

ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 10. Статический анализ исходного кода



ПРЕДСТАВИМСЯ!

Спикеры и гости вебинара



ГЛЕБ АСЛАМОВ

DEVELOPER ADVOCATE, C# DEVELOPER

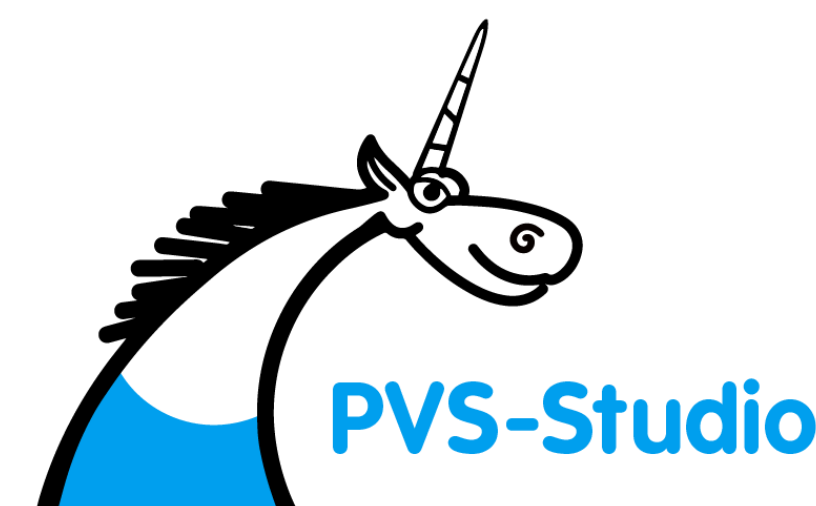
- Разработчик C# части анализатора PVS-Studio.
- Рассказываю про качество кода и безопасную разработку на конференциях, пишу технические и научные статьи для форумов и журналов.



@A-G-B



@AGBtlg



ВИТАЛИЙ ПИКОВ

ЭКСПЕРТ В ОБЛАСТИ ИТ, ИБ, ПРЕПОДАВАТЕЛЬ

- Стаж преподавательской работы более 10 лет.
- Заслуженный доцент Российского нового университета, преподаватель высшей школы.
- Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS.
- Автор более 30 научных публикаций.



О ЦИКЛЕ ВЕБИНАРОВ

«Вокруг РБПО за 25 вебинаров»

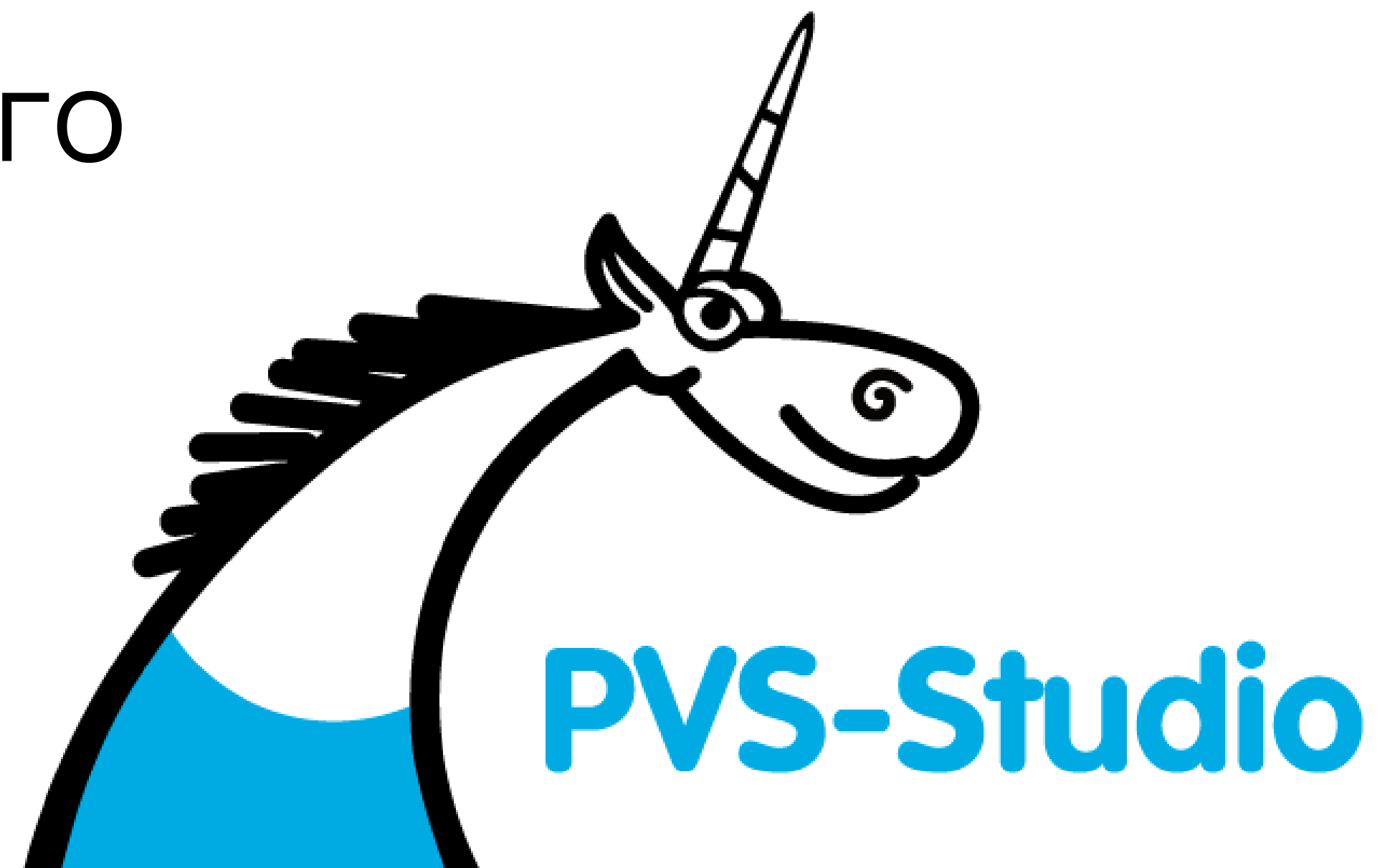


ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ: ГОСТ Р 56939-2024

- Организуют УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- ГОСТ Р 56939-2024 описывает 25 процессов, необходимых для реализации разработки безопасного ПО, поэтому и 25 вебинаров
- Мы открыты к сотрудничеству по разбору тем, пишите нам!

О ПРОЦЕССЕ

5.10 Статический анализ исходного кода



5.3.1 ЦЕЛИ

Предотвращение внесения потенциально опасных конструкций и ошибок в ПО, а также использования опасных конструкций и уязвимостей из заимствованного кода.



5.3.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

1. Разработать регламент проведения статического анализа исходного кода ПО.
2. Определить инструменты статического анализа для каждого используемого в ПО языка программирования.
3. Определить конфигурацию и параметры настройки инструментов статического анализа.
4. Проводить статический анализ с использованием инструментов статического анализа с регистрацией всех предупреждений о потенциальных ошибках, полученных по результатам работы инструментов статического анализа.

5.3.2 ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ

5. Осуществлять пересмотр конфигурации и параметров настройки инструментов статического анализа при выполнении установленных событий (изменениях в правилах сборки, применяемых статических анализаторах, получении информации об уязвимостях и т. п.).
6. Осуществлять повторный статический анализ ПО после:
 - устранения ранее выявленных ошибок и уязвимостей;
 - внесения изменений в ходе разработки в исходные тексты ПО;
 - изменения используемых версий компиляторов, сред выполнения (для компилируемого в промежуточное представление или интерпретируемого кода), обновлений используемых инструментов статического анализа.

5.3.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

Регламент проведения статического анализа исходного кода ПО должен содержать следующие сведения:

- обязанности сотрудников и их роли при проведении статического анализа;
- критерии выбора инструментов статического анализа;
- критерии выбора ПО (модулей ПО, компонентов ПО, функциональных подсистем ПО), подлежащих проведению статического анализа;
- правила обработки срабатываний средств статического анализа;
- типы и критичность ошибок (уязвимостей), выявляемых статическим анализатором, подлежащих устранению, и приоритеты устранения ошибок (уязвимостей);
- периодичность проведения статического анализа или события, при наступлении которых необходимо выполнять повторный статический анализ;
- критерии пересмотра конфигурации и параметров настройки инструментов статического анализа.

5.3.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Перечень инструментов статического анализа должен включать наименования инструментов статического анализа, их версии и информацию о соответствии используемым языкам программирования.
- Конфигурации и параметры настройки инструментов статического анализа должны обеспечивать выполнение требований регламента проведения статического анализа в части выявления типов и критичности ошибок (уязвимостей), периодичности проведения статического анализа или событий, при наступлении которых необходимо выполнять повторный статический анализ.

5.3.2 АРТЕФАКТЫ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ

- Отчеты по результатам проведения статического анализа должны включать:
 - срабатывания инструментов статического анализа;
 - результаты анализа (разметки) выявленных ошибок (срабатываний статического анализатора).
- Конфигурации и параметры настройки инструментов статического анализа, уточненные по результатам выполнения требований 5.10.2.5, должны обеспечивать выполнение требований регламента проведения статического анализа в части выполнения критериев их пересмотра.

СТАТИЧЕСКИЙ АНАЛИЗАТОР PVS-STUDIO В КОНТЕКСТЕ РБПО

- PVS-Studio включён в Реестр российского ПО: запись № 9837
- Совместим с ГОСТ Р 71207-2024 (Статический анализ кода)
- Соответствие требованиям "Методики выявления уязвимостей и недекларированных возможностей в программном обеспечении" от 25 декабря 2020 г.
- Может применяться для РБПО согласно ГОСТ Р 56939-2024
- Участвует в инициативе ФСТЭК по испытанию статических анализаторов

ПЕРЕХОДИМ К ДОКЛАДАМ



Сделай свой проект
чистым и безопасным
вместе с PVS-Studio



VOKRUG_RBPO25



Получи 10% скидку
на курсы «М БРПО»
в Учебном Центре «МАСКОМ»



VOKRUG_RBPO25

