

Программный комплекс «Litoria DVCS»

Руководство администратора

Аннотация

В документе приводится руководство администратора безопасности программного комплекса «Litoria DVCS» версия 6.14.0-4 (далее – ПК «Litoria DVCS», ПК или комплекс) по управлению модулем «Litoria Auth».

В разделе «Назначение модуля» приводятся сведения о назначении модуля «Litoria Auth», перечислены его основные функциональные возможности.

В разделе «Условия применения» указаны условия, необходимые для использования модуля, требования к аппаратным и программным средствам автоматизированного рабочего места (АРМ) на котором функционирует модуль.

В разделе «Настройка модуля «Litoria Auth» описан порядок действий по установке и настройке модуля.

В разделе «Использование модуля «Litoria Auth» описан порядок работы с модулем, описаны действия, необходимые для обращения к функциям модуля.

Содержание

1	Назначение модуля	4
2	Условия применения	5
2.1	Требования к среде функционирования.....	5
2.2	Требования к аппаратному и программному обеспечению	5
3	Настройка модуля «Litoria Auth»	6
3.1	Установка модуля «Litoria Auth» в ОС Windows.....	6
3.2	Установка модуля «Litoria Auth» в ОС Linux.....	10
3.2.1	Установка СКЗИ «КриптоПро CSP».....	10
3.2.2	Установка модуля «Litoria Auth»	11
4	Использование модуля «Litoria Auth»	12
4.1	Настройки файла конфигурации.....	16
4.1.1	Настройки лог-файла.....	16
4.1.2	Настройка использования сертификатов.....	17
4.1.3	Настройка типа криптографического средства.....	17
4.2	Двухфакторная аутентификация через REST API.....	17
	Приложение 1.....	20
	Перечень сокращений	21

1 Назначение модуля

Модуль «Litoria Auth» предназначен для возможности использовать двухфакторную аутентификацию при помощи цифрового сертификата при входе в web-кабинет ПК «Litoria DVCS».

Модуль позволяет пользователю выбрать один из сертификатов, установленных в хранилище сертификатов «Личные» и передает введенные данные в ПК «Litoria DVCS» для аутентификации в web-кабинете.

2 Условия применения

2.1 Требования к среде функционирования

Модуль «Litoria Auth» функционирует под управлением следующих операционных систем (ОС) Microsoft Windows:

- Windows 7 (32 бит/64 бит);¹
- Windows 8/8.1 (32 бит/64 бит);
- Windows 10 (32 бит/64 бит).
- Windows Server 2008 R2;
- Windows Server 2012/2012R2/2016R2/2019R2/2022 (64 бит).

и ОС семейств Linux, поддерживающих системную библиотеку GNU C Library (Glibc) версии не ниже 2.22.

Дополнительно должно быть установлено следующее программное обеспечение:

- Средство криптографической защиты информации, реализованное в соответствии с технологией Microsoft CSP (при работе с отечественной криптографией необходимо использовать соответствующие СКЗИ)².
- СКЗИ «КриптоПро CSP» с поддержкой графического представления.³

2.2 Требования к аппаратному и программному обеспечению

Минимальные требования к рабочей станции, на которой устанавливается модуль «Litoria Auth», обусловлены применением используемых ОС.

¹ Срок эксплуатации ОС определяется сроками выпуска обновлений критических уязвимостей.

² При функционировании модуля на ОС семейства Windows.

³ При функционировании модуля на ОС семейства Linux.

3 Настройка модуля «Litoria Auth»

При обращении к web-кабинету «ПК «Litoria DVCS» пользователя возможны следующие виды аутентификации:

- вход по паролю – аутентификация с предъявлением имени учетной записи и пароля, соответствующего введенному имени учетной записи;
- вход по сертификату – двухфакторная аутентификация с использованием цифрового сертификата.

Аутентификация по сертификату доступна при выполнении условий:

- в конфигурационном файле «*appsettings.json*» установлено разрешение на аутентификацию по сертификату (подробнее в документе «Руководство администратора «Litoria DVCS»);
- на рабочей станции, с которой происходит обращение к web-кабинету, установлен модуль «Litoria Auth»;
- для учетной записи пользователя/администратора задан сертификат в web-кабинете в пункте меню «*Пользователи*».

Примечание. Для возможности входа по сертификату необходимо наличие установленного сертификата пользователя в оснастке **Сертификаты** (*certmgr.msc*) в разделе **Личные**.

Перед началом использования модуля «Litoria Auth» необходимо выполнить следующие настройки:

- получить и установить сертификат пользователя в хранилище сертификатов «Личные»;
- установить модуль «Litoria Auth».

3.1 Установка модуля «Litoria Auth» в ОС Windows

Для установки модуля «Litoria Auth» выполните следующие действия:

- 1) Запустите файл-инсталлятор «litoria_auth.msi» и в окне приветствия нажмите на кнопку «**Далее**» (рисунок 1).

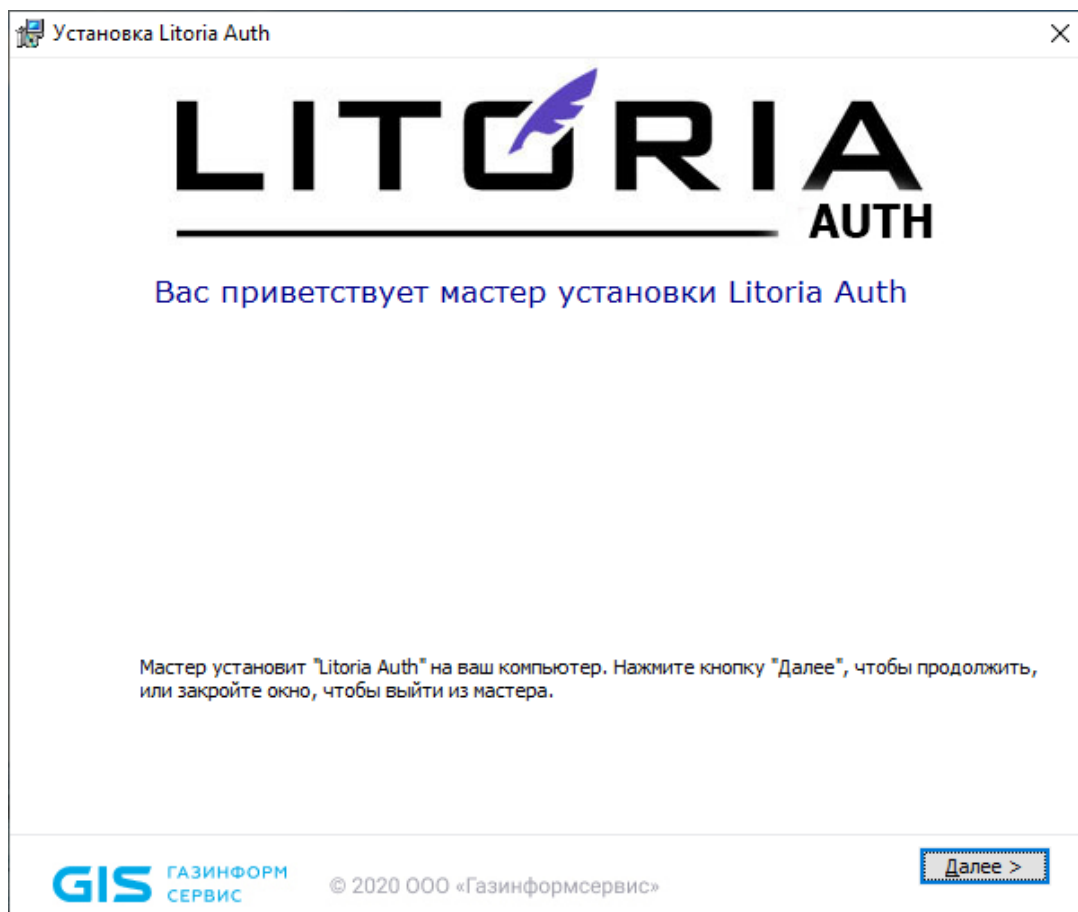


Рисунок 1 – Установка модуля «Litoria Auth»

- 2) Выберите директорию установки модуля (рисунок 2) и перейдите к следующему шагу по кнопке «Далее».

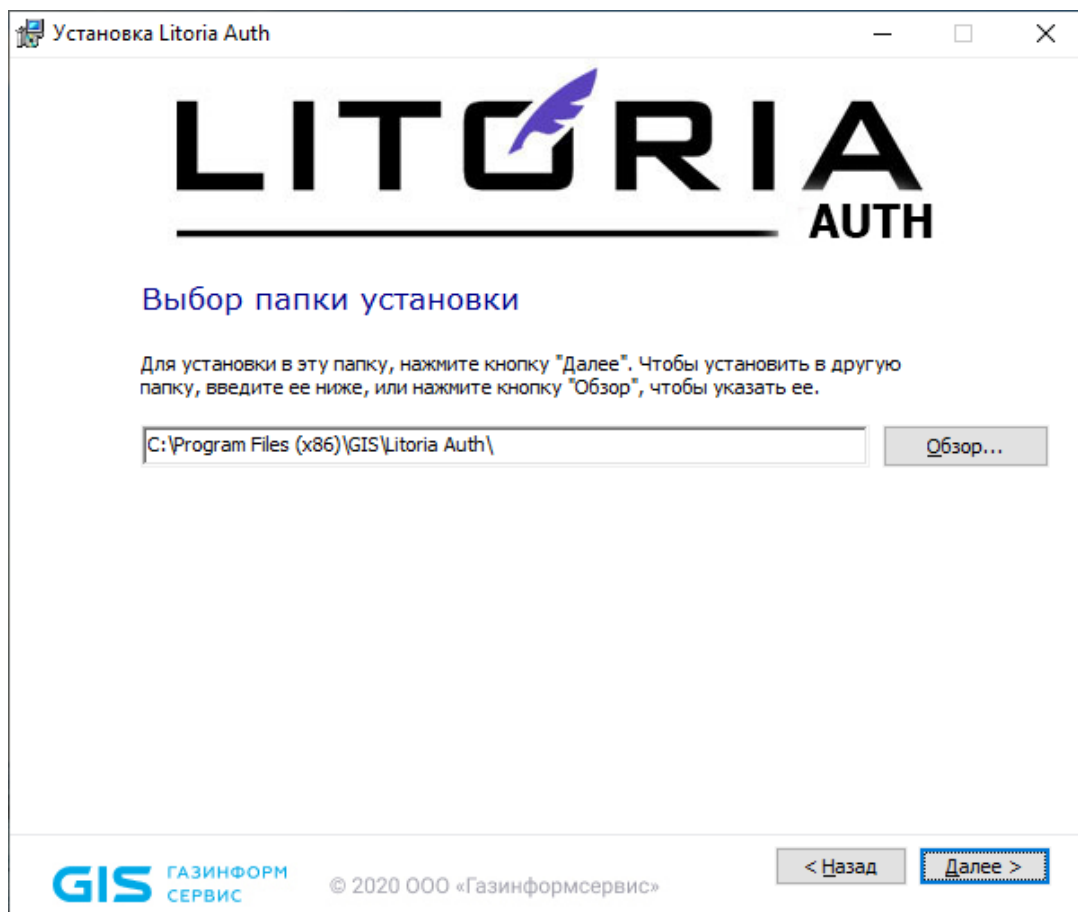


Рисунок 2 – Выбор директории установки

- 3) В появившемся окне подтвердите установку по кнопке «**Установить**» (рисунок 3).

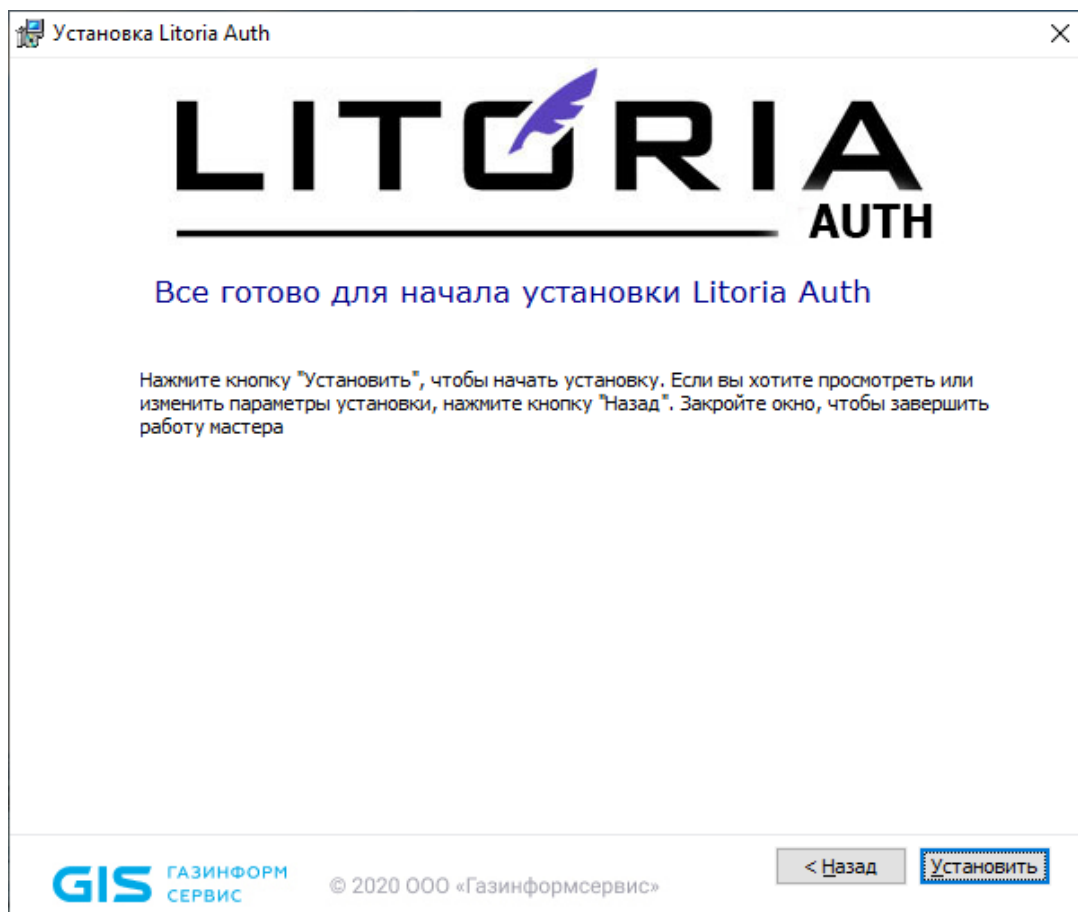


Рисунок 3 – Установка модуля

- 4) По окончании установки нажмите на кнопку «**Закр~~ы~~ть**» в окне завершения установки (рисунок 4).



Рисунок 4 – Успешное завершение установки

3.2 Установка модуля «Litoria Auth» в ОС Linux

Установка модуля «Litoria Auth» будет рассмотрена на примере ОС Альт.

Перед началом установки модуля «Litoria Auth» необходимо убедиться в выполнении требований к рабочей станции, на которую устанавливается модуль (см. подразделы 2.1 и 2.2).

Установка модуля «Litoria Auth» должна производиться пользователем, имеющим права администратора, в соответствии с эксплуатационной документацией на использование ПО под управлением ОС Альт.

3.2.1 Установка СКЗИ «КриптоПро CSP»

Перед началом использования модуля «Litoria Auth» необходимо установить СКЗИ «КриптоПро CSP» с поддержкой графического представления.

Для установки СКЗИ «КриптоПро CSP» необходимо выполнить следующие действия:

- 1) Извлечь все файлы из архива с помощью команды `tar -xzvflinux-amd64.tgz`.
- 2) Перейти в директорию распаковки архива СКЗИ с помощью команды `cd linux-amd64`.
- 3) Запустить установку СКЗИ «КриптоПро CSP» с помощью команды `./install_gui.sh`.

- 4) В результате выполнения скрипта появится графическая консоль установки СКЗИ «КриптоПро CSP» в которой необходимо выбрать устанавливаемые компоненты и активировать лицензию на продукт.

3.2.2 Установка модуля «Litoria Auth»

Для установки модуля «Litoria Auth» необходимо установить пакет *litoriaauth-
<версия>.rpm* командой `apt-get install litoriaauth-\
<версия>.rpm`.

После установки каталог с исполняемыми файлами будет находиться в директории */opt/GIS/litoriaauth*.

4 Использование модуля «Litoria Auth»

Для входа в web-кабинет «ПК «Litoria DVCS» с использованием цифрового сертификата необходимо:

- 1) Выполнить вызов модуля «Litoria Auth»:
 - путем запуска ярлыка (рисунок 5), созданного на рабочем столе компьютера при установке;
 - с помощью основного меню кнопки «Пуск» выбором пункта «Litoria Auth».

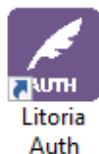


Рисунок 5 – Вызов СКЗИ путем запуска ярлыка

- 2) Для начала работы с ПК «Litoria DVCS» в строке web-браузера наберите адрес web-кабинета ПК «Litoria DVCS» (рисунок 6).

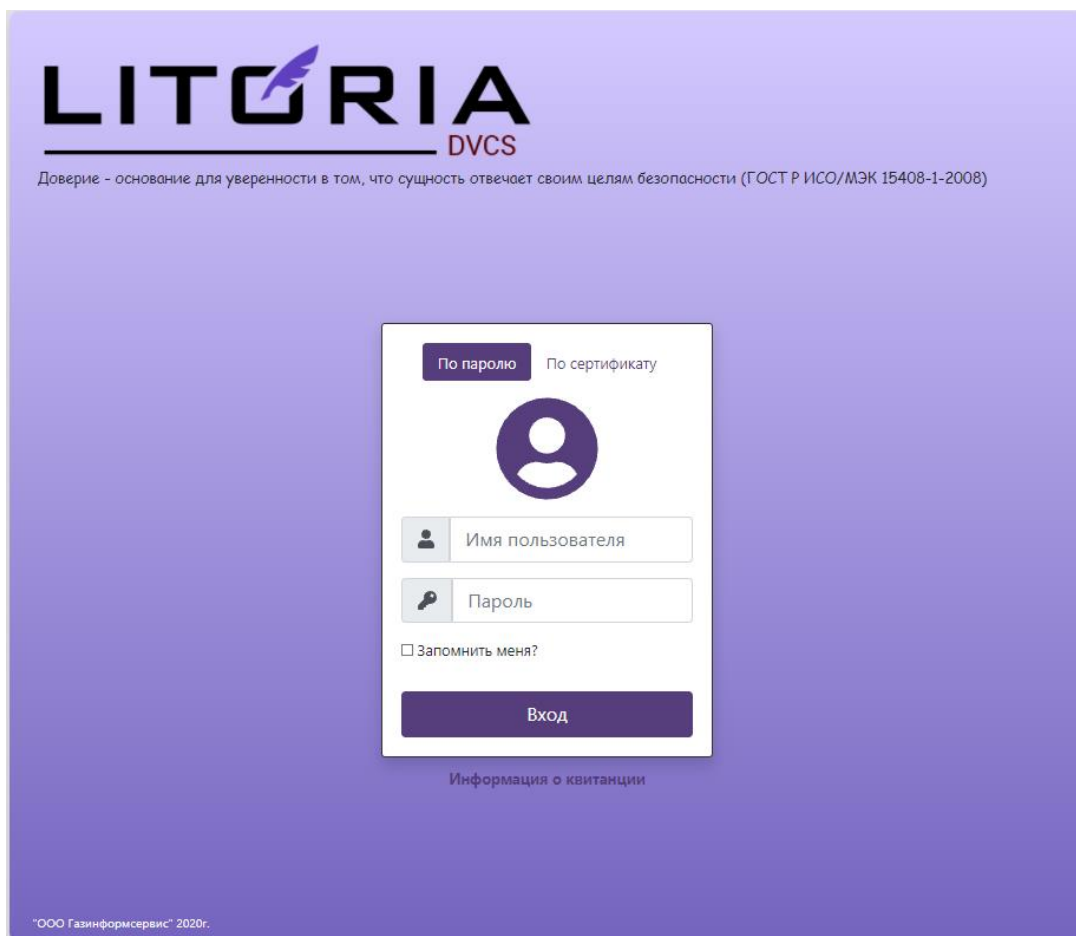


Рисунок 6 – Начальная страница web-кабинета ПК «СДТС «Litoria DVCS»

- 3) Если для пользователя доступны оба варианта аутентификации и по паролю, и по сертификату, перейдите на вкладку «По сертификату» (рисунок 7).

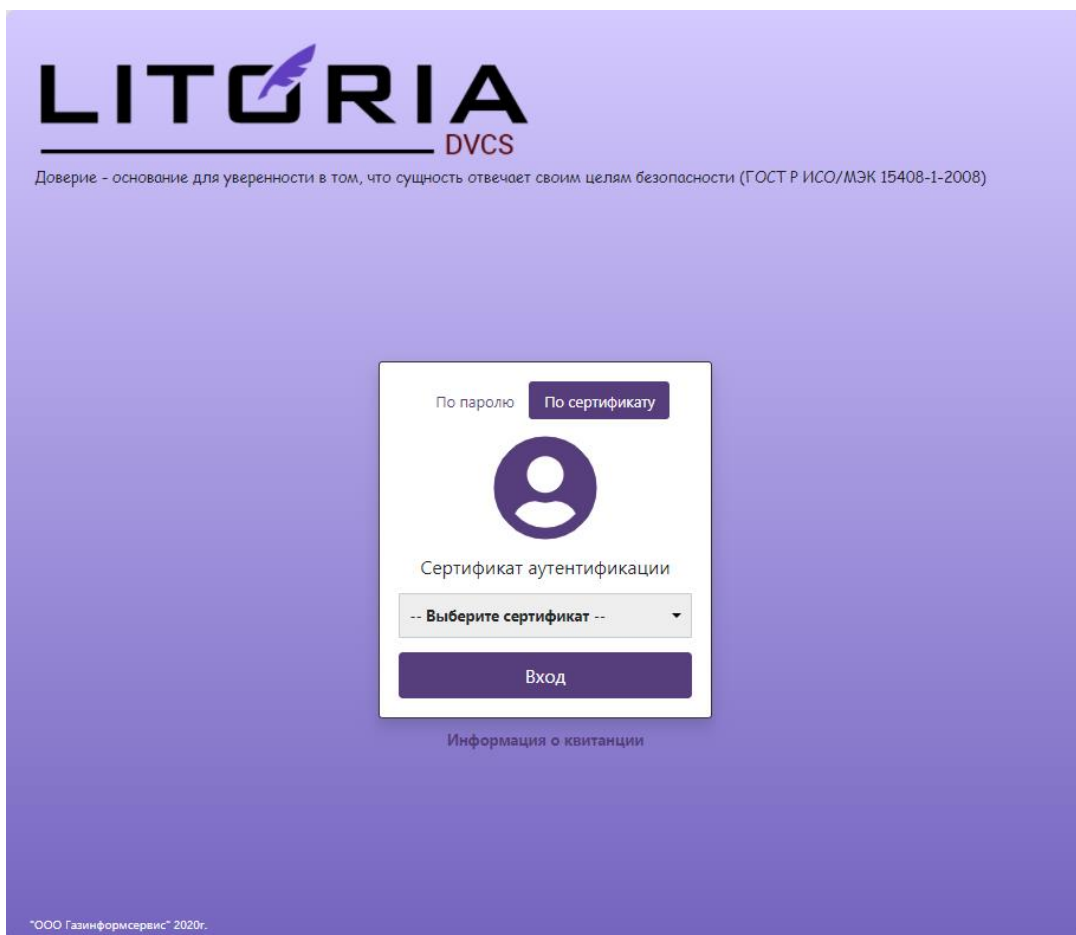


Рисунок 7 – Вход в web-кабинет по сертификату

- 4) Выберите сертификат для входа из списка сертификатов (рисунок 8) и нажмите на кнопку «Вход».

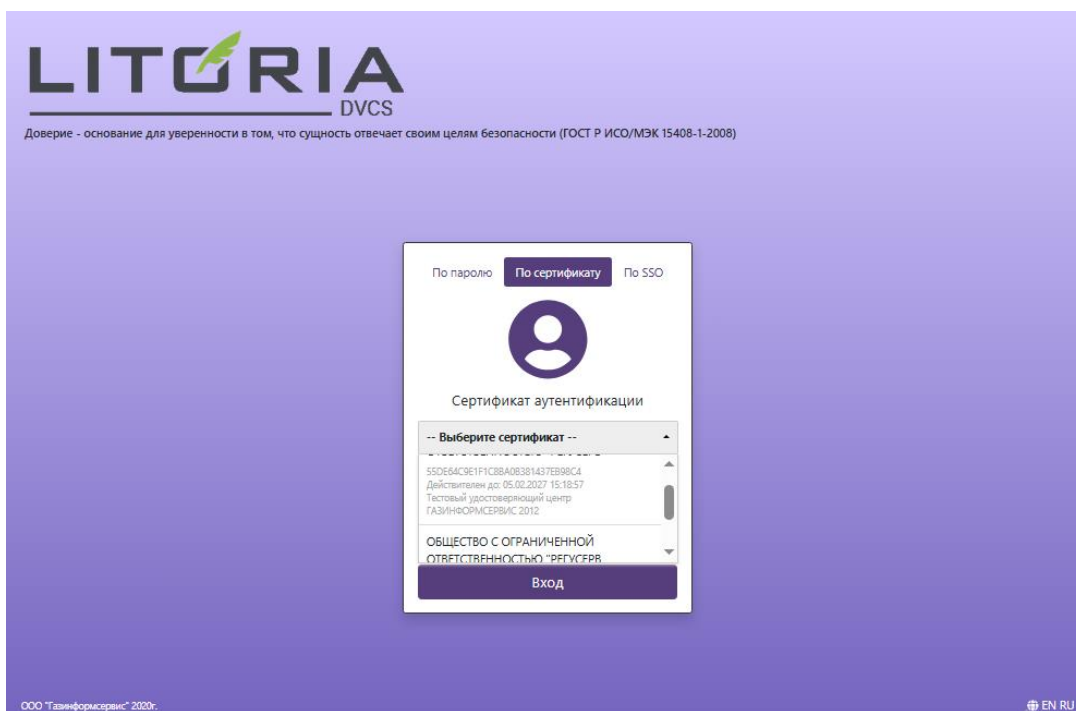


Рисунок 8 – Вход в web-кабинет по сертификату

Примечание. Если модуль «Litoria Auth» не установлен и не запущен, при попытке входа в web-кабинет ПК «Litoria DVCS» с использованием сертификата, вход пользователя не будет осуществлен (рисунок 9).

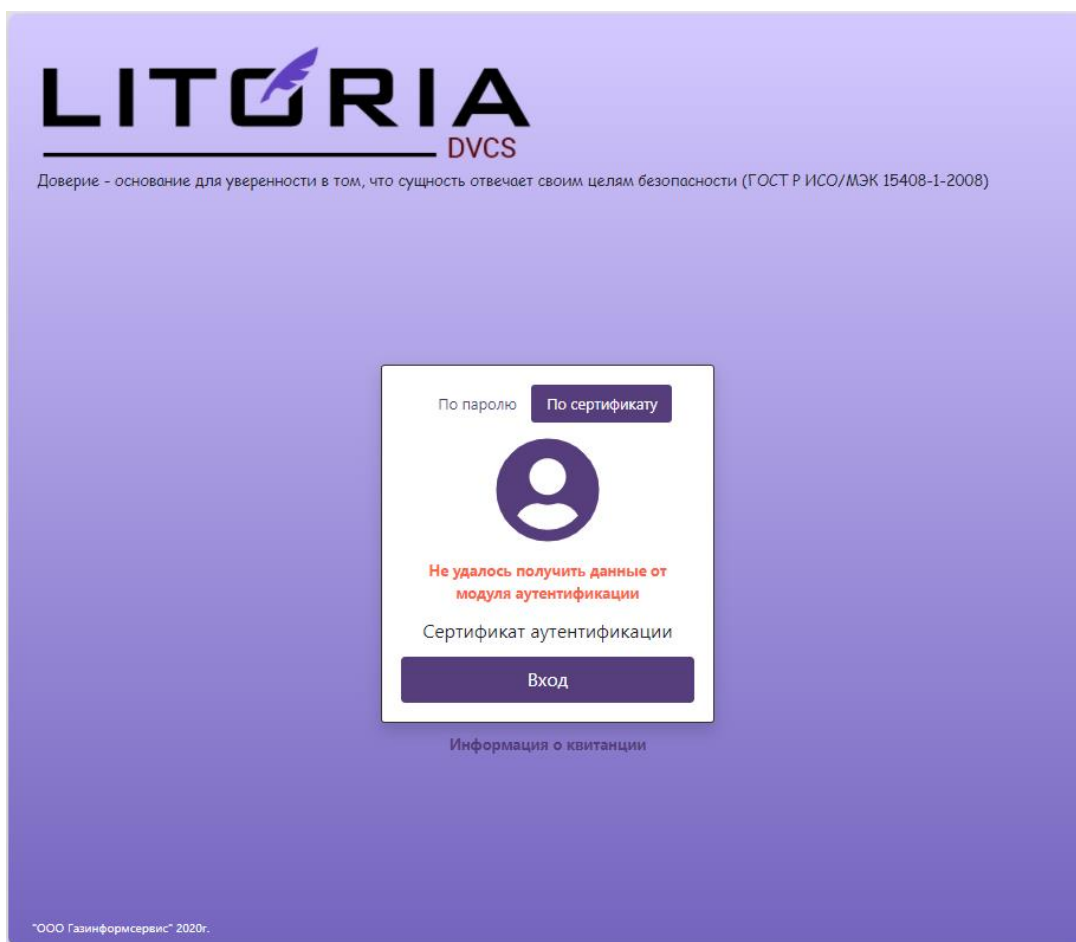


Рисунок 9 – Ошибка при попытке аутентификации по сертификату

- 5) В появившемся окне аутентификации СКЗИ введите пароль (ПИН-код от контейнера) и нажмите кнопку **«ОК»** (рисунок 10).

Примечание. При установке флага **«Сохранить пароль в системе»** аутентификация пользователя будет осуществляться без запроса пароля от контейнера.

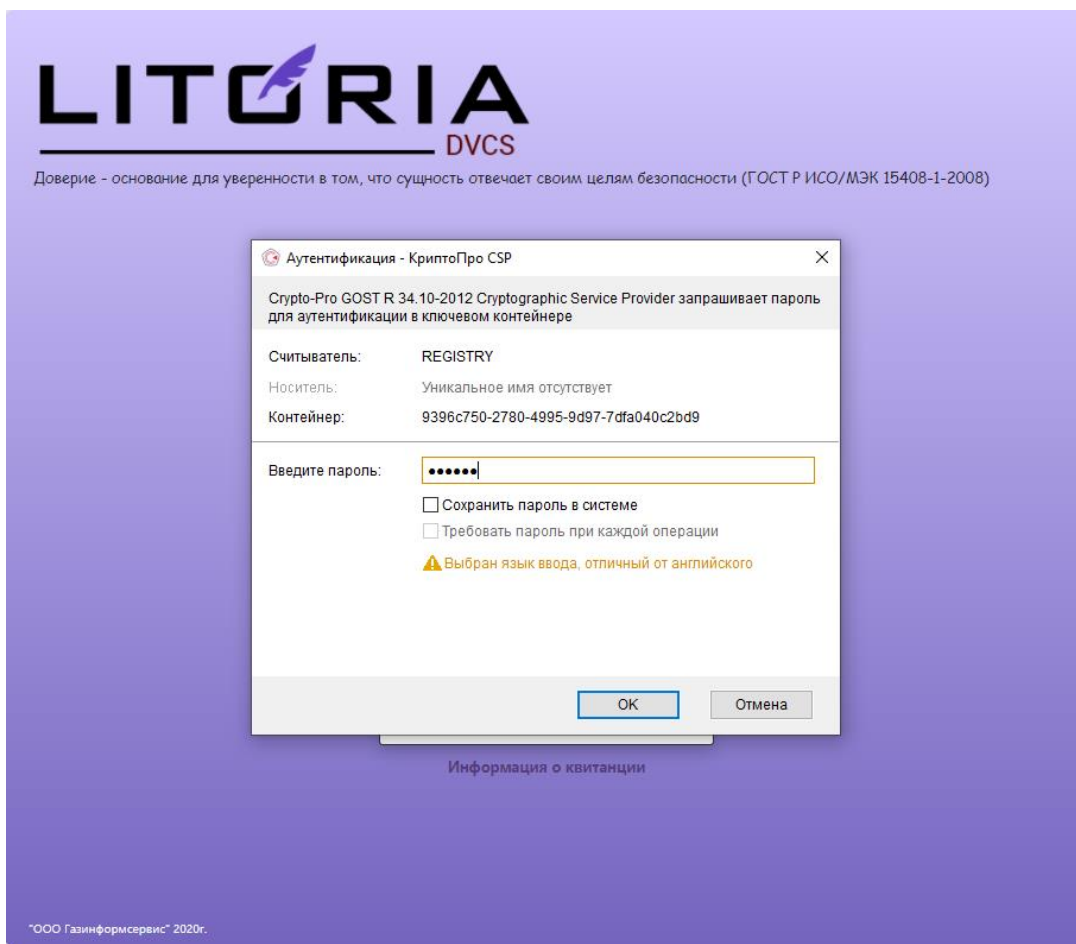


Рисунок 10 – Ввод пароля

Примечание. При вводе неверных данных для аутентификации, вход пользователя не будет осуществлен (рисунок 11).

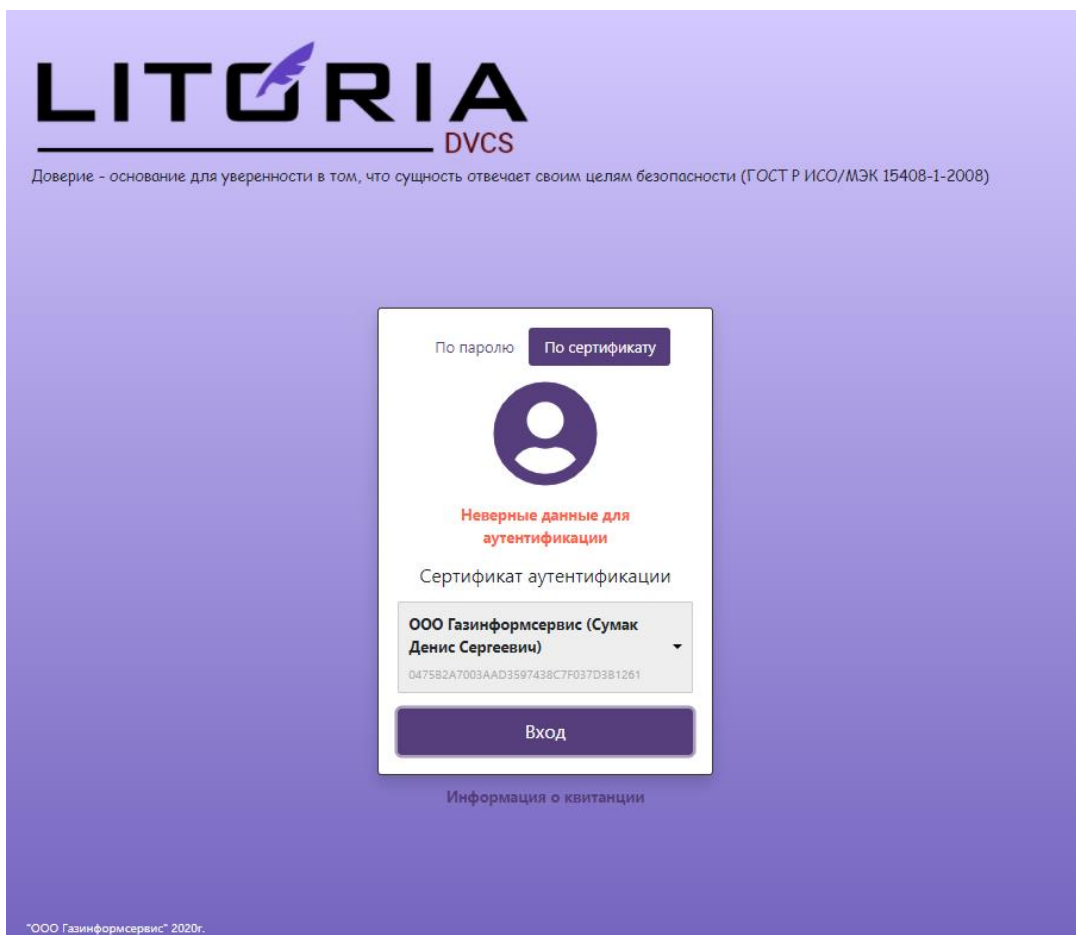


Рисунок 11 – Ввод пароля

4.1 Настройки файла конфигурации

Файл конфигурации предназначен для хранения настроек, связанных с функционированием модуля аутентификации.

Изменение настроек доступно в конфигурационном файле «appsettings.json», расположенном в директории установки модуля «Litoria Auth» по пути: C:\Program Files (x86)\GIS\Litoria Auth\auth (пример конфигурационного файла приведен в Приложении 1).

4.1.1 Настройки лог-файла

Лог-файл необходим для выяснения причин неработоспособности службы аутентификации. По умолчанию создание лог-файла выключено. Для изменения значения необходимо перейти к набору параметров для настройки ведения лога и установить в параметре «Logger»:

"None" – ведение лог-файла выключено;

"System" – в лог-файл пишутся только ошибки функционирования внутренней части веб-сайта;

"Both" – в лог-файл пишутся ошибки работы внутренней части веб-сайта и ядра;

и при необходимости изменить остальные параметры в соответствии с пояснениями к ним.

```
"FileLog": {  
  //Вести файловый лог  
  "Logger": "None",  
  //Название файла лога  
  "Path": "auth.txt",  
  //Возможность добавления  
  "Append": "True",  
  //Максимальный размер файла лога (байт)  
  "FileSizeLimitBytes": 0,  
  //Ротация файлов лога по достижению максимального размера  
  "MaxRollingFiles": 0  
}
```

4.1.2 Настройка использования сертификатов

По умолчанию для входа в web-кабинет «ПК «Litoria DVCS» служба аутентификации использует только сертификаты ГОСТ. Для возможности использовать все возможные сертификаты необходимо перейти к набору параметров для настройки сертификатов и установить нужный тип в параметре «*Certificates*»:

- "Gost" – используются только ГОСТ сертификаты;
- "All" – используются все сертификаты из хранилища Личные.

4.1.3 Настройка типа криптографического средства

По умолчанию в комплексе используется криптопровайдер «КриптоПро CSP». Для изменения криптопровайдера или добавления дополнительного необходимо указать в параметре «*Csp*» нужное значение:

"CryptoPro" – СКЗИ «КриптоПро CSP»;

"VipNet" – СКЗИ «VipNet CSP».

4.2 Двухфакторная аутентификация через REST API

Модуль REST API позволяет обращаться к следующим функциям «Litoria Auth» для возможности использовать двухфакторную аутентификацию при помощи цифрового сертификата при входе в web-кабинет ПК «Litoria DVCS».

- 1) Метод получения списка сертификатов – **GetCertificates**. Данный запрос позволяет выполнить поиск и получить список сертификатов из хранилища сертификатов «Личные». В качестве ответа возвращается список доступных сертификатов.

Content-Type: *application/json*

Метод: *GET*

URL: *http:///Api/GetCertificates*

JSON:

643.72410666.00081-01 95 01-03

```
{
  "commonName": " ",
  "serialNumber": " ",
  "notAfter": " ",
  "issuerInfo": " ",
  "index": " "
}
```

Параметр	Описание параметра
"commonName"	Общее имя сертификата
"serialNumber"	Серийный номер сертификата
"index"	Индекс в коллекции
"notAfter"	Срок окончания действия сертификата
"issuerInfo"	Название УЦ, выпустившего сертификат

Пример положительного ответа

```
[
  {
    "commonName": "EN  userrsa",
    "serialNumber": "55DADF82CFEB41B32A9B48F42D9FA4",
    "notAfter": "05.02.2027 15:18:57",
    "issuerInfo": " Тестовый удостоверяющий центр ГАЗИНФОРМСЕРВИС 2012\n",
    "index": 1
  },
  {
    "commonName": "administrator",
    "serialNumber": "55DADF4EE93DB0E68C054FE549259E",
    "notAfter": "12.02.2027 12:26:36",
    "issuerInfo": " Тестовый удостоверяющий центр ГАЗИНФОРМСЕРВИС 2012\n",
    "index": 2
  }
]
```

- 2) Метод получения подписи случайной последовательности. Запрос выполняет поиск сертификата в хранилище. Результатом выполнения операции являются данные подписи в формате Json.

Content-Type: *application/json*

Метод: *GET*

URL: *http:///Api/Auth?serialNumber={Sn}*

JSON:

```
{
  "signature": "",

```

```
"error": ""  
}
```

Параметр	Описание параметра
"signature"	Данные подписи
"error"	Ошибка, если есть

Пример положительного ответа

```
{  
  "signature":  
  "MIAGCSqGSIB3DQEHAgCAMIACAQExCTAHBgUrDgMCGjCABgkqhkiG9w0BBwGggCSABAIwY7MUs//aCAAAAAAAAAA  
KCCByowggcmMIIIGj6ADAgEAg9V2t906T2w5owFT+/IiceKJQamj3QZ+Lz/NqP6d0qnCxRBx0KZD/RhWv+h7vD  
IliDCzyGzwEujArBgsqhkiG9w0BCRACDDEcMBowGDAWBBSKkMoAVZWt6ga0ZXPdWD3ihpZ5VzANBgkqhkiG9w0  
BAQEFAASBgA5sfi1/WGIcd9epd9msVKAPASH5gEHhFEKevKt14M0s6/xlc4CqOVb7WPcqtzVCRX8BRHRiX1wds  
0J/NzG4U+eGfviaCGr12d8pUQKp8hncvFpp2YawDakq6UNQb4ikSsz78yzV0wyluK9YR3aCDebf34iI+nEYrjN  
Pns3zYDftAAAAAAAA",  
  "error": null  
}
```

Приложение 1

Конфигурационный файл службы аутентификации «*appsettings.json*»

```
{
  //Порт для работы сервиса
  "Urls": "http://*:23352",
  //Блок настроек логирования службы аутентификации
  "Logging": {
    "LogLevel": {
      // Лог службы аутентификации.
      "Default": "Information",
      // Лог райнтайма
      "Microsoft": "None"
    },
    //Набор параметров для настройки ведения лога
    "FileLog": {
      //Вести файловый лог
      "Logger": "None",
      //Название файла лога
      "Path": "auth.txt",
      //Возможность добавления
      "Append": "True",
      //Максимальный размер файла лога байт
      "FileSizeLimitBytes": 0,
      //Ротация файлов лога по достижению максимального рамера
      "MaxRollingFiles": 0
    }
  },
  "AllowedHosts": "*",
  "AuConfig": {
    //Сертификаты которые будут предложены для аутентификации
    "Certificates": "Gost",
    //Тип криптосредства для работы
    "Csp": "CryptoPro"
  }
}
```

Перечень сокращений

API	–	Application Programming Interface
CSP	–	Cryptographic Service Provider
DVCS	–	Data Validation and Certification Server
URL	–	Uniform Resource Locator
АРМ	–	Автоматизированное Рабочее Место
ОС	–	Операционная Система
ПК	–	Программный Комплекс
СКЗИ	–	Средство Криптографической Защиты Информации