

# ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

## Вебинар 16. Использование инструментов композиционного анализа





# ПРЕДСТАВИМСЯ!

Спикеры и гости вебинара



# Александра Уварова

Developer Advocate, C++ Developer

- Разработчик C++ части анализатора PVS-Studio.
- Рассказываю про качество кода и безопасную разработку на конференциях
- Пишу технические и научные статьи



@AleksandraUvarova



# 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





# Смирнов Алексей Алексеевич

Основатель и генеральный директор  
CodeScoring

- Занимается вопросами экспертного анализа исходных кодов на качество и безопасность с 2011 года
- Регулярно выступает на конференциях по вопросам применения композиционного анализа, состояния мирового open source и методическим аспектам внедрения процессов безопасной разработки

**Доклад:** Основы работы композиционного анализа и практика применения с CodeScoring



**CODE**  
**SCORING**

# Володченко Антон Валерьевич

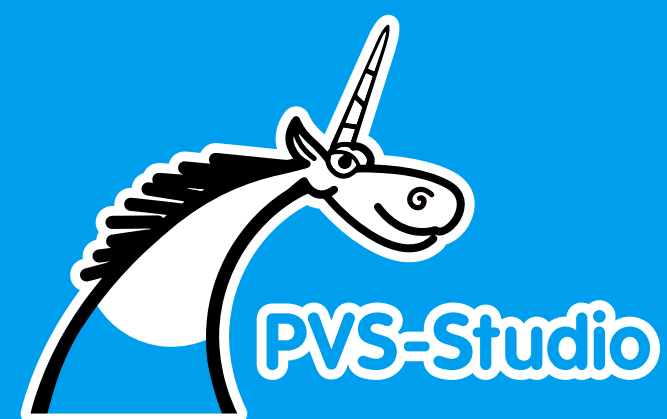
Руководитель разработки продуктов в  
CodeScoring

- 16 лет в IT
- 12 лет в кибербезе
- Путь от PHP-разработчика сайтов-визиток до PO ведущих российских AppSec-продуктов.



**CODE**  
**SCORING**

# О цикле 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
- Также, цикл включает в себя бонусные вебинары
- Мы открыты к сотрудничеству по разбору тем, пишите нам!

ЗАПИСИ ПРЕДЫДУЩИХ ВЕБИНАРОВ

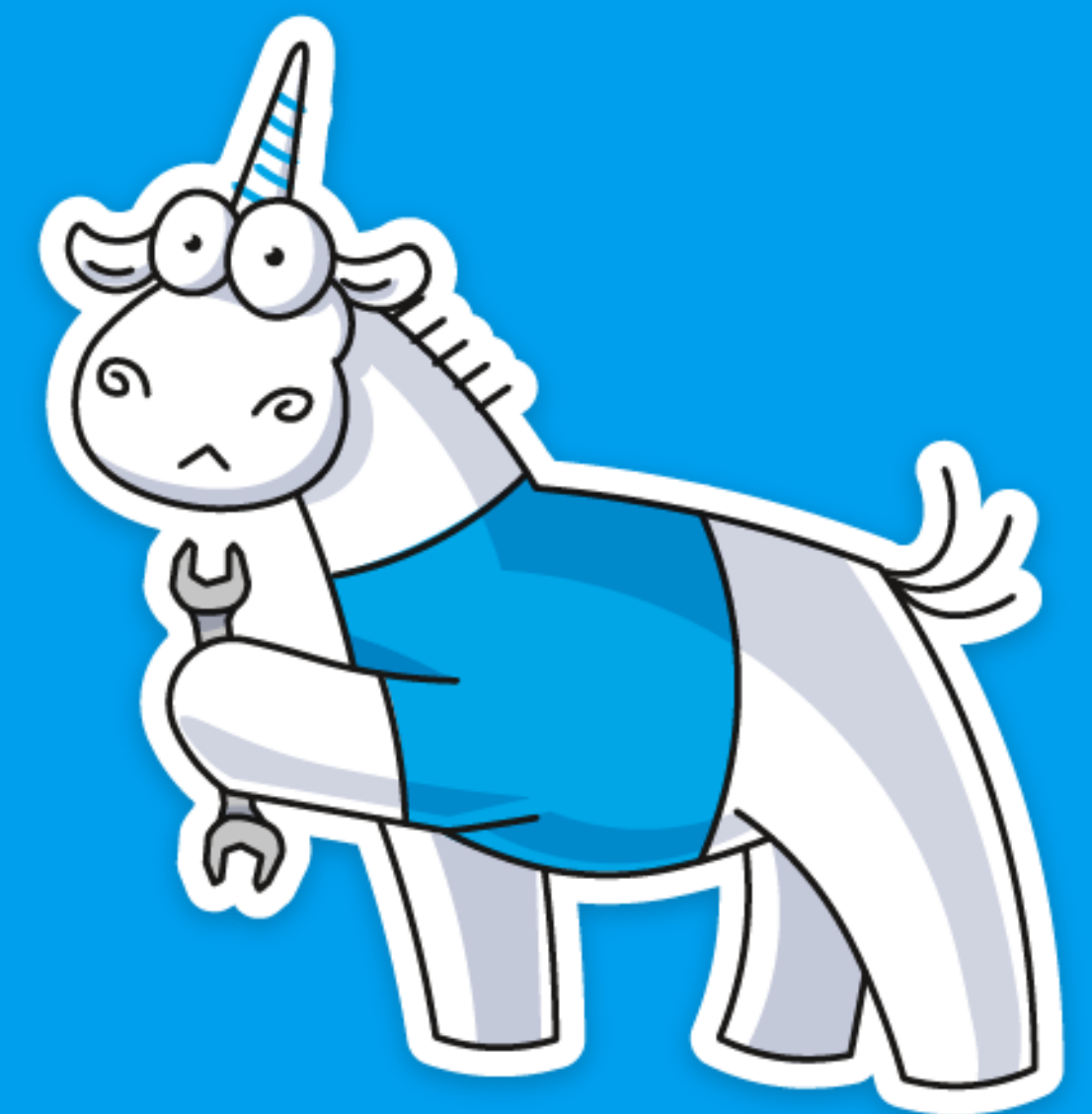
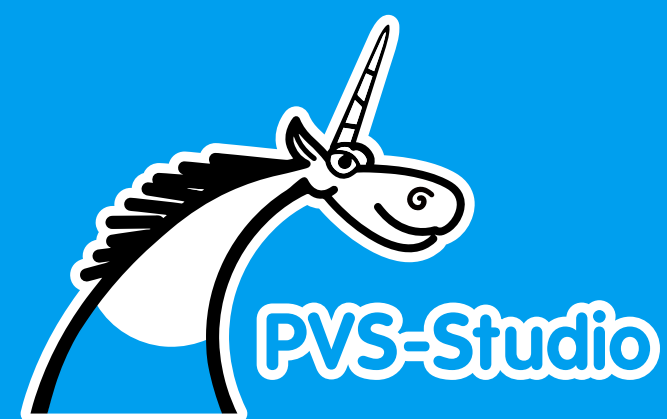


[pvs-studio.ru/ru/webinar/rbpo/](https://pvs-studio.ru/ru/webinar/rbpo/)



# Процесс 16

## Использование инструментов композиционного анализа



## 5.16.1 Цели

### 5.16.1.1 Создание условий для снижения рисков наследования уязвимостей и недекларированных возможностей при использовании заимствованного кода в коде ПО разработчика.

- Примечание — В данном подразделе под композиционным анализом понимается вид работ, основанный на формировании перечня зависимостей ПО, определении особенностей их использования, выявлении наличия уязвимостей и/или иных недостатков в зависимостях ПО.



## 5.16.2 Требования к реализации

- Разработать регламент композиционного анализа
- Формировать перечень зависимостей ПО.
- Контролировать и актуализировать перечень зависимостей ПО в соответствии с регламентом композиционного анализа на предмет наличия известных уязвимостей.
- Осуществлять анализ заимствованных компонентов, составляющих поверхность атаки, на предмет наличия известных уязвимостей
- Применять корректирующие воздействия по результатам анализа заимствованных компонентов на предмет наличия известных уязвимостей.



## 5.16.3 Артефакты реализации требований

**Регламент композиционного анализа должен содержать следующие сведения:**

- обязанности сотрудников и их роли при проведении композиционного анализа;
- правила отслеживания уязвимостей для заимствованных компонентов, участвующих в сборке ПО;
- правила проведения анализа заимствованных компонентов на предмет наличия известных уязвимостей;
- правила принятия компенсирующих и защитных мер по противодействию выявленным угрозам безопасности в цепочке поставки сторонних компонентов;
- периодичность проведения композиционного анализа в соответствии с установленными практиками сборки ПО.

## 5.16.3 Артефакты реализации требований

**Перечень зависимостей ПО должен включать следующие сведения:**

- перечень модулей заимствованного ПО с указанием их версий
- источник модулей заимствованного ПО

**Результаты анализа заимствованных компонентов должны содержать следующие сведения:**

- сведения о наличии/отсутствии известных уязвимостей в заимствованных компонентах
- сведения о критичности выявленных уязвимостей в заимствованных компонентах.

## 5.16.3 Артефакты реализации требований

**Результаты контроля актуальности перечня зависимостей ПО должны включать следующие сведения:**

- описание процедуры контроля перечня зависимостей ПО и его актуализации
- описание инструментов контроля актуальности перечня зависимостей ПО
- журналы регистрации событий, связанных с контролем актуальности перечня зависимостей ПО, а также связанных с обновлениями модулей заимствованного ПО, участвующих в сборке ПО



## 5.16.3 Артефакты реализации требований

**Результаты применения корректирующих воздействий по устранению уязвимостей в зависимостях ПО могут содержать:**

- для ПО с закрытыми исходными текстами:
  - результаты анализа применимости и реализуемости уязвимости
  - результаты обращения к поставщику уязвимых модулей ПО по поводу их обновления
  - результаты обновления зависимых компонентов ПО по мере поступления обновлений
  
- для ПО с открытыми исходными текстами:
  - результаты анализа применимости и реализуемости уязвимости,
  - результаты попыток обновления зависимых компонентов, в случае невозможности обновления путем обновления версии — применения собственного механизма исправления.

# К цепочкам поставок нужно относиться внимательно

Свежий пример:

- [В ходе атаки GhostAction скомпрометировано 817 репозиториев на GitHub](#)

Недавний круглый стол на рассматриваемую тему:

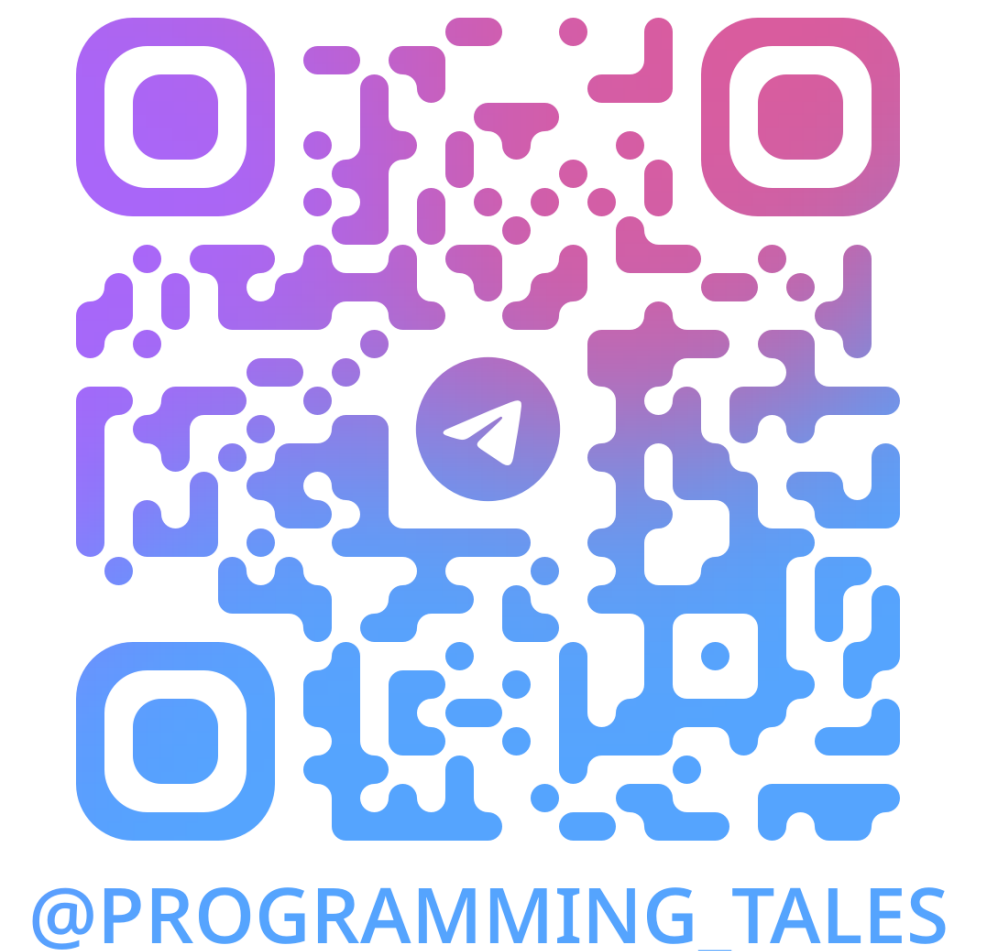
- [Цепочка поставок как угроза: как контролировать риски стороннего ПО](#)

Подборка [SCA-инструментов](#)

Процесс 17. Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок

# Дополнительные материалы

- [Software composition analysis](#)
- [SCA на языке безопасника](#)
- [Инструкция по SCA: генерация SBOM, инструменты, отличия](#)
- [Practical Guide to NTIA Compliant SBOM](#)
- [Методическая рекомендация № 2025-09-012. Алгоритм представления перечня заимствованных](#)
- Телеграм канал «[Бестиарий программирования](#)»:
  - Публикуется цикл постов, посвящённых РБПО
  - Пост «[РБПО-061. Процесс 15](#) – Использование инструментов композиционного анализа»





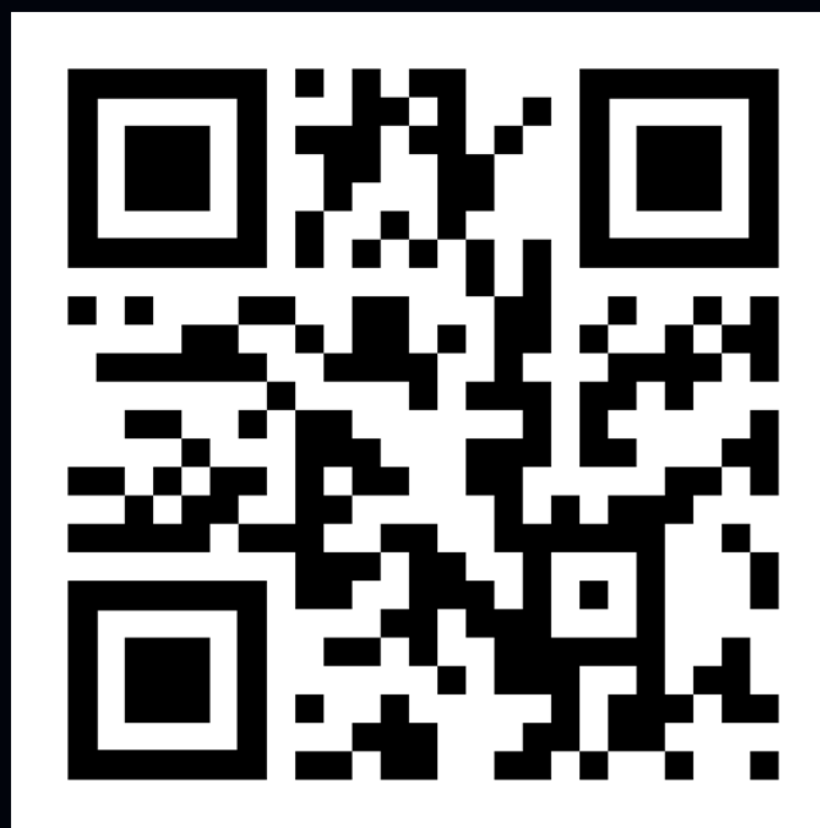
ПЕРЕДАЮ СЛОВО  
СЛЕДУЮЩЕМУ СПИКЕРУ



Сделай свой проект  
чистым и безопасным  
вместе с PVS-Studio



Telegram-канал  
CodeScoring



Сайт CodeScoring



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

