

# ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

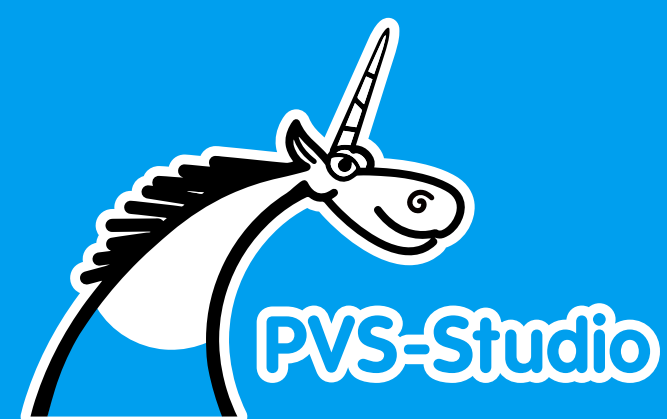
ГОСТ Р 56939-2024

Вебинар 24.  
Поиск уязвимостей  
в программном обеспечении  
при эксплуатации





# Спикеры и гость вебинара



# Владислав Богданов

Developer Advocate, Java Developer

- Разрабатываю ядро статического анализатора PVS-Studio для языка Java.
- Рассказываю про технологии статического анализа в статьях и на различных IT мероприятиях.



@vlade1k



# 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.



# Алина Ким

Специалист центра кибербезопасности ГК  
"Эшелон"

- Доклад: «Исследование защищенности с помощью Сканер-ВС 7»





# Артём Храмых

Руководитель отдела по анализу защищенности  
АКТИВ.CONSULTING (бизнес-направление Компании "Актив")

- Проводит всесторонние проверки безопасности ПО, внешнего и внутреннего периметра организации, Red Team, расследований киберинцидентов, а также внедрения процесса РБПО (DevSecOps).
- Принимает участие в отраслевых мероприятиях по теме ИБ, делится экспертизой в ведущих деловых изданиях и является постоянным автором TG-канала АКТИВ.CONSULTING.
- Доклад: «Поиск уязвимостей ПО – базовый минимум или роскошный максимум?»



**AKTIV.**  
CONSULTING

# Алексей Морозов

Руководитель Application Security в ecom.tech  
CEO ghack.ru

- Четырехкратный чемпион PHDays StandOFF в составе команды DreamTeam,
- Спикер на многих крупных профильных конференциях.
- Автор научных публикаций и CVE.
- Пентестер, ресерчер, хакер.
- Сертифицирован OSCP, OSWE, CEN. 12+ опыта в аппсек
- Доклад: «Применение AI для триажа и мультиагентных сетей»

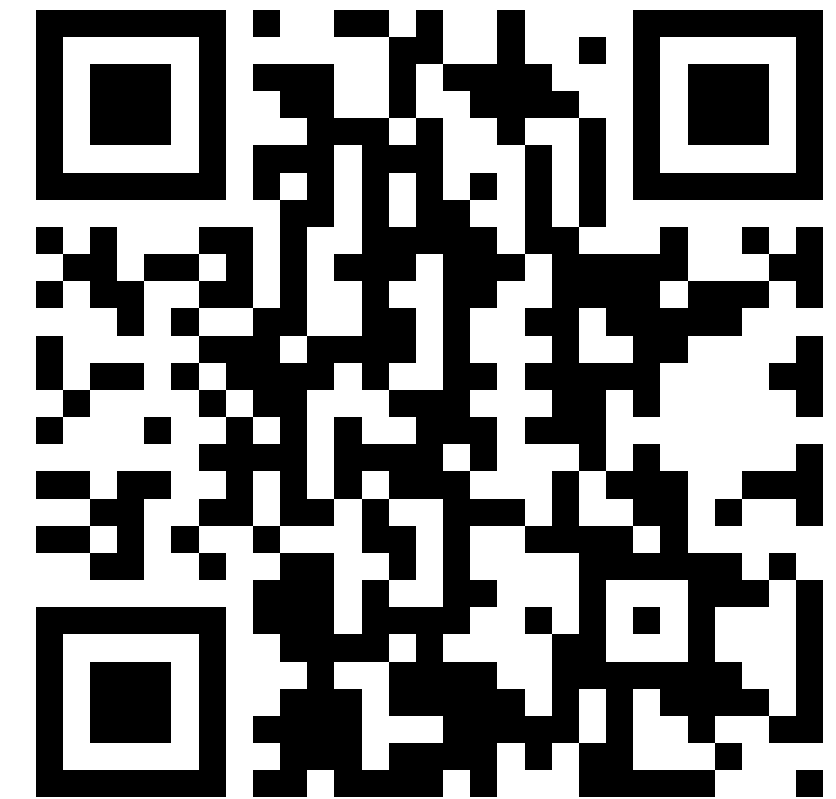


# Вокруг РБПО за 25 вебинаров

8

- Записи предыдущих вебинаров:

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



- Организует УЦ МАСКОМ и ООО «ПВС» (PVS-Studio)
- 25 вебинаров, т. к. ГОСТ Р 56939-2024 описывает 25 процессов для реализации разработки безопасного ПО



# Процесс 24

## Поиск уязвимостей в программном обеспечении при эксплуатации



1. Организация систематического и углубленного поиска ошибок и уязвимостей в ПО при его эксплуатации в целях упреждающего реагирования: обработки ошибок кода ПО и его конфигураций (настроек) до того, как они будут выявлены сторонними лицами и повлекут инциденты информационной безопасности.



## 5.24.2 Требования к реализации

11

1. Разработать регламент поиска ошибок и уязвимостей в ПО при его эксплуатации.
2. Актуализировать информацию об уязвимостях ПО из открытых источников на регулярной основе на всем протяжении срока действия его технической поддержки: выполнять поиск в открытых источниках информации об уязвимостях самого ПО и его сторонних компонентов.

## 5.24.2 Требования к реализации

12

1. Разработать регламент поиска ошибок и уязвимостей в ПО при его эксплуатации.
2. Актуализировать информацию об уязвимостях ПО из открытых источников на регулярной основе на всем протяжении срока действия его технической поддержки: выполнять поиск в открытых источниках информации об уязвимостях самого ПО и его сторонних компонентов.



3. Проводить проверки кода ПО и настроек конфигураций ПО на регулярной основе на всем протяжении срока действия его технической поддержки с целью поиска ошибок и уязвимостей.
4. Оценивать выявленные ошибки на предмет наличия уязвимостей.

3. Проводить проверки кода ПО и настроек конфигураций ПО на регулярной основе на всем протяжении срока действия его технической поддержки с целью поиска ошибок и уязвимостей.
4. Оценивать выявленные ошибки на предмет наличия уязвимостей.



1. Регламент поиска ошибок и уязвимостей в эксплуатирующемся ПО должен содержать:
  - обязанности сотрудников и их роли при поиске ошибок и уязвимостей в эксплуатирующемся ПО;
  - правила поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО, его программных компонентов и сред его функционирования;
  - состав проводимых проверок и периодичность их проведения на протяжении всего срока действия технической поддержки ПО для каждой версии ПО.

1. Регламент поиска ошибок и уязвимостей в эксплуатирующемся ПО должен содержать:
  - обязанности сотрудников и их роли при поиске ошибок и уязвимостей в эксплуатирующемся ПО;
  - правила поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО, его программных компонентов и сред его функционирования;
  - состав проводимых проверок и периодичность их проведения на протяжении всего срока действия технической поддержки ПО для каждой версии ПО.



1. Регламент поиска ошибок и уязвимостей в эксплуатирующемся ПО должен содержать:
  - обязанности сотрудников и их роли при поиске ошибок и уязвимостей в эксплуатирующемся ПО;
  - правила поиска известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях ПО, его программных компонентов и сред его функционирования;
  - состав проводимых проверок и периодичность их проведения на протяжении всего срока действия технической поддержки ПО для каждой версии ПО.

2. Регулярные отчеты по результатам проводимых проверок, в которые включается информация об исправлении найденных ошибок, выпуска обновлений ПО и доставки обновлений ПО пользователям.

# Дополнительные материалы

- Елена Дмитриева. [Обзор программ и площадок баг-баунти в России: практика, кейсы, суммы гонораров.](#)
- TAdviser. [Подборка: Белые хакеры в России.](#)
- РБК. [Как пентестеры помогают бизнесу найти уязвимости в IT-системах.](#)
- Пост в ТГ-канале «Бестиарий программирования»: [Процесс 24 — Поиск уязвимостей в программном обеспечении при эксплуатации](#)



ПЕРЕДАЮ СЛОВО  
СЛЕДУЮЩЕМУ СПИКЕРУ

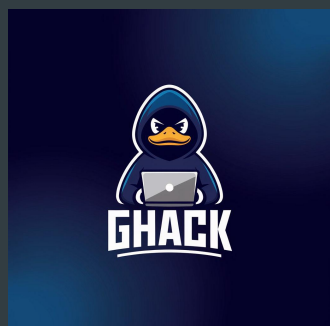




Триальный  
ключ на 30 дней



Пентест с  
участием  
7-кратных  
чемпионов  
Standoff



Скидка 10% на  
курсы «МБРПО»



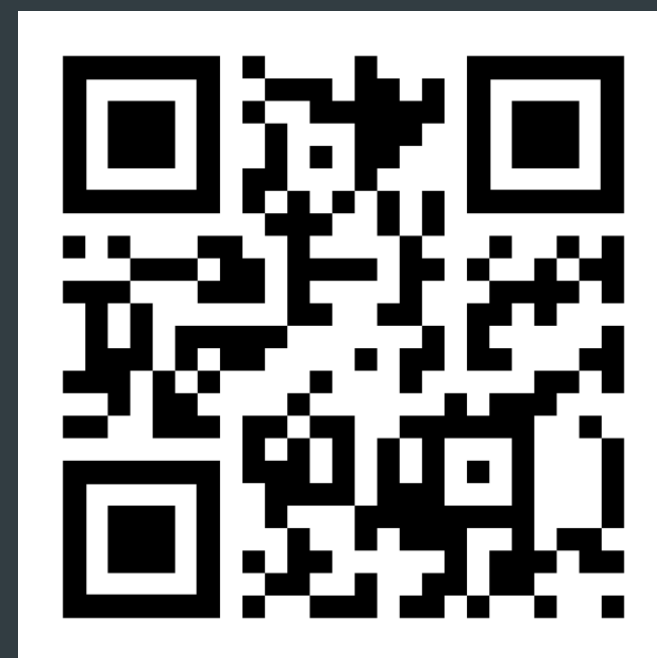
Сканер BC-7



Telegram-канал  
Сканер BC-7



Telegram-канал



Подкаст  
«Безопасный выход»



Сайт



AKTIV.  
CONSULTING