Руководство пользователя SafeTech CA 2.0

1. Начало работы с Личным кабинетом Пользователя

1.1. Авторизация

Для начала работы с Личным кабинетом Пользователю неообходимо перейти по адресу личного кабинета в используемом Браузере.
Браузеры доступные для работы:

- Chromium 90 (Chrome, Edge);
- Firefox 88;
- Safari 15.

Не поддерживаются браузеры:

- Edge (версия < 79);
- Internet Explorer.

В открывшейся форме (Рисунок 1) необходимо указать логин и пароль, переданные пользователю Администратором.

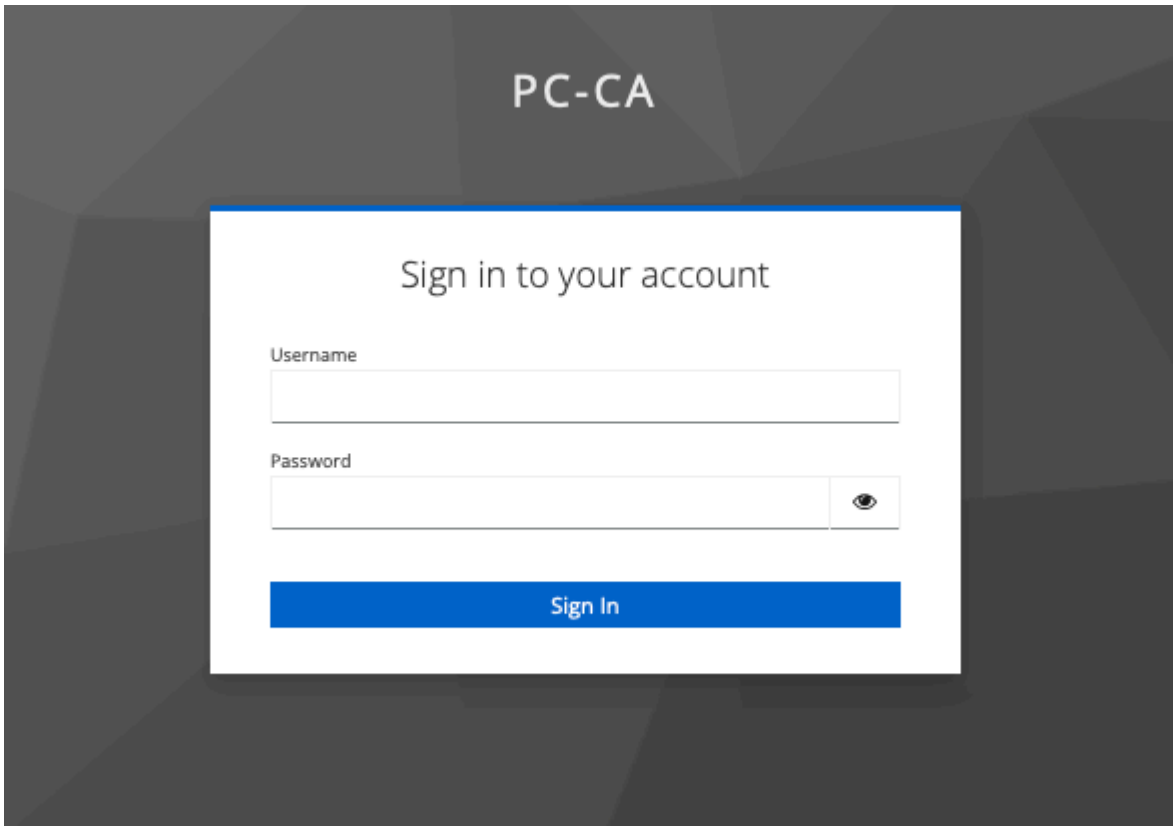

Рисунок 1. Ввод логина и пароля на странице авторизации.

2. Описание Личного кабинета Пользователя

2.1. Описание личного кабинета

Личный кабинет пользователя состоит из трех функциональных областей:

1. глобальные настройки;
2. запросы пользователя;
3. сертификаты пользователя.

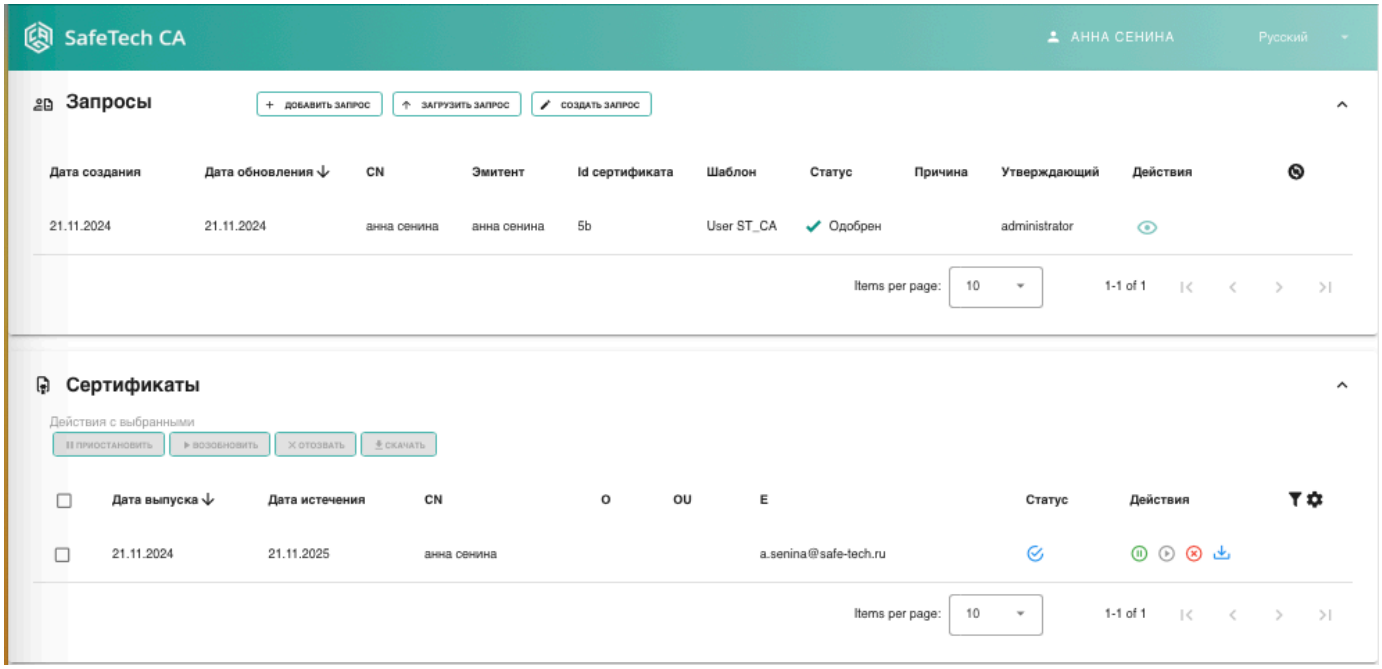

Рисунок 2. Личный кабинет Пользователя.

Функциональные области с запросами и сертификатами могут быть свернуты, в случае если Пользователю нет необходимости в работе с ними на текущий момент.

2.1.1. Глобальные настройки

2.1.1.1. Переключение языка

В шапке Личного кабинета Пользователю доступна функция переключения языка (Рисунок 3):

- русский;
- английский.

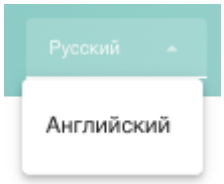

Рисунок 3. Кнопка переключения языка.

При этом локаль браузера, выбранная пользователем, определяется Личным кабинетом автоматически, что позволяет открывать Личный кабинет в соответствии с выбранной пользователем локалью автоматически.

2.1.1.2. Выход из Личного кабинета

В шапке Личного кабинета Пользователя при нажатии на логин Пользователь может выйти из авторизованной зоны.

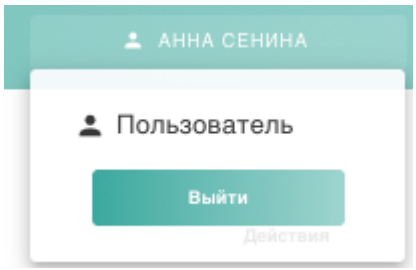

Рисунок 4. Кнопка настроек Личного кабинета Пользователя.

2.1.1.3. Смена роли

В шапке Личного кабинета Пользователя при нажатии на логин Пользователь (Рисунок 4, которому

Если Пользователю Администратор присвоил несколько ролей, например, Пользователя и Администратора/Оператора/Аудитора, при нажатии на свой логин в шапке Личного кабинета ему станет доступна кнопка "Сменить роль". Нажав на неё, Пользователь может ознакомиться со списком доступных ему ролей и переключиться на Личный кабинет другой роли.

2.1.2. Раздел запросы Пользователя

В данном разделе Пользователь может ознакомиться со своими запросами на выпуск сертификата.

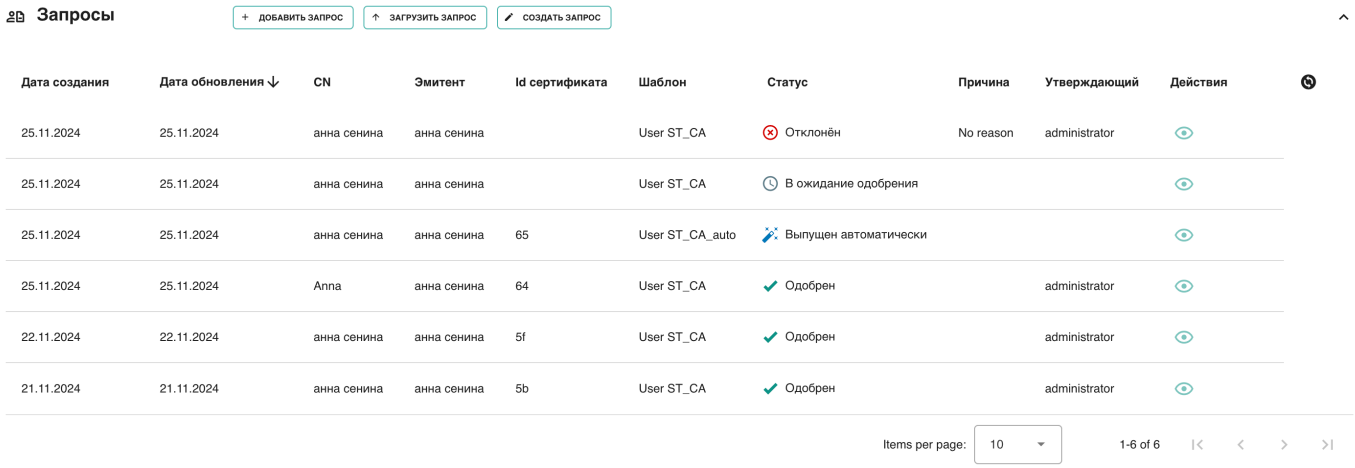

Рисунок 5. Запросы Пользователя.

В таблице отображения запросов Пользователя предусмотрена пагинация. В связи с чем Пользователь может выбрать удобное для себя количество отображаемых в таблице строк.

Рисунок 6. Пагинация и переключение между страницами запросов Пользователя.

Пользователь может управлять переходом между страницами таблицы с запросами с помощью стрелок в нижнем правом углу таблицы.

Пользователь может обновить данные таблицы нажатием на кнопку "Обновление" справа от таблицы.

2.1.2.1. Столбцы таблицы запросов Пользователя

В информационную таблицу о запросах Пользователя вынесена основная содержательная информация, которая может потребоваться для поиска и оперативного отслеживания статуса по конкретному запросу для выпуска сертификата.

Таблица 1. Значения столбцов таблицы запросов Пользователя

№	Название столбца	Значение
1	Дата создания	Дата направления запроса на выпуск сертификата
2	Дата обновления	Дата изменения статуса запроса
3	CN	Common Name, указанный в запросе на выпуск сертификата
4	Эмитент	Имя Пользователя, отправившего запрос на выпуск сертфиката
5	ID сертификата	Серийный номер сертификата, выпущенного по данному запросу. Не указывается в таблице, в случае если запрос на выпуск сертификата был отклонен Администратором
6	Шаблон	Имя шаблона, который указан в запросе на выпуск сертификата
7	Статус	Статус, в котором находится запрос на выпуск сертифката: - Выпущен автоматически - сертификат был выпущен по запросу без одобрения Администратором; - Отклонен - запрос на выпуск сертификата был отклонен Администратором; - В ожидании одобрения - запрос ожидает рассмотрения и одобрения Администратором; - Одобрен - запрос на выпуск сертификата был одобрен Администратором и сертификат был выпущен.
8	Причина	Причина отколонения запроса на выпуск сертификата Администратором. В случае одобрения запроса Администратором, значение в столбце не указывается
9	Утверждающий	Имя учетной записи Администратора, принявшего решение об одобрении/отклонении запроса на выпуск сертификата
10	Действия	Действия, доступные пользователю: - Предпросмотр состава запроса;

- Скачивание архива - действие доступно только один раз (подробнее в разделе 2.1.2.3).

2.1.2.2. Сортировка и фильтрация запросов на выпуск сертификата

Пользователь может изменить сортировку списка запросов по каждому из столбцов таблицы от меньшего значения к большему и наоборот. Для сортировки необходимо нажать на название необходимого столбца.

При нажатии на кнопку "Фильтр", справа от таблицы, для Пользователя станут доступны поисковые строки по каждому из столбцов таблицы.

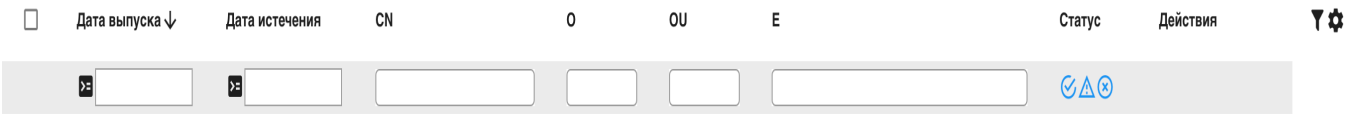

Рисунок 7. Строка фильтрации значений в таблице запросов Пользователя.

При введении Пользователем нескольких фильтров одновременно строки в таблице будут отфильтрованы с учетом этих фильтров (логическое "И").

2.1.2.3. Действия с запросами пользователя

Пользователю доступно два основных действия с запросами на выпуск сертификата:

1. предпросмотр состава запроса - Пользователь может ознакомиться с составом запроса в открывшемся модальном окне;
2. скачать архив, после одобрения запроса на выпуск сертификата Администратором.

Рисунок 8. Кнопки действий Пользователя с запросами: предпросмотр состава запроса и скачивание архива (соответственно слева-направо).

Архив содержит в себе PFX-контейнер, сертификаты в кодировках pem и der, а также текстовый файл с автоматически сгененированным паролем от PFX-контейнера. Архив доступен к скачиванию пользователем только один раз, после скачивания он будет безвовратно удален из инстанса SafeTech CA.

2.1.3. Раздел сертификаты Пользователя

В данном разделе Пользователь может ознакомиться с сертификатами:

- выпущенными по его запросам;
- выпущенными для Пользователя Администратором (в случае если в запросе был указан Common Name (CN) Пользователя).

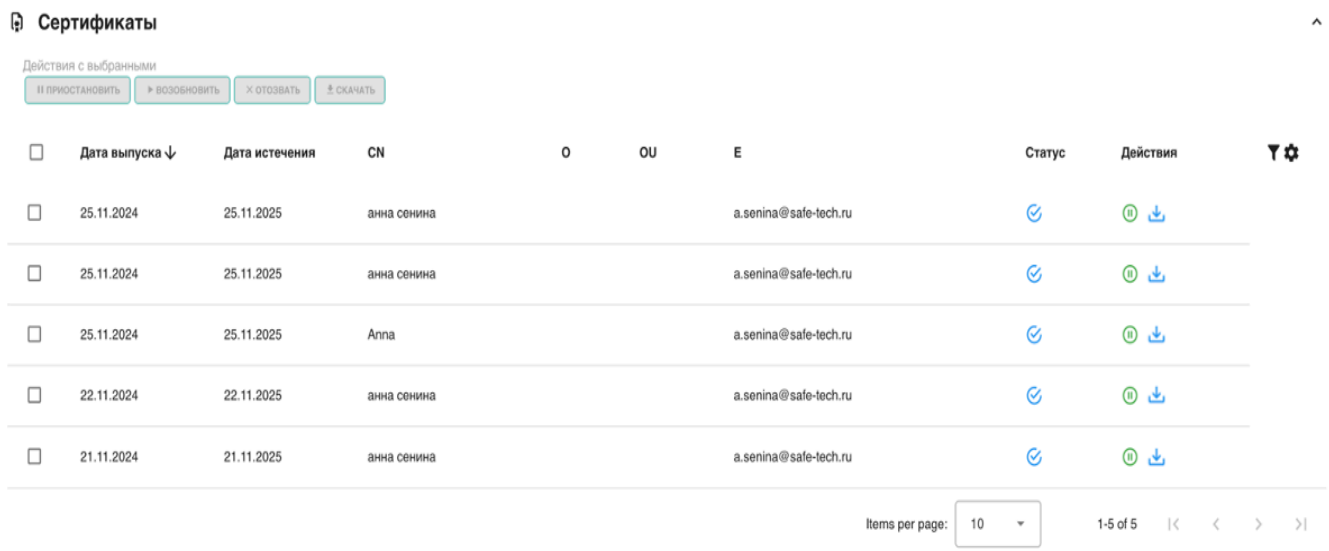

Рисунок 9. Сертификаты Пользователя.

В разделе отображения сертификатов Пользователя предусмотрена пагинация. В связи с чем Пользователь может выбрать удобное для себя количество отображаемых в таблице строк.

Рисунок 10. Пагинация и переключение между страницами сертификатов Пользователя.

Пользователь может управлять переходом между страницами таблицы с сертификатами с помощью стрелок в нижнем правом углу таблицы.

2.1.3.1. Столбцы таблицы сертификатов Пользователя

В информационную таблицу о сертификатах Пользователя вынесена основная содержательная информация, которая может потребоваться для поиска и оперативного отслеживания статуса по конкретному сертификату.

Таблица 2. Значения столбцов таблицы сертификатов Пользователя

№	Название столбца	Значение
1	Дата выпуска	Дата выпуска сертификата
2	Дата истечения	Дата истечения срока действия запроса
3	CN	Common Name, указанный в сертификате
4	O	Наименование организации, указанное в сертификате
5	OU	Наименование организационного юнита компании, указанное в сертификате
6	E	Адрес электронной почты, указанный в сертификате

7	Статус	Статус, в котором находится сертификат: - Активен - сертификат действителен; - Приостановлен - сертификат был приостановлен Пользователем или Администратором; - Просрочен - срок действия сертификата истек; - Отозван - сертификат находится в списке отозванных сертификатов и более не действителен.
8	Действия	Действия, доступные пользователю: - приостановить сертификат; - скачать сертификат.

2.1.3.2. Настройка и сортировка таблицы отображения выпущенных сертификатов

Пользователь может изменить сортировку списка запросов по каждому из столбцов таблицы от меньшего значения к большему и наоборот. Для сортировки необходимо нажать на название необходимого столбца.

При нажатии на кнопку "Фильтр", справа от таблицы, для Пользователя станут доступны поисковые строки по каждому из столбцов таблицы.

Рисунок 11. Строка фильтрации значений в таблице сертиикатов Пользователя.

Пользователь может скрыть столбцы таблицы, которые ему не нужны для работы на данный момент. Для этого ему необходимо нажать на "Шестеренку" справа-сверху от таблицы. Переключением свитчеров Пользователь может отключить ненужные для него столбцы.

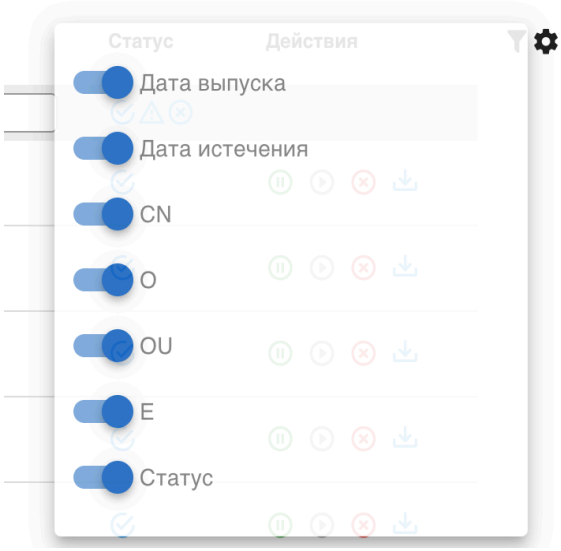

Рисунок 12. Строка фильтрации значений в таблице сертификатов Пользователя.

3. Выпуск сертификата

В разделе запросов Пользователю доступно три возможных способа выпуска сертификата с помощью кнопок:

1. "Добавить запрос" - загрузка запроса текстом в формате PKCS#10 (кодировка pem).
2. "Загрузить запрос" - загрузка файловых запросов.
3. "Создать запрос" - создание запроса на выпуск сертификата из web-интерфейса Личного кабинета Пользователя.

3.1. Создание запроса на выпуск сертификата

3.1.1. Текстовый запрос на выпуск сертификата

Для подгрузки текстового запроса Пользователю необходимо:

1. нажать на кнопку "добавить" в разделе "Действия", после чего требуется загрузить текст запроса в формате PKCS#10 (кодировка pem) в поле открывшегося окна.

Рисунок 13. Окно для загрузки тестового запроса.

2. нажать на кнопку "Подтвердить", после чего запрос будет:

- направлен на рассмотрение Администратору. После одобрения запроса сертификат будет выпущен. При отклонении запроса, Пользователь может ознакомиться с причиной отклонения в столбце "Причина";

- выпущен сразу, минуя рассмотрение запроса Администратором, если для указанного в запросе шаблона предусмотрен автовыпуск сертификата.

Пользователь может ознакомиться с составом запроса при нажатии на кнопку "Посмотреть состав запроса".

3.1.2. Файловый запрос на выпуск сертификата

Для массового выпуска сертификатов Пользователь может воспользоваться функциональностью выпуска сертификатов с помощью загруженных файловых запросов. Также Пользователь данным способом выпускать и единичный сертификат. Для этого Пользователю необходимо:

1. нажать на кнопку "Загрузить запрос", после чего требуется загрузить файлы запросов в открывшееся окно;

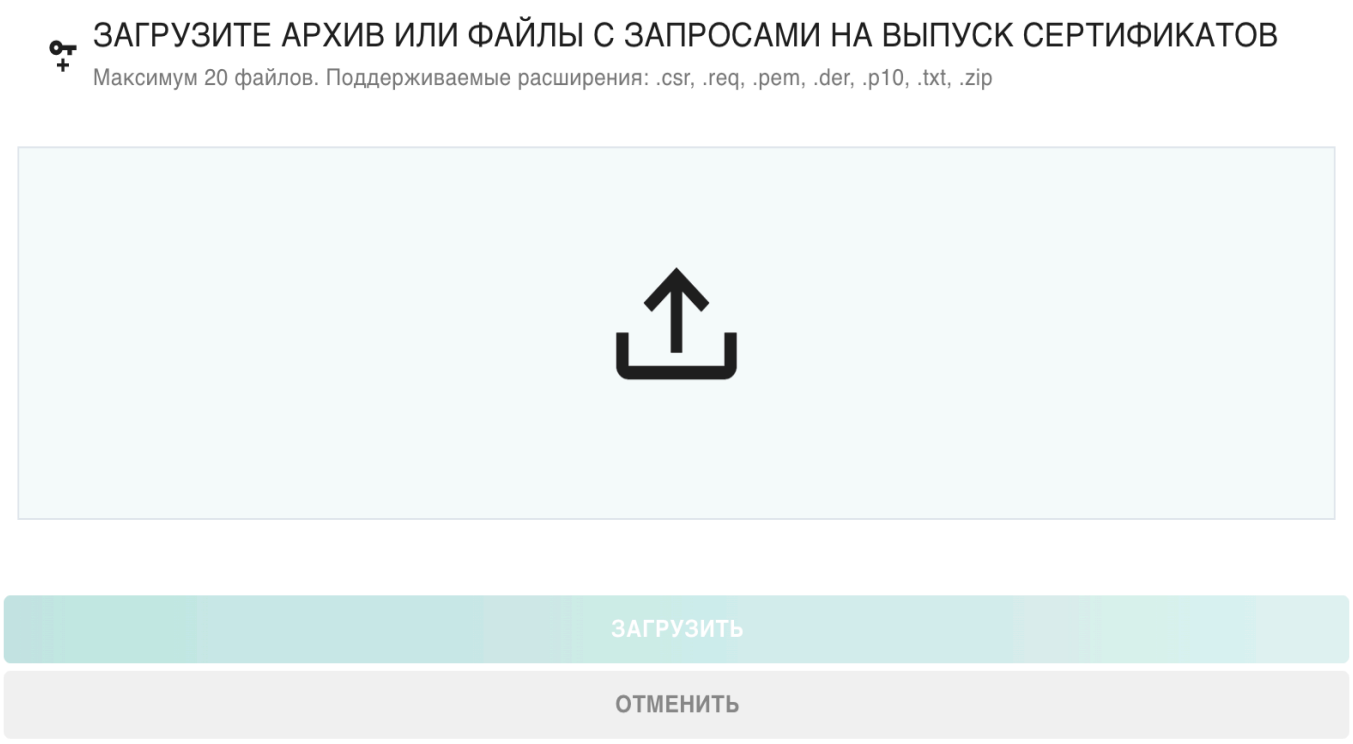

Рисунок 14. Окно для загрузки файловых запросов.

2. нажать на кнопку "Подтвердить", после чего запросы будут:

- направлены на рассмотрение Администратору. После одобрения запросов сертификаты будет выпущены. При отклонении, Пользователь может ознакомиться с причиной отклонения в столбце "Причина";
- выпущены сразу, минуя рассмотрение запроса Администратором, если для указанного в запросе шаблона предусмотрен автовыпуск сертификата.

Единоразово массово пользователь может загрузить 20 файлов форматов: csr, req, pem, der, p10, txt, zip. Zip-архив может включать в себя группу запросов на выпуск сертификата.

Пользователь может ознакомиться с составом запроса, нажав на кнопку "Документа" рядом с запросом.

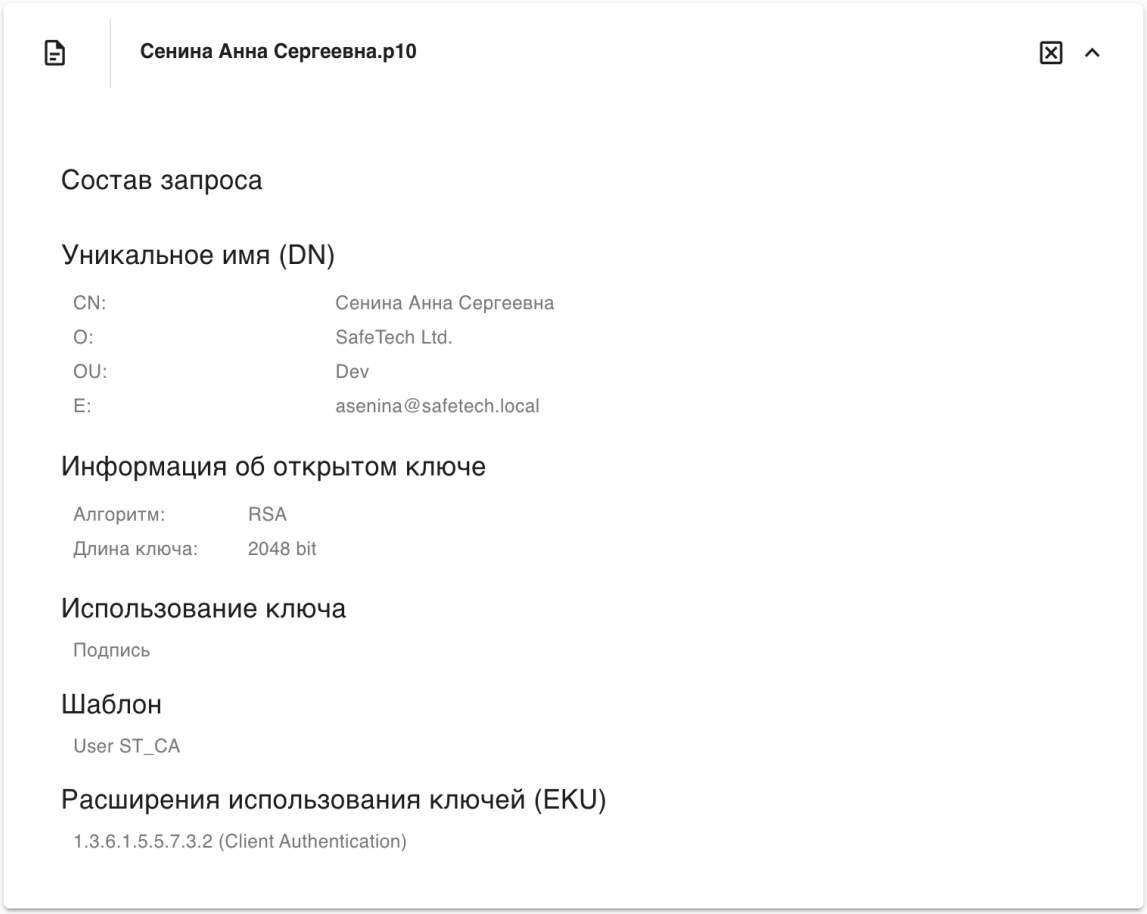

Рисунок 15. Предпросмотр состава запроса.

3.1.3. Создание запроса на выпуск сертификата из формы

Пользователь может сформировать запрос прямо из Личного кабинета (данная функциональность доступна только при работе с шаблонами протокола ST-CA). Для этого Пользователю необходимо:

1. нажать на кнопку "Создать запрос", после чего станет доступна форма создания запроса на выпуск сертификата;

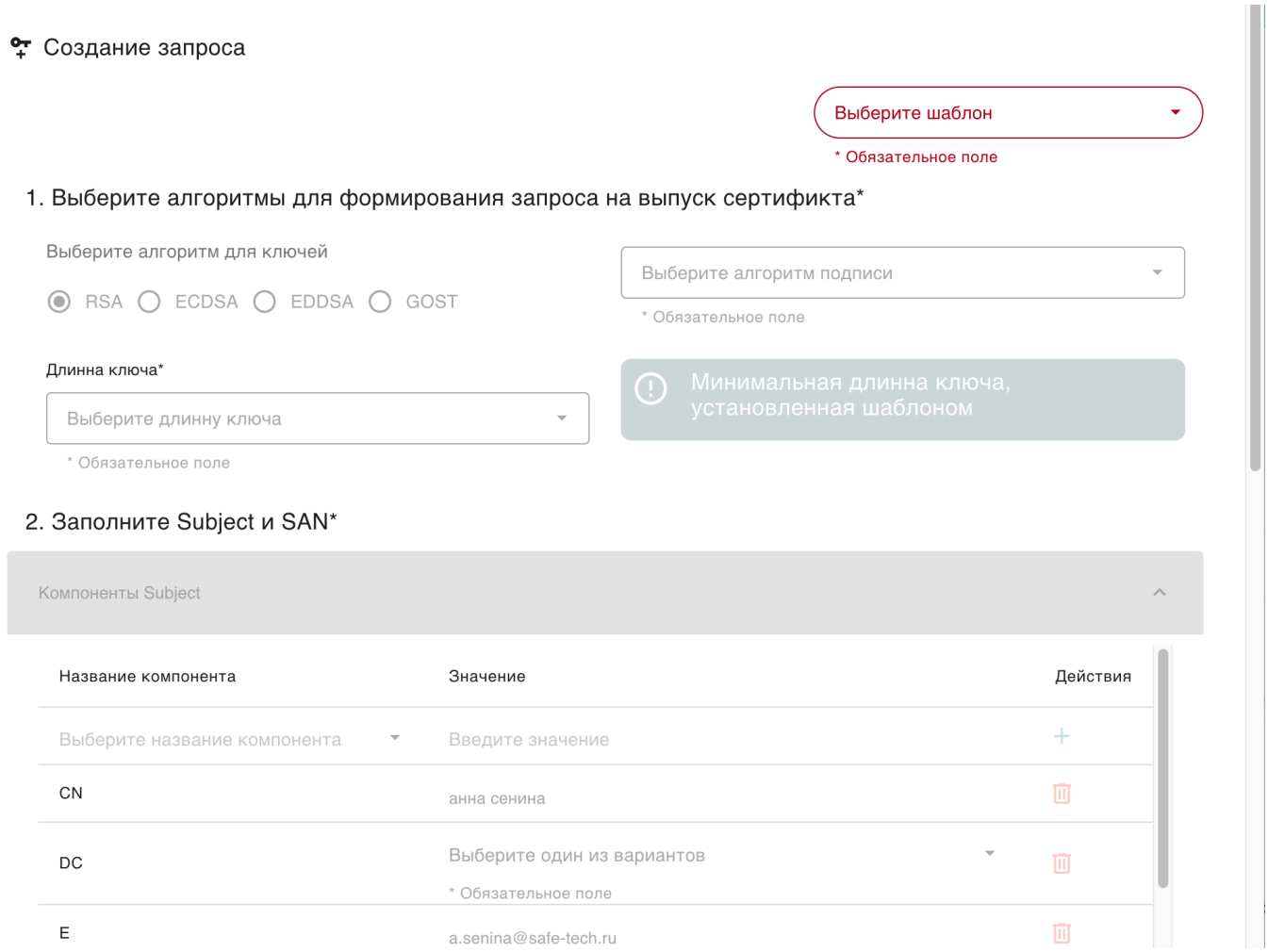

Рисунок 16. Создание запроса на выпуск сертификата из формы.

2. выбрать шаблон из списка доступных Пользователю;
3. Пользователю необходимо выбрать алгоритм для формирования запроса.

При выборе алгоритма для ключей RSA Пользователю будут доступны алгоритмы подписи SHA256withRSA, SHA384withRSA, SHA512withRSA. В завимимости от выбранного алгоритма для Пользователя будут менять доступные длины ключа:

- "SHA512withRSA" - 1024 бита, 2048 бит, 4096 бит
- "SHA384withRSA" - 1024 бита, 2048 бит, 4096 бит
- "SHA256withRSA" - 512 бит, 1024 бита, 2048 бит, 4096 бит

При выборе алгоритма для ключей ECSCA Пользователю будут доступны алгоритмы подписи SHA256withECDSA, SHA384withECDSA, SHA512withECDSA. Пользователю потребуется выбрать KeySpec: (prime256v1, secp384r1, secp521r1).

При выборе алгоритма для ключей EDDSA Пользователю останется указать только алгоритм подписи Ed25519.

При выборе алгоритма для ключей GOST Пользователю потребутся сделать выбор между алгоритмами подписи:

- GOST3411_2012_256withGOST3410_2012_256
- GOST3411_2012_512withGOST3410_2012_512

4. Пользователю необходимо заполнить компоненты Subject и SAN

При заполнении компонентов Subject часть данных будет подтянута автоматически из Сервиса управления доступом.

2. Заполните Subject и SAN*

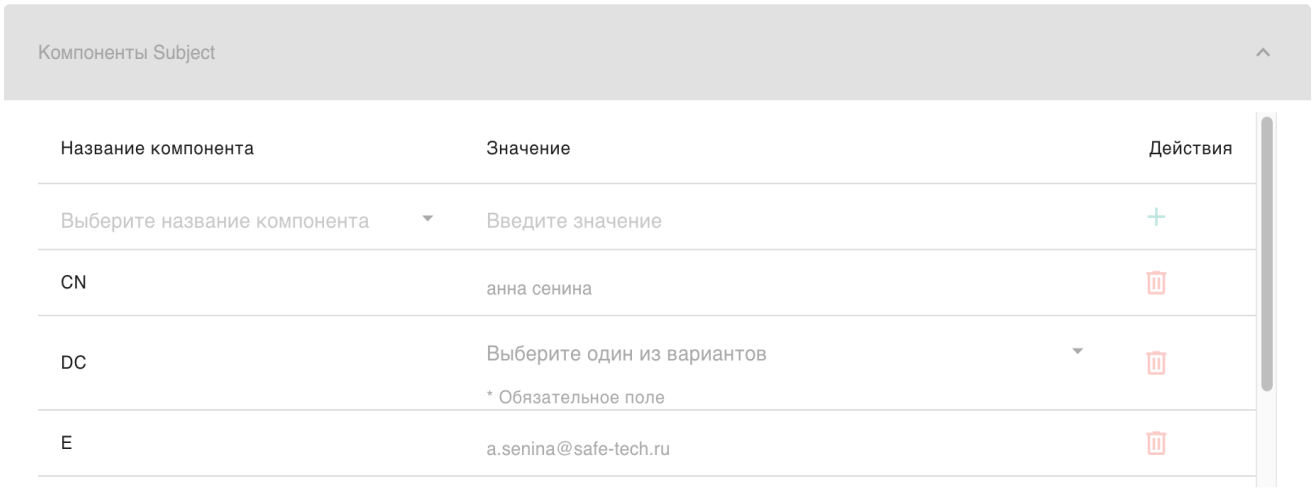

Рисунок 17. Заполнение компонентов Subject.

Если данных будет недостаточно, пользователь может самостоятельно добавить компоненты в первой строке таблицы из доступного ему списка и указать необходимые значения. Для добавления компонента в список, Пользователю необходимо нажать "плюс".

Пользователь может удалить значения, в которых нет необходимости для формирования запроса на выпуск сертификата, нажатием кнопки "корзина" в действиях.

При заполнении компонентов SAN часть данных будет подтянута автоматически из Сервиса управления доступом.

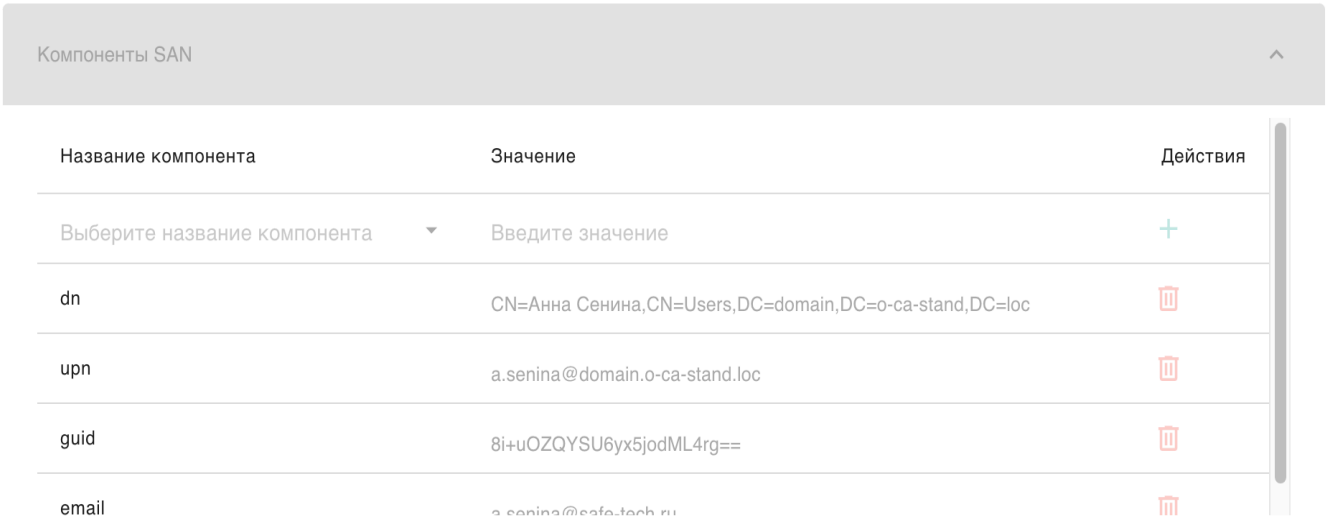

Рисунок 18. Заполнение компонентов SAN.

Если данных будет недостаточно, пользователь может самостоятельно добавить компоненты в первой строке таблицы из доступного ему списка и указать необходимые значения. Для добавления компонента в список, Пользователю необходимо нажать "плюс".

Пользователь может удалить значения, в которых нет необходимости для формирования запроса на выпуск сертификата, нажатием кнопки "корзина" в действиях.

5. Пользователю необходимо задать пароль от PFX контейнера, который будет сформирован при создании запроса на выпуск сертификата.

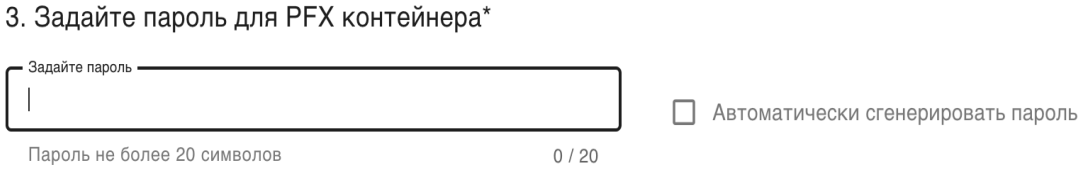

Рисунок 19. Пароль от PFX контейнера.

Пользователь может задать пароль самостоятельно, количество символов пароля не должно превышать 20. Также Пользователь может выбрать опцию автоматической генерации пароля, в этом случае пароль будет передан Пользователю вместе с PFX-контейнером.

6. дополнительно Пользователь может ознакомиться с настройками шаблона, такими как:

- срок действия сертификата;
- политики использования ключей, предусмотренные шаблоном;
- расширения использования ключей (EKU);
- атрибуты запроса на сертификат.

7. нажать на кнопку "Подтвердить", после чего запросы будут:

- направлены на рассмотрение Администратору. После одобрения запросов сертификаты будет выпущены. При отклонении, Пользователь может ознакомиться с причиной отклонения в столбце "Причина";
- выпущен сразу, минуя рассмотрение запроса Администратором, если для указанного в запросе шаблона предусмотрен автовыпуск сертификата.

3.2. Получение выпущенного сертификата

3.2.1. Получение сертификата, выпущенного из текстового или файлового запроса

При выпуске сертификатов способами, описанными в пунктах 3.1.1 и 3.1.2., Пользователь может скачать сертификат из раздела "Сертификаты". Пользователю необходимо выбрать необходимый сертификат, после чего нажать на кнопку "Скачивание" в действиях по данному сертификату.

3.2.2. Получение сертификата и pfx-контейнера

Получение сертификата вместе с PFX-контейнером возможно только в случае, если Пользователь создает запрос на выпуск сертификата из Личного кабинета. Для Пользователя будет сформирован архив, который будет включать в себя:

- PFX-контейнер с ключевой парой;
- текстовый файл (.txt) с паролем от PFX-контейнера (в случае если Пользователем была выбрана автоматическая генерация пароля от контейнера);
- сертификат в кодировке pem;
- сертификат в кодировке der.

Скачать архив Пользователь сможет только после одобрения запроса Администратором: рядом с одобренным запросом появится дополнительное действие "Скачать архив". Если по выбранному шаблону при создании запроса предусмотрен автовыпуск сертификата, то Пользователю будет предложено скачать архив сразу же после отправки запроса (подробнее в п. 2.1.2.3).

Пользователь может скачать архив только один раз, после чего он будет безвозвратно удален.