ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«WEBGARD 2.0»

Инструкция пользователя по эксплуатации WebGard 2.0

АННОТАЦИЯ

Настоящий документ представляет собой руководство пользователей по эксплуатацииWebGard 2.0, а также способы решения типичных проблем, возникающих при работе программы.

Программное обеспечение «WebGard 2.0» предназначено для защиты информации, не относящейся к государственной тайне, от несанкционированного доступа в web-системах массового обслуживания и реализует разграничение доступа при обращении к web-ресурсам для web-приложений.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ТЕРМИНОВ

Перечень используемых сокращений и терминов представлен в таблице (Таблица 1).

Таблица 1 – Перечень используемых сокращений и терминов

Сокращение	Полное наименование
DVD-ROM	Digital Versatile Disc - Read-Only Memory (привод цифрового многоцелевого диска)
HTTP	Hyper Text Transfer Protocol (протокол передачи гипертекста)
SQL	Structured Query Language (язык структурированных запросов)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
БД	База данных
БД ЗИС	База данных защищаемой информационной системы
ЗИС	Защищаемая информационная система
КС	Контрольная сумма
НСД	Несанкционированный доступ
ОС	Операционная система
ПИН	Персональный идентификационный номер
ПО	Программное обеспечение
Пользователь	Пользователь программного обеспечения «WebGard 2.0»
Программа	Программное обеспечение «WebGard 2.0»
СУБД	Система управления базой данных
УЦ	Удостоверяющий центр
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ЭКСПЛУАТАЦИИ ПРОГРАММЫ

Вход в ЗИС через Программу может осуществляться двумя способами:

– аутентификация по логину и паролю;
– двухфакторная аутентификация.

1.1. Аутентификация пользователя по паролю

Для корректного функционирования Программы необходимо использовать браузер актуальной версии с поддержкой сценариев JavaScript.

Для входа в ЗИС по паролю необходимо ввести данные пользователя в поля: «Имя пользователя», «Пароль» (Рис. 1).

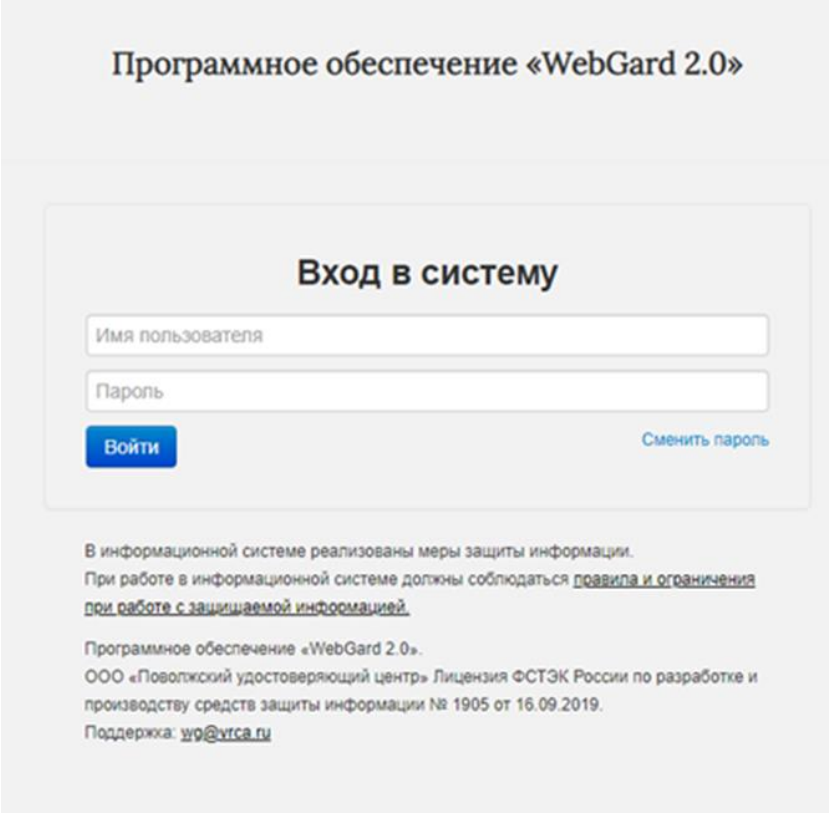

Рис. 1

В случае успешной попытки входа в ЗИС, открывается окно с сообщением об успешной аутентификации, датой и временем предыдущей успешной и неуспешной попытке аутентификации (Рис. 2).

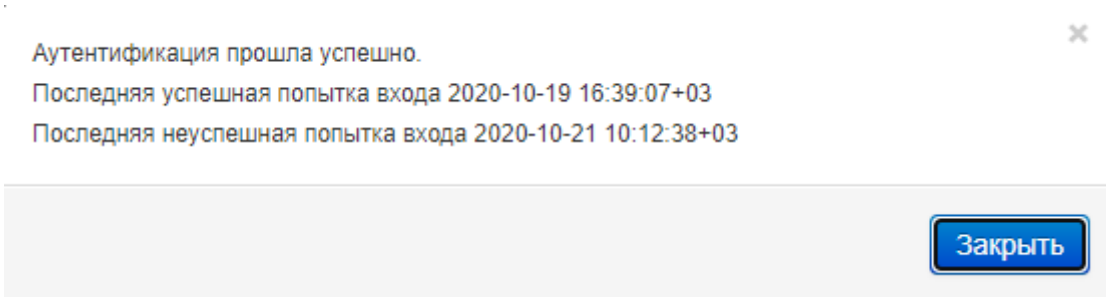

Рис. 2

В случае неуспешной попытки входа, Программа выводит ошибку «Неправильный логин и/или пароль» (Рис. 3).

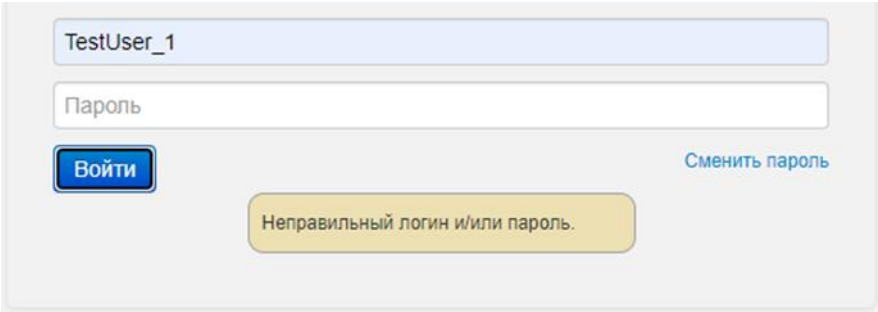

Рис. 3

Программа предупреждает пользователя, прошедшего аутентификацию, о времени истечения срока действия пароля. Период времени оповещения пользователя устанавливается администратором (Рис. 4).

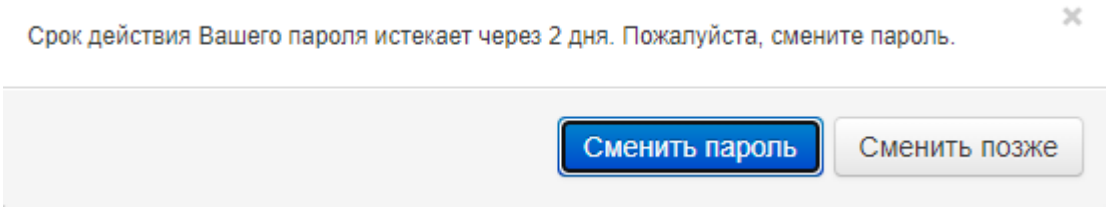

Рис. 4

Рекомендуется в течение данного периода изменить пароль на новый.

Также Программа после окончания срока действия пароля выводит другое сообщение (Рис. 5).

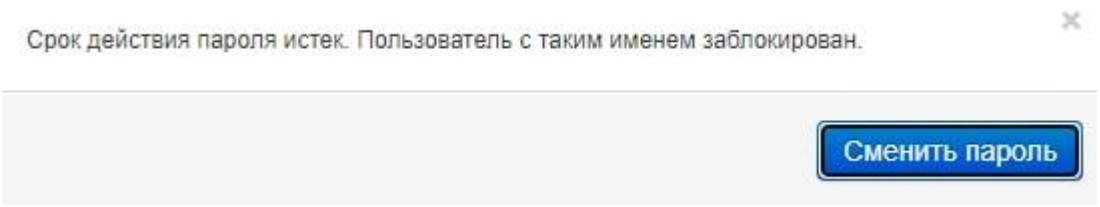

Рис. 5

В данном случае Программа требует изменить пароль пользователю. Пока пароль не будет изменен, пользователь не получит доступ к ЗИС.

Для смены пароля пользователю необходимо заполнить следующие поля: «Логин», «Текущий пароль», «Новый пароль» и «Подтверждение» (Рис. 6).

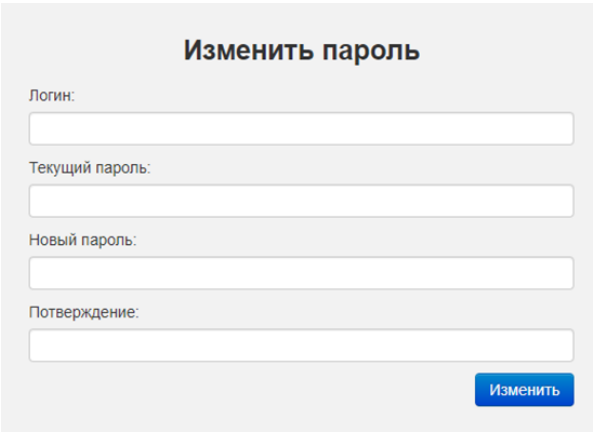

Рис. 6

1.2. Двухфакторная аутентификация пользователя

Для корректного функционирования двухфакторной аутентификации необходимо использовать браузер актуальной версии с поддержкой сценариев JavaScript и установленным плагином CryptoPro Extension for CAdES Browser Plug-in.

Двухфакторная аутентификация в Программе осуществляется с помощью смарт-карты или USB-идентификатора с записанным на нем сертификатом закрытого ключа, поддерживаемый сертифицированной версией КриптоПро CSP (Рис. 7).

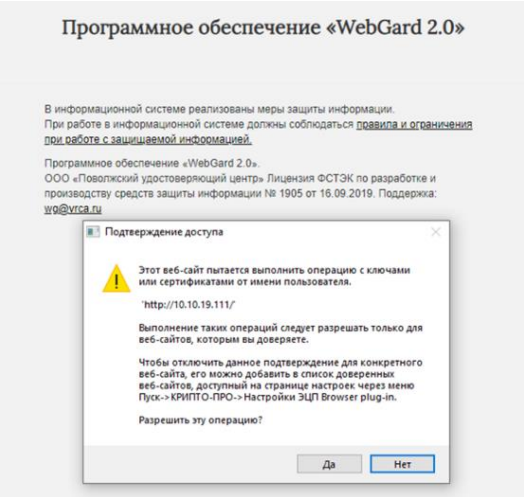

Рис. 7

После предъявления смарт-карты или USB-идентификатора Программа считывает данные и запрашивает ПИН-код.

В случае успешной попытки входа в ЗИС, открывается окно с сообщением об успешной аутентификации, датой и временем предыдущей успешной и неуспешной попытке аутентификации (Рис. 8).

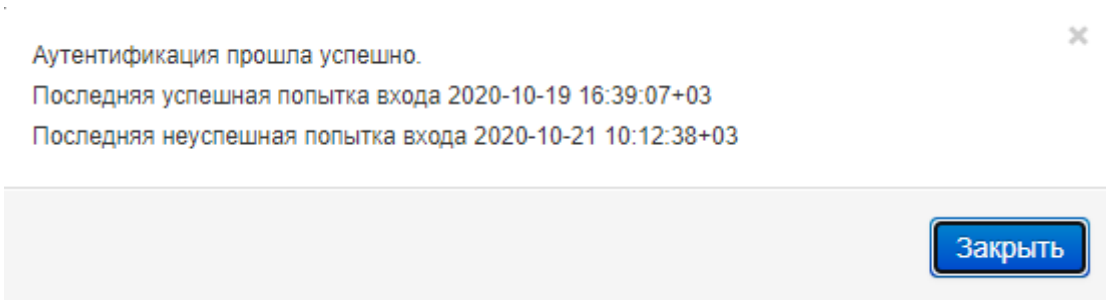

Рис. 8

Для реализации двухфакторной аутентификации необходимо соблюдение требований:

1) в защищаемой информационной системе должна быть реализована функция двухфакторной аутентификации;

1) в качестве смарт-карты и/или USB-идентификатора должна быть использована ESMART карта и/или USB-идентификатор, поддерживаемый КриптоПро CSP;

2) должен быть установлен плагин CryptoPro Extension for CAdES Browser Plug-in (при использовании USB-идентификатора) и/или ESMART Token Web Плагин (при использовании

3) поле e-mail до знака «@» (далее по тексту – аутентификационная информация) должно совпадать с логином пользователя в базе данных ПО «Webgard 2.0» и базе данных защищаемой информационной системы;

4) корневой сертификат удостоверяющего центра, выдавший сертификат пользователя, должен быть установлен на АРМ пользователя, сервер ПО «Webgard 2.0» и на сервере web-приложения защищаемой информационной системы.

1.3. Окно правил и ограничений при работе с защищаемой информацией

При нажатии на ссылку «правила и ограничения при работе с защищаемой информацией» откроется окно (Рис. 9).

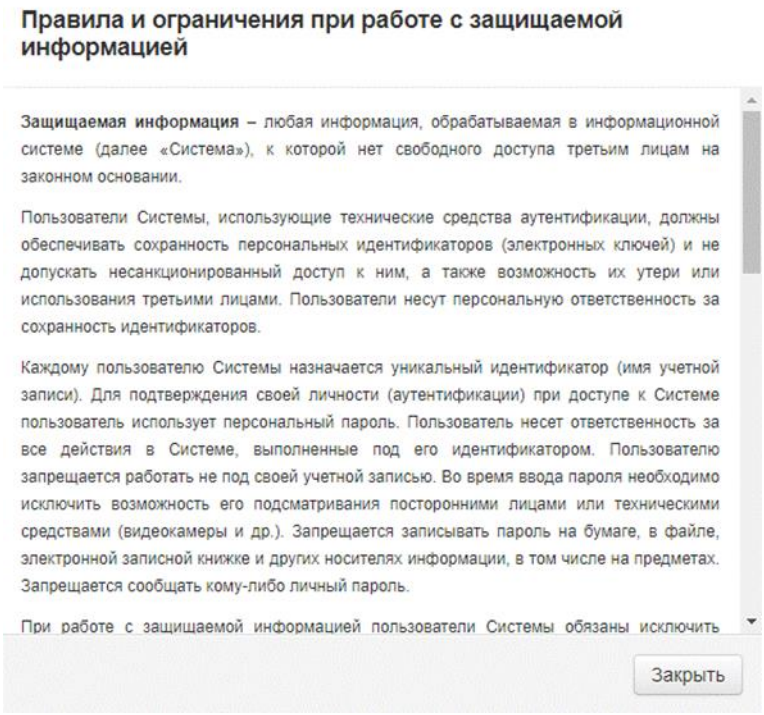

Рис. 9

В данном окне описаны правила и ограничения работы с Программой для пользователя.

1.4. Выход из Программы

Для выхода из Программы необходимо нажать кнопку «Выход». Пример кнопки «Выход» приведен на рисунке (Рис. 10).

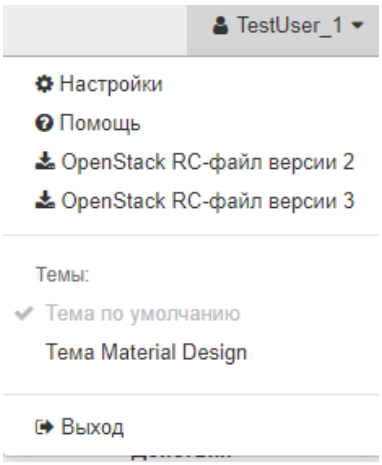

Рис. 10

В случае отсутствия в интерфейсе кнопки «Выход» необходимо ввести в адресной строке ip-адрес Программы и URL выхода `http://ip-адрес Программы/auth/logout`. Стандартным URL выхода является «/auth/logout» (Рис. 11).

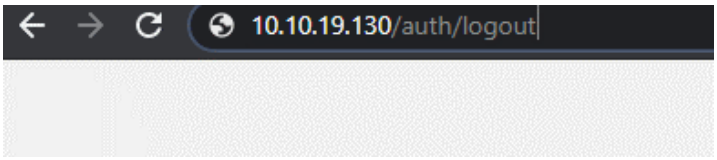

Рис. 11

После выполненных действий Программа завершит сессию пользователя и откроет страницу авторизации Программы (Рис. 12).

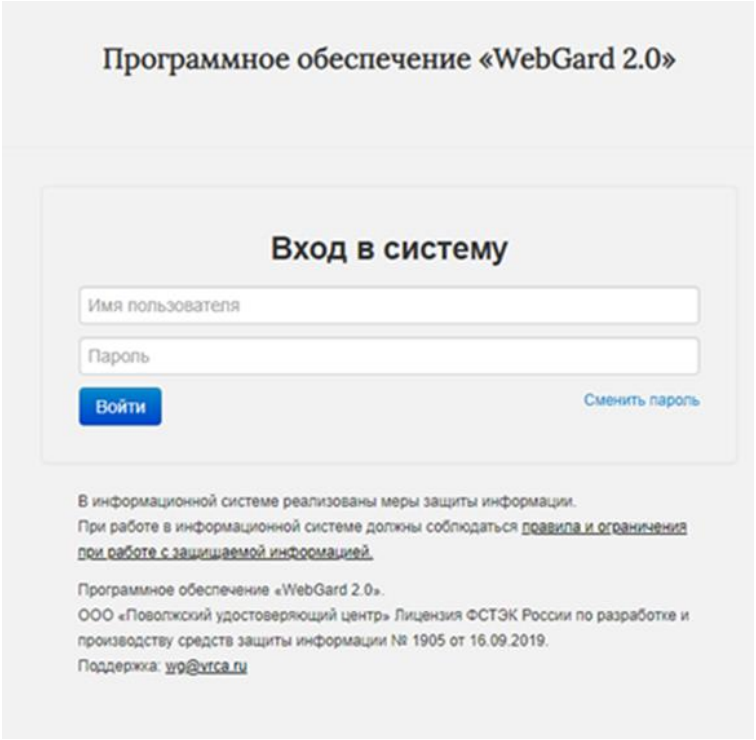
Программное обеспечение «WebGard 2.0»
Вход в систему
Имя пользователя
Пароль
Войти
Сменить пароль
В информационной системе реализованы меры защиты информации.
При работе в информационной системе должны соблюдаться правила и ограничения при работе с защищаемой информацией.
Программное обеспечение «WebGard 2.0».
ООО «Поволжский удостоверяющий центр» Лицензия ФСТЭК России по разработке и производству средств защиты информации № 1905 от 16.09.2019.
Поддержка: wg@vtca.ru

Рис. 12