

Настройки безопасности

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

Безопасная загрузка файлов	4
Выбрать режим проверки файлов	4
Настроить список типов файлов	4
Настроить ограничения для неизвестных типов файлов	5
Настроить исключение веб-сервисов из ограничений загрузки файлов	6
Рекомендуемые настройки информационной безопасности	6
Внедрить политику паролей организации	6
Время завершения сессии	7
Протокол TLS для Creatio on-site	7
Безопасные конфигурации заголовков для Creatio on-site	8
Ответы на запросы для Creatio on-site	9
Запрет одновременных сеансов для Creatio on-site	9
Предоставить удаленный доступ службе поддержки Creatio	9
Настроить безопасный доступ	10
Просмотреть результаты подключения	12

Безопасная загрузка файлов

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Для повышения безопасности работы в Creatio вы можете настроить ограничения форматов загружаемых в приложение сторонних файлов. Ограничения на загрузку файлов действуют как для пользователей, так и для интеграций, например, внешних веб-сервисов.


При настроенных ограничениях Creatio проверяет формат файлов, которые загружаются на деталь [*Файлы и ссылки*]. В случае соответствия настройкам файл будет успешно загружен. В другом случае файл загружен не будет, а пользователь получит уведомление, что загрузка данного файла запрещена настройками безопасности. Для файлов, загруженных в систему до включения ограничений, настройки не применяются.

Ограничения действуют только на загрузку файлов в Creatio, скачивать файлы могут все пользователи, имеющие к ним доступ.

В системе предусмотрены следующие способы ограничения загрузки файлов:

- Ограничения для файлов **определенных типов** — вы можете настроить список **разрешенных расширений** или список **запрещенных расширений** файлов. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов определенных типов.
- Ограничения для файлов **неизвестных типов**. В этом случае можно установить разрешение или запрет на загрузку в приложение файлов, у которых не указано расширение и невозможно определить тип по содержимому.

Выбрать режим проверки файлов

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку **“Режим проверки файлов”** (код “FileSecurityMode”).
4. В поле [**Значение по умолчанию**] выберите необходимый тип ограничения:
 - **“Проверка файлов отключена”** — чтобы отменить все ограничения на загрузку файлов в приложение.
 - **“Список запрещенных расширений”** — чтобы запретить загрузку в приложение файлов определенных типов.
 - **“Список разрешенных расширений”** — чтобы разрешить загрузку в приложение только файлов определенных типов.
5. **Сохраните** изменения.

Настроить список типов файлов


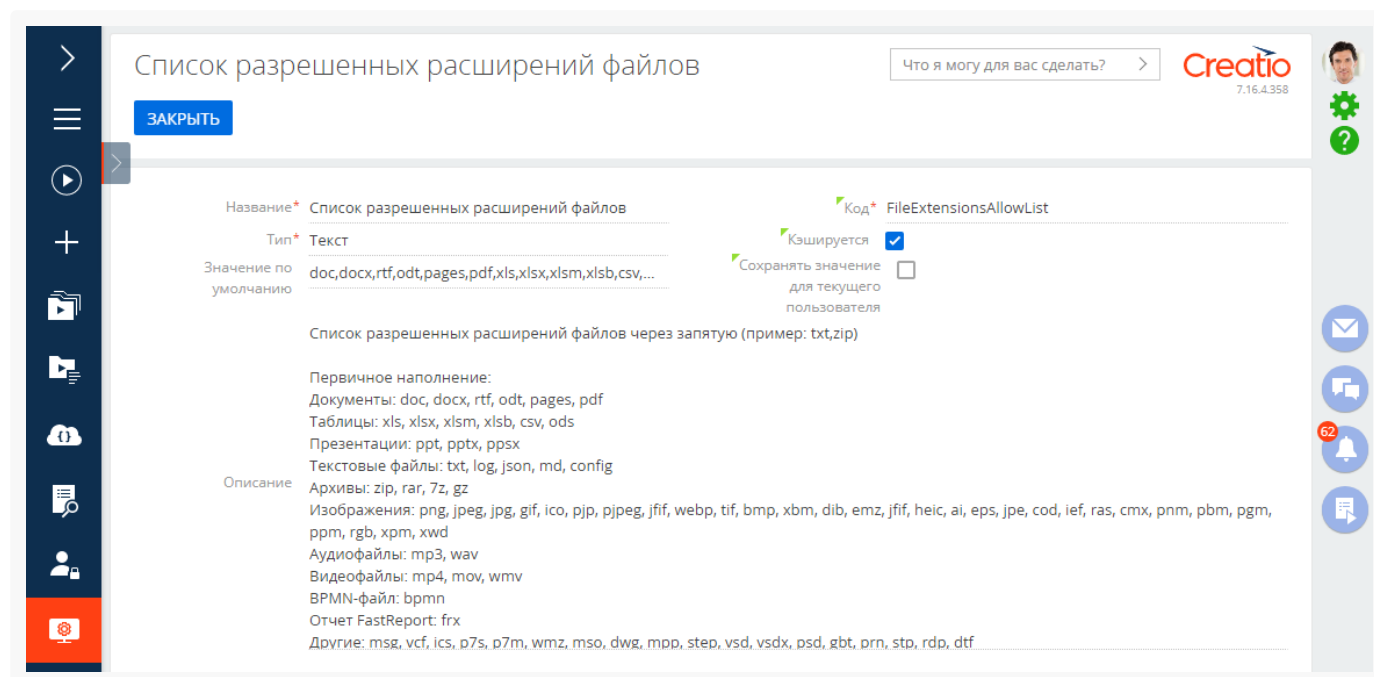
1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку
 - “**Список разрешенных расширений файлов**” (код “FileExtensionsAllowList”), чтобы настроить список разрешенных к загрузке типов файлов. По умолчанию в настройке приведены наиболее часто используемые типы файлов.
 - “**Список запрещенных расширений файлов**” (код “FileExtensionsDenyList”), чтобы настроить список запрещенных к загрузке типов файлов. По умолчанию в настройке приведены типы файлов, которые могут являться вредоносными.
4. В поле [**Значение по умолчанию**] через запятую без пробела укажите **расширения файлов** ([Рис. 1](#)) и проверьте корректность ввода.

Рис. 1 — Пример заполнения системной настройки “Список разрешенных расширений файлов”



5. **Сохраните** изменения.

Настроить ограничения для неизвестных типов файлов

Creatio определяет типы загружаемых файлов по их расширению. В случае если расширение не указано, система определяет тип файла на основании его содержимого. По умолчанию в систему разрешено загружать файлы неизвестных типов. Запрет загрузки таких файлов повысит безопасность работы в приложении, но в этом случае обязательно потребуется настроить список разрешенных или запрещенных расширений.

Чтобы **запретить загрузку** в Creatio файлов неизвестных типов:

1. Перейдите в **дизайнер системы** по кнопке .

2. Перейдите в раздел [**Системные настройки**].
3. Откройте системную настройку “**Разрешить работу с неизвестными типами файлов**” (код “AllowFilesWithUnknownType”).
4. Снимите признак [**Значение по умолчанию**].
5. **Сохраните** изменения.

Настроить исключение веб-сервисов из ограничений загрузки файлов

Ограничение загрузки файлов применяется для всех используемых в системе веб-сервисов, включая те, которые были добавлены в процессе кастомизации системы, в проектных решениях и приложениях Marketplace. Чтобы веб-сервисы могли добавлять в Creatio файлы тех типов, которые не разрешены пользователям, их необходимо **добавить в список исключений**. Для этого:

1. Перейдите в **дизайнер системы** по кнопке .
2. Перейдите в раздел [**Справочники**].
3. Откройте справочник [**Список исключений из проверки безопасности файлов**].
4. Нажмите [**Добавить**].
5. В поле [**Название**] укажите **URI** веб-сервиса, который необходимо добавить в исключения. Запись сохраняется автоматически.
 - Пример для приложений на **.NET Framework**: /0/rest/[*Название пользовательского сервиса*]/[*Конечная точка пользовательского сервиса*], без указания [*Адреса приложения*].
 - Пример для приложений на **.NET CORE**: /rest/[*Название пользовательского сервиса*]/[*Конечная точка пользовательского сервиса*], без указания [*Адреса приложения*].
6. **Повторите** для всех веб-сервисов, которым необходимо разрешить загрузку файлов в приложение.

Рекомендуемые настройки информационной безопасности

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Статья содержит лучшие практики настроек информационной безопасности Creatio.

Внедрить политику паролей организации

Убедитесь в том, что настройки логина и пароля соответствуют политике безопасности компании. Вы можете использовать рекомендованные значения, если не определены точные требования.

Длина пароля. Рекомендуем использовать пароли, состоящие из 8 и более символов. Установить сложность пароля вы можете в следующих [системных настройках](#):

- “Сложность пароля: Минимальная длина” (код “MinPasswordLength”);
- “Сложность пароля: Минимальное количество символов нижнего регистра” (код “MinPasswordLowercaseCharCount”);
- “Сложность пароля Минимальное количество символов верхнего регистра” (код “MinPasswordUppercaseCharCount”);
- “Сложность пароля Минимальное количество цифр” (код “MinPasswordNumericCharCount”);
- “Сложность пароля Минимальное количество специальных символов” (код “MinPasswordSpecialCharCount”).

История паролей. Creatio сравнивает предыдущий пароль пользователя с новым, чтобы убедиться, что они не совпадают. Количество предыдущих паролей, которые необходимо сравнить с новым, вы можете указать в системной настройке “Количество анализируемых паролей” (код “PasswordHistoryRecordCount”).

Количество попыток входа до предупреждающего сообщения и время блокировки пользователя. Рекомендуем установить 5 попыток входа до предупреждающего сообщения и 15 минут в качестве времени блокировки пользователя. Вы можете отрегулировать поведение блокировки в следующих системных настройках:

- “Количество попыток входа” (код “LoginAttemptCount”) — допустимое количество неудачных попыток ввода логина или пароля.
- “Количество попыток входа до предупреждающего сообщения” (код “LoginAttemptCount”) — порядковый номер неудачной попытки ввода логина или пароля, после которого отобразится сообщение о возможности дальнейшей блокировки учетной записи пользователя.
- “Время блокировки пользователя” (код “UserLockoutDuration”) — время блокировки (в минутах) учетной записи пользователя после указанного количества неудачных попыток ввода логина или пароля.

Подробнее: [Разблокировать учетную запись пользователя](#).

Сообщения о неверном пароле и блокировке при попытке входа. Рекомендуем отображать сообщение с общей информацией без уточнения конкретной проблемы. Для этого убедитесь, что у следующих системных настроек снят признак в значениях по умолчанию:

- “Отображать информацию о блокировке учетной записи при входе” (код “DisplayAccountLockoutMessageAtLogin”);
- “Отображать информацию о неверном пароле при входе” (код “DisplayIncorrectPasswordMessageAtLogin”).

Время завершения сессии

Задайте интервал в минутах, по истечении которого сессия будет закрыта, в системной настройке “Таймаут сеанса пользователя” (код “UserSessionTimeout”). Значение по умолчанию: “60”.

Протокол TLS для Creatio on-site

В Creatio реализована поддержка протокола TLS 1.2. Устаревшие версии протокола TLS 1.0 и 1.1 делают систему безопасности уязвимой.

Безопасные конфигурации заголовков для Creatio on-site

Примите необходимые меры для того, чтобы браузеры не поддавались уязвимостям, которые можно предотвратить. Для этого включите следующие заголовки, которые соответствуют [OWASP Secure Headers Project](#) (открытый проект обеспечения безопасности веб-приложений):

HTTP Strict Transport Security (HSTS). Включите заголовок `Strict-Transport-Security` и установите значение хранения параметра в памяти браузера, соответствующее одному году:

```
Strict-Transport-Security: max-age=3153600
```

Защита от кликджекинга (clickjacking). Включите заголовок `X-Frame-Options` и разрешите встраивание веб-страниц только на тех же адресах, что и у вашего приложения Creatio:

```
X-Frame-Options: sameorigin
```

Защита от атак межсайтового скриптинга (XSS). Включите заголовок `X-Frame-Options` и установите блокировку попыток XSS-атак:

```
X-XSS-Protection: 1; mode=block
```

Защита от MIME-сниффинга. Включите заголовок `X-Content-Type-Options` и установите режим “nosniff”. Этот режим предотвращает попытку браузера переопределить тип контента ресурса, если он отличается от объявленного типа контента:

```
X-Content-Type-Options: nosniff
```

Политика реферера (referrer policy). Включите заголовок `Referrer-Policy` и установите значение “origin-when-cross-origin”. Заголовок определяет, какой объем информации о реферере (отправленной с заголовком “Referer”) будет включен в запросы:

```
Referrer-Policy: origin-when-cross-origin
```

Безопасность контента. Включите заголовок `Content Security Policy` и настройте его следующим образом:

```
Content-Security-Policy: default-src 'self'; script-src 'unsafe-inline' 'unsafe-eval'; script-src
```


Ответы на запросы для Creatio on-site

Ограничьте количество и тип информации, доступной в ответах на запросы. Для этого измените файл [Web.config](#) в корневом каталоге Creatio следующим образом:

Отключите `X-Powered-By`.

```
<system.webServer> <httpProtocol> <customHeaders> <remove name="X-Powered-By" /> </customHeaders>
```

Отключите `X-AspNet-Version`.

```
<httpRuntime enableVersionHeader="false" />
```

Отключите `Server Header` (доступно для IIS версии 10 и выше).

```
<system.webServer> <security> <requestFiltering removeServerHeader ="true" /> </security> </syst
```

Запрет одновременных сеансов для Creatio on-site

Начиная с версии Creatio 7.13.3, вы можете запретить несколько одновременных входов в систему под одним пользователем. Creatio автоматически закроет старую сессию на другом устройстве, если пользователь откроет новую. Чтобы включить ограничение сессии, установите для параметра web.config **Feature-AllowOnlyOneSessionPerUser** значение "true":

```
<add key=""Feature-AllowOnlyOneSessionPerUser"" value=""true"" />
```

Функциональность доступна в режиме бета-тестирования. Не поддерживаются следующие функции:

- мобильное приложение;
- сквозная аутентификация Windows (UsePathThroughAuthentication);
- SSO (SAML).

Кроме того, для каждой интеграции необходима отдельная учетная запись Creatio, которая не используется пользователями.

Предоставить удаленный доступ службе поддержки Creatio

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Пользователи развернутых в облаке приложений могут предоставлять сотрудникам службы технической поддержки Creatio безопасный и контролируемый доступ к своим сайтам. При этом нет необходимости сообщать службе поддержки свои логин и пароль для доступа к сайту, что обеспечит безопасность персональных и коммерческих данных клиента.

На заметку. Для предоставления безопасного доступа в системе должны быть заполнены системные настройки: “Идентификатор приложения для предоставления доступа (по умолчанию)” (DefaultExternalAccessClientId), “Секретный ключ для Identity сервера” (IdentityServerClientSecret), “Адрес Identity сервера”(IdentityServerUrl), “Идентификатор приложения для Identity сервера” (IdentityServerClientId). Указанные настройки заполняются автоматически.

- Чтобы скрыть данные разделов системы от сотрудников службы поддержки, используется **режим изоляции данных**.
- Чтобы ограничить возможность менять настройки конфигурации для сотрудников службы поддержки используется **режим ограничения доступа на конфигурирование системы**. При этом настройки конфигурации, необходимые для решения обращения клиента, доступны для просмотра.

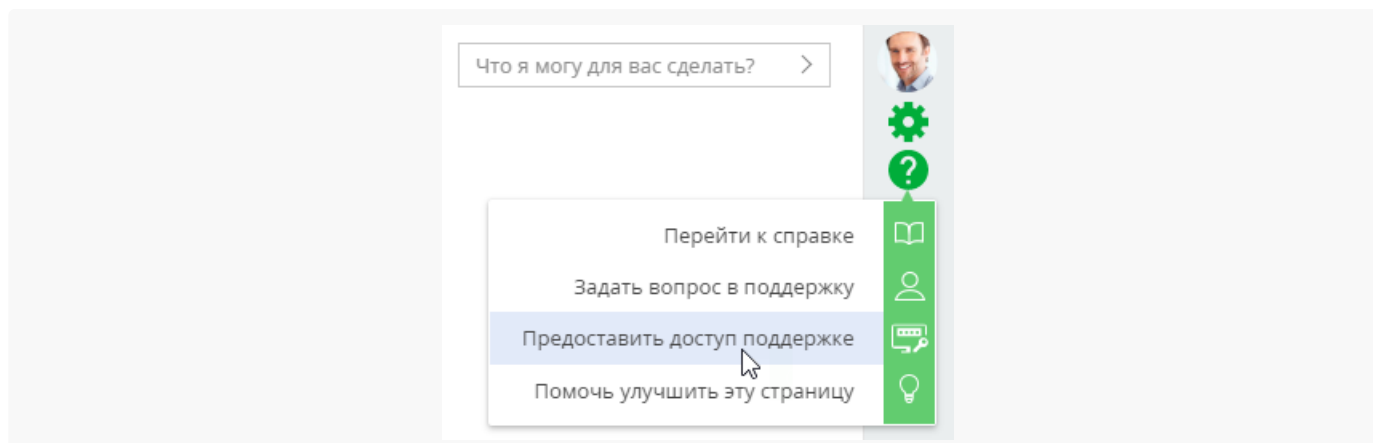
Настройка безопасного доступа выполняется администратором приложения (пользователем с ролью “System administrators”). Сотрудники службы поддержки могут подключаться под ученой записью администратора либо любого другого пользователя приложения. После того, как подключение состоялось, всю необходимую информацию по сеансу доступа можно получить в логах — когда состоялось подключение, а также какие данные были созданы при подключении.

Настроить безопасный доступ

На заметку. Для настройки доступа службы поддержки у вас должно быть право на чтение и добавление записей в объекте “Доступ внешних приложений”. У пользователей с ролью “System administrators” это право есть по умолчанию. Больше информации о правах на выполнение операций в объекте читайте в статье [“Настроить доступ по операциям”](#).

1. В правом верхнем углу приложения кликните  —> “Предоставить доступ поддержке” ([Рис. 1](#))

Рис. 1 — Переход к настройке доступа из справочного меню



2. Заполните поля открывшейся мини-карточки (Рис. 2):

Рис. 2 — Пример заполнения параметров доступа к клиентскому сайту

Доступ внешних приложений

Вы предоставляете службе поддержки Тerrasoft доступ к вашему приложению. Это поможет ускорить решение обращений и выполнение технических работ. Укажите параметры предоставления доступа. [Подробнее...](#)

Причина предоставления доступа*

Рассмотрение обращения SR00000068

Дата закрытия доступа*

23.12.2019

Предоставил

Авдоров Сергей

Запретить доступ к данным ☒

Запретить конфигурирование ☒

СОХРАНИТЬ **ОТМЕНА**

- a. В поле [**Причина предоставления доступа**] укажите, какая проблема привела к необходимости доступа, номер обращения или перечень работ, которые должен провести сотрудник службы поддержки.
- b. В поле [**Дата закрытия доступа**] укажите дату, до которой предоставляется доступ. В 23:59 указанной даты доступ будет автоматически отключен.
- c. В поле [**Предоставил**] по умолчанию указан пользователь, который настраивает доступ. Вы можете указать в этом поле любого пользователя, под учетной записью которого необходимо предоставить доступ сотрудникам службы поддержки.
- d. Признаки [**Запретить доступ к данным**] и [**Запретить конфигурирование**] позволяют предоставлять доступ к системе в режимах изоляции данных и ограничения доступа на конфигурирование. По умолчанию оба признака включены. Это означает, что при доступе к вашему приложению сотрудник службы поддержки не сможет видеть данные в разделах, а также не сможет выполнять настройку системы.
 - Если необходимо, чтобы у службы поддержки были такие же права доступа, как и у пользователя, под чьими учетными данными выполняется подключение, то снимите оба признака.
 - Если необходимо, чтобы сотрудник службы поддержки мог внести изменения в конфигурацию, но не видел данных в разделах системы, то снимите только признак [**Запретить конфигурирование**]. Так у него будет доступ к функциональности дизайнера системы, необходимой для выполнения настроек (например, к разделам [**Справочники**], [**Системные настройки**], [**Библиотека процессов**] и др.). При этом данные основных разделов будут ему недоступны.
 - Если необходимо, чтобы сотрудник службы поддержки мог просматривать данные в разделах, но не мог изменять конфигурацию системы, то снимите только признак [**Запретить доступ к данным**]. При этом у него будет возможность просмотреть настройки конфигурации.

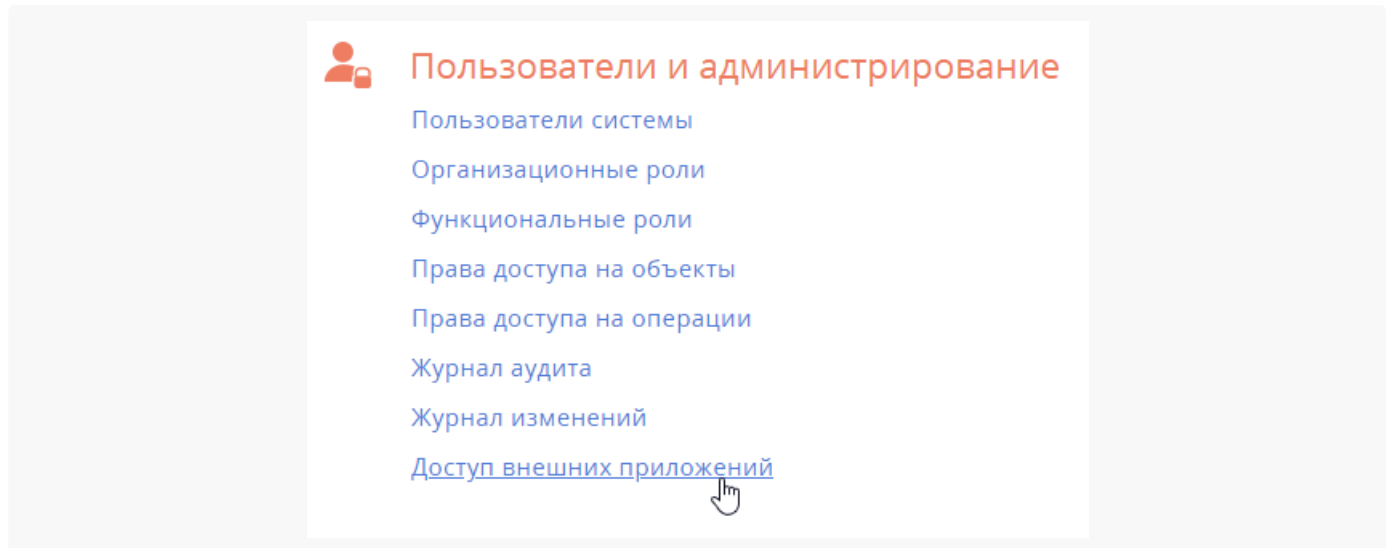
3. Сохраните запись.

В результате в разделе [*Доступ внешних приложений*] вашей системы будет создана новая запись. Сотрудники службы поддержки смогут войти на сайт клиента под учетной записью и с правами пользователя, указанного при настройке доступа, не используя учетных данных клиента. В 23:59 даты, указанной в настройках, доступ будет отключен автоматически.

Просмотреть результаты подключения

1. Перейдите в раздел [*Доступ внешних приложений*] дизайнера системы ([Рис. 1](#)).

Рис. 1 — Раздел [*Доступ внешних приложений*]



2. Откройте нужную запись в реестре раздела. На странице записи вы можете просмотреть все параметры доступа ([Рис. 2](#)). После того, как сеанс доступа службы поддержки состоится, на вкладке [*Сессии*] страницы записи автоматически отобразятся все данные, касающиеся этого сеанса — когда он состоялся, а также какие данные были созданы в системе во время сеанса.

Рис. 2 — Пример записи с параметрами доступа в разделе [*Доступ внешних приложений*]

>

≡

>

▶

+

▮

👤

👤

🏠

Рассмотрение обращения SR00000087

Что я могу для вас сделать? >

Creatio
7.15.3.606
ВИД ▾

🔧
?
☎
✉
💬
🔔
📄

ЗАКРЫТЬ

ДЕЙСТВИЯ ▾

🔗

Причина предоставления доступа*

Рассмотрение обращения SR00000087

Начало*

19.12.2019

Дата закрытия доступа*

22.12.2019

Предоставил

Авдоров Сергей

Активный

☒

Запретить доступ к данным

☒

Запретить конфигурирование

☒

< СЕССИИ

ДАННЫЕ ДОСТУПНЫЕ В РЕЖИМЕ ИЗОЛЯЦИИ

ФАЙЛЫ И ПРИМЕЧАНИЯ

ЛЕНТА

>

☑ Сеансы

Завершить сеанс