Инструкция

по настройке и установке программного обеспечения WebGard 2.0 в

в средстве виртуализации AccentOS

2022

Аннотация

Настоящий документ представляет собой руководство по развертыванию, настройке и использованию программного обеспечения WebGard 2.0 в среде виртуализации AccentOS, а также способы решения типичных проблем, возникающих при работе программы.

СОДЕРЖАНИЕ

[1. Назначение Программы 6](#_Toc111463753)

[1.1. Основные возможности Программы 6](#_Toc111463754)

[1.2. Ограничения, накладываемые на область применения Программы 15](#_Toc111463755)

[2. Условия применения 16](#_Toc111463756)

[2.1. Эксплуатационные ограничения 17](#_Toc111463757)

[3. Описание задачи 18](#_Toc111463758)

[3.1. Обработка http-запросов 18](#_Toc111463759)

[3.2. Аутентификация и авторизация субъектов доступа 18](#_Toc111463760)

[3.3. Регистрация и учет действий субъектов доступа 19](#_Toc111463761)

[4. Архитектура системы WebGard 2.0 21](#_Toc111463762)

[5. Создание виртуальных машин WebGard 2.0 23](#_Toc111463763)

[5.1. Создание с виртуальной машины из диска 23](#_Toc111463764)

[5.2. Создание виртуальной машины из снимка виртуальной машины 24](#_Toc111463765)

[6. Установка WebGard 2.0 В среде AccentOS 25](#_Toc111463766)

[6.1. Работа с сетевыми настройками в интерфейсе AccentOS 25](#_Toc111463767)

[6.2. Настройка второго сетевого интерфейса в виртуальной машине 25](#_Toc111463768)

[6.3. Настройка DNS 27](#_Toc111463769)

[6.4. Проверка доступности с помощью скрипта conn\_checker.sh 27](#_Toc111463770)

[6.5. Настройка скрипта для создания бэкапов 28](#_Toc111463771)

[6.6. Настройка и запуск конфигурации виртуальных машин 29](#_Toc111463772)

[6.7. Проверка работы кластера виртуальных машин 30](#_Toc111463773)

[7. Подключение к подсистеме фильтрации и подсистеме администратора WebGard 2.0 31](#_Toc111463774)

[7.1. Вход в подсистему администрирования и предварительные настройки 31](#_Toc111463775)

[7.1. Вход в подсистему фильтрации 31](#_Toc111463776)

[7.2. Вход в подсистему фильтрации с помощью rs-client AccentOS 31](#_Toc111463777)

[8. Организация работы программы WebGard 2.0 в режиме высокой доступности 32](#_Toc111463778)

[8.1. Проверка кластера виртуальных машин 32](#_Toc111463779)

[8.2. Создание снимка виртуальной машины с помощью интерфейса AccentOS 32](#_Toc111463780)

[8.3. Восстановление виртуальной машины из снимка виртуальной машины 32](#_Toc111463781)

[9. Дополнительное взаимодействие с системой WebGard 2.0 34](#_Toc111463782)

[9.1. Проверка кластера виртуальных машин 34](#_Toc111463783)

[9.2. Редактирование парольной политики 34](#_Toc111463784)

[9.3. Редактирование политики логина 34](#_Toc111463785)

[9.4. Удаление администратора WebGard 2.0 35](#_Toc111463786)

[Приложение 1 36](#_Toc111463787)

[Название скрипта: etcd\_cluster.sh 36](#_Toc111463788)

[Приложение 2 37](#_Toc111463789)

[Название скрипта: conn\_cheker.sh 37](#_Toc111463790)

Перечень сокращений и терминов

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

Таблица – Перечень используемых сокращений и терминов

|  |  |
| --- | --- |
| **Сокращение** | **Полное наименование** |
| HTTP | Hyper Text Transfer Protocol (протокол передачи гипертекста) |
| SQL | Structured Query Language (язык структурированных запросов) |
| URI | Uniform Resource Identifier (унифицированный идентификатор ресурса) |
| URL | Uniform Resource Locator (унифицированный указатель ресурса) |
| АС | Автоматизированная система |
| БД | База данных |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| Пользователь | Пользователь программного обеспечения «WebGard 2.0» |
| Программа | Программное обеспечение «WebGard 2.0» |
| СУБД | Система управления базой данных |
| УЦ | Удостоверяющий центр |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю России |

# Назначение Программы

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

## 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 c использованием ESMART карт и/или USB-идентификатора, поддерживаемого сертифицированной версией КриптоПро CSP:

1. с использованием сети связи общего пользования, в том числе сети Интернет;
2. без использования сети связи общего пользования.
3. 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.

1. 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:

1. установка минимальной и максимальной длины пароля в символах;
2. установка минимальной сложности пароля с определяемыми требованиями к регистру, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
3. установка требования к алфавиту пароля;
4. установка максимального времени действия пароля;

* назначение характеристик механизмов аутентификации:

1. срок, в течение которого возможно сменить пароль;
2. время жизни аккаунта (логина);
3. время, которое будет ожидать пользователь перед следующей попыткой аутентификации;
4. время, по истечении которого сбрасывается счетчик неуспешных попыток аутентификации.

* обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной администратором;
* защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

1. 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.

1. 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.

1. 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).

1. 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.

1. 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.

1. 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.

1. 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.

1. 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.

1. 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.

1. 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.

1. 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.

1. 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;

1. 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.

1. 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.

1. 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).

1. 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.

1. 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.

1. 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.

1. 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.

1. 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:

1. 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).

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

## Ограничения, накладываемые на область применения Программы

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

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

Реализация функций безопасности Программы протестирована на следующих web-серверах:

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

# Условия применения

Программа включает в себя следующие подсистемы:

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

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

Минимальные характеристики технических средств, используемых для функционирования Программы:

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

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

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

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

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

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

## Эксплуатационные ограничения

При эксплуатации Программы должны быть выполнены следующие ограничения:

1. отсутствие каких-либо сторонних сетевых маршрутов в настройках Программы и в установленных ОС;
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 только на следующих портах:

* 80;
* 5432;
* 11211
* 8080;
* 9009;
* 9010;
* 9011.

1. необходимо устранить уязвимости среды функционирования Программы посредством установки актуальных обновлений безопасности;
2. доступ к аутентификационной информации (в том числе хэшам паролей) Программы должен предоставляться только доверенному списку администраторов.

# Описание задачи

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

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

Осуществление ролевого управления доступом предусматривает выполнение следующих функций:

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

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

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

## Обработка http-запросов

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

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

## Аутентификация и авторизация субъектов доступа

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

Идентификация объектов доступа производится по их именам.

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

## Регистрация и учет действий субъектов доступа

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

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

События безопасности, регистрирующиеся в Программе:

1. вход (выход), а также попытки входа субъектов доступа в защищаемую информационную систему;
2. события, связанные с действиями от имени привилегированных учетных записей (администраторов):

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

1. события безопасности, связанные с действиями пользователей:

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

1. 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.

# Архитектура системы WebGard 2.0

Работа пользователей с WebGard 2.0 осуществляется с помощью клиентского ПО RS Client.

Система аутентификации WebGard 2.0 устанавливается на управляющие узлы в виде ВМ с ОС Альт 8.2 СП.

Система аутентификации WebGard 2.0 включает в себя:

* ПО WebGard 2.0;
* ПО Memcached (для базы правил и базы журнала);
* ПО PostgreSQL.

Система аутентификации WebGard 2.0 работает в режиме высокой доступности, для чего запускается несколько ВМ WebGard 2.0. В этом режиме работа пользователей с WebGard 2.0 осуществляется с настройками клиентского ПО RS Client через HA Proxy по порту 9365.

Система работает в режиме обслуживания двух доменов - MS AD и FreeIPA.

Для этого выполняется запуск двух копий (экземпляров) WebGard 2.0 внутри ВМ с использованием механизма Chroot. Каждый экземпляр WebGard 2.0 внутри ВМ пишет в свою базу СУБД PostgreSQL.

Для подключения к соответствующему экземпляру пользователи MS AD и FreeIPA и должны использовать разные IP адреса (у MS AD IP1 и FreeIPA IP2).

Режим высокой доступности обеспечивается для файловой системы ВМ, сервера приложения WebGard 2.0 и сервера баз данных PostgreSQL.

Высокая доступность серверов приложений WebGard 2.0 обеспечивается их одновременным запуском на двух ВМ и распараллеливанием их работы с независимыми Memcached экземплярами.

Высокая доступность серверов баз данных PostgreSQL обеспечивается их одновременным запуском на трех ВМ и организацией их бесперебойной работы с помощью ПО Patroni. Балансировка нагрузки на СУБД обеспечивается с помощью HA Proxy, встроенного в Patroni.

На двух ВМ WebGard 2.0 выполняется запуск полноценной ВМ с работающим WebGard 2.0, Patroni + PostgreSQL.

На третьей ВМ-Кворум запускается только Patroni + PostgreSQL для обеспечения кворума PostgreSQL.

Это позволяет обеспечить работу WebGard 2.0:

* в случае, когда одна ВМ WebGard 2.0 вышла из строя;
* в случае, когда ВМ-Кворум вышла из строя;
* в случае, когда одна ВМ WebGard 2.0 и ВМ-Кворум одновременно вышли из строя.

Patroni присваивает серверу СУБД на одной ВМ статус «активный» и остальным СУБД статус «пассивный». В случае выхода из строя «активной» ВМ, система выполняет автоматическое переключение в соответствии с установленным тайм-аутом. По умолчанию время тайм-аута составляет 30 сек.

После включения вышедшей из строя ВМ система скриптов синхронизации Patroni должна автоматически восстановить целостность СУБД, ввести ее в кластер со статусом «пассивный» и стартовать WebGard 2.0.

Схема взаимодействия компонентов WebGard 2.0 в кластерном двухдоменном режиме показана на рисунке (Рис. 1).

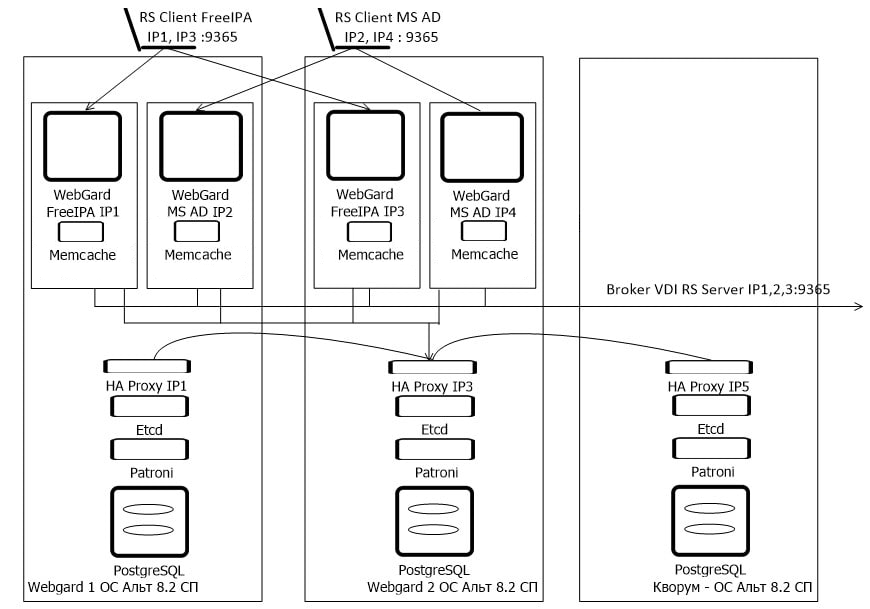


Рис. Схема взаимодействия компонентов WebGard 2.0

# Создание виртуальных машин WebGard 2.0

## Создание с виртуальной машины из диска

Для создания виртуальных машин с программным обеспечением WebGard 2.0 требуется создать 3 диска для виртуальных машин. Для этого необходимо:

1. войти в web интерфейс AccentOS;
2. перейти в раздел: Проект -> Ресурсы облачного хранилища, нажать «Диски»;
3. нажать кнопку «Создать диск»;
4. в открывшемся окне необходимо: заполнить поле «Имя диска» (например, wg-1);
5. в поле «Источник диска» выбрать «Образ»;
6. в поле «Использовать образ как источник» выбрать необходимый образ (например, wg-script-220720)

Примечание: если образ источник не видно в поле после выбора – ничего страшного. Выбор может не отображаться в поле, но диск создастся из выбранного образа.

1. в поле «Тип» выбрать «lvm»;
2. в поле «Размер» выбрать «15»;
3. нажать кнопку «Создать диск»;
4. повторить пункты 3-9 для второго и третьего диска;

Далее требуется создать 3 виртуальные машины на основе созданных дисков. Для этого необходимо:

1. перейти в раздел: Проект -> Виртуальные машины;
2. нажать кнопку «Запустить машину»;
3. перейти во вкладку «Детали»;
4. в поле «Имя виртуальной машины» ввести название для виртуальных машин – wg-1;
5. в пункте «Количество» ввести необходимое кол-во виртуальных машин - 1;
6. перейти во вкладку «Источник»;
7. в поле «Выберите источник загрузки» выбрать «Диск»;
8. в поле «Удалить диск при удалении виртуальной машины» выбрать «Нет»;
9. в разделе «Доступно» выбрать необходимый снимок виртуальной машины, нажав «стрелку вверх» Скриншот 04-08-2022 164153, например: wg-1;
10. перейти во вкладку «Тип инстанса»;
11. в разделе «Доступно» выбрать необходимый снимок виртуальной машины, нажав «стрелку вверх» C:\Users\a.zakirov\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Скриншот 04-08-2022 164153.jpg, например: 4cpu4g;
12. перейти во вкладку «Сети»;
13. в разделе «Доступно» выбрать необходимую сеть, , нажав «стрелку вверх» C:\Users\a.zakirov\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Скриншот 04-08-2022 164153.jpg, например: vlan18;
14. нажать «Запустить виртуальную машину»;
15. повторить пункты 2-14 для виртуальных машин wg-2 и wg-3.

## Создание виртуальной машины из снимка виртуальной машины

Для работы программного обеспечения WebGard 2.0 требуется установить 3 виртуальные машины. Для этого необходимо:

1. войти в web интерфейс AccentOS;
2. перейти в раздел: Проект -> Виртуальные машины, нажать «Запустить машину»;
3. перейти во вкладку «Детали»;
4. в поле «Имя виртуальной машины» ввести название для виртуальных машин - wg;
5. в пункте «Количество» ввести необходимое кол-во виртуальных машин - 3;
6. перейти во вкладку «Источник»;
7. в поле «Выберите источник загрузки» выбрать «Снимок виртуальной машины»;
8. в поле «Создать новый диск» выбрать «Нет»;
9. в разделе «Доступно» выбрать необходимый снимок виртуальной машины, нажав «стрелку вверх» Скриншот 04-08-2022 164153, например: wg-script-220720;
10. перейти во вкладку «Тип инстанса»;
11. в разделе «Доступно» выбрать необходимый снимок виртуальной машины, нажав «стрелку вверх» C:\Users\a.zakirov\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Скриншот 04-08-2022 164153.jpg, например: 4cpu4g;
12. перейти во вкладку «Сети»;
13. в разделе «Доступно» выбрать необходимую сеть, , нажав «стрелку вверх» C:\Users\a.zakirov\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Скриншот 04-08-2022 164153.jpg, например: provider;
14. Нажать «Запустить виртуальную машину».

Примечание: если при нажатии кнопки «Запустить виртуальную машину» появляется ошибка, тогда необходимо в пункте 8 в поле «Создать новый диск» указать «Да», в поле «Удалить диск при удалении виртуальной машины» указать «Да», после чего в поле «Размер диска (ГБ)» указать 16.

# Установка WebGard 2.0 В среде AccentOS

## Работа с сетевыми настройками в интерфейсе AccentOS

1. перейти в раздел: Проект -> Виртуальные машины;
2. нажать на «стрелку вниз», справа от виртуальной машины , выбрать «Отсоединить интерфейс»;



1. в открывшемся окне в поле «Порт» выбрать доступный ip-адрес и нажать кнопку «Отсоединить интерфейс»;
2. повторить пункты 2-3 для каждой виртуальной машины WebGard 2.0;
3. нажать на «стрелку вниз», справа от виртуальной машины C:\Users\a.zakirov\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Скриншот 04-08-2022 173049.jpg, выбрать «Подключить интерфейс»;
4. в открывшемся окне в поле «Сеть» выбрать сеть (например: vlan18), которую выбирали во время создания виртуальной машины, ввести необходимый ip-адрес, нажать кнопку «Подключить интерфейс»;
5. повторить для каждой виртуальной машины WebGard 2.0;
6. перезагрузить виртуальные машины;
7. повторить пункты 5-8 для второй подсети (если есть);
8. перейти в раздел Сетевые ресурсы -> Сети
9. выбираем сеть, которую выбрали в пункте 6;
10. выбираем вкладку «Порты»;
11. выбираем виртуальную машину, на которой установлен WebGard 2.0 (не кворум), справа от нее нажимаем «Редактировать порт»;
12. открываем вкладку «Группы безопасности», убираем все элементы из списка «Группы безопасности порта»;
13. возвращаемся на вкладку «Информация», убираем галочку с пункта «Безопасность порта»;
14. нажимаем кнопку «Обновление»;
15. повторяем пункты 10-16 для второй подсети;
16. повторить пункты 10-17 для второй виртуальной машины (не кворум).
17. перезагрузить виртуальные машины.

## Настройка второго сетевого интерфейса в виртуальной машине

Для подключения используются пользователь user (логин: user, пароль:user). Пароль рут пользователь: root.

1. зайти с помощью консоли на первую виртуальную машину (или через интерфейс консоли AccentOS или с помощью другого средства удаленного подключения, например, putty через сеть vlan18);
2. ввести логин и пароль пользователя, зайти через root с помощью команды

su -

1. узнать имя второго интерфейса сети:

ip a

1. необходимо проверить есть ли файл второго сетевого интерфейса в папке /etc/net/ifaces/[имя интерфейса сети]

если нет, создать командой mkdir, пример:

mkdir eth1

1. открыть (или создать) файл опций сетевого интерфейса options:

vim /etc/net/ifaces/[имя интерфейса сети]/options

изменить или добавить строки в открытом файле:

BOOTPROTO=static

TYPE=eth

CONFIG\_WIRELESS=no

CONFIG\_IPV4=yes

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. для настройки ip адреса виртуальной машины на втором сетевом интерфейсе необходимо, открыть (или создать) файл ipv4address:

vim /etc/net/ifaces/[имя интерфейса сети]/ipv4address

1. указать ip-адрес в CIDR-нотации:

Пример:

10.40.17.211/24

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. для указания маршрутизации на втором сетевом интерфейсе необходимо открыть (или создать) файл ipv4route:

vim /etc/net/ifaces/[имя интерфейса сети]/ipv4route

1. проверить, что по умолчанию установлен ip-адрес:

для второй подсети:

сеть/маска via ip-адрес шлюза

Пример:

10.40.17.0/24 via 10.40.17.254

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. перезагрузить ОС:

reboot

1. повторить пункты 1-13 для второй и третей виртуальных машин;

## Настройка DNS

1. чтобы узнать адреса DNS серверов необходимо посмотреть их в файле /etc/resolv.conf
2. для указания адресов DNS открыть (или создать) файл resolv.conf:

vim /etc/net/ifaces/[имя интерфейса сети]/resolv.conf

1. проверить DNS-серверы организации (если есть):

nameserver [DNS-сервер организации]

Пример:

nameserver 10.40.129.42

nameserver 10.40.116.2

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. перезагрузить ОС:

reboot

1. повторить пункты 1-5 для второй и третей виртуальных машин;

## Проверка доступности с помощью скрипта conn\_checker.sh

1. после перезагрузки, необходимо проверить доступность виртуальных машин между собой, с ipa и с ms ad, для этого вводим команду:

vim /home/user/conn\_checker.sh

если файла нет, содержимое скрипта находится в Приложении 2;

1. в открывшемся файле прописываем ip-адреса 1, 2, и 3 виртуальных машин, ms ad, ipa, сохраняем;
2. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
3. запускаем скрипт командой

bash /home/user/conn\_checker.sh

1. если в выводе, справа от ip-адреса узла написано «ok» - доступ есть, если «failed» - доступа нет, пример можно увидеть на рисунке (Рис. 2).

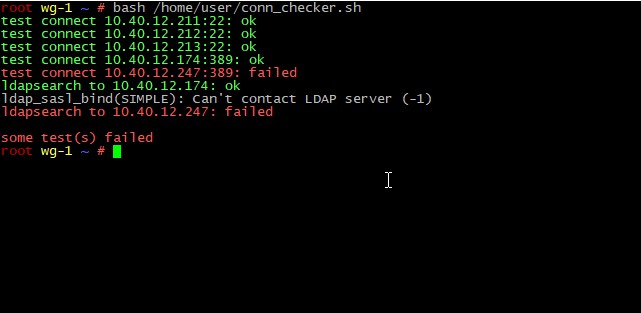


Рис. Проверка доступности

## Настройка скрипта для создания бэкапов

1. необходимо отредактировать скрипт etcd\_cluster.sh, для этого вводи команду

vim /usr/local/bin/etcd\_cluster.sh

если файл отсутствует, его содержимое можно найти в Приложении 2.

1. в строках, которые начинаются с ssh, необходимо поменять grep 9\:2380 и http://10.248.144.9:2380 на ip-адрес виртуальной машины WebGard 2.0, например

grep [последняя цифра ip-адреса текущей виртуальной машины]\:2380

и

http://[ip-адрес текущей виртуальной машины]:2380

1. в строках, которые начинаются с ssh, необходимо поменять wg2 на название другой виртуальной машины WebGard 2.0, например

* для wg1 – меняем на wg2;
* для wg2 – меняем на wg3;
* для wg3 – меняем на wg1;

Пример для wg1:

ssh wg2 -o StrictHostKeyChecking=no "ETCDCTL\_API=3 etcdctl member remove \`ETCDCTL\_API=3 etcdctl member list | grep 211\:2380 | sed 's|,.\*||g'\`"

ssh wg2 -o StrictHostKeyChecking=no "ETCDCTL\_API=3 etcdctl member add --peer-urls='http://10.40.18.211:2380' etcd1"

1. повторить пункты 1-4 для всех трех виртуальных машин WebGard 2.0.

## Настройка и запуск конфигурации виртуальных машин

Для подготовки к конфигурации виртуальных машин необходимо на первой виртуальной машине:

1. ввести команду:

vim /root/.wg\_init.conf

1. в открывшемся файле необходимо ввести ip-адреса в соответствии с таблицей (Таблица 2);

Таблица Таблица ip-адресов

|  |  |
| --- | --- |
| **Название** | **Описание** |
| wg1ipa\_ip | ip-адрес первой виртуальной машины, связанной с ipa, на которую будут заходить с ОС Linux (первичный адрес сервера для rs client) |
| wg1ad\_ip | ip-адрес первой виртуальной машины, связанной с ms ad, на которую будут заходить с ОС Windows (первичный адрес сервера для rs client) |
| wg2ipa\_ip | ip-адрес второй виртуальной машины, связанной с ipa, на которую будут заходить с ОС Linux (вторичный адрес сервера для rs client) |
| wg2ad\_ip | ip-адрес второй виртуальной машины, связанной с ms ad, на которую будут заходить с ОС Windows (вторичный адрес сервера для rs client) |
| wg3\_ip | ip-адрес третьей виртуальной машины, кворум |
| ipa\_ip | ip-адрес виртуальной машины с ipa |
| ad\_ip | ip-адрес виртуальной машины c ms ad |
| rs1\_ip | ip-адрес домена облака AccentOS, на котором находятся виртуальные машины |

Все ip адреса, указанные в таблице, должны быть различными. Если вы не знаете, какой указать ip-адрес, можно указать любой свободный. Пример:

* wg1ipa\_ip – ip адрес первой виртуальной машины;
* wg1ad\_ip – свободный ip-адрес;
* wg2ipa\_ip – ip адрес второй виртуальной машины;
* wg2ad\_ip – свободный ip-адрес;
* wg3\_ip - ip адрес третьей виртуальной машины.

При указании вторичного ip-адреса необходимо указать адрес из той же подсети, что первичная (например, vlan18). Пример заполнения на рисунке (Рис. 3).

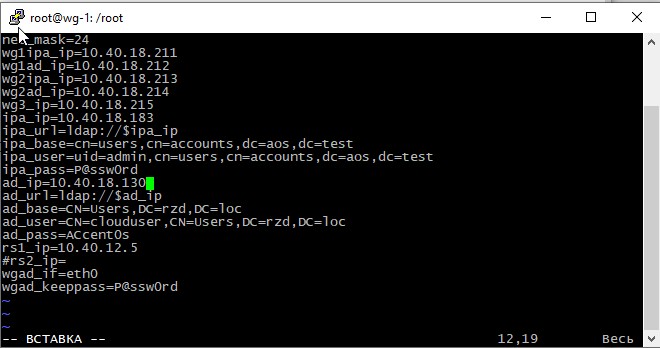


Рис. Пример заполненния wg\_init.conf

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. запустить скрипт конфигурации виртуальных машин командой:

bash /home/user/configure\_wg.sh

Примечание: после запуска, скрипт начинает настройку всех трех виртуальных машин. Изменения сильно влияют на все 3 виртуальные машины, поэтому стоит перепроверить правильность настройки виртуальных машин (в особенности файл wg\_init.conf). Для проверки доступности виртуальных машин друг до друга стоит повторить пункт 6.4.

1. дождаться завершения работы скрипта.

## Проверка работы кластера виртуальных машин

После завершения работы скрипта configure\_wg.sh, стоит проверить находятся ли виртуальные машины в кластере. Для этого необходимо выполнить команду:

ETCDCTL\_API=3 etcdctl endpoint status --cluster -w table

все 3 виртуальные машины должны находится в кластере.

# Подключение к подсистеме фильтрации и подсистеме администратора WebGard 2.0

## Вход в подсистему администрирования и предварительные настройки

Подсистема администрирования будет доступна по адресу: http[://wg\_ip:8080/security-](http://localhost:8080/security-manager/login.htm)manager/login[.](http://localhost:8080/security-manager/login.htm)htm (wg\_ip – ip-адрес первой или второй виртуальной машины). Необходимо перейти на данную ссылку и ввести логин – пароль администратора (по умолчанию логин admin, пароль admin).

Перейти во вкладку «Администраторы», выделить строку с администратором «admin», нажать кнопку «Редактировать», изменить пароль на более сложный (пароль должен состоять минимум из 8 символов и содержать 1 букву верхнего регистра, 1 букву нижнего регистра и 2 цифры), добавить существующую почту администратора.

## Вход в подсистему фильтрации

Подсистема фильтрации будет доступна по адресу: http[://wg\_ip:80](http://localhost:8080/security-manager/login.htm) (wg\_ip – ip-адрес первой или второй виртуальной машины) (Рис. 4). Необходимо будет ввести домен, логин, парол пользователя (например rgdipa vdi\_user1 P@ssw0rd).



Рис. Адрес посистемы фильтрации

## Вход в подсистему фильтрации с помощью rs-client AccentOS

Для входа в систему через rs client AccentOS необходимо выполнить следующие действия:

1. открыть приложение rs-client;
2. ввести значения в поля «Логин», «Пароль», «Проект»;
3. нажать подключиться;
4. после подключения откроется новая рабочая сессия, в ней открыть приложение «Веб-браузер Firefox»;
5. войти в подсистему фильтрации, как описано в разделе 7.1.

При указании первичного и вторичного ip адресов в настройках необходимо следовать таблице ip адресов (Таблица 2). При указании адресов, также не забудьте указать правильный домен.

# Организация работы программы WebGard 2.0 в режиме высокой доступности

## Проверка кластера виртуальных машин

Для подготовки к созданию резервной копии виртуальной машины необходимо:

1. проверить, что виртуальные машины находятся в одном кластере, для этого необходимо выполнить следующую команду:

ETCDCTL\_API=3 etcdctl endpoint status --cluster -w table

все 3 виртуальные машины должны находится в кластере;

1. необходимо проверить и отредактировать файл конфигураций etcd:

vim /etc/etcd/etcd.conf

1. в открывшемся файле необходимо найти строку ETCD\_INITIAL\_CLUSTER\_STATE в ней необходимо поменять «existing» на «new», пример:

ETCD\_INITIAL\_CLUSTER\_STATE="new"

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. повторить пункты 2 – 4 для каждой виртуальной машины.

## Создание снимка виртуальной машины с помощью интерфейса AccentOS

Для создания снимка виртуальной машины необходимо:

1. выделяем все три виртуальные машины, проставляя галочки слева от их названия;
2. нажимаем кнопку «Действие», выбираем «Выключить машины»;
3. справа от виртуальной машины выбираем кнопку со стрелкой вниз Скриншот 04-08-2022 173049, выбираем «Создать снимок»;
4. в открывшемся окне в поле «Имя снимка» пишем название создаваемого снимка виртуальной машины;
5. нажимаем кнопку «Создать снимок»;
6. повторяем пункты 3 – 5 для каждой виртуальной машины.

## Восстановление виртуальной машины из снимка виртуальной машины

Для восстановления виртуальной машины из снимка виртуальной машины:

1. справа от виртуальной машины выбираем кнопку со стрелкой вниз Скриншот 04-08-2022 173049, выбираем «Выключить машину»;
2. когда машина выключилась, справа от виртуальной машины выбираем кнопку со стрелкой вниз Скриншот 04-08-2022 173049, выбираем «Перестроить машину»;
3. в открывшемся окне в поле «Выберите образ» выбираем созданный ранее снимок виртуальной машины;
4. нажимаем «Перестроить машину»;
5. после окончания процесса восстановления, запускаем виртуальную машину, выбрав справа от виртуальной машины кнопку со стрелкой вниз Скриншот 04-08-2022 173049, выбрать «Запустить машину»;
6. необходимо проверить настройки сетевых интерфейсов, для этого повторяем пункты из раздела 6.2;
7. необходимо проверить и отредактировать файл конфигураций etcd:

vim /etc/etcd/etcd.conf

1. в открывшемся файле найти строку ETCD\_INITIAL\_CLUSTER\_STATE в ней поменять «existing» на «new», пример:

ETCD\_INITIAL\_CLUSTER\_STATE="new"

1. сохранить и выйти из файла, нажав клавишу «esc» и набрав «:wq!», нажать клавишу «Enter»;
2. выполнить перезагрузку виртуальной машины командой:

reboot

# Дополнительное взаимодействие с системой WebGard 2.0

## Проверка кластера виртуальных машин

Для того, чтобы проверить находятся ли виртуальные машины в кластере, необходимо выполнить следующую команду:

ETCDCTL\_API=3 etcdctl endpoint status --cluster -w table

## Редактирование парольной политики

Для редактирования парольной политики пользователя и администратора необходимо:

1. Перейти в файл с помощью команды

vim /root/wgipa/etc/webguard/url.conf

1. в файле необходимо найти следующие строки:

pswd\_min\_len = 8

pswd\_max\_len = 100

pswd\_complexity = ^((?!.\*[\\s])(?=(.\*\\d){2,})(?=.\*[a-zа-яё])(?=.\*[A-ZА-ЯЁ]).{8,100})$

1. где:

* pswd\_min\_len – минимальная длина пароль;
* pswd\_max\_len – максимальная длина пароля;
* pswd\_complexity – регулярное выражение с ограничениями и требованиями на создание пароля.

## Редактирование политики логина

Для редактирования политики логина пользователя и администратора необходимо:

1. Перейти в файл с помощью команды

vim /root/wgipa/etc/webguard/url.conf

1. в файле необходимо найти следующие строки:

username\_min\_len = 3

username\_max\_len = 100

username\_pattern = ^[a-zA-Zа-яА-ЯёЁ0-9\_@»«&\\{\\}\\[\\]\\^#\\$\\.\\?%,\\!\\\*\\(\\)\\+\\=~:;'"\\<\\>\\-\\|\\/\\\\]{3,100}$

1. где:

* username\_min\_len – минимальная длина логина;
* username\_max\_len – максимальная длина логина;
* username\_pattern – регулярное выражение с ограничениями и требованиями на создание логина.

## Удаление администратора WebGard 2.0

Для удаления пользователя необходимо ввести следующую команду:

psql -h 127.0.0.1 -U securitymanager -d securitymanageripa -c "delete from web\_admin\_user where web\_admin\_user\_id='sometest'"

где необходимо указать в sometest логин администратора, которого необходимо удалить.

# Приложение 1

## Название скрипта: etcd\_cluster.sh

Расположение: /usr/local/bin/etcd\_cluster.sh

Содержание:

#!/bin/bash

if [[ $(cat /etc/etcd/etcd.conf | grep existing) ]]; then

exit 0

fi

systemctl stop etcd patroni

rm -rf /home/user/data/ /var/lib/etcd/default.etcd/

sed -i 's|new|existing|g' /etc/etcd/etcd.conf

ssh wg2 -o StrictHostKeyChecking=no "ETCDCTL\_API=3 etcdctl member remove \`ETCDCTL\_API=3 etcdctl member list | grep 9\:2380 | sed 's|,.\*||g'\`"

ssh wg2 -o StrictHostKeyChecking=no "ETCDCTL\_API=3 etcdctl member add --peer-urls='http://10.248.144.9:2380' etcd1"

systemctl start etcd

sleep 5

systemctl start patroni

sleep 60

systemctl restart haproxy

# Приложение 2

## Название скрипта: conn\_cheker.sh

Расположение: /home/user/conn\_cheker.sh

Содержание:

#!/bin/bash

wg1\_ip=10.40.12.73

wg2\_ip=10.40.12.244

wg3\_ip=10.40.12.54

ipa\_ip=10.40.12.174

ad\_ip=10.40.12.247

ipa\_port=389

ad\_port=389

ipa\_user=uid=admin,cn=users,cn=accounts,dc=aos,dc=test

ipa\_pass=P@ssw0rd

ad\_user=uid=admin,cn=users,cn=accounts,dc=aos,dc=test

ad\_pass=P@ssw0rd

ipa\_attr=uid

ad\_attr=sAMAccountName

RED='\033[1;31m'

GREEN='\033[1;32m'

NC='\033[0m'

test=ok

check\_port() {

if [[ $(nc -z $1 $2 </dev/null; echo $?) == \*0\* ]]; then

echo -e "${GREEN}test connect $1:$2: ok${NC}"

else

echo -e "${RED}test connect $1:$2: failed${NC}"

test=failed

fi

}

check\_ldap() {

if [[ -n $(ldapsearch -w $1 -H ldap://$2 -D "$3" -b "$3" $4 | grep $4\:) ]]; then

echo -e "${GREEN}ldapsearch to $2: ok${NC}"

else

echo -e "${RED}ldapsearch to $2: failed${NC}"

test=failed

fi

}

check\_port $wg1\_ip 22

check\_port $wg2\_ip 22

check\_port $wg3\_ip 22

check\_port $ipa\_ip $ipa\_port

check\_port $ad\_ip $ad\_port

check\_ldap $ipa\_pass $ipa\_ip $ipa\_user $ipa\_attr

check\_ldap $ad\_pass $ad\_ip $ad\_user $ad\_attr

echo

if [[ $test == "ok" ]]; then

echo -e "${GREEN}all tests ok${NC}"

else

echo -e "${RED}some test(s) failed${NC}"

fi