# Документация по Stingray

* [Руководство по эксплуатации](UG.md)
* [Руководство по установке и обновлению](AAG.md)
* [Рекомендации по безопасной разработке приложений](RG.md) # Руководство по эксплуатации ## Основные понятия **Проект (Project)** — верхнеуровневая сущность, внутри которой определяются настройки и профили сканирования для конкретного приложения. Каждый проект однозначно связывается со сканируемым приложением (пакетом) либо на этапе создания, либо при первом сканировании. На уровне проекта могут быть переопределены правила сканирования, которые будут применяться только для этого проекта. Имя проекта уникально в рамках системы.

**Профиль (Profile)** — профиль сканирования, включающий в себя настройки каждого модуля, список проверяемых стандартов и требований информационной безопасности. Имя профиля уникально в рамках проекта, к которому он относится.

**Модуль (Module)** — компоненты для сбора различной информации во время сканирования приложения на устройстве (мониторинг системного журнала, использование файлов, операции с базой данных и т. д.). Каждый модуль имеет свои уникальные настройки и может быть зависимым от результатов других модулей.

**Тест кейсы (Test cases)** — записанный сценарий работы пользователя с приложением. Включает в себя все действия пользователя (нажатия, передаваемый текст, любые взаимодействия с интерфейсом приложения и т. д.). Тест кейс привязывается к конкретному проекту и может быть воспроизведен только в рамках него. Тест кейс запускается только если имя приложения (package\_id) при запуске совпадает с именем приложения, для которого был записан тест кейс. Сканирование — процесс анализа, во время которого пользователь вручную или система по записанным ранее тест кейсам взаимодействуют с приложением. Во время сканирования система Stingray собирает всю доступную информацию о работе приложения и затем проводит поиск уязвимостей и проверку на соответствие стандартам безопасности.

**Метод сканирования/запуска** — cпособ сканирования, определяющий, запускать ли записанный ранее тест кейс или ожидать ручных операций с приложением. Возможные варианты:

* **Автоматический** — запускает сканирование и запускает выбранный тест кейс.
* **Ручной** — после запуска сканирования необходимо вручную совершать операции с запущенным приложением.

**Имя пакета (Package name)** — имя пакета сканируемого приложения.

**Правила анализа (Rules)** — правила анализа, по которым происходит поиск части уязвимостей. Правила представляют собой набор строк или регулярных выражений, которые необходимо искать в собранных данных. Для удобства добавление правил оформлено в виде конструктора, в котором необходимо указать какую строку искать, в результатах каких модулей и в каком месте данных (XML-тэг, значение в JSON и т. д.).

**Требование (Requirement)** — требования информационной безопасности, на соответствие которому будет проверено приложение. С требованием соотносятся определенные типы дефектов, при нахождении которых в приложении требование будет считаться не выполненным. Требования могут быть сгруппированы в виде категорий или относиться напрямую к стандартам.

**Категория (Category)** — группировка требований информационной безопасности по различным признакам.

**Стандарт (Standard)** — совокупность требований или категорий требований информационной безопасности, на соответствие которым может проверяться приложение. Стандарты могут быть как общемировые, так и внутренние стандарты компании.

**Дефекты (Defects)** — выявленные во время сканирования дефекты приложения или, по-другому, уязвимости. У каждого дефекта есть тип, описание и рекомендации по устранению.

**Собранные данные (Collected Data)** — вся собранная информация о работе приложения за время сканирования. Данные разделены по модулям, каждый из которых отвечает за сбор определенной информации. Эти данные так же можно скачать и проанализировать локально, при желании.

**CI/CD (Continuous Integration / Continuous Delivery)** — системы для непрерывной интеграции и непрерывных поставок приложения. Примерами таких систем могут быть Jenkins, Teamcity, GitLab CI.

**Эмулятор (Emulator)** — виртуальный эмулятор имитирующее реальное устройство Android. Характеризуется различной архитектурой и версией операционной системы. ## О продукте ### Назначение

Stingray (Система) — это решение для поиска уязвимостей и автоматизации регрессионного тестирования информационной безопасности в мобильных приложениях с использованием технологий машинного обучения (Machine Learning).

Основной особенностью, отличающей систему Stingray, является уникальный механизм создания автоматических тест кейсов, которые воспроизводятся и адаптируются к изменению интерфейса приложения с минимальным участием пользователя, что существенно сокращает затраты человеческих ресурсов на тестирование, поиск уязвимостей и позволяет реализовать процесс тестирования безопасности в рамках непрерывного процесса разработки (DevOps). При всей сложности внутри, для пользователя запись тест кейса выглядит, как обычная работа с приложением, нет необходимости в написании скриптов или как-то по-особенному собирать приложение, просто пройдите необходимые шаги в приложении, как если бы оно было установлено на обычном мобильном устройстве.

Система поддерживает технологии байт код анализа (BCA), статического (SAST), интерактивного (IAST), динамического (DAST) тестирования и тестирования API (API ST), сбор и предоставление полной информации о работе приложения на устройстве. Система способна обнаруживать более 50 типов уязвимостей и производить проверку на соответствие регуляторным и индустриальным требованиям информационной безопасности: PCI DSS, OWASP Mobile Top-10, OWASP MASVS, а также позволяет создавать свои внутренние стандарты безопасности.

### Возможности

#### Различные режимы сканирования

В системе Stingray существует несколько режимов анализа безопасности приложений, которые подходят для различных сценариев тестирования. Ручной анализ для разового тестирования приложения и автоматический режим для встраивания в процесс разработки.

#### Гибкое изменение правил анализа

Изменение правил анализа позволяет достигнуть максимальной эффективности при нахождении дефектов. Компоненты системы, отвечающие за сбор данных представлены в виде модулей с простой и понятной конфигурацией. Модификация правил сделана в виде конструктора, благодаря которому изменение не займет много времени.

#### Встраивание в процесс CI/CD

Помимо полноценного REST API, предусмотрены интеграции в системы дистрибуции мобильных приложений. Максимальная гибкость и разнообразие настроек позволяет использовать систему Stingray в том процессе, который уже построен для разработки приложения, и информировать разработчиков о наличии уязвимостей еще на этапе первых сборок.

#### Проверка на соответствие стандартам безопасности

При анализе приложения доступны не только описания и рекомендации по устранению выявленных уязвимостей, но и вся собранная информация о работе приложения, а также детальный отчет о его соответствии всем актуальным мировым стандартам Информационной Безопасности.

#### Вся собранная информация о работе приложения

Все данные, собранные во время работы приложения на устройстве, сохраняются, структурируются, анализируются в процессе выявления уязвимостей и предоставляются в качестве артефактов сканирования.

#### Детальные рекомендации о выявленных уязвимостях

Stingray позволяет обнаруживать более 50 типов уязвимостей, технология базируется на наблюдении за поведением приложения на устройстве во время различных режимов сканирования.

После всех этапов анализа, выявленные в ходе работы приложения уязвимости отображаются в интерфейсе с подробной информацией о месте возникновения, критичности, детальными рекомендациями по исправлению и, самое главное, недопущению подобных уязвимостей в дальнейшем.

Рекомендации постоянно обновляются новыми способами защиты и лучшими мировыми практиками.

#### Уникальный механизм автоматизации регрессионного тестирования

Для автоматизации тестирования в системе Stingray разработан уникальный механизм записи, воспроизведения и адаптации тест кейсов. Механизм основан на глубокой интеграции с операционной системой и методах машинного обучения. При всей сложности внутри, для пользователя запись тест кейса выглядит, как обычная работа с приложением, не нужно писать скрипты или как-то по-особенному собирать приложение, просто пройдите необходимые шаги в приложении, как если бы оно было установлено на обычном мобильном устройстве. ## Требования к рабочему месту пользователя ### Требования к оборудованию Для работы с системой, установленной в корпоративной сети необходим компьютер, подключенный к внутренней сети компании.

Для работы с системой, представляемой в виде облачного сервиса — необходим компьютер, подключенный к сети Интернет.

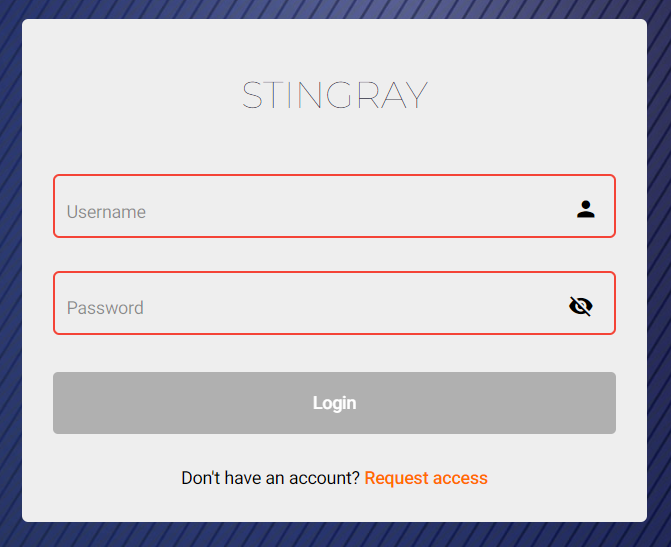
### Требования к программному обеспечению

На ПК должен быть установлен веб-браузер. Рекомендуемые браузеры:

* Google Chrome (рекомендуемый).
* Mozilla Firefox. ## Работа с приложением ### Аутентификация пользователя

Ссылка для доступа к веб-интерфейсу Stingray (GUI) должна быть предоставлена администратором. Перейдите по ссылке, чтобы открыть окно аутентификации.

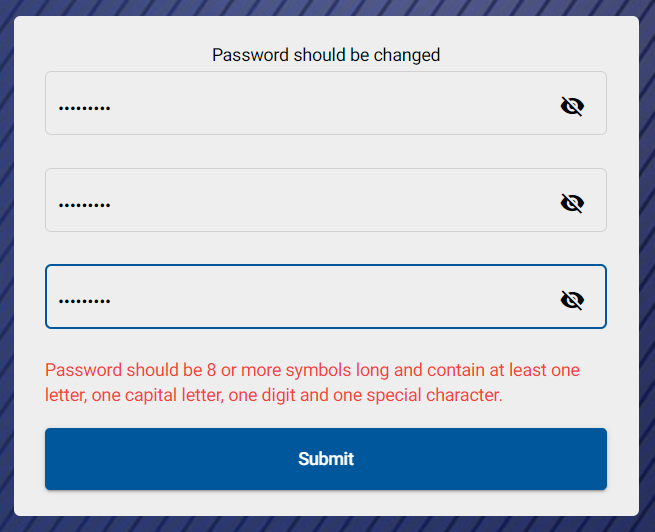
Для входа в систему введите имя пользователя (логин) и пароль, а затем нажмите кнопку **Login**.



Аутентификация пользователя

Если учетные данные введены неправильно, будет отображено сообщение о неверном имени пользователя или пароле.

Вместе со ссылкой доступа предоставляется временный пароль, который должен быть изменен пользователем при первом входе в систему. Вновь устанавливаемый пароль должен состоять не менее чем из 8 символов, а также содержать не менее одной прописной буквы, одной заглавной буквы, одной цифры и одного специального символа.



Аутентификация пользователя

После смены временного пароля пользователю будет предложено принять пользовательское соглашение и политику конфиденциальности, а затем он перенаправляется на страницу авторизации и в результате ввода учетной записи и нового пароля входит в систему.

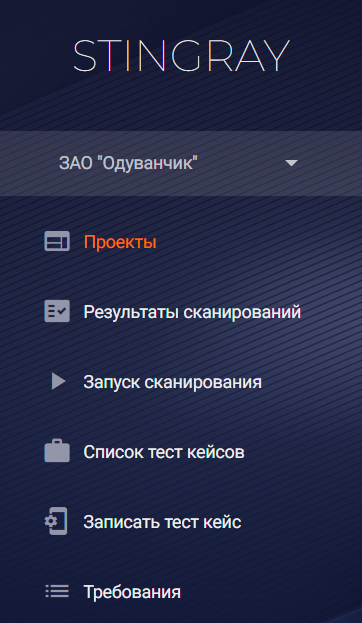
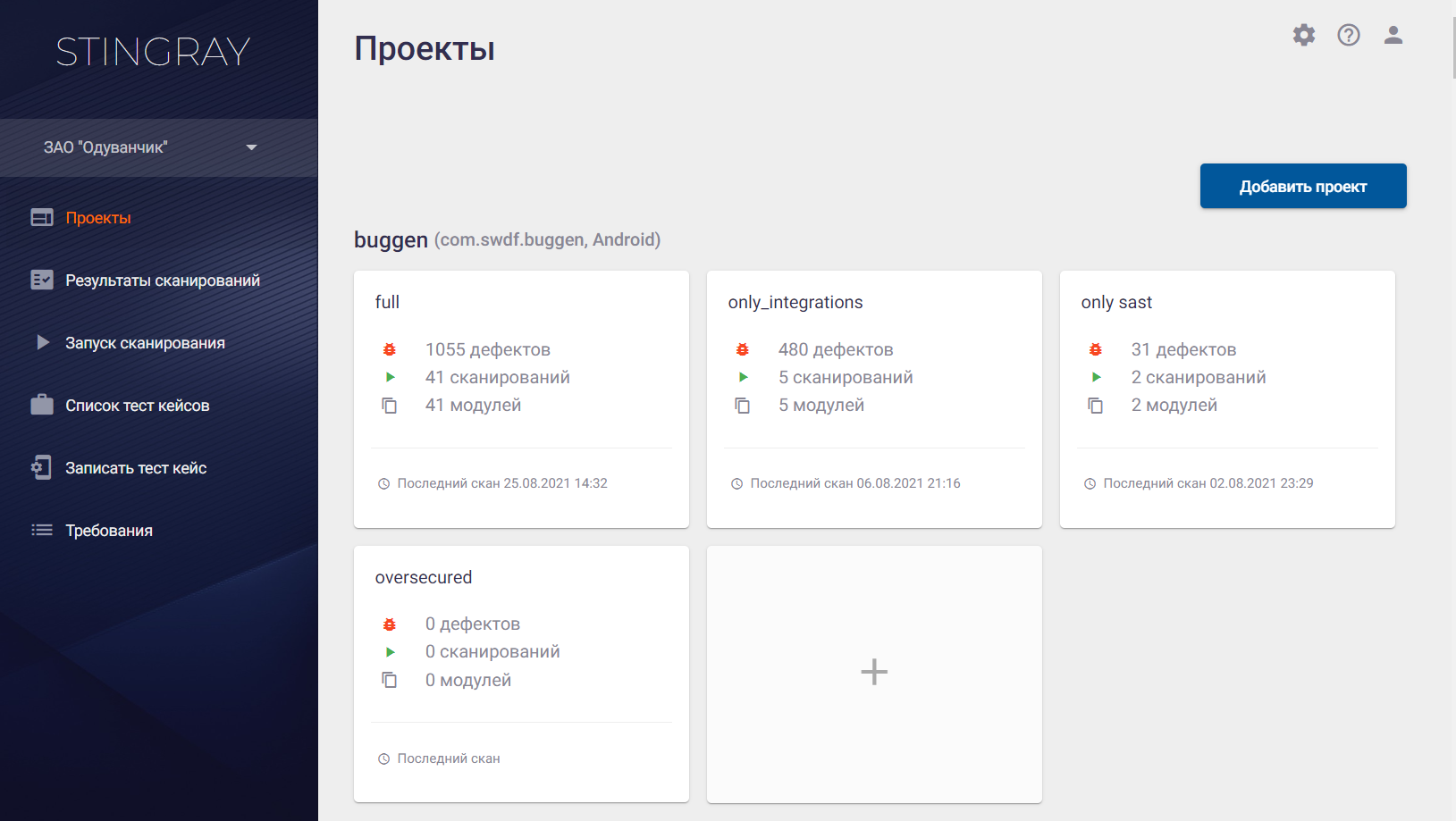
Если пароль будет введен неправильно пять раз, последующие попытки авторизации сопровождаются необходимостью введения защитного кода (captcha).

Если в профиле пользователя включена двухфакторная аутентификация, см. раздел [Профиль пользователя](Profil_polzovatelya.md), после ввода логина отображается дополнительное окно, в котором необходимо ввести код, появившийся в приложении Google Authenticator (скачать в [Google Play](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=ru&gl=US) или [App Store](https://apps.apple.com/ru/app/google-authenticator/id388497605)).

Если код двухфакторной аутентификации будет три раза введен неправильно, пользователь блокируется на 5 минут.

### Основное меню

В левой части экрана расположено меню с основными экранами системы: **Проекты**, **Результаты сканирований**, **Запуск сканирования**, **Список тест кейсов**, **Записать тест кейс**, **Требования**.

 ### Проекты #### Проекты ##### Список проектов На странице **Проекты** указаны все существующие в системе проекты и их профили сканирования. В скобках после названия проекта отображаются имя пакета (package name) и архитектура приложения. На данной странице можно получить краткую информацию о количестве найденных дефектов за все время существования проекта, количество проведенных сканирований и информацию о включенных модулях. Так же можно добавить новый Проект или добавить новый профиль сканирования для существующего Проекта.  По нажатию на имя Проекта открывается страница **Проект** с тремя вкладками: **Общая информация**, **Список профилей**, **Правила**.

##### Информация проекта

На первой вкладке **Проект** представлена общая информация по проекту, включающая: \* Аватар проекта. \* Имя. \* Описание. \* Имя пакета. \* Количество сканирований в рамках проекта. \* Количество дефектов, найденных за время существования проекта. \* Количество настроенных профилей сканирования. \* Архитектура проекта (Android или iOS).

##### Добавление / редактирование / удаление проекта

Для работы с проектами необходимо выбрать пункт **Проекты** в основном меню, расположенном в левой части экрана.

Для добавления нового проекта нажмите на кнопку **Добавить проект** вверху страницы **Проекты**.

В появившемся окне **Добавление проекта** введите имя проекта, его краткое описание и архитектуру (Android / iOS). Также в соответствующем поле можно указать имя сканируемого пакета (приложения). Если оставить это поле пустым, оно будет автоматически заполнено после первого сканирования. Нажмите кнопку **Добавить** в правом нижнем углу окна. Вновь созданный проект появится на странице **Проекты**.

Для редактирования или удаления кликните мышкой имя проекта на странице **Проекты**.

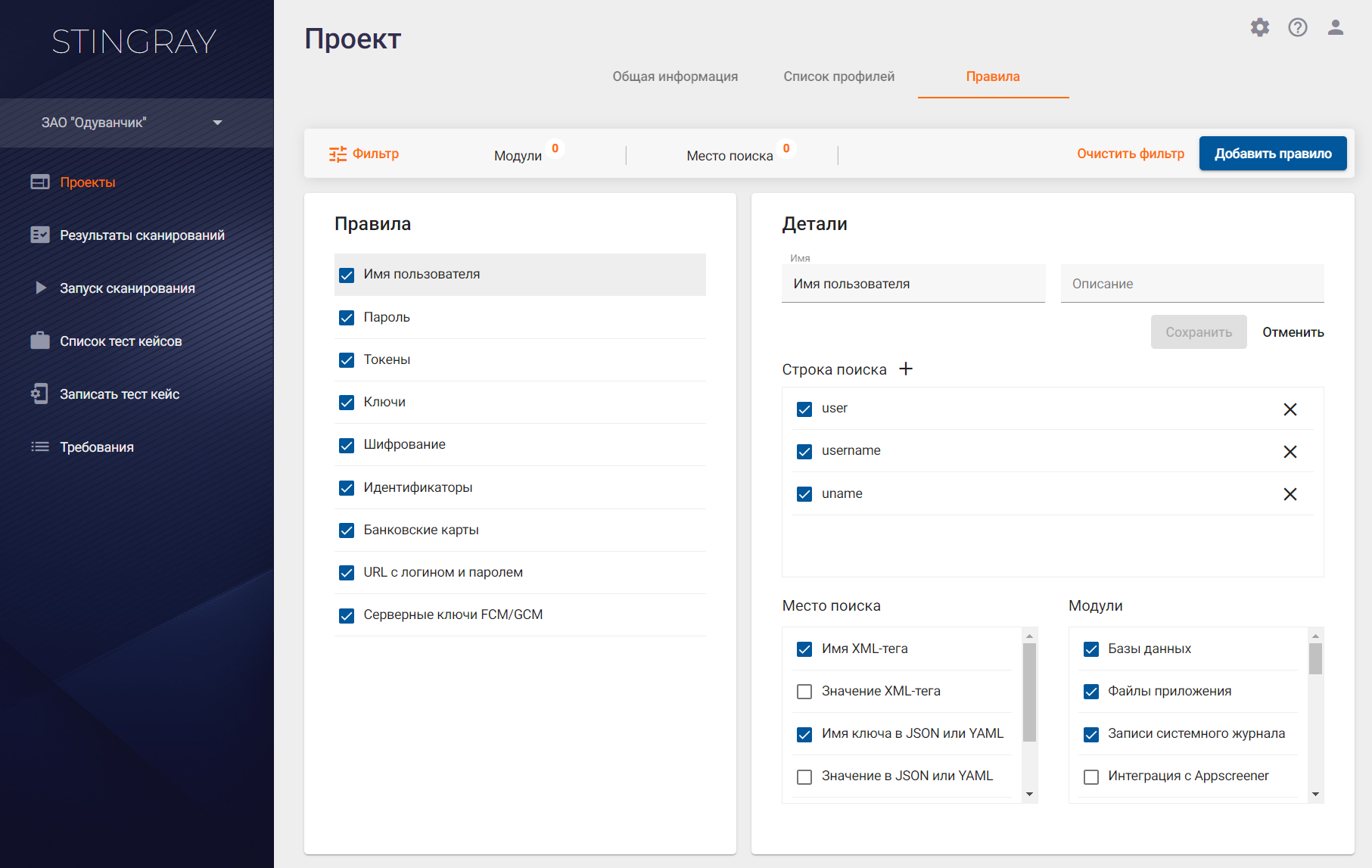
На открывшейся странице **Проект** можно отредактировать следующие параметры: \* В поле **Имя** отредактировать имя проекта. \* Изменить описание проекта в соответствующем поле. \* Изменить аватар проекта, кликнув мышкой текущий аватар и выбрав файл с картинкой для нового. **Примечание:** Имя пакета может быть добавлено только в незаполненное поле, в противном случае редактирование данного поля недоступно. После обновления информации профиля нажмите кнопку **Сохранить** в правой части экрана.

Также на странице **Информация проекта** можно удалить проект. Для этого нажмите кнопку **Удалить** в правой части экрана и подтвердите это действие нажатием на кнопку **Да** в появившемся окне **Удаление проекта**.

##### Список профилей проекта

На данной вкладке **Список профилей** доступно управление профилями сканирования, включенными в данный проект. Доступен просмотр и добавление нового профиля сканирования. Более подробная информация о работе с профилями приведена в разделе [Профиль](Profile.md).

#### Правила На данной вкладке представлены правила анализа уязвимостей, которые применяются для выбранного проекта. В общем случае правила соответствуют определенным на уровне организации (см. раздел <a href="../aag/pravila\_analiza\_na\_urovne\_organizacii.htm" title="Правила анализа на уровне Организации">Правила анализа на уровне Организации в Руководстве прикладного администратора), но есть возможность изменить или добавить правила в соответствии со спецификой сканируемого приложения. Необходимо отметить, что правила, добавленные непосредственно в проекте, будут применяться только в рамках этого проекта.



#### Переопределение правил анализа

На странице **Проект** на вкладке **Правила** представлены правила анализа собранных данных для поиска уязвимостей. На этой вкладке возможно добавить, изменить или удалить существующее правило анализа для конкретного проекта. То есть, заданное на этой вкладке новое или измененное правило будет применяться в рамках только этого проекта, а не для всех проектов данной Организации.

#### Описание работы правил анализа

Основная цель применения правил анализа — модификация системы под особенности своего приложения для эффективной работы по поиску уязвимостей. Каждое приложение и его данные уникальны по формату и содержанию и применение кастомизированных правил анализа позволяет максимально увеличить покрытие системой всех возможных кейсов для поиска уязвимостей для каждого конкретного приложения. Правила анализа, по которым происходит поиск части уязвимостей, представляют собой набор строк или регулярных выражений, которые необходимо искать в собранных в ходе сканирования приложения данных. Каждое правило определяет, какую строку или регулярное выражение искать, в данных каких модулей и в каком месте/каких форматах данных. Такой подход позволяет значительно сократить количество ложных срабатываний при поиске уязвимостей. В системе существует два вида правил анализа:

* Внутренние правила поиска уязвимостей, не подлежащие настройке и недоступные пользователю для просмотра и редактирования. Они не представлены на вкладке **Правила**.
* Правила, которые занимаются поиском чувствительной информации. Как раз они и представлены на вкладке **Правила** и описаны в этом разделе. Эти правила пользователь системы может модифицировать и настроить под работу со своим приложением. На вкладке **Правила** каждое правило анализа представлено отдельной строкой в левой части экрана. Строка правила имеет следующие поля:
* Индикатор состояния правила. Если в этом поле стоит значок , то правило является активным и будет применяться при анализе собранных данных для поиска уязвимостей. Если в этом поле стоит значок , то правило является неактивным и не будет применяться при анализе собранных данных для поиска уязвимостей.
* Имя правила для более удобной навигации.

Выбранное правило подсвечивается и в правой части экрана отображаются детали:

* **Имя** — имя правила для более удобной навигации.
* **Описание** — описание правила.
* **Строка поиска** — строка или регулярное выражение для поиска конфиденциальной информации.
* **Модули** — модули системы, для которых будет применяться данное правило.
* **Место поиска** — где именно искать необходимую информацию, в каких файлах и форматах данных.

Рассмотрим, как работают правила анализа на примере одного из правил.

Это правило анализа в данный момент является активным и называется «Пароль». Оно определяет, что следующие паттерны:

* Регулярные выражения вида **pin(?:[\_-]?code)?**.
* Строка **passphrase**.
* Строка **password**.
* Строка **passwd**.
* Строка **paswd**. Они будут искаться в данных, собранных всеми семнадцатью модулями системы (эти модули были выбраны в поле Модули), в следующих местах (эти значения были выбраны в поле Место поиска):
* Имя XML-тега.
* Имя ключа в паре key=value. Пользователь имеет возможность сделать неактивным, отредактировать или удалить это правило в случае необходимости. Для удобства работы с правилами существует возможность выбрать и применить для отображаемых правил фильтр в верхней части экрана по нажатию на кнопку **Фильтр**.

В появившемся поле можно выбрать из выпадающих списков одно или несколько значений для фильтрации по параметрам **Модули** и **Место поиска**. Фильтр может быть очищен по нажатию кнопки **Очистить фильтр** справа вверху. При повторном нажатии на кнопку **Фильтр** в левом вернем углу, поле фильтрации будет свернуто.

#### Добавление / редактирование правил анализа

Редактирование правил анализа может быть произведено на вкладке **Правила**. Для редактирования выберите необходимое правило в левом окне **Правила**. В правом окне **Детали** можно изменить и сохранить следующие параметры:

* **Имя** правила для более удобной навигации.
* **Описание** правила анализа (опциональный параметр).
* В поле **Строка поиска** можно задать строку или регулярное выражение для поиска конфиденциальной информации. Для вновь добавляемого регулярного выражения необходимо нажать на кнопку рядом с заголовком «Строка поиска», в появившемся поле **Значение** задать собственно новую строку или регулярное выражение и нажать кнопку **Сохранить**. Все ранее определенные регулярные выражения для данного правила перечислены в окне в списке ниже. Для удаления регулярного выражения нажмите значок справа в конце поля.
* **Место поиска** — активные места поиска отмечены значком , неактивные значком . Для изменения необходимо нажать на нужный элемент. Его статус изменится и будет отображено уведомлении об успешном изменении.
* **Модули**, для которых будет применяться данное правило. Любой из модулей сканирования в системе можно выбрать и добавить в правило. Включение и отключение происходит аналогично полю **Место поиска**.
* Для сохранения всех произведенных изменений в регулярном выражении нажмите кнопку **Сохранить** справа.

Для добавления нового правила анализа нажмите кнопку **Добавить правило** справа вверху экрана. В появившемся окне **Добавление нового правила** необходимо ввести имя и описание правила и нажать кнопку **Добавить** внизу справа. Добавленное правило будет отображено в списке и доступно для дальнейшего редактирования.

#### Удаление правил анализа

Удаление правил анализа может быть произведено на вкладке **Правила**. Для редактирования правила нажмите на кнопку **Удалить правило** в правом нижнем углу вкладки.В появившемся окне **Удаление правила** необходимо подтвердить или отменить удаление.

#### Профиль

Профиль <link rel="stylesheet" type="text/css" href="assets/css/default.css" /> `` </head> ``` `` <body> ``` `` <h2> ``` Профиль `` </h2> ``` `` <p> ``` По нажатию на имя профиля на странице \*\*Проекты\*\* или во вкладке \*\*Список профилей\*\* открывается страница \*\*Профиль\*\* с детальной информацией о нем. На странице можно получить информацию о настройках модулей сканирования в данном профиле (включить, отключить или настроить их), просмотреть и изменить стандарты безопасности, на соответствие которым будет проверяться анализируемое данным профилем приложение. А также получить информацию о количестве найденных дефектов за все время существования профиля сканирования. <img height="600" src="/img/image46.png" width="100%" /> На странице присутствуют три вкладки: \*\*Профиль\*\*, \*\*Модули\*\*, \*\*Требования\*\*. </p> ```

Управление профилями сканирования  
Профили сканирования относятся к проектам. На странице  
\*\*Проекты\*\* представлены ‎все существующие  
в системе проекты и их профили сканирования. Для каждого проекта показан  
список его профилей. На этой странице можно добавить новый профиль  
сканирования для существующего проекта или просмотреть информацию о  
существующих профилях.  
`<img src="/img/image64.png" />  
Для добавления нового профиля в проект нажмите на значок  
«`<img alt="Picture 121" height="18.0" src="/smimg/image32.png" width="20.6" />»  
в пустой карточке для профиля рядом с существующими профилями. В  
появившемся окне \*\*Добавление профиля\*\*  
введите название профиля и его краткое описание, а затем нажмите кнопку  
\*\*Добавить\*\* в правом нижнем углу окна.  
Вновь созданный профиль появится в списке профилей проекта.  
<img height="360" src="/img/image50.png" width="50%" />  
Для редактирования или удаления профиля кликните мышкой имя профиля,  
который необходимо отредактировать или удалить.  
<img height="326" src="/img/image51.png" width="30%" />  
``  
</p>

``

Откроется окно \*\*Профиль\*\*.  
<img src="/img/image67.png" style="cursor: nwse-resize;" />  
На первой вкладке \*\*Профиль\*\*  
представлена общая информация:  
  
Имя.  
Описание.  
Проект, к которому относится профиль.  
Количество сканирований в рамках профиля.  
Количество модулей, которые используются в данном профиле.  
Количество дефектов, найденных за время существования профиля.  
  
На этой вкладке можно отредактировать следующие параметры:  
  
В поле \*\*Имя\*\* отредактировать имя  
профиля.  
Изменить описание профиля в соответствующем поле.  
В поле \*\*Проект\*\* выбрать проект из  
выпадающего списка. Таким образом профиль вместе со всеми настройками  
можно перенести из одного проекта в другой.  
  
После обновления информации профиля нажмите кнопку  
\*\*Сохранить\*\* справа.  
<img height="420" src="/img/image52.png" width="100%" />  
Также на вкладке \*\*Профиль\*\* можно  
удалить профиль. Для этого нажмите кнопку  
\*\*Удалить\*\* в правой части экрана и  
подтвердите это действие нажатием на кнопку  
\*\*Да\*\* в появившемся окне  
\*\*Удаление профиля\*\*.  
<img height="246" src="/img/image53.png" width="60%" />  
Добавление, удаление и редактирование профиля можно осуществить двумя  
способами. Рассмотрим второй способ.  
На странице \*\*Проекты\*\* показаны имена  
проектов и список их профилей. По нажатию ‎на имя проекта открывается  
страница \*\*Проект \*\*с вкладками  
\*\*Общая информация\*\*,  
\*\*Список профилей \*\*и  
\*\*Правила\*\*.  
<img height="609" src="/img/image54.png" width="100%" />  
На вкладке \*\*Список профилей\*\* можно  
добавить новый профиль:  
``  
</p>

``

Для добавления нового профиля в проекте нажмите на кнопку  
\*\*Добавить профиль\*\*.  
  
‎В появившемся окне \*\*Добавление  
профиля\*\* введите название профиля и его краткое  
описание и нажмите кнопку \*\*Добавить\*\* в  
правом нижнем углу окна. Вновь созданный профиль появится в списке  
профилей проекта.  
Нажмите строку профиля в списке профилей, чтобы изменить информацию  
профиля или удалить профиль. Откроется страница  
\*\*Профиль\*\*. Описание редактирования ‎и  
удаления профиля на странице \*\*Профиль\*\*  
приведено выше в этом разделе.  
``  
</li>

</ul> ```

Модули  
На данной вкладке представлены настройки модулей для сбора информации о  
приложении, на основе которой будет произведен дальнейший анализ. На  
этой вкладке возможно включить или выключить конкретный модуль и  
провести соответствующие настройки.  
`<img src="/img/image55.png" />  
Система включает девятнадцать модулей сканирования. Список всех  
модулей ‎для сканирования и сбора информации о приложении представлен на  
вкладке \*\*Модули\*\* на странице  
\*\*Профиль\*\*. Из этого списка можно  
выбрать и настроить те модули, которые будут включены при сканировании  
приложения с этим профилем. Дальнейший анализ и поиск уязвимостей  
приложения будет производиться на основе собранных в ходе сканирования  
данных.  
Для эффективной работы с приложением возможно включить или выключить  
каждый конкретный модуль и провести соответствующие настройки.  
Все включенные модули отмечены значком  
«`<img alt="Picture 123" height="15.7" src="/smimg/image39.png" width="15.7" />»,  
все выключенные модули отмечены значком  
«`<img alt="Picture 19" height="13.8" src="/smimg/image40.png" width="13.1" />».  
Для изменения статуса модуля с «включен» на «выключен» и наоборот  
достаточно кликнуть мышкой на значок статуса модуля.  
Каждый модуль имеет набор специфических для него настроек. При выборе  
модуля ‎из списка модулей в левой части вкладки в правой части вкладки  
\*\*Настройки модуля\*\* отображаются его  
настройки, которые можно изменить и сохранить, нажав соответствующую  
кнопку справа внизу.  
`<img src="/img/image56.png" />  
Настройки для каждого модуля включают:  
  
\*\*Имя\*\* модуля.  
\*\*Описание\*\*.  
Список модулей, от которых зависит этот модуль.  
\*\*Настройки\*\*, которые можно изменить  
(если применимо для данного модуля --- ряд модулей не имеет изменяемых  
настроек).  
  
Работа некоторых модулей зависит от результатов других модулей. Это  
отмечено ‎в списке модулей в левой части экрана через дополнительную  
информацию, расположенную снизу имени модуля, см. рис. ниже. Если все  
«родительские» модули выключены, то зависящий от них модуль также будет  
автоматически выключен.  
<img height="59" src="/img/image59.png" width="50%" />  
``  
</p>

<h3 data-list-level="3"> ``` Требования На данной вкладке доступно управление стандартами информационной безопасности, на которые будет проверено анализируемое приложение. Создание и редактирование самих требований ‎и стандартов описано в разделе `<a data-xref="{title}" href="Trebovaniya.htm">Требования`</a>. На странице \*\*Требования\*\* основного меню перечислены все стандарты информационной безопасности и входящие в них требования, на соответствие которым можно проверить приложение. Список всех стандартов требований представлен также на вкладке \*\*Требования\*\* на странице \*\*Профиль\*\*. Из этого списка можно выбрать стандарты, на соответствие которым будут проверяться результаты тестирования приложения с этим профилем. Список входящих в стандарт требований представлен на правой части вкладки. Система предоставляет возможность включить или выключить проверку на соответствие стандартам информационной безопасности. Все включенные для проверки стандарты отмечены значком «`<img alt="Picture 124" height="15.7" src="/smimg/image43.png" width="15.7" />», все выключенные стандарты отмечены значком «`<img alt="Picture 83" height="13.8" src="/smimg/image44.png" width="13.1" />». Для изменения статуса стандарта с «включен» ‎на «выключен» и наоборот достаточно кликнуть мышкой на значок статуса стандарта. `<img height="1137" src="/img/image60.png" width="100%" />

``  
</body>

``

#### Результаты сканирований  
Результаты сканирований  
`<link rel="stylesheet" type="text/css" href="assets/css/default.css" />  
``  
</head>

<body> ```

Результаты сканирований  
``  
</h2>

``

Список результатов  
При выборе пункта меню \*\*Результаты  
сканирования\*\* отображается список всех проведенных  
сканирований. На этой странице можно посмотреть все прошедшие  
сканирования. Каждое сканирование представлено одной строкой. Данные о  
результатах сканирований автоматически обновляются каждые 10 секунд, что  
освобождает пользователя от необходимости обновлять страницу вручную.  
<img height="1152" src="/img/image61.png" width="100%" />  
В списке отображаются сканирования, отсортированные по  
\*\*Id\*\* сканирования. В таблице  
присутствует следующая информация:  
  
\*\*Id\*\* --- внутренний идентификатор  
сканирования.  
\*\*Имя проекта\*\* --- имя проекта, в рамках  
которого проводилось сканирование.  
\*\*Имя профиля\*\* --- профиль сканирования,  
с которым было проанализировано приложение.  
\*\*Режим\*\* --- режим сканирования, ручной  
или автоматический.  
\*\*Имя пакета\*\* --- имя анализируемого  
приложения в системе Android.  
\*\*Статус\*\* --- статус сканирования, может  
принимать несколько значений:  
``  
<ul>

<li class="a0"> ``` \*\*Успешно\*\* --- сканирование завершилось без ошибок. Если сканирование в целом прошло успешно, но наблюдались сбои в работе отдельных модулей, рядом со статусом отображается значок `<img alt="Изображение выглядит как текст, снимок экрана, внутренний Автоматически созданное описание" height="13.1" src="/smimg/image47.png" width="18.9" />. При наведении на него курсора появляется более подробная информация о сбоях. \*\*Создан\*\* --- сканирование создано. \*\*Запускается\*\* --- сканирование запущено, идет процесс установки и запуска целевого приложения. \*\*Запущен\*\* --- происходит процесс сканирования. \*\*Анализируется\*\* --- сканирование остановлено, осуществляется процесс анализа собранной информации. \*\*Отменяется\*\* --- сканирование было запущено, но инициирована его отмена с использованием расположенного справа раскрывающегося меню.`<img alt="Изображение выглядит как текст, внутренний, снимок экрана, компьютер Автоматически созданное описание" src="/smimg/image48.png" style="cursor: nwse-resize;" />

\*\*Отменено\*\* --- сканирование отменено с  
использованием расположенного справа раскрывающегося меню.  
``  
</p>

<p class="a0"> ``` \*\*Ошибка\*\* --- сканирование завершено с ошибкой. Рядом со статусом отображается значок `<img alt="Изображение выглядит как текст, снимок экрана, внутренний, компьютер Автоматически созданное описание" height="15.1" src="/smimg/image49.png" width="16.0" />. При наведении на него курсора появляется более подробная информация об ошибке.

``  
</li>

``

</li>  
 <li class="a0"><strong>Изменено</strong> — время запуска сканирования.</li>  
  
``  
</ul>

<p class="a1"> ``` Для отображения только необходимых результатов предусмотрен фильтр. При выборе нескольких фильтров они работают вместе, то есть при выборе режима \*\*Ручной\*\* и статуса \*\*Успешно\*\* будут найдены и отображены все успешные сканирования с ручным режимом запуска. <img src="/img/image62.png" /> При нажатии на нужную строку в таблице \*\*Результаты сканирований\*\* происходит переход к результатам выбранного сканирования. Кроме этого, находясь на данной странице, можно скачать PDF-отчет о сканировании, инициировать повторный анализ или удалить результаты сканирования. Для выполнения перечисленных действий используйте расположенное справа раскрывающееся меню. `<img alt="Изображение выглядит как текст, снимок экрана, внутренний, компьютер Автоматически созданное описание" src="/smimg/image51.png" />

``  
<h3 data-list-level="3">

Результаты сканирования Чтобы перейти на страницу **Результат сканирования**, нажмите на строку нужного сканирования в таблице **Результаты сканирования**. На открывшейся странице содержится вся информация по анализу приложения: выявленные уязвимости, собранные за время работы приложения данные, соответствие стандартам и требованиям. Для выбора доступно четыре или пять вкладок ‎в зависимости от типа сканирования: **Общая информация**, **Дефекты**, **Собранные данные**, **Требования**, **Запись сканирования**.

Общая информация

Вкладка **Общая информация** содержит сведения о проведенном сканировании и краткую информацию о проверенном приложении. ` На этой вкладке представлена общая информация по сканированию:

**Название пакета** — имя приложения в системе. **Название версии / код версии** — версия, указанная в манифесте приложения для более точной идентификации анализируемого приложения. **Target SDK/Min SDK** — версии SDK, для которых собрано данное приложение **Файл** — информация о загруженном файле. <ul> ```

\*\*Размер\*\* --- размер файла.  
\*\*md5\*\* --- хэш сумма файла.  
\*\*Тип архитектуры / Архитектура\*\* ---  
архитектура сканируемого приложения (Android / iOS).  
``  
</li>

``

</li>  
 <li class="a0"><strong>Проект</strong>, в рамках которого проводилось сканирование. Данное значение представлено в виде ссылки, нажав которую можно перейти в соответствующий проект.</li>  
 <li class="a0"><strong>Профиль</strong>, в рамках которого проводилось сканирование. Данное значение представлено в виде ссылки, нажав которую можно перейти в соответствующий профиль сканирования.</li>  
 <li class="a0"><strong>Изменено</strong> — дата сканирования.</li>  
 <li class="a0"><strong>Статус</strong> — статус сканирования.</li>  
 <li class="a0"><strong>Тест кейс</strong> — название используемого тест кейса.</li>  
  
``  
</ul>

<p class="a1"> ``` Кнопки, расположенные в правом верхнем углу, позволяют выполнить следующие действия:

``  
<ul class="Disc">

<li class="Numbering48 a0"> ``` \*\*Повторный анализ\*\* --- провести повторный анализ результатов сканирования с применением актуальных правил анализа уязвимостей для данного приложения.

``  
<li class="Numbering48 a0">

**Скачать логи** — скачать лог-файл сканирования. **Скачать отчет** — получить подробный отчет о результатах сканирования в формате pdf. **Скачать приложение** — скачать файл сканируемого приложения. </li> ```

``  
<h4 data-list-level="4">

Дефекты

На каждую выявленную уязвимость системой заводится дефект. Список всех найденных во время сканирования дефектов показан в левой половине вкладки **Дефекты**. ‎В правой части данный вкладки представлена информация о выявленной уязвимости ‎с ее детальным описанием, а также даны рекомендации по ее устранению. Для удобства работы с дефектами существует возможность выбрать и применить ‎для отображаемых дефектов фильтр. Для этого нажмите кнопку **Фильтр** в левом верхнем углу и выберите из выпадающих списков одно или несколько значений для фильтрации по параметрам **Критичность**, **Статус** и **Состояние**. Если выбран уровень критичности **Высокий** и статус **Подтвержден**, то будут отображаться все подтвержденные дефекты с высоким уровнем критичности. Фильтр может быть очищен по нажатию кнопки **Очистить фильтр** справа вверху. При повторном нажатии на кнопку **Фильтр** в левом верхнем углу, поле фильтрации будет свернуто. На вкладке **Дефекты** представлены следующие сведения о дефекте:

ID дефекта в системе. Уязвимость — требование, соответствие которому нарушает данный дефект. Критичность дефекта: <ul> ```

«`<img alt="Picture 151" height="17.6" src="/smimg/image54.png" width="16.2" />»  
--- критичный;  
«`<img alt="Picture 152" height="17.5" src="/smimg/image55.png" width="15.5" />»  
--- высокий;  
«`<img alt="Picture 153" height="18.3" src="/smimg/image56.png" width="15.5" />»  
--- средний;  
«`<img alt="Picture 154" height="17.6" src="/smimg/image57.png" width="15.5" />»  
--- низкий;  
«`<img alt="Picture 155" height="17.5" src="/smimg/image58.png" width="15.5" />»  
--- инфо.  
``  
</li>

``

</li>  
 <li class="a0">Статус дефекта:  
 <ul>  
 <li class="a0">«<img alt="Picture 159" height="16.2" src="/smimg/image59.png" width="16.2" />» — подтвержден;</li>  
 <li class="a0">«<img alt="Picture 160" height="16.1" src="/smimg/image60.png" width="16.8" />» — ложное срабатывание;</li>  
 <li class="a0">«<img alt="Picture 161" height="16.9" src="/smimg/image61.png" width="16.9" />» — не обработан.</li>  
 </ul>  
 </li>  
  
``  
</ul>

<p class="a1"> ``` Начальное заполнение значений полей дефектов производится системой автоматически во время анализа результатов. При нажатии на дефект в левой половине вкладки \*\*Дефекты\*\* справа отображается детальная информация о нем. <img src="/img/image75.png" /> Приводится следующая информация:

``  
<ol class="RoundSquare">

<li class="a0"> ``` \*\*ID\*\* дефекта в системе. \*\*\*\*Название выявленной уязвимости. Рядом с названием располагается иконка «`<img src="/img/image8.png" />», нажав которую можно скачать отчет об уязвимости в формате PDF. Состояние дефекта:

``  
<li class="a0">

**Новый** — если этот дефект был впервые найден во время этого сканирования, либо он уже встречался ранее, а затем проблема была решена и дефект был закрыт, но при этом сканировании вновь проявился. **Старый** — если этот дефект был уже ранее найден во время предыдущих сканирований. **Исправленный** — это состояние для тех дефектов, которые были найдеры в предыдущих сканированиях, но в текущем сканировании их уже нет. </li> ```

</li>  
 <li class="a0"><strong>Критичность</strong> дефекта. В этом поле отображается текущее значение критичности дефекта и предоставляется возможность поменять критичность, выбрав новое значение из выпадающего списка. Важно отметить, что при смене критичности дефект автоматически получает статус «Подтвержден», то есть, присваивая дефекту уровень критичности, мы признаем, что он существует.</li>  
 <li class="a0"><strong>Статус</strong> дефекта. В этом поле отображается текущий статус дефекта и предоставляется возможность поменять статус, выбрав новое значение из выпадающего списка.</li>  
 <li class="a0"><strong>Описание</strong> дефекта в краткой форме характеризует найденную уязвимость. Рядом с описанием располагается ссылка на Wiki-страничку с подробным описанием уязвимости, рекомендациями по исправлению, примерами исходного кода и ссылками на материалы по этой уязвимости.</li>  
  
``  
</ol>

<p class="a0-no-list"> ``` \*\*Примечание:\*\* Отдельно следует отметить дефекты, выявленные модулем «Поиск ранее найденной чувствительной информации». В поле \*\*Описание\*\* таких дефектов, кроме упомянутой выше информации, можно найти ссылку на уязвимости (\*\*Смотреть детали\*\*), которые послужили основанием для создания такого дефекта (\*\*`<a class="expandspot" data-rhwidget="ExpandSpot" data-target="expanding" href="#" style="color: #000080">подробнее`</a>[: В основе работы данного модуля лежит анализ информации, собранной другими модулями, вычисление популярных хеш-функций и кодирование обнаруженных параметров с последующим повторным поиском по всем данным]{.expandtext data-targetname="expanding" style="color: #0000FF"}[[]{style="text-align:left;"}]{style="color:#0000ff;"}\*\*[)]{style="text-align:left;"}.

``  
<p class="a0-no-list" style="text-align: center">

`

Место возникновения дефекта. Если обнаружено несколько уязвимостей одного типа, они группируются в один дефект, а справа от данного поля появляются стрелки, с помощью которых можно переходить между уязвимостями. Ниже приводится важная фактическая информация по найденной уязвимости, например, обнаруженная чувствительная информация, место ее обнаружения, и т. п. В поле Результат отображается фрагмент кода или содержимое файла (до 5000 знаков), в котором обнаружена уязвимость. Если необходимо загрузить соответствующий файл целиком, нажмите ссылку **Загрузить**, расположенную справа.

Если в результате анализа были найдены уязвимости, которые определяются нами как ложные срабатывания, они могут быть добавлены в исключения как на уровне проекта, так и на уровне организации (ко всем проектам организации). Для этого необходимо выбрать один или несколько обнаруженных дефектов, изменить их статус на «Ложное срабатывание» и нажать кнопку **Добавить в исключения**, расположенную в верхнем правом углу вкладки **Дефекты** окна **Результат сканирования**. </p> ```

[[`<img height="1023" src="/img/image80.png" width="100%" />]{style="text-decoration:underline;"}]{style="color:#000000;"}  
``  
</p>

<p> ``` [В появившемся окне \*\*Добавление исключений\*\* выберите, на каком уровне вы хотите добавить исключения --- на уровне проекта или на уровне организации, а затем нажмите кнопку \*\*Добавить\*\*.]{style="color:#000000;"}

``  
<p style="text-align: center">

<img height="451" src="/img/image83.png" width="50%" />]{style="color:#000000;"} `` </p> ``` `` <p> ``` [Также можно добавить исключение для отдельной уязвимости, нажав кнопку \*\*Добавить исключение\*\* рядом с заголовком \*\*Найдено правилом\*\* в описании соответствующей уязвимости.]{style="color:#000000;"} `` </p> ``` `` <p style="text-align: center"> ``` [ </p> ```

[В появившемся окне \*\*Добавление  
исключения\*\* выберите, на каком уровне вы хотите  
добавить исключение --- на уровне проекта или на уровне организации, а  
затем нажмите кнопку  
\*\*Добавить\*\*.]{style="color:#000000;"}  
``  
</p>

<p style="margin:0cm 0cm 8pt;text-align:center"> ``` [`<img height="451" src="/img/image82.png" width="NaN" />]{style="color:#000000;"}

``  
<p>

В результате добавления исключений при повторном анализе результатов или при следующем сканировании в рамках этого проекта, если выбран уровень проекта, или для всех проектов организации, если выбран уровень организации, такие уязвимости учитывать не будут.

Собранные данные

На вкладке **Собранные данные** отображается вся информация о работе приложения, собранная за время сканирования. Информация разделена по модулям, которые отвечают за сбор данных. Для модулей предусмотрена возможность скачивания собранных данных в виде zip-архива с помощью кнопки **Загрузить данные модуля**, или же, возможно скачать все данные сканирования сразу в одном архиве с помощью кнопки **Загрузить все данные**. Для работы с собранными в ходе сканирования данными выберите на странице **Результаты сканирований** вкладку **Собранные данные**. На данной вкладке доступны данные, собранные во время сканирования приложения всеми включенными в профиле модулями. Модуль для просмотра собранных данных может быть выбран из выпадающего списка в верхнем левом углу. Каждый из модулей собирает данные, специфичные только для него. Соответственно, формат представления данных на вкладке отличается для каждого модуля. На рисунке выше в качестве примера приведены данные, собранные модулем «Сетевая активность». В этом случае были собраны данные, переданные по сети — адрес, хост, протокол, время, метод, порт, а также содержание запроса и ответа. Такого сорта дополнительная информация может оказаться полезной в работе с результатами анализа. На рисунке ниже приведен еще один пример, иллюстрирующий другую область работы приложения — данные, собранные модулем «Отслеживание Activity». Здесь Activity — это все различные экраны приложения, которые были запущены во время сканирования. Для каждого экрана (Activity) приведены его имя и параметры запуска. <img src="/img/image11.png" /> Результаты работы всех модулей собраны в одной системе, что значительно упрощает их анализ. Такой подход обладает явными преимуществами по сравнению с ситуацией, когда данные о работе приложения последовательно и в различных форматах собираются несколькими утилитами. Помимо предоставления пользователям возможности работы с собранными данными, система на их основе делает выводы об уязвимостях приложения. Правила анализа собранных данных для поиска уязвимостей подробно описаны в разделах Правила</a> Руководства пользователя и Правила анализа на уровне Организации` Руководства прикладного администратора.

Требования

Для работы с требованиями выберите на странице **Результат сканирования** вкладку **Требования**. На этой вкладке отображаются результаты проверки выполнения требований для проанализированного приложения. На вкладке **Требования** представлено соответствие стандартам безопасности, выбранным в профиле сканирования. Требования и стандарты, в которых были выявлены несоответствия, отмечаются красным цветом. <img src="/img/image12.png" style="cursor: nwse-resize;" /> Красным цветом отмечены требования, которые не выполнены. Если кликнуть мышкой по невыполненному требованию на вкладке \*\*Стандарт \*\*в левой части, в правой части на вкладке \*\*Дефекты \*\*появится список типов дефектов, которые были проверены для выбранного требования. В случае обнаружения дефектов определенного типа при проверке требования, этот тип дефектов отмечается значком «<img alt="Picture 21" height="12.4" src="/smimg/image69.png" width="13.9" />», а само требование считается невыполненным и отмечается красным цветом. Если дефектов определенного типа при проверке требования выявлено не было, такой тип дефектов отмечается значком «». Требование в целом считается выполненным, если при его проверке не было выявлено ни одного дефекта из числа относящихся к этому требованию типов дефектов. При нажатии в области **Дефекты** на тип дефекта, отмеченного значком «<img alt="Рисунок 56" height="15.3" src="/smimg/image71.png" width="15.3" />», появится окно с детальной информацией по дефектам данного типа: Для возвращения к списку требований нажмите кнопку **Вернуться к списку требований** в левом верхнем углу. На вкладке **Требования** доступны данные по выполнению требований всех выбранных в профиле сканирования стандартов. Если в профиле добавить еще один стандарт ‎к списку проверяемых, то после этого при просмотре результатов всех уже ранее проведенных с этим профилем сканирований, на вкладке **Требования** будет отображаться также соответствие ранее собранных результатов и вновь выбранного в профиле стандарта.

Запись сканирования

Данная вкладка доступна только для результатов автоматического сканирования ‎и предоставляет возможность просмотра видеозаписи проведенного сканирования ‎и процесс выполнения тест кейса. </p> ```

``  
</p>

</body> ```

#### Работа со сканированиями  
##### Запуск сканирования  
Запуск сканирования  
`<link rel="stylesheet" type="text/css" href="assets/css/default.css" />  
``  
</head>

<body> ```

Запуск сканирования  
``  
</h2>

<p data-list-level="2"> ``` Запуск сканирования может быть произведен в ручном или в автоматическом режиме. Запустить сканирование можно через пункт основного меню \*\*Запуск сканирования\*\*.

``  
<p data-list-level="2">

` На странице **Запуск сканирования** представлены необходимые поля для запуска анализа приложения:

Кнопка **Выбрать файл** справа вверху позволяет выбрать файл приложения (*.apk или* .ipa) для загрузки. Пока файл приложения не выбран, остальные поля на данной странице недоступны для редактирования.<br /> \*\*Примечание:\*\* Если пакет с выбранным именем и хеш суммой уже загружен, в целях экономии ресурсов его повторная загрузка не производится, а используется файл, уже имеющийся на сервере. После загрузки файла тестируемого приложения в заголовке страницы отображается следующая информация о нем: **имя пакета**, **название/код версии**, **Target SDK**, **Min SDK**, **имя/размер/хеш файла** и **тип архитектуры**. **Проект** — проект, в рамках которого будет проводиться сканирование.<br /> \*\*Примечание:\*\* Для выбора доступны либо проекты с незаполненным при создании полем \*\*Имя пакета\*\* (см. раздел Проекты</a>), либо те, для которых в данном поле указан пакет, выбранный в предыдущем шаге. Таким образом, не исключена ситуация, когда в данном поле будут отсутствовать доступные для выбора элементы. В этом случае следует создать новый проект с пустым полем \*\*Имя пакета\*\* или, указав в нем соответствующий пакет. \*\*Профиль\*\* --- профиль сканирования, для которого будет проводиться сканирование. \*\*Режим сканирования\*\* --- ручной или автоматический режим сканирования. \*\*Тест кейс\*\* --- эта опция появляется в случае выбора автоматического режима. Выбор тест кейса, который будет воспроизведен. **Примечание:** Отображаются только тест кейсы выбранного проекта. **Архитектура** — архитектура устройства, на котором будет запущено приложение.

    </p> ```

``  
</html>

# Руководство по установке и обновлению

# Рекомендации по безопасной разработке приложений