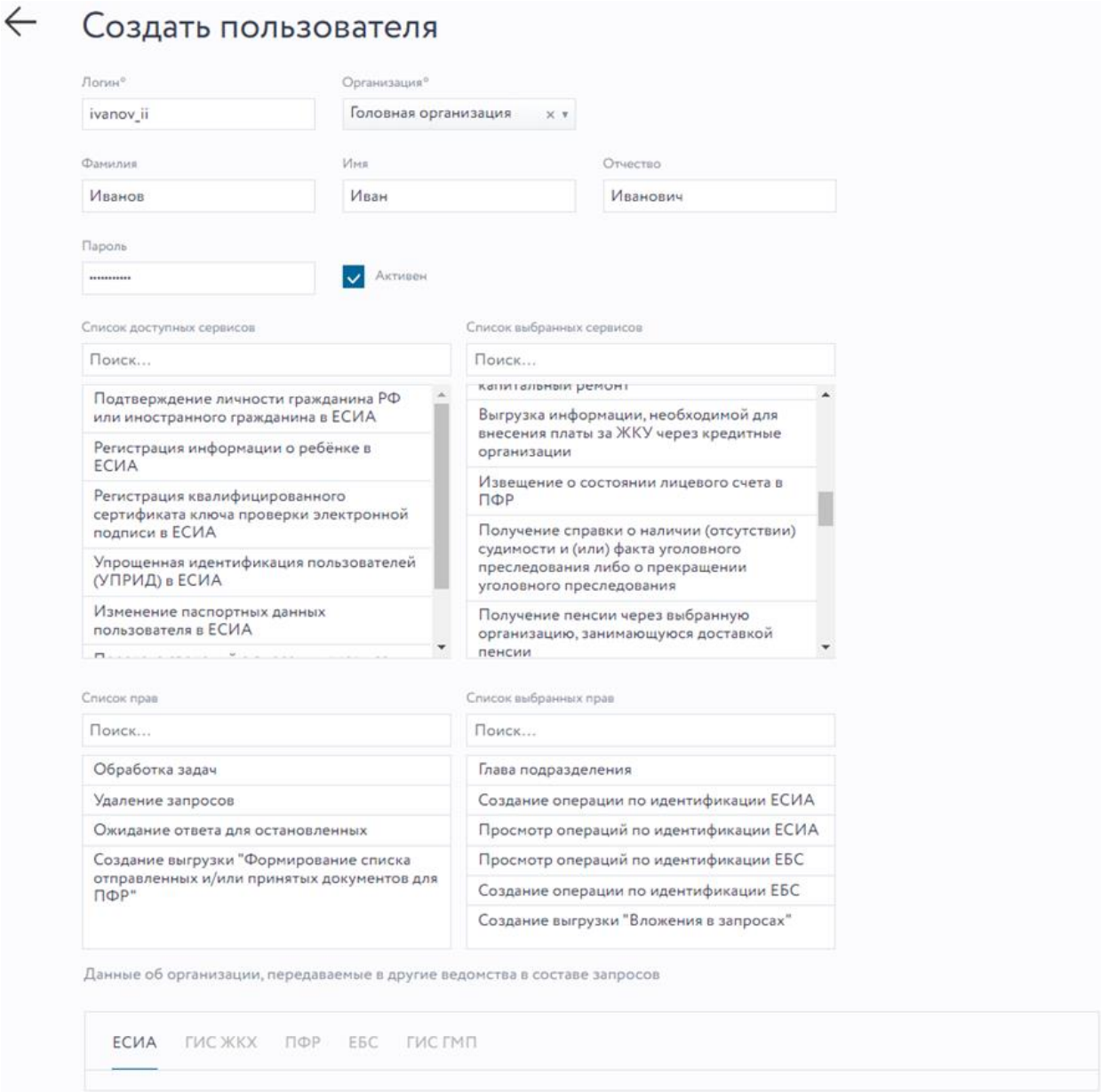


Рисунок18. Заполнение параметров нового оператора

6 На странице **Создать пользователя** в группе **Данные об организации, передаваемые в другие ведомства в составе запроса** укажите информацию, необходимую для отправки запросов с использованием учетной записи этого оператора.

Состав передаваемых об операторе данных и настройки файловой интеграции зависят от сервисов, выбранных для организации, к которой принадлежит оператор.

7 Нажмите кнопку **Сохранить**.

Примечание. Все пользователи, которые создаются персоналом, имеют ограниченные права на работу с ПО TrustGate (роль «Оператор»).

После создания учетная запись пользователя доступна в разделе **Список пользователей**.

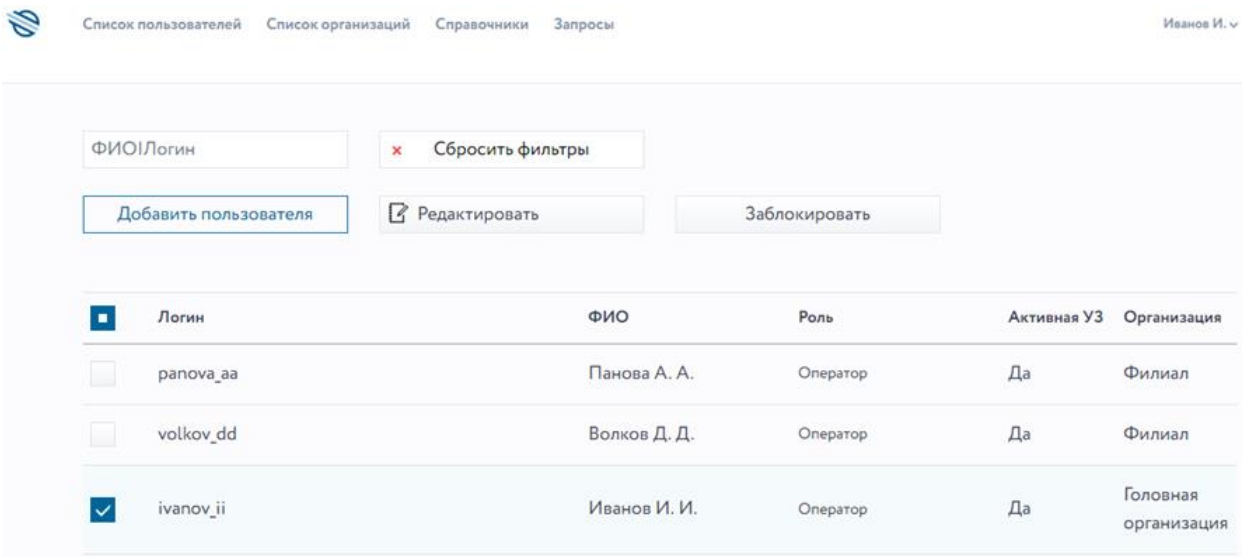


Рисунок 19. Список учетных записей операторов

Настройки пользователя для отправки запросов в ЕСИА

Если оператор принадлежит к организации, которая взаимодействует с Единой системой идентификации и аутентификации — ЕСИА, в параметрах пользователя в группе **Данные об организации, передаваемые в другие ведомства в составе запроса** появляется вкладка **ЕСИА** со следующими полями:

- **СНИЛС оператора центра обслуживания.**
- **Идентификатор центра обслуживания.**

Заполните данные поля, если оператор будет отправлять в ЕСИА следующие запросы:

- Восстановление доступа к подтвержденной учетной записи в ЕСИА с выдачей пароля для входа.
- Подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА.
- Подтверждение учётной записи в ЕСИА, созданной на основе существующей упрощённой.
- Поиск учетной записи в ЕСИА.
- Регистрация информации о ребёнке в ЕСИА.
- Регистрация подтвержденной учетной записи в ЕСИА с отправкой пароля для первого входа в систему на контактные данные.
- Удаление учетной записи в ЕСИА.

Данные поля необязательны для заполнения, если оператор будет отправлять в ЕСИА следующие запросы:

- Регистрация квалифицированного сертификата ключа проверки электронной подписи в ЕСИА.
- Упрощенная идентификация пользователей (УПРИД) в ЕСИА.

Настройка файловой интеграции

Для настройки файловой интеграции с сервером TrustGate вы можете использовать любой клиент, который поддерживает протокол передачи FTP.

Чтобы настроить файловую интеграцию, укажите в настройках FTP-клиента:

- **Протокол передачи** — FTP.
- **Шифрование** — Без шифрования.
- **Имя хоста** — адрес сервера TrustGate.
- **Номер порта** — 21 (используется по умолчанию).
- **Имя пользователя и пароль** — параметры учетной записи оператора TrustGate.

Обновление TrustGate

Обновление ПО TrustGate выполняет администратор операционной системы (root) после получения информационного письма от ОАО «ИнфоТеКС Интернет Траст» о выходе новой версии.

ПО обновляется только локально, новая версия устанавливается без предварительного удаления прежней версии.

Перед началом обновления:

- Убедитесь, что на сервере установлена старая версия ПО TrustGate.

  Чтобы узнать установленную у вас версию ПО, введите в адресной строке браузера `<host>/api/version`, где `<host>` — это адрес сервера TrustGate.

  На открывшейся странице вы увидите номер версии ПО и номер сборки.

- Убедитесь, что у вас есть установочный файл новой версии — `g2g_ng_dist-<номер сборки>.zip`.

Чтобы обновить ПО TrustGate, выполните следующие действия:

1 Распакуйте дистрибутив новой версии в каталог дистрибутива ПО TrustGate с помощью команды:

```
hostname# unzip -x g2g_ng_dist-<номер сборки>.zip
```

2 Чтобы заменить все текущие файлы в каталоге, после вопроса `Replace <наименование файла>?` введите символ `A`.

3 Запустите процесс обновления ПО TrustGate с помощью команды:

```
hostname# sudo python install.py -v
```

4 Чтобы подтвердить свое согласие на создание кластера, после вопроса `Need create cluster?` введите символ `y`.

5 Чтобы подтвердить свое согласие на формирование SSL-сертификата, после вопроса `Create SSL crt?` введите символ `y`.

   При необходимости укажите запрашиваемую информацию об организации и нажмите клавишу **Enter**. SSL-сертификат будет сформирован в любом случае — ввели вы данные организации или нет.

   Дождитесь завершения процесса создания сертификата.

Примечание. SSL-сертификат обеспечивает защищенное соединение между АРМ оператора и сервером TrustGate. Обязательно сформируйте сертификат, если организация будет отправляет запросы в ЕБС.

Если SSL-сертификат был сформирован ранее, этот шаг будет пропущен.

---

6 Чтобы указать адрес прокси-сервера, после вопроса `Has proxy server?` введите символ `y`.

Адрес сервера имеет вид `http://<host>:<port>`, где `host` — это адрес прокси-сервера, `port` — номер порта, через который работает сервер.

7 Чтобы создать учетную запись администратора:

- Введите имя учетной записи (`Input admin username`).
- Введите пароль (`Input admin password`).
- Нажмите клавишу **Enter**.

Внимание! Если вы отменили создание учетной записи, то для ее повторного формирования выполните команду:

```
hostname# docker exec -it g2g_web_1 python manage.py createsuperuser
```

---

8 Чтобы установить систему мониторинга, после вопроса `Install netdata for monitoring system?` введите символ `y`.

Примечание. В ПО TrustGate включена система мониторинга Netdata.

Для отслеживания состояния работоспособности ПО в адресной строке браузера введите `http://<host>:19999`, где `host` — адрес сервера TrustGate.

---

9 Дождитесь завершения процесса обновления. После обновления сервер будет автоматически перезагружен.

В результате ПО TrustGate будет обновлено на новую версию. Информация о процессах, происходящих при обновлении, записывается в файл `install.log`, расположенный в каталоге `/var/log/trust_gate/`.

После того, как процесс обновления ПО TrustGate будет завершен, произведите проверку работоспособности ПО (см. Проверка работоспособности TrustGate на стр. 34).

Проверка работоспособности TrustGate

Для проверки работоспособности ПО TrustGate после первичной настройки и обновления выполните действия, перечисленные ниже:

1. Чтобы проверить настройки файловой интеграции, войдите на сервер TrustGate через настроенный FTP-клиент. Для входа используйте учетную запись оператора TrustGate.
2. Чтобы проверить отправку запросов в СМЭВ, войдите в веб-интерфейс TrustGate с использованием учетной записи оператора. Создайте запрос (нажмите кнопку **Новый запрос**) и отправьте его в СМЭВ.
3. Чтобы проверить функционал поиска запросов, отправьте запрос в СМЭВ. Когда статус запроса изменится на статус **Ожидание отправки,** выберите пункт **Расширенный поиск** на панели инструментов.
4. Чтобы проверить поиск по базе ФИАС, создайте новый запрос и начните вводить адрес в строке **Поиск по базе адресов**.

2

Администрирование TrustGate

Резервное копирование базы данных TrustGate

Резервное копирование базы данных TrustGate выполняет администратор операционной системы (root).

Для надежного хранения данных выполняйте резервное копирование базы не реже одного раза в день. При этом храните на сервере копии базы за три последних дня и три последних месяца (по одной копии за день и за месяц).

Чтобы создать резервную копию базы, выполните следующие действия:

1 Перейдите в каталог, который содержит распакованный дистрибутив ПО TrustGate, при помощи команды:

```
hostname# cd <каталог дистрибутива>
```

2 Запустите процесс резервного копирования базы:

- Чтобы сохранить файл с резервной копией базы в текущий каталог, выполните команду:

  ```
  hostname# sudo python dump.py -v
  ```

  В результате будет создан файл — `dump.tar.bz`.

  > **Примечание.** При последующем резервном копировании базы TrustGate информация в файле будет перезаписана. Чтобы сохранить предыдущую копию базы, переименуйте текущий файл с резервной копией.
  >
  > Новая копия будет сохранена в файл — `dump.tar.bz`.

- Чтобы сохранить файл с резервной копией базы в другой каталог, выполните команду:

  ```
  hostname# sudo python dump.py -v -p <каталог, в который будет сохранен
  файл/имя файла.tar.bz>
  ```

3 Дождитесь завершения процесса создания резервной копии.

В процессе копирования создается полная копия имеющейся на сервере информации, что может занять продолжительное время. Длительность копирования зависит от количества и состава данных.

> **Совет.** Планируйте работы по созданию копии базы заранее.
>
> Рекомендуем делать резервное копирование в моменты малой нагрузки на сервер и по возможности ограничить работу операторов с базой TrustGate на время создания копии.

В результате будет создан файл с резервной копией базы данных TrustGate. Информация о процессах, происходящих при резервном копировании, записывается в файл `dump.log`, расположенный в каталоге `/var/log/trust_gate/`.

Вы можете настроить автоматическое резервное копирование по расписанию через файл заданий `crontab`. Для этого выполните следующие действия:

1. Создайте файл `crontab` при помощи команды:

   ```
   hostname# crontab -e
   ```

2. Укажите в файле команду: `1 2 3 4 5 cd <каталог дистрибутива ПО TrustGate> && python dump.py -v`

   Где `1` — это минута, `2` — час, `3` — день месяца, `4` — месяц и `5` — день недели, когда будет запускаться процесс копирования базы данных TrustGate.

Рекомендуем добавить в скрипт команды для переименования текущего файла с резервной копией (по умолчанию он перезаписывается) и для удаления ненужных копий.

Восстановление базы данных TrustGate из копии

Восстановление базы данных TrustGate из резервной копии выполняет администратор операционной системы (root).

Чтобы восстановить базу данных TrustGate, выполните следующие действия:

1. Перейдите в каталог, который содержит распакованный дистрибутив ПО TrustGate, при помощи команды:

   ```
   hostname# cd <каталог дистрибутива>
   ```

2. Запустите процесс восстановления данных:

   - Если файл с резервной копией находится в текущем каталоге, выполните команду:

     ```
     hostname# sudo python dump.py -v -l 1
     ```

     Примечание. По умолчанию база восстанавливается из файла `dump.tar.bz`.

     Если в каталоге хранится несколько файлов с резервной копией, и вы хотите восстановить базу из другой копии, выполните команду:

     ```
     hostname# sudo python dump.py -v -p <имя файла.tar.bz> -l 1
     ```

   - Если файл с резервной копией находится в другом каталоге, выполните команду:

     ```
     hostname# sudo python dump.py -v -p <каталог файла/имя файла.tar.bz> -l 1
     ```

В результате текущая база данных TrustGate будет заменена резервной копией. Информация о процессах, происходящих при восстановлении базы из копии, записывается в файл `dump.log`, расположенный в каталоге `/var/log/trust_gate/`.

Изменение параметров криптопровайдера

В процессе эксплуатации ПО TrustGate могут измениться параметры криптопровайдера, которые были указаны в файле `config.json` в процессе установки ПО на сервер (см. Установка TrustGate на стр. 10):

- Если ПО TrustGate эксплуатируется совместно с программой ViPNet CSP, может измениться путь или пароль к контейнеру ключей, появиться новый контейнер или устареть текущий.
- Если ПО TrustGate эксплуатируется совместно с ПАК ViPNet PKI Service, может измениться адрес ПАКа, добавиться новая учетная запись пользователя или устареть текущая.

Все эти изменения должны быть обязательно отражены в файле `config.json`.

Чтобы изменить json-файл, выполните следующие действия:

1. Перейдите в каталог, который содержит распакованный дистрибутив ПО TrustGate, при помощи команды:

   ```
   hostname# cd <каталог дистрибутива>
   ```

2. Перейдите в каталог, в который после установки ПО TrustGate был автоматически перезаписан файл `config.json` из каталога `libs/containers`, с помощью команды:

   ```
   hostname# cd opt/itcs/bin
   ```

3. Внесите в файл необходимые изменения.
4. Чтобы применить изменения, выполните команду:

   ```
   hostname# sudo systemctl restart iit_signer
   ```

Внимание! При обновлении ПО TrustGate на новую версию json-файл, расположенный в каталоге `opt/itcs/bin`, автоматически перезаписывается данными файла `config.json` из каталога `libs/containers`.

Настройка сценария идентификации в ЕСИА

Внимание! Для работы сценария требуется дополнительная лицензия. Без лицензии вы сможете настроить сценарий, но не сможете его использовать.

Чтобы оператор смог работать со сценарием, назначьте ему следующие права:

- Создание операции по идентификации ЕСИА.

Для настройки сценария удаленной идентификации клиентов в ЕСИА:

1. Войдите в веб-интерфейс АРМ администратора с использованием учетной записи персонала (см. Аутентификация в веб-интерфейсе АРМ администратора на стр. 15).
2. На главной странице веб-интерфейса выберите раздел **Справочники**.
3. В блоке **Настройки сценариев в строке Идентификация в ЕСИА (ЕБС)** щелкните ссылку **Редактировать** и обязательно заполните следующие параметры:
   - **Адрес в ЕСИА для авторизации** — https://esia.gosuslugi.ru.
   - **Доступ к сервисам получения персональных данных клиента ЕСИА** — https://172.16.104.200.
   - **Сертификат организации**, от имени которой будет отправляться запрос на идентификацию.
   - **Идентификатор системы-клиента**, который организация использует для подключения своей информационной системы к ЕСИА.
   - **Ссылка, по которой будет направляться пользователь после того, как даст разрешение на доступ к ресурсу**.
4. В блок **Файл сертификата** добавьте файл сертификата для проверки ЭП под маркером. Для этого:
   - **4.1** Загрузите файл сертификата по ссылке.
   - **4.2** Нажмите кнопку **Добавить файл** и выберите файл сертификата или перенесите файл в область, выделенную пунктирной линией.

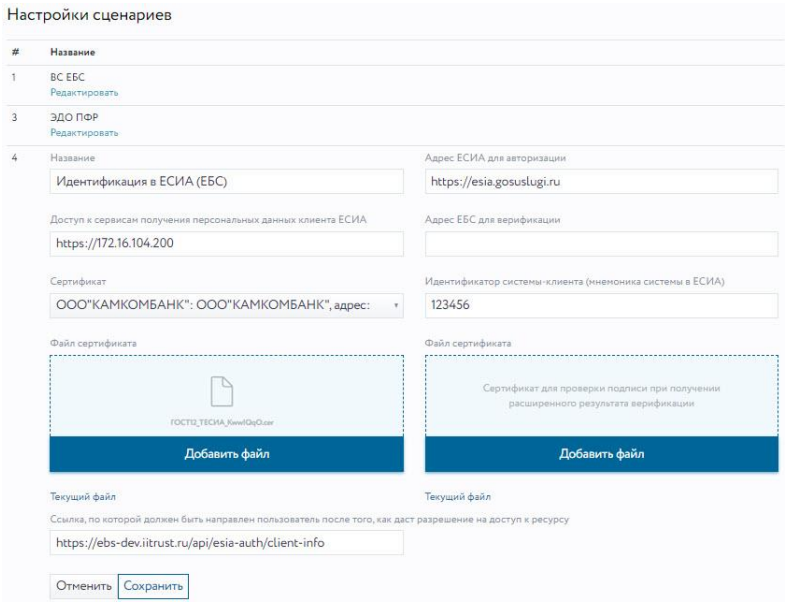


Рисунок 20. Настройка сценария идентификации в ЕСИА

Просмотр параметров запросов

В веб-интерфейсе АРМ администратора TrustGate вы можете получить подробную информацию о всех запросах, которые были сформированы операторами.

Для просмотра параметров запросов выполните следующие действия:

1 Войдите в веб-интерфейс АРМ администратора с использованием учетной записи персонала На главной странице веб-интерфейса выберите раздел **Запросы**.

2 Информация о запросах операторов будет отображена в таблице. Используйте поля фильтрации на панели инструментов для быстрого поиска конкретного запроса.

   Вы можете отфильтровать запросы по следующим параметрам:

   - **Тип запроса**.
   - **Статус запроса** — текущий статус запроса.
   - **Исполнитель** — оператор, с использованием учетной записи которого был сформирован запрос.

     Примечание. Тип, статус запроса и исполнитель выбираются из предустановленных справочников. Чтобы быстро найти нужное значение, воспользуйтесь строкой **Поиск**. Начните вводить наименование значения, справочник будет автоматически отфильтрован по тексту в поисковой строке.

   - **Период** — временной диапазон, в который был создан запрос.

     Вы можете выбрать один из предустановленных периодов (**День**, **Вчера**, **Неделя**, **Месяц**, **Год**) или указать конкретный диапазон дат.

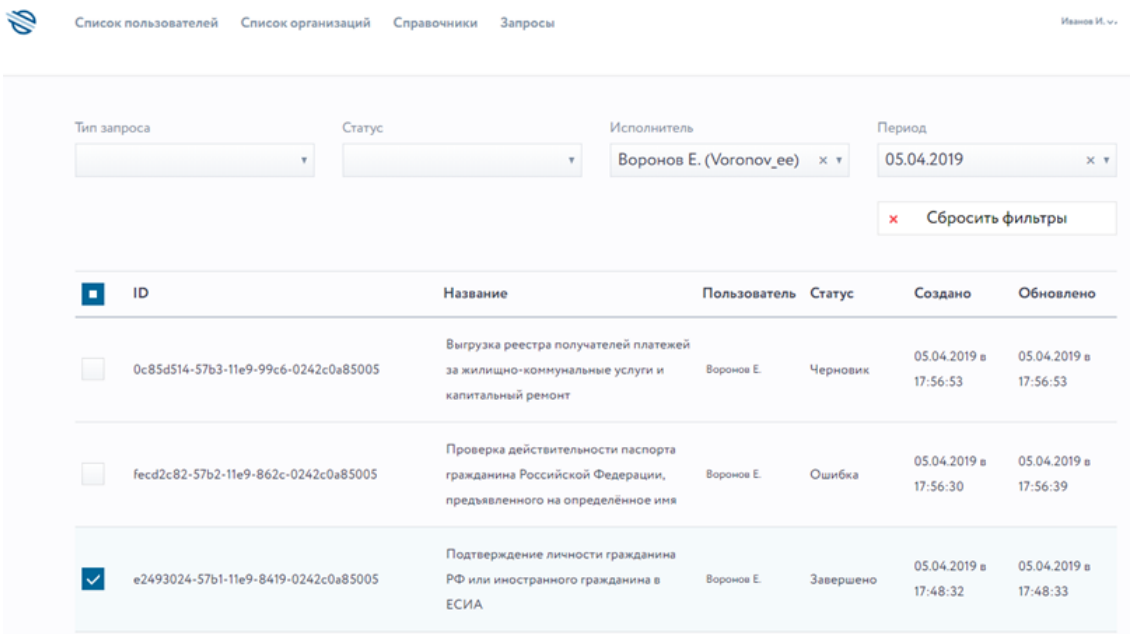
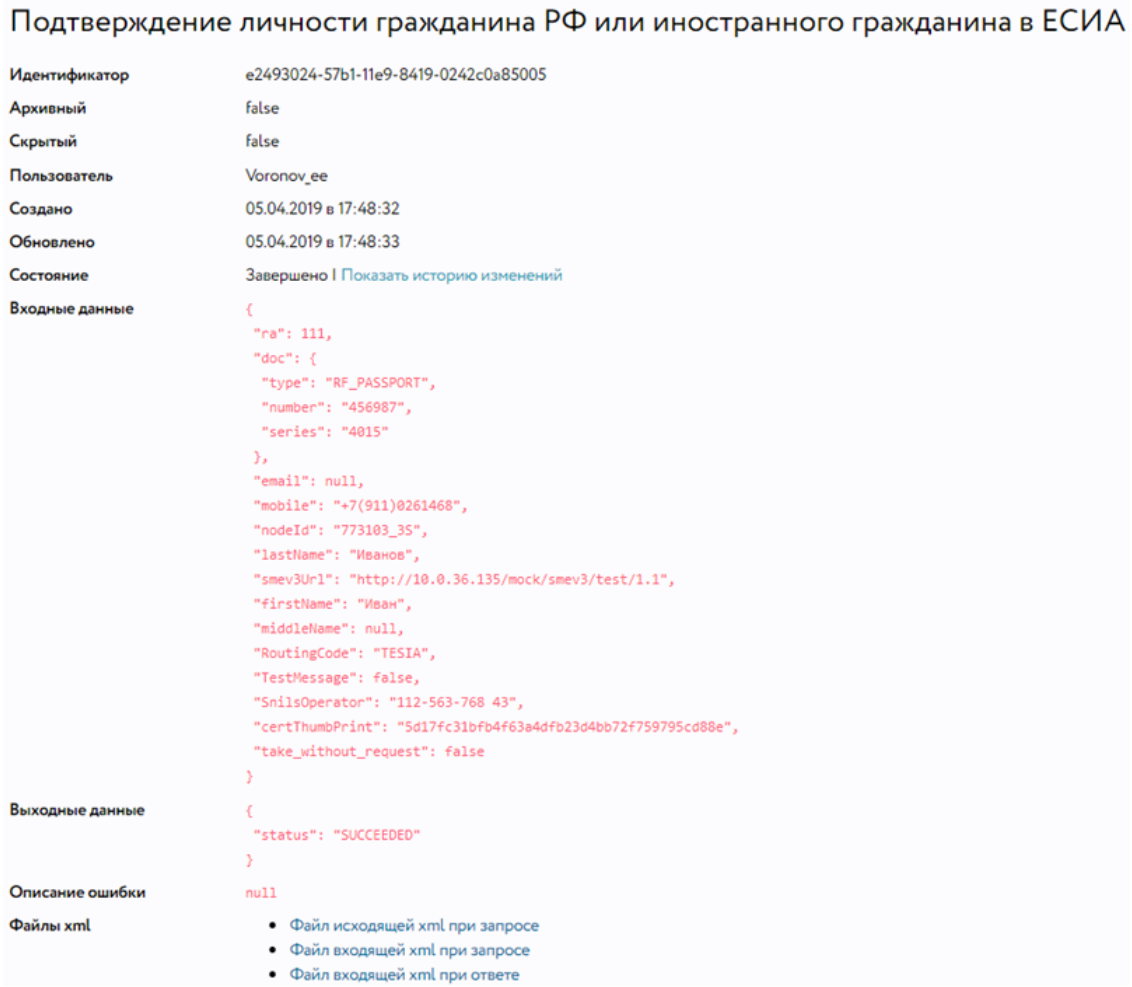


Рисунок 21. Список запросов

3 Чтобы открыть запрос, дважды щелкните его.



Подтверждение личности гражданина РФ или иностранного гражданина в ЕСИА

Идентификатор	e2493024-57b1-11e9-8419-0242c0a85005
Архивный	false
Скрытый	false
Пользователь	Voronov_ee
Создано	05.04.2019 в 17:48:32
Обновлено	05.04.2019 в 17:48:33
Состояние	Завершено | Показать историю изменений
Входные данные	{ "ra": 111, "doc": { "type": "RF_PASSPORT", "number": "456987", "series": "4015" }, "email": null, "mobile": "+7(911)0261468", "nodeId": "773103_3S", "lastName": "Иванов", "smev3Url": "http://10.0.36.135/mock/smev3/test/1.1", "firstName": "Иван", "middleName": null, "RoutingCode": "TESIA", "TestMessage": false, "SnilsOperator": "112-563-768 43", "certThumbPrint": "5d17fc31bfb4f63a4dfb23d4bb72f759795cd88e", "take_without_request": false }
Выходные данные	{ "status": "SUCCEEDED" }
Описание ошибки	null
Файлы xml	• Файл исходящей xml при запросе • Файл входящей xml при запросе • Файл входящей xml при ответе

Рисунок 22. Карточка запроса

В карточке запроса содержатся его подробные параметры:

- **Идентификатор** — уникальный номер запроса, который был присвоен ему при создании.
- **Архивный** — этот параметр в значении **true** имеют только те запросы, которые были перенесены оператором в архив. Для остальных запросов выводится значение **false**.
- **Скрытый** — этот параметр в значении **true** имеют только те запросы, которые были созданы в рамках сценария ЕБС. Для остальных запросов выводится значение **false**.
- **Пользователь** — учетная запись оператора, который сформировал запрос.
- **Создано** — дата и время создания запроса.
- **Обновлено** — дата и время последнего обновления статуса запроса.
- **Состояние** — текущий статус запроса. Чтобы увидеть историю изменений статуса, щелкните ссылку **Показать историю изменений**.

Состояние	Завершено I Скрыть историю изменений			
	#	Пользователь	Из какого состояния перешли	В какое состояние перешли
	795408		wait_ack_request	complete
	795407		process_response	wait_ack_request
	795406		wait_response	process_response
	795405		wait_create_request	wait_response
	795404	Воронов Е.	created	wait_create_request

Рисунок 23. История изменений статуса запроса

- **Входные данные** — информация, которая была отправлена в СМЭВ в составе запроса.
- **Выходные данные** — информация, которая была получена из СМЭВ в составе запроса.
- **Описание ошибки** — информация об ошибке, которая возникла в процессе обработки запроса в СМЭВ.
- **Файлы xml** — файлы в формате XML, которые были сформированы при отправке запроса и получении на него ответа. Чтобы сохранить файл на компьютер, щелкните ссылку с его именем.

Ограничения при использовании учетных записей пользователей

Система TrustGate предусматривает следующие ограничения при использовании учетных записей пользователей:

1. Если пользователь не входит в систему более 90 календарных дней, то его учетная запись блокируется и авторизация пользователя становится недоступной;
2. Если для учетной записи пользователя указан срок ее действия и указанный срок действия завершен или еще не наступил, то авторизация пользователя недоступна;
3. Учетная запись оператора требует смены пароля не реже одного раза в год: если прошел один год с момента последней смены пароля, то авторизация пользователя недоступна;
4. Учетная запись персонала требует смены пароля не реже одного раза в квартал, если прошел один квартал с момента последней смены пароля, то авторизация пользователя недоступна;
5. Учетная запись администратора (создается при установке системы) требует смены пароля не реже одного раза в квартал, если прошел один квартал с момента последней смены пароля, то авторизация пользователя недоступна;
6. Если пользователем было выполнено 5 неуспешных попыток авторизации, то его учетная запись временно блокируется на 60 мин и авторизация пользователя становится недоступной;
7. Если пользователь бездействует в системе более 15 минут (не вызывает какие-либо сервисы), то его автоматически разлогинивает, при этом токен авторизации пользователя становится недействительным;
8. При каждой авторизации пользователя система выдает новый токен авторизации, старый токен авторизации становится недействительным (то есть работа пользователя на старом АРМ будет невозможной).

A

Глоссарий

ViPNet CSP

Криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей электронной подписи.

ViPNet PKI Service

ViPNet PKI Service — это программно-аппаратный комплекс, который предназначен для создания и защищенного хранения ключей электронной подписи, вычисления значения хэш-функции, формирования и проверки электронной подписи, а также для согласования ключей шифрования, вычисления имитовставки и шифрования данных при реализации защиты данных по протоколу TLS.

Удовлетворяет требованиям к средствам криптографической защиты информации класса КВ и требованиям к средствам электронной подписи класса КВ2.

ЕСИА

Единая система идентификации и аутентификации, разработчиком которой является ПАО «Ростелеком».

ЕСИА предназначена для обеспечения зарегистрированным в ней пользователям доступа к электронным ресурсам и услугам, предоставляемым на государственных порталах, без необходимости повторной регистрации. Доступ предоставляется на основе единых идентификационных параметров с использованием различных носителей: СНИЛС и пароль, электронная подпись, SIM-карта или смарт-карта.

Мнемоника точки подключения к СМЭВ

Специальный идентификатор, который организация использует для подключения своей информационной системы к СМЭВ. Этот идентификатор предоставляется участнику межведомственного электронного взаимодействия при регистрации информационной системы в Ростелекоме.

Если организация располагает собственным сервером ViPNet ЭДО Шлюз безопасности, то мнемоника точки подключения к СМЭВ организации задается непосредственно на сервере. Если же организация использует общий сервер для нескольких организаций ViPNet ЭДО Шлюз безопасности, то на каждом рабочем месте пользователя необходимо отдельно указать мнемонику точки подключения к СМЭВ организации.

СМЭВ

Федеральная государственная информационная система межведомственного взаимодействия, включающая:

- Информационные базы данных.
- Сведения об истории движения в СМЭВ запросов и ответов на запросы при предоставлении государственных и муниципальных услуг в электронном виде.
- Программные и технические средства, обеспечивающие взаимодействие организаций через СМЭВ.

СМЭВ отвечает за технологическую сторону информационного взаимодействия между организациями, предоставляющими государственные и муниципальные услуги в электронном виде.

Подробную информацию см. на сайте СМЭВ.

ФЦОД

Федеральный центр обработки данных, в котором консолидирована вся информация о налогоплательщиках (физических и юридических лицах). Отвечает за процессы, связанные с обработкой, хранением и передачей информации, а также ее аналитической обработкой.

Основная цель деятельности ФЦОД состоит в предоставлении государственным органам, физ. и юр. лицам данных из госреестров (ЕГРЮЛ, ЕГРИП, ЕГРН) на безвозмездной основе.