# DerScanner 11

Новинки релиза

# Новые возможности

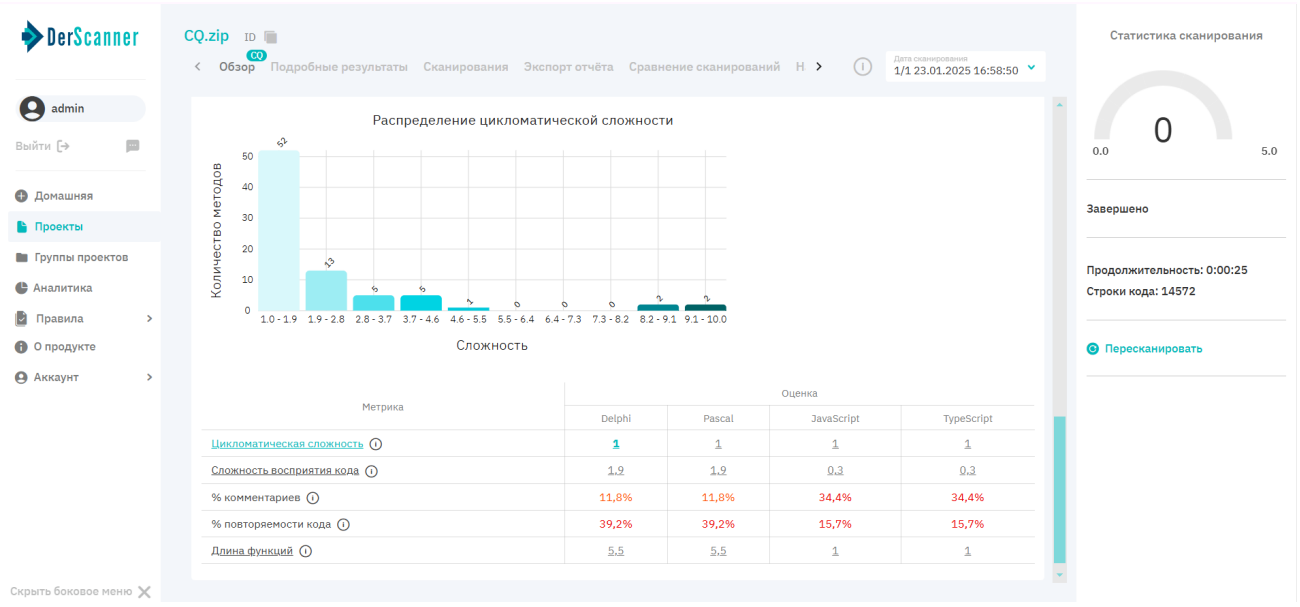
## Статический анализ качества кода

### Почему это важно

Написание чистого, удобного в обслуживании кода необходимо для создания безопасных, надежных и долговечных приложений. Однако устаревший код, плохая практика и чрезмерно сложные структуры могут внести ненужную путаницу, увеличить технический долг и замедлить разработку. Новый анализ качества кода в DerScanner решает эти проблемы. Эта функция, включающая почти **100 новых правил,** помогает разработчикам выявлять и устранять проблемы на ранних стадиях, улучшая читаемость, снижая будущие затраты на сопровождение и сводя к минимуму количество ошибок. Опираясь на лучшие отраслевые практики, Code Quality Analysis гарантирует, что ваши проекты будут не только функциональными, но и перспективными, а также более простыми в управлении.

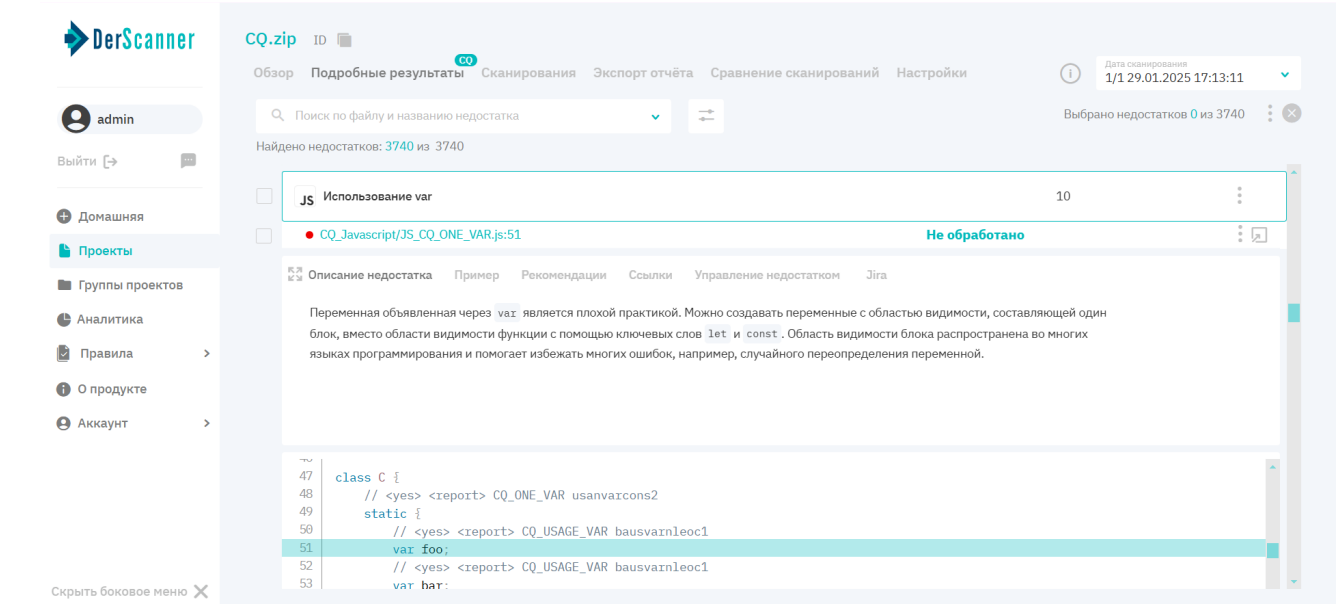
### Как это работает

Анализ качества кода интегрирован непосредственно в DerScanner и поддерживает приложения, написанные на **JavaScript/TypeScript/TSX**, а **также Delphi/Pascal**. Он выявляет устаревший код, плохие практики, дублирующиеся секции и слишком сложные функции или методы. Функция работает, применяя расширенные статические правила для обнаружения структурных и концептуальных несоответствий в коде. Ее можно запустить вместе со стандартным статическим анализом для беспрепятственной интеграции или использовать самостоятельно для целенаправленной проверки качества.



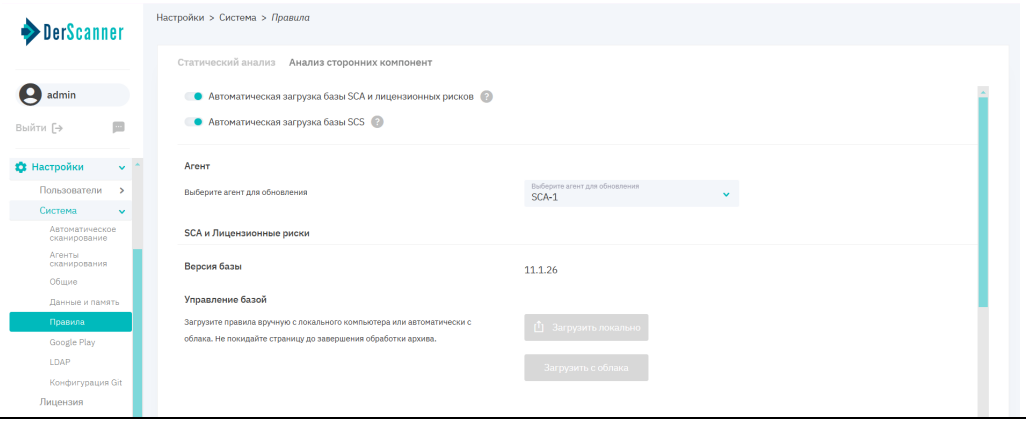


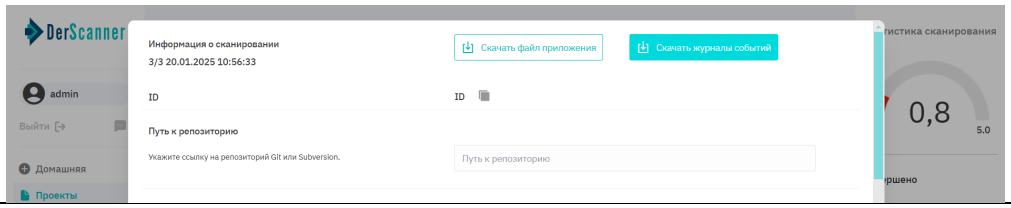
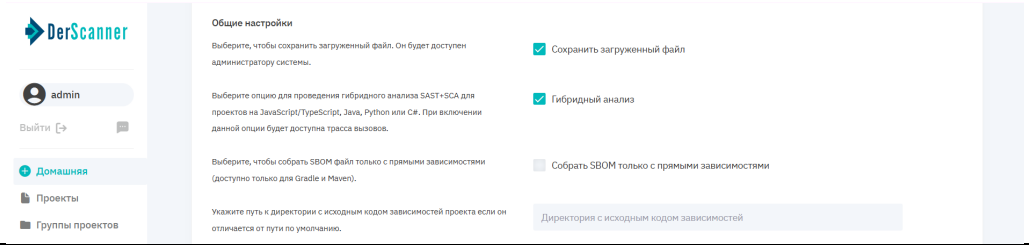

DerScanner




- ## Значительное обновление анализа состава программного обеспечения

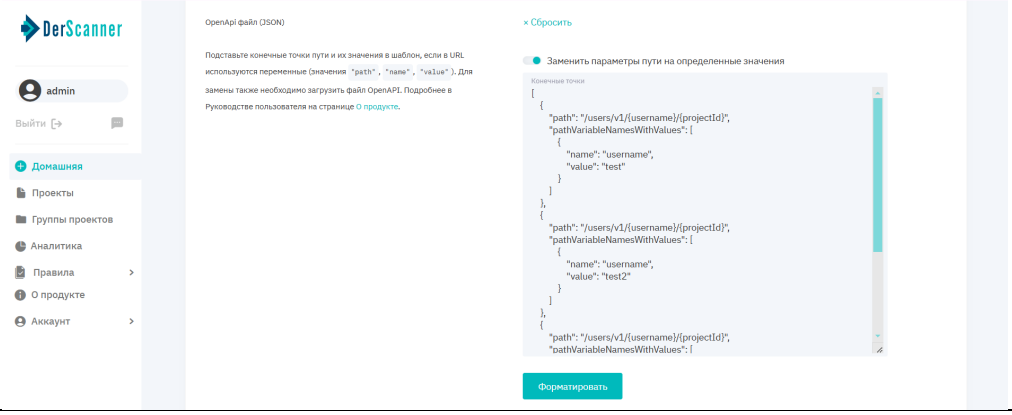
  Мы внесли значительные улучшения в анализ состава программного обеспечения (SCA), чтобы сделать его более быстрым, точным и удобным для пользователя.

| Возможности | Почему это важно и как это работает |
|---|---|
| Обновления уязвимостей в режиме реального времени | Наши базы данных уязвимостей для SCA и SCS теперь обновляются каждые 1-2 часа, благодаря чему вы никогда не пропустите новые опасные угрозы. Такой последовательный цикл обновлений обеспечивает защиту ваших проектов от возникающих уязвимостей. *Для инсталляций с воздушной защитой возможно обновление вручную.*  |
| Улучшенный гибридный анализ | Усовершенствования обеспечивают более точное обнаружение уязвимых функций или импорта, снижая вероятность пропуска проблем при гибридном анализе. |
| Более быстрое и эффективное | Благодаря улучшенным алгоритмам построения графов, отрисовка графиков зависимостей теперь происходит значительно быстрее и создает |

| | |
|---|---|
| отображение зависимостей | минимальную нагрузку на устройство, повышая отзывчивость интерфейса. Оптимизированные алгоритмы трассировки импорта библиотек позволили сократить общее время сканирования и получить более быстрые результаты. |
| Расширенная система регистрации и диагностики | Теперь подробные журналы сканирования можно сохранять и загружать отдельно, что позволяет получить четкое представление о любых проблемах. Эта функция упрощает поиск и устранение неисправностей и повышает общую надежность.<br>  |
| Оптимизация скорости | Возможность отключения гибридного анализа SCA+SAST значительно повышает скорость сканирования, особенно для проектов с большим количеством зависимостей. Эта опция может сократить время сканирования больших проектов на несколько часов.<br>  |
| Исправление ошибок и улучшение точности | Мы устранили такие проблемы, как дублирование импорта библиотек, некорректные триггеры уязвимостей и ошибки при сравнении версий библиотек, чтобы обеспечить более точные результаты.<br>Устранены ошибки в построении графов на нескольких языках, что позволило сократить количество ошибок при работе над многоязычными проектами. |
| Сбор прямых зависимостей для проектов JAVA | Эта новая функция позволяет решить проблемы, возникающие при анализе Java-проектов с зависимостями из частных репозиториев или при ограниченном доступе к публичным репозиториям. Позволяя собирать прямые зависимости непосредственно из файлов проекта, она гарантирует, что даже в средах с ограниченным доступом к репозиториям можно провести тщательный и точный анализ. |

## • Динамическое тестирование безопасности приложений

| Возможности | Почему это важно и как это работает |
|---|---|
| Сканирование переменных URL | Новая функция сканирования переменных URL значительно улучшает покрытие тестов. Позволяя анализировать несколько комбинаций URL-адресов за один прогон, она обеспечивает тщательную и всестороннюю оценку различных сценариев конечных точек, выявляя потенциальные проблемы, на которые раньше можно было не обращать внимания. |

| | |
|---|---|
| | Благодаря этой функции пользователи могут указывать конечные точки и значения переменных непосредственно в настройках анализа. Предоставив файл OpenAPI, система может точно отобразить и протестировать указанные комбинации, предоставляя подробные результаты и повышая общую эффективность тестирования.<br>  |
| Поддержка авторизации NTLM | Добавление поддержки авторизации NTLM повышает безопасность и совместимость сред, использующих аутентификацию NTLM. Это обеспечивает беспрепятственное взаимодействие с системами и ресурсами, защищенными NTLM, предоставляя пользователям более надежную и безопасную работу. |

# Улучшения

## Правила обнаружения уязвимостей:

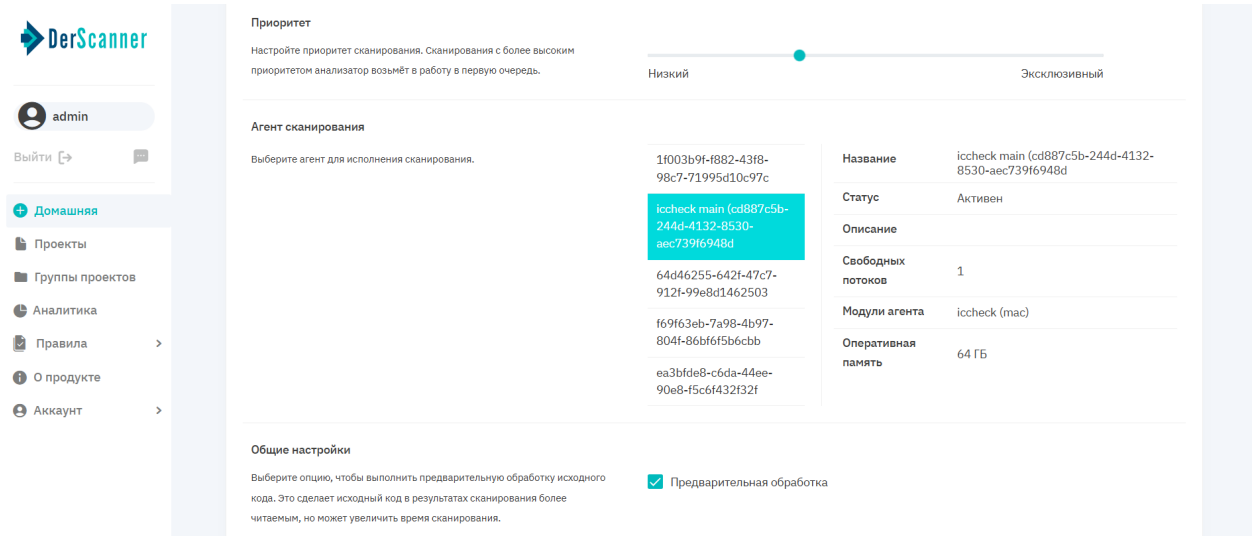
- Значительно улучшен анализ испорченности для **Delphi**.
- Расширенное освещение фреймворка **FireMonkey** для Delphi.
- Улучшен анализ потока данных для **Go**.
- Обновленные полезные ссылки для 500+ правил.
- Добавлено более **300** новых паттернов уязвимостей и качества кода для **C#, Delphi/Pascal, JavaScript, TypeScript, Perl, PHP и Python**.

## Модули анализа:

- Повышена скорость анализа и оптимизировано потребление памяти, что особенно заметно на больших проектах.
- Значительно ускорена предварительная обработка файлов JavaScript.
- Улучшена логика работы паттернов для анализа ошибок, в частности управление флагами при срабатывании нескольких паттернов в одном и том же месте кода.
- Улучшена работа с файлами **.asp** для VBScript.

## Пользовательский интерфейс:

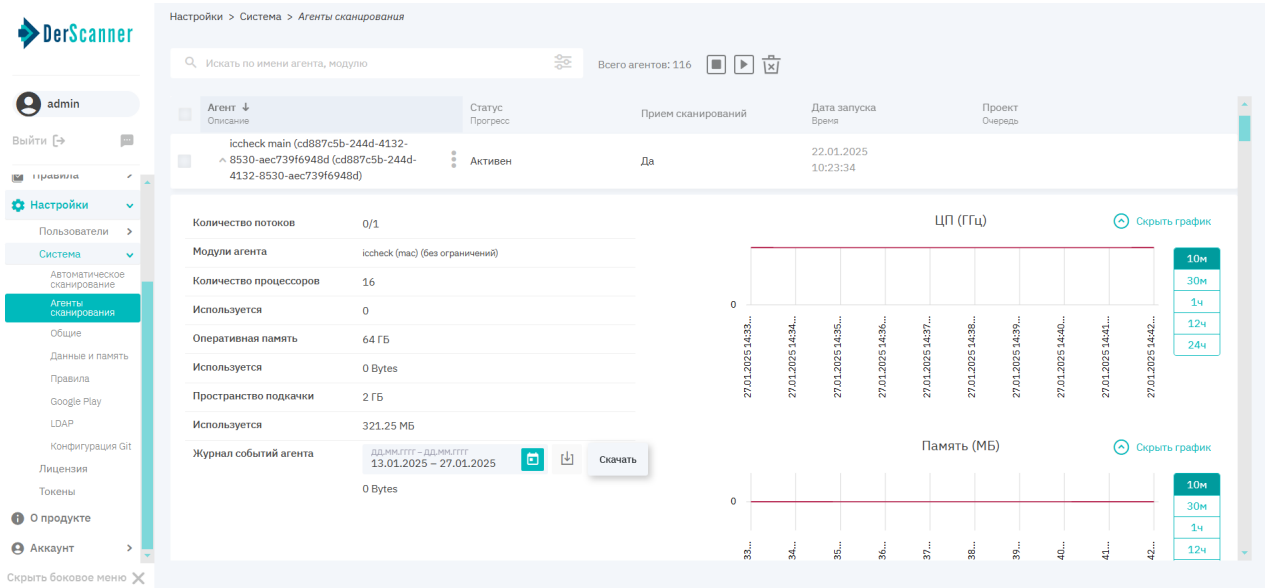
- Представляем управление **агентами сканирования**. Эта функция повышает прозрачность и гибкость управления ресурсами, например, для тяжелых Java-проектов.
  Список агентов находится в настройках анализа. Щелкните на агенте, чтобы получить подробную информацию о его статусе, рабочей нагрузке и поддерживаемых технологиях. Ваш выбор может быть сохранен для последующих сканирований, чтобы ваши проекты всегда получали нужные ресурсы.



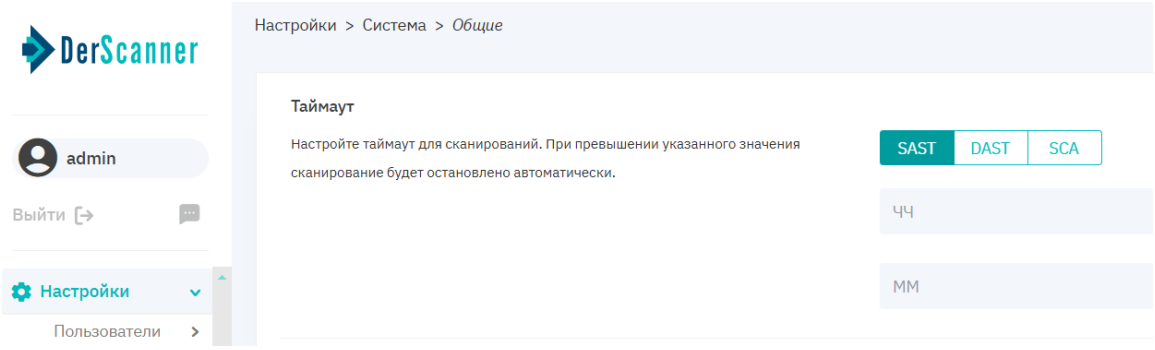

- Обновление качества жизни для **просроченных лицензий**. Теперь результаты выполненных сканирований будут доступны для просмотра постоянно.

## Администрация:

- В панель администратора добавлена новая вкладка **"Сканировать агентов"**. На ней находятся все агенты, а также инструменты управления. Каждый агент содержит информацию о своих технических характеристиках, данные о рабочей нагрузке и исторические данные об использовании: графики и журналы.
  Управляйте потоками анализа и распределением памяти, чтобы облегчить сканирование больших проектов. При необходимости отсюда можно отключить агентов.




- Добавлена настройка **таймаута сканирования** для каждого типа анализа. Это также будет полезно для управления очередью сканирования.




- **Развертывание:**
  - Пришло время попрощаться с модулем ENV. Это изменение обеспечивает поддержку большего числа дистрибутивов Linux, а также упрощает процесс установки и обновления системы.

- **Пользовательский интерфейс:**
  - Отчет:
    - Внесены изменения в формат отчетов SARIF для совместимости с предыдущими версиями Defect Dojo.