ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«WEBGARD 2.0»

Инструкция пользователя по эксплуатации WebGard 2.0

Листов 26

2021

АННОТАЦИЯ

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

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

1. НАЗНАЧЕНИЕ 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.

1.1. Основные возможности Программы

Программа обеспечивает выполнение следующих функций безопасности по защите информации:

- идентификация и аутентификация (логин/пароль, двухфакторная, LDAP) пользователей защищаемых web-систем (ИАФ.1);
- идентификация и аутентификация администраторов Программы (ИАФ.1);
- управление идентификаторами (синхронизация, блокирование, предотвращение повторного использования) (ИАФ.3);
- управление средствами аутентификации (хранение, обновление, защита) пользователей web-систем (ИАФ.4);
- возможность изменения характеристик пароля (ИАФ.4);
- назначение механизмов аутентификации (ИАФ.4);
- защита аутентификационной информации (ИАФ.5);
- управление учётными записями (заведение, активация, блокирование, контроль, уничтожение) пользователей web-систем (УПД.1);
- оповещение администраторов об изменении привилегий пользователей и параметров Программы (путем формирования почтового сообщения) (УПД.1);
- управление учётными записями администраторов (УПД.1);
- разграничение доступа в соответствии с ролевой политикой безопасности (УПД.2);
- ограничение неуспешных попыток входа пользователей в защищаемую информационную систему (УПД.6);
- оповещение пользователя при входе в защищаемую информационную систему (УПД.7, УПД.8);
- ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя защищаемой информационной системы (УПД.9);
- блокирование (закрытие) сеанса доступа пользователя в защищаемую информационную систему при наступлении определенных событий (УПД.10);
- регистрация и защита информации о событиях безопасности пользователей web-систем (РСБ.1, РСБ.2);
- регистрация и защита информации о событиях безопасности администраторов Программы (РСБ.1, РСБ.2);
- сбор, запись и хранение информации о событиях безопасности (РСБ.3);
- предоставление администраторам возможности реагирования на сбои при регистрации событий безопасности (РСБ.4);

– предоставление возможности просмотра результатов регистрации событий безопасности (РСБ.5);

– защита информации о событиях безопасности (РСБ.7);

– разделение полномочий пользователей web-систем и администраторов Программы (разделение интерфейса пользователя и интерфейса администратора) (ЗИС.1);

– контроль вводимых данных для исключения ввода недопустимых символов (ОЦЛ.7);

– идентификация и аутентификация пользователей в интерфейсе управления виртуальной инфраструктурой (ЗСВ.1);

– управление доступом пользователей к интерфейсу управления виртуальной инфраструктурой (ЗСВ.2);

– регистрация событий безопасности в интерфейсе управления виртуальной инфраструктурой (ЗСВ.3);

– управление ресурсами виртуальной инфраструктуры через интерфейс управления виртуальной инфраструктурой (ЗСВ.6);

– фильтрация HTTP- запросов пользователей защищаемых web-систем;

– возможность автоматизированного внесения пользователей защищаемой информационной системы в список легитимных пользователей Программы.

Реализация выполнения функций безопасности обеспечивается в соответствии с:

– «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (приказ ФСТЭК России № 17 от 11.02.2013 г.) (далее по тексту - [1]);

– Методическим документом «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 г.);

– «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (приказ ФСТЭК России № 21 от 18.02.2013 г.) (далее по тексту - [2]).

Основные возможности Программы:

1) Обеспечивается идентификация и аутентификация пользователей, являющихся работниками оператора (ИАФ.1) [1,2]:

– идентификация и аутентификация пользователей с использованием паролей;

– идентификация и аутентификация администраторов с использованием паролей;

– при аутентификации по протоколу LDAP, выполнение запроса на аутентификацию пользователя в существующий сервер службы каталогов;

– возможность однозначного сопоставления идентификатора пользователя с выполняемыми от его имени запросами;

– многофакторная (двухфакторная) аутентификация пользователей для удаленного доступа в систему с использованием ESMART карт и/или USB-идентификатора, поддерживаемого сертифицированной версией КриптоПро CSP:

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования.

2) Установлены и реализованы функции управления идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3) [1,2]:

– присвоение идентификатора пользователя в Программе, который позволяет однозначно идентифицировать пользователя;

– предотвращение повторного использования идентификатора пользователя в Программе в течение установленного администратором периода времени;

– автоматическое блокирование идентификатора пользователя после установленного администратором времени неиспользования логина.

3) Установлены и реализованы функции управления средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4) [1,2]:

– предоставление возможности изменения аутентификационной информации.

– установление характеристик пароля, а именно:

а) установка минимальной и максимальной длины пароля в символах;

б) установка минимальной сложности пароля с определяемыми требованиями к регистру, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;

в) установка требования к алфавиту пароля;

г) установка максимального времени действия пароля;

– назначение характеристик механизмов аутентификации:

а) срок, в течение которого возможно сменить пароль;

б) время жизни аккаунта (логина);

в) время, которое будет ожидать пользователь перед следующей попыткой аутентификации;

г) время, по истечении которого сбрасывается счетчик неуспешных попыток аутентификации.

– обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной администратором;

– защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

4) Обеспечивается защита обратной связи при вводе аутентификационной информации (ИАФ.5) [1,2]:

– защита аутентификационной информации в процессе ее ввода для аутентификации путем сокрытия ее отображения условными знаками.

5) Установлены и реализованы функции управления (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1) [1,2]:

– в Программе установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

– наличие типов учетных записей (временная, внутренняя, внешняя и предустановленная);

- объединение учетных записей в группы при помощи ролей;
- заведение, активация, блокирование и уничтожение учетных записей пользователей;
- заведение и редактирование учетных записей администраторов;
- возможность редактирования учетных записей пользователей;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, полномочиях, ограничениях;
- предоставление администратору возможности блокирования и уничтожения временных учетных записей пользователей, предоставленных для ограниченного по времени выполнения задач в Программе;

– в Программе осуществляется автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования;

– в Программе осуществляется автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после окончания периода времени неиспользования, установленного администратором;

– в Программе осуществляется автоматическое блокирование учетных записей пользователей при превышении установленного администратором числа неуспешных попыток аутентификации пользователя.

6) Обеспечена реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2) [1,2]:

– ПО обеспечивает ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа (пользователей и администраторов) к объектам доступа (web-ресурсам и настройкам безопасности Программы) на основе ролей:

Примечание: Объектами доступа должны являться функции, для которых назначаются элементы защищаемых web-ресурсов. К каждому субъекту доступа (пользователь) должна назначаться роль с функциями, разрешенными к выполнению, при получении доступа к защищаемым web-ресурсам.

- в ПО выделяются роли пользователей и администраторов;
- для каждой пары (субъект – объект) в ПО должно быть задано явное и недвусмысленное перечисление допустимых http-запросов (GET, POST, OPTIONS, HEAD, PUT, DELETE, PATCH, ANY), т.е. для тех http-запросов, которые являются санкционированными для данного субъекта доступа к данному – объекту доступа;
- контроль доступа должен быть применим к каждому объекту и каждому субъекту;

– ПО обеспечивает управление доступом субъектов к защищаемым web-ресурсам при входе в Программу, и разграничивает доступ к следующим полномочиям:

- создание правил управления доступом (для каждой пары (субъект – объект) в ОО должно быть задано явное и недвусмысленное перечисление

допустимых http-запросов (GET, POST, OPTIONS, HEAD, PUT, DELETE, PATCH, ANY), т.е. для тех http-запросов, которые являются санкционированными для данного субъекта доступа к данному – объекту доступа);

- переход на защищаемый ресурс;
- редактирование правил управления доступом;
- удаление правил управления доступом;
- создание субъекта доступа;
- редактирование субъекта доступа;
- удаление субъекта доступа;
- синхронизация прав доступа;
- создание защищаемых ресурсов;
- редактирование защищаемых ресурсов;
- удаление защищаемых ресурсов;
- изменение привилегий учетных записей;
- вход (выход), а также попытки входа субъектов доступа в панель управления компонентами виртуальной инфраструктуры;
- изменение в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска и функционирования;
- изменение правил разграничения доступа к компонентам виртуальной инфраструктуры;
- размещение и перемещение файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);
- размещение и перемещение исполняемых виртуальных машин (контейнеров) между серверами виртуализации;
- размещение и перемещение данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

7) Обеспечивается ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6) [1,2]:

– в Программе обеспечивается автоматическое блокирование учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в Программу за установленный период времени.

8) Реализовано предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных правил обработки информации (УПД.7) [1,2]:

– обеспечивается предупреждение пользователя в виде сообщения («окна») о том, что в Программе реализованы меры защиты информации, а также о том, что при работе пользователем должны быть соблюдены установленные правила и ограничения на работу с информацией.

9) В Программе обеспечивается оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему (УПД.8) [1,2]:

– обеспечивается оповещение пользователя после успешного входа в Программу (завершения процесса аутентификации) о дате и времени предыдущего успешного и (или) неуспешного входа в Программу от имени этого пользователя, а также об успешности процесса аутентификации.

10) Обеспечивается ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы (УПД.9) [1,2]:

– выполняется ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя;

– предусмотрена возможность задавать ограничения на число параллельных (одновременных) сеансов (сессий) пользователей, основываясь на идентификаторах пользователей;

– для привилегированных учетных записей (администраторов) количество параллельных (одновременных) сеансов (сессий) от их имени не превышает 2;

– в случае попытки входа под учетной записью пользователя или администратора, для которых достигнуто максимальное значение допустимых параллельных сеансов, при успешной аутентификации пользователя или администратора выдается сообщение о превышении числа параллельных сеансов доступа;

– в Программе предусмотрены средства, позволяющие контролировать и отображать администратору число активных параллельных (одновременных) сеансов (сессий) для каждой учетной записи пользователей.

11) Обеспечивается блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10) [1,2]:

– обеспечивается блокирование (закрытие) сеанса доступа пользователя после установленного администратором времени его бездействия (неактивности) в Программе или по запросу пользователя;

– для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации;

– блокирование сеанса доступа пользователя в Программу сохраняется до прохождения им повторной идентификации и аутентификации.

12) Регистрируются события безопасности и сроки их хранения (РСБ.1) [1,2]:

– вход (выход), а также попытки входа субъектов доступа в защищаемую информационную систему;

– события, связанные с действиями от имени привилегированных учетных записей (администраторов):

- создание правил управления доступом;
- редактирование правил управления доступом;
- удаление правил управления доступом;
- создание субъекта доступа;
- редактирование субъекта доступа;
- удаление субъекта доступа;

- синхронизация прав доступа;
- события безопасности, связанные с действиями пользователей в Программе:
  - переход на защищаемый ресурс;
  - создание защищаемых ресурсов;
  - редактирование защищаемых ресурсов;
  - удаление защищаемых ресурсов;
- события безопасности, связанные с изменением привилегий учетных записей пользователей;
- обеспечивается хранение информации о зарегистрированных событиях безопасности.

13) Определен состав и содержание информации о событиях безопасности, подлежащих регистрации (РСБ.2) [1,2]. Для каждого события безопасности регистрируются:

- состав и содержание информации о действиях администраторов, включаемой в записи регистрации о событиях безопасности, обеспечена возможность регистрации:
  - имя субъекта, совершившего инициацию события безопасности;
  - ip-адрес хоста;
  - дата и время события безопасности;
  - тип выполненной операции;
  - результат совершения операции;
- состав и содержание информации о действиях пользователей, включаемой в записи регистрации о событиях безопасности, обеспечена возможность регистрации:
  - дата и время события безопасности;
  - ip-адрес хоста;
  - идентификатор пользователя;
  - имя субъекта, совершившего действие;
  - метод запроса;
  - унифицированный указатель ресурса;
  - выполненную функцию;
  - статус события;
  - параметры HTTP-запроса;
  - параметры тела HTTP-запроса;
- при регистрации входа (выхода) пользователей в Программу состав и содержание информации включает дату и время входа (выхода) в систему (из системы), результат попытки входа (успешная или неуспешная), идентификатор, предъявленный при попытке доступа, метод запроса и путь web-ресурса;
- при регистрации попыток удаленного доступа к защищаемой информационной системе состав и содержание информации включает дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа, метод запроса и путь web-ресурса.

14) Осуществляется сбор, запись и хранение информации о событиях безопасности в течение установленного времени (РСБ.3) [1,2]:

– выбор и просмотр администраторами событий безопасности из списка совершенных событий (фильтрация параметров);

– генерация (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, определенными в соответствии с параметрами регистрации;

– хранение информации о событиях безопасности.

15) Обеспечивается возможность реагирования на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (РСБ.4):

– обеспечивается возможность изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, запись поверх устаревших хранимых записей событий безопасности;

16) Осуществляется мониторинг (просмотр) результатов регистрации событий безопасности и реагирование на них (РСБ.5) [1,2]:

– обеспечивается возможность просмотра записей регистрации, в документации на ПО установлена периодичность анализа записей регистрации администратором.

17) Обеспечивается защита информации о событиях безопасности (РСБ.7) [1,2]:

– обеспечивается защита информации о событиях безопасности в Программе;

– доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администраторам Программы.

18) Реализовано разделение в Программе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы (ЗИС.1) [1,2]:

– в Программе обеспечено разделение функциональных возможностей по управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации (наличие выделенного интерфейса администрирования).

19) Обеспечивается контроль точности, полноты и правильности данных, вводимых в информационную систему (ОЦЛ.7) [1,2]:

– контроль точности, полноты и правильности данных, вводимых (email, дата, числовые значения настроек безопасности) в Программу. Обеспечивается путем установления и проверки соблюдения форматов ввода данных, (допустимые наборы символов, размерность, область числовых значений, допустимые значения, количество символов) для подтверждения того, что ввод информации соответствует заданному администратором формату и содержанию.

20) Обеспечивается идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1) [1,2]:

– идентификация и аутентификация администраторов управления средствами виртуализации;

– идентификация и аутентификация субъектов доступа при удалённом обращении к объектам доступа в виртуальной инфраструктуре;

– блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;

– защита аутентификационной информации субъектов доступа от неправомерного доступа к ней, уничтожения или модифицирования;

– защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;

– идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения элементов виртуальной инфраструктуры.

21) Установлены и реализованы следующие функции управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2) [1,2]:

– контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;

– контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;

– управление доступом к виртуальному аппаратному обеспечению защищаемого ресурса, являющимся объектом доступа;

– обеспечение доступа к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания образов, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры;

– обеспечение доступа к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры.

22) Обеспечивается регистрация событий безопасности в виртуальной инфраструктуре, (ЗСВ.3) [1,2]:

– запуск (завершение) работы компонентов виртуальной инфраструктуры;

– доступ субъектов доступа к компонентам виртуальной инфраструктуры;

– изменение в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска и функционирования;

– изменение правил разграничения доступа к компонентам виртуальной инфраструктуры.

23) Обеспечено управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных (ЗСВ.6) [1,2]:

– управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);

– управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации;

– управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных);

– полный запрет перемещения виртуальных машин (контейнеров);

– ограничение перемещения виртуальных машин (контейнеров) в пределах защищаемой информационной системы (сегмента защищаемой информационной системы.

Дополнительные основные возможности:

24) Фильтрация HTTP - запросов, поступающих в защищаемую web-систему:

– фильтрация запросов, поступающих в защищаемую систему по протоколу HTTP;

– фильтрация запросов по режимам (все запрещено, все разрешено).

25) Обеспечивается возможность автоматизированного занесения данных пользователей (аутентификационных данных) защищаемой информационной системы в базу данных Программы.

1.2. Ограничения, накладываемые на область применения Программы

Программу предполагается использовать как элемент защиты государственных информационных систем и информационных систем персональных данных.

Программа может быть использована в автоматизированных системах до класса защищенности 1Г включительно, в информационных системах персональных данных до 1 уровня включительно и в государственных информационных системах до класса К1 включительно.

Реализация функций безопасности Программы протестирована на следующих web-серверах:

– Apache HTTP Server;

– nginx;

– IIS;

– lighttpd;

– litespeed.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Программа включает в себя следующие подсистемы:

- подсистема администрирования;
- подсистема HTTP фильтрации;
- подсистема хранилища данных СУБД PostgreSQL;
- подсистема кэширования данных.

Для выполнения Программой всех заявленных функций необходимо использовать ОС «Альт 8 СП» ЛКНВ.11100-01.

Минимальные характеристики технических средств, используемых для функционирования Программы:

- процессор: 2 ядра, 2,4 ГГц;
- оперативная память: от 4 ГБ;
- жёсткий диск: от 250 ГБ;
- сеть: Ethernet-интерфейс со скоростью 1 Гбит/с, 2шт.;
- DVD-ROM.

Окружение, в котором предполагается функционирование Программы, состоит из следующих компонентов:

- Java 9;
- gnu tar, gzip;
- СУБД PostgreSQL 12;
- Apache Tomcat/9.0.13.

Для проверки требований по защите среды виртуализации используется платформа виртуализации под управлением ПО OpenStack с графическим интерфейсом администрирования Horizon и/или ПО AccentOS и гипервизор из состава сертифицированной ОС.

Для выполнения Программой всех заявленных функций, необходимо соблюдение следующих организационных мер:

- прохождение обучения сотрудников, допускаемых к работе с Программой, и ознакомление их с эксплуатационной документацией;
- наличие администратора (или службы) защиты информации, ответственного за функционирование, а также контроль работы Программы;
- осуществление физической охраны информационных систем персональных данных (устройств и носителей информации), предусматривающее контроль доступа посторонних лиц в помещения с установленной информационной системой персональных данных, наличие надежных препятствий для несанкционированного проникновения в указанные помещения и хранилище носителей информации, особенно в нерабочее время;
- осуществление учета всех защищаемых носителей информации с помощью их маркировки с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);

– обеспечение возможности восстановления используемых средств защиты персональных данных, предусматривающая ведение двух копий каждого средства защиты, их периодическое обновление и контроль работоспособности.

2.1. Эксплуатационные ограничения

При эксплуатации Программы должны быть выполнены следующие ограничения:

26) отсутствие каких-либо сторонних сетевых маршрутов в настройках Программы и в установленных ОС;

27) подключение к ЗИС должно быть организовано только через ПО «WebGard 2.0», сторонние сетевые подключения через другие технические средства должны отсутствовать (в том числе виртуальные);

28) использование Программы предполагается только на следующих портах:
– 80;
– 5432;
– 11211
– 8080;
– 9009;
– 9010;
– 9011.

29) необходимо устранить уязвимости среды функционирования Программы посредством установки актуальных обновлений безопасности;

30) доступ к аутентификационной информации (в том числе хэшам паролей) Программы должен предоставляться только доверенному списку администраторов.

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача Программы – защита информации, не относящейся к государственной тайне, от несанкционированного доступа в web-системах массового обслуживания, реализация разграничения доступа при обращении к web-ресурсам для web-приложений.

Для реализации функции защиты информации от несанкционированного доступа Программа реализует ролевое управление доступом. Ролевое управление доступом является основным механизмом обеспечения конфиденциальности, целостности и доступности объектов многопользовательской системы. Конфиденциальность и целостность информации обеспечивается путем запрещения обслуживания неавторизованных пользователей.

Осуществление ролевого управления доступом предусматривает выполнение следующих функций:

- выполнение аутентификации и авторизации субъектов доступа;
- регистрация и учет действий, выполняемых субъектами доступа в защищаемой системе;
- фильтрация http-запросов.

Для осуществления ролевого управления доступом определяется множество допустимых функций для каждой пары «роли» – «функции», а также производится контроль выполнения правил вызова функций http-webguard (фильтр запросов). Описание функций содержится в базе данных Программы и включает в себя следующую информацию:

- наименование функции;
- URL;
- тип запроса;
- тип функции;
- перечень входных параметров.

3.1. Обработка http-запросов

Обработка http-запросов Программой включает в себя выполнение следующих этапов:

- прием http- запросов по протоколу HTTP;
- выполнение аутентификации субъектов доступа;
- авторизация субъектов доступа;
- при успешной авторизации – выполнение операций в http-webguard;
- регистрация запроса и результатов авторизации для запрошенной операции;
- фильтрация http-запросов субъектов доступа;
- аудит http-запросов.

3.2. Аутентификация и авторизация субъектов доступа

При входе в систему производится идентификация и проверка подлинности субъектов доступа по паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов и имеющим минимум 2 цифры и 2 буквы.

Идентификация объектов доступа производится по их именам.

Контроль доступа субъектов к объектам доступа осуществляется на основе проверки у них необходимых прав доступа в соответствии с матрицами доступа «роль» – «функция», «роль» – «запрос».

3.3. Регистрация и учет действий субъектов доступа

Программа позволяет осуществлять сбор и накопление информации о событиях, происходящих в Программе. События подразделяются на внутренние (аудит действий в администрировании безопасности) и внешние (аудит действий пользователя). В процессе регистрации и учета реализуются следующие задачи:

- обеспечение подотчетности субъектов доступа;
- обеспечение возможности реконструкции последовательности событий;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

События безопасности, регистрирующиеся в Программе:

31) вход (выход), а также попытки входа субъектов доступа в защищаемую информационную систему;

32) события, связанные с действиями от имени привилегированных учетных записей (администраторов):

- создание объекта доступа;
- редактирование объекта доступа;
- удаление объекта доступа;
- создание субъекта доступа;
- редактирование субъекта доступа;
- удаление субъекта доступа;
- синхронизация прав доступа;

33) события безопасности, связанные с действиями пользователей:

- переход на ресурс в защищаемой информационной системе;
- создание ресурсов защищаемой информационной системы;
- редактирование ресурсов защищаемой информационной системы;
- удаление ресурсов защищаемой информационной системы;
- просмотр объектов базы данных защищаемой информационной системы;
- создание объектов базы данных защищаемой информационной системы;
- редактирование объектов базы данных защищаемой информационной системы;
- удаление объектов базы данных защищаемой информационной системы;

34) события безопасности, связанные с изменением привилегий учетных записей пользователей.

В Программе обеспечивается хранение информации о зарегистрированных событиях безопасности.

Состав и содержание информации, включаемой в регистрацию о событиях безопасности (администраторов):

- имя субъекта, совершившего инициацию события безопасности;
- ip-адрес хоста;
- тип объекта доступа;
- дата и время события безопасности;
- тип выполненной операции;
- результат совершения операции.

Состав и содержание информации, включаемой в регистрацию о событиях безопасности (пользователя):

- дата и время события безопасности;
- ip-адрес хоста;
- идентификатор пользователя;
- имя субъекта, совершившего действие;
- метод запроса;
- унифицированный указатель ресурса;
- выполненную функцию;
- статус события.

4. ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ЭКСПЛУАТАЦИИ ПРОГРАММЫ

Вход в ЗИС через Программу может осуществляться двумя способами:

– аутентификация по логину и паролю;
– двухфакторная аутентификация.

4.1. 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).

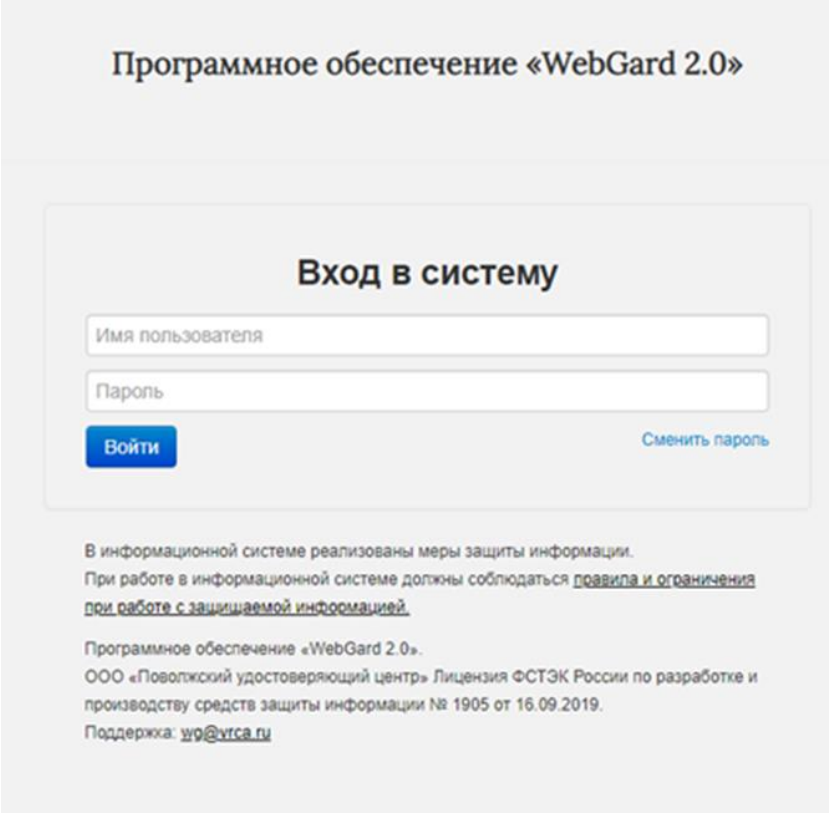

Рис. 1

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).

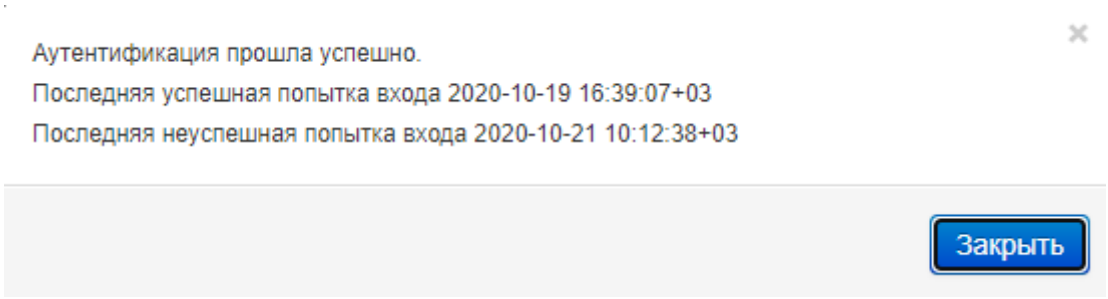

Рис. 2

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

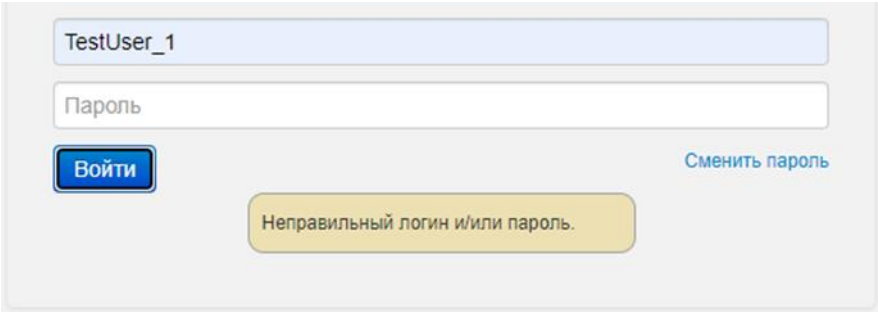

Рис. 3

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

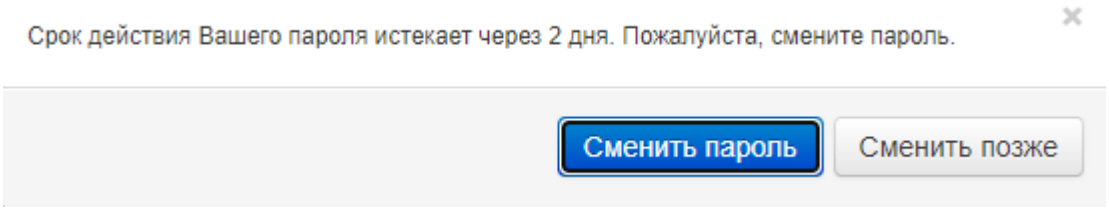

Рис. 4

Рекомендуется в течение данного периода изменить пароль на новый.

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

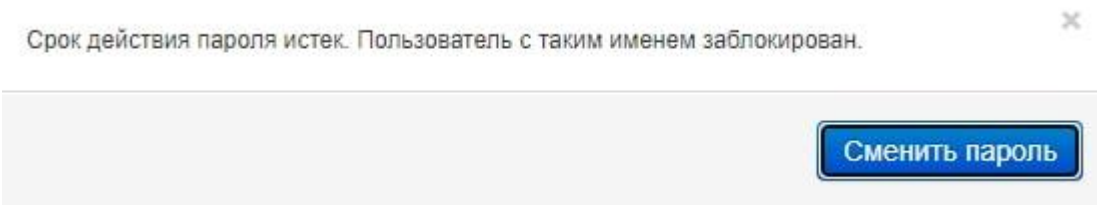

Рис. 5

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).

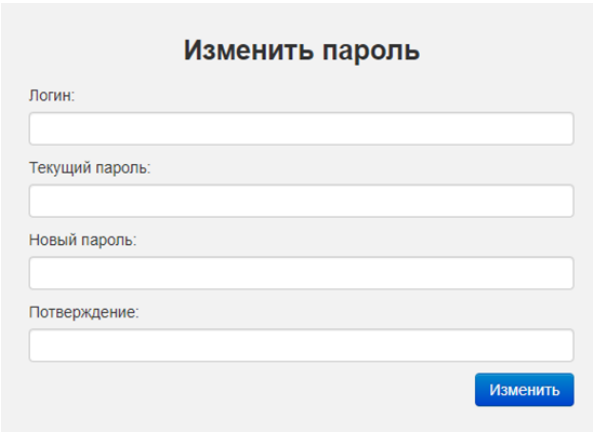

Рис. 6

4.2. 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).

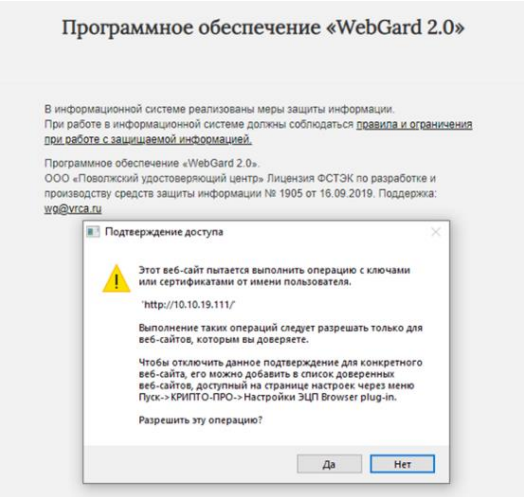

Рис. 7

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).

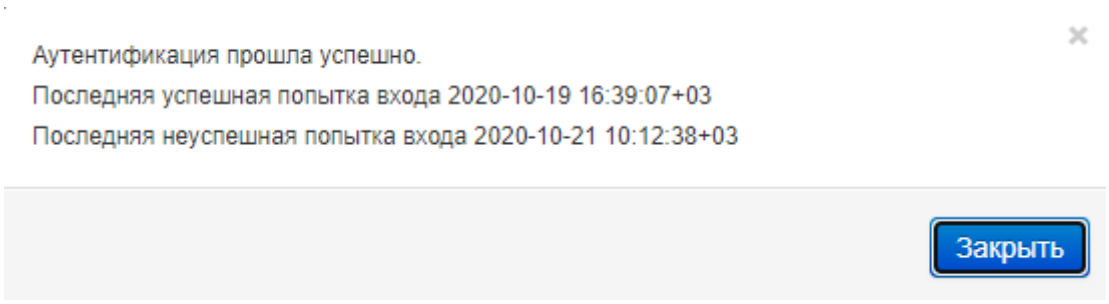

Рис. 8

Для реализации двухфакторной аутентификации необходимо соблюдение требований:

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

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

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

38) 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;

39) 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.

4.3. 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).

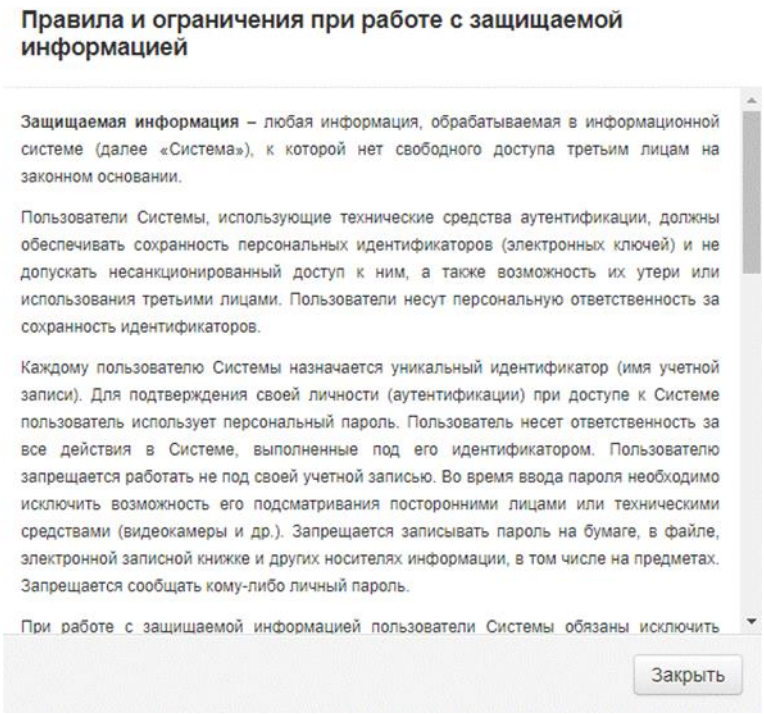

Рис. 9

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

4.4. Выход из Программы

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

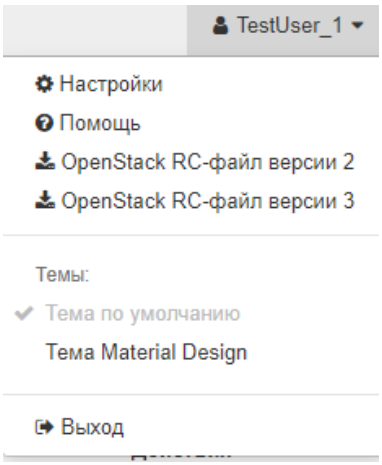

Рис. 10

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).

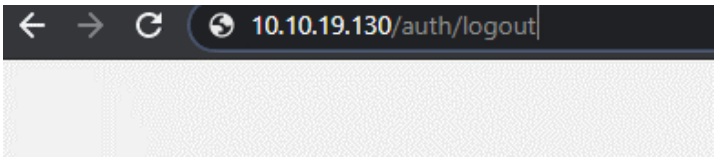

Рис. 11

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

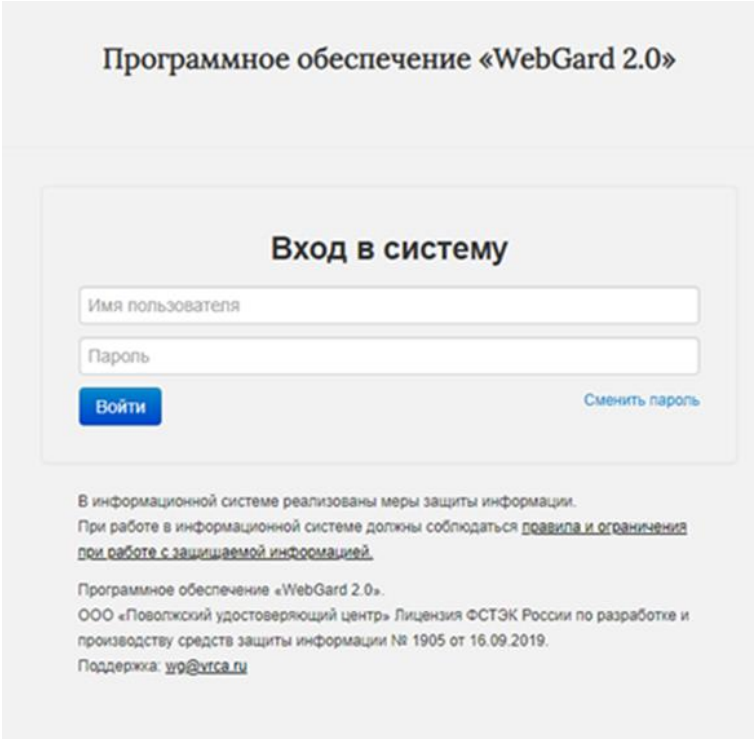
Программное обеспечение «WebGard 2.0»
Вход в систему
Имя пользователя
Пароль
Войти
Сменить пароль
В информационной системе реализованы меры защиты информации.
При работе в информационной системе должны соблюдаться правила и ограничения при работе с защищаемой информацией.
Программное обеспечение «WebGard 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