ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«WEBGARD 2.0»

Руководство администратора

2023

АННОТАЦИЯ

Настоящий документ предназначен для администраторов, руководителей служб и отделов по защите информации, аттестационных центров, а также всех заинтересованных специалистов в области защиты информации и представляет собой руководство администратора программного обеспечения «WebGard 2.0». В нем приведены описание функционала и работы 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
CD	Compact Disc (Компакт-диск)
DVD-ROM	Digital Versatile Disc - Read-Only Memory (привод цифрового многоцелевого диска)
HTTP	Hyper Text Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hyper Text Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования в целях повышения безопасности)
JDBC	Java Data Base Cennectivity (соединение с базами данных на Java)
JSON	JavaScript Object Notation (текстовый формат обмена данными, основанный на JavaScript)
SQL	Structured Query Language (язык структурированных запросов)
URI	Uniform Resource Identifier (унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
БД	База данных
БД ЗИС	База данных защищаемой информационной системы
ЗИС	Защищаемая информационная система
КС	Контрольная сумма
НСД	Несанкционированный доступ
ОС	Операционная система
ПО	Программное обеспечение
ПИН	Персональный идентификационный номер
Программа	Программное обеспечение «WebGard 2.0»
СУБД	Система управления базой данных
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

Программное обеспечение «WebGard 2.0» предназначено для защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, от несанкционированного доступа в web-системах массового обслуживания и реализует разграничение доступа при обращении к web-ресурсам для web-приложений.

Объект доступа – web-ресурс защищаемой информационной системы, доступ к которой регламентируется ролевой политикой доступа, реализуемой с помощью ПО «WebGard 2.0».

Защищаемая информационная система – информационная система (web-система), предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности, для защиты которой используется ПО «WebGard 2.0», устанавливаемое для контроля и разграничения доступа подключаемых пользователей при обращении к web-ресурсам для web-приложений.

Субъект доступа – пользователи, выполняющие операции (действия) над объектами доступа, действия которых регламентируются правилами разграничения доступа. Пользователи должны быть представлены двумя категориями – 1) пользователи защищаемой системы, 2) администраторы ПО «WebGard 2.0».

Операции – действия субъектов доступа над объектами доступа:

- вход (выход), а также попытки входа субъектов доступа в Программу;
- создание правил управления доступом;
- редактирование правил управления доступом;
- удаление правил управления доступом;
- создание субъекта доступа;
- редактирование субъекта доступа;
- удаление субъекта доступа;
- синхронизация прав доступа;
- переход на защищаемый ресурс;
- 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).

Перечень подсистем ПО «WebGard 2.0», реализующих функции безопасности:

– подсистема администрирования;
– подсистема HTTP-фильтрации.

Перечень внешних пакетов, необходимых для функционирования ПО «WebGard 2.0»:

– пакет подсистемы хранилища данных СУБД PostgreSQL;
– пакет подсистемы кэширования данных.

Внешние подсистемы не поставляются в составе ПО «WebGard 2.0». Внешние подсистемы устанавливаются с репозитория сертифицированной ОС «Альт 8 СП».

Руководство администратора Программы определяет требования и ответственность администратора, а также последовательность действий, обеспечивающие выполнение Программы.

В документе представлено графическое описание Программы и настройка необходимых элементов для ее функционирования.

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 неправомерного 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.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Для выполнения Программой всех заявленных функций, необходимо использовать операционную систему ОС «Альт 8 СП».

Окружение, необходимое для функционирования Программы, состоит из следующих компонентов:

– Java 9;
– gnu tar, gzip;
– СУБД PostgreSQL 12;
– Apache Tomcat/9.0.59.

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;
– DVD-ROM.

Реализация функций безопасности Программы протестирована на следующих web-серверах:

– Apache HTTP Server;
– nginx;
– IIS;
– lighttpd;
– litespeed.

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:

1) отсутствие каких-либо сторонних маршрутов в настройках Программы;

2) 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);

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

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

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

6) доступ к установке и запуску программ на серверах, где устанавливается ПО «WebGard 2.0», должен предоставляться только доверенному пользователю (администратору);

7) параметр регистронезависимости должен быть настроен до использования Программы и не должен изменяться во время эксплуатации Программы. Данный параметр запрещено изменять во время эксплуатации.

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача Программы – защита информации, не относящейся к государственной тайне, от несанкционированного доступа в web-системах массового обслуживания и 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 подсистемы фильтрации. 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 подсистеме фильтрации;
– 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 Программу 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 (1 верхнего регистра, 1 нижнего регистра).

При создании пользователя в подсистеме администрирования Программа осуществляет хэширование пароля пользователя, используя одну из выбранных хэш-функций:

- md4;
- md5;
- bcrypt;
- pbkdf2_sha256;
- sha-1;
- sha-256;
- sha-512.

При автоматической синхронизации пользователя и аутентификации пользователя в подсистеме фильтрации Программа осуществляет хэширование пароля пользователя, используя одну из выбранных хэш-функций:

- md4;
- md5;
- bcrypt;
- pbkdf2_sha256;
- sha-1;
- sha-256;
- sha-512;
- ssha-1;
- ssha-512;
- ntlm.

Идентификация субъектов 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 (подсистема администрирования)) и внешние (аудит действий пользователя (подсистема фильтрации)). 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:

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

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

– вход/выход администраторов;
– создание объекта доступа;
– редактирование объекта доступа;
– удаление объекта доступа;
– создание субъекта доступа;
– редактирование субъекта доступа;
– удаление субъекта доступа;
– синхронизация прав доступа;

3) 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;

4) 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. ОБРАЩЕНИЕ К ПРОГРАММЕ

4.1. Вход в подсистему администрирования

Для входа в подсистему администрирования необходимо открыть браузер и ввести адрес сервера. Подсистема администрирования доступна по адресу: http://localhost:8080/security-manager/login.htm (localhost – ip-адрес системы, на котором установлена подсистема администрирования Программы). Появится окно авторизации, ввести выданный логин и пароль, нажать кнопку «Войти» (Рис. 1).

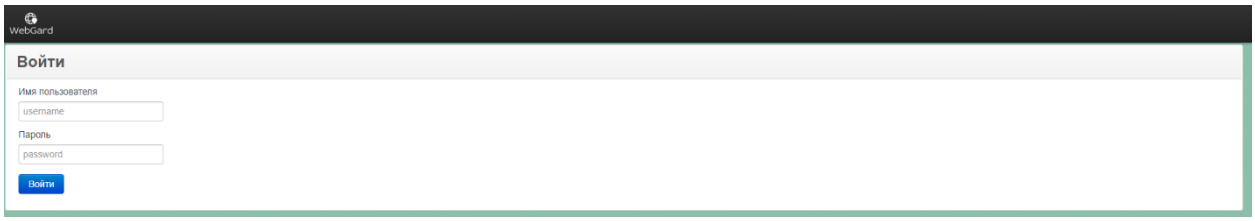

Рис. 1

4.2. Вкладка «Ресурсы»

По умолчанию после авторизации осуществляется переход на форму вкладки «Ресурсы» (Рис. 2).

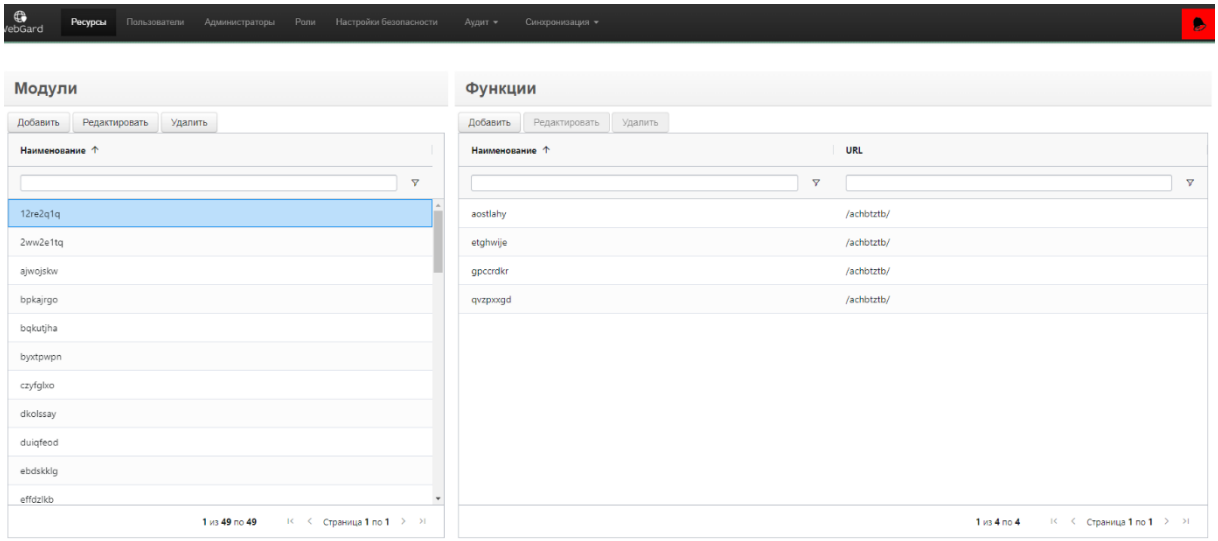

Рис. 2

В данной форме осуществляется управление ресурсами HTTP-фильтра.

Вкладка HTTP разделена на две области: в левой представлен список наименований модулей, в правой – наименования функций, относящихся к тому или иному модулю. На панели управления представлены кнопки управления (Добавить, Редактировать, Удалить). Для каждого модуля отображаются следующие данные: наименование модуля, наименование и URL функции этого модуля (Рис. 3).

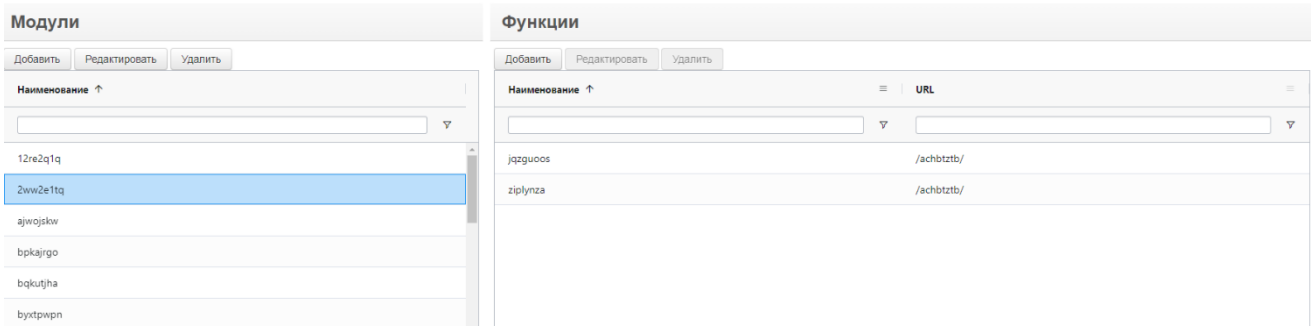

Рис. 3

4.2.1. Создание нового модуля

Для создания нового модуля следует нажать на кнопку добавления нового модуля в левой части экрана (Рис. 4).

Рис. 4

Далее открывается форма создания модуля (Рис. 5).

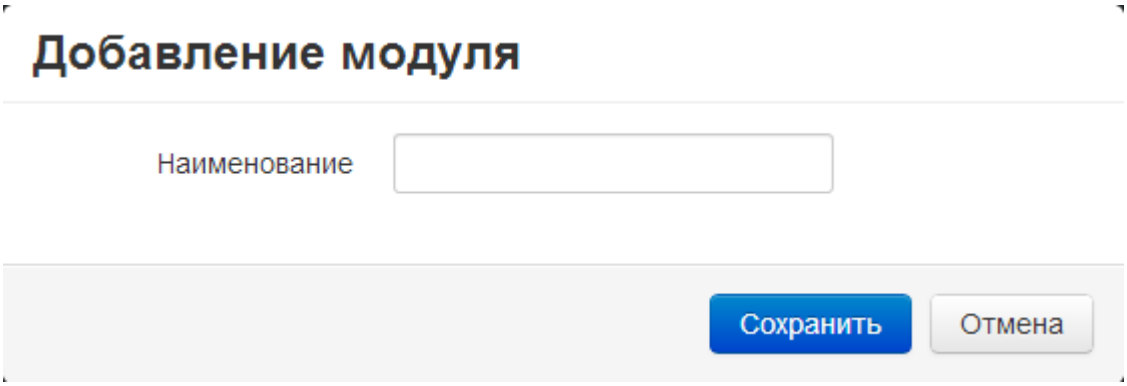

Рис. 5

В открывшемся диалоговом окне необходимо заполнить обязательное поле «Наименование» и сохранить модуль нажатием на кнопку «Сохранить».

После сохранения модуль появится в списке на форме вкладки «Модули» в левой части экрана.

4.2.2. Редактирование существующего модуля

При нажатии на кнопку «Редактировать» модуль отображается для изменения (Рис. 6).

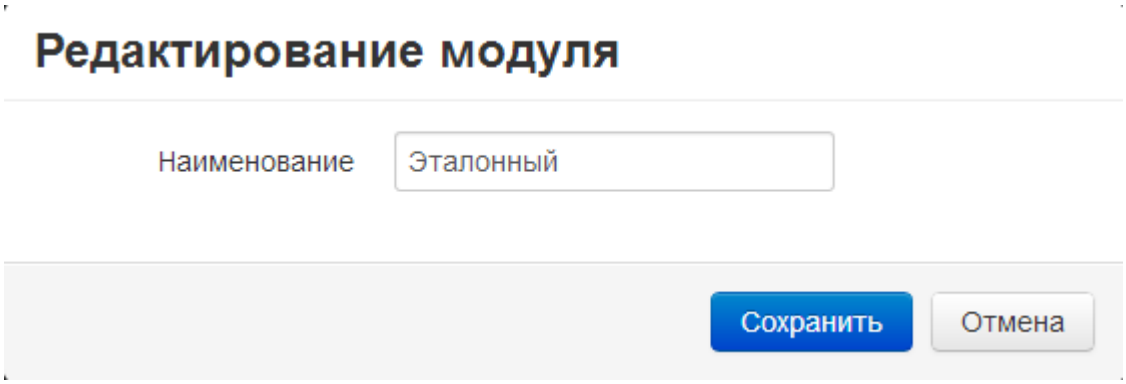

Рис. 6

4.2.3. Удаление модуля

Кнопка «Удалить» отвечает за удаление существующего модуля. При её нажатии открывается окно подтверждения, где можно подтвердить или отменить операцию (Рис. 7).

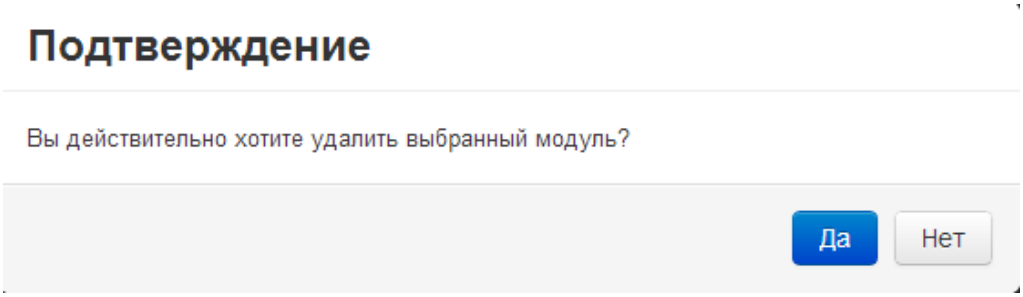

Рис. 7

4.2.4. Создание новой функции модуля

Прежде чем добавить новую функцию, необходимо выбрать модуль из списка предложенных вариантов. Далее нажать на кнопку добавления новой функции в правой части экрана (Рис. 8).

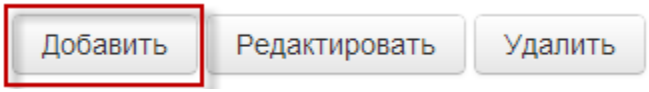

Рис. 8

После нажатия открывается форма создания функции (Рис. 9).

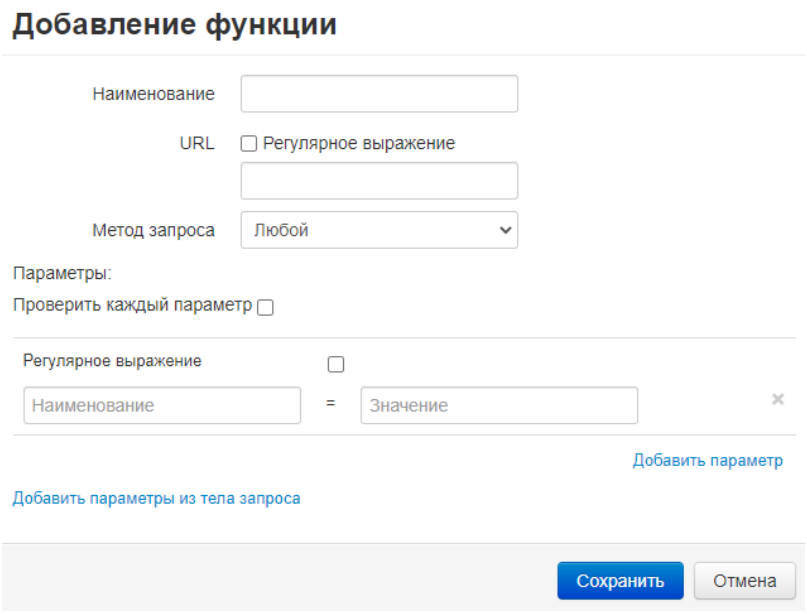

Рис. 9

В открывшемся диалоговом окне необходимо заполнить обязательные поля: «Наименование», «URL» и сохранить функцию нажатием на кнопку «Сохранить».

Поле «URL» не должно содержать символа «\», только наименование URL, заключенное в символы «/» или просто наименование, например:

`handleActionButton` или `/handleActionButton/`

Если проставить галочку во флаге «Регулярное выражение», то функция будет рассматриваться как регулярное выражение. Тогда в строке задания URL необходимо вводить регулярное выражение вместо конкретного URL, например:

```
^\/sc\/quotas\/\d+\/edit$
```

Этот флаг используется, например, в случае обращения функции к файлам, лежащим в одной директории.

Также при создании функции можно заполнить дополнительные необязательные поля:

«Метод запроса» – идентификатор, указывающий на основную операцию над ресурсом. Типы запросов подразделяются на:

– Любой – используется в случае, если запрос не определен;

– Get – используется для запроса содержимого указанного ресурса. С помощью метода GET можно также начать какой-либо процесс. В этом случае в тело ответного сообщения следует включить информацию о ходе выполнения процесса;

– Post – применяется для передачи пользовательских данных заданному ресурсу;

– Put – применяется для загрузки содержимого запроса на указанный в запросе URI;

– Delete – удаляет указанный ресурс;

– Head – аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело;

– Options – используется для определения возможностей web-сервера или параметров соединения для конкретного ресурса;

– Patch – изменяет или создает одну или несколько записей в источнике данных или объединяет записи вне этого источника.

В поле «Параметры функции» указывается, какие конкретные параметры доступны пользователю. Параметры функции задаются двумя полями: «Наименование» и «Значение», связанными знаком «=». Например:

```
action = cancel
```

В качестве параметра может быть задано регулярное выражение, если поставить галочку во флаге «Регулярное выражение». Тогда в полях «Наименование» и «Значение» необходимо ввести регулярное выражение, а не конкретные наименование и значение параметра.

У одной функции может быть несколько параметров. Для того чтобы добавить параметр функции, необходимо кликнуть по ссылке «Добавить параметр».

При нажатии на флаг «Проверить каждый параметр» не рассматриваются параметры регулярного выражения, не указанные в правилах.

При нажатии на кнопку «Добавить параметр из тела запроса» в окне «Добавление функции» появляются новые параметры настройки функции (Рис. 10). Выбор параметров состоит из:

– Любой – любой формат из тела запроса;

– JSON-RPC – тело запроса должно быть json-объектом, где ключ – имя параметра, а значение – значение параметра;

– JSON-строка – application/json – тело запроса должно быть json-строкой;

– www-form-urlencoded – тип содержимого application/x-www-form-urlencoded описывает данные формы, которые отправляются одним блоком в теле сообщения HTTP. В отличие от части URL-адреса в запросе GET, длина данных не ограничена.

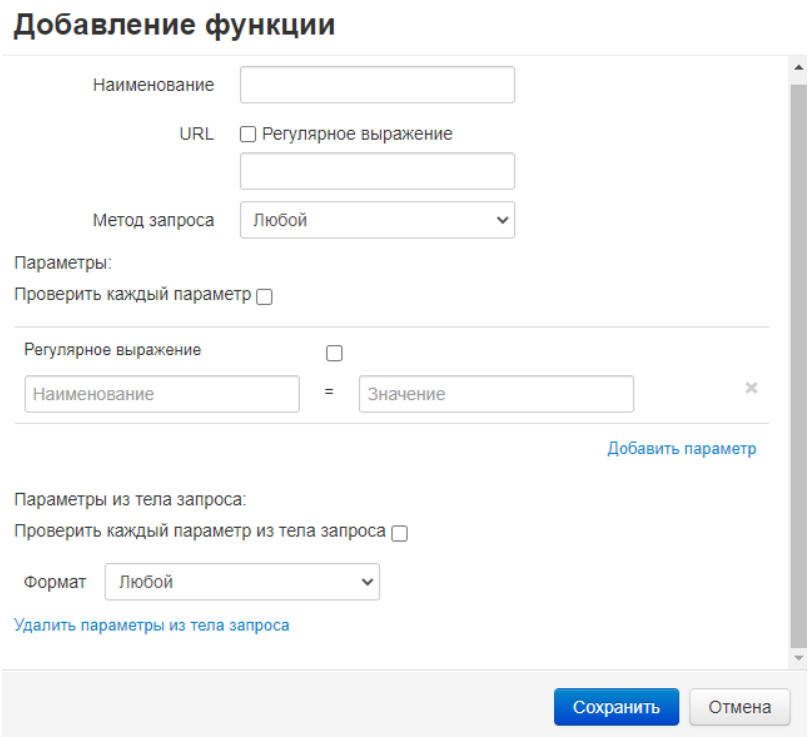

Рис. 10

В качестве параметра из тела запроса также может быть задано регулярное выражение, если поставить галочку во флаге «Регулярное выражение». Тогда в полях «Наименование» и «Значение» необходимо ввести регулярное выражение, а не конкретные наименование и значение параметра. Если поставить галочку во флаге «Разрешить параметры другого формата» выражение параметра можно будет проверять разные форматы заполненных строк. Фильтр http-запросов имеет поддержку задания правил разграничения доступа по параметрам, переданным в теле http-запроса. При этом правила разграничения должны описывать формат тела. Формат тела определяется по http-заголовку и по особенностям анализа тела. Кнопка «Удалить параметры из тела запроса» удаляет добавленные параметры и возвращает кнопку «Добавить параметры из тела запроса».

При нажатии на флаг «Проверить каждый параметр из тела запроса» не рассматриваются параметры регулярного выражения, не указанные в правилах.

После сохранения функция появится в списке на форме вкладки «Модули и функции» в правой части рабочей области.

Более подробное описание работы с функциями описано в главе 5.

4.2.5. Редактирование существующей функции модуля

При нажатии на кнопку «Редактировать» открывается окно «Редактирования функции», где выбранная функция отображается для изменения (Рис. 11).

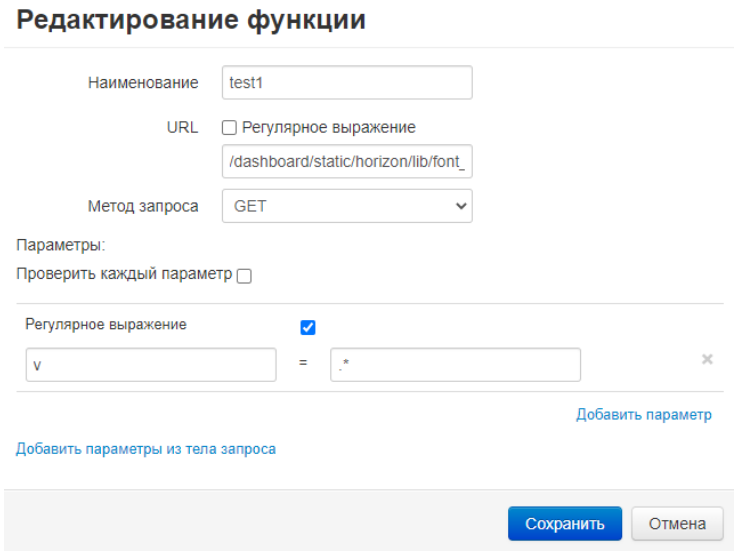

Рис. 11

Данная форма имеет аналогичные поля для заполнения, как и форма «Добавление функции». Добавить необходимые изменения и нажать кнопку «Сохранить». При нажатии кнопки «Отмена» внесенные изменения не сохранятся.

4.2.6. Удаление функции модуля

Кнопка «Удалить» отвечает за удаление существующей функции. При её нажатии открывается окно подтверждения, где можно подтвердить или отменить операцию (Рис. 12).

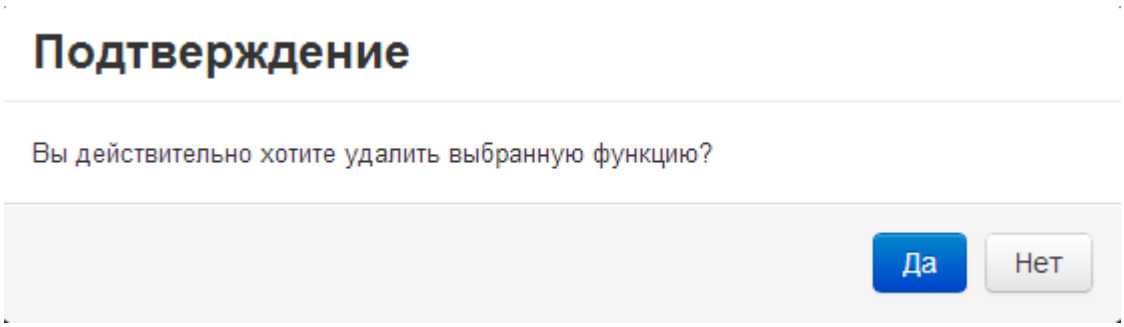

Рис. 12

Примечание: перед удалением функции необходимо открепить ее от роли.

4.3. Вкладка «Пользователи»

На вкладке «Пользователи» осуществляется управление пользователями защищаемой системы. На панели управления представлены кнопки управления (Добавить, Редактировать, Роли, Удалить), список пользователей и «Фильтр». Для каждого пользователя отображаются следующие данные (Рис. 13):

– логин пользователя;
– отметка смены пароля после первого входа;
– срок действия пароля;
– отметка о блокировке пользователя;
– максимальное количество параллельных сессий;
– число активных сессии;
– отметка о временном пользователе;
– тип доступа;
– описание пользователя.

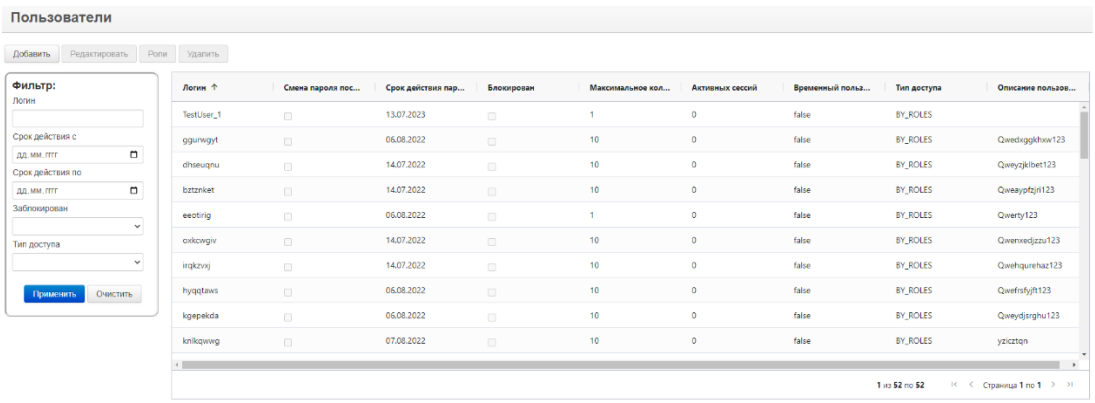

Рис. 13

4.3.1. Создание нового пользователя

Для добавления нового пользователя необходимо нажать кнопку «Добавить» (Рис. 14).

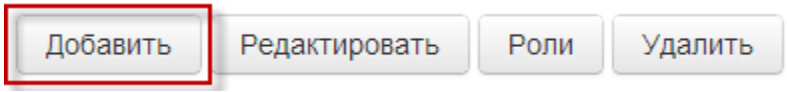

Рис. 14

После чего открывается форма создания пользователя (Рис. 15).

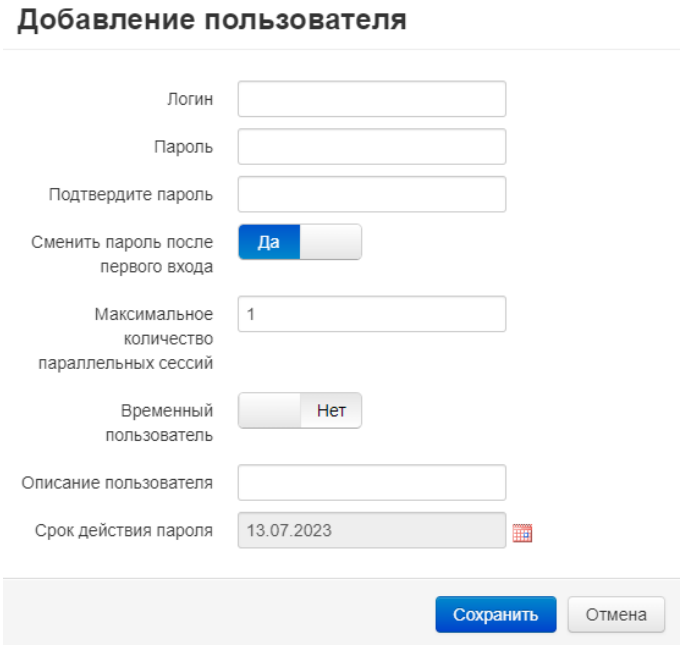

Рис. 15

В открывшемся диалоговом окне необходимо заполнить обязательные поля: «Логин», «Пароль», «Подтвердите пароль», «Максимальное количество параллельных сессий», «Срок действия пароля» и сохранить пользователя нажатием на кнопку «Сохранить». Также при создании пользователя можно заполнить дополнительное (необязательное) поле «Описание пользователя». Поставить поля «Временный пользователь» и «Сменить пароль после первого входа» в положение «Да» при необходимости.

После сохранения пользователь появится в списке во вкладке «Пользователи».

Примечание 1: после создания пользователя, ему автоматически назначается роль «Default».

Примечание 2: «Тип доступа» пользователя зависит от настройки привязанной роли. В случае удаления всех ролей пользователя, тип доступа автоматически меняется на выбранный в Программе (черный или белый). Существует 3 вида типа доступа:

– все запрещено (белый список);
– все разрешено (черный список);
– по ролям (в случае привязки к роли).

При создании пользователя в ПО «WebGard 2.0» пользователь в ЗИС не создаётся. Для корректной работы необходимо добавить пользователя идентичного в ЗИС.

4.3.2. Редактирование существующего пользователя

При нажатии на кнопку «Редактировать» открывается форма редактирования выбранного пользователя (Рис. 16).

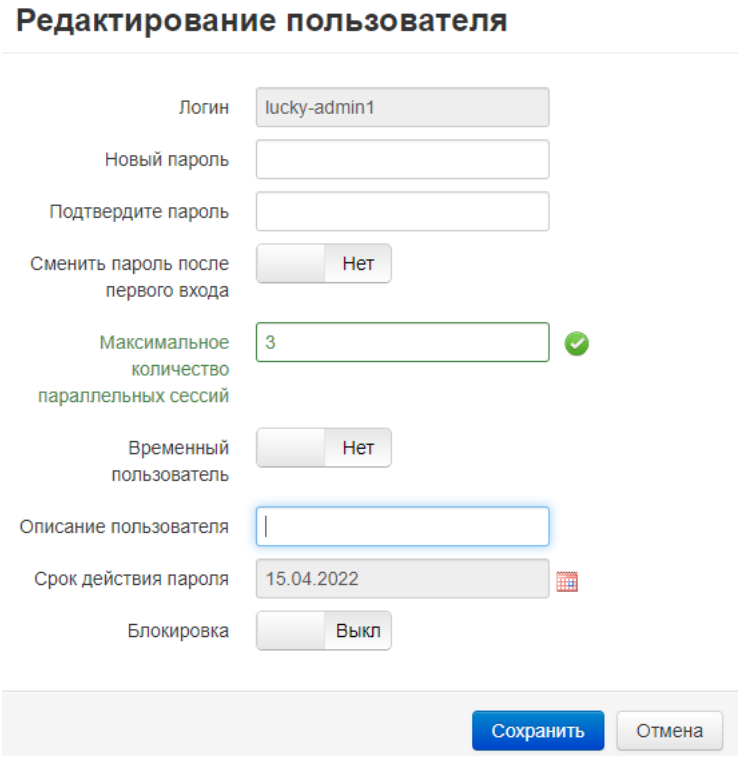

Рис. 16

В форме редактирования отображается дополнительное поле для смены пароля «Новый пароль» и «Подтверждение пароля», кнопка блокировки пользователя, которая блокирует пользователю доступ к ЗИС, поле «Максимальное количество сессий», которое позволяет войти в аккаунт с нескольких устройств, отметка о временном пользователе, кнопка изменения пароля после первого входа, поле описания пользователя, срок действия пароля, изменить логин нельзя.

Примечания:

– при редактировании пользователя в ПО «WebGard 2.0», данные пользователя в ЗИС не меняются. Для корректной работы необходимо отредактировать данные пользователя в ЗИС идентично данным в ПО «WebGard 2.0»;

– при установке флага «Блокировка» в положение «Вкл» все открытые сессии блокированного пользователя автоматически блокируются. Чтобы разблокировать пользователю доступ к Программе необходимо флаг «Блокировка» в положение «Выкл» и примерить права.

4.3.3. Кнопка «Роли»

Кнопка «Роли» (Рис. 17) используется для вызова формы редактирования ролей пользователя.

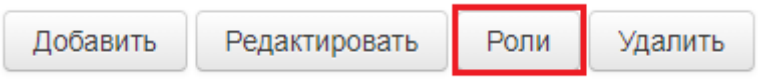

Рис. 17

Форма редактирования ролей пользователя (Рис. 18).

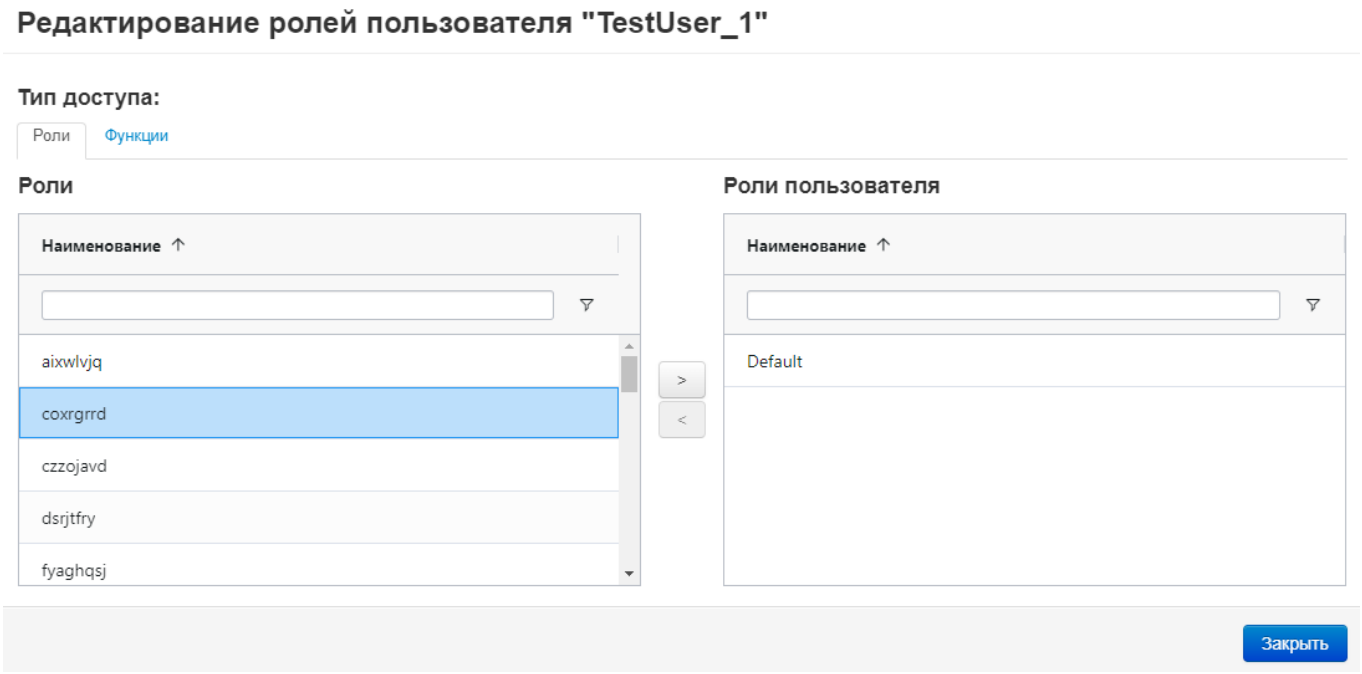

Рис. 18

Форма редактирования ролей пользователя позволяет назначить/удалить роль или несколько ролей выбранному пользователю.

В данном окне можно добавлять определенному пользователю необходимые роли. Для поиска ролей используется окно поиска.

Вкладка «Функции» показывает, какие функции назначены пользователю от добавленных ролей (Рис. 19).

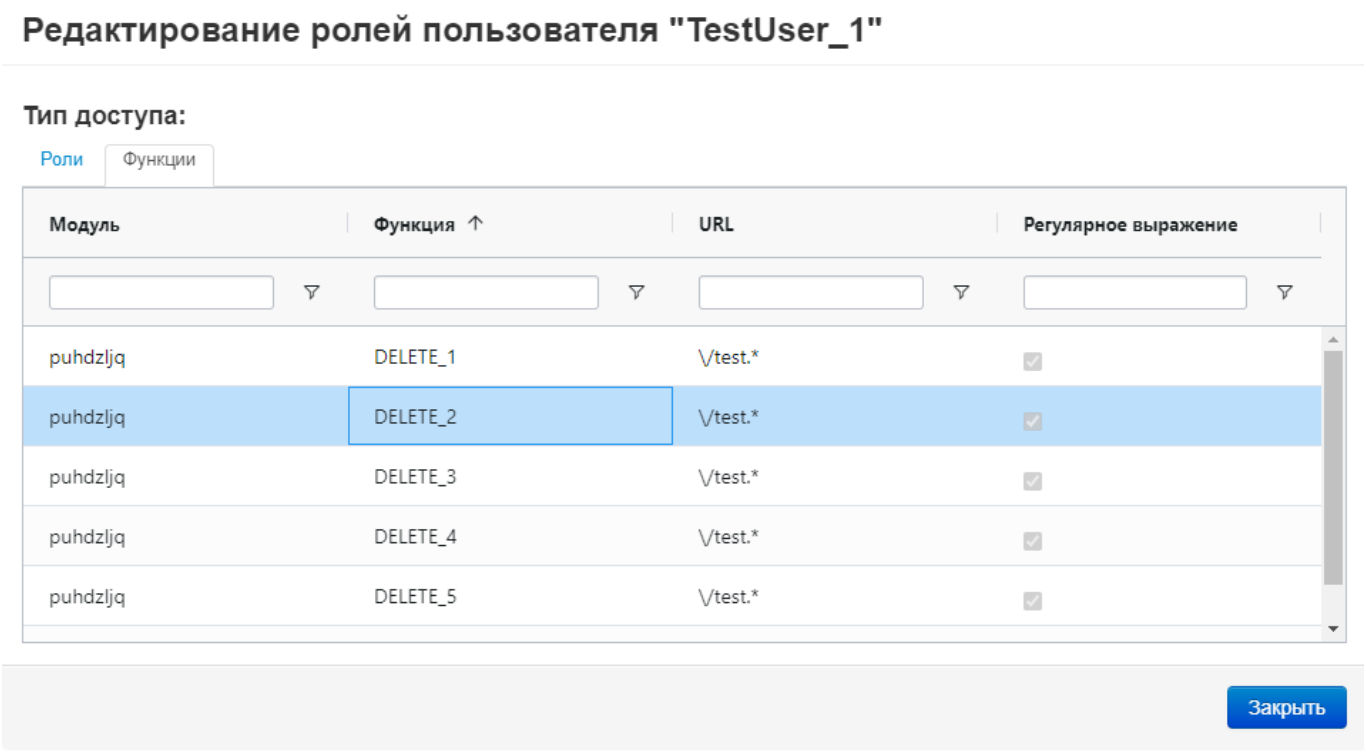

Рис. 19

Чтобы найти определенную функцию можно воспользоваться поиском.

4.3.4. Удаление пользователя

Кнопка «Удалить» отвечает за удаление существующего пользователя. При её нажатии открывается окно подтверждения, где можно подтвердить или отменить операцию (Рис. 20).

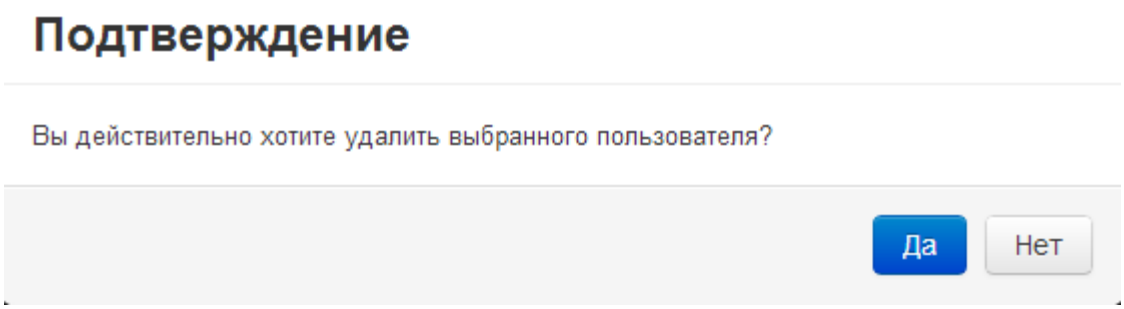

Рис. 20

Примечание: при удалении пользователя в ПО «WebGard 2.0» данные пользователя в ЗИС сохраняются. Для полного удаления пользователя его также необходимо удалить в ЗИС.

4.3.5. Поиск пользователей с использованием формы «Фильтр»

Окно «Фильтр» производит поиск пользователей по заданным параметрам (Рис. 21):

– логин – производит поиск по столбцу «Логин» и выводит пользователей, у которых введенная фраза неточно совпадает со значением в столбце «Логин»;

– срок действия с – производит поиск по столбцу «Срок действия пароля» и выводит пользователей, у которых срок действия пароля заканчивается позже назначенной даты;

– срок действия по – производит поиск по столбцу «Срок действия пароля» и выводит пользователей, у которых срок действия пароля заканчивается раньше назначенной даты;

– заблокирован – производит поиск по столбцу «Блокирован» и выводит пользователей с выбранной меткой;

– тип доступа – производит поиск по столбцу «Тип доступа» и выводит пользователей с выбранной меткой;

– кнопка «Применить» производит поиск пользователей по заданным параметрам, а кнопка «Очистить» возвращает все строки с данными о пользователях к исходному виду.

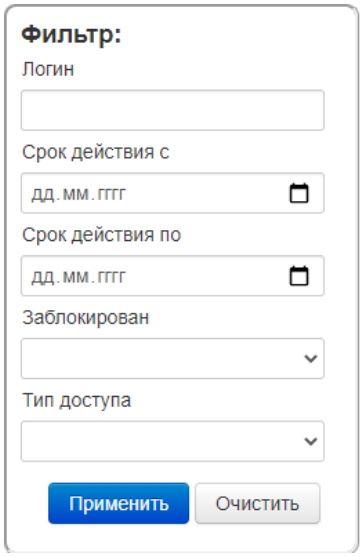

Рис. 21

4.3.6. Вкладка «Пользователи» при автоматической синхронизации паролей с ЗИС

При автоматической синхронизации паролей с ЗИС администратор не может создавать пользователей в Программе. Кнопка «Добавить» отсутствует (Рис. 22).

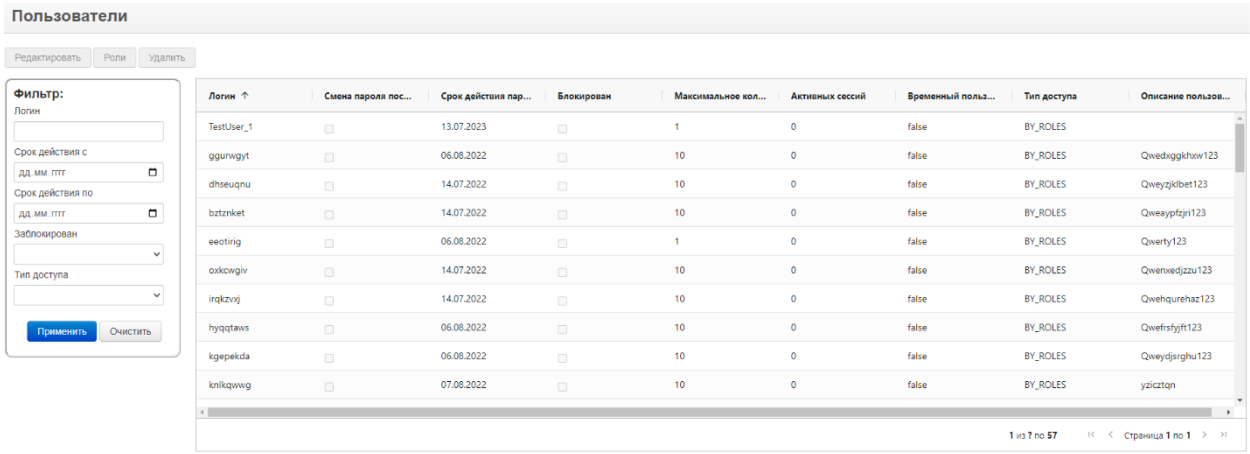

Рис. 22

Все пользователи Программы должны создаваться в ЗИС. Пользователи будут автоматически обновляться в течение определенного промежутка времени, которое указано в конфигурационном файле подсистемы администрирования.

Администратору запрещено изменять пароль пользователю во время его редактирования. При автоматической синхронизации поля смены пароля пользователя отсутствуют (Рис. 23).

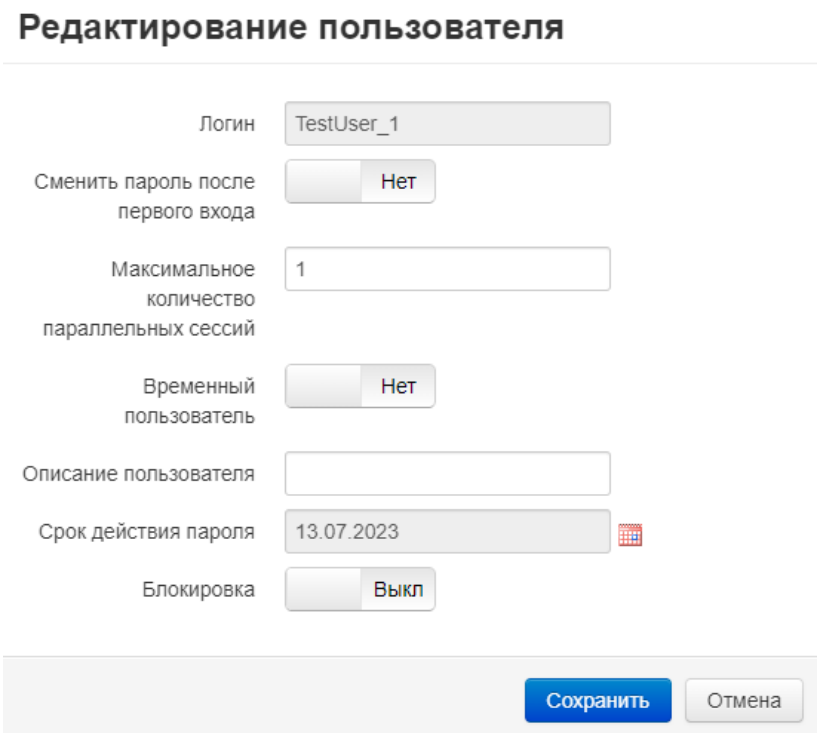

Рис. 23

Оставшиеся данные формы имеют аналогичные поля для заполнения, как и форма «Редактирование пользователя». Можно добавить необходимые изменения и нажать кнопку «Сохранить». При нажатии кнопки «Отмена» внесенные изменения не сохранятся.

Настройка автоматической синхронизации указана в пп. 5.2.10 и 5.2.11 документа «Программное обеспечение «WebGard 2.0». Руководство администратора по развертыванию (подсистема администрирования).

Примечания:

– при редактировании пользователя в ПО «WebGard 2.0», данные пользователя в ЗИС не меняются. Для корректной работы необходимо отредактировать данные пользователя в ЗИС идентично данным в ПО «WebGard 2.0»;

– при установке флага «Блокировка» в положение «Вкл» все открытые сессии блокированного пользователя автоматически блокируются. Чтобы разблокировать пользователю доступ к Программе необходимо флаг «Блокировка» в положение «Выкл» и примерить права.

4.4. Вкладка «Администраторы»

На вкладке «Администраторы» осуществляется создание новых администраторов Программы и их редактирование (Рис. 24).

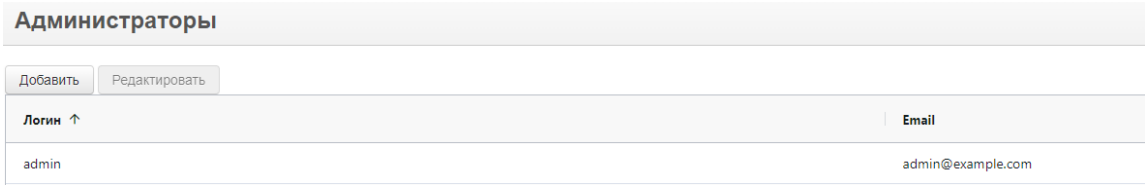

Рис. 24

На панели управления находятся кнопки управления (Добавить и Редактировать), с их помощью осуществляется управление учетными данными администратора.

4.4.1. Создание нового администратора

Для создания нового администратора необходимо нажать кнопку «Добавить» (Рис. 25).

Рис. 25

После произведенных действий открывается форма создания администратора (Рис. 26).

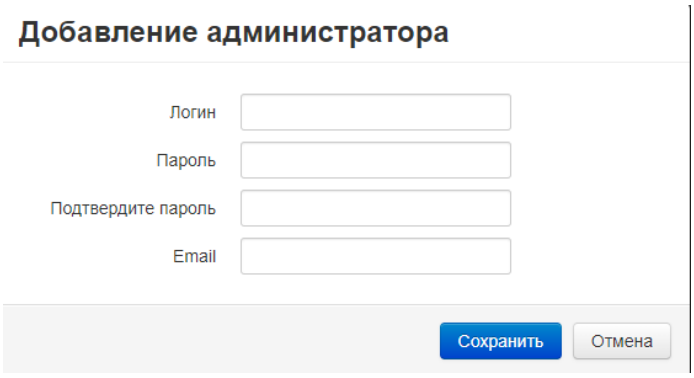

Рис. 26

В открывшемся диалоговом окне необходимо заполнить обязательные поля: «Логин», «Пароль», «Подтвердите пароль», «Email» и нажать на кнопку «Сохранить». После сохранения данные нового администратора появятся в таблице.

4.4.2. Редактирование администратора

При нажатии на кнопку «Редактировать» открывается окно изменения администратора (Рис. 27).

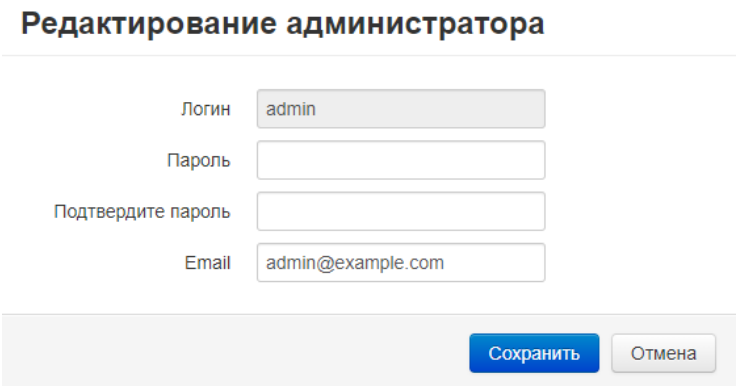

Рис. 27

В форме редактирования администратора осуществляется изменение пароля и Email, изменить логин администратора нельзя.

Чтобы изменить поле «Email» необходимо ввести новый пароль в поля «Пароль» и «Подтвердите пароль».

Примечание: администратор имеет право редактировать только свои учетные данные. Запрещено изменять другого администратора. Чтобы удалить администратора Программы необходимо отправить запрос в БД Программы. Пример запроса указан в п. 5.3 документа «Программное обеспечение «WebGard 2.0». Руководство администратора по развертыванию (подсистема администрирования).

Примечание 1: при редактировании поля «Email» необходимо заполнить поля «Пароль» и «Подтвердите пароль».

Примечание 2: у паролей администратора нет времени жизни пароля. Администратор должен сам изменять свой пароль согласно требованиям организационно-распорядительной документации организации.

4.5. Вкладка «Роли»

На вкладке «Роли» осуществляется создание новых ролей Программы их редактирование и удаление (Рис. 28).

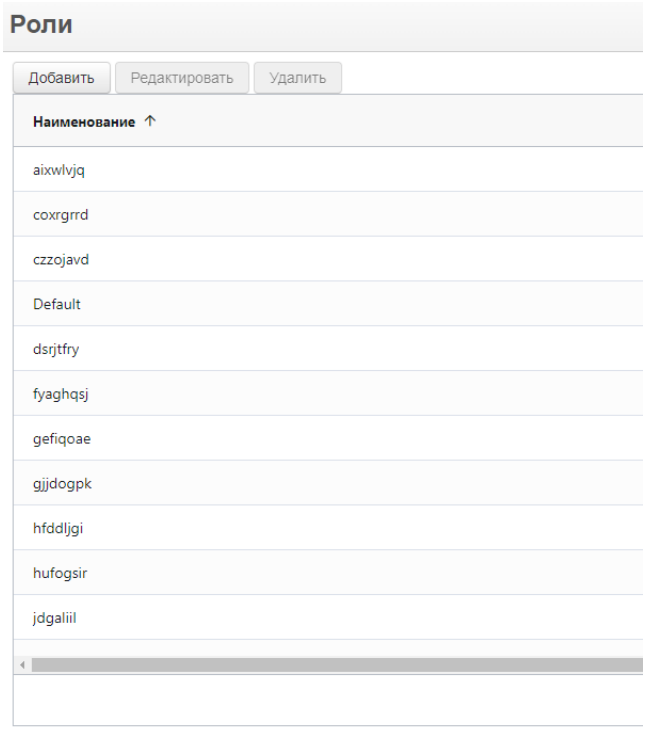

Рис. 28

Предназначение формы – присвоение созданным пользователям определенной роли в Программе, выдача прав на тот или иной функционал. На панели управления представлены кнопки управления (Добавить, Редактировать, Удалить) и список ролей. Для каждой роли отображается её наименование.

4.5.1. Создание новой роли

Для создания новой роли необходимо нажать кнопку «Добавить» (Рис. 29).

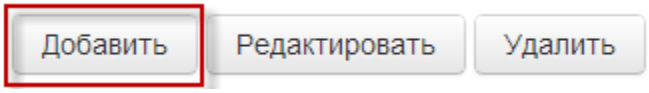

Рис. 29

После произведенных действий открывается форма создания роли (Рис. 30).

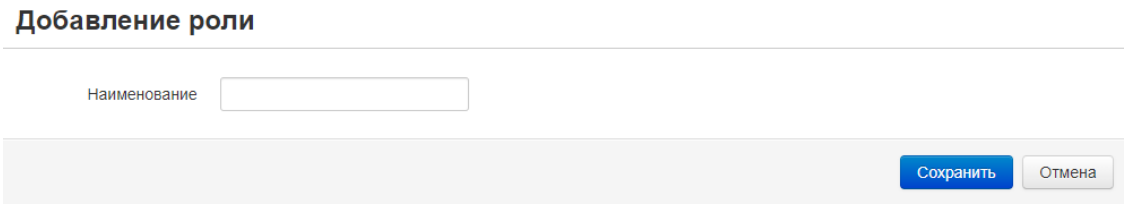

Рис. 30

В открывшемся окне необходимо заполнить поле: «Наименование» и нажать на кнопку «Сохранить». После сохранения автоматически открывается редактирование созданной роли.

4.5.2. Редактирование существующей роли

При нажатии на кнопку «Редактировать» открывается окно изменения выбранной роли (Рис. 31).

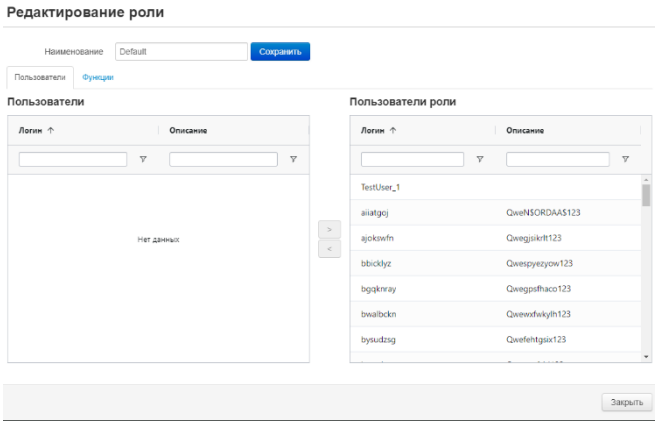

Рис. 31

Редактирование роли позволяет изменять наименование роли, а также присваивать пользователей и функции к выбранной роли.

Так же имеется поиск по столбцам, для более быстрого поиска определенного пользователя/модуля/функции.

4.5.3. Назначение/удаление ролей пользователям

В форме редактирования роли отображается дополнительный функционал, осуществляющий назначение и удаление пользователей и функций в выбранной роли. Описанные действия осуществляются с помощью вкладок «Пользователи» и «Функции».

Вкладка «Пользователи» разделена на две области: в левой представлен список всех существующих пользователей, в правой – список пользователей, назначенных к редактируемой роли. Назначение или удаление осуществляется нажатием на кнопки «>» или «<», находящиеся между списками. Одновременно можно назначать и удалять несколько выделенных пользователей (Рис. 32).

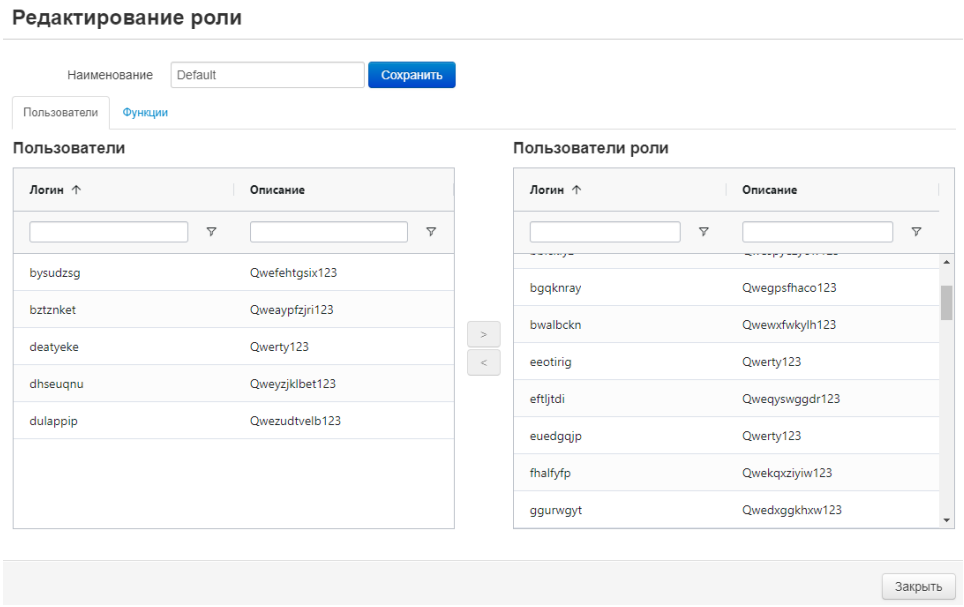

Рис. 32

При удалении последней роли пользователя во вкладке «Пользователи» в столбце «Тип доступа» записывается тип доступа по списку, который выбран администратором Программы.

4.5.4. Назначение/удаление ресурсов роли

Вкладка «Функции» аналогично разделена на две области: в левой представлен список всех существующих функций, в правой – список функций, назначенных к редактируемой роли (Рис. 33).

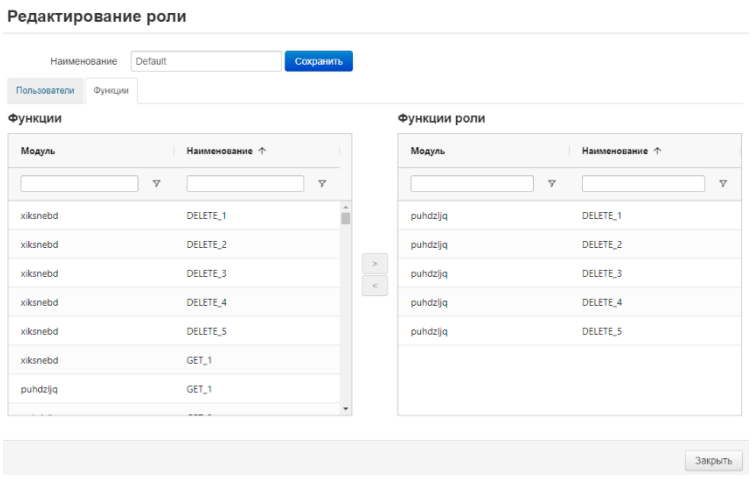

Рис. 33

Во таблице «Функции» представлен список существующих функций, а в таблице «Функции роли» представлен список функций, назначенных редактируемой роли. Для каждой функции отображается её модуль и наименование. Присвоение или удаление функции для роли происходит при помощи «<» или «>» (Рис. 34).

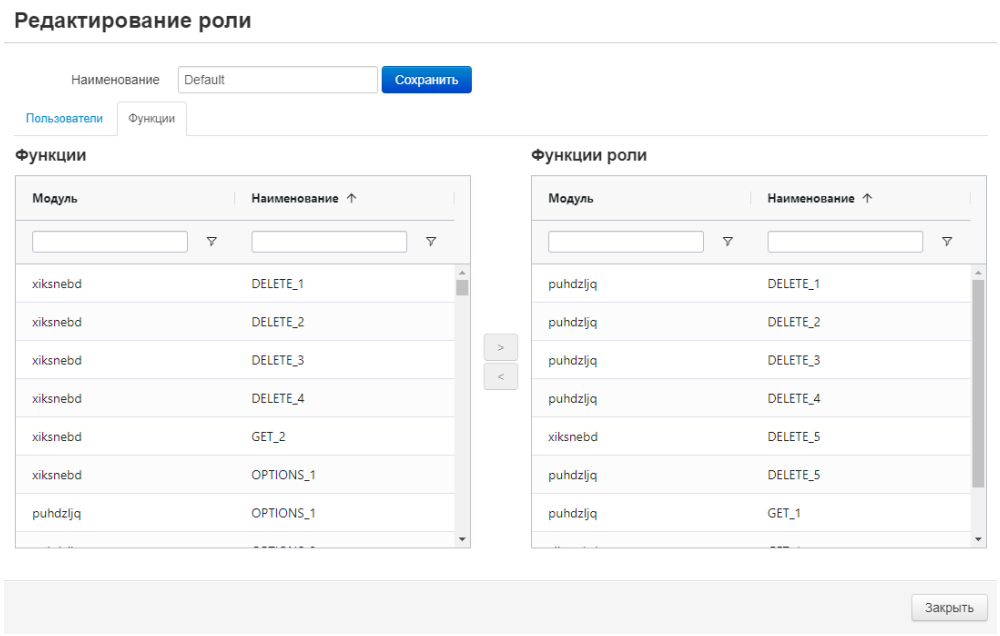

Рис. 34

4.5.5. Удаление роли

Кнопка «Удалить» отвечает за удаление выбранной роли. При её нажатии открывается окно подтверждения, где можно подтвердить или отменить операцию (Рис. 35).

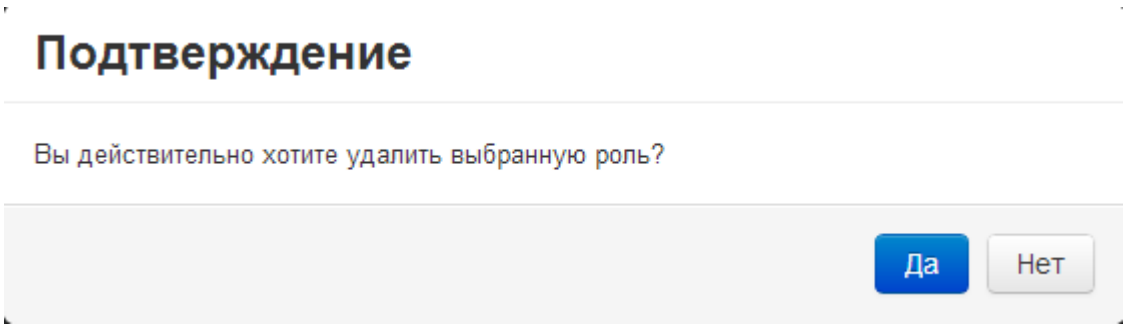

Рис. 35

4.6. Вкладка «Настройки безопасности»

На вкладке «Настройки безопасности» осуществляется изменение настроек безопасности Программы (Рис. 36).

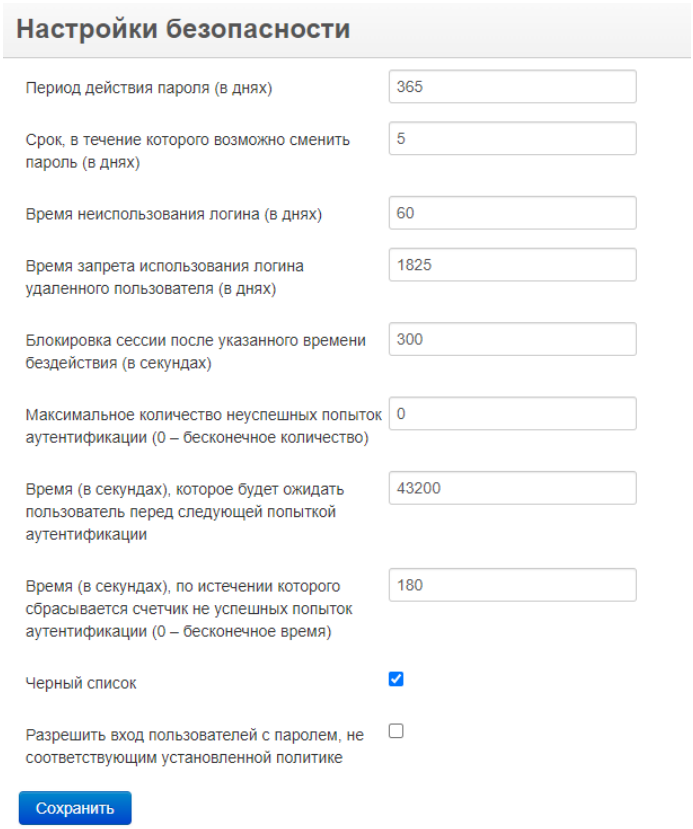

Рис. 36

Предназначение вкладки «Настройки безопасности» – изменение глобальных настроек безопасности Программы. В окне представлены существующие настройки безопасности:

– период действия пароля (в днях). В случае изменения данного параметра, срок действия пароля у существующих пользователей не изменится. Измененная настройка будет относиться только к новым изменениям пароля пользователя (самим пользователем или администратором) и к созданию новых пользователей. Данное поле в ЗИС и в Программе должны иметь одинаковые значения;

– срок, в течение которого возможно сменить пароль (в днях);

– время неиспользования логина (в днях). При установке данного параметра блокировка учитывается целыми сутками. Например, при установке значения 1 в 12:00:00 пользователь будет заблокирован только в 23:59:59 следующего дня, в случае если он не будет проходить аутентификацию в течении всего времени бездействия;

– время запрета использования логина удаленного пользователя (в днях);

– блокировка сессии после указанного времени бездействия (в секундах). Данное поле в ЗИС и в Программе должны иметь одинаковые значения;

– максимальное количество неуспешных попыток аутентификации (0 – бесконечное количество);

– время (в секундах), которое будет ожидать пользователь перед следующей попыткой аутентификации. При превышении максимального количества попыток аутентификации, учетная запись пользователя будет автоматически временно заблокирована. Временная блокировка длится в течении времени, указанного в параметре «время (в секундах), которое будет ожидать пользователь перед следующей попыткой аутентификации». После истечения

времени «время (в секундах), которое будет ожидать пользователь перед следующей попыткой аутентификации» учетная запись автоматически разблокируется и пользователю будет предоставлена еще одна попытка аутентификации;

– время (в секундах), по истечении которого сбрасывается счетчик неуспешных попыток аутентификации (0 – бесконечное время);

– перевод режима работы Программы с белого списка на черный;

– разрешить вход пользователей с паролем, не соответствующим установленной политике.

Принцип режима работы черного/белого списка:

– белый список. В данном режиме работы в Программе по умолчанию запрещен доступ ко всем ресурсам ЗИС. Для разрешения доступа пользователям, необходимо присвоить права с разрешенными к доступу ресурсами;

– черный список. В данном режиме работы в Программе по умолчанию разрешен доступ ко всем ресурсам ЗИС. Для запрета доступа пользователям, необходимо присвоить права с запрещенными к доступу ресурсами.

Разрешение входа пользователей с паролем, не соответствующей политике выключает существующую политику пароля Программы только для подсистемы администрирования.

Кнопка «Сохранить» сохраняет все изменения настроек безопасности в базу данных Программы.

4.6.1. Минимальные значения настроек безопасности

Минимальные значения настроек безопасности представлены на рисунке (Рис. 37).

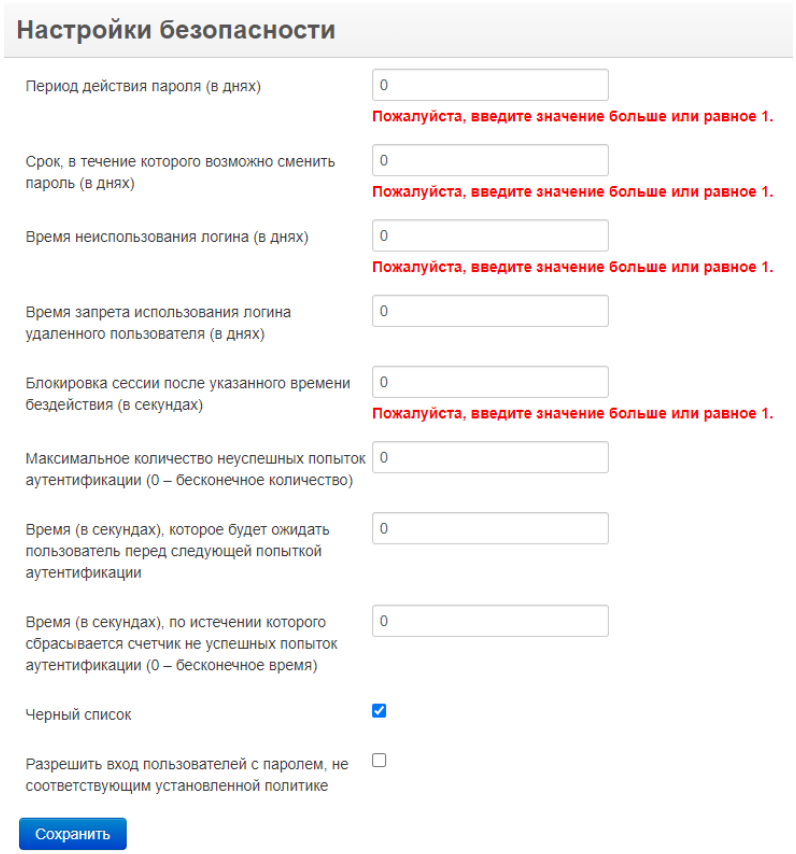

Рис. 37

Минимальные значения:

– период действия пароля (в днях): 1 день;

– срок, в течение которого возможно сменить пароль (в днях): 1 день;

– время неиспользования логина (в днях): 1 день;

– время запрета использования логина удаленного пользователя (в днях): 0 дней;

– блокировка сессии после указанного времени бездействия (в секундах): 1 секунда;

– максимальное количество неуспешных попыток аутентификации (0 – бесконечное количество): 0 – бесконечность, минимальное значение – 1;

– время (в секундах), которое будет ожидать пользователь перед следующей попыткой аутентификации: 0 секунд;

– время (в секундах), по истечении которого сбрасывается счетчик неуспешных попыток аутентификации (0 – бесконечное время): 0 – бесконечность, минимальное значение – 1.

4.6.2. Безопасные значения настроек безопасности

Безопасные значения настроек составлены согласно требованиям приказа ФСТЭК России от 11 февраля 2013 г. № 17:

– период действия пароля (в днях): не более 60 дней;

– срок, в течение которого возможно сменить пароль (в днях): оператором должен быть определен срок в организационно-распорядительной документации;

– время неиспользования логина (в днях): 45 день;

– время запрета использования логина удаленного пользователя (в днях): 1095 дней и более;

– блокировка сессии после указанного времени бездействия (в секундах): 300 секунда;

– максимальное количество неуспешных попыток аутентификации (0 – бесконечное количество): не более 4 попыток;

– время (в секундах), которое будет ожидать пользователь перед следующей попыткой аутентификации: оператором должен быть определен срок в организационно-распорядительной документации;

– время (в секундах), по истечении которого сбрасывается счетчик неуспешных попыток аутентификации (0 – бесконечное время): от 900 секунд до 2400 секунд.

4.7. Вкладка «Аудит»

Вкладка «Аудит» состоит из двух подпунктов: «Логи безопасности» и «Аудит администрирования безопасности» (Рис. 38).

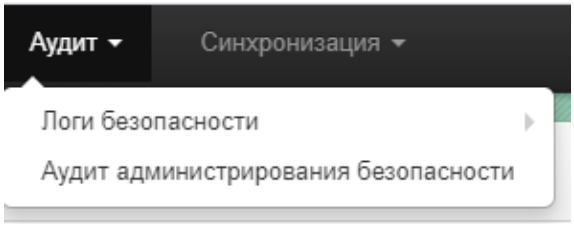

Рис. 38

Подпункт «Логи безопасности» состоит из двух подпунктов: «Настройки логов безопасности» и «Аудит HTTP-запросов» (Рис. 39).

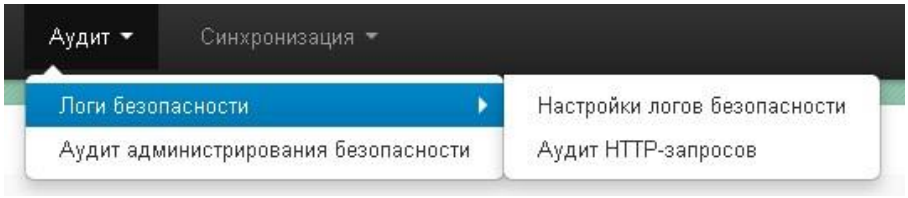

Рис. 39

4.8. Вкладка «Настройки логов безопасности»

Во вкладке «Настройки логов безопасности» происходит настройка подключения аудита к базе данных Программы (Рис. 40).

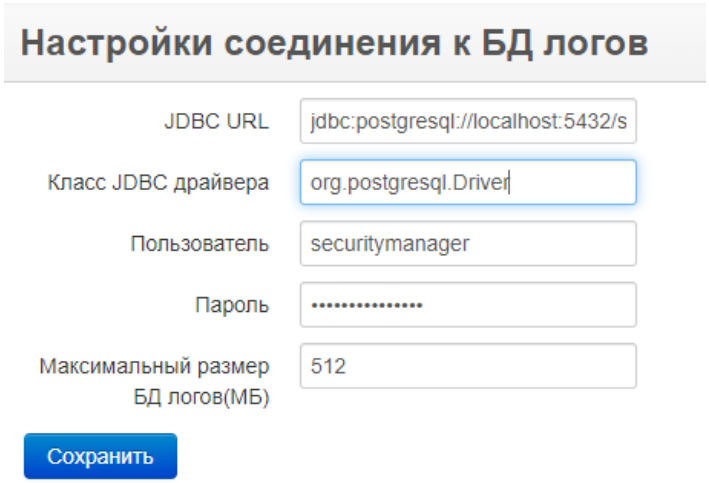

Рис. 40

В окне «Настройки соединения к БД логов» представлены настройки чтения таблицы аудита для вкладки «Аудит HTTP-запросов»:

– JDBC URL – путь к базе данных;
– класс JDBC драйвера – класс драйвера для подключения к базе данных;
– пользователь – логин пользователя базы данных Программы;
– пароль – пароль пользователя базы данных Программы;
– максимальный размер БД логов(МБ) – максимальный размер хранилища аудита.

4.9. Вкладка «Аудит HTTP-запросов»

В форме «Аудит HTTP-запросов» представлен список http-запросов, выполняемых пользователями. Для каждого запроса отображаются следующие данные (Рис. 41):

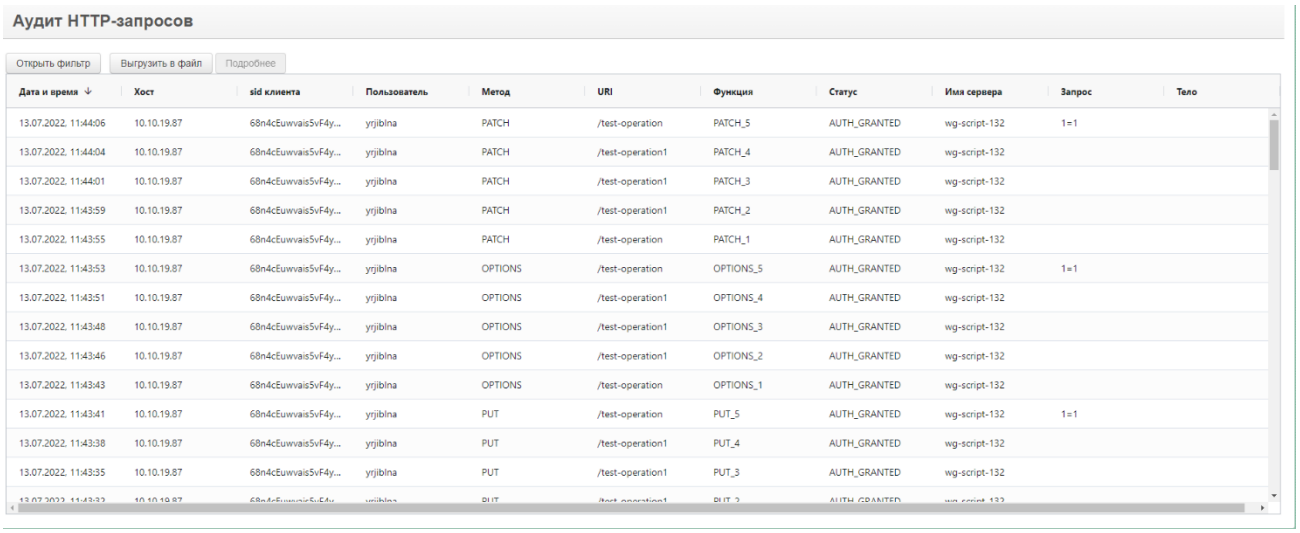

Рис. 41

– дата и время – дата и время выполнения функции;
– хост – ip клиентской машины, с которой выполнялась функция;

– sid клиента – идентификатор сессии;
– пользователь – логин пользователя, выполнявшего функцию;
– метод – метод запроса;
– URI (Запрошенный URI) – URI, запрошенный пользователем;
– функция (Наименование правила) – наименование функции, выполняемой пользователем;
– статус – статус запроса;
– имя сервера – имя сервера, на котором установлена подсистема фильтрации;
– запрос – параметры запрошенного URI;
– тело – параметры из тела запроса.

Также на панели управления представлена кнопка «Подробнее», при нажатии на которую открывается форма отображения информации о выбранном совершившемся событии безопасности (Рис. 42).

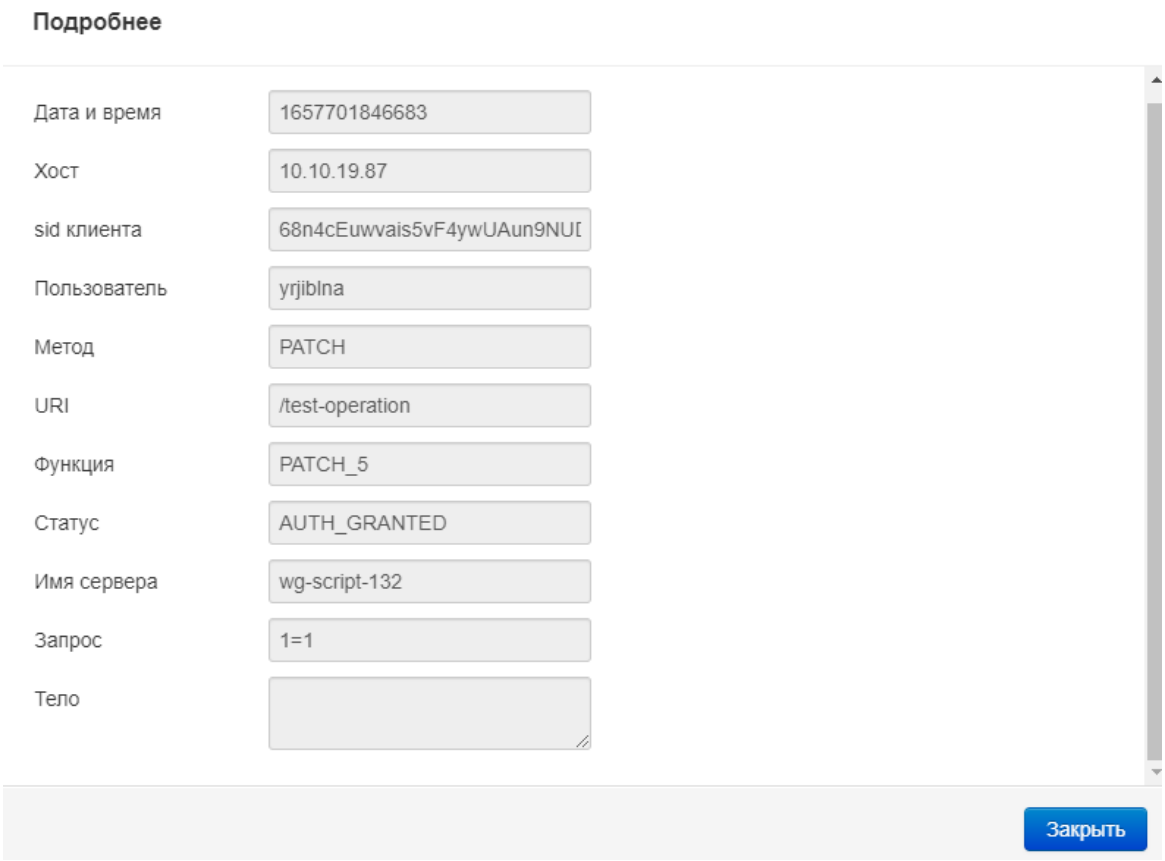

Рис. 42

Анализ записей регистрации событий безопасности http-запросов пользователей должен выполняться администратором не менее одного раза в сутки.

4.9.1. Выгрузка аудита http-запросов в файл

При нажатии кнопки «Выгрузить в файл» открывается окно «Выгрузка аудита в файл» (Рис. 43).

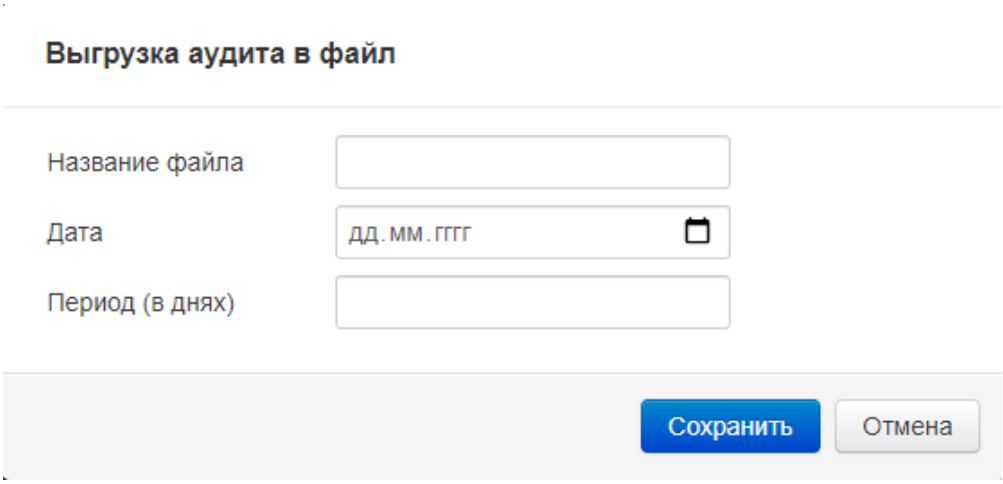

Рис. 43

В данном окне необходимо заполнить название файла аудита, с какой даты, за какой промежуток времени будет производиться выгрузка данных аудита http-запросов. Если нажать на кнопку «Сохранить», будет произведено сохранение файла на носитель. При нажатии кнопки «Отмена» выгрузка аудита не будет произведена.

4.9.2. Поиск http-запросов с использованием формы «Фильтр»

При нажатии кнопки «Открыть фильтр» появляется форма «Фильтр», которая производит поиск http-запросов по заданным параметрам (Рис. 44).

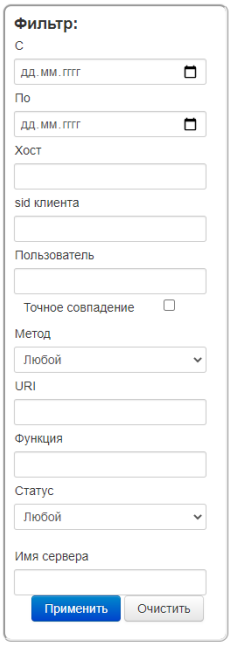

Рис. 44

– с – производит поиск по столбцу «Дата и время» и выводит строки аудита, в которых дата выполнения больше или равно введенным значениям;

– по – производит поиск по столбцу «Дата и время» и выводит строки аудита, в которых дата выполнения меньше или равно введенным значениям;

– хост – производит поиск по столбцу «Хост» и выводит строки, в которых введенная фраза неточно совпадает со значением в столбце «Хост»;

– sid клиента – производит поиск по столбцу «sid клиента» и выводит строки, в которых введенное значение совпадает со значением в столбце «sid клиента»;

– пользователь – производит поиск по столбцу «Пользователь» и выводит строки, в которых введенная фраза неточно совпадает со значением в столбце «Пользователь». Можно выбрать точное совпадение, тогда выведутся только однозначное совпадение с введенными данными;

– метод – производит поиск по столбцу «Метод» и выводит строки, в которых выбранное значение совпадает со значением в столбце «Метод»;

– URI – производит поиск по столбцу «URI» и выводит строки, в которых введенное значение совпадает со значением в столбце «URI»;

– функция – производит поиск по столбцу «Функция» и выводит строки, в которых введенная фраза неточно совпадает со значением в столбце «Функция»;

– статус – производит поиск в столбце «Статус» и выводит строки, в которых выбранное значение совпадает со значением в столбце «Статус»;

– имя сервера – производит поиск в столбце «Имя сервера» и выводит строки, в которых выбранное значение совпадает со значением в столбце «Имя сервера»;

– тело – производит поиск в столбце «Тело».

Кнопка «Применить» производит поиск пользователей по заданным параметрам, а кнопка «Очистить» возвращает все строки с данными аудита к исходному виду.

Описание статусов аудита HTTP-запросов приведено в таблице (Таблица 2).

Таблица 2 – Описание статусов аудита HTTP-запросов

Статус	**Описание**
AUTH_ERROR	Произошла непредвиденная ошибка
AUTH_FAIL	Пользователь не прошел аутентификацию по паролю
AUTH_SUCCESS	Пользователь успешно прошел аутентификацию по паролю
AUTH_DENIED	Пользователь не прошел авторизацию
AUTH_GRANTED	Пользователь успешно авторизован
AUTH_CLIENT_NOT_IDENTIFIED	Клиент пользователя не идентифицирован
AUTH_USER_NOT_IDENTIFIED	Пользователь не идентифицирован
AUTH_TEMPORARILY_BLOCKED	Пользователь временно заблокирован
AUTH_AUTHENTICATION_FAILED	Попытка аутентификации неуспешна
AUTH_PERMANENTLY_BLOCKED	Пользователь заблокирован на постоянной основе
AUTH_PASS_EXPIRED	Срок действия пароля пользователя истек
AUTH_TOO_MANY_SESSIONS	Превышен лимит параллельных сессий пользователя
AUTH_LOGGED_IN	Выполнена успешная авторизация пользователя

Статус	Описание
AUTH_LOGGED_OUT	Выполнено успешное закрытие сессии пользователя
AUTH_PASS_MUST_CHANGE	Пароль пользователя должен быть заменен

4.10. Вкладка «Аудит администрирования безопасности»

В форме вкладки «Аудит администрирования безопасности» представлен список операций, выполняемых администраторами в подсистеме администрирования. Для каждой операции отображаются следующие данные (Рис. 45):

– субъект – логин пользователя, производивший операцию;
– хост – ip клиентской машины, с которой выполнялась операция;
– дата и время – дата и время выполнения операции;
– объект – объект, над которым выполнялась операция;
– тип операции – тип операции;
– результат (успешно или нет) – результат выполнения операции;
– дополнительная информация к операции.

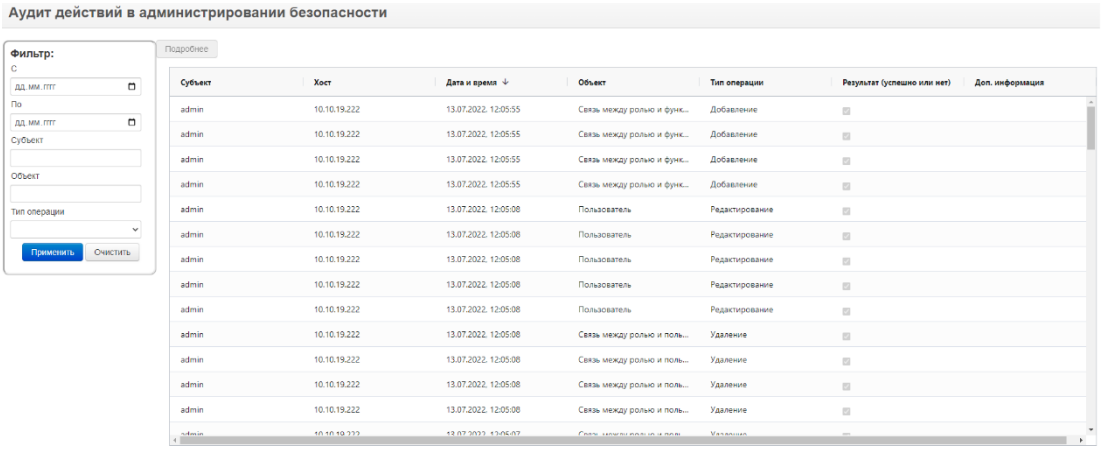

Рис. 45

Также на панели управления представлена кнопка «Подробнее», при нажатии на которую открывается форма отображения информации об измененных полях по выбранной операции (Рис. 46):

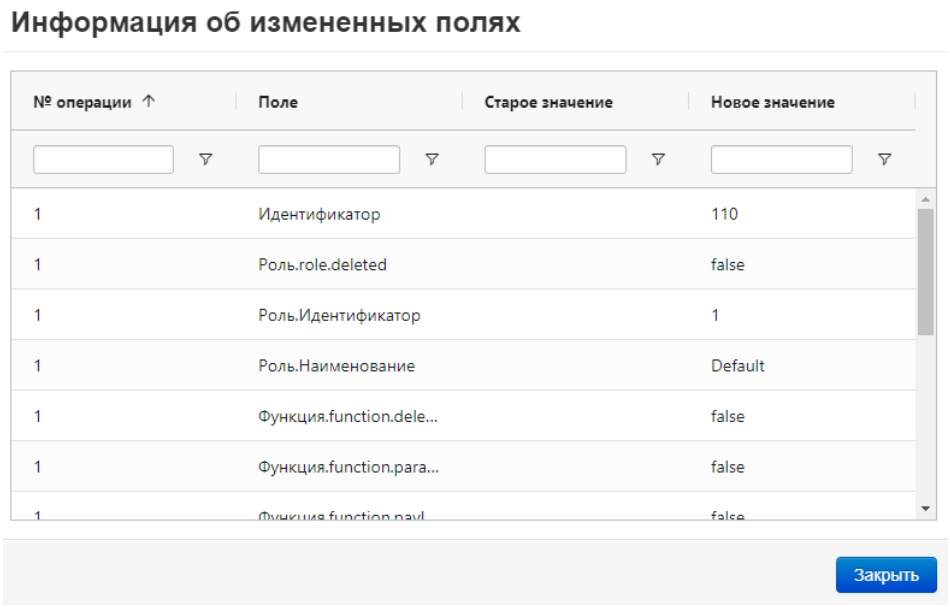

Рис. 46

В форме представлен список измененных полей. Для каждого поля отображается номер операции; наименование поля; старое значение и новое значение.

Анализ записей регистрации событий безопасности в подсистеме администрирования должен выполняться администратором не менее одного раза в сутки.

4.10.1. Поиск действий в администрировании безопасности используя «Фильтр»

Окно «Фильтр» производит поиск изменений в администрировании безопасности по заданным параметрам:

– с – производит поиск по столбцу «Дата и время» и выводит строки аудита, в которых дата выполнения больше или равно введенным значениям;

– по – производит поиск по столбцу «Дата и время» и выводит строки аудита, в которых дата выполнения меньше или равно введенным значениям;

– субъект – производит поиск по столбцу «Субъект» и выводит строки аудита, в которых введенная фраза неточно совпадает со значением в столбце «Субъект»;

– объект – производит поиск по столбцу «Объект» и выводит строки аудита, в которых введенное фраза неточно совпадает со значением в столбце «Объект»;

– тип операции – производит поиск по столбцу «Тип операции».

Кнопка «Применить» производит поиск пользователей по заданным параметрам, а кнопка «Очистить» возвращает все строки с данными аудита к исходному виду (Рис. 47).

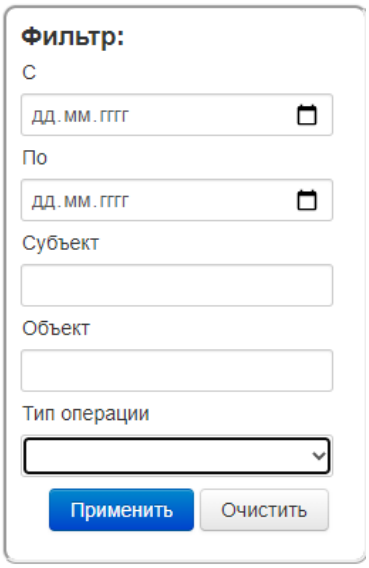

Рис. 47

Описание типов операции приведено в таблице (Таблица 3).

Таблица 3 – Описание типов операций в подсистеме администрирования.

Тип операции	Описание
Добавление	Событие, связанное с добавлением объекта
Удаление	Событие, связанное с удалением объекта
Редактирование	Событие, связанное с редактированием объекта
Выгрузка прав	Событие, связанное с выгрузкой прав
Вход	Событие, связанное со входом администратора в подсистему администрирования
Выход	Событие, связанное с выходом администратора из подсистемы администрирования
Применить права	Событие, связанное с применением прав объекта
Загрузка прав	Событие, связанное с загрузкой прав

4.11. Вкладка «Синхронизация»

Вкладка «Синхронизация» состоит из трех подпунктов: «Применить права», «Загрузить права» и «Выгрузить права» (Рис. 48).

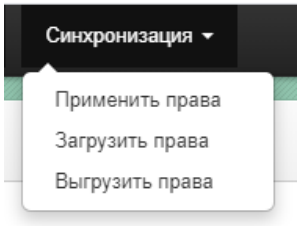

Рис. 48

4.11.1. Вкладка «Применить права»

После изменения любой информации в подсистеме администрирования Программы, необходимо синхронизировать данные с подсистемой фильтрации Программы с помощью вкладки «Применить права» (Рис. 49).

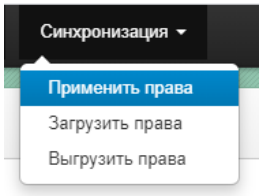

Рис. 49

Окно для синхронизации данных подсистемы администрирования с подсистемой фильтрации (Рис. 50).

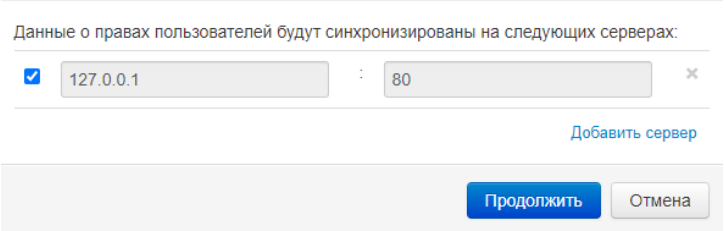

Рис. 50

В данном окне при помощи кнопки «Добавить сервер» можно добавить новые серверы подсистемы фильтрации для синхронизации данных подсистем администрирования и фильтраций. Кнопка «Продолжить» синхронизирует эти права и открывает окно с подтверждением изменений этих прав, кнопка «Отмена» закрывает окно применения прав.

К одной подсистеме администрирования можно добавить несколько подсистем фильтрации при условии, что для каждой подсистемы фильтрации будет установлена своя подсистема кэширования данных и аудит.

При успешном применении прав выводится сообщение об успешном применении прав на всех серверах подсистемы фильтрации (Рис. 51).

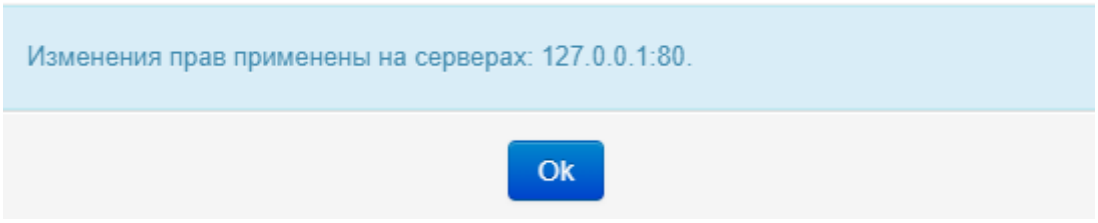

Рис. 51

Если права применились успешно не на всех серверах, уведомление показывает на каких серверах права были применены, а где нет (Рис. 52).

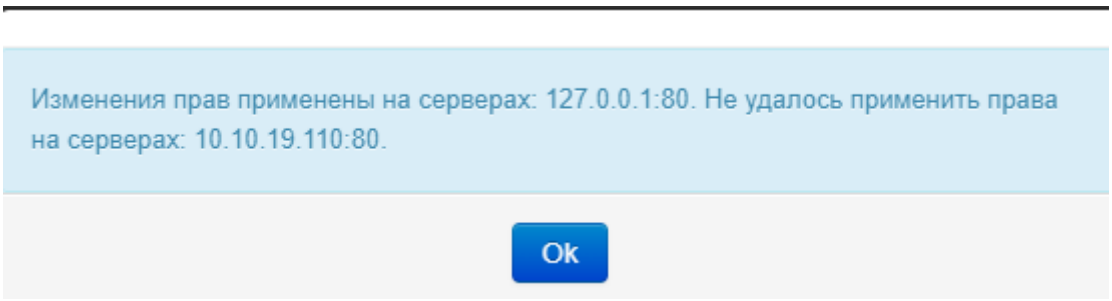

Рис. 52

При полном отсутспии соединения с серверами, выводится третий тип уведомления (Рис. 53).

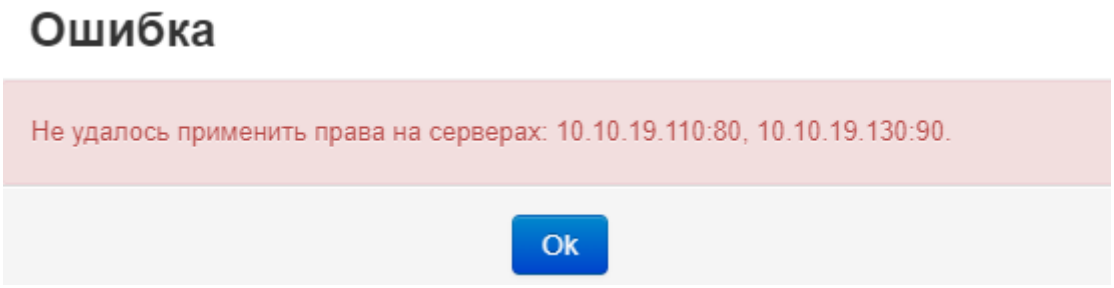

Рис. 53

4.11.2. Вкладка «Загрузить права»

Вкладка позволяет загрузить уже готовые права в Программу с локального носителя (Рис. 54). Формат загрузки XML, разрешено выбрать какие права загрузить (Функции, Пользователи, Роли), либо выбрать «Все права» или «Полная перезапись прав, с удалением старых» (можно выбрать оба флага одновременно). Кнопка «Выберите файл» позволяет выбрать нужный файл с правами из директории. Кнопка «Загрузить» загружает права с выбранной конфигурацией в Программу, а кнопка «Отмена» закрывает окно загрузки прав.

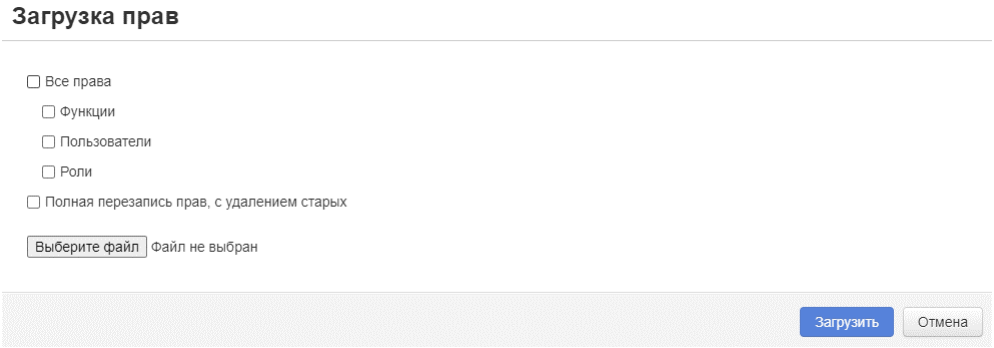

Рис. 54

4.11.3. Вкладка «Выгрузить права»

Вкладка позволяет сохранить права в Программе на локальный носитель. Можно выбрать формат файла. Для формата файла XML выгружать разрешено категории «Функции», «Пользователи», «Роли», кнопка «Выгрузить» позволяет выгрузить файл прав, а кнопка «Отмена» закрывает окно загрузки прав (Рис. 55).

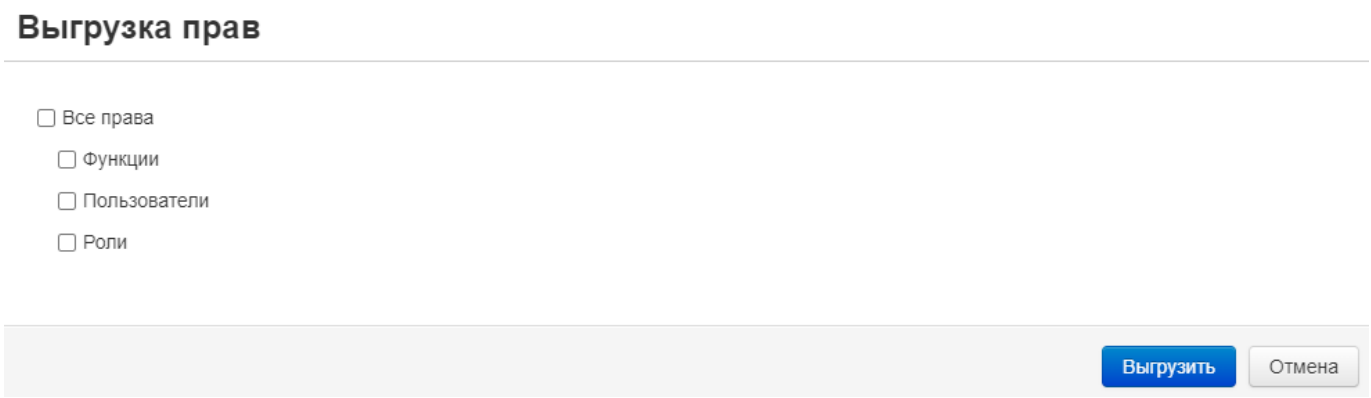

Рис. 55

4.12. Применение прав

Кнопка применения прав представлена на рисунке (Рис. 56).

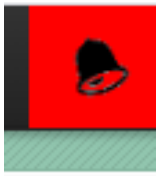

Рис. 56

После наведения на кнопку всплывает окно изменения прав (Рис. 57), с помощью указанного окна можно применить изменения, которые произошли в настройках Программы, нажимая на кнопку «Применить права».

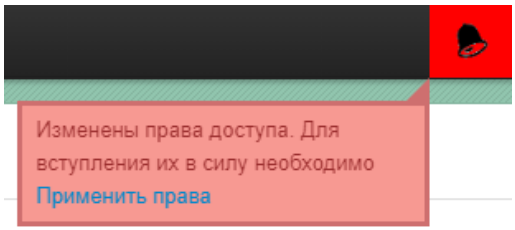

Рис. 57

4.13. Выход из подсистемы администрирования

При нажатии на стрелку, всплывает подпункт «Выход» (Рис. 58).

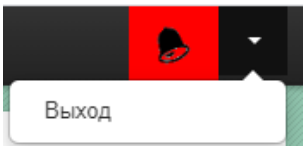

Рис. 58

После нажатия «Выход» происходит выход администратора из подсистемы администрирования и открывается страница аутентификации (Рис. 59).

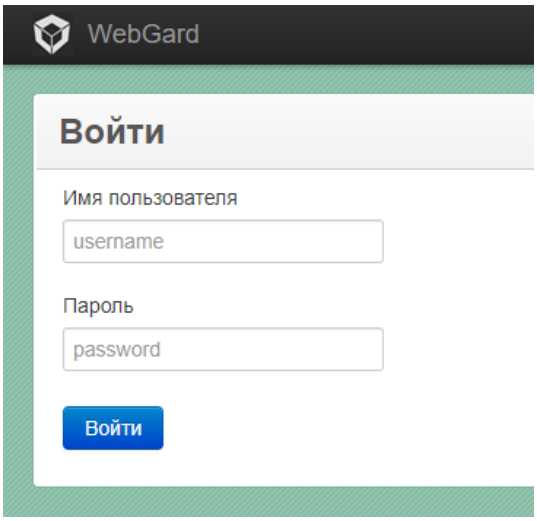

Рис. 59

4.14. Вход в защищаемую информационную систему

Вход в ЗИС через Программу может осуществляться двумя способами:
– аутентификация по логину и паролю;
– двухфакторная аутентификация.

4.14.1. Аутентификация пользователя по логину и 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. 60).

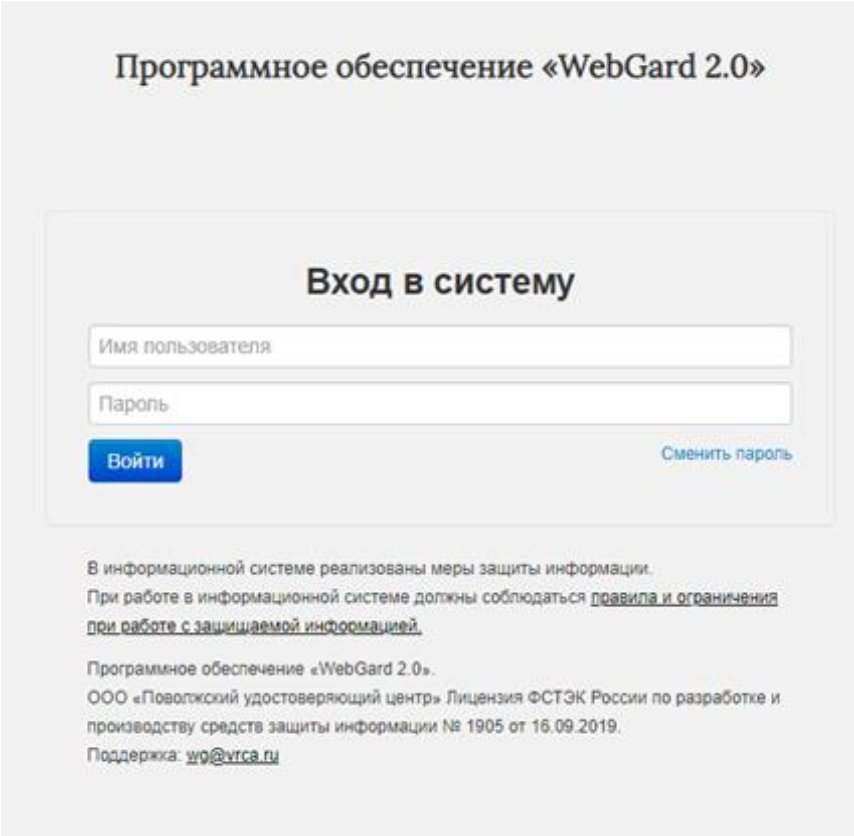

Рис. 60

В случае успешной попытки входа в ЗИС, открывается окно с сообщением об успешной аутентификации, датой и временем предыдущей успешной и неуспешной попытке аутентификации (Рис. 61).

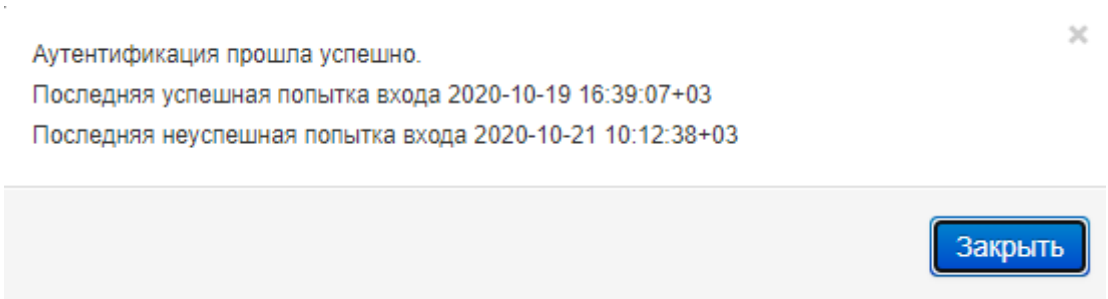

Рис. 61

В случае неуспешной попытки входа, Программа выводит ошибку «Неправильный логин и/или пароль» (Рис. 62).

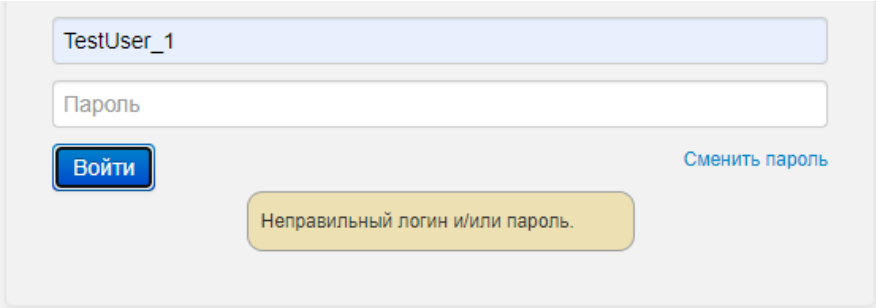

Рис. 62

Программа предупреждает пользователя, прошедшего аутентификацию, о времени истечения срока действия пароля. Период времени оповещения пользователя устанавливается администратором (Рис. 63).

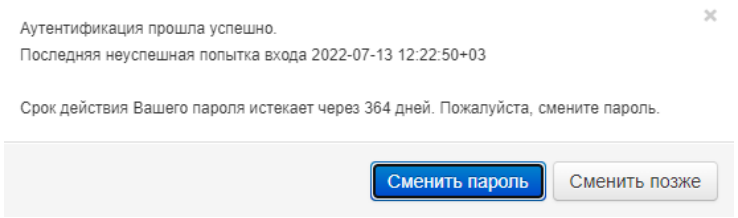

Рис. 63

Рекомендуется в течение данного периода изменить пароль на новый.

Так же Программа после окончания срока действия пароля выводит другое сообщение (Рис. 64).

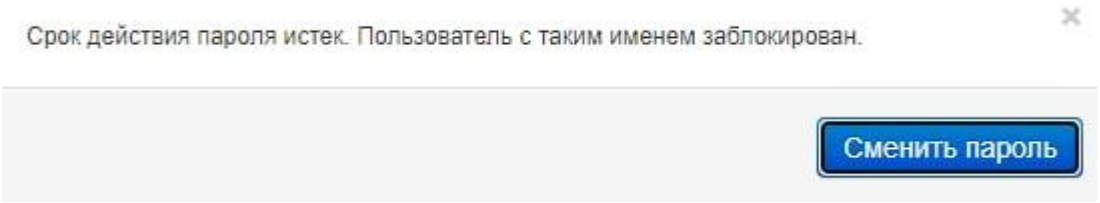

Рис. 64

В данном случае Программа требует от пользователя изменить пароль. Пока пароль не будет изменен, пользователю будет заблокирован доступ к ЗИС.

Для смены пароля, пользователю необходимо заполнить следующие поля: «Логин», «Текущий пароль», «Новый пароль» и «Подтверждение» (Рис. 65).

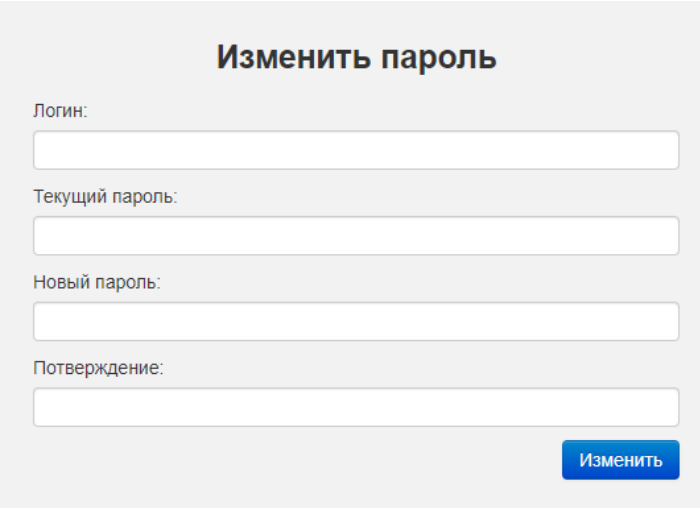

Рис. 65

Примечание: при замене пароля в ПО «WebGard 2.0» пароль в ЗИС не меняется. Для корректной работы необходимо поменять пароль пользователя в ЗИС на идентичный в ПО «WebGard 2.0».

4.14.2. 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 (Рис. 66).

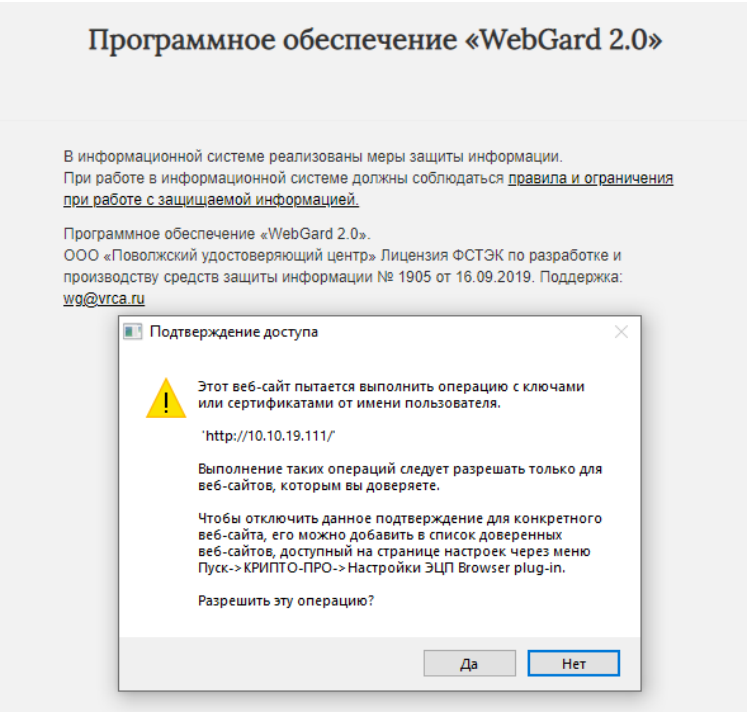

Рис. 66

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. 67).

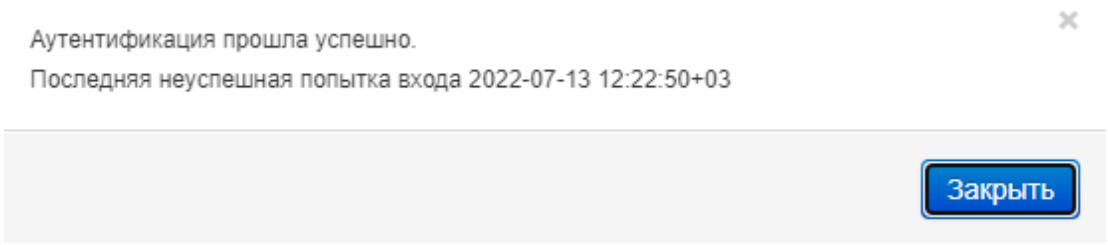

Рис. 67

Для реализации двухфакторной аутентификации необходимо соблюдение требований:

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

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

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

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

5) 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.

4.14.3. Окно правил и ограничений при работе с защищаемой информацией

При нажатии на ссылку «правила и ограничения при работе с защищаемой информацией» откроется окно (Рис. 68).

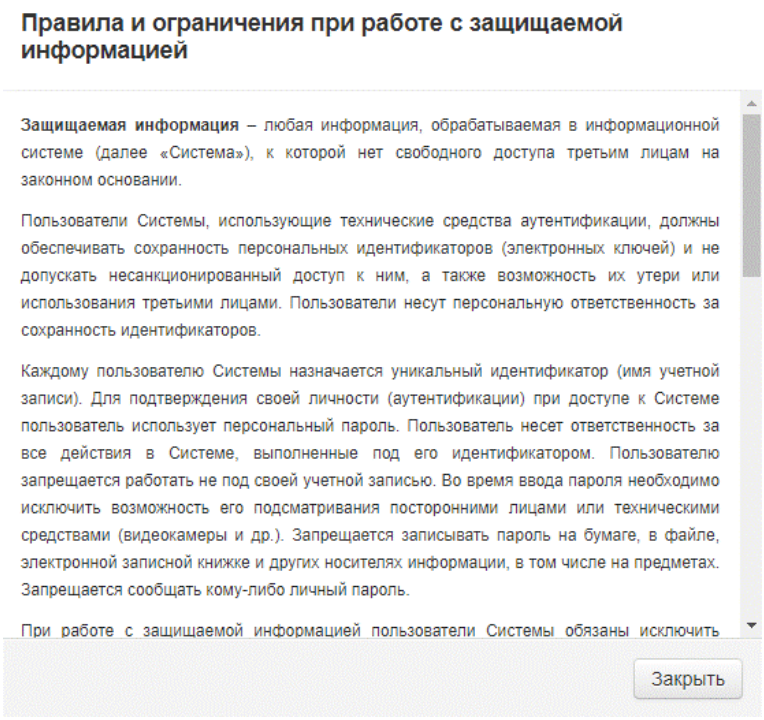

Рис. 68

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

4.14.4. Выход из Программы

Для выхода из Программы необходимо нажать кнопку «Выход». Пример кнопки «Выход» приведен на рисунке (Рис. 69).

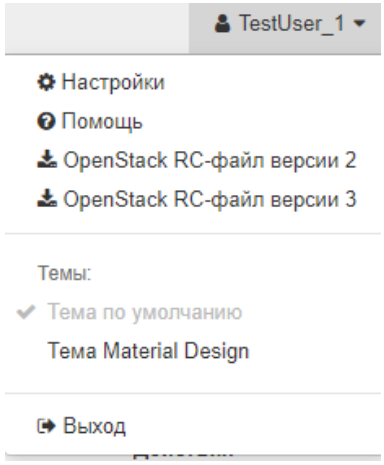

Рис. 69

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. 70).

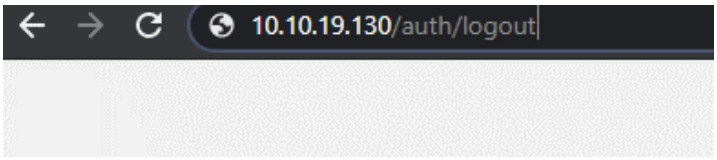

Рис. 70

После выполненных действий Программа завершит сессию пользователя и откроет страницу авторизации Программы (Рис. 71).

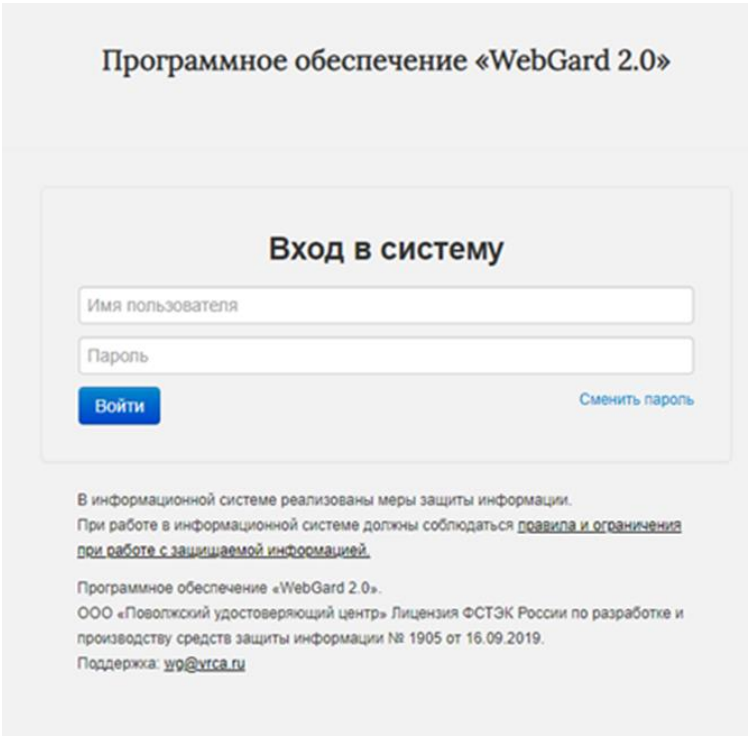

Рис. 71

5. ФИЛЬТРАЦИЯ ЗАПРОСОВ

5.1. Специальные символы

Регулярное выражение – формальный язык поиска и осуществлений манипуляций со строками в тексте, основанный на использовании специальных символов. Для создания регулярных выражений в Программе используются символы:

1) флаги, влияющие на поиск:

– i – поиск не зависит от регистра, не существует разницы между A и a;

– g – этот флаг ищет все совпадения, без этого флага ищется только первой совпадение;

– m – многострочный режим;

– s – включает режим «dotall», при котором точка «.» может соответствовать символу перевода строки \n;

– u – включает полную поддержку UTF-8;

– y – режим поиска на конкретной позиции в тексте.

– Классы:

– \d – класс «цифра», соответствует любой одной первой цифре, то же самое, что и [0-9];

– \D – любой символ, кроме цифры;

– \w – класс «слово», соответствует любой одной первой букве, то же самое, что и [a-zA-Z0-9_];

– \W – любой символ, кроме \w;

– \s – класс «пробелы», любые пробельные символы, то же самое, что и [\t\n\v\f\r];

– \S – любой символ, кроме \s;

– . – это специальный символьный класс, который соответствует «любому символу, кроме новой строки».

2) якоря:

– ^ – символ, обозначающий начало строки, при помощи которого Программа ищет совпадение с началом текста;

– $ – символ, обозначающий конец строки, при помощи которого Программа ищет совпадение с концом текста;

– m – многострочный режим, влияющий только на якоря «^» и «$».

3) экранирование, диапазоны, квантификаторы:

– g – флаг, при помощи которого происходит поиск всех совпадений, а не только первого символа;

– \ – экранирование или буквальное совпадение. Программа ищет буквальное совпадение строки или данную часть строки в длинном URL. Экранирование разрешает использовать специальные символы (^$.), которые имеют какой-то функционал в регулярных выражениях;

– [nbc] – несколько символов или символьных классов в скобках означают «искать любой символ из заданных»;

– [^nbc] – исключающий диапазон, означает любой символ, за исключением добавленных в скобки;

– | – альтерация соответствует выражению «ИЛИ», означает то же самое, что [nbc];

– {n} – число или диапазон значений в фигурных скобках;

– + – частный случай {n}, «один или более», означает {1,};

– ? – частный случай {n}, «ноль или один», означает {0,1}. По сути, делает символ необязательным;

– * – частный случай {n}, обозначающий {0,}. То есть символ может повторяться много раз или отсутствовать.

5.2. Изучение ЗИС

Для правильного использования функционала Программы по созданию функций администратору необходимо определить тип и принцип работы защищаемого web-сервера.

В качестве примера ЗИС используется платформа виртуализации на базе гипервизора KVM под управлением ПО OpenStack с графическим интерфейсом администрирования Horizon и/или ПО AccentOS и WordPress 5.5.3.

Пример: при использовании модулей, предназначенных для преобразования URL, необходимо блокировать не только видимый URL, но и URL, на который перенаправляет модуль.

5.3. Работа с подсистемой фильтрации

Вид страницы «Инстансы» с URL (/dashboard/project/instances/) представлен на рисунке (Рис. 72).

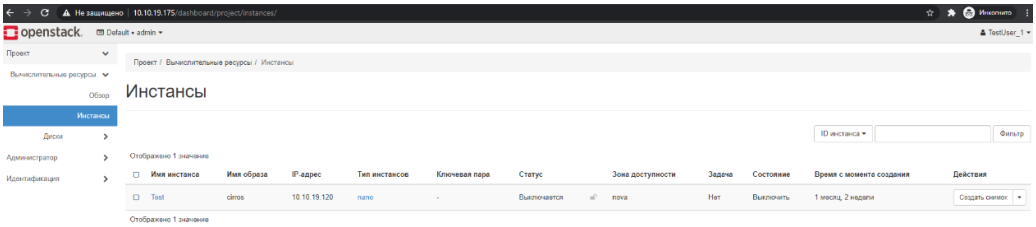

Рис. 72

Страница «Инстансы» находится во вкладке «Вычислительные ресурсы», которая располагается во вкладке «Проекты». На данной странице находится вкладка «Создать снимок» и открывающийся список, который содержит «Перестроить инстанс».

При нажатии происходит открытие окна, но при этом URL в адресной строке не изменился (Рис. 73).

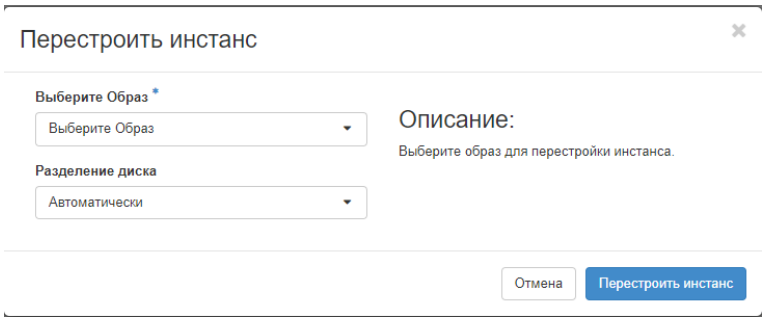

Рис. 73

Чтобы запретить пользователю открывать это окно, необходимо закрыть окно «Перестроить инстанс», нажать клавишу F12. В новом окне откроется DevTools. Нажать кнопку «Перестроить инстанс» еще один раз. В окне DevTools появляется новый используемый файл (Рис. 74).

Рис. 74

Выбрать файл «rebuild». Откроется информация о файле. Необходимо скопировать Request URL (/dashboard/project/instances/378c85ce-cda5-4203-9220-5dcdb505c760/rebuild) (Рис. 75).

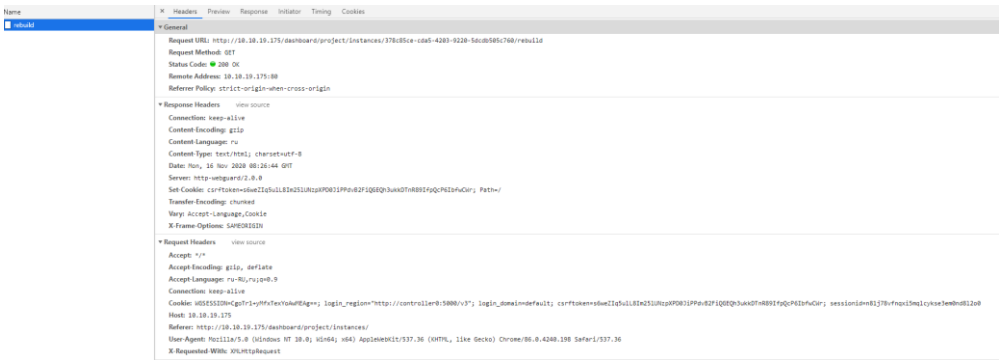

Рис. 75

Далее необходимо перейти в подсистему администрирования, создать модуль «Вычислительные ресурсы», добавить функцию с названием «Перестроить.инстанс» в этом модуле и вставить скопированный URL в пустую строку рядом с URL (Рис. 76).

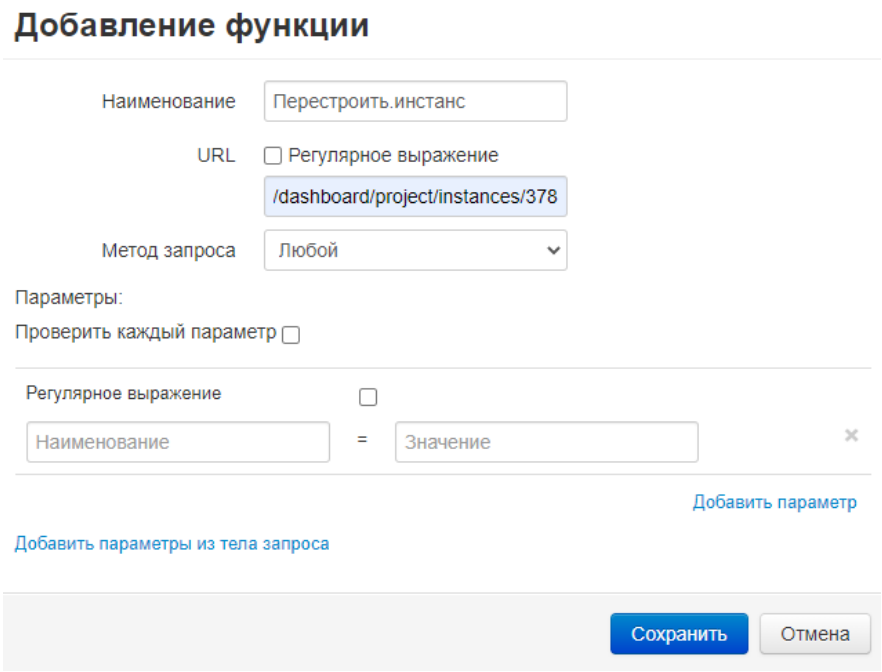

Рис. 76

Вместо постоянного URL можно использовать регулярные выражения. Для этого необходимо поставить галочку во флаге «Регулярное выражение» напротив URL. И заполнить строку URL. Вместо 378c85ce-cda5-4203-9220-5dcdb505c760 можно записать соответствующее регулярное выражение: [\w\d]{8}-[\w\d]{4}-[\w\d]{4}-[\w\d]{4}-[\w\d]{12} (Рис. 77).

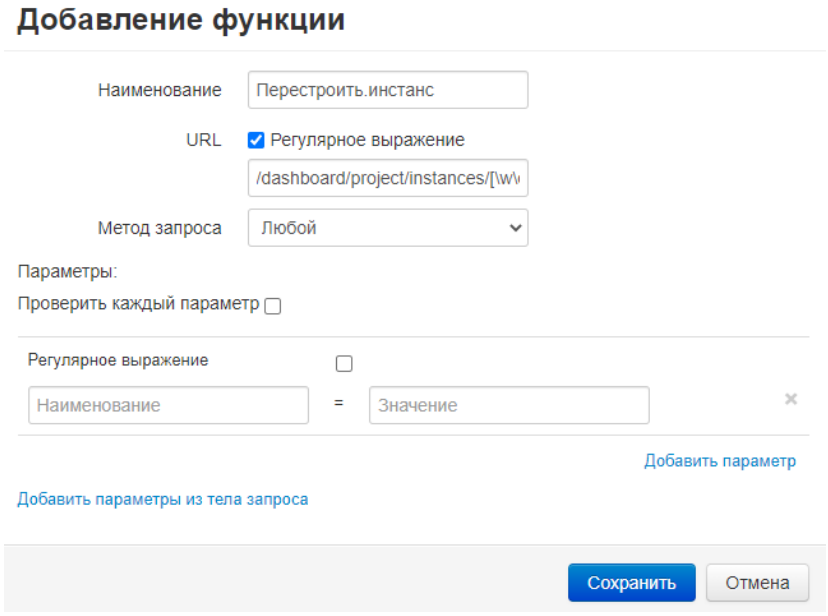

Рис. 77

Нажать кнопку «Сохранить», открыть вкладку «Роли» и привязать функцию к роли «test», и привязать пользователя TestUser_1 к роли. Применить права.

Перейти в подсистему фильтрации, пройти аутентификацию пользователем TestUser_1 и нажать кнопку «Перестроить инстанс». Окно «Перестроить инстанс» не открывается.

Раскрыть вкладку «Администратор», далее открываются «Вычислительные ресурсы» и «Диск». При нажатии на вкладку «Вычислительные ресурсы» откроется 4 вкладки: «Гипервизоры», «Инстансы», «Типы инстансов», «Образы» (Рис. 78).

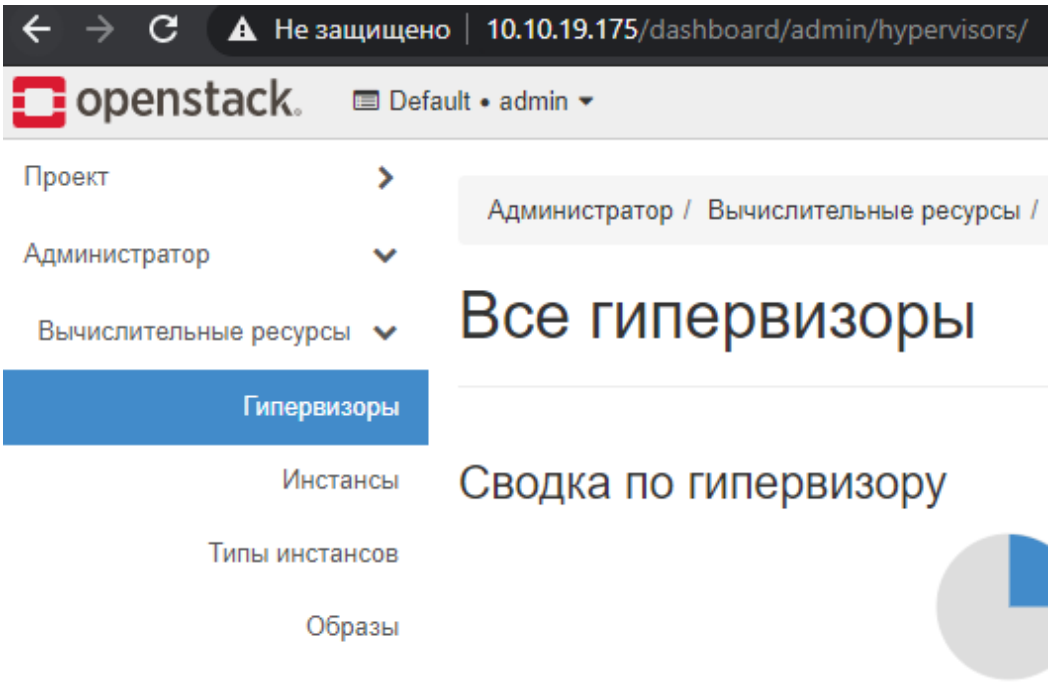

Рис. 78

Необходимо заблокировать все ресурсы, принадлежащие вкладке «Администратор».

Перейти в подсистему администрирования, добавить модуль «Администратор». Добавить функцию с названием «Администратор» в этом модуле. Поставить галочку во флаге «Регулярное выражение» рядом с надписью «URL» и записать в строку URL следующую запись: `^\/dashboard\/admin\/.*$` (Рис. 79).

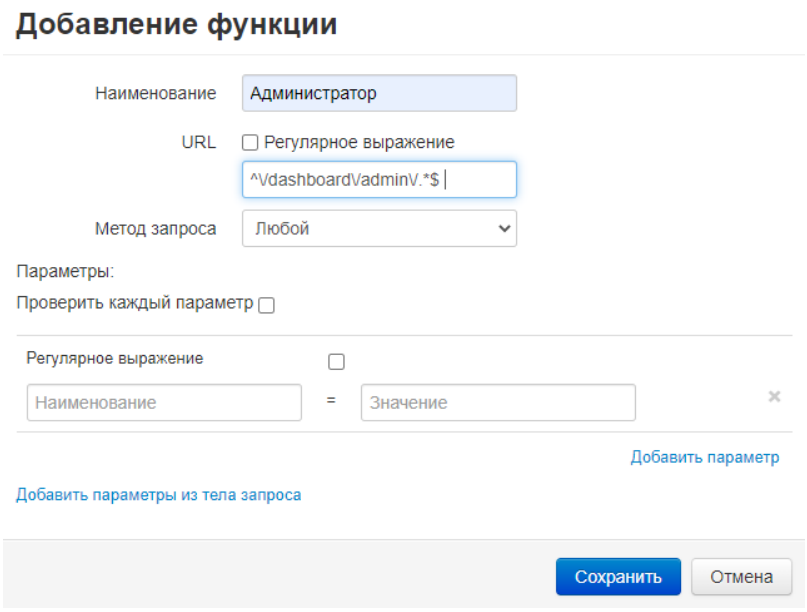

Рис. 79

Нажать кнопку «Сохранить», открыть вкладку «Роли» и привязать функцию к роли «test». Применить права.

Перейти в подсистему фильтрации, пройти аутентификацию пользователем TestUser_1 и поочередно перейти по вкладкам, которые содержит вкладка «Администратор». Во всех случаях откроется страница запрета доступа (Рис. 80).

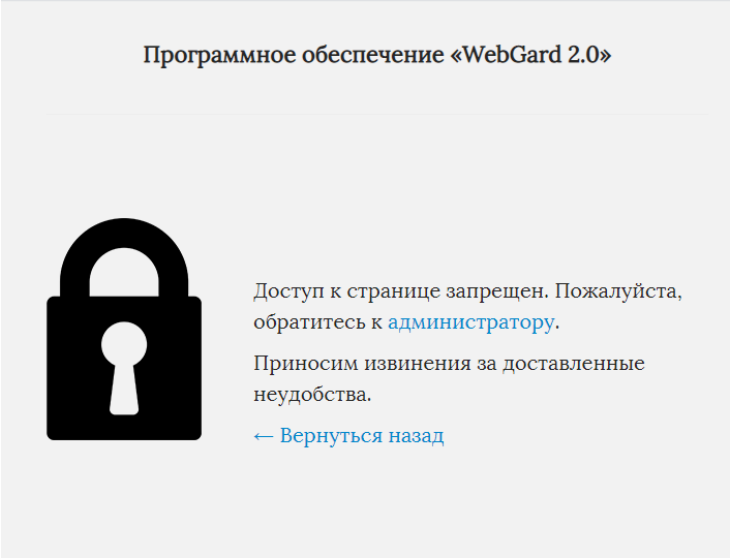

Рис. 80

5.3.1. Раздел «Параметры»

Перейти на вкладку «Pages», открывается вкладка с параметрами: post_type=page (Рис. 81).

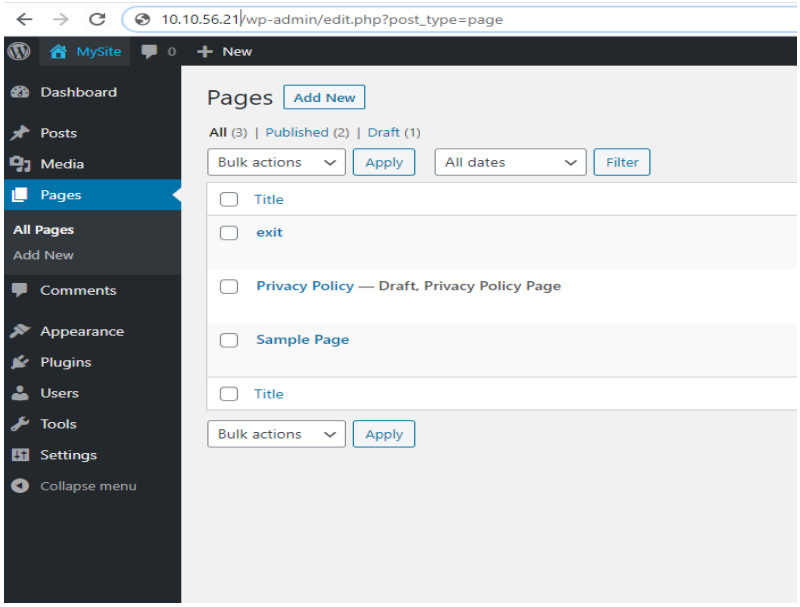

Рис. 81

Открыть DevTools и выбрать файл edit.php?post_type=page открывается окно с информацией о файле (Рис. 82).

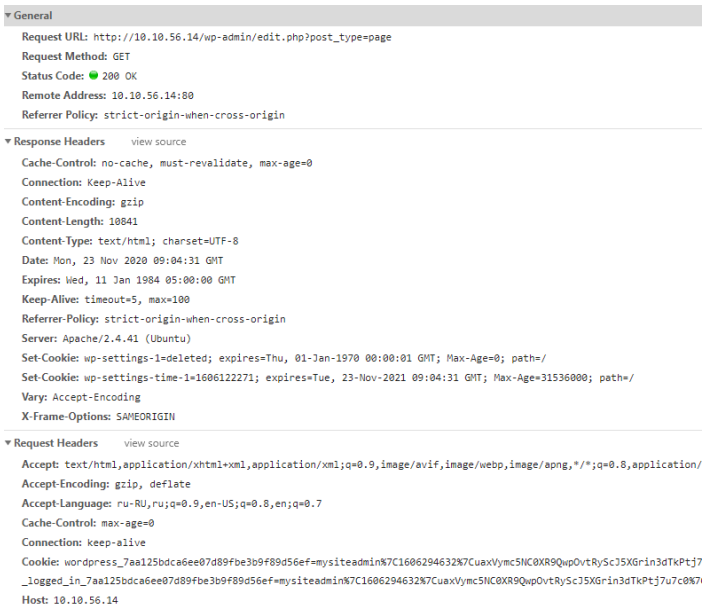

Рис. 82

В таком URL параметры могут меняться. Допустим, необходимо заблокировать только URL, где есть post_type=page. Зная метод запроса и параметры можно заблокировать эту страницу.

Необходимо перейти в подсистему администрирования, создать модуль «test», добавить функцию с названием «test1» в этом модуле. Вставить URL до знака «?» не включительно в поле URL. Добавить метода запроса «GET» и добавить параметры (Рис. 83).

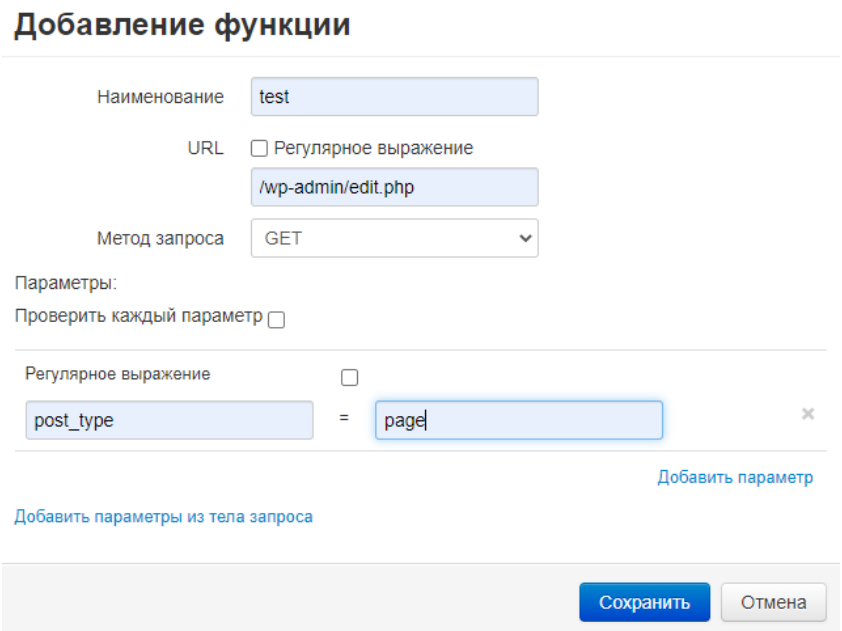

Рис. 83

Нажать кнопку «Сохранить», открыть вкладку «Роли» и привязать функцию к роли «test». Применить права.

Пройти аутентификацию пользователем «TestUser_1», Программа запрещает запуск этого ресурса пользователю (Рис. 84).

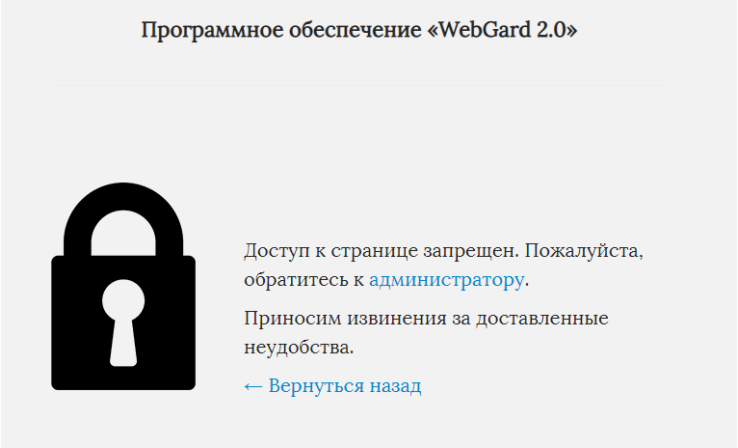

Рис. 84

Если необходимо заблокировать URL с методом запроса GET по одному параметру, но при этом передающихся параметров больше одного или необходимый параметр может стоять не первым, следует добавить новый параметр с регулярным выражением (Рис. 85) или установить галочку во флаге «Проверить каждый параметр» (Рис. 86).

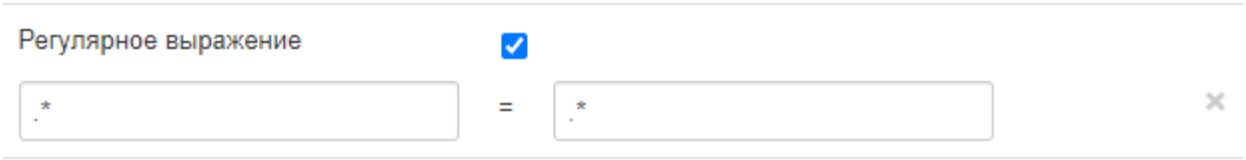

Рис. 85

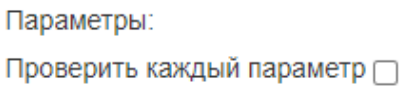

Рис. 86

Добавленный параметр позволяет Программе проверить все параметры в URL.

Перейти в подсистему фильтрации с установленным ЗИС WordPress. На странице находится ссылка «Hello world!» (Рис. 87).

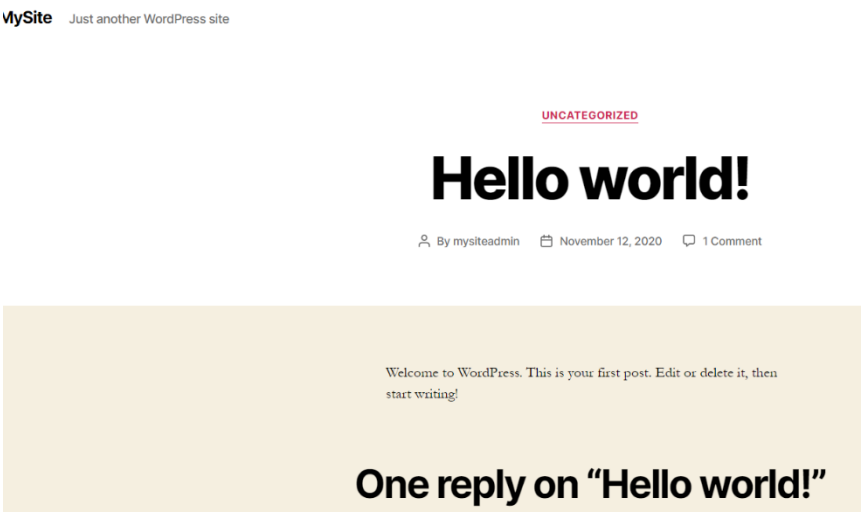

Рис. 87

Нажать клавишу F12 и перейти по ссылке «Hello world!». В DevTools высвечиваются файлы, задействованные в подгрузке страницы. Выбрать файл style.css?ver=1.5 и скопировать Reques URL (Рис. 88).

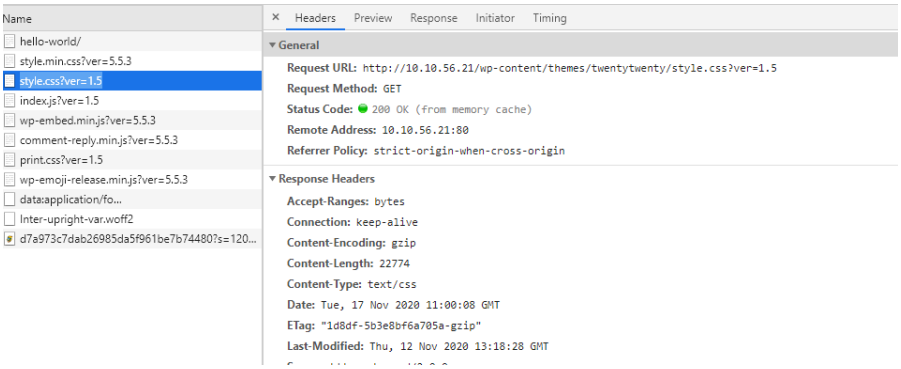

Рис. 88

Перейти в подсистему администрирования, добавить модуль «Print» и добавить функцию «Style». Вставить скопированный URL до знака вопроса не включительно (/wp-content/themes/twentytwenty/style.css) в пустую строку URL. Далее поставить галочку во флаге «Регулярное выражение» в разделе «Параметры». В первой строке вписать выражение запроса (ver), а во второй строке регулярное выражение, которое необходимо запретить (.*) (Рис. 89).

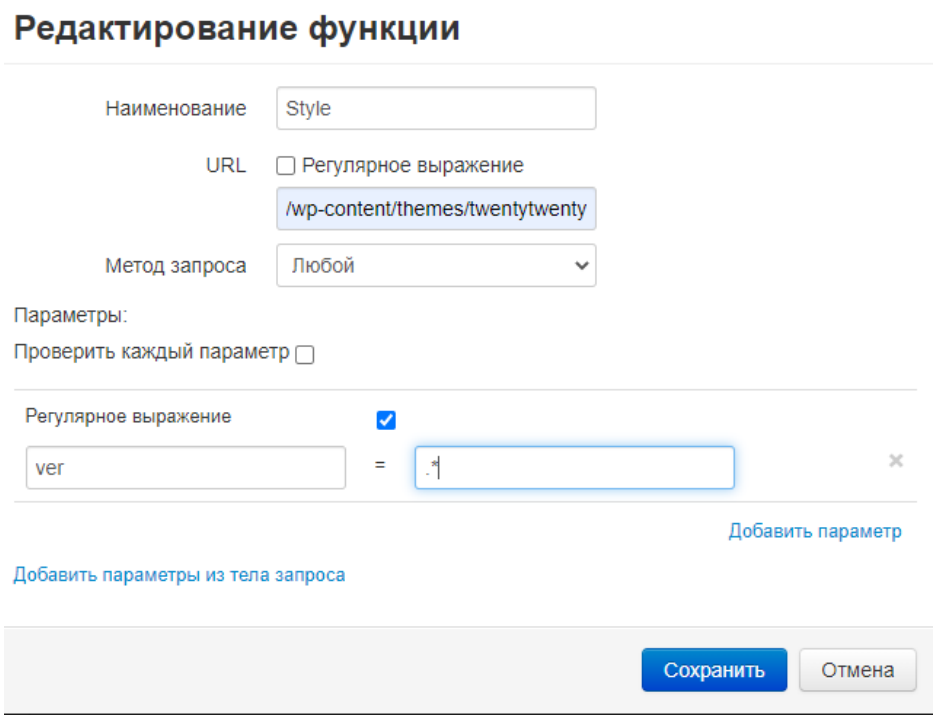

Рис. 89

Нажать кнопку «Сохранить», открыть вкладку «Роли» и привязать функцию к роли «default», а также привязать пользователя TestUser_1 к роли. Применить права.

Перейти в подсистему фильтрации, пройти аутентификацию пользователем TestUser_1 и становится понятно, что стиль страницы изменился (Рис. 90).

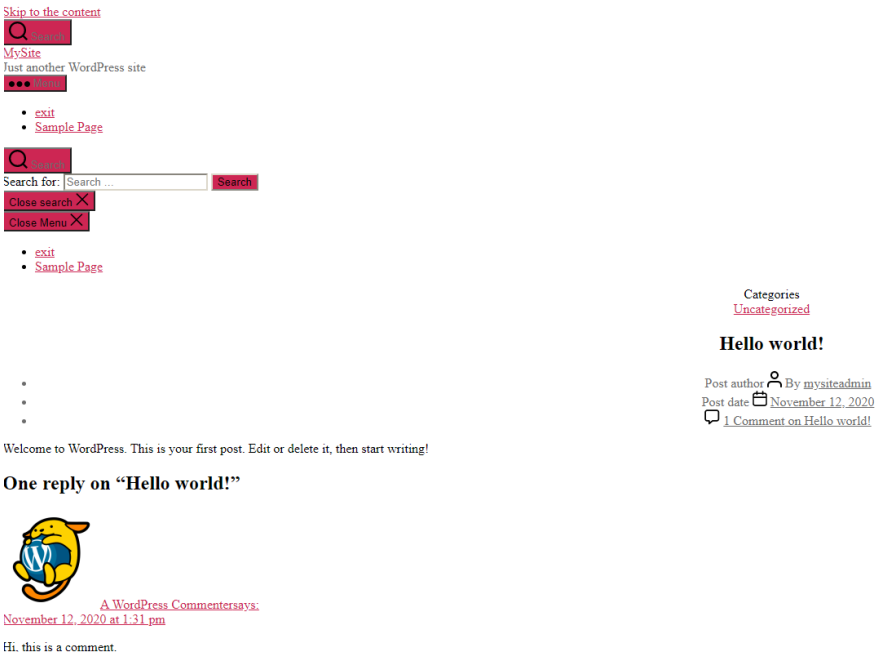

Рис. 90

Чтобы вернуть обратно заблокированный стиль необходимо удалить созданную функцию из роли.

5.3.2. Раздел «Добавить параметры из тела запроса»

Фильтр http-запросов имеет поддержку задания правил разграничения доступа по параметрам, переданным в теле http-запроса. При этом правила разграничения должны описывать формат тела. Формат тела определяется по http-заголовку Content-Type и по особенностям анализа тела запроса. HTTP-фильтр поддерживает следующие форматы тел http-запросов:

– JSON-RPC – application/json тело запроса должно быть json-объектом, где ключ – имя параметра, а значение – значение параметра;

– JSON-строка – application/json тело запроса должно быть json-строкой;

– www-form-urlencoded – тип содержимого application/x-www-form-urlencoded описывает данные формы, которые отправляются одним блоком в теле сообщения HTTP. В отличие от части URL-адреса в запросе GET, длина данных не ограничена.

Также возможно задание правила для разрешения или запрета тела http-запроса любого формата, при этом для авторизации тело запроса не собирается автоматически. В этом случае на авторизацию в качестве формата передается ключ OTHER.

Требования по авторизации параметров, переданных в теле запроса:

– по умолчанию, если не задано никакого правила, тело запроса запрещено;

– приоритет отдается точному соответствию. Если ключ подошел, а значение нет, то другие правила не рассматриваются;

– для каждого отдельного формата задается свое правило;

– если в запросе тело имеет формат, для которого не задано правило, то производится поиск правила «OTHER» Внимание! Правило «OTHER» перекрывает все правила с указанием конкретного формата. В этих случаях необходимо использовать галочку «Разрешить тело запроса другого формата»;

– чтобы создать правило «Любое тело формата, отличающегося от основного», надо создать правило для основного формата с пустыми параметрами и поставить галочку «Разрешить тело запроса другого формата»;

– правило «OTHER» рассматривается как правило «Тело запроса обязательно». Чтобы разрешить запросы без тела, нужно создать отдельное правило;

– авторизация параметров в теле запроса аналогична авторизации query-string параметров.

5.3.3. Фильтрация метода запроса «POST»

Чтобы найти методы POST в DevTools, необходимо в строке поиска добавить «method:POST». Далее в списке появляются файлы с используемым методом. Открыть файл, который необходимо будет заблокировать (В данном случае это «Удалить инстанс»). В открытом файле можно заметить вкладки (Рис. 91).

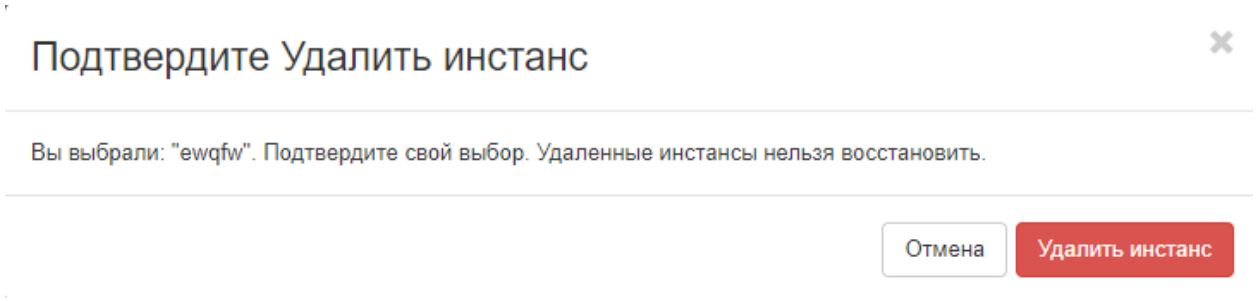

Рис. 91

Поскольку необходимо увидеть отправленные методом POST данные, то необходимо перейти во вкладку «Headers».

Открыть файл с POST запросом и перейти в тело запроса. Тут можно заметить разные параметры (Рис. 92).

Рис. 92

Можно заметить отправленные переменные и их значения в строке (Рис. 93).

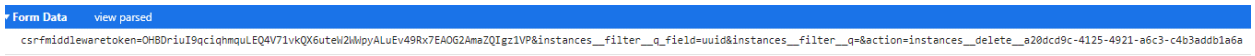

Рис. 93

Чтобы заблокировать такой запрос, необходимо во вкладке «Ресурсы» создать «Модуль», к модулю добавить «Функцию». В созданной функции добавить название Request URL-запроса. Выбрать «Метод запроса» POST. Обратить внимание на «Request Headers» и строку Content-Type. Content-Type показывает тип данных, передающиеся в теле запроса. При создании функции необходимо иметь это ввиду. Чтобы запретить доступ по параметрам из тела запроса, необходимо создать функцию в модуле. Записать URL, выбрать метод запроса POST, добавить параметры из тела запроса. Выбрать необходимый формат, который можно узнать в строке Content-Type, заполнить строки с нужными параметрами (Если такого параметра нет, то можно выбрать любой формат, добавить в него необходимые параметры и поставить галочку напротив «Разрешить параметры другого формата»). Нажать кнопку «Сохранить». Добавить к необходимой роли созданную функцию. Применить права.

При использовании этого параметра будет выводиться окно блокировки.

6. НАСТРОЙКА ПРОГРАММЫ

6.1. Настройка параметров подсистемы фильтрации Программы:

1) войти в Подсистему администрирования, которая находится по адресу http://ip-address:8080/security-manager/login.htm, где ip-address – ip-адрес сервера с установленной Подсистемой администрирования;

2) далее необходимо ввести учетные данные администратора и пройти аутентификацию;

3) после входа в подсистему администрирования необходимо создать пользователя Программы во вкладке «Пользователи» (п. 4.3.1);

4) следующим этапом настройки является создание роли во вкладке «Роли» (п. 4.5.1);

5) следующим этапом настройки Программы является добавление защищаемых ресурсов ЗИС:

– создать модуль – группу защищаемых функций ЗИС (п. 4.2.1);
– создать функцию во вкладке «Функция» (п. 4.2.4);

6) если уже имеются готовые «Ресурсы», «Пользователи», «Роли» то необходимо загрузить права (п. 4.11.2);

7) для создания администратора Программы необходимо перейти во вкладку «Администраторы» и добавить администратора (п. 4.4.1);

8) следующим этапом необходимо добавить роли созданным пользователям и ресурсам. Войти во вкладку «Роли» добавить пользователя к роли (п. 4.5.3) и добавить ресурсы к роли (п. 4.5.4);

9) также необходимо указать настройки безопасности Программы во вкладке «Настройки безопасности» согласно безопасным значениям (п.4.6.2);

10) после настройки прав в подсистеме администрирования необходимо их синхронизировать с подсистемой фильтрации (п. 4.11.1).

6.2. Проверка функционирования подсистемы фильтрации

1) для входа в ЗИС необходимо пройти аутентификацию в подсистеме фильтрации Программы, которая находится по адресу http://ip-address/auth/login?backurl=Lw, где ip-address – ip-адрес сервера с установленной Подсистемой фильтрации;

2) после аутентификации пользователя осуществляется вход в ЗИС. Функции, которые запрещены ролью Пользователя, будут недоступны. При попытке перехода к запрещенному ресурсу будет выводиться сообщение на экран (Рис. 94).

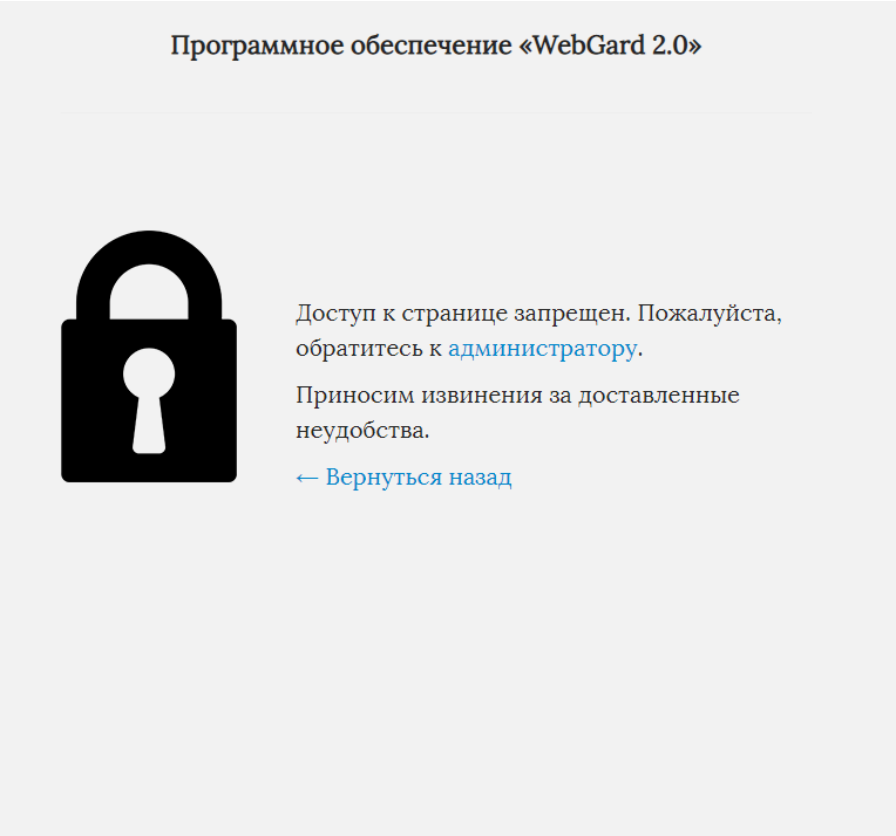
Программное обеспечение «WebGard 2.0»
Доступ к странице запрещен. Пожалуйста, обратитесь к администратору.
Приносим извинения за доставленные неудобства.
← Вернуться назад

Рис. 94