AppChecker

Руководство администратора

Эшелон
комплексная безопасность

Содержание

1 О руководстве 3
2 Общая информация 4
3 Установка и запуск программы 6
3.1 Установка и запуск на ОС Windows 6
3.2 Установка и запуск на ОС Linux 7
3.3 Установка и запуск в среде виртуализации 8
4 Администрирование 10
4.1 Пользователи 10
4.2 Роли пользователей 11
4.3 Группы пользователей 14
4.4 Пример работы с пользователями, ролями и группами 15
4.5 Добавление проектов 19
4.6 Управление сервером 21
4.7 Настройка сервера 22
4.8 Подключение https 23
4.9 Интеграция с системами управления 24
4.10 Журналы работы 26
5 Поддержка 27
6 Глоссарий 28
7 О компании 30
Приложение - Активация лицензии 31

1 О руководстве

Этот документ представляет собой Руководство Администратора AppChecker.

Руководство предназначено для следующих целей:

- помочь установить и запустить AppChecker;
- рассказать о ролях и группах пользователей;
- научить управлять сервером AppChecker;
- рассказать об интеграции с системами управления версиями.

Разделы документа

Этот документ содержит следующие разделы.

Общая информация (стр. 4)

Раздел содержит описание функций AppChecker и перечень минимальных требований для компьютера, на который устанавливается AppChecker.

Установка и запуск программы (стр. 6)

Раздел содержит инструкции по установке и запуску программы.

Администрирование (стр.10)

Раздел содержит информацию о работе с пользователями, об управлении сервером, об интеграции с системами управления версиями и о просмотре журналов работы.

Поддержка (стр.27)

Раздел содержит информацию о технической поддержке AppChecker.

Глоссарий (стр.28)

Раздел содержит определение терминов, встречающихся в документе.

О компании (стр.30)

Раздел содержит информацию о ЗАО «НПО «Эшелон».

2 Общая информация

AppChecker — статический анализатор кода, предназначенный для поиска дефектов в исходном коде приложений, разработанных на C/C++, C#, Java, PHP.

Функции

- поиск дефектов кодирования с помощью постоянно обновляемой базы правил и технологии анализа потоков данных;
- поиск программных закладок.

Преимущества

- поиск свыше 100 типов дефектов кодирования;
- постоянное пополнение базы правил поиска дефектов;
- поддержка классификации CWE;
- применение технологии анализа потоков данных;
- возможность проводить совместный аудит кода несколькими экспертами;
- гибкая конфигурация анализируемых проектов.

Системные требования

Процессор	64-битный Intel-совместимый
Оперативная память	4 Гб
Жесткий диск (Свободно)	30 Гб (Рекомендуется 100 Гб)
Порты	USB порт для ключа безопасности
Поддерживаемые браузеры	Internet Explorer 10+ Google Chrome 30+ Mozilla Firefox 25+
Операционная система	Linux Ubuntu 14.04 Server LTS x64 Microsoft Windows 7 SP1 x64 Microsoft Windows 8 x64 Microsoft Windows 10 x64 Microsoft Windows Server 2008 x64
Среда виртуализации	VMWare Virtual Box
Дополнительное ПО	Software Platform .Net Framework 4.0 (только для ОС Windows) Java Runtime Environment 7 CodeMeter Runtime 4.5

3 Установка и запуск программы

AppChecker поставляется с аппаратным или программным ключом.

При наличии аппаратного ключа вставьте его в USB-порт перед установкой.

При использовании программного ключа активируйте его после установки (см. приложение).

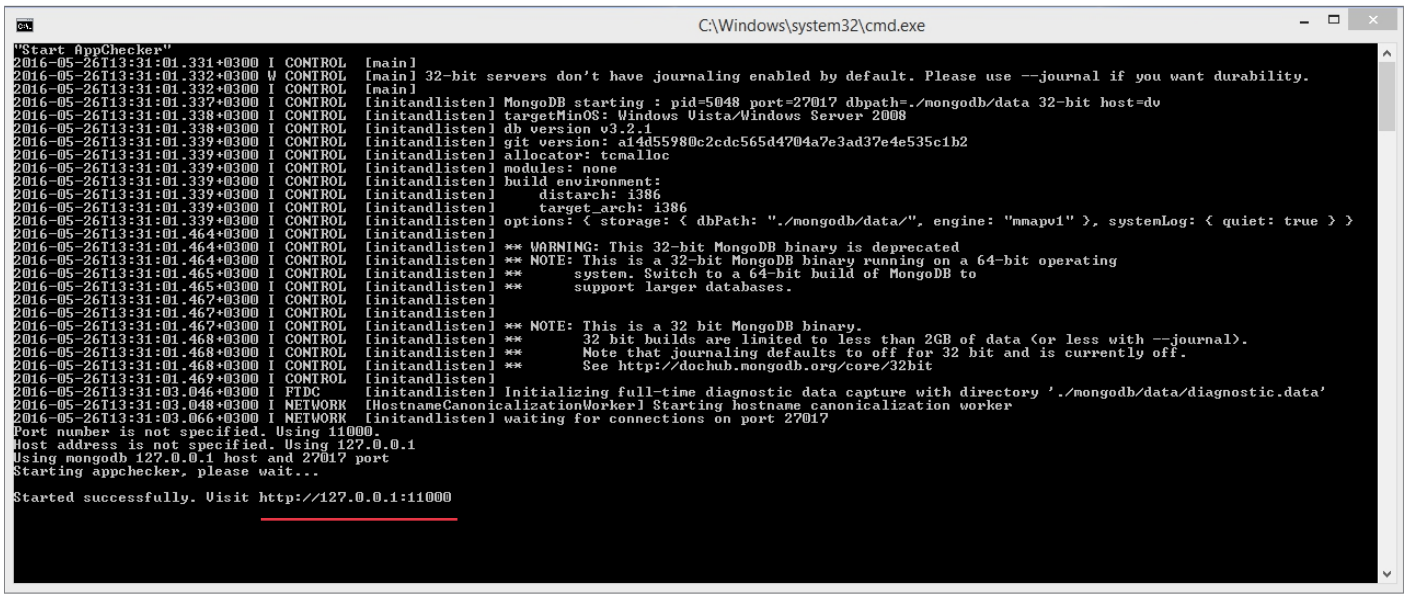
3.1 Установка и запуск на ОС Windows

Запустите установочный файл appchecker_setup.exe.

Следуйте дальнейшим инструкциям, чтобы установить AppChecker.

Запустите файл start.bat, который находится в директории установки.

Запуск сервера на ОС Windows



Сервер AppChecker будет запущен.

Введите в адресной строке браузера адрес веб-интерфейса AppChecker, указанный в консоли.

3.2 Установка и запуск на ОС Linux

Распакуйте архив с программой, используя следующую команду:

```
tar -zxvf appchecker.tgz -C имя_директории
```

Установите пакеты clang-3.5, mono, mono-runtime, mono-devel, monogodb-server и openjdk-7-jre, используя команду:

```
sudo apt-get install имя_пакета
```

Загрузите codemeter с сайта разработчика. Для установки пакета следуйте инструкциям, приведенными на сайте.

Запустите файл start.sh, который находится в директории установки. Сервер AppChecker будет запущен.

Введите в адресной строке браузера адрес веб-интерфейса AppChecker, указанный в консоли.

Запуск сервера на ОС Linux

```
echelon@appchecker:~$ ./start.sh
echelon@appchecker:~$ Port number is not specified. Using 11000.
Host address is not specified. Using 127.0.0.1
Using mongodb 127.0.0.1 host and 27017 port
Starting appchecker, please wait...

Started successfully. Visit http://localhost:11000

echelon@appchecker:~$
```

3.3 Установка и запуск в среде виртуализации

AppChecker может быть запущен в средах виртуализации VMWare и VitrualBox.

Импортируйте образ AppChecker формата OFV в среду виртуализации.

Запустите виртуальную машину и выполните вход в гостевую ОС.

Логин — appchecker. Пароль — appchecker.

Вход в виртуальную машину

```
Ubuntu 14.04.2 LTS appchecker tty1

appchecker login: appchecker
Password: _
```

Для системы виртуализации VMware необходимо пробросить порт 11000 виртуальной машины, чтобы иметь доступ к AppChecker. Для этого:

1. Узнайте IP-адрес виртуальной машины с помощью команды «ifconfig».
2. Откройте Virtual Network Editor через пункт меню «Edit».
3. Выберите сеть типа «NAT» из предложенного списка и нажмите на кнопку «NAT Settings...».
4. Нажмите кнопку «Add» в разделе «Port Forwarding».
5. Введите значение «11000» в поле «Host port».
6. Введите IP-адрес виртуальной машины, полученный на шаге 1, в поле «Virtual machine IP address».
7. Введите значение «11000» в поле «Virtual machine port». Нажмите «Применить все изменения».

Для системы виртуализации Virtual Box дополнительная настройка не требуется.

В корне домашней директории расположен файл start.sh для запуска сервера AppChecker.

Введите команду ls для просмотра домашней директории.

Просмотр домашней директории

```
appchecker@appchecker:~$ ls
appchecker  start.sh  stop.sh
appchecker@appchecker:~$ _
```

Запустите start.sh для запуска сервера AppChecker.

Введите в браузер адрес веб-интерфейса AppChecker, указанный в консоли.

Запуск сервера

```
Ubuntu 14.04.4 LTS appchecker tty1

appchecker login: Port number is not specified. Using 11000.
Using server host 0.0.0.0
Using mongodb 127.0.0.1 host and 27017 port
Starting appchecker, please wait...

Started successfully. Visit http://0.0.0.0:11000
```

4 Администрирование

Введите логин и пароль для входа в AppChecker.

По умолчанию логин — admin, пароль — admin.

AppChecker поддерживает назначение ролей пользователям.

Администрирование доступно только пользователям с системными ролями.

Пользователь *admin* имеет роли «System administrator» и «Projects administrator». Пользователя *admin* нельзя изменить или удалить.

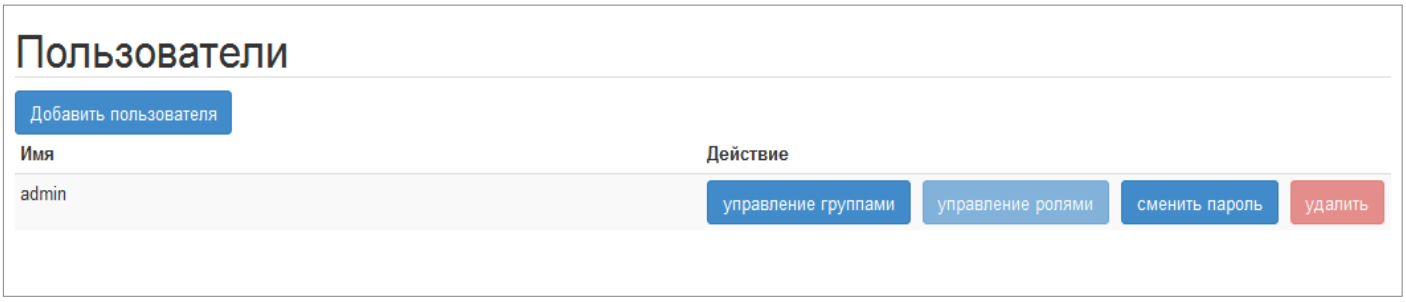
За более подробной информацией по работе с пользователями и ролями обратитесь к пунктам 4.1, 4.2, 4.3, 4.4 настоящего руководства.

4.1 Пользователи

Для добавления, редактирования и удаления пользователей воспользуйтесь вкладкой «Пользователи».

Имя пользователя может содержать только латинские буквы, цифры, дефис и нижнее подчеркивание

Вкладка «Пользователи»



4.2 Роли пользователей

AppChecker позволяет создавать роли и назначать их пользователям.

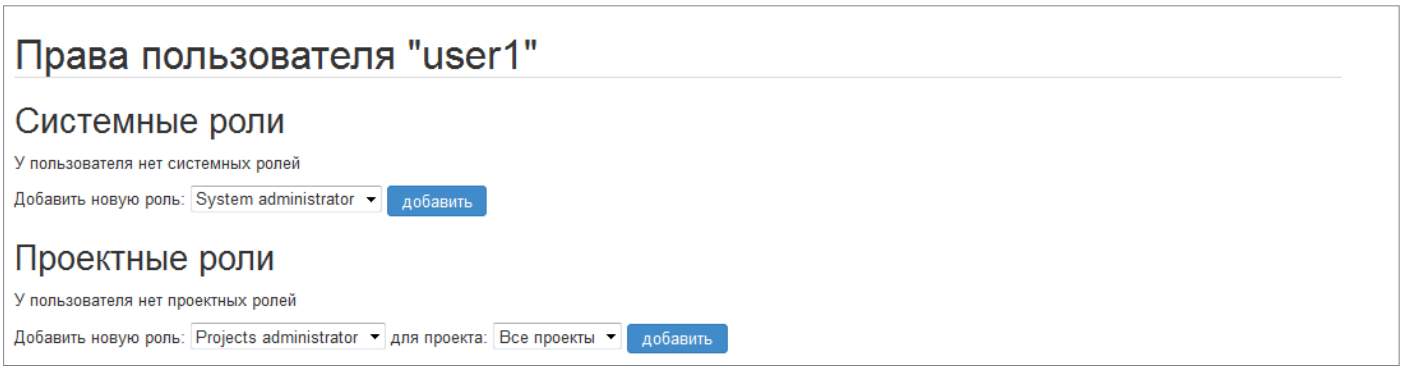
Роль это набор разрешений, соответствующих тому, какие действия может выполнять пользователь. Роли делятся на системные и проектные. Различия между системными и проектными ролями описаны далее в настоящем руководстве.

Для добавления, редактирования и удаления ролей воспользуйтесь вкладкой «Управление ролями».

Вкладка Управление ролями

Для назначения роли пользователю нажмите «Управление ролями» во вкладке «Пользователи».

Управление ролями пользователя



Системные роли

Системные роли содержат следующий набор разрешений: «Управление сервером», «Управление пользователями» и «Создание проекта».

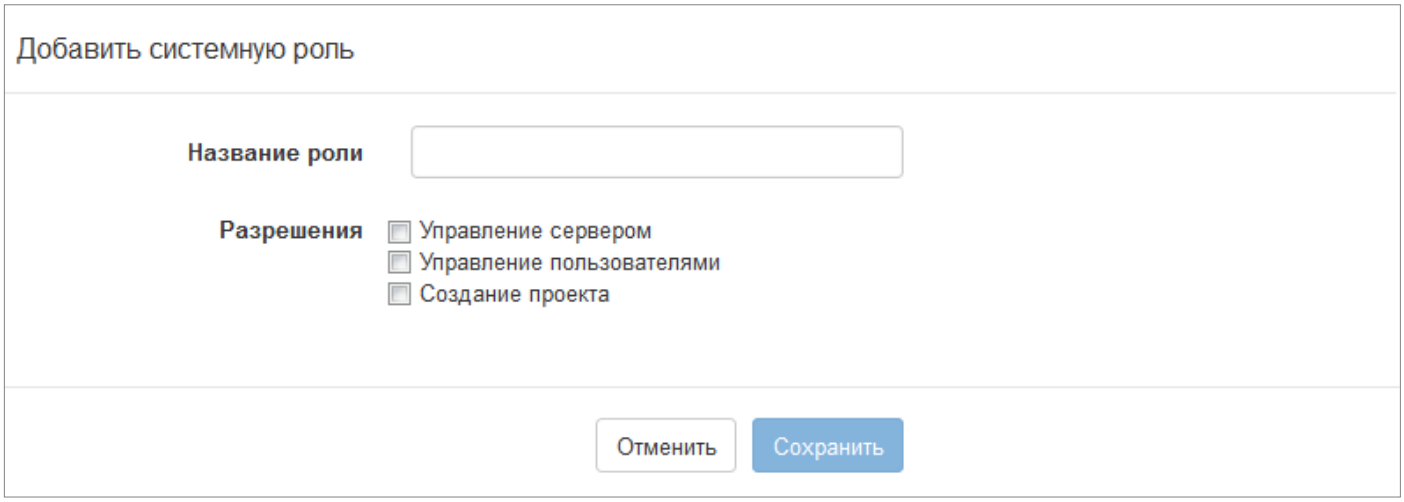
Разрешение «Управление сервером» позволяет выключать сервер, создавать и редактировать шаблоны систем управления версиями (СУВ), а так же просматривать журналы работы сервиса и ошибок сервиса. Подробнее про сервер AppChecker, про интеграцию с шаблонами СУВ и про журналы работы смотрите в пунктах 4.6 - 4.10 ,4.9 ,4.8 данного руководства.

Разрешение «Управление пользователями» позволяет добавлять, редактировать и удалять пользователей, их роли и группы.

Разрешение «Создание проекта» позволяет создавать новый проект в системе. Подробнее про добавление проекта смотрите пункт 4.5 данного руководства.

Одной из системных ролей является роль *System administator* с максимальным набором разрешений. Ее нельзя изменить или удалить.

Добавление системной роли

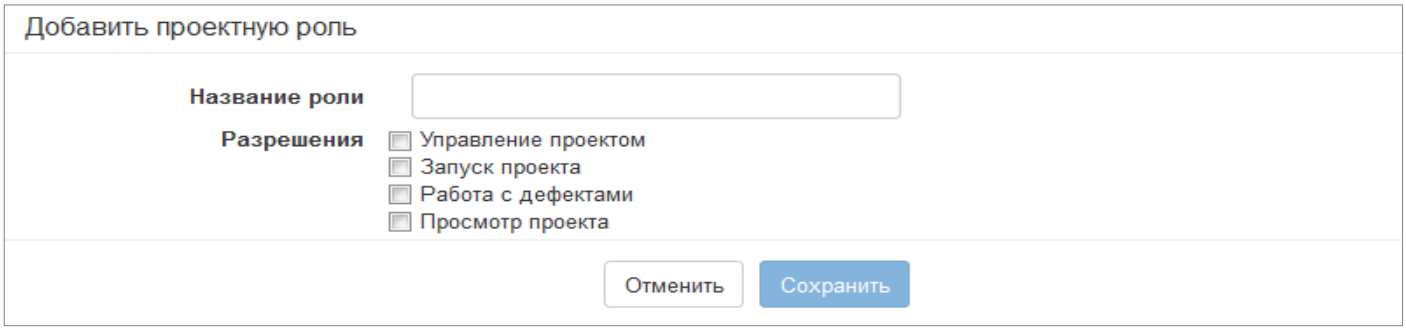


Проектные роли

Проектные роли содержат следующий набор разрешений: «Управление проектом», «Запуск проекта», «Работа с дефектами» и «Просмотр проекта».

Укажите проект при назначении проектной роли. Так же можно создать проектную роль, которая будет распространяться на все проекты в системе.

Добавление проектной роли



Разрешение «Управление проектом» позволяет удалять проекты.

Разрешение «Запуск проекта» позволяет запускать проект на новое сканирование, загружать новые версии исходного кода и конфигурации.

Разрешение «Работа с дефектами» позволяет изменять статус у дефекта и комментировать свое решение.

Разрешение «Просмотр проекта» позволяет просматривать отчеты проекта.

Разрешения «Запуск проекта», «Работа с дефектами» и «Просмотр проекта» доступны только при выборе разрешения «Просмотр проекта».

Одной из системных ролей является роль *Projects administator* с максимальным набором разрешений. Ее нельзя изменить или удалить.

Действия, доступные пользователям с проектыми ролями, подробно описаны в Руководстве Пользователя.

4.3 Группы пользователей

AppChecker позволяет объединять пользователей в группы.

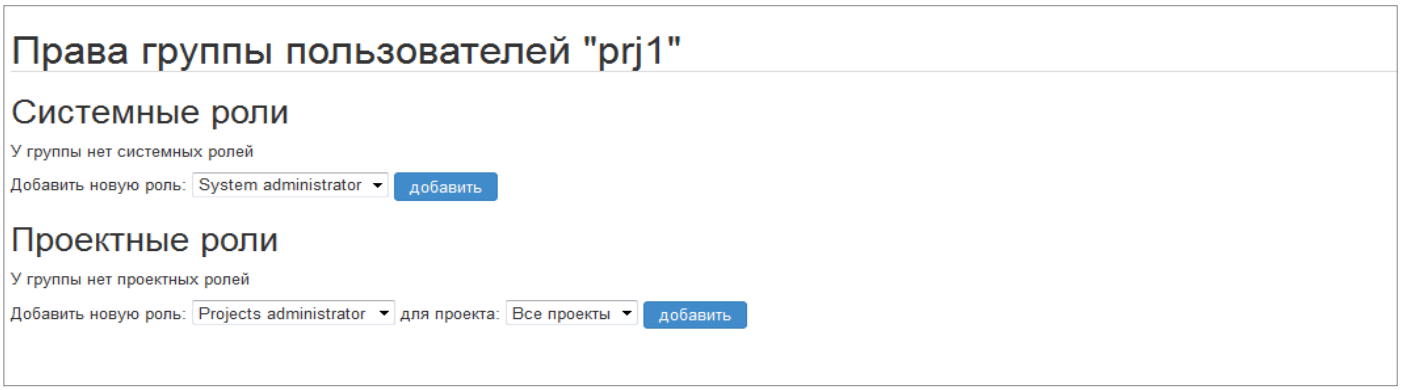
Для создания группы нажмите «Добавить группу» во вкладке «Группы пользователей».

Для добавления пользователя в группу нажмите «Управление группами» во вкладке «Пользователи».

Вкладка Группы пользователей

Для назначения роли группе нажмите «Управление ролями» во вкладке «Группы пользователей».

Управление ролями группы



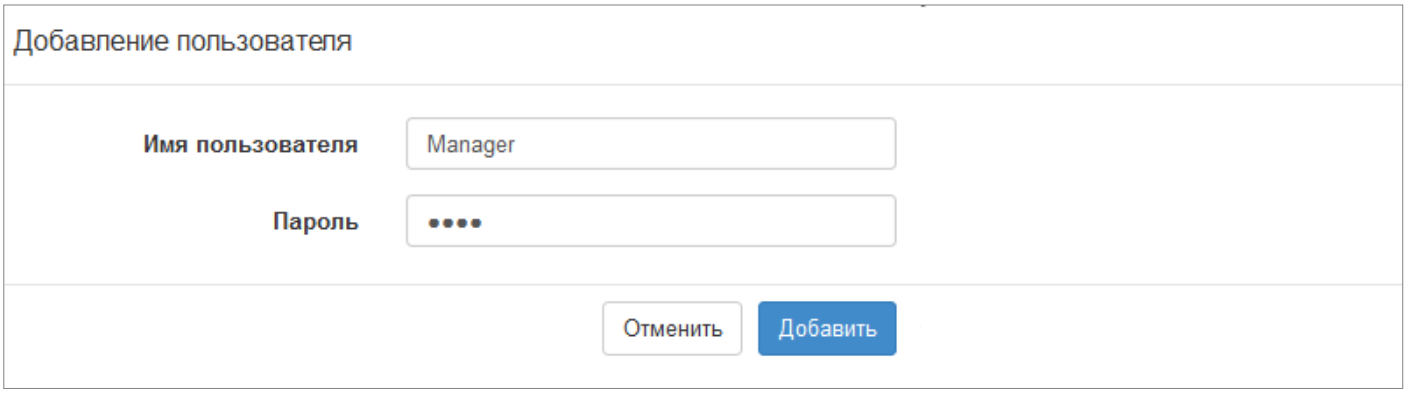
Роли пользователя складываются из сообственных ролей, а также из ролей групп, в которых он состоит.

4.4 Пример работы с пользователями, ролями и группами

Предположим, в компании работают системный администратор, менеджер, аудитор и два специалиста. Ведется работа над двумя проектами. Менеджер создает проекты. Первый специалист работает над первым проектом, второй — над вторым. Аудитор проверяет оба проекта. Рассмотрим действия системного администратора в данной ситуации.

Создайте пользователя «Manager» для менеджера компании.
Для этого во вкладке «Пользователи» нажмите «Добавить пользователя». Введите имя пользователя и пароль. Нажмите «Ок».

Добавление пользователя Manager



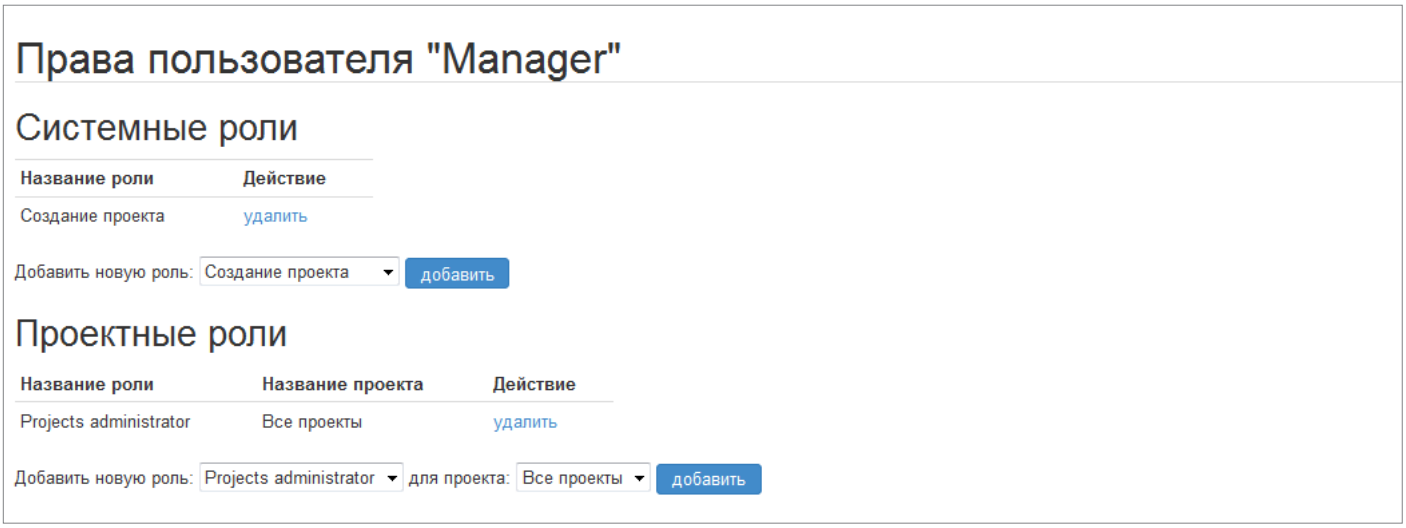
Назначьте пользователю «Manager» роли. Для менеджера рекомендуется назначить проектную роль «Projects administrator», дающую максимальные полномочия для действий с проектами, а так же создать системную роль с разрешением «Создать проект».

Чтобы создать системную роль, разрешающую создание проектов, во вкладке «Управление ролями» нажмите «Добавить системную роль». Введите имя роли и выберите разрешение «Создание проекта». Нажмите «Сохранить».

Чтобы назначить роль «Projects administrator» во вкладке «Пользователи» нажмите «Управление ролями» напротив пользователя «Manager». В разделе «Проектные роли» выберите роль «Projects administrator» для всех проектов и нажмите «Добавить».

Чтобы назначить системную роль, разрешающую создавать проекты, во вкладке «Пользователи» нажмите «Управление ролями» напротив пользователя «Manager». В разделе «Системные роли» выберите созданную роль с разрешением «Создание проектов» и нажмите «Добавить».

Управление ролями пользователя Manager

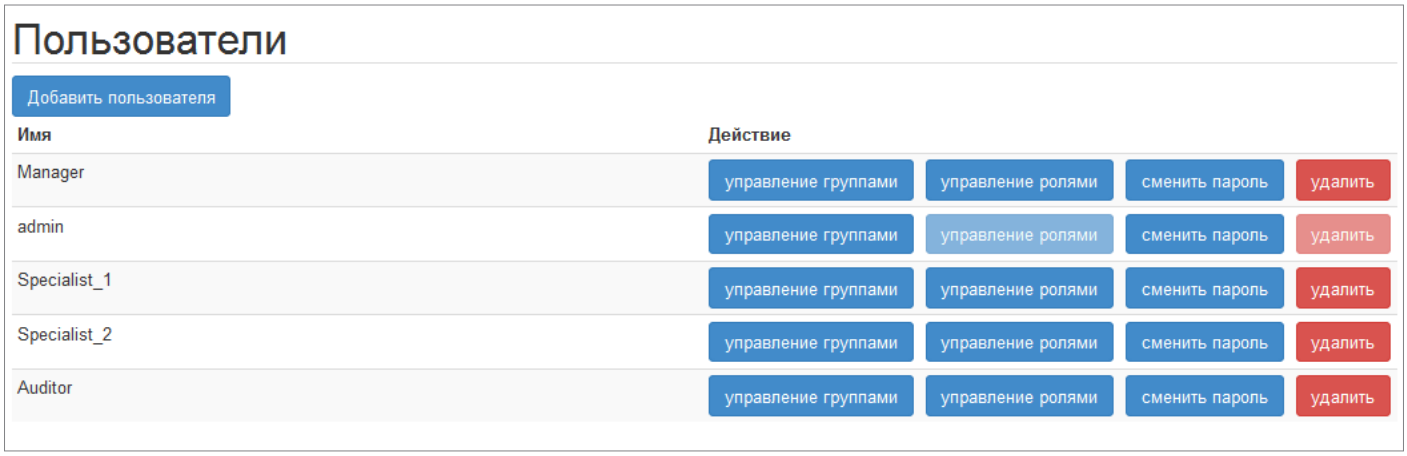


Создайте пользователей Specialist_1, Specialist_2 и Auditor для двух специалистов и аудитора соответственно.

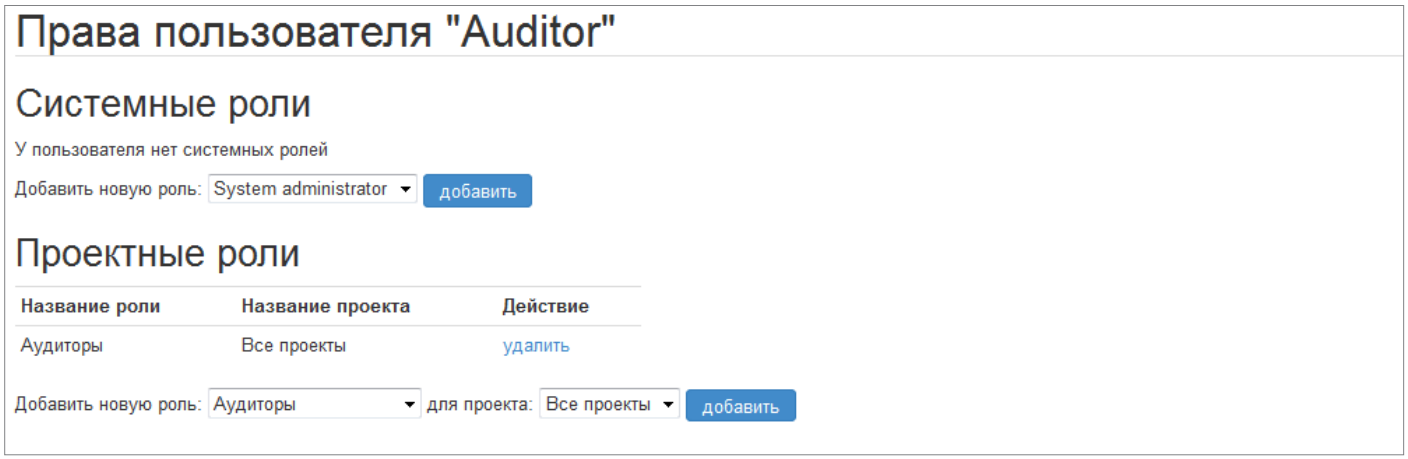
Для аудитора рекоменуется создать проектную роль с разрешением «Работа с дефектами». Для специалистов рекоменуется создать роли с разрешениями «Управление проектом», «Запуск проекта» и «Работа с дефектами».

Создание пользователей, создание и назначение ролей происходит аналогично созданию пользователя «Manager» с определенным набором ролей.

Список пользователей



Права пользователя "Auditor"

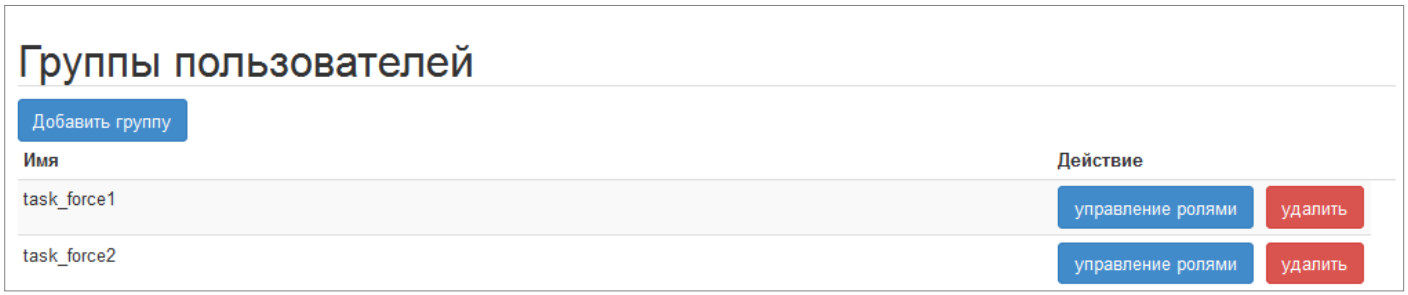


Создайте две группы для сотрудников, работающих на двух проектах.

Для этого во вкладке «Группы пользователей» нажмите «Добавить группу».

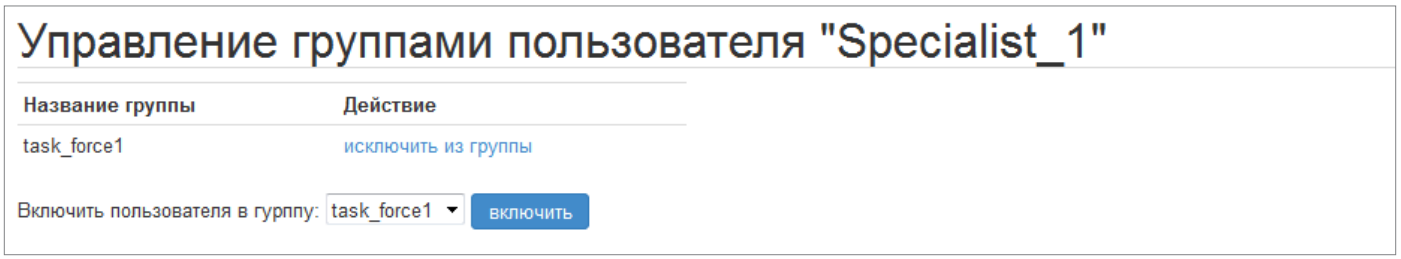
Введите название группы и нажмите «Сохранить».

Группы пользователей



Добавьте в каждую группу по специалисту и аудитору. Для этого во вкладке «Пользователи» нажмите «Управление группами» напротив выбранного пользователя. Выберите группу и нажмите «Включить».

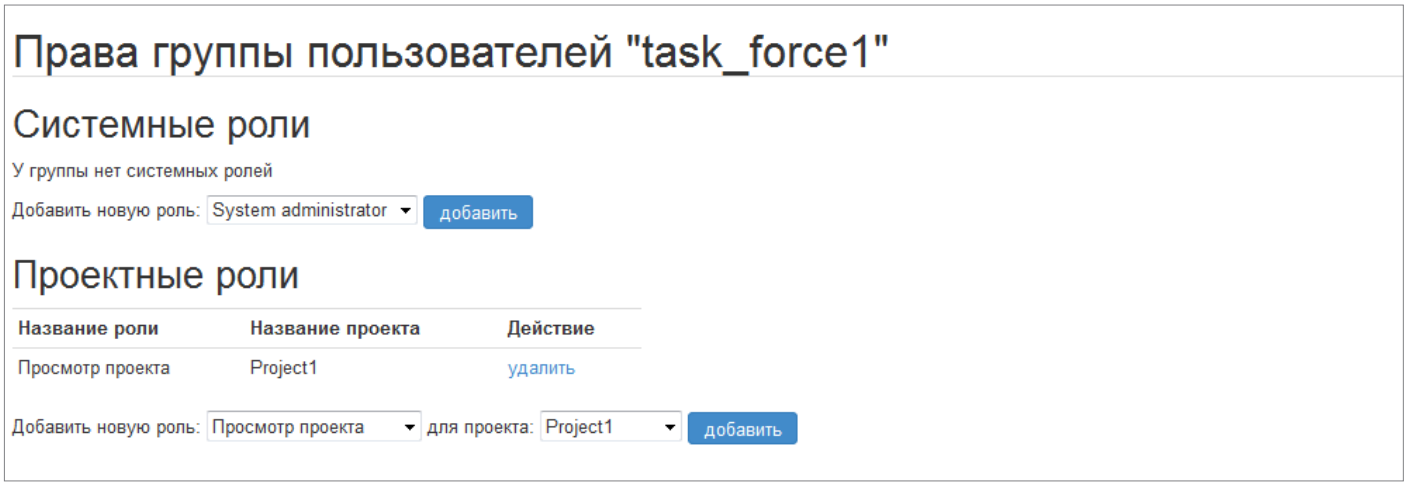
Добавление пользователя Specialist_1 в группу task_force1



Создайте и назначьте группе проектную роль для просмотра проекта с соответствующим разрешением.

Чтобы назначить роль группе во вкладке «Группы пользователей» нажмите «Управление ролями» напротив группы. В разделе «Проектные роли» выберите созданную роль для проекта, над которым работает группа пользователей, и нажмите добавить.

Права группы task_force1



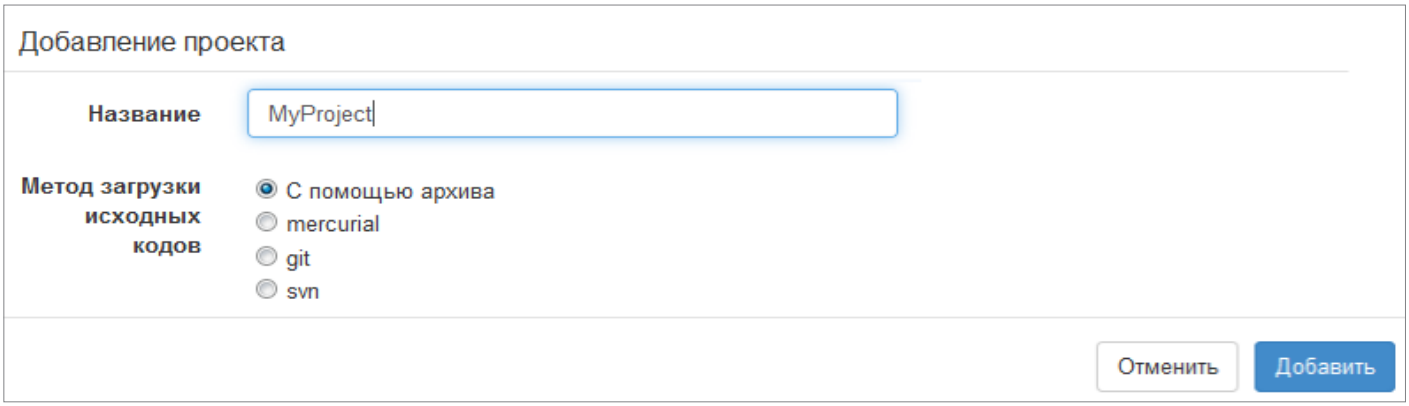
4.5 Добавление проектов

Нажмите «Добавить проект» в верхнем левом углу. Введите имя проекта.

Имя проекта может содержать только латинские буквы, цифры, дефис, нижнее подчеркивание и точку.

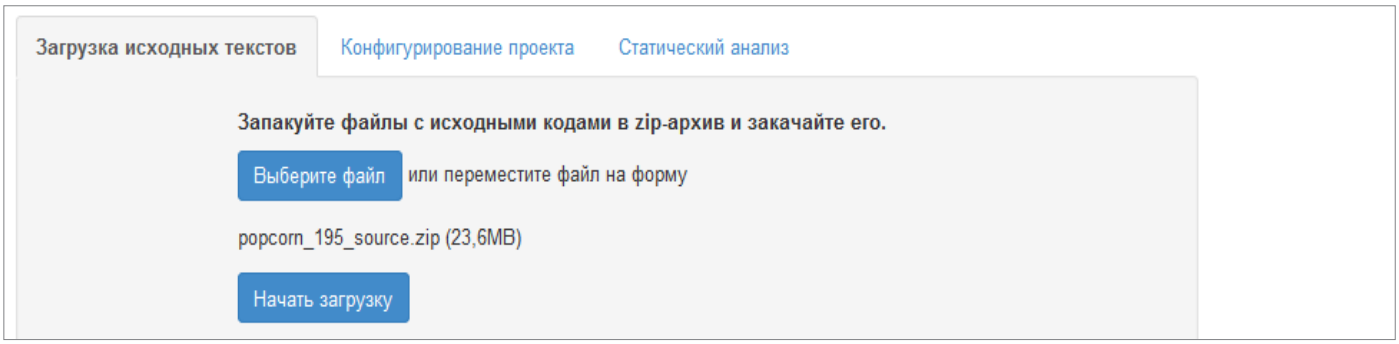
Укажите метод загрузки файлов проекта. Загрузка может осуществляться с помощью архива или с помощью системы управления версиями.
По умолчанию установлены шаблоны git, svn и mercurial. Администратор может добавлять, редактировать и удалять шаблоны. Для получения более подробной информации смотрите главу 4.9 настоящего руководства. Нажмите «Добавить».

Добавление проекта



Загрузите проект в AppChecker, нажав «Выберите файл». Нажмите «Начать загрузку».

Загрузка исходных текстов проекта

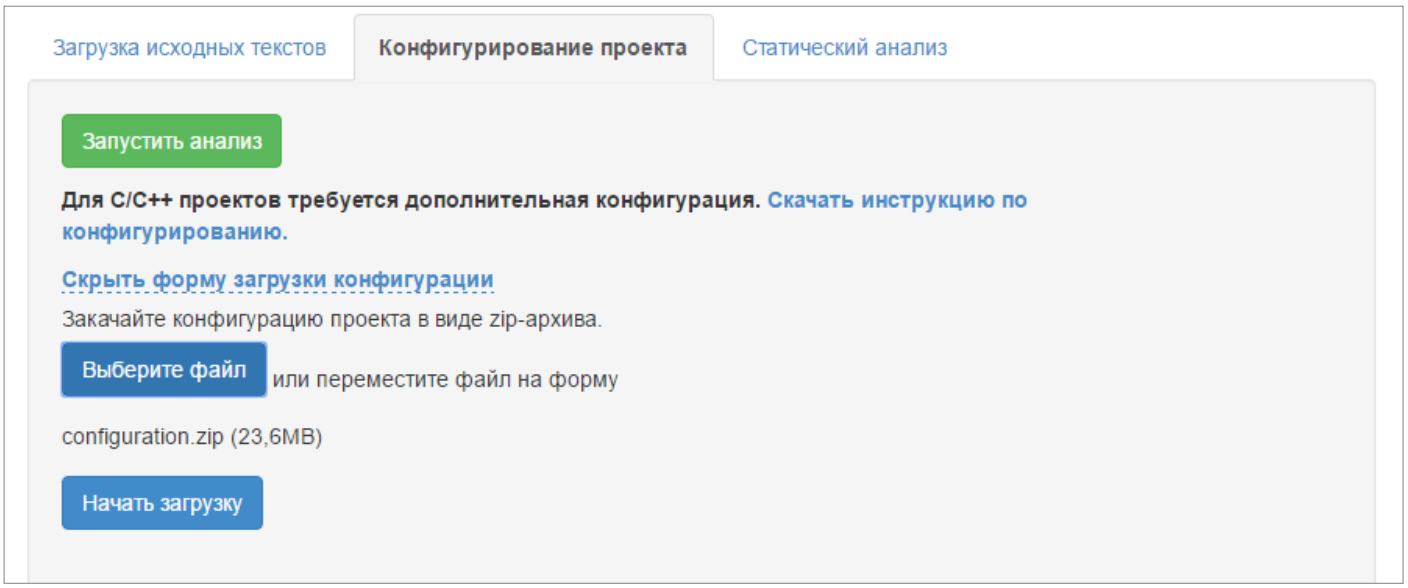


Для проектов, написанных на C/C++, требуется дополнительная конфигурация для улучшения качества анализа.

Сконфигурируйте проект. Создайте архив с конфигурацией проекта. За более подробной информацией нажмите «Скачать инструкцию по конфигурированию».

Откройте вкладку «Загрузка конфигурациии» и загрузите конфигурацию проекта в AppChecker, нажав «Выберите файл». Нажмите «Начать загрузку»

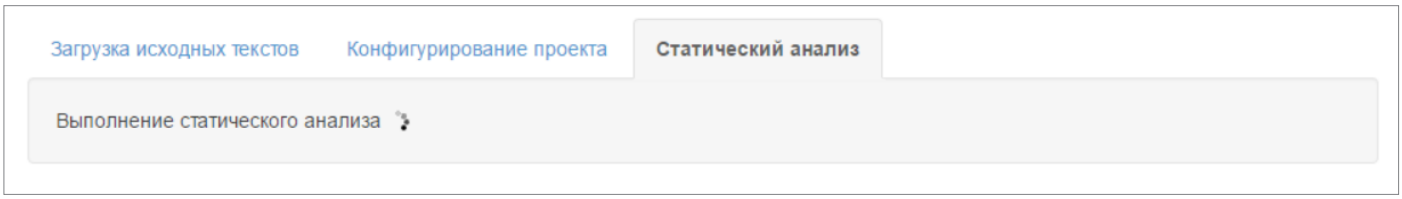
Конфигурирование проекта



Дождитесь окончания загрузки.

Запустите анализ проекта, нажав «Запустить анализ».
Статический анализ будет запущен.

Выполнение статического анализа



4.6 Управление сервером

AppChecker по умолчанию использует порт 11000 для запуска веб-сервера.

При необходимости настройки сервера можно изменить (см. пункт 4.7 данного руководства).

Работать с сервером можно через интерфейс или через консольное приложение.

Общую информацию о сервере можно посмотреть во вкладке «Управление сервером» в веб-интерфейсе. Так же в этой вкладке можно выключить сервер.

Для выключения сервера нажмите «Выключить сервер» в разделе «Управление сервером».

Для включения сервера запустите файл **start.bat** для ОС Windows и **start.sh** для ОС Linux и для виртуальной машины.

Вкладка Управление сервером

4.7 Настройка сервера

Настройте сервер AppChecker через конфигурационный файл default.ini, расположенный в директории config.

Описание параметров

Группа параметров [rest] описывает параметры работы сервиса

Параметр	Описание	Значение по умолчанию
host	адрес сервиса	127.0.0.1
port	порт сервиса	11000

Группа параметров [analyzer] описывает опции java-машины при запуске анализатора.

Параметр	Описание	Значение по умолчанию
javaopts	дополнительные параметры для JVM	отсутствует

Группа параметров [mongo] описывает настройки доступа к базе данных.

Параметр	Описание	Значение по умолчанию
login	Логин. Может отсутствовать. В этом случае авторизация не используется.	отсутствует
password	Пароль. Должен присутствовать, если есть логин.	отсутствует
dbName	имя базы данных	appsec
server	ip-адрес сервера	127.0.0.1
port	порт сервера	27017

Группа параметров [https] описывает настройки https-протокола.

Параметр	Описание	Значение по умолчанию
enabled	Флаг включения https	false
keystoreFile	абсолютный путь к файлу-ключу	отсутствует
keystorePass	пароль	отсутствует
keystoreType	тип файла-ключа	отсутствует
keystoreProvider	наименование провайдера	отсутствует
keystoreAlias	алиас сервера	отсутствует

Пример файла

```
[rest]
host=127.0.0.1
port=11000

[analyzer]
javaopts=-Xmx2g

[https]
enabled=true
keystoreFile=/home/user/ssl/keystore.p12
keystorePass=Seclab1234
keystoreType=PKCS12
keystoreProvider=SunJSSE
keystoreAlias=tomcat

[mongo]
login=dbuser
password=12345
dbName=rest
server=127.0.0.1
port=27017
```

4.8 Подключение https

Купите или сгенирируйте ключи для использования https.

Укажите в конфигурационном файле группу параметров https. Обратите внимание, что для keystoreFile необходимо указать абсолютный путь.

Перезапустите сервис.

4.9 Интеграция с системами управления версиями

AppChecker поддерживает загрузку исходных текстов с помощью СУВ.

По умолчанию настроены шаблоны трех СУВ.

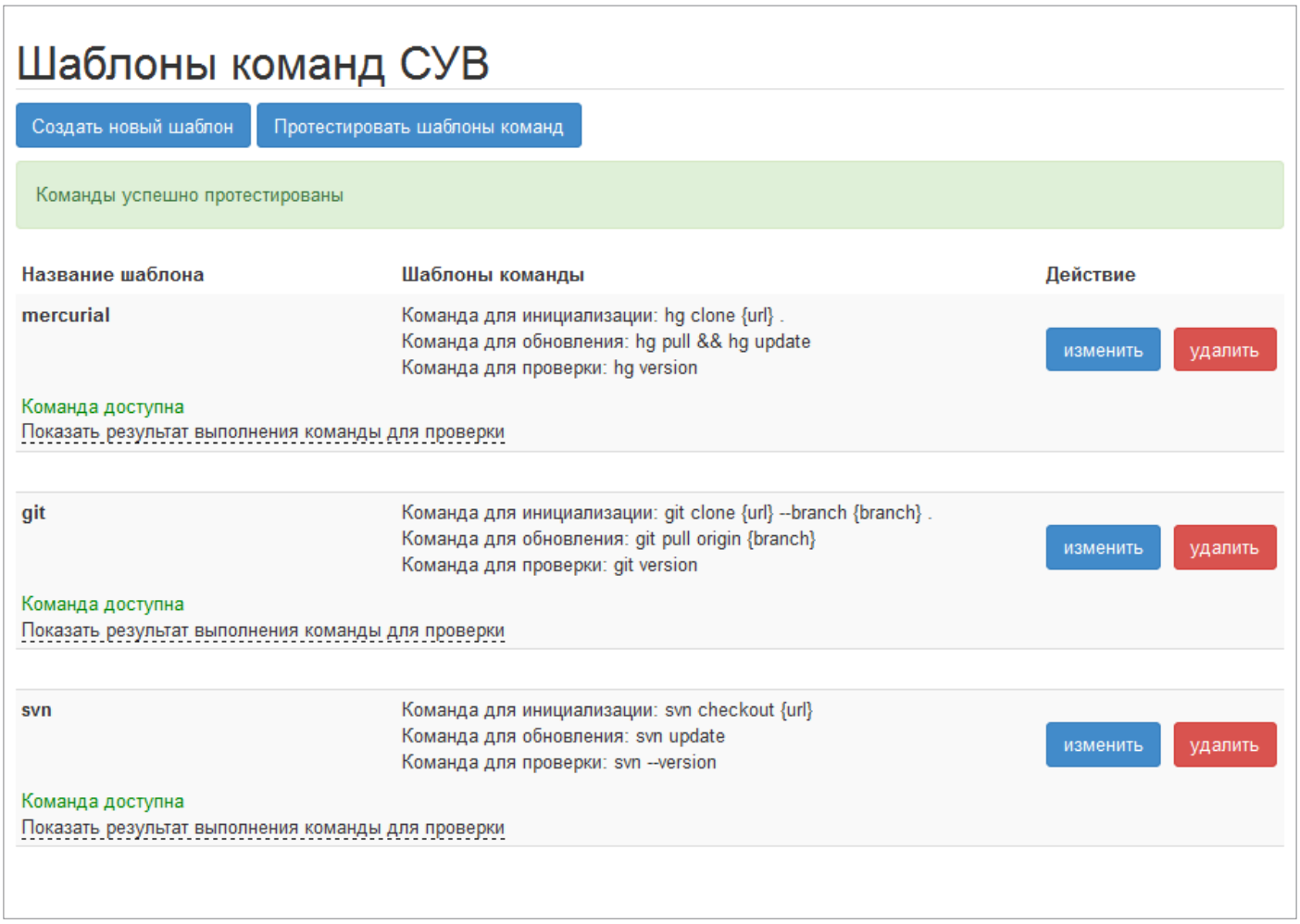
Для работы с шаблонами воспользуйтесь вкладкой «Шаблоны команд СУВ».

Для создания шаблона нажмите «Создать новый шаблон».

Для редактирования шаблона нажмите «Изменить».

Для удаления шаблона нажмите «Удалить».

Вкладка Шаблоны команд СУВ



Каждый шаблон системы управления версиями включает в себя три команды:

1) Команда для инициализации.

Данная команда выполняется единожды после создания проекта.

Примеры команды: git clone, svn checkout

2) Команда для обновления исходных текстов.

Данная команда служит для получения новых версий исходных файлов.

Примеры команды: git pull, svn update.

3) Команда для проверки доступности.

Данная команда проверяет доступность СУВ.

Примеры команды: hg version, svn --version

Команда для проверки доступности выполняется при загрузке системы, при измении команды или с помощью функции «Протестировать шаблоны команд» во вкладке «Шаблоны команд СУВ».

Если команда выполнилась успешно, то данный шаблон можно будет использовать при создании проекта.

Если команда выполнилась неудачно, то данный шаблон будет считаться неактивным и не будет отображаться при выборе метода загрузки исходных файлов.

Команда для проверки необязательна — в случае ее отсутствия шаблон будет считатся активным.

Для команд инициализации и обновления исходных текстов можно **задать переменные**, значения которых пользователь может ввести при создании проекта. Примеры таких переменных — адрес сервера, название ветки и т.д. Переменная оборачиватся фигурными скобками.

Пример команды: git clone {url} --branch {branch}

В данном случае заданы две переменные - url и branch, их значение указывает пользователь при создании проекта.

4.10 Журналы работы

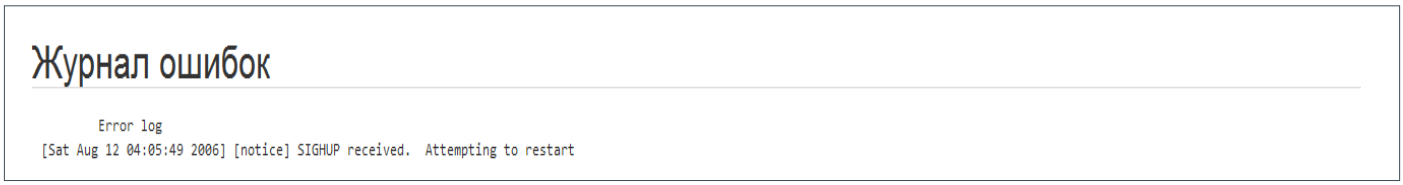
Для просмотра журнала обращений к серверу и журнала ошибок воспользуйтесь вкладкой «Журналы работы». Логи хранятся в директории data/logs.

Журнал обращений к серверу регистрирует входящие запросы.

Журнал обращений

Журнал ошибок регистрирует сбои в работе системы.

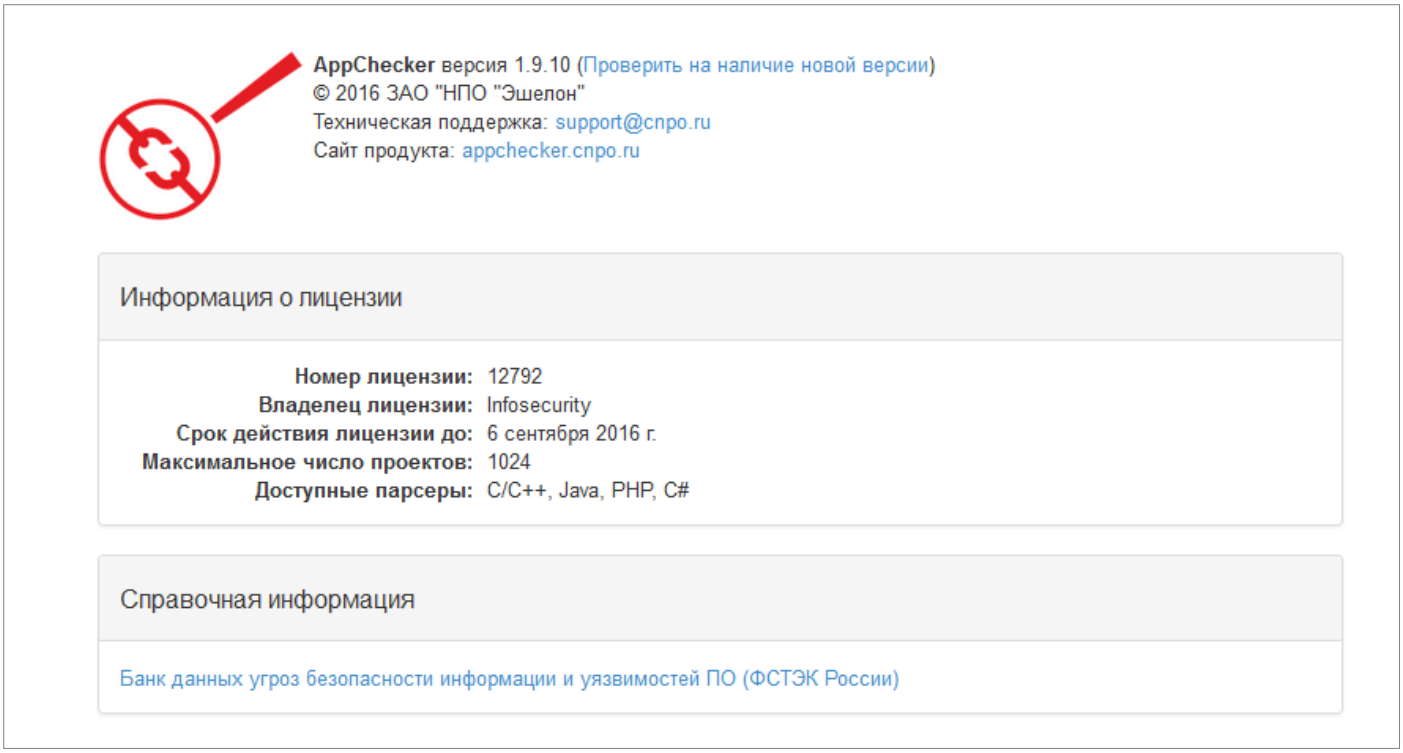
Журнал работы



5 Поддержка

Вкладка о программе содержит информацию о версии AppChecker, информацию о лицензии и ссылку на банк данных угроз безопасности информации и уязвимостей ПО (ФСТЭК).

Вкладка о программе



Для проверки актуальности версии нажмите на ссылку «Проверить на наличие новой версии».

Для получения технической поддержки отправьте электронное письмо на адрес support@cnpo.ru.

6 Глоссарий

Виртуальная машина

Модель вычислительной машины, созданной путем виртуализации вычислительных ресурсов: процессора, оперативной памяти, устройств хранения и ввода/вывода информации.

Гостевая ОС

ОС, устанавливаемая на виртуальную машину.

Дефект кода

Ошибка в исходном тексте программы, которая может привести к уязвимости.

Ключ программы

Ключ, который подтверждает право пользоваться AppChecker. Ключ бывает программным с расширением webb или аппаратным в виде usb-флешки.

Конфигурация проекта

Настройка проекта для повышения качества анализа.

Программная закладка

Скрытно внедрённый в систему код, позволяющий злоумышленнику осуществить несанкционированный доступ.

Роль

Набор разрешений, соответствующий тому, какие действия может выполнять пользователь или группа пользователей.

Статический анализ

Анализ программного обеспечения, производимый без реального выполнения исследуемых программ.

Система управления версиями

Программное обеспечение, позволяющее хранить несколько версий одного документа.

CWE

Common Weakness Enumeration. Представляет собой список дефектов безопасности программного обеспечения. CWE охватывает более 15000 дефектов безопасности и включает в себя детальную структуру классификации из различных научных источников и примеров.

CWE-совместимость

Позволяет продукту быть зарегистрированным в качестве официально «CWE-совместимого». CWE-совместимый продукт должен предоставлять пользователям возможность поиска дефектов безопасности по CWE-идентификаторам и получения связанных с ними CWE-идентификаторов.

7 О компании

ЗАО "НПО "Эшелон" специализируется на комплексном обеспечении информационной безопасности.

Основными направлениями деятельности являются:

- проектирование, внедрение и сопровождение комплексных систем обеспечения информационной безопасности;
- сертификация, аттестация и лицензирование в области защиты информации;
- аудит информационной безопасности организаций;
- проектирование и аудит систем управления информационной безопасностью;
- разработка и поставка оборудования и средств защиты информации, в том числе в защищенном исполнении;
- обеспечение технической поддержки и сопровождение поставляемых решений, систем и продуктов;
- испытания, экспертизы, исследования в области безопасности информации.

Более детальную информацию о компании вы сможете найти на сайте npo-echelon.ru.

Приложение

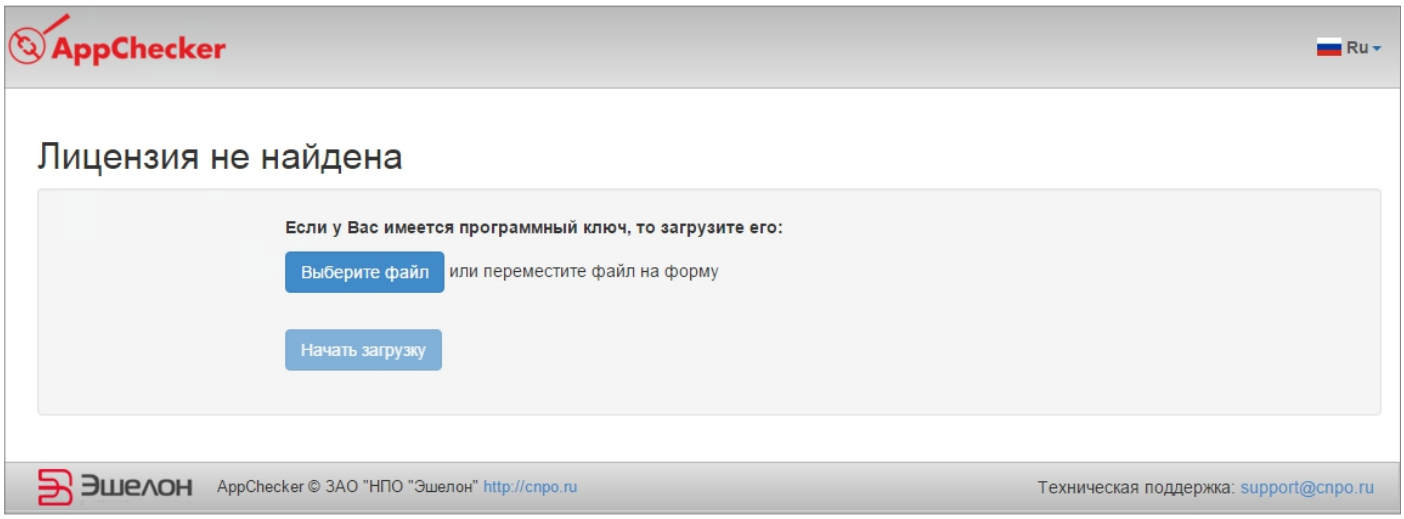
Активация лицензии

Установите и запустите AppChecker. Более подробная информация содержится в главе 3 настоящего руководства.

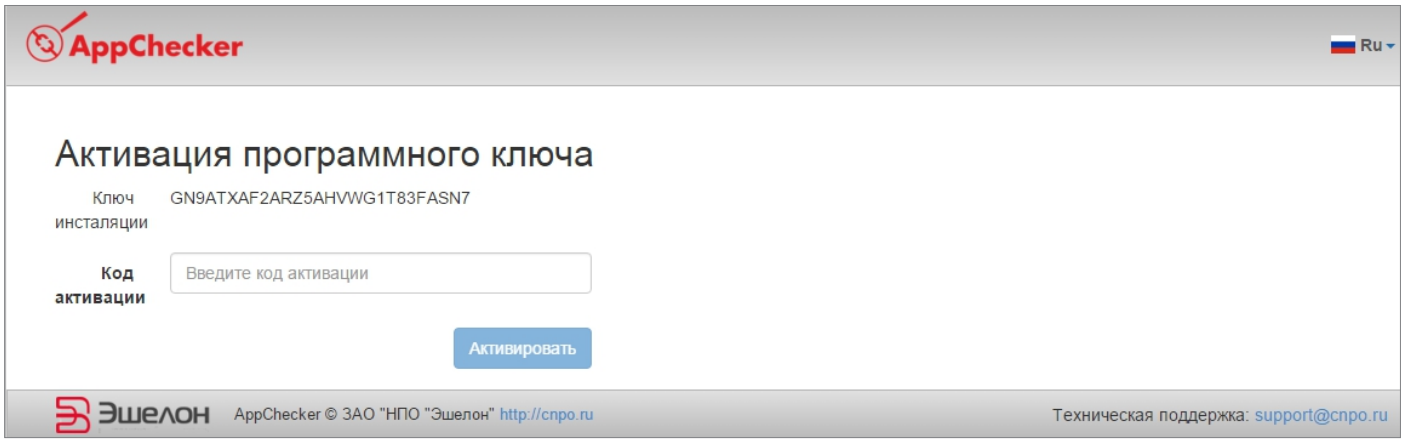
Загрузите программный ключ с расширением wbb. После загрузки в веб-интерфейсе вам будет показан ключ инсталяции.

Отправьте ключ инсталяции на support.appc@npo-echelon.ru.

Загрузка программного ключа



В ответ вы получите код активации.

Введите код активации и нажмите «Активировать».

Активация лицензии