

ВОКРУГ РБПО ЗА 25 ВЕБИНАРОВ

ГОСТ Р 56939-2024

Вебинар 21. Безопасная поставка программного обеспечения пользователям



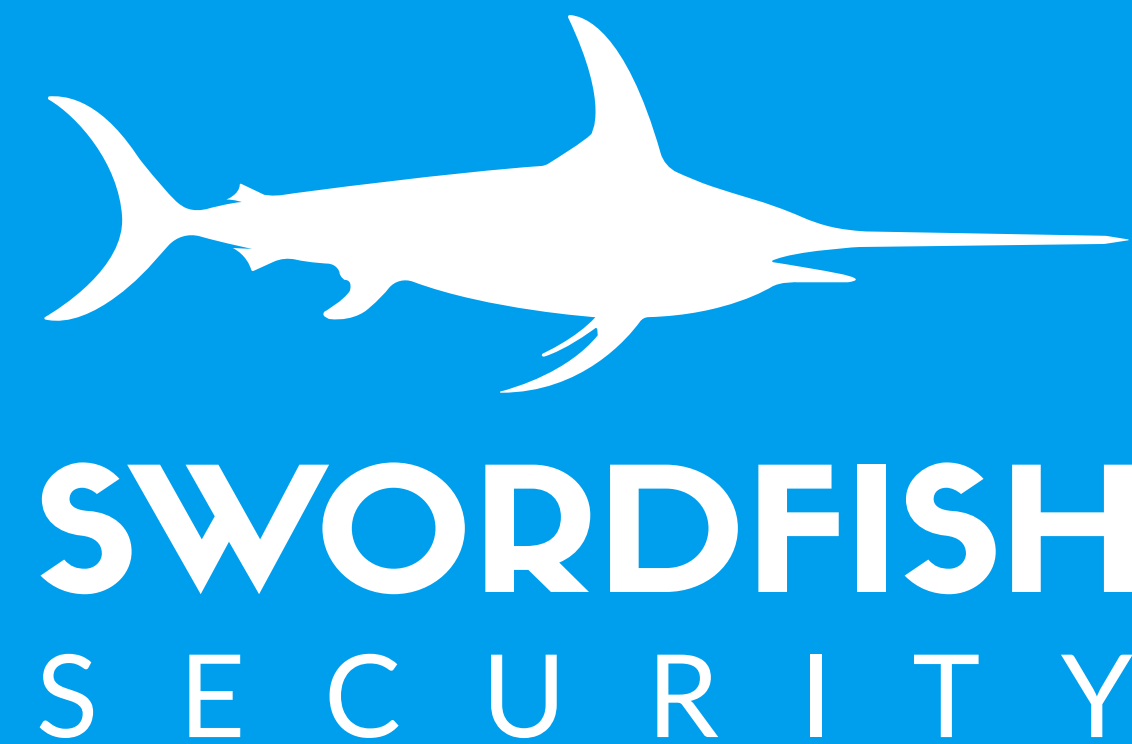
- Виталий Пиков
Учебный Центр «МАСКОМ»
Эксперт в области ИТ, ИБ,
преподаватель
- Андрей Карпов
ООО «ПВС»
Директор по развитию бизнеса
(CBDO)



Мария Рачёва

Ведущий аналитик процессов безопасной разработки в ООО «СВОРДФИШ СЕКЬЮРИТИ»

- Эксперт в области кибербезопасности и разработке безопасного ПО с опытом в отрасли более 15 лет
- Специализируется на внедрении процессов безопасной разработки ПО для бизнеса и государственного сектора
- E-Mail: mracheva@swordfishsecurity.ru



Александр Гадай

Руководитель службы консалтинга в
ООО «СВОРДФИШ СЕКЬЮРИТИ»

- Эксперт в области кибербезопасности и РБПО
- Специализируется на комплексных проектах в области DevSecOps и AI Security



Вокруг РБПО за 25 вебинаров

5

- Записи предыдущих вебинаров:

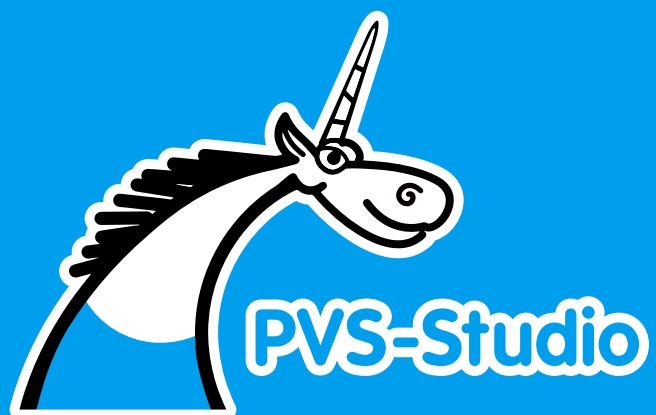
pvs-studio.ru/ru/webinar/rbpo/



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

Процесс 21

Безопасная поставка
программного обеспечения
пользователям



Цель (п. 5.21.1.1)

7

- Обеспечение защиты ПО, в том числе документации ПО, от угроз, возникающих в процессе передачи ПО пользователю.
- Близко к предыдущему процессу 20 – Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения

- **Разработать регламент безопасной поставки ПО пользователям**
- **Фиксировать версии** поставляемого пользователям ПО и соответствующей поставляемой документации
- **Организовать хранение копий** версий поставляемого пользователям ПО и соответствующей поставляемой документации

- **Поставлять ПО вместе с эксплуатационной документацией, содержащей как минимум:**
 - описание штатного функционирования ПО
 - параметров настроек (конфигураций) ПО и среды функционирования
 - действий по установке и настройке средства
 - как с точки зрения штатного функционирования
 - так и с точки зрения обеспечения безопасности

- Здесь нам повезло, т. к. у нас одна ветка релизов:
 - Обновляемый релиз
 - В случае необходимости можем предоставить старую версию
 - Или beta-версию
- Документация PVS-Studio – большой подпроект
- В варианте сборки всей документации в PDF-файл получается 1185 страниц

- Регламент безопасной поставки ПО должен содержать:
 - обязанности сотрудников и их роли при осуществлении безопасной доставки ПО
 - процедуры хранения копий версий поставляемого пользователям ПО
 - процедуры снятия копий поставляемого пользователям ПО
 - процедуры поставки ПО (обновлений ПО, включая обновления безопасности, предназначенных для устранения недостатков, в том числе уязвимостей)
 - процедуры проверки подлинности ПО (обновлений ПО) пользователем

- Сведения о версии поставляемого пользователям ПО должны быть зафиксированы в поставляемой документации
- Сведения о месте хранения копий (подлинников, дубликатов) версий поставляемого пользователям ПО должны быть зафиксированы в документации, например в регламенте безопасной поставки ПО

- Сведения о поставляемой эксплуатационной документации на ПО должны быть зафиксированы, например в регламенте безопасной поставки ПО, в паспорте (формуляре) ПО
- В общем, процесс во многом сводится к содержанию и оформлению документации

- Процесс №4

pvs-studio.ru/ru/blog/video/11398/



- Цели:

- Осуществление уникальной идентификации ПО, документации...
- Контроль реализации изменений ПО, документации на ПО...

- Напомню, что при разработке регламента идентификации ПО (версий ПО) можно оттолкнуться от [ГОСТ 19.103-77](#)

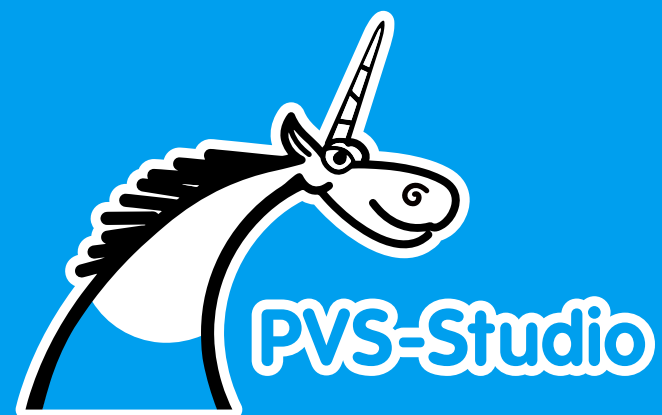
Передаю слово приглашённым экспертам



Мария Рачёва

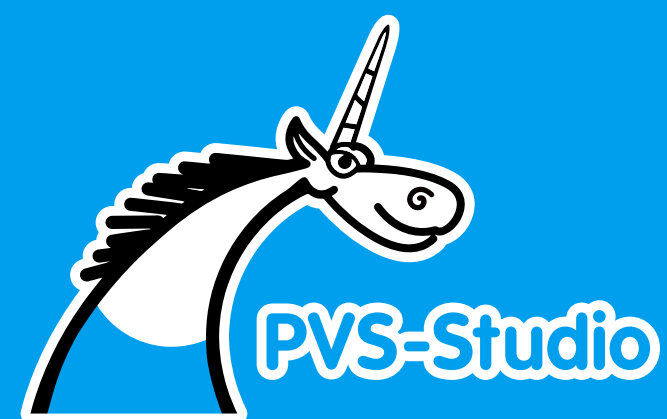


Александр Гадай

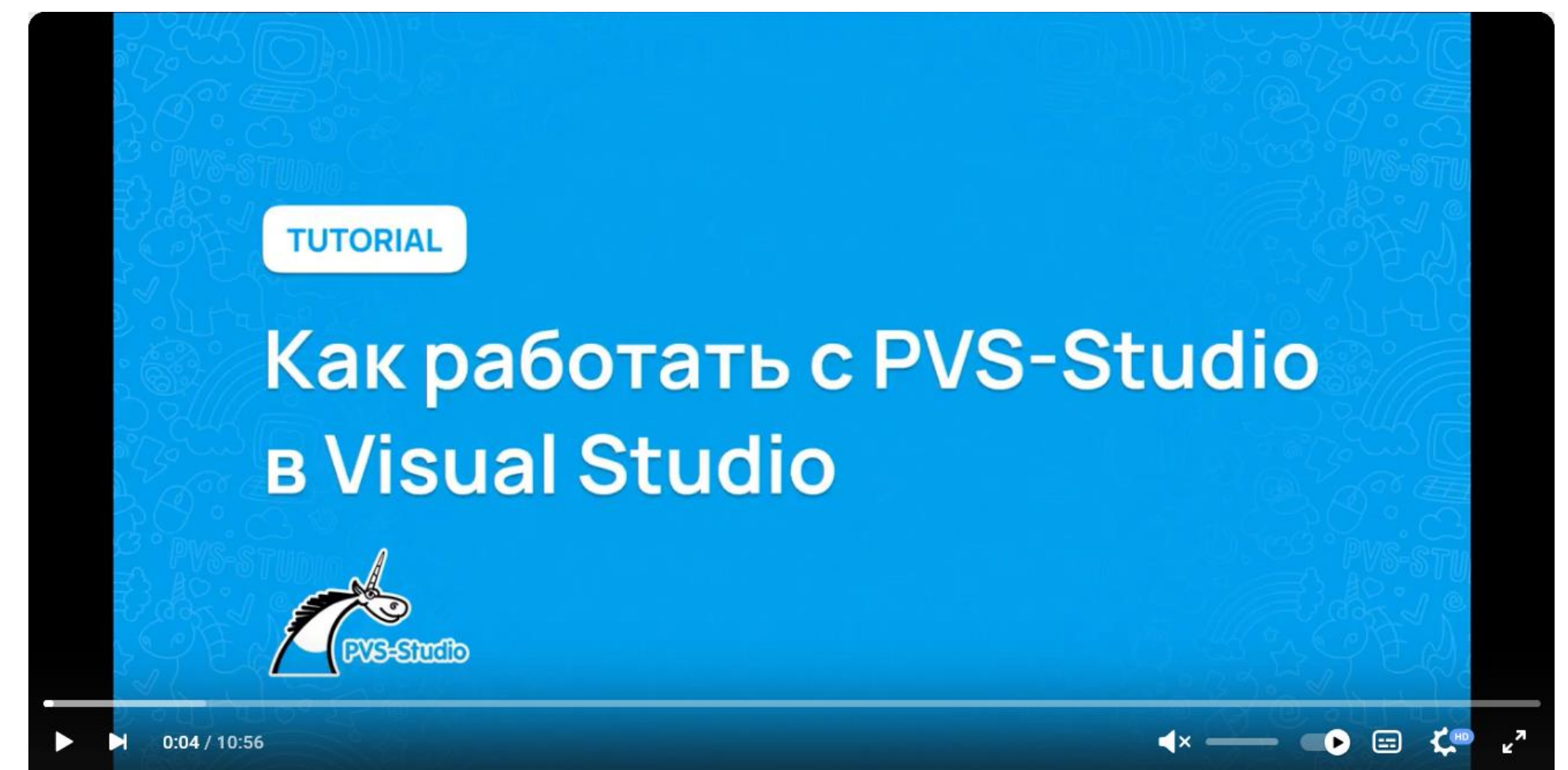


- Сделай свой проект чистым и безопасным вместе с PVS-Studio (лицензия на месяц)
- Получи 10% скидку на курсы «М БРПО» в Учебном Центре «MACKOM»
- **Swordfish Security**
 - Сайт swordfish-security.ru
 - Аудит процесса РБПО по ГОСТ Р 56939-2024
 - Swordfish: SAIMM. Фреймворк оценки зрелости безопасности ИИ

Дополнительная информация



- Статический анализатор кода для поиска ошибок и потенциальных уязвимостей
- Поддерживает: C, C++, C#, Java
- Краткое знакомство:



vkvideo.ru/video-11805870_456239344

- 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**
- Бесплатные лицензии для студентов и преподавателей

- Сайт – swordfish-security.ru
- Аудит процесса РБПО по ГОСТ Р 56939-2024
swordfish-security.ru/audit-rbpo
- Swordfish: SAIMM. Фреймворк оценки зрелости безопасности ИИ
swordfish-security.ru/saimm
- Порядок сертификации процессов РБПО. White Paper
disk.yandex.ru/i/yZG1YLdmO6DERA
- Роль РБПО в промышленной автоматизации. Практические сценарии внедрения. Видео
rutube.ru/video/463f116e86ca1e1e991ff4bbf8112343/?r=wd

Карпов Андрей Николаевич

21

- Карпов Андрей Николаевич, 1981
- ООО «ПВС», директор по развитию бизнеса
- Более 18 лет занимается темой статического анализа кода и качества программного обеспечения. Автор большого количества статей, посвящённых написанию качественного кода на языке C++. Один из основателей проекта PVS-Studio. Долгое время являлся СТО компании и занимался разработкой C++ ядра анализатора. Основная деятельность на данный момент — развитие компании, обучение сотрудников и DevRel деятельность
- [Другая информация и контакты](#)





ПИКОВ
Виталий
Александрович

Общий стаж работы: более 26 лет.

Стаж преподавательской работы: более 10 лет.

Образование: высшее, Тамбовский военный авиационный инженерный институт по специальности «Автоматизированные системы обработки информации и управления».

Заслуженный доцент Российского нового университета, преподаватель высшей школы.

В 2017 году прошёл профессиональную переподготовку в МГТУ им. Н. Э. Баумана по направлению подготовки «Информационная безопасность».

В 2019 году прошёл профессиональную переподготовку по программе «Противодействие иностранным техническим разведкам».

В 2020 году прошёл профессиональную переподготовку по программе «Педагогика профессионального обучения, профессионального образования и дополнительного профессионального образования».

В 2021 году прошёл профессиональную переподготовку по дополнительной профессиональной программе «ТЗИ».

В 2022 году прошёл профессиональную переподготовку по программе «Практическая психология».

Microsoft Certifications Earned: MCT, MCPS, MCSA, MCTS.

Автор более 30 научных публикаций.

Постоянный участник, спикер, эксперт на мероприятиях по информационной безопасности: Positive Hack Days Fest 2, Национальный форум информационной безопасности «Инфофорум», Международный военно-технический форум «АРМИЯ», Международная выставка InfoSecurity Russia, Международная научная конференция «Цивилизация знаний: российские реалии» (РосНОУ) и некоторых других.

Имею награды и звания Минобороны России.

Авторизованный преподаватель по продуктам «Группы Астра» с правом проведения курсов по ОС Astra Linux Special Edition 1.8

Читаю курсы, провожу занятия в области информационной безопасности, защиты информации и информационных технологий.

